IST Integrated Project No 507023 – MAESTRO

D4-4

Network Requirements for R2

Contractual Date of Delivery to the CEC:	31/12/2004
Actual Date of Delivery to the CEC:	02/12/2004
Author(s):	British Telecom
Participant(s):	see table Document Authors
Workpackage:	WP04
Est. person months:	5
Security:	Pub.
Nature:	R
CEC release:	1.0
Version:	3.7
Total number of pages:	30

Abstract:

This document presents the network layer requirements for the MAESTRO Test Bed Release 2 (R2). It indicates the features required and the features that the test bed should verify.

The ideal commercial features of the network are discussed, but the report majors on the restricted network to be provided by R2. This includes an end-to-end view of the functions to be implemented together with a description of how those functions are distributed within the elements of the test bed.

Keyword list: MAESTRO, Test Bed Release 2, Network Layer

EXECUTIVE SUMMARY

This document contains deliverable **D4-4** of the IST Integrated Project MAESTRO – Mobile Applications & sErvices based on Satellite and Terrestrial inteRwOrking (IST Integrated Project n° 507023).

The MAESTRO project aims at studying technical implementations of innovative mobile satellite systems concepts targeting close integration & interworking with 3G and Beyond 3G mobile terrestrial networks.

MAESTRO aims at specifying & validating the most critical services, features, and functions of satellite system architectures, achieving the highest possible degree of integration with terrestrial infrastructures. It aims not only at assessing the satellite systems' technical and economical feasibility, but also at highlighting their competitive assets on the way they complement terrestrial solutions.

This is the first of 3 tasks in Work Package 4.3 – "network high-level designs". The WP defines network high level designs for the test bed release 2 (R2) and indicates wider commercial implementations. Issues considered in WP6 will also be taken into account.

This deliverable describes the Network Layer requirements and specifications for the MAESTRO Test Bed Release Two (R2) and the features that the test-bed should verify.

The task is lead by BT and is supported actively by Alcatel and LogicaCMG as MAESTRO partners.

COPYRIGHT

DOCUMENT HISTORY

Vers.	Issue Date	Content and changes
3.2	13 September 2004	Draft A
3.3	08 October 2004	Draft B
3.4	29 October 2004	Draft C
3.5	01 December 2004	Draft D
3.6	01 December 2004	Final version for review
3.7	02 December 2004	Final version for delivery

DOCUMENT AUTHORS

This document has been generated from contributions coming from most of the MAESTRO partners. The contributors are the following:

Partners company	Contributors
BT	Ken Fowler George Vogiatzis Mike Fitch
LogicaCMG	Nick Green Mark Cole
Alcatel	Catherine Dargeou

DOCUMENT APPROVERS

This document has been verified and approved by the following partners:

Partners company	Approvers
Alcatel Space	• Paul Vincent • Christophe Selier

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

This document describes the Network Layer requirements and specifications for the MAESTRO Test Bed Release Two (R2) and the features that the test-bed should verify, and thus constitutes MAESTRO Deliverable D4.4.

The Network Layer for the envisaged commercial system is significantly more sophisticated than is required for R2. For example, the DRM network will not be used. Additionally, for the R2 implementation, it will be necessary to make use of existing mechanisms as the enhanced range of functionality considered for a commercial system is outside of the original scope of the R2 test bed (as defined in the technical annex). Thus, aspects such as user and content provider authentication and authorisation, ciphering, deciphering, etc. will differ from a commercial implementation.

The MAESTRO test bed is an extension of that used for FP5 MoDIS. Within the scope of R2, the MAESTRO study includes the setting up of two platforms, a laboratory trial and a field trial. The laboratory trial will not include a terrestrial network.

The objective of the laboratory test bed is to provide a platform to complement simulation results. A key requirement of the laboratory platform is to allow reproducibility.

The objective of the field trial is to demonstrate the basic feasibility of the SDMB system by using an integrated terminal.

In order to put the network layer requirements into context, this report first describes the network layer for the commercial system and then more fully describes the simplified network layer to be used for R2.

Section 2 provides a Network Layer overview for the envisaged commercial system, and describes how this applies to the R2 test bed.

Section 3 describes the Network Layer functional architecture of the R2 test bed, that is an end-to-end view of the functions to be implemented and which network functions of the commercial SDMB system will be supported and tested within R2.

Section 4 illustrates the Network Layer Logical (or Organic) Architecture of the R2 test bed. This can be considered as an organic or logical view of the network functions, that is a description of how the functions are split among the different organs of the test bed. It comprises a high-level description of each organ and interface of the test beds and identifies specific network scenarios to be tested in R2.

2 NETWORK LAYER OVERVIEW FOR A COMMERCIAL SYSTEM

There are two phases in the design of the network architecture, the design of the commercial model and the design of the test bed model that will be used to simulate the successful operation of the proposed commercial network.

This commercial design indicates the probable (eventual) network layer architecture of the SDMB network, but this differs from the practical implementation of R2 that is by necessity limited by available resources and time. The test bed model is described in later chapters.

The commercial network design is shown in Figure 1, and can be envisaged as comprising five parts:

- Content provider network
- Aggregator network
- Satellite network
- Mobile operator network
- DRM network

Each of these smaller networks is physically located in a different area. Thus, the content provider network will focus on the content provider server and interfaces, the aggregator network will include routers 1, 2 and 3, firewall 1 and the BM-SC, the DRM network will include the DRM servers and firewall 2, the Mobile Operator (MO) network will include the terrestrial network and the AAA and finally the satellite network will include the SSN, the IMR, the earth station and the satellite itself.

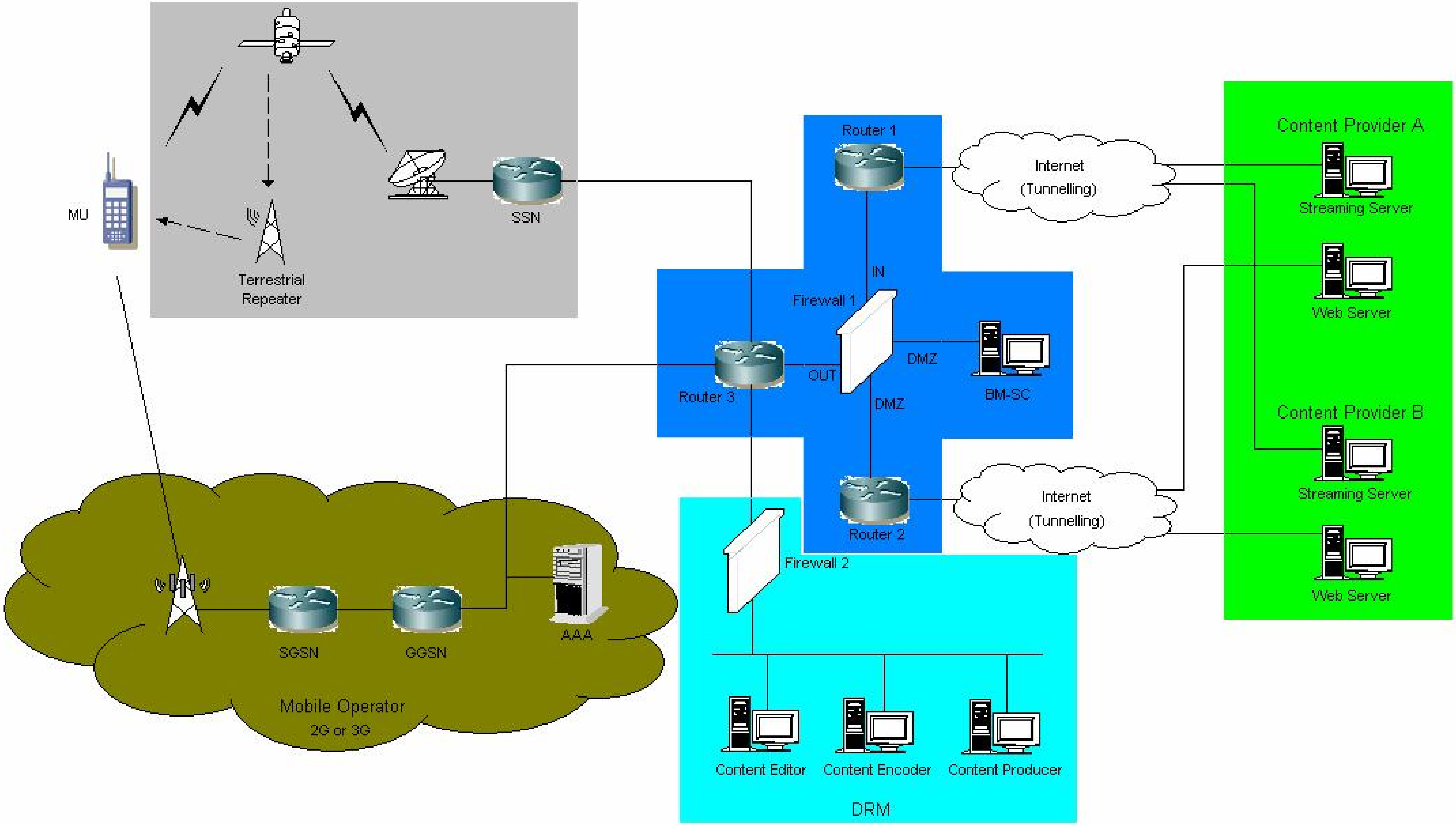

Figure 1: Commercial Design of the Network

2.1 Content Provider Network

The content provider network consists of the streaming server and the web server. There are some other servers that can possibly be used, but we will focus on those two here. The streaming server is used to stream broadcast content to the UE, while the web server is used to send data upon request to the user.

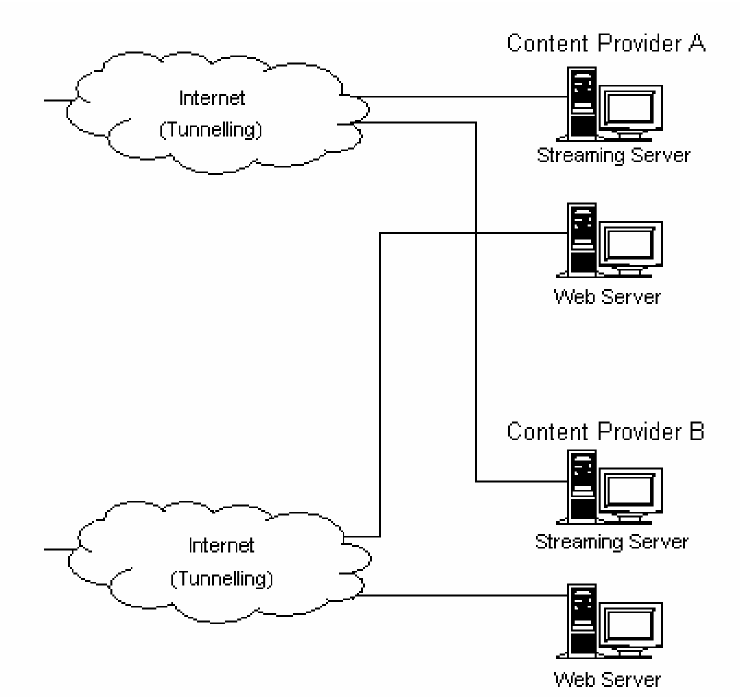

Figure 2: Content Provider Network

2.1.1 Functionality

In Figure 2 two content providers are shown, but multiple content provider interaction could similarly be provided. The streaming servers are separated from the web servers and are terminated to a different router for reasons of security. The *streaming servers* are independent devices with limited access requirements. Content is streamed to the BM-SC in accordance with a schedule, which can be managed by the BM-SC. However, no request is received at the streaming server from a UE to start or terminate the content delivery, so a return path through to the UE is not required for this purpose. In the other hand, the *web servers* operate on a per request basis. Either the user or the BM-SC requests certain data and the web server delivers it. Thus, a return path from the BM-SC to the web servers is required. As the level of security for these two services is different, different paths are required.

2.1.2 Connectivity

The link between the content provider network and the aggregator network can either be a tunnel or a leased line. A tunnel via the public Internet can provide secure connection between the content provider and the aggregator if encryption is used. The tunnel will be terminated to a router (router 1 or 2), which is located in the aggregator network.

By using this architecture it is possible to use IPv6 networks, if this is required. Both the content provider network and the aggregator network can be operated in IPv6 and an IPv6toIPv4 tunnel can be used to link these two networks via the public IPv4 Internet. The existence of the two routers, one at each end of the tunnel makes this feasible.

It is also possible to terminate multiple tunnels in a single router interface. The tunnels created by the different content providers can be terminated in a single interface in the aggregator network, thus limiting the number of interfaces and routers required to one for each service.

However, using tunnelling via the public network may have a huge impact on the QoS that can be supported on this interface.

2.2 Aggregator Network

The aggregator network consists of routers 1, 2 and 3, firewall 1 and the BM-SC. Routers 1 and 2 are used to terminate the tunnels from the content providers and route the traffic to the BM-SC. Router 3 is used to route the traffic between the aggregator, the DRM, the MO and the satellite networks. Firewall 1 is used to provide security to the network and prevent unauthorised access and finally the BM-SC is the key element of the network.

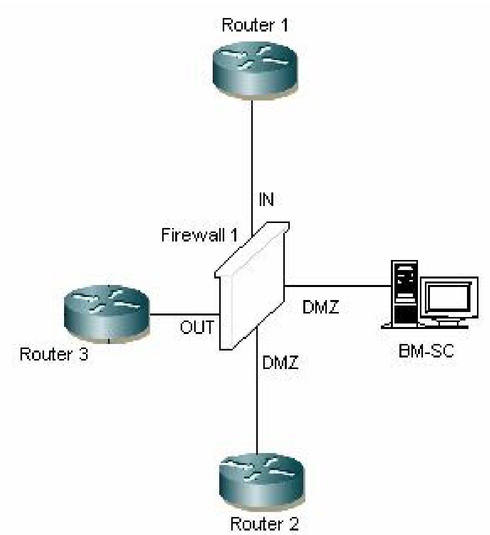

Figure 3: Aggregator Network

2.2.1 Functionality

The BM-SC acts as a central controller for the SDMB network and underpins all network activities.

The BM-SC determines whether information is to be sent to users terrestrially or via satellite. This will depend on a number of factors, for example, satellite will be the best option if the information is to be broadcast to many users. The tasks of the BM-SC will also depend on the type of information to be sent and the encryption and conditional access methods to be followed. For example, free to air and public service broadcasting can be accomplished without conditional access and a return path. A more flexible content provision will require these features, and will give a more comprehensive user experience. This functionality is described below.

Content from the content providers is sent to the BM-SC, which then decides when to forward it, if the content should be included in the carousels and which path to follow (the satellite or the terrestrial path). The BM-SC also requests and retrieves authentication and authorisation information from the MO, in order to be able to deny access to unauthorised users. If the MO is not willing to pass subscriber details to the BM-SC, then the BM-SC is likely to have to refer user authentication and service authorisation to the MNO. Finally, the BM-SC is responsible for the billing information.

Firewall 1 is responsible for providing security. There are two ways to provide security. The firewall is capable of having an access list with all the names of the users that are registered to the service. This list can be updated dynamically from the BM-SC as soon as it retrieves the AAA information from the MO. However, this technique adds a lot of overhead to the network and it is not efficient. It also allows access to all applications, which is not preferable. A more appropriate technique is to use port filters in the firewall and allow only selected applications to be accessed, like port 80, which is the web port. The BM-SC also retrieves authentication information from the MO and restricts unauthorised access to the network.

Thus, by combining these two techniques, only authorised users accessing a specific service will be allowed through the firewall. However, the retrieval of authentication information from the MO is only possible if the MO is willing to allow the aggregator to access its server. This cooperation from the MO may be difficult to achieve in which case the MO could push this information to the BM-SC every time a new user is subscribed to, or deleted from, the SDMB network. All of the above however are subject to the willingness of the MO to pass authentication and authorisation information to the BM-SC.

Routers 1 and 2 are mainly used to terminate the IP tunnel and route all traffic as required. Router 3 has more applications. This router provides routing capabilities for the traffic sent from the BM-SC to the UE, depending on the route (satellite or terrestrial) decided by the BM-SC. It is also routes all traffic from the UE to the BM-SC and all the DRM licence requests to the DRM servers.

2.2.2 Connectivity

The firewall is used to limit access between all the interfaces. Interface IN enables the streaming server to stream content and blocks all access towards the server, providing complete security. Interface OUT provides bi-directional traffic with no restrictions. Finally, interface DMZ provides bi-directional traffic with certain restrictions, based on the access lists configured. The DMZ interface that connects the BM-SC to the firewall allows requests from the user to be passed to the BM-SC and also bi-directional traffic between the two DMZ interfaces (BM-SC and web servers). The last DMZ interface allows only bi-directional traffic between the BM-SC and the web servers.

Router's 3 connectivity to the satellite, MO and DRM networks is achieved by using leased lines or IP tunnelling, similar to the case of the content providers. Thus, router 3 can also be used for tunnel termination. The interconnectivity between the three routers, the firewall and the BM-SC is achieved with regular Ethernet interfaces.

2.3 Satellite Network

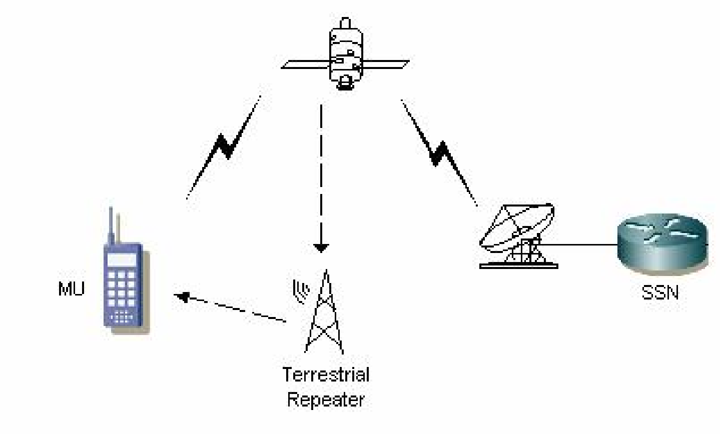

Figure 4: Satellite Network

2.3.1 Functionality

The satellite network consists of the hub (SSN, satellite dish) and the terrestrial repeater if required. The satellite path is only used for the forward path. There is no return path via satellite. This network is managed entirely by the satellite network operator, which could be the same actor as the terrestrial network operator. The system supports terrestrial repeaters in order to increase service coverage in areas subject to high blocking.

2.3.2 Connectivity

The connectivity between the MO and router 3 can be achieved by leased line or secure IP tunnelling.

2.4 MO Network

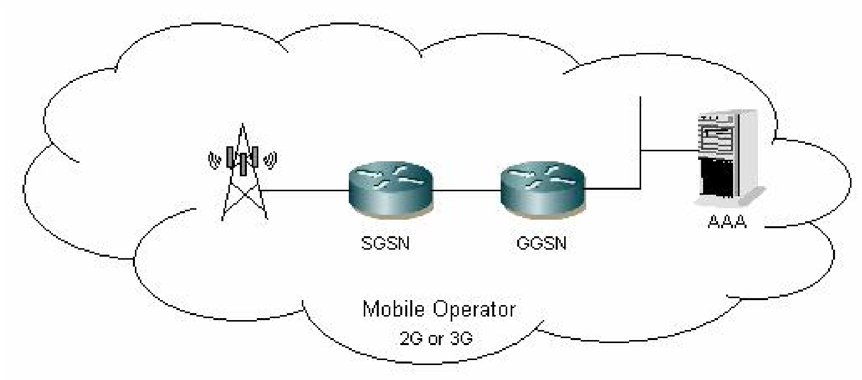

Figure 5: MO Network

2.4.1 Functionality

The Mobile Operator network is used to provide the return link for the SDMB network. It is also used to deliver data to the UE that the BM-SC determines to send via the terrestrial link. Such data may be multicast content that is targeted to relatively few users and that it is not efficiently sent via satellite. However, this assumes an MBMS capable mobile network. This network is managed entirely by the mobile operator. Its main features are the GGSN, the SGSN and the base station. It also holds the AAA server with all the information for the subscribed users. This information is either accessed by the BM-SC or is pushed from the MO to the BM-SC to acquire authorisation information.

2.4.2 Connectivity

The connectivity between the MO and router 3 can be achieved by leased line or a secure IP tunnelling.

2.5 DRM Network

The DRM network consists of the content editor, the content encoder, the content producer and firewall 2.

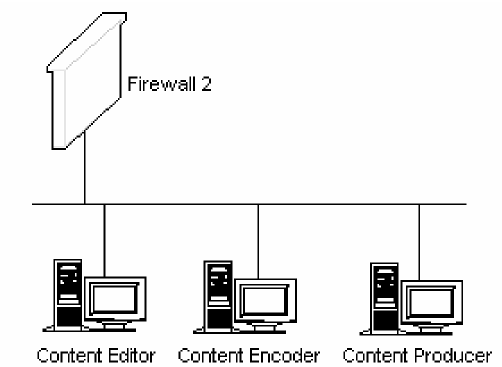

Figure 6: DRM Network

2.5.1 Functionality

The following is only a suggestion of the possible functionality of the DRM network. The BM-SC schedules certain content for delivery. If it decides that the content needs to be DRM protected, the BM-SC forwards the content to the DRM network where it is protected and packaged before delivered to the user. As soon as the user attempts to access the protected content, a request for a licence is sent to the DRM network, which upon payment releases the licence to the UE.

2.5.2 Connectivity

Firewall 2 provides security to the DRM network. The internal interface is a DMZ interface and this allows selected bi-directional traffic. Port filters can be used to restrict attempts for accessing other applications. A tunnel can also be used between router 3 and a potential router in the DRM network to provide connectivity with the BM-SC and the UE.

2.6 Applicability of the commercial system design to the Test Bed R2

The test bed model is designed to test the successful operation of the network. As it is a test model, the services are not fully integrated, but some elements are simulated and simplified. The following text specifies the applicability of the commercial design to the test bed R2.

For test bed R2, no content providers will be used. The streaming and web servers can be located next to the BM-SC, feeding the data via a router and a switch. They are also used to achieve the closest possible simulation to the real system. If this is the case, routers 1 and 2 will not be needed. IP tunnelling can still be configured and supported if required. Router 3 is still needed. The DRM network will not be used and security aspects will be simulated.

The satellite and the return links will be configured differently in the laboratory and field test beds. In the laboratory test bed, the satellite link will be simulated. A SIMSTAR emulator will be used to replace and simulate the satellite and an RNC simulator will replace the RNC. For the return link, no terrestrial network operator will be involved. The GPRS return link will be replaced with a direct Ethernet connection. A GPRS emulator will be used in conjunction with the second handset to allow the dual mode capabilities of this handset to be analysed. In the field test bed, the satellite and the transmission part of the hub will be replaced by an equivalent transmitter located in a high altitude place and the RNC will be replaced by an RNC simulator. Finally, for the return link, a live GPRS network will be used.

3 NETWORK LAYER FUNCTIONALITY FOR THE R2 TEST BED

The Network Layer functional architecture is an end-to-end view of the functions to be implemented and an indication of which network functions of the commercial SDMB system should be supported and tested within R2.

The basic functional architecture is shown in **Figure 7** (from WP6).

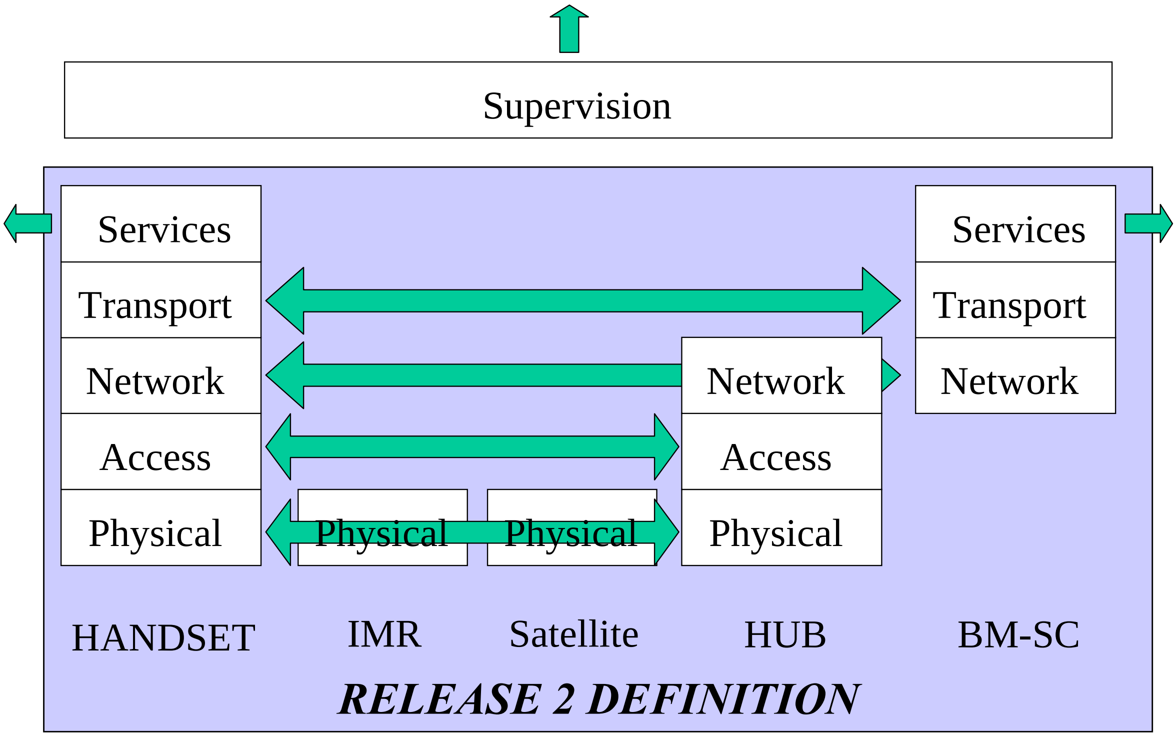

Figure 7: R2 Basic Functional Architecture

The end-to-end protocol stack is presented in Figure 8. There are certain differences of this stack with the commercial one. The first one is the need for security between the application servers and the BM-SC. These two entities will be in different physical locations and thus security is needed on this path. Furthermore, the SDMB MT and TE will be the same physical entity (i.e. UE) and no USB connections will be needed. Finally, the UE will be communicating with the GPRS network wirelessly and not via any physical connection as it is designed for the test bed.

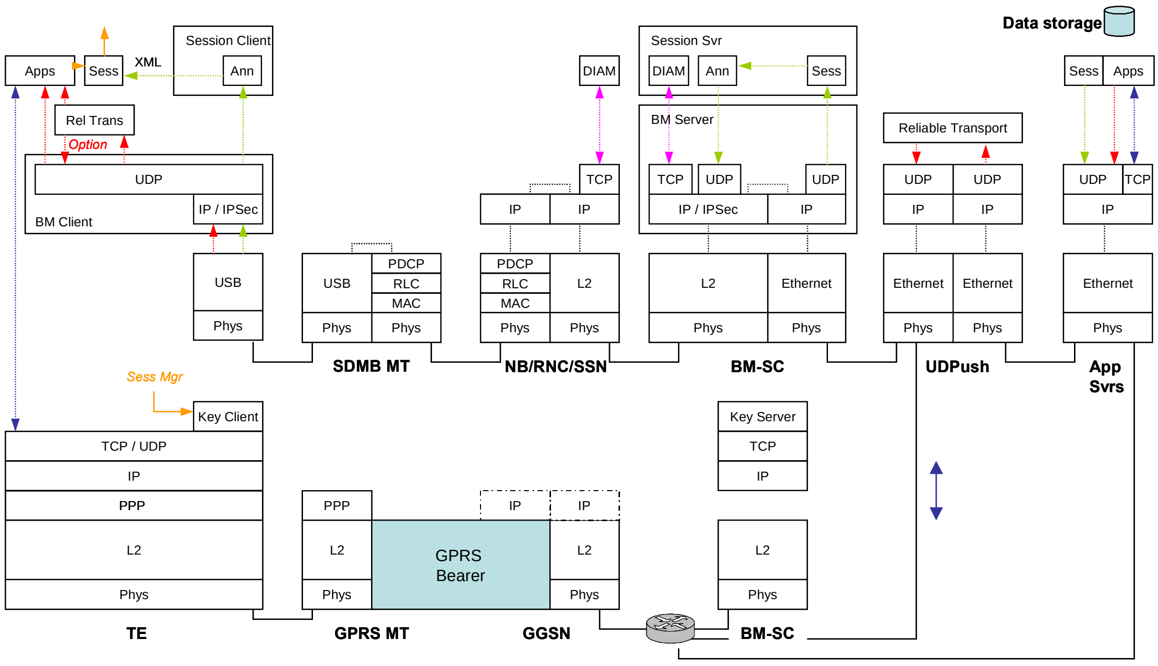

Figure 8: Test Bed Protocol Stack

3.1 Network functions of the commercial SDMB system that should be supported and tested within R2

In the scope of the R2 test bed, it is proposed that the following network functions will be implemented.

- User Authentication
- User Authorisation
- Cyphering
- QoS
- Addressing Scheme

For the scope of R2 test bed, no external content providers will be used, but internal local servers will substitute them. Thus, there is no need of authentication and authorisation of the content providers. Furthermore, billing functions will not be implemented for R2. A live DRM network will not be used and thus, alternative protection and encryption mechanisms should be followed.

The following sections define what functionality will be supported by the test bed under each of the categories listed above.

3.1.1 User Authentication

Authentication can be performed at two levels in the system:

- During attachment to the GPRS network to set up the unicast PDP context between the handset/TE and the test-bed servers. This will use standard

  GSM Authentication and Key Agreement (AKA) mechanisms either with the SIM in the handset, or SIM-enabled GPRS card for insertion into the TE (eg PCMCIA card in laptop). A forwarding mechanism may be required between the GPRS network and the BM-SC where the servers lie.

  - During SDMB ‘session join’, ie a user requesting access to one or more SDMB services. While work ongoing in the TSG SA3 WG on MBMS security is currently focussing on bootstrapping this session-level authentication onto the AKA mechanism, this will not be possible for the R2 testbed and an alternative mechanism will be used instead. This will authenticate the user based on a PKI certificate stored on the TE device, with the session-level join negotiated through signalling exchanges between the TE and BMSC.

The first level applies to the field test bed only, while the second level will be used within both the field and laboratory test beds.

3.1.2 User Authorisation

Authorization is the process of checking that a user actually has permission to access the particular network service that they are requesting. Typically these permissions are stored in a database that defines in detail the individual services that the user is allowed to access.

To demonstrate user authorisation, the release 2 test bed can provide the following functionality:

- A database (in the BM-SC) into which the following information can be provisioned as a minimum:
  - Details of the services that are to be supported by the test bed
  - Details of all of the users of the test bed including their access privileges to the services.
- A mechanism for the user to request access to one or more of the services;
- A mechanism for the BM-SC to verify that the user has the necessary privileges to be able to receive the service;
- A mechanism to communicate the authorisation decision back to the user.

3.1.3 Ciphering/Deciphering

Ciphering (or encryption) provides the means to secure and control user access to the SDMB application content and ensure the confidentiality of information exchange on communications networks. Through the use of ciphering, only registered subscribers are able to receive the content, thereby enabling the value chain from content source to user to be tightly controlled.

In the SDMB context, an important aspect will be that the ciphering mechanism employed is capable of securing transmissions to large groups of users rather than to individual users. In addition, it will also be important that the ciphering mechanism employed minimises the management overheads on the network to ensure that precious bandwidth is not wasted and the benefits of broadcast undermined.

It is proposed that the release 2 test bed will support ciphering between the BM-SC and the TE using an IP-based encryption method. The key management protocol employed within the test bed will be able to support groups of users in an efficient manner that will minimise management overheads on the network.

3.1.4 QoS

There are two aspects to QoS control within the test bed:

- The network connection that will carry user traffic between the BM-SC and the Hub (ie the Gi* interface) may need to be configured to support a particular QoS for each of the services that are to be supported over the test bed. However, the requirement for supporting QoS management on this interface will largely be dictated by the nature of the interface between these two entities. This subject is for further study between LogicaCMG and ERCOM.
- The establishment of broadcast bearers, whether in the propagation channel emulator in the laboratory test bed or the transmission equivalent in the field test bed, will be controlled using the signalling control plane interface between the BM-SC and the Hub (ie the Gmb* interface). This interface will include specifying the QoS parameters that must be provided by the radio bearer.

3.1.5 Addressing Scheme

The addressing scheme to be adopted is dependent on the overall physical architecture to be adopted, in particular the means for integrating the test bed architecture with the MNO network for supporting the back channel.

This principally affects the addresses allocated to the SDMB UEs (in MT or TE), which could be allocated within some private SDMB address space (if the back channel can be tunnelled over the MNO GPRS network all the way to a router sited at the test-bed ‘head end’) or within the MNO address space itself. The means for setting up back channel connectivity through the GPRS network needs to be agreed with the MNO concerned.

Another aspect requiring further attention is the means for supporting delivery of IP multicast packets over the R2 radio broadcast link. It is believed that IP multicast packets (with suitably allocated Class D private multicast addresses) can be generated by the BM-SC and directly transported over the radio link through the MT and onto the TE device. The alternative, less-desirable option, is to tunnel IP multicast packets over IP unicast for point-to-point transmission to the TEs.

4 NETWORK LAYER LOGICAL ARCHITECTURE FOR THE R2 TEST BED

The Network Layer Logical (or Organic) Architecture of the R2 test bed can be considered as an organic or logical view of the network functions, that is a description of how the functions are split among the different organs of the test bed. It comprises a high-level description of each organ and interface of the test beds and identifies specific network scenarios to be tested in R2

Within the scope of R2, the MAESTRO study includes the setting up of two platforms, a laboratory trial and a field trial.

The objective of the laboratory test bed is to provide a platform to complement simulation results. The laboratory test bed will not use an established GPRS network, rather is proposed that this will use a direct Ethernet connection. A key requirement of the laboratory platform is to allow reproducibility.

The objective of the field trial is to demonstrate the basic feasibility of the SDMB system by using an integrated terminal. The field test-bed will include a live GPRS network.

Figure 9 illustrates the basic SDMB architecture and how it is split within the test bed. This architecture requires the use of the return link to authenticate the terminal from the BM-SC perspective.

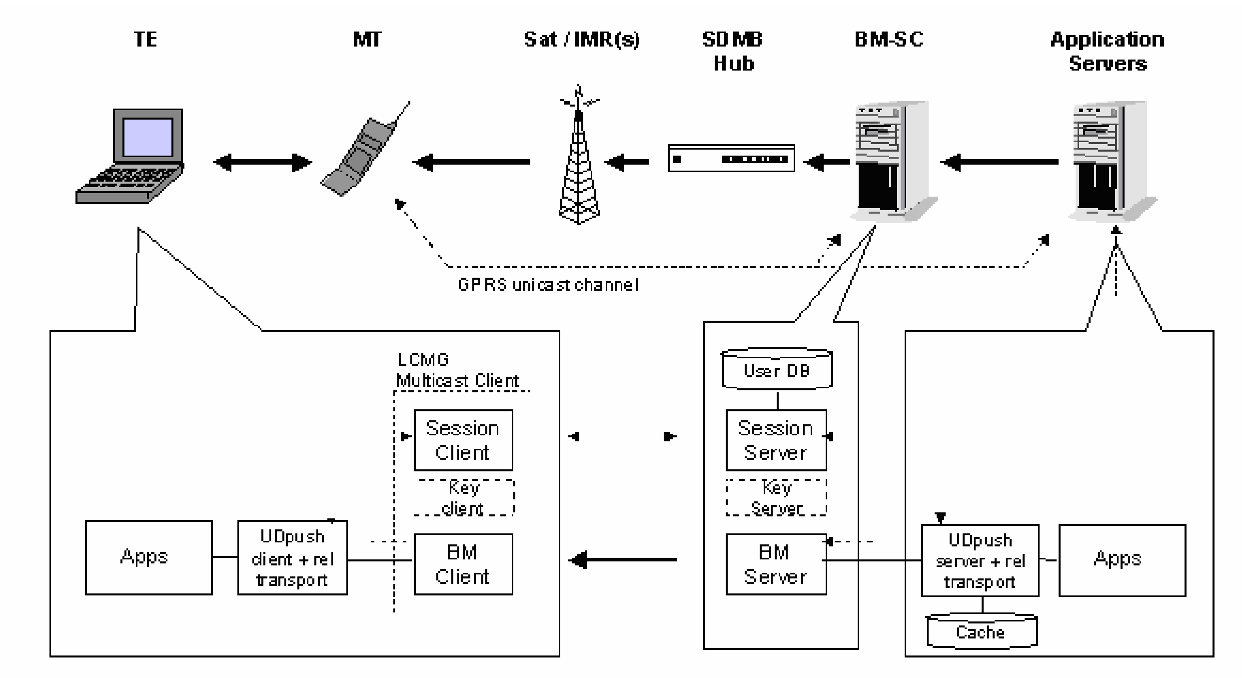

Figure 9: Basic Test Bed Network Architecture

Test Bed Application Servers

There are no application requirements described in the MAESTRO technical annex, so it is proposed to use very simple streaming applications. The content servers are outside the scope of this network layer report.

Test Bed BM-SC

The BM-SC contains the user database, session and broadcast / multicast servers. The authentication and authorisation mechanisms are likely to differ from the commercial system because the range and functionality required for a commercial system has not yet been developed. The BM-SC is a key element for the network layer design.

Test Bed User Equipment

The UE comprises a modified 3GPP mobile terminal connected to a PC. The mobile implements Layer 1 (Physical) and Layer 2 (Link) functionality only, so is outside the scope of this report. However, the PC implements network layer functionality.

4.1 Laboratory Test Bed

The Laboratory Test Architecture Bed is shown in **Figure 10** (from WP6) and is described in [Ref D6-2].

The laboratory platform differs from the commercial model in the following:

- The SIMSTAR emulator replaces the satellite. It features both satellite and terrestrial multi-path channels. Each channel can emulate up to 6 uncorrelated multi-path. The SIMSTAR emulator operating in the IF domain, frequency conversion modules are required at each end of the emulator.
- The RNC simulator is adapted to provide the broadcast Hub functions. It features broadcast support.
- The UE comprises a modified 3GPP mobile terminal connected to a PC. The mobile implements physical and access layers functionality while the PC implements network, transport and application functions.
- The terrestrial link will be simulated by a GPRS emulator.

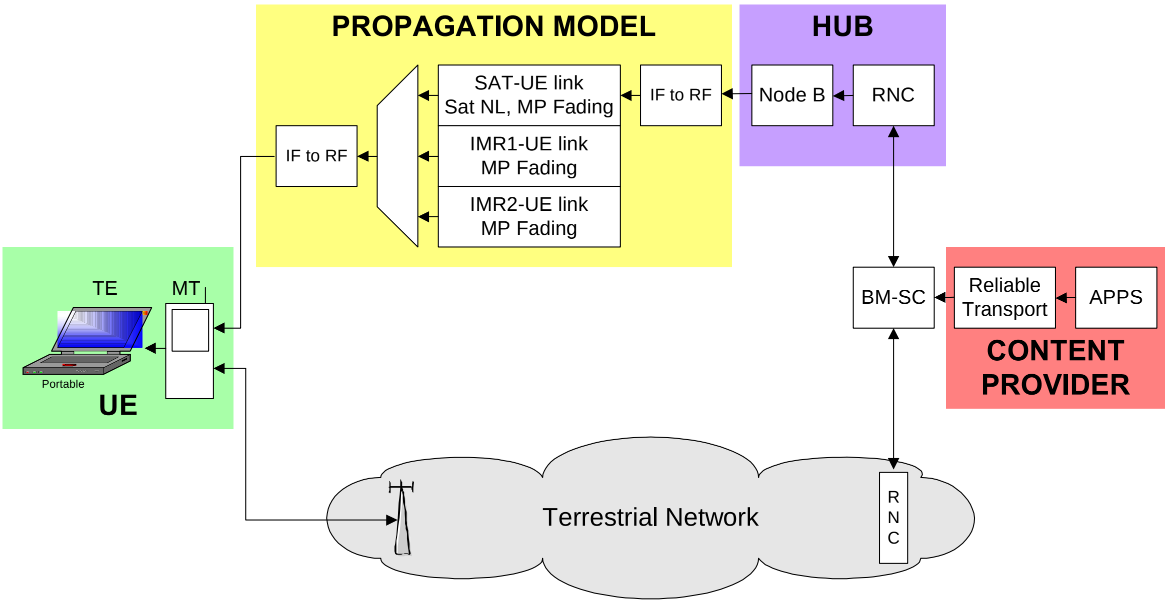

Figure 10 : Laboratory Test Bed Network Architecture

Test bed Network Layer design applies mainly to the BM-SC, but the RNC and UE are also relevant.

4.1.1 BM-SC Network

The BM-SC is proposed to support all of the network layer functionality described in chapter 3.1. An overview of how this functionality can be provided is summarised below.

- User authentication

  The test bed BM-SC can support the necessary functionality to implement a dedicated PKI infrastructure for the test bed system. This will include the capability to generate certificates and public keys and store these securely on the TE and on the BM-SC itself. This will ensure that all management exchanges between each TE and the BM-SC will be mutually authenticated.

- User authorisation

  The test bed BM-SC can provide a service management facility to allow the provisioning of service and user details onto the system. It will be possible to define the services, which are to be transmitted across the test-bed network, and the access rights of each user within the test bed to access these services.

- Ciphering / Deciphering

  The test bed BM-SC can provide a facility which handles the generation and distribution of ciphering keys to authorised users within the test bed so that they are able to decrypt one or more of the services to be demonstrated and access the content. A highly efficient key management mechanism will also be provided that will help ensure that security management overheads are kept to a minimum. The above mechanisms will be based on two emerging standards being developed within the Internet community to manage subscriber access and distribution of keys. These are the Group Secure Association Key Management Protocol (GSAKMP) and Logical Key Hierarchy (LKH).

- Qos Control

  The test-bed BM-SC will support the Gmb* interface with the Hub. The Gmb* interface will allow the BM-SC to specify the QoS parameters that must be supported by the radio bearer. The ability to apply QoS control on the Gi* interface will be dependent on the nature of this interface in the test bed e.g. if a tunnelled internet connection has to be used then QoS control will not be possible. Alternatively, if a high bandwidth connection is used the need to apply QoS control at all for the purposes of the test bed is questionable.

4.1.2 RNC Network

The RNC main function is to receive SDMB Data from the data generator and to forward them to the Node B. The RNC is implemented by ERCOM and includes a set of UMTS protocol layers. Even though the terminal will only be able to decode one S-CCPCH, the RNC must be able to generate multiple S-CCPCH to allow interference performances measurement.

4.1.3 UE Network

The UE can be split in two entities namely the terminal equipment (TE) and the mobile terminal (MT).

The MAESTRO release 2 MT will be based out of a 3GPP compliant mobile terminal, which has been modified so as to be able to receive SDMB broadcast data while processing basic signalling on the GPRS network. The MT hosts physical and access layers functionality of the UE.

The MAESTRO release 2 TE will be a PC. It hosts network, transport and application layers functionality of the UE.

The TE connects to the MT using modem like interfaces. There should be one unidirectional interface from the MT to the TE for the SDMB data and one bidirectional interface for the GPRS data to allow the use of return link. The TE also provides some debugging tools such as RTA.

The limit of a 3G channel is 384kbps. If more bandwidth is required, more channels will be needed.

Figure 11 illustrates the high level UE architecture.

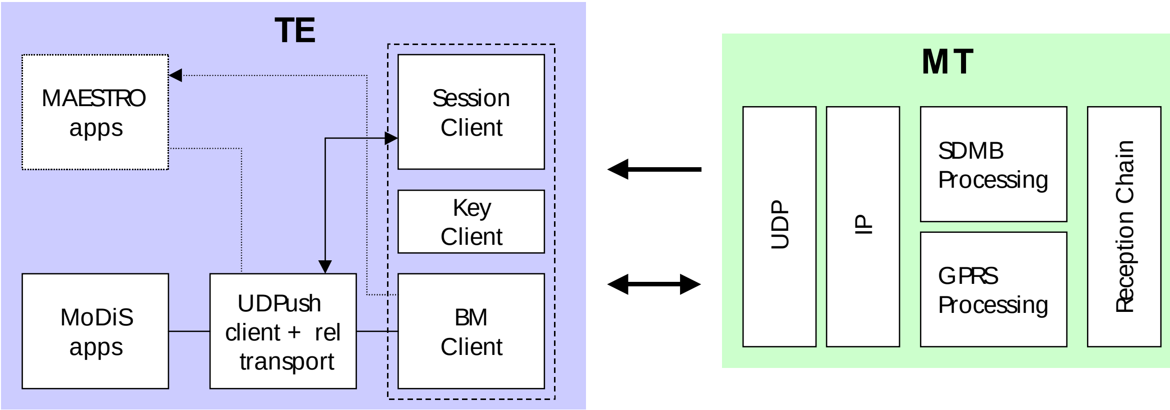

Figure 11 : UE Architecture

4.1.4 Terrestrial network

One of the goals of MAESTRO release 2 test bed is to prove the dual mode operation of the UE, which should allow SDMB content reception in parallel of basic signalling from GPRS/UMTS network processing.

It is suggested that this mode will be tested using a GPRS network emulator This solution is really attractive because it would allow to evaluate the performances of the reliable transport for different DRX periods and to eventually measure the impact of a relocation on those performances. However, such an equipment is really expensive and has not been budgeted in the scope of MAESTRO. Therefore this solution will be implemented only if one of the MAESTRO partner (MSPS for example) could lend a GPRS emulator for the duration of the release 2 laboratory test bed integration and validation.

4.2 Field Test Bed

Figure 12 illustrates the Field Test Bed network architecture.

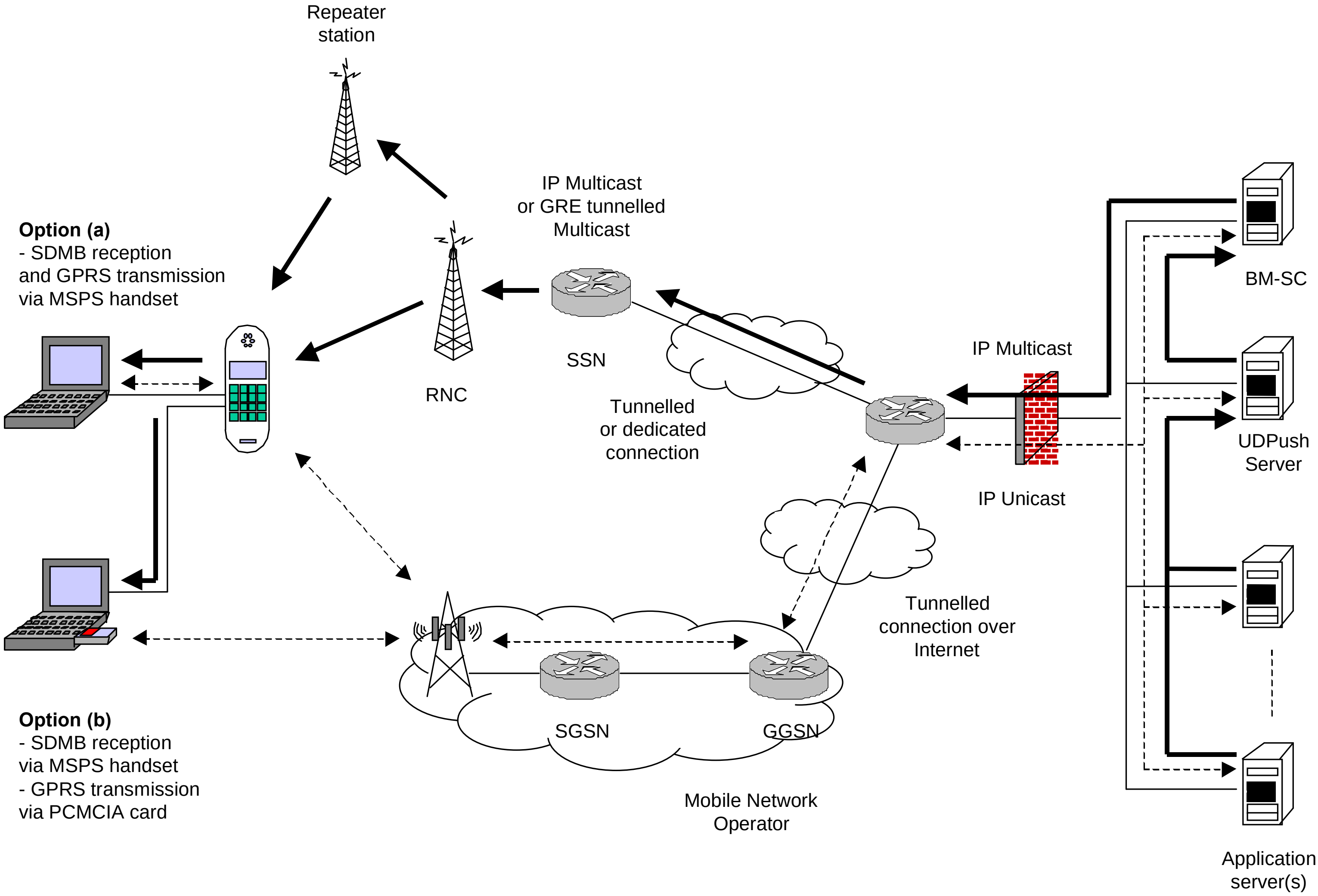

Figure 12 : Field Test Bed Architecture

The ideal is to transmit IP multicast over SDMB and through the handset, however the handset may not allow this facility at this stage of development, in which case the alternative is to tunnel the multicast down a point-to-point link, e.g. using GRE tunnelling. This latter alternative is not favoured because the use of statically configured point-to-point tunnels will reduce the impact of the demonstration. It is believed that class D addresses will be supported by the TE and thus, the first case will be used.

The field platform differs from the real SDMB system in the following:

- The satellite and the transmission part of the Hub will been replaced by an equivalent transmitter located on a high altitude place (mountain, etc.), set in such a way that the received radio level at the terminal is about equivalent to what would be received from a satellite. For the trial, transmission will be performed in the terrestrial IMT2000 frequency band. Compared to the laboratory test bed, the propagation channel emulator has been completely removed from the picture, thus constituting the main difference between the two platforms.

- The Hub network function emulator feeds the terrestrial repeaters directly.
- The Hub network functions are fulfilled by a RNC simulator featuring broadcast support and adapted to the MAESTRO application.
- The MAESTRO terminal is composed of a modified 3GPP mobile terminal connected to a PC. The mobile implements physical and access layers functionality while the PC implements network, transport and application functions.

4.2.1 BM-SC Network

Identical to the release 2 laboratory test bed. Refer to chapter 4.1.1

4.2.2 RNC Network

Identical to the release 2 laboratory test bed. Refer to chapter 4.1.2

4.2.3 UE Network

Identical to the release 2 laboratory test bed. Refer to chapter 4.1.3

4.2.4 Terrestrial Network

The field test bed will interact with an existing UMTS network. This latter will be used to test that the terminal can receive SDMB content while performing basic signalling processing on the UMTS network.

5 Conclusions

This document presents recommendations of the possible network layer functions and architectures that could be supported on the MAESTRO release 2 test bed. Two different trials have been proposed, the laboratory and field test bed trials with similar configurations. The main differences are identified on the satellite and return links. In the laboratory test bed, both the satellite and terrestrial links will be simulated using a satellite and a GPRS emulator respectively. In the field test bed, the satellite link will be replaced by an equivalent transmitter located on a high altitude place, while the terrestrial link will be a GPRS network.

The functions that will be implemented include user authentication and authorisation, ciphering and QoS.

6 REFERENCES

[1] D6-2 MAESTRO Release 2 Test Bed Design Document

7 SYMBOLS AND ABBREVIATIONS

2G	2nd Generation (Wireless Communication System)
3G	3rd Generation (Wireless Communication System)
3GPP	3rd Generation Partnership Project
AAA	Authentication Autorisation & Accounting
BM-SC	Broadcast Multicast Switching Centre
DMZ	DeMilitarised Zone
DRM	Digital Rights Management
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
IF	Intermediate Frequency
IMR	Intermediate Module Repeater
IP	Internet Protocol
IPv4 / IPv6	Internet Protocol version 4/ Internet Protocol version 6
FP5	5th Research Framework Program of the European Commission
LAN	Local Area Network
MoDIS	IST FP5 - MObile DIgital broadcast Satellite
MO	Mobile Operator
MT	Mobile Terminal
PCMCIA	Personal Computer Memory Card International Association
R2	Release 2
RF	Radio Frequency
RNC	Radio network Controller
SDMB	Satellite Digital Multimedia Broadcasting
SSN	Service Specific Node
TE	Terminal Equipment
TLS	Transport Layer Security
UE	User Equipment
VLAN	Virtual LAN