Policy-Based Resource Management

Future Internet Program,

Activity 2.4 Deliverable DA2.4.1, 2H2008

1. Introduction

The work of Future Internet Program [1] is divided to five work packages. In this document, the concept work of activity 2.4 – the fourth activity of work package 2 – is described. Activity 2.4 concentrates on Policy-Based Resource Management (PBRM). The high-level and long-term aim of the work is to apply policy-based mechanisms on any network resources and their management. Within activity 2.4, bottom-up method has been selected: in order to start applying concepts on some practical network setup, the work has been concentrated only on radio interface of different wireless technologies during the first Future Internet program project year (lasting till 31st of May, 2009). The idea is to widen the concept for other network interfaces and network elements as well, when the work progresses.

Together with the concept wok of activity 2.4, also a simulation environment has been built. The purpose of the simulator is to verify the developed concepts and compare different options to find the best combinations for all stakeholders. The simulation work continues during the first FI program year, and the results will be documented and published in a separate document at the end of May 2009.

The structure of the document is following: on chapter 2, the reasons why we need PBRM mechanisms are discussed. On chapter **Error! Reference source not found.**, the concept itself is described, as currently seen. Chapter 5 concentrates on known issues with the described PBRM mechanism: in addition to technical issues, there are possibly also economical and even political challenges to solve before PBRM can be deployed in real life networks. Finally, chapter 6 summarizes the document.

1.1 Abbreviations

AAA	Authentication, Authorization, Accounting
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
BTS	Base Station
CN	Core Network
DM	Device Management
DSMIPv6	Dual Stack MIP version 6
EAP	Extensible Authentication Protocol
FI	Future Internet
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HSPA	High-Speed Packet Access
ICT	Information and Communication Technology
LAN	Local Area Network
LTE	Long Term Evolution (3GPP “4G” access technology)

MIP	Mobile IP
NAP	Network Access Provider (WiMAX)
NAT	Network Address Translation
NSP	Network Service Provider (WiMAX)
NWDS	Network Discovery and Selection
OMA	Open Mobile Alliance
PBRM	Policy-Based Resource Management
PLMN	Public Land Mobile Network
PMIPv6	Proxy MIP version 6
RAT	Radio Access Technology
RNC	Radio Network Controller
RRM	Radio Resource Management
SAE	System Architecture Evolution (3GPP CN evolution)
SIM	Subscriber Identity Module
SHOK	Strategisen HuippuOsaamisen Keskus (in Finnish)
SSID	Service Set Identifier
TLS	Transport Layer Security
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN

2. Drivers for Policy-Based Resource Management

Today, the communication networks reach every corner of the world: the Internet can be accessed basically anywhere from the globe. The number of deployed networks, as well as the size and the complexity of the networks, has increased constantly. This poses new challenges on network management and also on resource management. Resource management is a critical function in any network, and it is the intention of the network operator – whatever the network is – to take most of the network investments.

Today’s networks should be able to cope with quick changes in network environment: for example, overload situations can come and go in different parts of the network. Also, new currently unforeseen services may change the user and traffic behavior completely from what the network was initially planned for. This means that the networks should be able to maintain the optimum resource usage also in very dynamic environment, where it is impossible to prepare for all different scenarios e.g. during network planning phase.

With the increased complexity of today’s networks, it comes harder and harder to have only one central point of control for the whole network. Instead, it is often more feasible to have a distributed network management and control system. This also enables different parts of networks to behave independently.

Sometimes, it is either not possible or desirable to have a direct control of a network entity. For example, the network entity may belong to another network domain, or direct control requires too heavy manual work.

For all the above described scenarios, policy-based mechanisms provide a flexible and dynamic solution to manage the networks. For example, general policies can be defined so that they adapt the function of the network based on different (over)load situations. Also, it is not necessary to define separate policies for every single network entity: instead, the same set of policies may be deployed to all the network elements, but the policies affect different network elements based on their unique setup, load situation, etc. in a different way.

2.1 Heterogeneous Wireless Network Environment

As stated on chapter 1, the work of FI program activity 2.4 has concentrated so far on wireless networks. The above described, more general scenarios apply to any type of network, but the nature of wireless networks sets some more specific requirements on policy-based resource management.

So far, it has been proven impossible to build a cost-efficient, single wireless network solution to fit all the different usage models and environments. Instead, various wireless networks designed and optimized for a specific purpose of use – e.g. local area networks – are dominating the current wireless network landscape. It seems that this development trend is not going to change in the near future. Thus, wireless network operators might have - and some operators already do have – several wireless access technologies in their service offering. This is called heterogeneous network environment. Of course, heterogeneous networks can span over a number of operator networks, i.e. heterogeneous network environment can be formed by any number of operators, as shown in Figure 1.

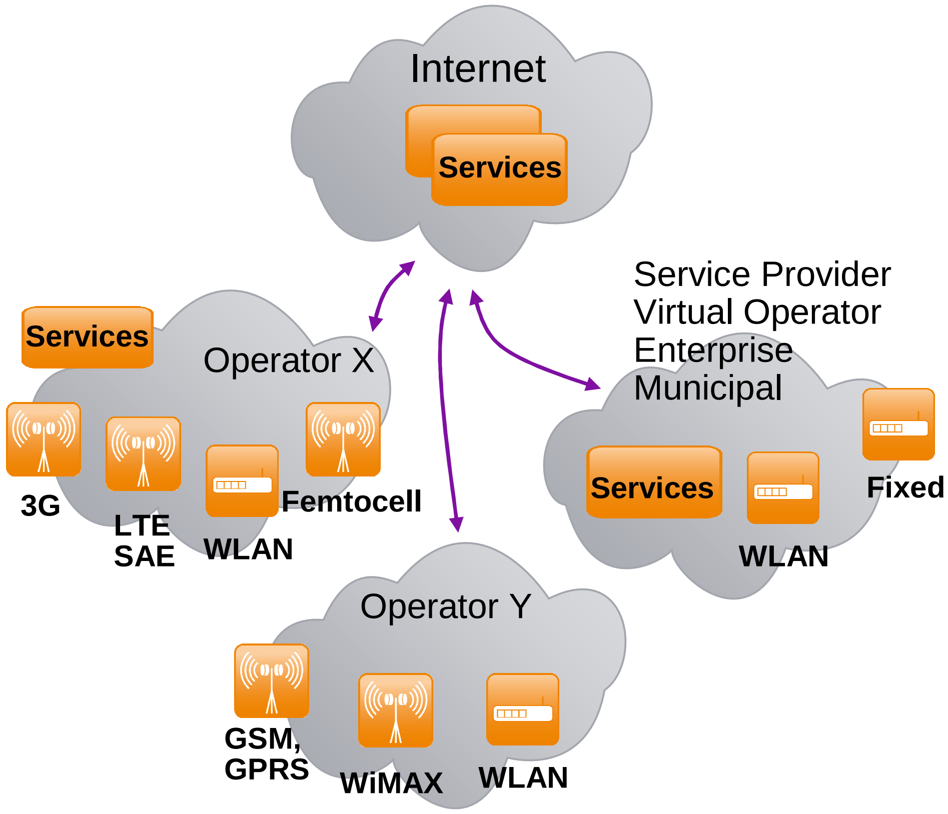

Figure 1. Heterogeneous network environment.

Usually, for each separate wireless network technology, different network operations – like network discovery and selection – are well defined. However, they are only defined within that specific technology. For a heterogeneous network environment, there is currently no standardized and deployed solution for Interworking between different networks. At the moment, this is basically left for users and terminal manufacturers to decide what network to use and when.

From network operator point of view, this is far from optimal solution: since the operator owns the networks it operates, the operator should also be allowed to affect how its networks are being used. For example, operator should have tools e.g. to control overload situations, guarantee necessary service level for its subscribers, etc. Policy based resource management provides light-weight solution to enable this, as described in more detail in chapter 4.

3. Policy-Based Decision Making in General

Before going to the description of PBRM itself, first some background information about general policy-based decision making is given.

Today’s networking environments have to accommodate various access technologies, have to cope with dynamic subscriber population and have to support versatile service provision. Therefore, these environments are dynamic and complex. In view of the existing complexity and the anticipated further increase of the complexity in the future, pre-defined and static behavior cannot meet the complex and dynamic operator and user needs. As such, techniques are needed which help to automate and to optimize the realization of network and service functions as well as the operation of the networks or the network entities involved.

This can be achieved by a policy-based approach to realize a flexible and dynamic system behavior. Using policy-based approach, the actual functionality of a system and the policies which govern its behavior are separated.

Policies are a form of guidance used to determine decisions and actions. In general, a policy is a formal set of statements that define e.g. how the network's resources are to be allocated. Basically, policy can appear in various forms: ideally, policy statements can be written with natural language, like:

Give gold-users highest available bitrate

In practice, policy-based mechanisms require more artificial language.

Decision points are the entities in the network that make decisions based on the policies and the related input information. For example, the service/management/mobility behavior can be altered by changing some of the policies or by activating a new set of policies. The general information flow for policy-based decision making is illustrated on Figure 2

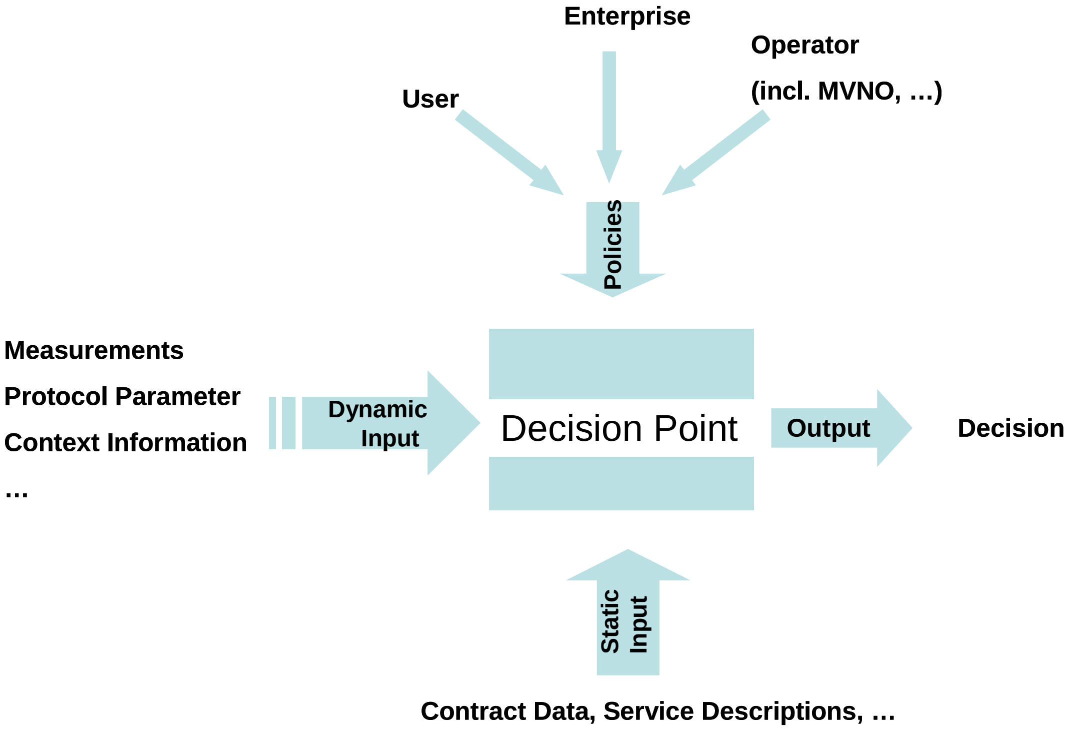

Figure 2. General Policy-Based Resource Management decision process.

As is shown in the above figure, the decision point is responsible for “calculating” the required actions. It is configured with policies and static information such as subscriptions of a user. During run time the decision point is triggered by dynamic inputs (“triggers”). Based on the triggers and the static configurations, the decision point calculates the optimal decision according to its policy rules.

Basically, the above described decision point can reside in any part of the network. There also may be arbitrary number of decision points in a network. As discussed further in chapter **Error! Reference source not found.**, PBRM mechanism assumes that the policies are delivered from the network to the terminals, and the final decision point for PBRM resides in the terminal.

4. Policy-Based Resource Management Concept

For each network, the resource allocation and management is normally well defined within that network. For example in 3G networks, a specific entity called Radio Resource Management (RRM) – located in RNC – is responsible for managing all the radio resources in the area of that RNC. Also, core network resources are efficiently managed.

When designing the network, the operator tries to achieve an optimum network setup in terms of available capacity and spent money. This kind of procedure works well, if the operator is in beforehand able to predict what kind of traffic there will be, how much and in what parts of the network most of the traffic will happen. If there is a sudden increase of traffic in some part of the network, there is not much the operator can do to fix the acute problem. In longer term, operator may of course install new hardware to increase capacity.

In a heterogeneous network environment, it is possible to balance the network load between multiple networks. For example, if a cellular network gets congested, the operator could guide certain number of users to use some other network, e.g. available WLAN network. Another, related interesting idea is to take advantage of the numerous home WLAN access points (APs): when the user enters the vicinity of his/her home, network instructs the user (i.e. the terminal) to access the home WLAN AP for any services.

Current networks do not support above described scenarios. To introduce this to the existing networks, we can use Policy-Based Resource Management (PBRM). In order to support users accessing different networks from their terminals, we need to have a solution to at least the following issues:

1. Network discovery and selection: in order the terminals to use any network, the network has first to be discovered and then successfully accessed.
2. Mobility support: normally, terminal mobility is well defined within a wireless technology: for example for the intra-system handovers, there may be resource reservations involved in the target cell/AP etc. However, mobility across network boundaries is much more difficult. In minimum, support for changing IP address is required.
3. Service continuity: when changing from a network to another, it is not guaranteed that the user can continue using the same set of services without any interruptions. It is also possible that a service does not work via any other (wireless) access network. Network should not guide a terminal to a network that does not support subscriber’s services.

All the above listed issues are wide topics, and there is extensive research and development associated with every issue. The work of FI activity 2.4 concentrates most on the first issue. In this document, there is also some discussion about the two other topics.

4.1 Network Discovery and Selection

Network discovery and selection (NWDS) are basic procedures in any wireless technology: before any network services can be used, terminal has to discover the available networks and then select the most suitable one(s) for the service in question. Currently, almost all multiradio-capable devices leave the network selection for the user, leading to complex and cumbersome user experience when operating in heterogeneous network environment. For example, if a user starts web browser on a terminal, the user is requested to select what access network should be used. While some users might find selecting the network interesting, an average user is not willing to select access technology every time a new application is launched. Thus, the network selection should happen automatically, without user intervention. The target of PBRM is to make NWDS an automatic process.

4.1.1 Responsibility Split between Terminal and Network

Generally, neither terminal nor network can make an optimized network discovery and selection alone without the help of the other. Terminals and networks have limited view of their environment, so in optimal case strengths of both terminal and network need to be utilized in discovering and selecting networks. This avoids introducing unnecessary complexity into both terminals and networks. The terminal is well-positioned to have knowledge for the requirements of ongoing services and device capabilities for using different networks. The network is well-positioned to know neighbors, service availability and overall network information, such as network load.

In today's networks, cellular networks and WLAN networks represent the two extremes in network selection within the radio access network: in cellular networks, the mobility of the terminal is tightly controlled by the network, whereas in WLAN it is completely up to the terminal to decide what AP – or network – is chosen. Mobility within and between 3G networks works very well, but in WLAN the mobility is far from perfect.

However, what works well within a radio technology, might not work when making a selection between radio technologies. If we want to enable the network to have full control on the selection of the access network, terminal should provide various kind of information to the network about itself:

- Services being run and their QoS requirements: in order to enable the network to choose the best network for the terminal, the network needs to know the current services terminal is running. Also, the QoS requirements for each service is required, at least some basic ones like throughput, delay and jitter.
- Terminal multiradio capabilities: network needs to know what network technologies terminal can support.
- Security requirements: in minimum, this information defines does terminal require encrypted radio interface or not. For example, most of public WLAN hotspots do not provide encryption. If the security is implemented on application level for all the services, this information can be omitted.
- Neighbor networks visible to the terminal: network should know where the terminal is in order to select an access for the terminal.
- Mobility status: in minimum, terminal should tell to the network the speed and direction of its movement. For example, if terminal is moving faster than pedestrian speed, network should not select WLAN network for the terminal (unless the WLAN network happens to have wide coverage on the area).

With the information above and the information available from the network (e.g. load status of different BTSs/APs), the network may control the network selection of the terminal. However, even if all this information was available and possible to transfer from the terminal to the network, it would unnecessarily increase the complexity of network and terminal implementations compared to benefits gained. Thus, a full-blown network-controlled network selection is not currently seen as feasible option in a heterogeneous network environment. However, network-controlled network selection (or handover) would ensure for example voice call quality during mobility and thus can't be completely excluded.

If the network selection is left completely to the terminal – as many terminal vendors would like it to happen – controlling the network usage comes a problem: for example, it is only the network operator that is willing and capable of taking care of even traffic distribution and congestion avoidance in its networks, network users should not be responsible for that. Also, if a virtual mobile operator e.g. leases cellular capacity from another operator but has also his own WLAN network available, the virtual operator may want to guide his subscribers to use the most profitable network, i.e. his own WLAN network. In order to enable such guidance for network selection, the network should have some mean to affect the terminal's network selection.

As a bottom line, for the optimal network selection both terminal and NW have to be utilized in a well-controlled way.

4.2 Policy-Based Resource Management for NWDS

As described on previous chapter, several factors have an impact on network discovery and selection (NWDS): radio quality, terminal capabilities, application requirements, network load, operator preferences etc. When network does not need to consider information local to terminal (i.e. information that is kept only within the terminal), less complex network implementation is achieved. However, network should provide its view on NWDS to terminal to give an operator some control on network selection. The following model enables this:

1. The network provides information to help terminal in NW selection from PBRM server. Operator can define this information so that it proactively distributes traffic across the operator's networks. The network provides this information to terminals either automatically (push) or on request (pull). This NW selection information provided by PBRM server is referred as policies.
2. Taking advantage of the policies, terminal makes the final decision for NW selection based on its application requirements and multi-radio capabilities.

This kind of model assumes the control is on terminal, i.e. we are talking about terminal-centric, network-assisted model. With the model, minimal complexity is introduced, and existing terminal and network capabilities can be utilized. The model is illustrated on Figure 3.

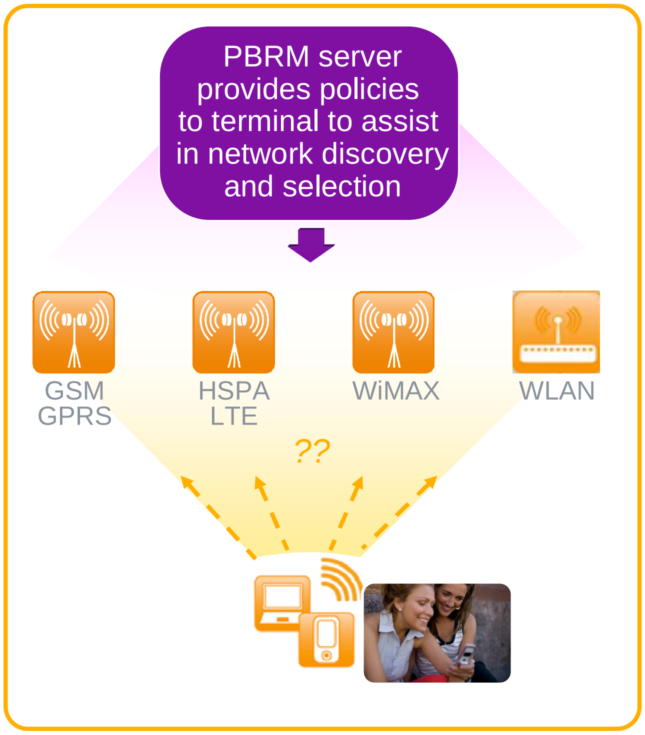
PBRM server provides policies to terminal to assist in network discovery and selection
GSM GPRS
HSPA LTE
WiMAX
WLAN
??

Figure 3. PBRM model for network selection.

Basically, policies indicate what networks the operator wants its subscribers to use. As an example, a policy can be in its simplest form “Use WLAN with SSID=Operator_A, if available”. The policies can be static or they can be dynamically changed e.g. based on load situation in the network. Also, policies can be general and the same for all the subscribers, or they can be specific for subscriber groups (e.g. “gold” user policies) or specific for each subscriber. More detailed discussion about policies can be found from chapter 4.3.

It is important to note that it is also possible to use these same policies for inter-system (inter-RAT) handovers as well. With the policies used for NWDS, terminal may also be instructed how to execute inter-system handovers. If PBRM functionality is used together with NW-assisted/controlled handover, PBRM and handover control shall give the same result: the initial network selection cannot be separated from the consecutive network selections (i.e. handovers).

For the actual network selection, there may be other tasks to complete before successfully accessing the network is possible: for example, GPRS settings or WLAN security settings may be needed on terminal before network access can be made. For this, PBRM server may co-operate with e.g. Device Management (DM) that can be used to deliver various device settings automatically to terminal. DM is defined by Open Mobile Alliance (OMA), and it is currently widely used by e.g. operators to provide uniform and working settings to the subscriber’s terminals for various applications. The topmost DM specification is [10].

4.2.1 Transporting PBRM Information

The PBRM policies can be delivered to terminal in many ways. First, the policies can be pre-provisioned to the terminal (e.g. SIM card) by the operator. However, this does not cope that well with any changes on network. So, better option is to enable the network to update the policies on the terminal. For this, either L3 or L2 solution can be used. In practice, L3 solution would be implemented using IP, and L2 using message transport provided by a specific radio access network, e.g. dedicated radio channels on 3G systems.

Preferably, PBRM information should be possible to deliver with both push and pull mechanisms. With push model, the PBRM server uses some push mechanism, e.g. broadcasting method specific to a radio access network, to inform the terminal or all the terminals about new PBRM information. With pull model, it is the terminal that initiates the PBRM information delivery by explicitly requesting information from the server.

When introducing PBRM functionality into a network, traffic in the network is increased by the PBRM signaling. The total volume of increased traffic is affected by the number of messages sent during a given period and the average size of the messages. Since every terminal is performing its own information request individually, the number of requests sent to PBRM server increases proportionally to the number of terminals in a system.

The amount of transferred data is probably not a problem for the network. However, this might be an issue, if the operator implements charging based on transferred bytes. The users are not willing to pay extra money for signaling, so an alternate solution should be found. One possibility is to leave PBRM messages out of the charging. However, this increases the complexity of the charging and might not be feasible from the operator’s point of view, especially when the subscriber is roaming in a visited network. Using overlay solution would fit best to flat rate charging, where introducing additional signaling does not bring any new costs for the end users.

4.2.1.1 L2 Solution

The main benefit of L2 solution is that it is relatively easy to provide the location of the terminal to the PBRM. For example, if terminal is using a WLAN AP as its radio access, the location of the terminal can be estimated within accuracy of couple of tens of meters (given that the location of WLAN AP itself is known). With cellular networks, the cell size may be pretty big (kilometers), so the location estimate of the terminal might not be very accurate, if no other location mechanism is in use. However cell id would be natural location information already providing substantial limitation to available neighboring options.

L2 solution also enables terminal to access PBRM before making actual radio network access. This may accelerate PBRM request considerably compared to L3 solution. However, with the current plans, this will only be possible for WLAN (refer to [2] for more details).

When using L2 solution, it is possible to use the existing security infrastructure provided by the system. No additional security mechanisms are needed; instead, PBRM will be integral part of the network functionality. This avoids introducing extra network complexity in the form of security mechanisms compared to L3 solution.

The biggest issue with L2 solution is that it is required to be specified for each radio technology separately. For existing, legacy networks it is, however, practically impossible. Thus, in the best case, L2 support for PBRM may be provided only for future networks (including WLAN), but not for the existing.

Another issue with L2 solution is that it cannot be used for organizations that do not have their own physical network (e.g. service provider or virtual network operator). Also, accessing remote PBRM servers might be problematic (e.g. when roaming, terminal cannot access home PBRM).

4.2.1.2 L3 Solution

L3 solution requires that terminal has an active radio connection to network. As long as the terminal has active L3 connection open, it is consuming battery. This means that the time for active connection to the network needs to be minimized.

One of the main benefits of L3 solution is that it can be deployed in practice on any network. Basically, such an L3-based overlay solution requires only deployment of a PBRM server and corresponding support on terminals. It is not necessary to apply any changes on other network elements, so this kind of overlay solution is relatively easy and cheap to introduce into an existing network.

In L3 solution all PBRM messaging is transported on IP, so PBRM can be contacted also when terminal is roaming, as long as terminal can address PBRM from a visited network. With L3 solution, it is also possible to deploy PBRM by an organization not having its own physical network (e.g. enterprise, service provider or virtual network operator).

One issue with L3 solution is the lack of any inherent location information: since no location information is automatically carried in L3 packets, terminal (or NW) has to provide it separately for location-based information queries, if location-based PBRM services will be used.

With L3 solution, terminal has to send the information request directly to the PBRM. Thus, terminal has to have means to figure out the address of PBRM, also when roaming. For this, there are several possibilities: the address of (home) PBRM might be pre-provisioned to the terminal, network might broadcast the address of PBRM (e.g. in system info messages in cellular systems, beacons in WLAN, etc.), or the terminal might use DNS and/or DHCP for solving the PBRM address.

Due to its easier deployment to the existing networks, L3 solution is currently seen as better option for PBRM information transport.

4.3 PBRM Policies

The specific usage of PBRM functionality directly impacts what information is transferred between terminal and PBRM server. Basically, the information PBRM server provides can be divided to network discovery and network selection information.

Terminals can use network discovery information to facilitate network discovery procedures, i.e. scanning: for example, network discovery information may contain radio related information, e.g. possible frequency band(s) and channel(s) to speed up the scanning process.

Network selection information is often referred as policies. Basically, network selection information defines what networks terminals should use when making the initial access or inter-system mobility decisions.

4.3.1 PBRM Information Flow

The easiest way to make PBRM information provision to work in heterogeneous network environment is to use simple client-server solution with information exchange on top of IP. This way, all the peculiarities of different network technologies can be ignored. On Figure 4, a general message flow for PBRM information query is shown.

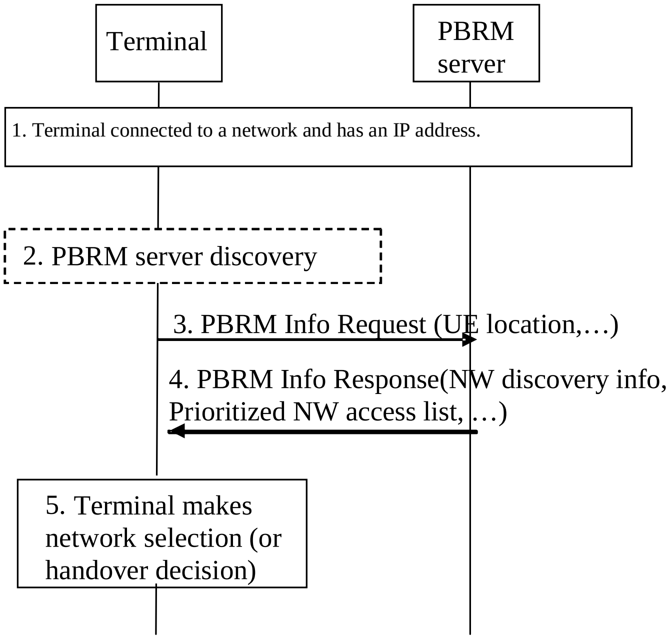
Terminal
PBRM server
1. Terminal connected to a network and has an IP address.
2. PBRM server discovery
3. PBRM Info Request (UE location,…)
4. PBRM Info Response(NW discovery info, Prioritized NW access list, …)
5. Terminal makes network selection (or handover decision)

Figure 4. Simple PBRM information request message flow.

On the following, each step is briefly described:

1. Before terminal can access PBRM server, terminal needs to have an access to a network with connection to PBRM server. Also, an IP address has been allocated for the terminal. This may sound a bit contradictory: before the terminal can make a query for network discovery and selection information, terminal has to have made a successful network discovery and selection to get the information. In practice, this means that terminal has to have default PBRM information for initial network access. Further, PBRM information from network has to be valid and usable also some time

after PBRM information query itself, i.e. PBRM information is meant to be used for future network selections.

2. Since PBRM information is accessible from a certain IP address, terminal has to discover the server. For this, standard IP mechanisms can be used, e.g. DNS, DHCP and EAP extensions are possible solutions.
3. Terminal initiates PBRM information query with request message. Terminal should send this message at least when it is switched on, and the message may be sent also after other triggers, e.g. when a new application is launched, etc.
4. PBRM server replies with response message. The message may contain separate information for network discovery and network selection. The content of the message is discussed with more detail on chapters 4.3.2 and 4.3.3.
5. Terminal utilizes the received information. If PBRM server returned discovery information (e.g. to define used radio channels for a specific network), terminal can take advantage of this in searching – i.e. scanning – for networks in the area. If PBRM information defines network selection information (e.g. prioritized network lists), terminal shall take the information into account in subsequent network selections. Terminal can also utilize network selection information in inter-system handover decisions. PBRM information should have some validity constraints (time, location); when PBRM information is valid, previously queried PBRM information can be used for future network selection decisions.

In the following two sub-chapters, the PBRM information for both network discovery and network selection is discussed in more detail.

4.3.2 PBRM Network Discovery Information

With the network discovery information, terminal can reduce the amount of scans. When the network IDs (e.g. SSID for WLAN) and used channels are known, terminal can limit the scanning only for those networks. For example, if terminal knows the SSID and channel of a WLAN network, it may use active scanning (i.e. send the Probe message to AP) instead of passive scanning (listening through all the channels to find out the active APs). Even bigger gains can be achieved with WiMAX: with the current implementations on market, full scan of the whole WiMAX spectrum may take up to 15 minutes to complete. With the network discovery information, scanning is faster and consumes much less battery.

On the following table, the potential parameters for network discovery information are described.

Parameter type	Description
Network type	Defines the type of network, e.g. 3GPP WCDMA, WLAN, etc. If the response defines networks to scan, this is parameter mandatory. **Applicability:** Needed
Network ID – SSID – WiMAX NSP IDs,	Defines the network ID terminal should try to discover. This network ID is only used with NW discovery, not for NW selection. This may also be a list of network IDs. If the response defines networks to scan, this parameter is

NAP IDs	mandatory. **Applicability:** Needed e.g. for WLAN and WiMAX, not applicable for 3GPP due to its strictly defined PLMN selection procedure.
Channel information – Freq. band and channels for WLAN – Channel plan for WiMAX	Frequency band and used channels, according to used access network type – or information used to find correct frequency and channels. If the response defines networks to scan, this parameter is mandatory. **Applicability:** Needed
PLMN access info	Defines to what networks (i.e. 3GPP PLMN IDs, WiMAX NSP IDs) this network provides access. If the response defines networks to scan, this parameter is mandatory. **Applicability:** Needed
Network capabilities	Defines network capabilities, e.g. .11g etc. for WLAN networks, or supported features for 3GPP networks. **Applicability:** Questionable
Validity – Location – Time	Defines where/when the information in this message is valid. If terminal provided location in info request, also response is restricted to certain geographical area. Validity field may also indicate that the information is always valid (until new information is acquired from PBRM server). **Applicability:** Needed

Table 1. PBRM parameters for network discovery information.

4.3.3 PBRM Network Selection Information / Policies

With network selection information, operator may influence the network selection decisions of terminal: PBRM server provides network selection policies to terminal that then utilizes the provided information when making the final decision on network selection. In this context, inter-system handovers are considered network selections as well, i.e. terminal can apply network selection policies in inter-system mobility decisions too.

When making the network selection, terminal has to take into account various parameters: application requirements, available access networks, link quality for each access, network selection policies, etc. If PBRM server provides prioritized network access list as policy, terminal could utilize policy information for example like this:

1. From the highest priority network, check if radio link quality and load status (if available) could fulfill the application requirements (e.g. by estimating probable bitrate achieved in the given situation).
2. If yes, select that network.
3. If not, continue to the next highest priority network.
4. If no prioritized network access can fulfill the current requirements, select the best network based on signal quality (and load, if available).

It is up to the operator (or other entity offering PBRM services, e.g. enterprise) to define the network selection policies and what network is preferred over the others. Depending on the exact contents of the network selection policies, they may be very simple (e.g. a prioritized list of operator's networks) or more complex. Simple policies can easily be configured even manually, but for more complex policies some automatic mechanism is required. For example, if load information is included in the policies, PBRM server needs to collect load information more or less real-time. On the following table, the potential parameters for PBRM Info Response message with network selection information are described.

Parameter type	Description
Response type	Defines if the response contains NW discovery or NW selection information, or both. **Applicability:** Needed
Network selection policy	Defines the network selection policy, look at Table 3. **Applicability:** Needed
Blacklist	List of access networks that are not allowed to access. **Applicability:** Maybe needed
Validity – Location – Time	Defines where/when the information in this message is valid. If policy includes dynamic information (e.g. load information, or the policy is constructed based on load info), the validity time/location is pretty short/small. **Applicability:** Needed

Table 2. PBRM parameters for network selection information.

In minimum, PBRM policy should define prioritized list of network accesses to the terminal. Whether the policy should include e.g. some dynamic information, like load, is still under study. Within FI activity 2.4, different policy contents are compared by simulations. The following table shows some possible parameters that are seen as important. The policy itself is a list of the following parameters (one list item for each network).

Parameter type	Description
Network Info – Network type (M) – Network ID (O) – Priority (M)	Defines the type of network, the network ID (SSID, PLMN ID, WiMAX NAP ID) and priority for this network selection item. **Applicability:** Needed
List of AP (/cell) IDs – MAC address	List of AP (/cell) IDs associated with a specific Network Info. For some use cases, it is required that a unique identifier for AP (/cell) is available. For example, if PBRM provides information for the home WLAN APs, the only unique identification is the WLAN AP MAC address. **Applicability:** Maybe needed
Load information (associated with AP/cell)	Load information is associated with a specific AP/cell. In order to optimize terminal network selection, terminal should know load status of each candidate AP/cell (or network). Together with link quality information, terminal can better estimate the service an access network can provide. Load information could be provided from PBRM server in policies, or broadcast on

	radio interface (e.g. beacon in WLAN). **Applicability:** Maybe needed
Policy info per application / application class	Network selection policy may also be bound to a certain application or application class (or priority/QoS class). For example, policy could define “use Network_type=WLAN for video”. **Applicability:** Maybe needed

Table 3. Possible data types for network selection policy.

4.4 PBRM Security

Security is about confidentiality (encrypted traffic), integrity validation, authentication of the peers, anti-replay protection and non-repudiation.

PBRM information needs to be trusted as this will influence user behavior. Malicious information may lead the device to connect to untrusted networks, even though the user thinks he is using trusted network. This will expose the user data to third parties, who should not have access to it. Even if the network provides correct service, there could be better networks to use, either by service quality or service cost. At minimum, counterfeited information will lead to decreased user happiness.

Device must be able to authenticate the PBRM server. The server may wish to authenticate the device too, but this mandatory only if PBRM information contains user identity. Data integrity must be preserved. Device must know that data has not been tampered by any means available. Secure e2e communication is mandatory for any type of PBRM information exchange.

Depending on the implementation, there are several security mechanisms that provide the features described above. For example, if the device is 3GPP capable, it has SIM or USIM smart card. These cards hold pre-known secret, known only to the operator. This could be basis for user authentication. EAP-SIM and EAP-AKA are respective authentication mechanisms for this purpose. EAP-AKA can also provide network authentication. By using this information, PBRM could work without any additional credentials; it would be ready to run immediately once installed. RADIUS would be used to convey the EAP messages between the PBRM server and operator AAA server. It is the AAA server, which authenticates the user.

Also, IPSec and TLS based solution can be used. TLS/IPSec schemes provide also anti-replay protection, non-repudiation and also protection for service denial type of attacks.

4.5 IP Mobility and Session Continuity

Seamless handovers require mobility support (e.g. Mobile IP). Applications should continue working even if low level radio connection is changed. Mobile IP (MIP) is one generic framework to achieve this. IPv4 networks are predominant currently, but IPv6 will emerge as

IPv4 address space is estimated to be fully consumed within 3-4 years. Solution must work in both IP address environment seamlessly. Dual stack MIP version 6 (DSMIPv6) [3] is compelling solution, and is being considered by 3GPP for LTE networks. This requires support from both terminal and network as the mobile IP tunnel is created between terminal and Home Agent.

Another option also considered by 3GPP is to use Proxy MIPv6 (PMIPv6) [4]. Here the terminal tunnel endpoint is moved to access network. PMIPv6 has mechanisms to support also IPv4 addresses in the terminal [5]: To keep the terminal address same through all interfaces, the access networks supporting PMIPv6 will assign same IP address to the terminal in all radio interfaces during mobility. Application layer connections remain alive even though radio interface is changed. CDMA and WiMAX networks implement PMIP as internal mobility enabler.

One possibility is to take care of IP mobility completely inside the terminal. This requires support from the applications, as the application itself (especially the peer) must be able to recover from temporary connection loss. For example, application from the terminal provider will probably have local IP mobility support, but applications downloaded from the Internet may or may not support it. If there is no support for either MIP or local IP mobility support, there is no IP service mobility and applications stop working after a handover.

4.6 Related Work

There have been two standardization activities related to the PBRM concept described in this document. In 3GPP, Access Network Discovery and Selection Function (ANDSF) is being standardized (refer to [6], [7], [8] for details). ANDSF is introduced in 3GPP Rel-8. ANDSF work within 3GPP will also continue for Rel-9 during 2009. ANDSF is based on L3 solution, and there is an ANDSF server that provides network discovery and selection information to the terminals. The information ANDSF provides is only basic, there is e.g. no dynamic information included. This also restricts how ANDSF is used: it is assumed that the terminals pretty seldom contact the ANDSF server and update the information. Thus, ANDSF is not meant to be used e.g. during handovers.

Another related standardization activity is run in IEEE. Working group 802.21 defined somewhat similar framework, but it was meant also for controlling handovers between different networks in heterogeneous network environment. 802.21 specification [9] defined also a similar mechanism to PBRM for network discovery and selection. Currently, it seems that there will be no implementations for 802.21, but that does not seem to hinder further developments too much. The main problem of the work was that it was conducted without any link to existing real networks and their specification, i.e. no 802.11, 3GPP or 802.16 working groups were contacted during the work. The result is a too academic approach without link to real life networks, and thus the specification is not well suited for real implementations.

5. Known Issues

Since the concept of PBRM spans over a number of network technologies, and possibly also over a number of operator networks, there are both technical and non-technical issues that should be solved before PBRM can be deployed on real networks.

The composition of an operator's network is an important asset for the operator: some operators may be reluctant to give any information that would expose their network structure to a terminal. Especially for roaming terminals, the operator might want to have confidence that the information is not misused. However, if the information PBRM provides is managed by an operator, at least some of these concerns should be taken care of.

For technical issues, this document hasn't concentrated e.g. on authentication or charging. For example, if PBRM guides terminal to another network, the terminal should be able to perform the authentication also via the new access network and get the access working. Currently, this cannot be guaranteed, and basically the only way to find this out is to try the network: if it is possible to authenticate via new network, then it is ok to use that, but if not, then something else should be tried. The reasons for failing authentication may be outside of operator power to change: for example, some intermediate operator may drop the authentication messages, or they are not sent from the new AP forward in the first place. Also, intermediate firewalls and NAT boxes may block the packets without any indication to the UE.

Also charging may have significant impact on PBRM: first of all, PBRM information should not cost extra for the subscribers. Secondly, the networks PBRM recommends to use should not cost more than alternative networks (i.e. those networks that would be used without PBRM). In order to guarantee no extra costs incur for PBRM-recommended network usage, the operators should employ flat rate plans.

6. Summary

In this paper, the concept of Policy Based Resource Management (PBRM) is described. For the network operator, PBRM concept gives tools to influence how the subscribers use the operator various networks. For the users, PBRM enables easy and smooth experience also in a heterogeneous network environment: with the PBRM server deployed, the users can concentrate on the services, not on the peculiarities of different radio access technologies.

One of the biggest benefits of the PBRM concept is that it is a light-weight solution for both the terminals and the networks. PBRM usage logic is relatively straightforward; the basic PBRM functionality can be achieved with a simple server implementation and minimal changes to the terminal implementation.

When deploying PBRM as L3 solution (on top of IP), the PBRM concept can be used basically on any network available today or tomorrow.

7. References

[1] ICT SHOK Future Internet Programme (ICT SHOK FI), Programme Plan 1.4.2008-31.3.2010, Draft 9.3.2008.

[2] Draft Amendment to Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: IEEE 802.11 Interworking with External Networks, IEEE P802.11u/D1.0, IEEE

[3] Internet draft, Mobile IPv6 support for dual stack, Hosts and Routers (DSMIPv6), November 2007, http://tools.ietf.org/id/draft-ietf-mip6-nemo-v4traversal.

[4] Internet draft, Proxy Mobile IPv6, April 2008, http://tools.ietf.org/id/draft-ietf-netlmm-proxymip6

[5] Internet draft, IPv4 Support for Proxy Mobile IPv6, November 2007, http://tools.ietf.org/id/draft-ietf-netlmm-pmip6-ipv4-support

[6] 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses, Release 8, v8.3.0, September 2008.

[7] 3GPP TS 24.302, Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks (Release 8, Stage 3), v0.3.0, April 2008.

[8] 3GPP TS 24.312, Access Network Discovery and Selection Function (ANDSF) Management Object (MO), Release 8, v0.2.0, November 2008.

[9] IEEE Draft Standard 802.21, Media Independent Handover Services, D13.0, June 2008.

[10] OMA-ERELD-DM-V1_2, Enabler Release Definition for OMA Device Management, Approved version 1.2, February 2007.

8. 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).