



Automated PBRM Server Configuration

Future Internet Program of TIVIT,
Activity 2.4 Deliverable DA2.4.2, 1H2009

Contributors:

Sami Heinonen, NSN
Janne Tervonen, NSN



1. Introduction	3
1.1 Abbreviations.....	3
2. Operation and Maintenance	4
2.1 General	4
2.2 Operation and Maintenance of PBRM Server	5
2.2.1 PBRM Configuration	6
2.2.2 PBRM Server Database	6
2.2.3 Constructing Data for Network Discovery and Selection in PBRM	8
2.2.4 Benefits of Automated PBRM Server Configuration.....	9
3. UE-Based Automated Configuration	10
3.1 Concept Descriptions	10
3.1.1 Automated Neighbor Relation.....	10
3.1.2 Concept for Automatic PBRM Configuration	11
3.2 Methods for PBRM Server Configuration.....	13
3.3 Verifying the Validity of Information	16
3.4 Summary.....	16
4. Network-Based Automated Configuration	17
4.1 Methods for PBRM Server Configuration.....	17
4.2 Summary.....	19
5. Other Issues Related to Automatic Configuration.....	19
5.1 Trusted vs. Untrusted Networks.....	19
5.2 Managed and Un-Managed Networks	20
6. Corresponding Systems in Use.....	21
7. Conclusions	22
8. References	23
9. Acknowledgements.....	24
10. Notes	24



1. Introduction

This document is deliverable DA2.4.2 for activity 2.4 of Future Internet program of TIVIT. This document covers the task for automatic configuration of PBRM server within activity 2.4. In this paper, the results of work during 1H2009 are documented.

The PBRM concept itself is defined in earlier FI deliverable [1]. As described on that document, PBRM server can provide to the UEs both network discovery and network selection information. Basically, network discovery information can assist UE's scanning procedure by defining how, when and what networks to scan. Network selection information is a tool for the operators or service providers to influence what networks UEs are using.

The information PBRM server provides may cover different geographical areas: for example, the information may be intended for a whole country (e.g. "access Elisa 3G network in Finland where available"), or the information only has local relevance (e.g. "scan for home WLAN when under your home cell coverage"). In order to support this kind of functionality, PBRM server needs to have an accurate network map configured into its database. Also, UE is required to define its current location – e.g. in terms of GPS coordinates or some radio access network specific identifier, like cell ID – so that PBRM server is able to map the UE's location with the known network map of the server.

In this document, different methods to automate the PBRM server configuration are considered. First, chapter 2 describes in general level what kind of functionality is needed for operation and maintenance of network equipment. The focus of this document is on how network information can be configured to PBRM server. Next, on chapter 3 some UE-based mechanisms for automatic configuration are discussed. Corresponding network-based mechanisms are considered on chapter 4. Chapter 5 concentrates on issues that relate to automatic PBRM configuration and what real-life restrictions exist. On chapter, some related 6 mechanisms in use are briefly described. Chapter 7 concludes the document.

1.1 Abbreviations

3GPP	3 rd Generation Partnership Project
ANR	Automated Neighbor Relation
AP	Access Point (WLAN)
BTS	Base Station
EAP	Extensible Authentication Protocol
ESS	Extended Service Set (i.e. WLAN network)
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HESSID	Homogeneous ESS Identifier
GPS	Global Positioning System
HW	Hardware
IP	Internet Protocol
IPSec	IP Security Architecture
LTE	Long Term Evolution
MAC	Medium Access Control
NAP	Network Access Provider
NR	Neighbor Relation
NRT	Neighbor Relation Table



NSP	Network Service Provider
O&M	Operation & Maintenance
PBRM	Policy-Based Resource Management
RAC	Routing Area Code
RAT	Radio Access Technology
RRC	Radio Resource Control
SIM	Subscriber Identity Module
SON	Self Organized Networks
SSID	Service Set Identifier
SW	Software
TAC	Tracking Area Code
UE	User Equipment
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN

2. Operation and Maintenance

2.1 General

In communication networks, operation and maintenance (O&M) system includes number of different functions. For example, when setting up a network element, it has to be first configured properly: normally this is done via a remote interface between the installed network element and centralized O&M center. When the network element is up and running, it may send e.g. periodic reports of its status including load level, served connections, possible error situations etc. Also, the network element may need to be monitored to verify e.g. its current status. An overview of a generic O&M system is illustrated in the following figure.

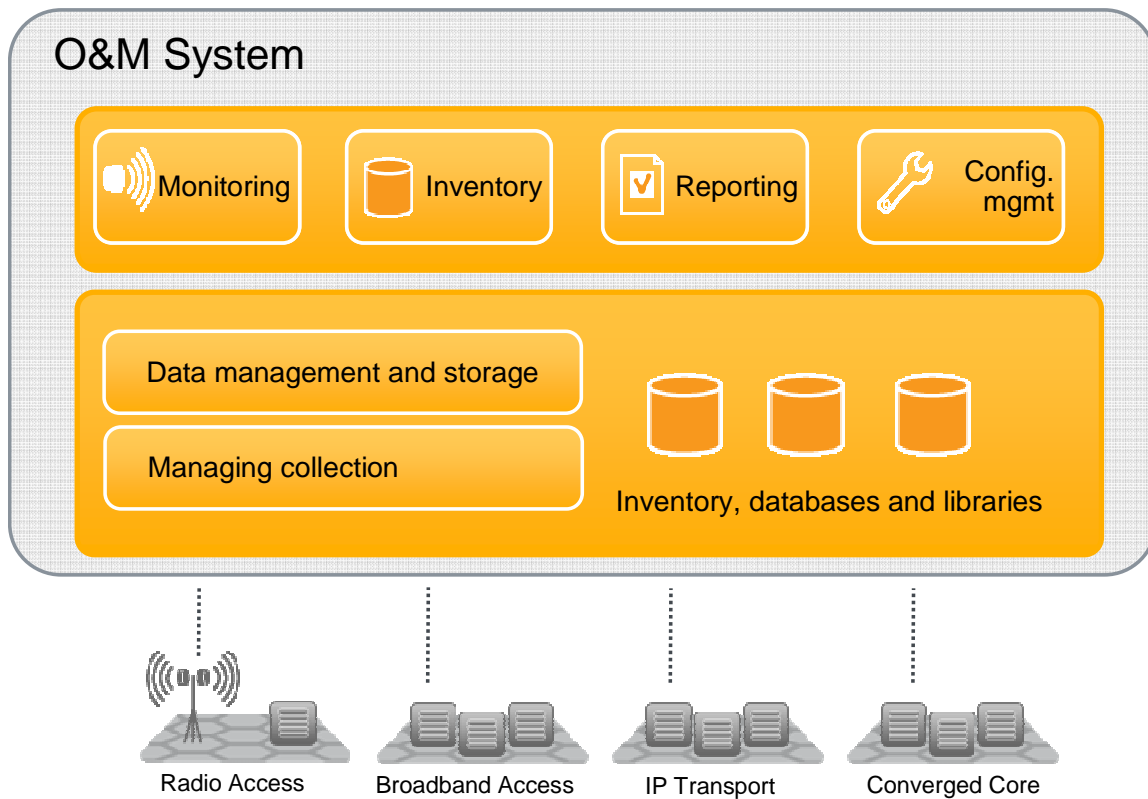


Figure 1. General overview of O&M system.

For all kinds of network operators, the operation and maintenance of the network and its equipment represent a big share of the operator's costs. Traditionally, especially initial equipment configuration but also operational management have required a lot of manual labor and monitoring. For example, when deploying a new base station into a cellular network, there are number of parameters that are unique for that given base station, and needs to be set manually. When an operator is managing hundreds of base stations, it is clear that this kind of approach is time and labor consuming as well as error-prone.

Recently, there has been a lot of development and research work around automating the O&M processes. The term self-organized networks (SON) is often used to describe automated O&M solutions. In general, the main principle is that the network elements – or UEs and network – exchange information about network status, and self-adjust e.g. the network configuration accordingly. Of course, it is not currently possible to completely exclude human supervision of the system functioning. If taking cellular network as an example, SON concept can be applied e.g. on base station neighbor list configuration: in a cellular network, neighboring base stations have to be configured for each base station to be used in handover decisions.

2.2 Operation and Maintenance of PBRM Server

In this document, for operation and maintenance of PBRM server the most emphasis is put on configuration. Of course, other O&M functionality – like monitoring and reporting – has also to be defined and implemented for a real PBRM server product.



2.2.1 PBRM Configuration

The data the PBRM server provides to the UEs affect heavily what kind of configuration mechanisms can be used. As defined in [1], PBRM server can provide network selection and / or network discovery information. In its simplest form, both network selection and network discovery information can be general without any relation to e.g. location data. The other possibility is that all the information PBRM server provides is tied to some location information or network map. All these different options are discussed briefly below:

General PBRM network selection information (no relation to location): PBRM server provides very generic network selection information that is applicable everywhere. For example, the prioritized network list could be: 1. WLAN SSID=WLAN_A, 2. 3G. Since the information PBRM server provides is very simple, this kind of information can be configured manually.

PBRM network selection information with location reference: PBRM server provides network selection information that is applicable only in certain area. For example, for each separate location areas defined for PBRM, there should be a separate prioritized network list. The location areas in PBRM can be tied e.g. to cellular location areas, or areas defined by geographical coordinates. Depending on the complexity of PBRM information (e.g. how many location areas defined, etc.), automatic configuration may be needed.

General PBRM discovery information (no relation to location): PBRM server provides network selection information that is applicable e.g. everywhere in the operator's network coverage. For example, this information could be used to define WLAN bands and channels that the UEs should scan to find the specific WLAN network. In the case of WLAN, the operator could only have a couple of used channels throughout the whole network, so it is possible to bundle the information into one entity. If the amount of configuration information is not too big, possibly manual configuration could be applied.

PBRM network discovery information with location reference: PBRM server provides network discovery information that is applicable only in certain area, e.g. under one 3G cell. This could be used to inform UE to scan for a certain WLAN network with very specific location reference: for example, UE could get network discovery information from the PBRM server to scan for the subscribers home WLAN AP when entering the "home" 3G cell area. Only with the specific location reference, UE can really exploit the network discovery information and use it to reduce battery consumption; with this information, UE doesn't try to find a network when it is not available. In order to provide this kind of information from the PBRM server, an exact network map would be needed in the PBRM server. For this, automatic configuration should be used.

In summary, if PBRM server needs to have some sort of network map in order to provide network selection or network discovery information, automatic PBRM configuration should be applied.

2.2.2 PBRM Server Database

On PBRM concept description document [1], it is described what kind of information PBRM server might be sending to the UEs as network discovery and selection information. In short, discovery information may include some or all the following information (further details on [1] on chapter 4.3.2):

- Network type (e.g. 3GPP WCDMA, WLAN, etc.)
- Network ID (e.g. SSID for WLAN, and NSP ID or NAP ID for WiMAX networks)
- Channel information (e.g. used frequency band and channels)
- Network capabilities (e.g. the network supports .11n capabilities, etc.)
- Location information. This defines the area where the provided network discovery information is valid and UE should try to find that network.

Correspondingly, at least the following information should be included in network selection information PBRM server provides (further details on [1] on chapter 4.3.3):

- Prioritized network list:
 - o Network type ((e.g. 3GPP WCDMA, WLAN, etc.)
 - o Network ID (e.g. SSID for WLAN, and NSP ID or NAP ID for WiMAX networks)
 - o Priority. Defines the priority for a network, UE should consider highest priority network first during network (re-)selection procedure.
 - o Validity information. Defines when and/or where the prioritized network list element information is valid, i.e. when UE should consider the information.
 - o Load information of different networks or BTSs / APs (optional)
- Network blacklist (forbidden networks):
 - o The same information may be included as in prioritized network list.

The above listed information is information that PBRM server should be able to construct from its database to be sent to the UEs. An example of PBRM database structure is given on the following figure.

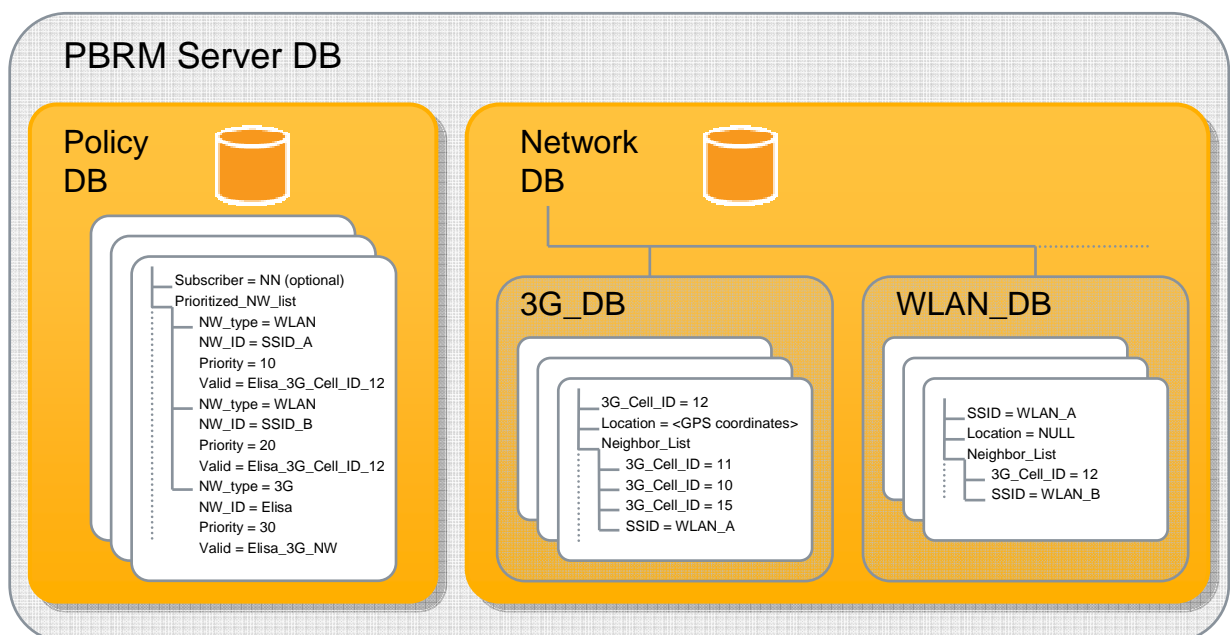


Figure 2. An example of PBRM server database.



In the figure, also policy database contains location information in the 'Valid' field. This field represents the area where the network selection information (i.e. policy) is applicable. Of course, the 'Valid' field may include more than one entry to indicate larger or more complex location definition. This field can be used to define different policies for different location areas, as discussed in the previous sub-chapter.

In the figure, network database contains the network map or topology. Depending on the used location representation, the network topology is more or less accurate. When representing location information of each base station or AP, there are basically two possibilities: either, the location of base station/AP is expressed with exact geographical coordinates (e.g. GPS coordinates), or the location is defined relatively by using some pre-known location reference, e.g. another base station/AP whose location is already known. For example, the location of a WLAN AP may be expressed by giving the 3G cell ID under which the AP resides. This is illustrated in the figure above by defining a neighbor list for 'WLAN_A': the interpretation of the neighbor list is that the WLAN AP with SSID 'WLAN_A' is accessible in a location where also the base stations and APs listed in the neighbor list have coverage.

The benefit of representing location with geographical coordinates is the location information accuracy. However, finding out e.g. GPS coordinates of every base station and AP location can be impossible, especially if PBRM server database contains information from networks not directly under the operator control (e.g. partner networks). So, the geographical coordinates can be used, if they are easily available. This is normally the case e.g. for the operator cellular base stations.

UE may limit the information the PBRM server provides by including its own location in the PBRM information request (PBRM information flow represented in [1] in chapter 4.3.1). UE's location can be expressed with either geographical coordinates or with some radio technology specific identifier, e.g. cell ID. The best result would be achieved, if both PBRM server and UEs operated only with geographical coordinates. However, this is not a realistic requirement at least in the near future.

For PBRM purposes, sufficient accuracy may be achieved without geographical coordinates: if UE provides its location with e.g. cell ID, PBRM may limit decently the information it provides. The problem with using radio technology specific identifiers for location is that the covered area may range from couple of tens meters (e.g. WLAN) to several kilometers (e.g. rural area cellular network cell area). For example, if PBRM informs UE about a specific WLAN network by defining the location of the AP to be under a certain 3G cell, UE can't know if it really is in the coverage of the AP or not, even if UE is attached to the correct 3G cell. However, UE may still use this information to control the scan procedure: when UE is under the 3G cell, it may turn on WLAN scanning and switch it off elsewhere.

2.2.3 Constructing Data for Network Discovery and Selection in PBRM

Once the network topology is defined for sufficiently large area, PBRM can start using the network topology data to compose a list of candidate networks for UE. For the network discovery information, the purpose is to select networks that the UE most likely can detect in its current location.

The obvious method is to select the networks whose cells are near the UE based on geographic location. This method requires the knowledge of the location of cells in each



network as well as the location of the UE. Another approach is to use the neighbor relation (NR) information gathered by the Automated Neighbor Relation (ANR, look at [2] for further details) function to determine networks that are in the 'neighborhood' of the cell serving the UE. This method requires that PBRM can identify the serving cell because the neighbor relations are expressed in relation to the serving cell. These two methods can also be combined to benefit from the strengths of both.

Selection based on cell geographical location is potentially the more effective of the two methods because it will not select networks that are neighbors to the serving cell but on the far side of it in relation to the UE. However, the geographical location based method may also select networks that are near enough but whose signal quality is poor due to obstructions, a problem which the neighbor relation based selection method avoids. The combination of the both methods should be able to avoid the both problems.

2.2.4 Benefits of Automated PBRM Server Configuration

As discussed in 2.2.1, PBRM server may provide information that either does have or does not have reference to location. From operator point of view, if there is no location reference in PBRM information, automated PBRM server configuration does not bring too much benefit. If location reference is needed, the network topology can in principle be configured to the PBRM server manually. However, that is only feasible for static data, whereas much of the network topology data is dynamic. Base stations are added and removed, they crash and are brought up again. Characteristics of base stations may also change. The dynamic nature of the network topology is only augmented by the introduction of WLAN APs and 3G Femto base stations that go on an off without prior notice and are easily moved around. So, it is clear that PBRM server would greatly benefit from automatic configuration that would update changes in the network topology as they happen.

From end user point of view, the benefits of the automated PBRM server configuration are not necessarily direct: it doesn't matter how the PBRM server is configured, as long as the service provided remains the same. However, automatic PBRM server configuration can be used to enable beneficial services, like location-dependent PBRM information.

For network selection information, there is not much difference between no location reference and location reference information: although operator may define more accurate network selection policies with location reference information, the UE still performs the same network selection, i.e. network selection is not considerably improved with the added information from the user point of view. However, the operator may see improved usage of its networks with location references e.g. in terms of better load balancing between different networks.

The most benefit from automated PBRM server configuration for the end user comes when the network discovery information does have location reference: with this information, the UE can optimize its scanning process by switching the scan on only when PBRM information indicates that it may be possible to find a network. This way, it is possible to save battery on the UE. However, it is not clear how big the gained advantage is with the real products: for WLAN, a normal scan of a band takes only a second, so it is not possible to gain a lot from a single scan procedure. More benefit could be gained by reducing the amount of repeated scans needed to find a network. On the other hand, also UE may implement some clever scanning algorithms by itself making PBRM server network discovery information less useful. While this is the case with WLAN, other radio technologies may be completely different story: for example, WiMAX



blind full scan may take up to 15 minutes. With PBRM network discovery information – and especially with location reference – WiMAX scanning time and battery usage can be reduced considerably.

As a summary, the operator may benefit from the automatic PBRM server configuration if location reference is needed in PBRM information. For the end users, the benefits depend on the used radio technologies: for WLAN, only limited benefit can be gained, but for WiMAX the benefits can be considerable.

3. UE-Based Automated Configuration

In this chapter, options for automated PBRM configuration with UE-based mechanisms are discussed. First, an existing corresponding mechanism – called Automated Neighbor Relation (ANR) – for LTE is described. Based on the ideas of ANR, a specific mechanism for PBRM is then presented. Based on these two mechanisms, three different methods for automatic PBRM configuration are presented in general level in chapter 3.2. Issues related to checking the validity of automatic configuration information provided by the UEs are discussed in chapter 3.3.

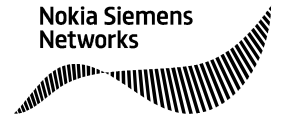
3.1 Concept Descriptions

3.1.1 Automated Neighbor Relation

The purpose of the Automatic Neighbor Relation (ANR) function is to relieve the operator from the burden of manually managing Neighbor Relations (NRs). In cellular networks, the neighbor relations are needed for handover management: each base station – or eNB (evolved NodeB) as they are called in LTE system – has to be aware of its neighboring base stations in order to be able to command the UE to perform a handover to the best target base station (based on signal strength, current load, etc.).

The Automated Neighbor Relation (ANR) is defined in [2], and the corresponding report message contents in [3]. The general idea of ANR is represented in Figure 3. In short, from time to time UE measures the received signal strength of its neighboring base stations (eNBs), and informs the results to the currently serving base station. The serving base station updates its own neighbor relation table with the information received from the UE. At least cell IDs (CI_? in the figure) are stored in the neighbor relation table for each base station. When there is some change in the neighbor relation table, UE informs O&M system about it. This way, O&M has system has a centralized up-to-date view of the base stations and their neighbor relations from the whole network. This gathered automatic neighbor relation information can be used e.g. for dynamic optimization of the network.

Since in cellular networks UEs are anyway required to report signal strengths of the neighboring base stations to the network, applying ANR function does not increase the burden of measurements in the UE. Of course, the ANR function has to be implemented both in UE and network, but probably the existing corresponding mechanisms can be extended to include also ANR function. Another benefit of ANR is that utilizes already setup signaling connections on layer 2, i.e. no additional connection setup is required and reports are easily transmitted without any extra overhead caused by upper protocol layers (like IP). The drawback of the



ANR is that it is defined only for 3GPP technologies: currently, only 3G and LTE base stations can be reported within ANR.

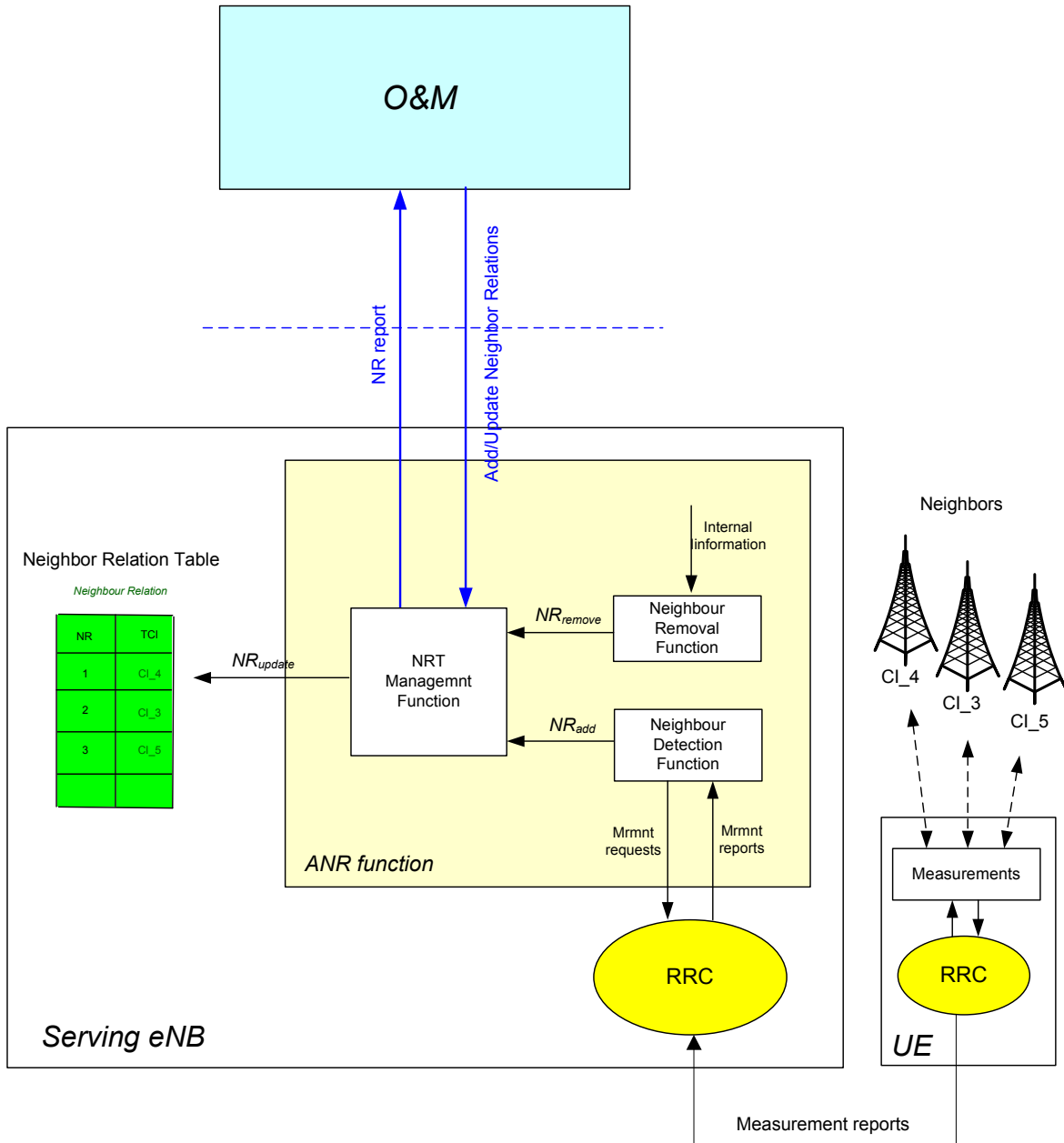


Figure 3. ANR functionality with O&M interface.

3.1.2 Concept for Automatic PBRM Configuration

Based on ANR described above, this chapter describes a similar, stand-alone method for PBRM configuration. In this document, the method is called stand-alone automatic PBRM server configuration.



UE-based stand-alone automatic PBRM server configuration is a function that gathers information from UEs about cells or networks they have detected. UEs scan cells/networks with RAT specific mechanisms and send the scan results to PBRM, which uses the information to construct the topology of the network. UEs can report the scan results either as a separate report message to PBRM server or the scan results can be incorporated into the existing PBRM information request message. The benefit of the latter is that no extra signaling is required compared to normal PBRM operation: whenever UE contacts PBRM server to request PBRM information, the same message exchange is used to convey also scan result information from the UE to the PBRM server. However, this requires that UEs can store the scan results for later submission to PBRM server. Also, more sophisticated mechanisms can be used in scan result reporting: for example, PBRM server could request UEs to provide scan results when entering to certain area, etc.

The following figure depicts an example scenario where a UE scans cells and sends the scan results to PBRM. The UE is attached to the cell A (3G cell in this example) and communicates with PBRM through that cell. UE reports to PBRM the neighboring cells/APs it can hear from different radio technologies together with the current serving cell. This way, PBRM server can associate all the scanned cells/APs to the serving cell, and can deduce the relative location of the reported cells/APs. Gradually, the PBRM server can construct a network map when enough reports from the UEs are available.

The exact content of the reported information is somewhat open, but at least RAT-specific cell IDs (e.g. cell IDs of 3G and LTE base stations, SSID for WLAN networks) are required in addition to location information. For WLAN, only global ID identifying that specific AP is the MAC address, so that is candidate information as well (refer to 5 for additional discussions on WLAN identities). Also, it is possible to include additional information to the reports, like signal strength, load status (if applicable), etc.

In order to exclude the radio accesses that do not provide end-to-end connectivity – e.g. due to firewall or NATs blocking some leg of the route – UEs should first verify that it is possible to connect to the PBRM server using that radio access (i.e. UE is not allowed to report e.g. all random WLAN networks it found during the full scan). So, after being able to establish a connection through a base station / AP to the network of the operator or service provider that offers PBRM services, UE may report the new base station / AP to the PBRM server.

The stand-alone automatic PBRM server configuration sets some burden on UE: since the communication with PBRM server is implemented on IP, UE cannot be connected to the PBRM all the time. Also, setting up the IP connection takes more time and energy than e.g. with ANR's layer 2 based mechanism. If it is defined UE is not required to report its network topology information to the PBRM server after any specific trigger, UE can just provide the information to PBRM server when it would otherwise contact the server. This way, the extra burden on UE would not be too big.

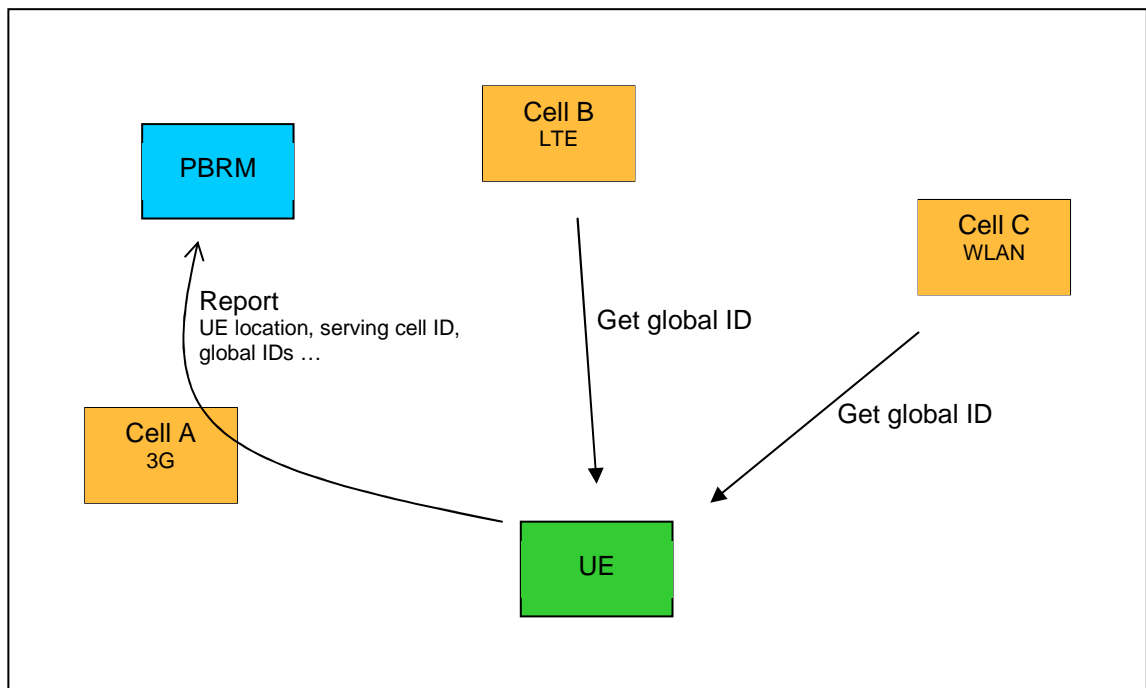


Figure 4: UE scans cells and reports the results to PBRM.

3.2 Methods for PBRM Server Configuration

There are a number of ways how the automatic configuration can work. The methods identified and described here are categorized by the type of the gathered information and by the method used to deliver the information to PBRM. It is assumed that a UE can collect the information needed for the ANR function and for the automatic PBRM configuration with one scan, i.e. the UE does not have to perform separate scans for the two operations.

With all these methods, the information sent by UEs must be checked to be valid or reasonably reliable. Methods of doing this check are described in 3.3.

1. **Stand-alone automatic PBRM server configuration (as defined in 3.1.2).** In this method UEs send reports to PBRM about cells they have detected. UEs and PBRM communicate through a logical interface on top of IP. The reported information includes global cell IDs and possible cell locations. Cell locations can be e.g. GPS coordinates, Tracking Area Codes (TAC) and/or Routing Area Codes (RAC).

Pros:

- Standalone (independent of the ANR function)
- Does not require changes to existing network elements.

Cons:

- Duplicates a lot of the ANR functionality.
- Increases UE load and system load.
- PBRM has to check the validity of the information.
- Communication between UE and PBRM on TCP/IP.

- Requires authentication between the UE and PBRM server also for the network topology reports.

One example of this method is presented in [4].

2. **PBRM server connected to ANR data through O&M.** This method combines parts of ANR function and PBRM configuration function. In this method UEs send reports to ANR about cells they have detected. The information sent by UEs is as defined in the 3GPP specification for the ANR function [2] extended to support non-3GPP cells. The ANR function verifies the validity of the information and updates the Neighbor Relation Table (NRT) and informs the O&M system about changes to NRT. The O&M system relays changes to PBRM. The O&M system only relays Neighbor Relations (NR) because PBRM does not need NR attributes. The O&M system also sends the ID of the cell serving the UE (the cell that reported the NRT changes).

One drawback of this method is that it cannot be applied on any radio access technology: currently, ANR is specified only for 3GPP networks, and ANR functionality will not most probably be included in a standard WLAN AP. In practice, this means that all the network topology reports need to be sent via a 3GPP network. However, this is not as bad as it sounds: the UEs supporting 3GPP radio access technologies are most of the time connected to a 3GPP cell anyway, so UE can still easily have a reporting channel for its network topology reports, even if only reporting found non-3GPP cells / APs.

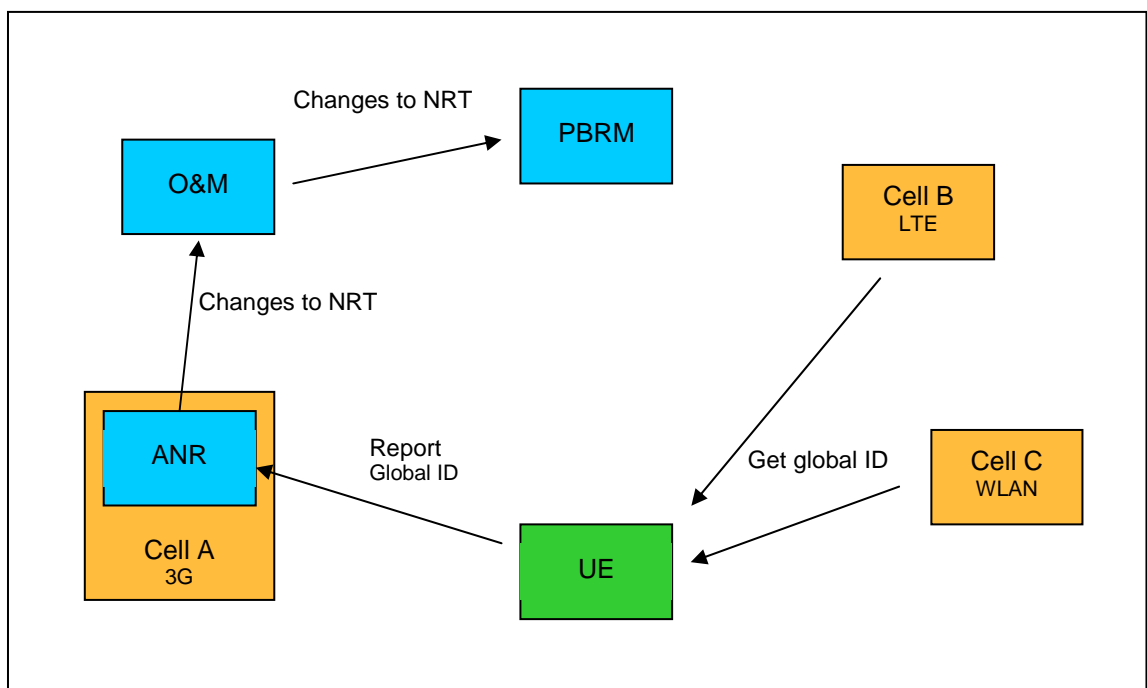


Figure 5: The flow of PBRM configuration data. Global WLAN cell ID is FFS.

Requirements (potential cons from the implementation point of view):

- Changes to ANR message to support non-3GPP RATs

- a change to the O&M system to make it relay the configuration information to PBRM.

Pros:

- PBRM does not have to check the validity of the information, since ANR function is taking care of that.
 - Only new and verified information is relayed to PBRM.
 - Does not require authentication to PBRM. Authentication to the network is enough.
3. This method is a modification from the second method. The differences are in the gathered information and the method used to relay it from ANR to PBRM. The information sent by UEs is as defined in the 3GPP specification for the ANR function [2] extended to include PBRM specific configuration information (e.g. cell location).

The ANR function verifies the validity of the ANR specific information and updates the NRT. When the validity has been verified, the information that caused changes in neighbor relations is relayed to PBRM through a dedicated interface instead of via the O&M system. PBRM verifies the validity of the PBRM specific information.

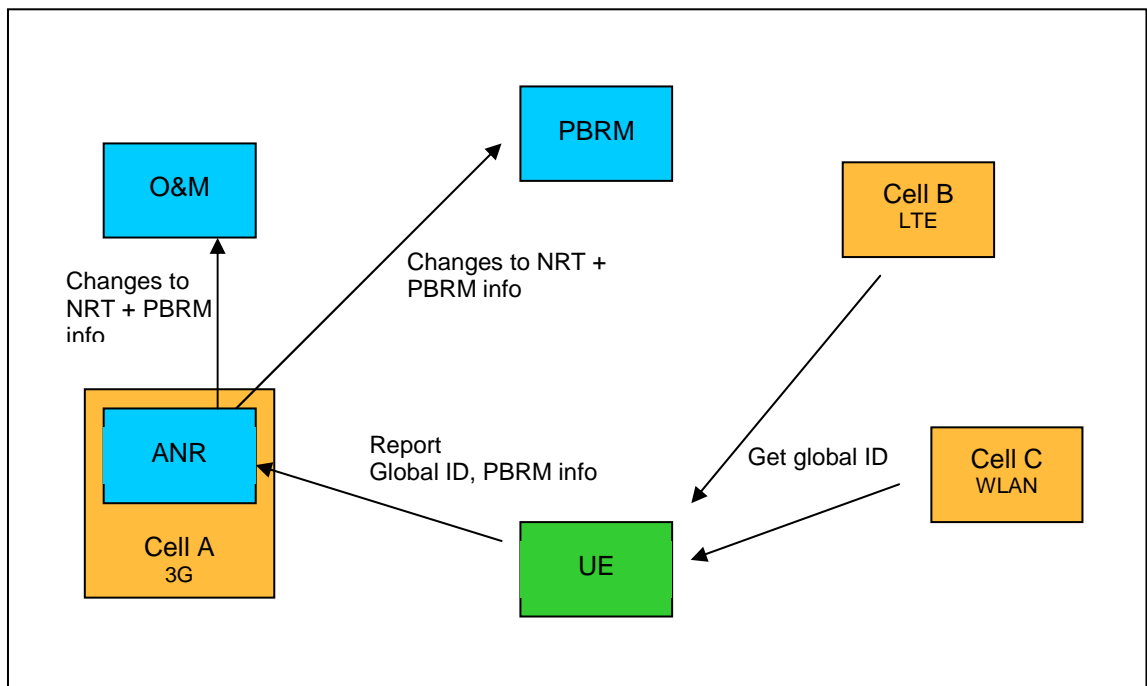


Figure 6: The flow of PBRM configuration data.

Requirements (potential cons from the implementation point of view):

- Changes to ANR messages: support for non-3GPP RATs, addition of PBRM specific information)
- Creation of a new interface between cells and PBRM.
- Reports on non-3GPP RATs possible to transport only over 3GPP connection



Pros:

- PBRM only has to check the validity of the PBRM information.
- Only new and verified information is relayed to PBRM.
- Does not require authentication to PBRM. Authentication to the network is enough.

3.3 Verifying the Validity of Information

PBRM must be able to verify the validity or a reasonable reliability of the information sent by UEs. Verifying the validity means that the information is checked against a set of trusted information. Verifying a reasonable reliability means that the information is estimated reliable enough e.g. through statistical analysis. It is also possible to consider information reliable, when enough many UEs have reported the same information.

Despite the dynamic nature of the network topology data, some of it is static and known to the operator. Some information pertaining to base stations owned by operators rarely changes once a base station has been set up. The location and the ID of a base station are such information. Operator owned base stations are stationary and stay on-line all the time (apart from the occasional crash or maintenance break). The O&M system is used to configure PBRM with this static data. This initial configuration can be done automatically or manually. Static data must be retained even when the related base stations go off-line because it will still be valid when the base station comes back on-line. Static data must only be deleted when a base station is permanently removed. Static data is the only data that can be trusted and used to verify the validity of information sent by UEs.

Some of the network topology data is dynamic. Status and characteristics of all base stations, including those owned by operators, are subject to change without notice, especially in self-organizing networks (SON). Private base stations (WLAN APs and 3G Femto base stations) may be moved and go on and off at the whim of the owner. Location, availability and even IDs may change at any time. Dynamic data cannot be used to verify the validity of information sent by UEs but it can be used to estimate the reliability of that information. Dynamic data may also be stored for statistical analysis in order to improve reliability estimates.

These principles and methods can also be applied to the ANR function. With ANR, it is also possible to exploit the fact that base stations are managed by an operator: if UE can authenticate to the operator network – i.e. UE is a legitimate network user – the information provided by the UE from the network should be trusted. Of course, it is always possible to implement badly behaving devices, and some measures to filter these out should be considered: however, the operator can easily ban access for a device that is not following the operator's network usage guidelines.

If automatic PBRM configuration uses the NR information gathered by the ANR function, it must be able to trust that information. Therefore, the ANR function must verify the validity or a reasonable reliability of the information sent by UEs. This makes the implementation of PBRM simpler, since there is no need for additional validity checking logic in the PBRM.

3.4 Summary

The stand-alone automatic PBRM server configuration and ANR both implement similar kinds of functions. It makes sense to combine these two, if possible. If the operator deploying PBRM



server has also ANR function in its network, the PBRM server configuration should take the advantage of the ANR data already available. In order to apply this also for non-3GPP networks, ANR should be extended so that it can also convey information about non-3GPP networks (namely WLAN and WiMAX). To avoid any additional change in the network elements, it is probably the best choice to implement an interface between PBRM server and O&M system, i.e. follow the option 2 from above.

Currently, ANR carries only cell ID information: if some PBRM-specific information would be needed in PBRM server (e.g. load), ANR could not be used. In this case, stand-alone automatic PBRM server configuration should be implemented. Also, if there is no ANR support in the network, the only option is then to go with the stand-alone automatic PBRM server configuration, i.e. with the option 1 from above.

4. Network-Based Automated Configuration

4.1 Methods for PBRM Server Configuration

As described in chapter 3.1, UE-based mechanisms are built on UE reporting information either directly to the PBRM server or to some other corresponding service / server, like ANR. In the case of network-based mechanisms, the same principles can be used: PBRM server gets network information either from other network elements (e.g. base stations or WLAN APs), or PBRM server has an interface to some other network information repository e.g. through O&M system.

In the following, some mechanisms are discussed in more detail.

1. **GPS chip included in base stations / APs.** Some operators have set a requirement to have GPS capability built in the Femto (home) base stations. Since the Femto base stations are installed in the property of the subscriber, the operator cannot access and configure home equipment directly. It is very easy to carry Femto base stations from one location to another; having GPS included helps in tracking the location of Femto base station.

With PRBM server, the base stations / APs having GPS capability could report their location periodically directly to the PBRM server. If this reporting is realized using IP, there is no need for additional physical interfaces. In practice, this solution could be applied to equipment sold through an operator retail chain.

Pros:

- Gives very accurate network map, assuming all the base stations / APs support the mechanism

Cons:

- Requires additional HW & SW in all home base stations and WLAN APs.
- Does not work with existing installed equipment.



- GPS does not work well indoors. The equipment – or at least GPS receiving antenna – should be installed next to a window. This may make the system unreliable.
2. **Base stations and / or WLAN APs perform periodic scans.** It is probably safe to assume an operator knows the location of its cellular base stations. Taking advantage of this knowledge, it is possible to map new (or previously unknown) base stations / APs with relation to the known location of base stations. To do the mapping only with the help of network elements, the base stations and APs should be able to scan for their neighborhood and report the results either directly to PBRM or to some O&M element. In practice for scanning for the same radio technology, this would mean that either the base station / AP is able to switch off the normal operation for the duration of the scan procure, or there is another radio unit installed in the base station / AP to do the scanning. For inter-RAT scans, a corresponding radio unit is anyway needed. This method is probably applicable only for local area equipment: for cellular base station it is not reasonable to scan for WLAN APs since the base station probably hears only fraction of the present WLANs. On the other hand, WLAN APs may easily hear several base stations making the location deduction of the AP more accurate.

Pros:

- Good business for chip vendors

Cons:

- May require additional radio unit for single-radio operation.
- For inter-RAT scan, additional radio is needed. Cost and complexity of the equipment is increased.

3. **PBRM server taking advantage of existing information.** When purchasing service or equipment from an operator, the subscriber data is stored into operator's database e.g. for charging purposes. For example, if a customer purchases ADSL subscription, the location of the ADSL line is known by the address of the subscriber. If the customer buys also the terminal equipment – including WLAN – via the operator, the location of WLAN is stored in the subscriber database. The PBRM server could have an access to this information.

Also, PBRM server could have a connection to the operator other network configuration information, e.g. base station database, and read all the network information from there. However, this works only for the operator's own networks, and not for e.g. partner networks. Mechanisms exploiting ANR information through O&M interfaces were already covered in chapter 3.

Pros:

- No modification to UE

Cons:

- In the case of using street addresses, mapping between an address and network map required



- Cannot cover all the possible networks, only the ones under the operator control
- Requires a new O&M interface for PBRM
- The process requires manual work, although not from PBRM point of view

4.2 Summary

With network-based automated configuration methods, it means in most cases modifying or adding additional functionality on existing network elements, e.g. WLAN APs. While this may technically be doable for the new devices, the old installed equipment cannot support it. Further, any extra cent for productions costs should be justified, and if the extra costs only mean adding some network management feature, the customers are not willing to pay for it in the form of increased equipment price.

Compared to UE-based mechanisms, the network-based methods do not provide clear additional benefits. When taking into account the fact that the required additions for UE-based mechanisms may be implemented in UEs anyway (e.g. for ANR) regardless of PBRM configuration methods, it makes more sense to pursue UE-based mechanisms than network-based.

5. Other Issues Related to Automatic Configuration

PBRM cannot blindly accept anything a UE sends to it. Firstly, authentication must be required to prevent unauthorized access and use. In practice, a UE first need to authenticate itself as legitimate user of the access network, and after that another authentication is needed for PBRM server itself. Authentication also helps in identifying misbehaving users and preventing malicious behavior. Secondly, PBRM must be able to verify the validity or reasonable reliability of the information sent by UEs (refer to chapter 3.3 for discussion on validation of reported information).

5.1 Trusted vs. Untrusted Networks

In principle, PBRM server can be deployed by any organization benefiting of providing network selection information to the UEs. However, since the PRBM information may affect on the costs incurred, the user of the PBRM has to accept and benefit from the usage of PBRM server information. In practice, this means e.g. the network operators would be potential organizations deploying PBRM. Another example is enterprises that could benefit from providing network selection information e.g. to employees traveling abroad.

If PBRM server is managed by an operator, it resides in the operator core network. From operator point of view, it makes sense to advertise only the access networks that provide connection to the services via the operator's own core network. This may include the access networks owned and operated by the operator, and partner networks.

For cellular networks, 3GPP defines in [5] two types of non-3GPP radio accesses for 3GPP core network: trusted and non-trusted. As specified in [5], whether a non-3GPP IP access network is trusted or untrusted is not a characteristic of the access network, but it is a matter of decision: the operator decides whether a non-3GPP access network is trusted or un-trusted. In practice, the biggest difference between the two is that with un-trusted access network, UE is



required to establish IPsec tunnel from the UE all the way to the operator core network. Basically this means that in future, it should be possible to get an access to a 3GPP operator core network services (or any services through the operator core network) from virtually any access network, including one's own home WLAN. From PBRM's viewpoint, this opens new issues, as discussed in the next chapter.

5.2 Managed and Un-Managed Networks

From an operator point of view, networks can be divided to two groups: the networks managed by the operator or by a partner, and the un-managed networks. To the latter group belongs for example WLAN hotspots, café WLAN networks, private networks etc. The cellular networks – e.g. 3GPP networks including 2G, 3G and LTE technologies and WiMAX networks – are always managed networks. Also WLAN network can be considered managed, if it is operated by the operator or by a partner. Thus, if PBRM receives automatic configuration information about a managed network, the PBRM server can trust the information to be correct in most cases (assuming the information was not sent by a malicious device). However, with the un-managed networks – in practice the term un-managed network refers only to WLAN networks here – this is not the case. There are several reasons for that:

- The only global unique ID available for WLAN AP is the MAC address. However, normally only SSID is used to identify a WLAN network. There is a good reason for that: a WLAN with single SSID may have hundreds of separate APs all with different MAC address. From automatic PBRM configuration point of view, SSID is also problematic: when PBRM server gets 500 hits from different locations with SSID "default", there is not much PBRM server can do with that information. IEEE 802.11u draft amendment [6] introduces a new network identifier into WLAN, HESSID (Homogeneous ESS Identifier). In practice, HESSID is the MAC address of a single WLAN AP belonging to the WLAN network, and thus in conjunction with SSID uniquely defines the WLAN network. In PBRM context, SSID with HESSID could be used to identify WLAN networks. However, the 802.11u is still in draft status, and it will take years before it is implemented in products.
- Another issue with SSID is that although for managed WLAN networks certain naming convention is used – e.g. Homerun for TeliaSonera WLAN network – there is no way to limit anyone else to name his or her network with the same SSID. Thus, when noticing a known SSID, it does not yet guarantee there is access to anywhere. Also, even if PBRM receives configuration information about known, managed WLAN network (indicated by SSID), there is no way for PBRM to know does the reported WLAN AP really belong to the managed network, unless MAC address (or HESSID) is included in the information.
- PBRM configuration information can only contain information about open WLAN networks (no air interface encryption), or networks that support operator/partner managed authentication method (e.g. EAP-SIM method). The information PBRM provides to the UEs should be valid for all the subscribers. For example, if a user knows WLAN air interface encryption credentials and reports that WLAN AP to PBRM, the other subscribers probably do not get access through that AP.
- In Finland, it is illegal to use someone else's WLAN network without permission. Thus, PBRM cannot contain information about private networks, unless the information is limited only to certain subscribers (e.g. certain subscriber's home network). For automatic PBRM configuration, this means that no private networks can be reported to the PBRM server. How to know if a WLAN network is meant for public or private use?



That is a tricky question, but in Finland the current interpretation of the law is such that if the openness is clearly indicated, e.g. in the SSID, then the network is for everyone. Otherwise, it is the burden of the PBRM server to verify that a WLAN network is for public use and it is not illegal to use it.

As a summary, PBRM automatic configuration can only be applied for the following WLAN networks:

- Public, open networks
- Trusted networks from the operator point of view
 - networks managed by the operator
 - networks managed by a partner

Also, if automatic PBRM configuration is used for WLAN networks, MAC address (or HESSID) is required in the automatic configuration information provided by the UEs.

6. Corresponding Systems in Use

With today's multi-radio capable terminals, it is possible to build interesting applications that take advantage of the terminal different radio technologies, including GPS. For example when launched, such an application may turn GPS receiver on, and then continuously scan for available networks. When any network – e.g. WLAN AP or base station – is found, the network ID with the corresponding GPS coordinates is sent to a centralized server. The server gradually gets more reports of new networks as the number of users and/or scan report increase. After a while, the server can have a full network map from certain area.

Mobile Google Maps is one example of an application using above described mechanism. Mobile Google Maps is downloadable for various operating systems, like Symbian S60. When downloading the application, the user is asked to accept the terms of usage: on those, it is defined that the application may send data from the UE to Google servers, including location data. Mobile Google Maps uses the gradually built network map to locate the user on the map. When location service is requested, the application contacts the Google map server to get the latest network map information. If the UE does not support GPS, or the GPS is not switched on, Google Maps can locate the UE based on the current cell ID UE reported to the server. This kind of location service works pretty well, when the cell size is small enough: in the city areas, 3G cell size is normally only couple of hundreds meters, so the application can give a ballpark estimation of the location. However, this is not accurate enough e.g. for navigation. In the Figure 7, a screenshot of mobile Google Maps application giving location is shown (unfortunately in Finnish).

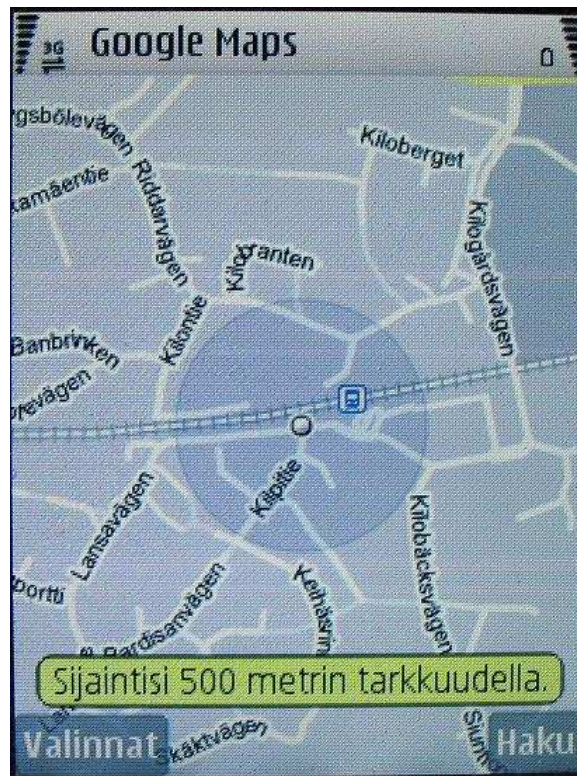


Figure 7. A screenshot of mobile Google Map application giving location estimate based on 3G cell IDs.

Another example of corresponding applications is various network sniffer services that are mainly used for finding and publishing information on open WLAN networks. The database operator may be e.g. a public community that gathers information about open WLAN networks for the common benefit of the community members. There also was couple of companies offering this kind of network information commercially: first, user downloaded a specific client that reported found WLAN networks with GPS coordinates to the company servers. The gathered information was then offered for various service providers as valuable data. However, it seems this kind of business was not viable enough, and the recession has put these companies out of business.

7. Conclusions

The operator has to know all kinds of information about the networks it is managing. This information includes for example the location of all the operator's base stations and access points. For managed networks – either cellular or WLAN networks – it may not be sensible to develop an additional mechanism for configuring the managed network information to the PBRM server. Instead, a better option would be taking advantage of the already existing information, especially if ANR function is already deployed in the network. For that, a new interface would be needed for PBRM server. However, PBRM has to be connected to O&M system for PBRM own management anyway, so this new interface might not be a big addition.

For un-managed networks – i.e. WLAN networks – automatic PBRM configuration can only be used if:



- the WLAN network is open, or supports e.g. EAP-SIM authentication with the operator AAA server
- the WLAN network is public, or belongs to the operator (or partner) managed networks
- MAC address (or HESSID) is included in the configuration information

The above requirements for un-managed networks restrict pretty much the set of networks that the automatic configuration can be applied for.

Further, the benefits of the automatic PBRM server configuration from the end user point of view depend on the used radio technologies: for WLAN, the benefit is questionable but for WiMAX clear advantage can be achieved.

Thus, it is unclear is the added complexity really worth of making completely new feature into the UEs and networks.

As a bottom line, if the automatic PBRM configuration is needed, the most cost-efficient solution can be implemented by adding a new interface between existing O&M network information and PBRM server.

8. References

- [1] Policy-Based Resource Management, Future Internet Programme, Activity 2.4 Deliverable DA42.4.1, Janne Tervonen (ed.)
- [2] 3GPP TS 36.300 Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Overall description, Stage 2 (Release 8), version 8.8.0, March 2009.
- [3] 3GPP TS 36.331 Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC), Protocol specification, (Release 8), version 8.5.0, March 2009.
- [4] TD S2-092592, Telecom Italia & Orange contribution to SA2#72 meeting, March 2009.
- [5] 3GPP TS 23.402 Architecture enhancements for non-3GPP accesses (Release 8), version 8.4.1, January 2009.
- [6] IEEE P802.11u™/D8.0, Draft STANDARD for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: Interworking with External Networks, version D8.0, July 2009.



9. 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).

10. Notes

Issues that were not covered in this release of the paper can be studied and documented during 2H2009. Such issues currently include roaming scenarios and the exact information included in reporting messages of the stand-alone automatic PBRM server configuration mechanism.