PUBLIC

IST R&D. FP6-Priority 2.

SPECIFIC TARGETED RESEARCH PROJECT

Project Deliverable

SUIT Doc Number	SUIT_125
Project Number	IST-4-028042
Project Acronym+Title	SUIT- Scalable, Ultra-fast and Interoperable Interactive Television
Deliverable Nature	Report
Deliverable Number	D1.3
Contractual Delivery Date	30 September 2006
Actual Delivery Date	16 October 2006
Title of Deliverable	All-IP Support Requirements
Contributing Workpackage	WP1
Project Starting Date; Duration	01/02/2006; 27 months
Dissemination Level	PU
Author(s)	Juan Carlos Plaza (UPM), Julián Cabrera (UPM), Fernando Jaureguizar (UPM), Narciso García (UPM), Z. Ahmad (UniS), C. Liew (UniS), S. Dogan (UniS), S. Worrall (UniS), A. Navarro (IT), José Ferreira (Wavecom), Mario Rui (Wavecom), Pedro Pratas (Wavecom), Moti Goldstein (RUNCOM), Alois Zistler (IRT), Michael Probst (IRT)

Abstract

This document analyzes different mechanisms and solutions at the IP level to allow interoperability among the different wireless networks considered in the SUIT project: DVB-T/H/RCT, WiMAX and Wi-Fi networks. It also defines the interfaces at physical, link and network levels for different scenarios according to the type of terminals considered in the project.

Keyword list: All-IP, DVB-T/H/RCT, WiMAX, Wi-Fi.

PUBLIC

All –IP Support Requirements

SUIT 125

16-10-2006

Table of Contents

1. Introduction

This deliverable aims at identifying and analysing different mechanisms and solutions at the IP level to make interoperable the different wireless networks considered in the SUIT project: DVB, WiMAX and Wi-Fi networks. It contains the results of activity 1.3 “All-IP Support Requirements”. This activity is part of WP1 “Architecture Requirements and Specifications” whose main objective is to specify the requirements of the end-to-end SUIT system. Thus, this deliverable acts as an input to activity 1.4 “Architecture and Reference Scenarios” and has strong relationships with the activities of WP1: activity 1.1 “User Terminal Requirements” and activity 1.2 “QoS Requirements”.

This deliverable is organized as follows: Section 2 identifies the main requirements of an All-IP based networks from the SUIT project perspective; Section 3 reviews the main characteristics and services offered by the current versions of the Internet Protocol; Section 4 describes the main functionalities provided by the networks considered; Sections 5, 6 and 7 present different mechanisms and solutions used to support IP over DVB, WiMAX and Wi-Fi respectively; Section 8 deals with interoperability issues among the three wireless networks particularized for the different scenarios considered in the project; Section 9 presents the main conclusions of this document.

2. All-IP approach and the SUIT Project

2.1. Introduction to All-IP concept

The use of Internet Protocol (IP) in the design of networking has become a dominant trend during the last years. Due to the popularization of the Internet thanks to the breakthrough of HTML-based Web and Browser-based user interfaces, new IP-based services are evolving rapidly. At the same time a general change of context from circuit switching networks, which reserve a dedicated and continuously connected path between those points in communication, to a more efficient packet switching approach is taking place. The adoption of this approach influences both the management of network resources, and the convergence of services and technologies.

Vertically-integrated network architectures, such as those dedicated to a single service, are becoming obsolete. Novel applications demand a new model of distributed, fully-compatible network, with the ability to support a great variety of services in a medium-independent manner. In this scenario, the need for a versatile, universal network-layer protocol, which can act as “glue” in between, has been fulfilled with the adoption of IP.

More specifically, the concept of “all-IP network” involves the use of IP-based Core and Radio Access Network architectures, in order to provide services to mobile terminals which are essentially IP host devices. Those services could be voice, data, multimedia contents, or in general any other packetizable flow. An important consequence of this is that the air interface must be optimized for packet data delivery.

An “all-IP” scheme makes possible the interconnection of networks, including the Internet, in a completely direct way. WAP-like translation protocols are no further mandatory, making a wide range of Internet applications directly available for wireless devices. This flexibility livens up the development of new services, contributing to the developing of the networks. Moreover, according to some studies in the matter, the costs of implementation and maintenance can be reduced in an “all-IP” scheme.

Telecom operators and institutions have pushed forward the development of the “all-IP” concept. For example, both 3rd Generation Partnerships (3GPP and 3GPP2) have made an effort in order to define a standard for “all-IP” mobile network architecture [1] [2], capable of providing multimedia services (such as VoIP, videoconferencing, MMS…).

The concept of an All-IP Network (AIPN) was first introduced by the 3GPP (3rd Generation Partnership Project) in its Release 4. According to the definition taken from the 3GPP technical report TR 22.978 v7.0.0, an AIPN is “a collection of entities that provide a set of capabilities for the provision of IP services to users based on IP technology where various access systems can be connected. The AIPN provides a set of common capabilities (including mobility, security, service provisioning, charging and QoS) which enable the provision of services to users and connectivity to other external networks. An AIPN requires one or more connected access systems to allow users to access the AIPN.”

Following with the work of 3GPP, AIPNs implement features such as:

- Network performance: User-to-user, user-to-group and user-to-server IP traffic must be handled and optimized. Multicast models could be supported in the user-to-group case. Generally, the AIPN will take advantage of IP routing and addressing technologies.
- Management of different types of traffic: Huge amounts of traffic from different types (non-real time, real time, mission-critical…) must be managed efficiently, also providing several grades of QoS.
- Addressing: User must be unaware of addresses allocation, which must be carried out automatically and in a completely secure fashion, preventing foreigners from being assigned a valid address.
- IP session control: AIPN operator must manage several aspects of session control and adaptation:
    - Terminal capability, user preferences, subscriber properties, network conditions, user-to-group sessions, power resources, etc.
- Quality of Service: QoS supply shall be guaranteed in user-to-user and user-to-group (multicast) transmissions. Depending on the QoS capabilities of each access system, AIPN must deal with certain constraints.
- Mobility: AIPN must supply end-user, session and terminal mobility, in a fully reliable way and according to several factors such as radio conditions, service requirements, user preferences and operator policies. Mobility should be ‘seamless’, what implies that final user will not experiment an interruption in his/her communication when changing of access system, or during terminal mobility. If due to the terminal mobility the QoS worsens, user could be informed of this by any mean.
- Multi access: Final users must be able to connect to the AIPN through various access systems (EUTRAN, I-WLAN, UTRAN and GERAN…). Mechanisms for identification, authentication and addressing must be supported, and also selection of the best access system according to operator policies, user preferences, service requirements of applications, access system conditions…

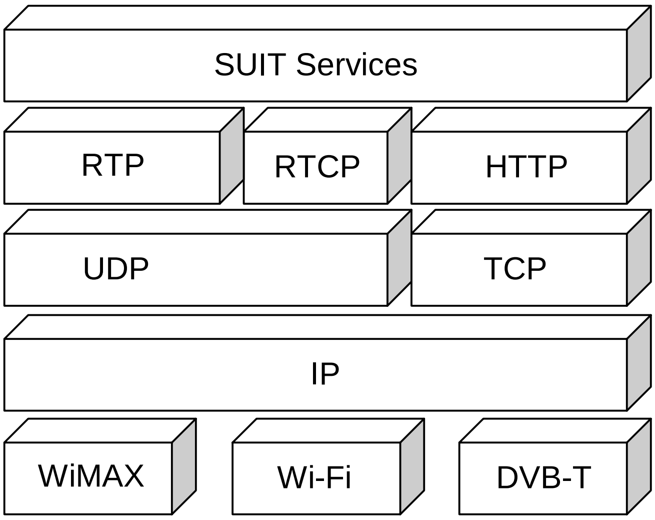


Figure -1 All –IP approach in the SUIT project.

2.2. SUIT Project requirements

One of the main objectives of SUIT project is to demonstrate a 4G multi-network environment for interactive TV under the umbrella of the universal wireless access paradigm. More specifically, SUIT will broadcast and stream audiovisual content to fixed and mobile subscribers through DVB and WiMAX networks. In addition, it will also consider an extended local environment where end user terminals can access the services via a Wi-Fi network. Therefore, there is a close relationship between the required SUIT network and an AIPN (see Figure -1). In particular, following the “all-IP” philosophy the following requirements can be identified for the SUIT project:

- **Encapsulation:** The use of IP as a common network-level protocol within a system with different link layers (DVB, WiMAX and Wi-Fi) requires the definition of the encapsulation of IP datagrams in the different frames of the used layer-2 protocols. Although in some cases, such as in Wi-Fi networks, this issue is straightforward due to the close relationship between Wi-Fi networks and IP protocol, in other cases, as with DVB, the encapsulation is more complex and different approaches may be used.
- **Addressing:** The association of layer-2 info with the IP address of a system usually requires a mechanism for Address Resolution (AR). A common way for layer-2 technologies to perform this association is via unicast AR at the sender. In this case, the only information required for AR is the association between IP and MAC addresses. Nevertheless, in some cases AR may involve finding other information than the MAC address, as PIDs in MPEG-2 TS. In addition, address resolution has different purposes depending on the type of transmission, either unicast or multicast/broadcast.
- **Network performance:** In addition to broadcasting audiovisual material, the SUIT project also considers streaming unicast contents, the provision of Internet access via the SUIT platform, and the existence of a return channel for end user interactivity. The provision of these services results in diverse types of IP traffic that must be efficiently managed and optimized (user to user, user to multicast group…). This optimized management may take advantage of the layer-2 capabilities of the wireless networks considered (reliability, unicast/multicast services) and of the technologies involved in IP routing and IP addressing.
- **Quality of Service:** SUIT project aims at providing QoS, in terms of bandwidth and delay, for the end to end services. Diverse techniques can be used to satisfy QoS requirements at

different levels: at layer-2, taking advantage of QoS provided by the wireless channels if any, at IP level if the version of the IP supports it, and at higher levels using specific protocols or mechanisms such as ‘Diffserv’.

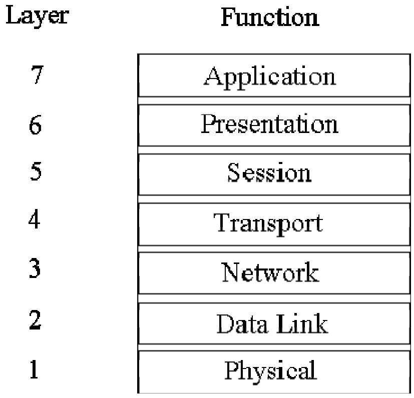
- **Mobility:** Both horizontal and vertical handovers are expected to be supported by SUIT project. Techniques driving to these implementations have to be considered again at different levels: at layer-2, taking advantage of mobility support if provided by the wireless, at IP level if provided, and at higher levels using specific protocols or mechanisms. In addition, handover should take into account QoS information if used.
- **Multi access:** SUIT terminals will be able to access the network through DVB-T/H, WiMAX or synergetic combination of both. Besides, SUIT gateway will extend accessibility to Wi-Fi terminals. A wide range of devices (PDAs, HDTV terminals, laptops…) will be able to receive scalable content adapted to their particular needs and network conditions.
- **Inter-working:** The diverse radio technologies used in SUIT project network must be kept as interoperable as possible. Using a common IP network layer will enable this, though best mechanisms at IP driving to this convergence must be evaluated.

3. Internet Protocol overview

3.1. IPv4

3.1.1. Introduction

Data transmission within a network, or from one network to another, requires a complete set of inter-working protocols (“protocol suits”). These protocols can be grouped into different functional layers, depending on the particular tasks they accomplish. According to the ISO/OSI network model up to seven layers are distinguished:



Layer	Function
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Figure -2 Layers in the OSI model

Internet Protocol [3] is located at the network layer (layer 3). Consequently, it must be able to direct datagrams across the network, therefore implementing a series of services and functionalities:

- Adequate addressing of network interfaces.
- Efficient routing, both in one-to-one and one-to-group transmissions.
- Datagram segmentation/reassembly, depending on the capacity of each network.

Particularly, the Internet Protocol offers an “unreliable” (best effort) service, what implies that:

- Data in packets may be corrupted in the transmission
- Packets may arrive duplicated, out of order, or not arrive at all.

Reliability issues must be carried out by upper layer protocols, for example TCP.

Nowadays, most extended version of Internet Protocol is IPv4. Versions from 0 to 3 were reserved or never used, while number 5 was assigned to an experimental protocol. IPv4 is expected to be replaced by IPv6, a new generation protocol that takes into account the unforeseen success of IPv4 and tries to solve some of its limitations, such as address shortage, quality of service provision and scalability issues. In the following sections the main characteristics and functionalites of IPv4 are described.

3.1.1.1. Header format

Packets coming from upper-layer protocols (TCP, UDP…) are embedded into IP datagrams, by adding a “header” with some useful information for the Internet Protocol (addressing, fragmentation settings…). The following figure shows IPv4 header fields:

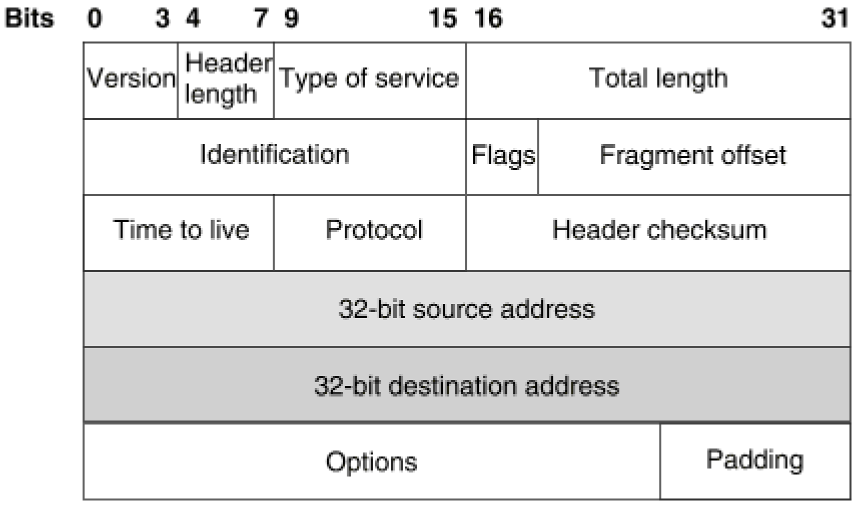


Figure -3 IPv4 header

These fields have the following length and meaning:

- **Version** (4 bits): Format of the IP packet header.
- **HL, Header Length** (4 bits): Length of the IP packet header in 32 bit-words. Its minimum value is 5.
- **TOS, Type of Service** (6 bits): Parameter specifying the type of service requested. May be utilized to define the management of the datagram during transport.
- **Total length** (16 bits): Length of the datagram in bytes.
- **Identification** (16 bits): This value must be unique for each source-destination pair while the datagram is valid.
- **Flags** (3 bits).

  - **R, Reserved.** 1 bit (should be set up to 0)
  - **DF, Don't Fragment.** 1 bit.
  - **MF, More Fragments.** 1 bit.

- **Fragment Offset.** (13 bits). Controls the reassembly of a fragmented datagram.
- **TTL, Time to Live.** (8 bits). This counter can be decremented in each hop. When it is equal to zero, the packet is dropped.
- **Protocol.** (8 bits). Specifies the encapsulated protocol.
- **Header checksum.** (16 bits). A 16 bit one's complement checksum of the IP header and IP options.
- **Source IP address.** (32 bits). IP address of the sender.
- **Destination IP address.** (32 bits). IP address of the receiver.
- **Options.** (Variable length).

3.1.1.2. Addressing

As it has been seen above, IPv4 uses 32-bit address fields, so 4,294,967,296 interfaces are theoretically identifiable. However, this apparently enormous quantity is short in fact, since many address ranges are reserved or destined for special purposes (private networks, multicast…).

IPv4 addresses are usually represented in “dot-decimal” notation. Decimal values of each one of the four bytes that form the IP address are separated by dots, adopting (for example) this form: “138.100.17.59”.

Taking the first octet as a network identifier and the rest as interface identifiers, up to 256 networks were formerly defined. These were clearly insufficient, so the next “classful” scheme was set up:

Class	First bits	Number of networks	Number of addresses per network
Class A	0	126	16,777,214
Class B	10	16,384	65,534
Class C	110	2,097,152	254
Class D	1110	Multicast addresses	
Class E	11110	Reserved range	

Figure -4 Classful addressing scheme

The problem with this scheme was that most of the LANs had some more than 254 hosts, and consequently were assigned a Class B range, wasting a huge quantity of addressing space.

Classless Inter-Domain Routing (CIDR) was introduced in 1993 in order to overcome this drawback. Division between network and host identifiers is made more flexible, by adopting a binary mask solution. Network prefixes (or address ranges) are specified by an IP address followed by a slash and a number between 1 and 32 (prefix length); for example, “172.16.0.0/12”.

Prefix length denotes the minimum number of initial bits that addresses within that range share with address specified. Following the example, all addresses whose 12 first bits are the same than the first 12 bits of 172.16.0.0, form part of that range/network (for instance 172.24.131.12).

This scheme leads to a more efficient routing, that takes advantage, for example, of "prefix aggregation" (that is, all networks that share a same prefix can be managed as a single CIDR block).

3.1.1.3. Delivery schemes

IP Unicast

Unicast is the term employed to describe communication between two single points, so there is just one sender, and one receiver. IP Unicast delivery, in which IP packets are sent from one source to a single specified destination, is the leading way of transmission through the Internet.

IP Multicast

When distributing the same content to a group of destination terminals, sending an individual copy from the source to each receiver can be rather inefficient. This is especially relevant in high-bandwidth demanding applications, such as video transmission. IP Multicasting techniques preserve resources by sending, if possible, a single copy of the packet stream and replicating it in routers only when necessary for distribution purposes.

Multicast is based on the concept of "multicast group". By means of Internet Group Management Protocol (IGMP), hosts that want to receive a particular content ask for being included in its distribution group (Membership Report). Periodically, source emits a "Membership Query" in order to verify there is at least one host in the group, and stops transmission if not. IGMP version 2 includes some additional features, such as a specific "Leave Group" message. Each multicast group must be assigned an individual multicast address within the Class D range (224.0.0.0 to 239.255.255.255), which is included in IGMP messages.

Two different structures are used for multicasting distribution:

- Shortest Path Trees (SPTs): the root of the distribution tree is located in the source, and packets are forwarded through the network according to a shortest path algorithm. Streams from different sources which are sent to the same multicast group make use of separate SPTs.
- Shared Distribution Trees (SDTs): all sources sending packets to the same multicast group forward their streams to a common root, or "Rendezvous Point". This reduces the state information that must be stored at routers, reducing memory requirements, but latency can be increased as a result of not using shortest paths.

IP Broadcast

When a piece of data is intended to be distributed to all receivers connected to the network, the term "Broadcast" is used. Different IP addresses are set up for supporting broadcast (one-to-everyone) traffic.

- Network Broadcast Address: for the distribution of packets to every host within a "classful" network, an address with all its "host bits" set up to 1 can be used.
- Subnet Broadcast Address: the same concept is exported to "classless" addresses by means of subnet broadcasting address, where all "host bits" in the CIDR scheme are also set up to 1.

- All-Subnet Broadcast Address: when all “host bits” of the “classful” address containing a “classless” address are set to 1, the packet is intended to be forwarded to all hosts within the subnetted “classful” net. However, this technique is not frequently implemented in routers.
- Limited Broadcast Address: packets sent to 255.255.255.255 are distributed to all hosts within the local network, with no need of knowing their actual IP addresses. This feature is commonly used by some protocols, such as DHCP.

3.1.1.4. Fragmentation and reassembly

In order to enable the transmission of datagrams through diverse networks, fragmentation is implemented in IPv4. Thus, if the Maximum Transmission Unit (maximum length of a packet that a concrete network is able to manage -MTU-) is lower than the IP datagram length, it is split in several pieces. This process was decided to take place at IP level so as to avoid redundant fragmentations in other protocols and to improve efficiency at link level.

Fragmentation and reassembly is controlled by some fields in the IP header:

- More fragments (MF): The MF flag is set to one in every fragment except the last fragment.
- Total length: according to each segment size; must be inferior to the MTU.
- Fragment offset: indicates how many data bytes have been already sent in anterior packets.

According to these parameters, reassembly at final host is fully determined. If MF is set to one, or if total length is not equal to zero, then the received packet forms part of a fragmented datagram, which can be recomposed taking into account the fragment offset fields.

A special flag (DF) prevents a packet from being fragmented.

3.1.2. IPv4 limitations

3.1.2.1. Address shortage

Not only the limited set of addresses and their suboptimal distribution, but also the growing number of terminals connected to the Internet (new mobile devices, always-on devices which do not free their IP addresses…) demand a solution for the IP addresses shortage. IPv6 is expected to solve it, but other approaches are being tried meanwhile:

- Private networks and Virtual Private Networks (VPN)

  In IPv4, hosts inside a non-public network are normally assigned IP addresses from the “private internet” ranges (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16). Routers are configured to discard all packets with addresses within those ranges, to increase security and confidentiality. In order to connect with external devices, proxy servers or NAT gateways (as explained later) are needed.

  To communicate hosts in two private networks as if they were a single one, a VPN (Virtual Private Network) is used. With this technique, private IP packets from a private network are encapsulated (maybe encrypted) into public IP packets, and sent across the Internet to the other private network. When they arrive to their destination, they are decapsulated and considered as if they had been originated in the final network.

- Network Address Translation (NAT)

  This technique enables multiple hosts to access the Internet with a single public IP address, by modifying source/destination addresses in IP packet headers. These changes take place in a router or a firewall, and improve security within the private network. However, NAT carries several drawbacks, such as malfunction of some end-to-end protocols or applications (FTP, UDP, SIP, IPsec…). These could be overcome partially by using “application-layer gateways” (ALGs).

- Network renumbering

In the first years of the Internet huge ranges of IP addresses were granted without taking into account its possible development in the future. In order to solve that situation, recent efforts have been made to fairly redistribute this short resource.

- Dynamic Host Configuration Protocol (DHCP)

DHCP is a client-server networking protocol, used to grant a client device specific information (for example the name of DNS server) about how to connect to an IP network. It is also used to assign IP addresses dynamically. Different implementations of DHCP make use of different methods for this allocation:

  - Manual assignment: administrator manually sets up a table of MAC address / IP address pairs.
  - Automatic assignment: administrator specifies a range of IP addresses and DHCP allocates them automatically.
  - Dynamic assignment: IP addresses within the range specified are allocated to client hosts for a certain period of time, and by means of TCP/IP software. This technique facilitates addresses to be reutilized.

3.1.2.2. Quality of service

Some applications (like real-time ones) need a guaranteed quality of service, in terms of percentage of packet loss, jitter, delay… etc. IPv4 was not designed with this philosophy, but as a “best-effort” protocol. Nevertheless, depending on the characteristics of the network, several approaches to solve this problem are suitable. If enough bandwidth is available, the most practical solution is over-dimensioning resources destined to such applications. Otherwise, different techniques have been proposed:

- Multiprotocol Label Switching (MPLS) [7]: defines an architecture and its corresponding protocol for encapsulating IP traffic. It adds QoS-efficient routing information, using 4-byte extra-headers. These labels allow routers to forward MPLS packets through predefined paths, depending on the type of traffic, by assigning them a given Forward Equivalence Class (FEC). MPLS makes some assumptions about the underlying layer-2 protocols in order to optimize mapping, for example, to connection-oriented ATM virtual circuits.
- Integrated Services (IntServ): QoS is guaranteed by reserving network resources for demanding applications. This technique makes use of the Resource Reservation Protocol (RSVP), which forces core routers to attend petitions and maintain reservations from those applications, overcharging network infrastructure in a hardly scalable way.
- Differenciated Services (DiffServ): [6][8] is an IETF standard. It’s an evolution from IntServ (Integrated Services). However, DiffServ is more scalable, and doesn’t need any kind of reservation protocol. Unlike MPLS, DiffServ is strictly Layer-3, so that it works directly over any Level-2 infrastructure supporting IP.

  Old Type of Service (ToS) field is recycled into a new DS byte, which is used in practice to assign different priorities to the packets. Thus, five bits specify the Per Hop Behaviour

(PHB), the chosen forwarding procedure. Two main PHBs are defined for DiffServ: “Default” (DE) and “Expedited Forwarding” (EF). DE consists basically of a FIFO (“first-in first-out”) queue, while datagrams marked with EF-PHB are sent to a preferential queue, supposed to maintain low values of packet loss, latency and jitter. DS field also includes an IN bit, used for congestion control. Packets with IN bit set to 0 are the first to be dropped out in a congestion context. PHB+IN six-bits field is also known as Differenciated Service Code Point (DSCP).

This approach shows an important drawback: all packets marked with the same forwarding class will be treated equally, so distinguishing between individual flows within is not possible. DiffServ demands packet priorities to be set up at network edge routers. This causes an inevitable increase in end-to-end delay. From that point, DS-supporting core routers will take per-packet forwarding decisions, by interpreting headers in two possible ways: “Behaviour Aggregate” (BA), which classifies datagrams according their DS byte, or “Multifield” (MF), also reading other fields of the IP header.

3.2. IPv6

3.2.1. Introduction

Internet Protocol Next Generation [5] (IPng, now commonly known as IPv6 [4]) was designed to overcome some limitations of IPv4, fundamentally related to addressing capabilities, and to provide new features, for instance, security or quality of service, always keeping scalability and extensibility in mind. It is expected to replace IPv4 in the next decades, though it has to face some questions such as interoperability and corporative resistance to change.

3.2.1.1. Header format

This is a scheme showing IPv6 header fields:

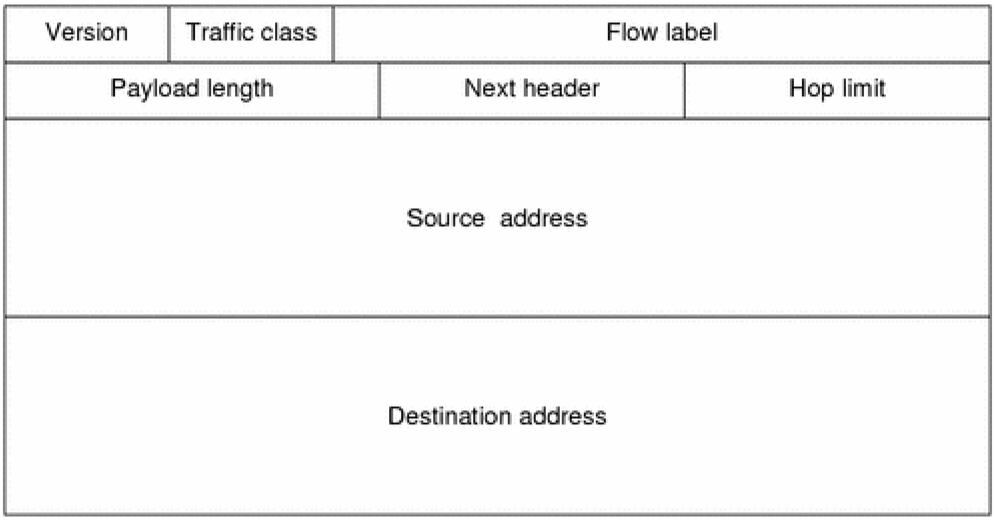


Figure -5 IPv6 header format

- **Version –** Internet Protocol Version number (6 for IPv6).
- **Traffic class –** This field is used to set up some priority grades on delivery of the packets. Priority values are classified into two groups depending on whether the source supports congestion control or not.

- **Flow label** – A packet flow is uniquely identified by the couple formed by a source address and a non-zero flow label. By means of it, special handling at the IPv6 router can be requested.
- **Payload length** – Length of data field in the datagram.
- **Next header –** Type of header following the IPv6 header.
- **Hop limit** – Analogous to TTL field in the IPv4 packet. Decremented in each node that forwards the packet, forces packet to be discarded if it is equal to zero.
- **Source address –** 128 bit address of the source of the packet.
- **Destination address –** 128 bit address of the intended recipient of the packet, which might not be the final recipient if there is a “Routing” header.

3.2.2. IPv6 extensions

3.2.2.1. Expanded addressing and routing

Length of IPv6 addresses is 128 bits, instead of 32 bits used in IPv4. These are grouped into two 64-bit pieces: one for the “network number” and the other for the “host number”. This separation has its origin in an IPv6 requirement, that expects IPv6 to be able to address around 10^{40} networks and 10^{50} hosts. This allocation of bits is sufficient for both needs.

The addressing capacity of IPv6 (around $3 \cdot 10^{38}$) is unimaginably large. Nevertheless, it must be considered that many of these addresses could be reserved for special purposes, or that one host could need more than one address, depending on number of interfaces used by future applications.

IPv6 also names addresses differently. An IPv6 address is formed by groups of four hexadecimal digits, where the dot (‘.’) has been substituted with the colon (‘:’) as a separator. Typically, an IPv6 address looks like ‘fe80::4bb:3fba:aaaa:cb23’, where double colon means “padded with zeros”. As in IPv4, ranges of addresses can be specified by indicating the number of fixed bits from header, by using the slash (‘/’) prefix, like in ‘fe80:800::/24’.

Most characteristic groups in IPv6 addressing space are:

::1	Loopback
2001::/16	Normal addresses
2002::/16	IPv6 to IPv4 automatic tunnels
3FFE::/16	"6bone" (experimental network)
FE80::/10	Link-local-use
FEC0::/10	Site-local-use
FF00::/8	Multicast

Figure -6 IPv6 addressing space

3.2.2.2. Unicast, anycast and multicast addresses

There are three different types of IPv6 addresses:

- Unicast addresses identify a single interface. Some classes of unicast addresses can be distinguished:

- Provider-based unicast addresses: structured hierarchically, these addresses carry specific prefixes identifying the Internet service provider, its Internet addressing registry and the particular subscriber identifier.
- Local use addresses: defined with local subnet scope, they can either be “link-local” or “site-local”. They have specific prefixes that prevent them from being used as global addresses, and an interface identifier that must be unique within the scope of the subnet.
- Embedded IPv4 addresses: defined for IPv6/IPv4 compatibility purposes, they have basically an IPv4 format, padded with zeros and a special prefix dependent on their function. IPv6 nodes that have to deal with IPv4 infrastructures use the “FFFF” prefix before the IPv4 address. On the other hand, IPv4 nodes that do not support IPv6 and need an IPv6 address to be assigned use “0000” prefix instead.

- Anycast makes possible to define a group of various nodes, and to send the packets only to the nearest single receiver among them. The aim of this technique is enabling that actual route could be managed efficiently by the intervenient nodes. Formats of anycast and unicast addresses are identical, so explicit information must be provided to nodes.
- Multicast in IPv6 is quite similar to IPv4’s, but with the limitation of a scope (“SCOP”) field which constrains range of the delivery, so as to preserve scalability of routing. SCOP is composed of 4 bits, indicating “node-local”, “link-local”, “site-local”, “organization-local” or “global-local” scopes (most of the values are reserved or not yet assigned). Broadcast is not specified in IPv6 as a differenced service. If it is needed to broadcast some information, a “wide-range” multicast can be used (“ff02::1”), analogously to IPv4’s “255.255.255.255” address.

3.2.2.3. Address autoconfiguration

Manual configuration of IP connections is inefficient, especially in public environments where many hosts are connected for a short period of time. IPv4 makes extensive use of Dynamic Host Configuration Protocol (DHCP), where a server assigns addresses dynamically and automatically within a subnet. However, IPv6’s objective is to provide a stateless, serverless method for address autoconfiguration, at network layer, that makes possible a host to connect in an easy “plug-and-play” manner.

Autoconfigured address is composed by adding a subnet prefix (which is advertised periodically by the router) to a particular “token”, unique for each singular interface. These tokens can be extracted from link-layer addresses (for example, from IEEE 802’s MAC addresses). Following this scheme, addressing is easily reconfigurable.

Routers supporting this feature also advertise two lifetime values along with the prefix, which point out:

- If the composed address is valid
- If the composed address is deprecated

Although valid, a deprecated address is one which is about to be invalid. Thus, it must not be used as a source address for new sessions, considering that upper transport protocols like UDP or TCP are not able to overcome address changes along a transmission. If the prefix is advertised again, validity lifetime counters are reset. If not, lifetime expires and those addresses are valid no more.

IPv6 also supports a “stateful”, DHCP-like address configuration protocol. So, routers must be aware of which protocol is being used (where both options are feasible).

3.2.2.4. Simplified header format and extension headers

Although addressing field in IPv6 is four times longer than IPv4 one, IPv6 headers are only twice the length of IPv4's. This is a result of the effort in header simplification, to reduce bandwidth as much as possible. However, if some additional functionality is needed, it can be added by using "extension headers" in a flexible manner, another novelty technique in IPv6.

Extension headers are located between IPv6 header and transport-layer payload. Unlike IPv4's approach, this Options field is not limited in length, and it has no need to be necessarily examined until it arrives to its final destination. This way, packet processing is much faster and light in computational cost, enabling the use of many new services.

These are some of IPv6 extension headers defined:

- Routing: used to specify one or more intermediate nodes, in order to define the path the packet must follow towards its destination.
- Fragmentation: for fragmentation and reassembly of packets which are longer than the maximum MTU size. In IPv6, fragmentation must be carried out at source. Fragmentation in intermediate nodes is not allowed, because it decreases efficiency (one of the drawbacks in IPv4).
- Authentication: provides integrity and authentication.
- Security encapsulation: for confidentiality.
- Hop-by-Hop option: for options that require processing at every node.
- Destination options: information to be examined at destination only.

3.2.2.5. QoS support

One of the biggest challenges for the new generation of IP was to implement some mechanisms so as to support quality of service (QoS). IP is basically a "best effort" protocol that tries to do its best with each packet, independently of their characteristic needs. In IPv6, packets can be labelled in order to identify different flows, and sources can also assign higher priority to those packets with stronger constraints (for example, real time services). This philosophy has been taken into account from the very beginning of headers design, which contains two specific fields for this purpose:

- Flow label: flows are sequences of packets that require to receive a special handling (by means of resource reservation protocol or other techniques). A flow is identified by the couple formed by a source address and a non-zero 24-bit flow label. Flow label's value is assigned randomly between 000001 and FFFFFF. Routers can use these identifiers as cache keys for some other routing information regarding the flows.
- Priority: 4-bit priority field provides some help for an adequate dropping of packets, being aware of the particular characteristics of the source. One half of the possible values of this field are dedicated to mark congestion-controlled traffic:
    0. Uncharacterized traffic
    1. Filler traffic
    2. Unattended data transfer (e-mail…)
    3. (Reserved)
    4. Attended bulk transfer (FTP, HTTP…)
    5. (Reserved)

6. Interactive traffic (Telnet…)
7. Control traffic (routing protocols, SNMP…)

The other marks non-congestion-controlled traffic, where the more priority it demands, the higher is the value.

3.2.2.6. Security

Some security enhancement procedures must be developed to overcome the lack of protection in communications under the application layer. These services can be defined as follows:

- **Authentication:** the mission of authentication processes is determining the identity of the user, machine or application that initiates a transmission. This can be carried out, for example, by means of a log-in step.
- **Data Integrity:** data must remain valid and unaltered during secure transmissions. For instance, account number in an e-commerce operation must be protected from being changed by malicious attacks or transmission errors.
- **Confidentiality:** a confidentiality procedure ensures that certain user, machine or application, has the authorization to perform certain operation. This agent could have been previously *authenticated*.

IPsec is a standard for security in network layer transmissions, which applies to IP datagrams. Although it can be used for IPv4, for IPv6 it is mandatory. It provides several functionalities such as encryption, authentication, integrity validation, and avoidance of session replays.

IPsec makes use of two different mechanisms standardized with this aim:

- **Authentication Header (AH):** an extension header that provides authentication and integrity, without confidentiality. It contains several security parameters and a counter that prevents from replay sessions.
- **Encapsulating Security Payload (ESP):** another extension header, this time providing confidentiality together with authentication and integrity; and whose fields also contain an anti-replay attacks counter and security parameters information.

3.2.2.7. IP Mobility

In the deployment of an “all-IP” wireless network, mobility management is another important issue to deal with. It allows mobile terminals to bring their context information (IP address, QoS parameters, authentication, etc.) with them as they travel from one subnet to another.

Mobile IP, described in IETF RFC 3344 [9], makes all this possible by assigning a “care-of” IP address to the terminal in the visited subnet. This address is registered in the home agent, so that all packets destined to the terminal are tunneled to it. “Tunneling” is wide used to provide mobility in wireless networks such as UMTS because it only requires mobility support in tunnel end-points. Due to the invisibility of packet headers for intermediate routers, implementing multicast, caching or QoS differentiation is rather complicated. This situation could be solved if mobility were implemented at IP level. In an “all-IP” context, routing to local resources is efficient: packets don’t have to travel to the edge of the network if they are destined to another terminal in the same cell. Dynamic reconfiguration and maintenance are also easier, thanks to DHCP and SNMP protocols.
Some enhancements to the Mobile IP technique are developed, such as Mobile IPv6 [10] and Hierarchical Mobile IPv6 (HMIPv6). These are expected to make communication more efficient and secure.

4. Description of networks considered

4.1. Ethernet

Ethernet [11] is by far the most prevalent LAN technology. As Ethernet has been so popular, Ethernet hardware (Adapters, Hubs and Switches) is remarkably cheap. Ethernet can be used to transmit at 10Mbps, 100Mbps or 1Gbps over a coaxial cable or cooper wire. SUIT will use the Ethernet technology to connect several components/equipments as discussed in Section 8. The Ethernet frame structure is shown below.

Preamble	Dest. Address	Source Address	Type	Data	CRC
8	6	6	2	46-1500	4

Figure -7 Ethernet packet structure

A short description of 802.3 (Ethernet) frames is described in the following table:

Field	**Bits**	**Description**
Preamble	64	Identifies an Ethernet packet. 0xAA….AB
Destination Address	48	Destination adapter address
Source Address	48	Source adapter address
Type	16	Identifies the network protocol in the data field.
Data	230-12000	The field carries the data. It can be an IP datagram.
CRC	32	It is used to check frame errors

Table 1- Ethernet fields

For VLANs (Virtual LANs) as defined in 802.1Q [11], the Type is equal to 0x8100, denoting the new frame format. It adds extra 4-bytes in the original Ethernet header. The Type, 0x8100, is followed by a header that contains the following fields:

- User_priority: this 3-bit field can be used to store a priority level for the frame. Use of this field is defined in IEEE 802.1p.
- CFI: a 1-bit flag denoting whether MAC addresses in the frame are in canonical format. This is called the Canonical Format Indicator.
- VID: a 12-bit VLAN ID, allowing up to 4096 VLANs.

and then the original Type.

In consequence of inserting this new header, it is required to recalculate the original FCS field in the Ethernet trailer.

As described in Section 8, we will make use of two VLANs, one is associated to WiMAX and the other is associated to DVB.

4.2. DVB-T/H/S2

This section describes some DVB standards with emphasis on the most recent issued standards like DVB-S2 [12] and DVB-H [13].

Generally speaking, DVB-T is a transmission system defined at the physical and link layers. At the physical layer, it uses two possible modulators modes, 2k and 8k. At the link layer, it defines a framing structure called Transport Stream (TS) as shown in the figure below.

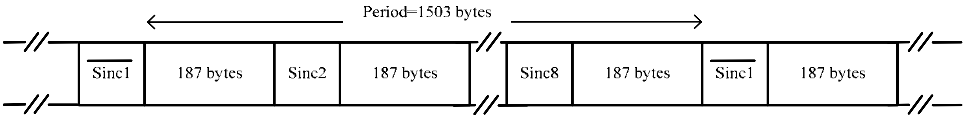


Figure -8 Transport Stream

The TS stream is conceptually very simple since it is a consecutive linked set of packets with a fixed sized, 188 bytes from which the first one, the Sinc byte is 0x47 or its complement appearing in the beginning of each set of 8 TS packets as shown in the figure above.

The TS will encapsulate any data or in other words, the data will be sliced into 187 bytes and transmitted to the destination sequentially. Therefore, the TS is able to transport any packet type with variable length which may lead to some TS packets with stuffing bits. Very similar to the Ethernet packet [11], the DVB standards specifies the MPE (Multi-Protocol Encapsulation) [16] packet used to transport IP traffic.

Recently, the DVB group defined new mechanisms in the satellite and terrestrial standards, DVB-S [18] and DVB-T [19], and baptized them as DVB-S2 [12] and DVB-H [13], respectively. We should point out that the new mechanisms included in DVB-S2 may influence the future versions of DVB-T/H.

The new features introduced by DVB-S2 relatively to DVB-S are (some of them are of low importance in the context of this deliverable):

- The inclusion of higher order modulators, 8-PSK, 16-APSK e 32-APSK beyond of the existing QPSK.
- Replacement of the concatenated code RS+Conv by BCH+LDPC. The internal CoDec, LDPC [14] allows using 11 different code rates in the range from 1/4 and 9/10.
- Supports *on-line* ACM (Adaptive Coding and Modulation). Each receiver requests from a return channel, the level of protection to be applied to the traffic addressed to it (unicast).
- Supports multiple input stream formats, i.e., TS and GS (Generic Stream), the later, packetized or continuous.
- The framing structure at the link layer is not TS any more. The framer (PL Framer) is the last element before the modulator in the transmission chain as can be observed in the figure below. Each frame is composed of a 90 symbols header and a payload of either 64800 or 16200 bits. Each header is encoded with a low code rate, 7/64, and BPSK modulated (using constellation points of QPSK). The smallest payload is used for interactive applications corresponding to a lower channel encoding delay.

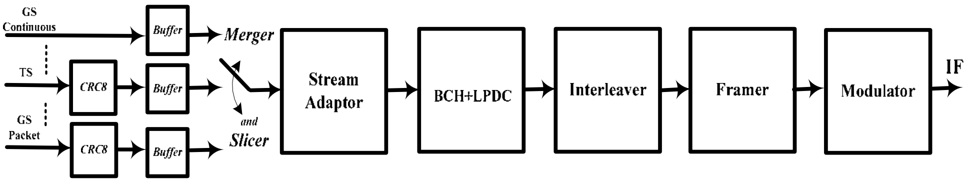


Figure -9 DVB-S2 System

- The merger/slicer multiplexes the input streams, buffer them and after yields a variable packet size called BBFrame with a size slightly less than either 64800 or 16200 bits. A CRC is added to each input packet and in the case of a TS, the CRC replaces the Sinc byte (0x47).

In 2004, the DVB group approved the DVB-H [13] standard, a new DVB-T version for mobile devices. Truly speaking, there were some amendments to the DVB-T physical layer, ETSI EN 300 744 V1.5.1 [15] and to the DVB-Data (transport layer), ETSI EN 301 192 V1.4.1 [16] as well as to the service information, ETSI EN 300 468 V1.6.1 [17]. The most important features introduced by DVB-H in the context of this deliverable are at the transport layer:

- In DVB-Data, the IP packets are encapsulated into MPE packets where, as usual in the Internet, the next node MAC physical address is indicated the in MPE header. However, before that MPE encapsulation takes place, a RS(255,191) is applied to a set of IP packets. Therefore, it results in MPE-FEC sections whereas the IP packets themselves result in MPE-Application Data Sections.
- The time (time slicing) between one MPE packet and the next one is indicated in its header in order to allow the receiver to standby and save energy.

4.3. WiMAX

The purpose of this chapter is to define the wireless networks system from the single-cell level and up to the multiple cell level, and to define their operation scenario.

4.3.1. Single-cell block diagram

Single cell consist of one or more sector cards. All the sector cards represent a BST (BaseStation) or a single cell. Each sector card is operating with one or more User Terminals (UT) using the air interface (MAC) and RF bandwidth (could be the same frequency bandwidth or another frequency bandwidth for each sector). The MAC interface between the sector card and the user terminals is considered as layer 2 in the OSI layers. If the User terminal is a mobile it can move from one sector to another by doing HandOff (Handover). HandOff or other information transformed between the sector cards are using the 3rd layer consist of Switch/Router that is connected to the sector card by Ethernet cable using the sector card Ethernet connector usually RJ-45. As it can be seen in the figure below the switch/router is connected to the backbone IP network by wired (fiber, for instance) or some time by micro-wave. BST becomes manageable through the backbone IP network, and can access the management and configuration servers and obtain data relating to the network topology (i.e. frequency and RF parameters, neighbours, network related parameters, server addresses, etc.)

The system is a Point To Multi Point (PTMP) system, so one user terminal is able to connect other user terminal, even in the same sector, only via the sector card(s).

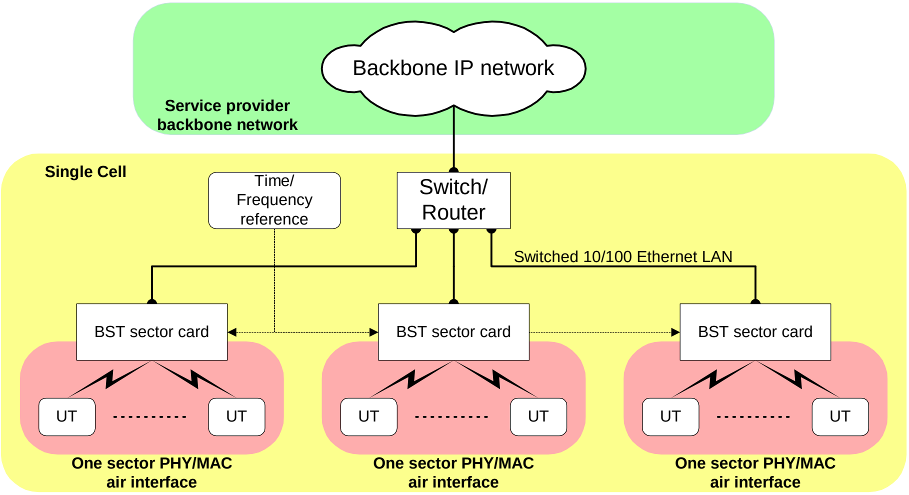

Backbone IP network
Service provider backbone network
Single Cell
Time/ Frequency reference
Switch/ Router
Switched 10/100 Ethernet LAN
BST sector card
BST sector card
BST sector card
UT
UT
UT
UT
UT
UT
One sector PHY/MAC air interface
One sector PHY/MAC air interface
One sector PHY/MAC air interface

Figure -10 Single sector block diagram

4.3.2. Multiple-cell block diagram

Multi cell consist of several single cells (several BST's). HandOff or other information transformed between the cells are using the backbone.

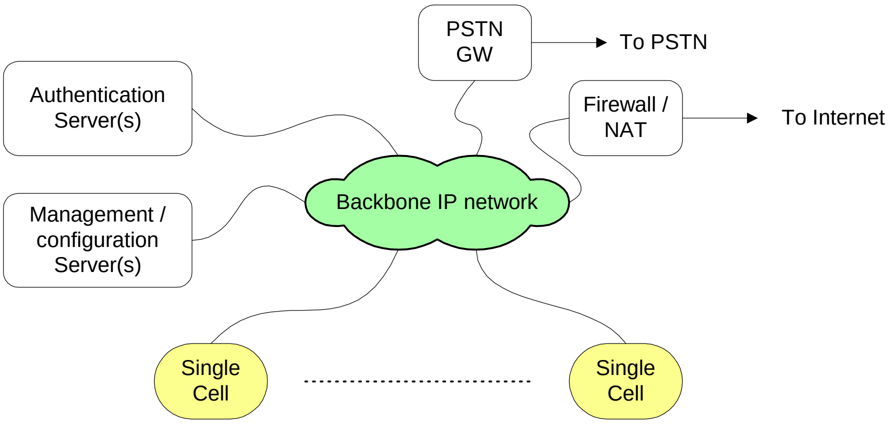


Figure -11 Multiple-sector block diagram

4.3.3. Operation state definition

4.3.3.1. BST

Upon connection of a new BST to the network, the BST becomes manageable through the backbone IP network, and can access the management and configuration servers and obtain data relating to the network topology (i.e. frequency and RF parameters, neighbors, network related parameters, server addresses, etc.). At the next stage the BST has to synchronize in timing and frequency to the timing and frequency settings used in the system. The time/frequency source would normally be a GPS receiver located at the BST site, but other methods are also possible to provide a time/frequency reference. After the BST is synchronized to the network it starts its air interface and starts supporting UT. The BST uses the backbone to access the provisioning and authentication servers whenever information about a UT is required.

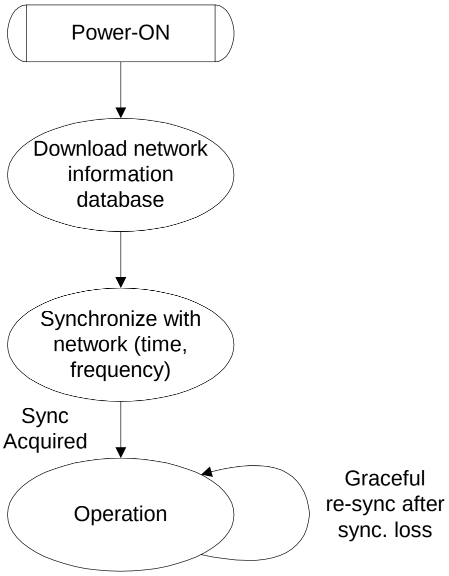

Power-ON
Download network information database
Synchronize with network (time, frequency)
Sync Acquired
Operation
Graceful re-sync after sync. loss

Figure -12 BST sector operation states

4.3.3.2. UT

The UT features three major operation states. Upon power-on the UT attempts **initial network entry**. During this process the UT scans for a suitable downlink channel and synchronizes with a specific BST sector. After physical level synchronization is achieved, the UT registers with the network through the BST. The network entry process terminates once the UT is assigned an IP address and is capable of opening transport connections for data. It should be emphasized that the network entry process does not include any setup operations required in order to transmit data in layers above layer 2.

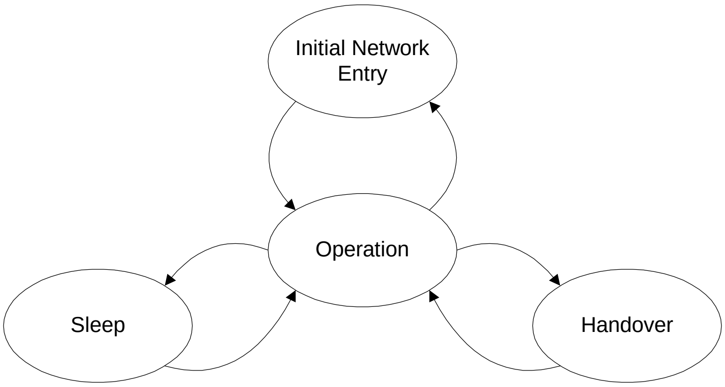


Figure -13 UT operation states

After initial network entry the UT is in the **operation** mode, where it is capable of full functionality and bi-directional transfer of data in compliance with the air-interface PHY/MAC specifications.

The UT may leave the operational mode to go into **sleep** mode. During sleep the UT wakes up occasionally in a manner synchronized with the BS, and goes back to sleep if no data is available for it. In case that there is data for a sleeping SS, the SS returns to the operation mode.

The last major of the UT is handover. Handover is the process where a UT registered with one BST sector transitions to another BST sector. The process involves tearing down the existing data connection at the old BST and re-establishing them in the new BST after synchronizing and registering with it.

4.4. DVB-RCT

The DVB-RCT networks system serves the wireless Service Providers and Broadcasters wishing to offer a converged solution that combines interactive TV and broadband wireless access or purely telecommunication applications such as VoIP, video conference, televoting, e-commerce, fast Internet browsing and other multimedia applications.

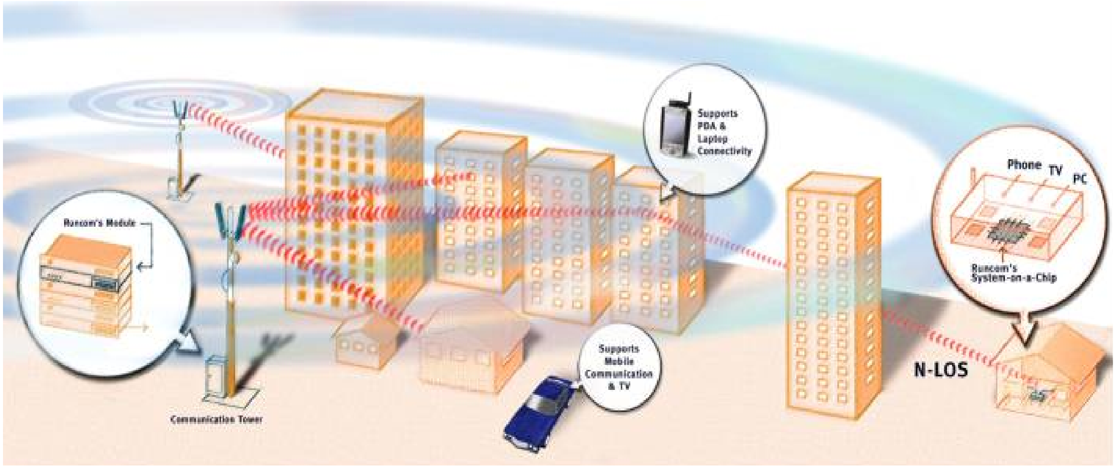

Runcom's Module
Communication Tower
Supports PDA & Laptop Connectivity
Supports Mobile Communication & TV
Phone
TV
PC
Runcom's System-on-a-Chip
N-LOS

Figure -14 DVB-RCT Network and applications (LOS and NLOS environments).

The DVB-RCT system is a point-to-multipoint system that has a Base Station (BS) at its center. The BS supports both, bi-directional interactive communication and DVB-T broadcasting. The BS is connected to an IP network (typically the Internet) and a video (MPEG2) distribution infrastructure. The BS function is to multiplex the MPEG2 transmission stream with the traffic of the forward (downlink) channel, and to receive the uplink channel. The video transport stream is obtained from the video distribution network, while the data for the interactive channel is backhauled to the IP network.

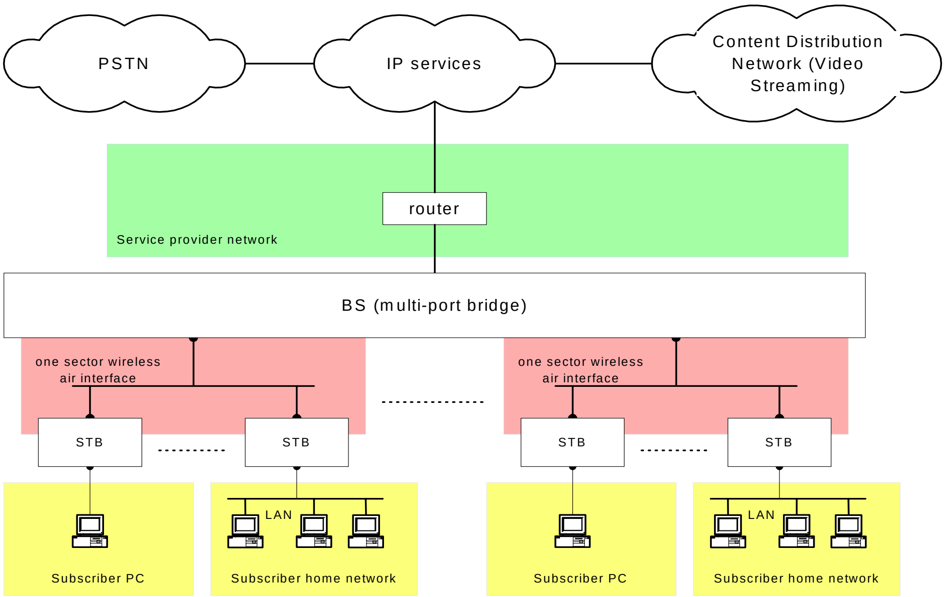


Figure -15 Multi sectorized infrastructure.

The BS coverage area can be divided into several sectors, with each sector covered by dedicated antennas and processing hardware. The division into sectors in the downlink channel may be different than the division of the uplink channel. The sectors can be synchronized to each other in time and frequency by using a common time and frequency reference, such as a GPS receiver.

4.5. Wi-Fi

Wireless local area networks, where data is transmitted through low-powered radio waves, add extra functionalities to traditional wired LAN data transmission: mobility, flexibility, low cost and a fast and easy deployment. In the last decades, many standards for WLANs have been set up such as IEEE 802.11 (Wi-Fi) or HIPERLAN. The first one, considered as the wireless version of Ethernet, is now a leading technology that has succeeded in the market. The next sections will describe the main characteristics of Wi-Fi networks and standards.

4.5.1. Network elements and network architectures

A Wi-Fi [20][23] WLAN is basically formed by four types of components:

- **Stations:** Final hosts, typically portable such as laptops, among which communication takes place.
- **Access Points (APs):** The main function of these devices is allowing stations to communicate with other machines outside the WLAN, by wireless-to-wired bridging. Presence of an AP gives the WLAN an infrastructure.
- **Wireless medium:** Physical wireless medium through which packets are sent is another part of the network. Several physical layers are specified, even infra-red, though radio frequency ones have been much more popular.
- **Distribution system:** When various APs are involved in order to achieve a greater coverage, the distribution system is in charge of interconnecting the APs, usually via Ethernet connections.

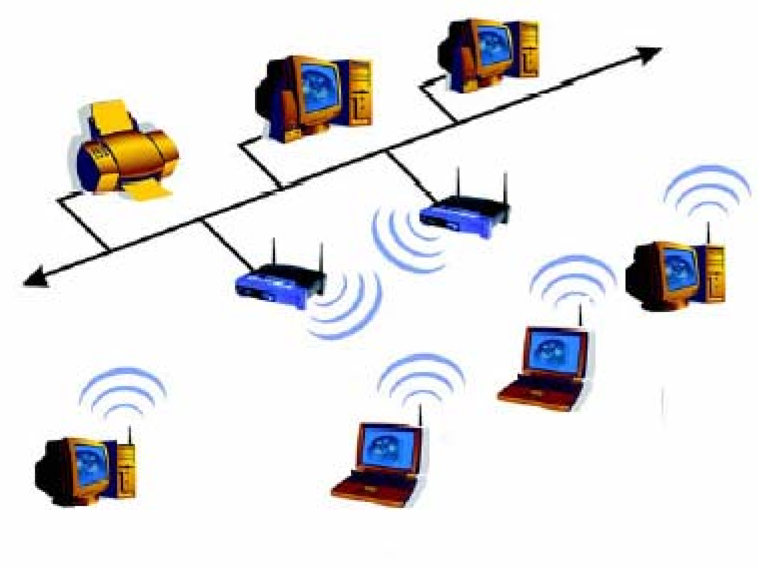


Figure -16 Infrastructure Wi-Fi WLAN

Depending on how these components interrelate, different types of architecture can be found:

- **“Ad-hoc” networks:** with the appropriate equipment, a station can communicate directly to others, with no need of an access point; this way establishing an “independent base service set” (IBSS) or “ad hoc network”, easy to put up but of reduced capabilities.
- **Infrastructure networks or infrastructure BSSs:** this kind of networks makes use of an access point that controls communication providing some additional services such as bridging, access granting or power saving. Packets between two stations must necessarily go through the AP. This way, neighbour relationships information at hosts is simplified, and transmission is only constrained by the distance to the AP.
- **Extended service sets (ESS):** extended coverage can be provided when many access points are linked through a distribution system, thus needing link-layer mobility support. In this scheme, access points must act as bridges.

4.5.2. Standard description

802.11 forms part of IEEE 802, a set of standards for Local Area Network (LAN) technologies. In particular, these standards focus on the two lowest layers of the OSI model (physical and data link layers). Data link layer can be divided into two sublayers:

- **Logical Link Control (LLC):** LLC is specified in IEEE 802.2. This sublayer multiplexes protocols and encapsulates packets through the MAC.
- **Medium Access Control (MAC):** regulates how a common medium can be used, in an organized manner, by all participants in the communication. Many MAC standards are able to work under 802.2 LLC, such as Carrier Sense Multiple Access with Collision Detection (CSMA/CD, also IEEE 802.3, used in Ethernet) or Token Ring (IEEE 802.5).

In fact, 802.11 specifies a MAC sublayer (CSMA with Collision Avoidance, CSMA/CA), working under 802.2 LLC; and diverse physical (PHY) layers, depending on the particular version of the standard.

The family of standards 802.11 consists of the following elements:

- **802.11 legacy:** The original standard, was able to transmit at 1Mbps and 2Mbps in the 2.4 GHz band. Defines two different PHY layers: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS).
- **802.11b:** Also operating at 2.4 GHz, can support rates up to 11 Mbps, by employing High Rate DSSS (HR/DSSS) as the PHY layer. These equipments were the first with some commercial success.
- **802.11a:** By using Orthogonal Frequency Division Multiplexing (OFDM) with 52 carries, can theoretically transmit at 54, 48, 36, 24, 18, 12, 9 or 6 Mbps. It works in the 5 GHz band, in order to avoid interferences produced by other devices operating at 2.4 GHz. However, coverage range is diminished as a result of this choice, and equipments are incompatible with 802.11b ones.
- **802.11g** [24]**:** Defines an Extended Rate PHY (ERP) that allows transmission rates up to 54 Mbps while in 2.4 GHz band. This standard was defined to be fully interoperable with 802.11b, though working in interoperability mode reduces efficiency drastically.
- **802.11n:** It is expected that 802.11n, a new version of the standard currently under development, was able to operate at 500 Mbps or more. Final specifications could be finished for the end of 2006.

4.5.3. Functionalities provided by 802.11

In this section, we describe those functionalities of interest for the deployment of the SUIT platform following the "All-IP" scheme.

4.5.3.1. Reliability

802.11 link-layer protocol provides a reliable data service. Data arrival and integrity is guaranteed to a certain extent, collaborating with other higher-layer protocols. In particular, a set of techniques that control data delivery are specified by a "coordination function". Distributed Coordination Function (DCF) is the basic and most popular among them, supporting Ethernet-like contention-based services.

Some methods implemented in DCF to provide reliable data transmissions are:

- To avoid collisions in a shared medium, stations use a basic set of rules. Prior to the transmission, a station checks if the channel is idle by means of "carrier sensing" techniques (both physical and virtual). If the medium is busy, access is deferred and sender station waits for its turn for a random period of time ('backoff window').
- Senders expect an acknowledge frame (ACK) for each transmitted data frame, since it is the only indication of the success of the delivery. If no ACK is received, sender station is responsible for retrying. In contrast to Unicast – where each data packet is always acknowledged – for Multicast there are situations where ACKs cannot be used (this would leads to malfunction due to the fact that all clients would send its ACK simultaneously). Thus the reliability of multicast traffic in such situations is reduced.
- Number of retransmissions is controlled by the "retry counters". When transmission of a frame fails (no ACK is received or it is impossible to gain access to the medium) the corresponding retry counter is increased. If the counter exceeds a certain retry limit, the frame is considered as lost and this is reported to higher-layer protocols. In addition to this, when a frame is segmented a "lifetime" value is added to each fragment.

4.5.3.2. Multi-rate support

Each version of the IEEE 802.11 standard supports a set of different data transmission speeds, in order to switch adaptively among them as distance or channel conditions vary. Actual mechanisms employed for rate selection and adaptation are not specified in the standard, though some general rules are assumed:

- Each station holds a list of "operational rates", both supported by it and the access point.
- On the other side, the access point maintains a "basic rate set", composed of transmission speeds that are mandatory for all stations within the WLAN.
- Unicast frames can be transmitted at any operational rate, supported by the destination as well as by the sender.
- Multicast and broadcast frames must be transmitted at a rate in the "basic rate set". These data rates are preset for all stations in the BSS
- Control frames must be transmitted at a common rate supported by all stations.

Adaptation techniques can be carried out in a signal-to-noise ratio or packet loss / retry counter basis.

4.5.3.3. Addressing

Another task for a link layer protocol is to identify univocally each device in the network by means of a link-layer address. 802.11 layer-2 addresses follow MAC-48 format, the same as in Ethernet. These are formed by 6 bytes, whose first three stand for the organization which issued the identifier and the last three for the concrete device.

Local network broadcast MAC address is specified to be FF:FF:FF:FF:FF:FF, while multicast addresses must have the least significant bit of their first byte set to one. Another kind of addresses (locally administered) have the second bit of their first octet set to one, indicating that its value has been assigned by network administrator, instead of the hardware vendor.

4.5.3.4. Different transmission schemes

802.11 enables link-layer unicast, multicast and broadcast delivery, in a similar way as Ethernet. However, the frame exchange scheme in Wi-Fi is slightly more sophisticated. Group frames (broadcast data frames, multicast data frames and broadcast management frames) are sent without most of the reliability support methods described for unicast transmission. Delivery of group frames is not acknowledged, and neither fragmentation is allowed.

This way, despite of the fact that wireless link is intrinsically a broadcast medium, unicast transmission has a better service quality than broadcast or unicast ones, thanks given to additional reliability provided by the MAC.

4.5.3.5. Fragmentation

As a way to deliver long packets from higher layers, or to increase throughput in channels with interferences, fragmentation of packets into smaller ones is implemented in 802.11 MAC. Fragments are marked with a common frame sequence number and increasing fragment numbers to facilitate reassembly. Each fragment has the ability of reserving the channel until the corresponding ACK is sent.

4.5.3.6. Prioritized traffic

A way for giving transmissions different priorities is establishing a set of waiting periods, depending on the characteristics of the communication. The lower the priority of the transmission, the longer the period the station has to wait, then giving a chance to highest priority traffic. However, neither DCF nor PCF+DCF have the ability to offer true QoS to Wireless LAN.

When the channel turns idle, stations must wait a certain time determined by one of the following:

- **Short Inter-Frame Space (SIFS):** reserved for the highest priority traffic, such as RTS/CTS signalling and positive ACKs.
- **PCF Inter-Frame Space (PIFS):** PCF stands for Point Coordination Function, a type of MAC access mode for transmissions without contention. It has the highest priority below SIFS, although it is not widely implemented.
- **DCF Inter-Frame Space (DIFS):** On the other hand, DCF stands for Distributed Coordination Function, the standard mode for CSMA/CA access. DCF is contention-based, so its priority is inferior to PIFS.
- **Extended Inter-Frame Space (EIFS):** EIFSs do not have a fixed length, and they are used when there is an error in frame transmission.

In order to avoid collision when DCF mode is used, a “contention window” or “backoff window” is set up when the DIFS expires. This window is divided in a certain number of transmission slots. Each station that wants to send a frame chooses randomly a slot within that range, and waits for its turn. Thus, the station with the slowest random slot transmits the first. When a transmission fail occurs, window length is approximately doubled (possible lengths are 31, 63, 127, 255…), being its maximum size limited by the physical layer.

4.5.3.7. Association and authentication

Every station that pretends to make use of the WLAN must be previously registered with the access point. In the case of an ESS, the distribution system must be in charge of assigning the incoming station to the most appropriate AP. When this association process is done, a subsequent authentication procedure is carried out, in order to ensure that the station is authorized to use those WLAN resources.

4.5.3.8. Encrypting

Confidentiality of communications is provided by cryptographic algorithms, such as WEP, TKIP or CCMP, which encrypt data frames. This service relies on additional authentication and key management protocols that must be also implemented.

4.5.3.9. Mobility

Mobility is one of the strong points of WLANs, since it enables terminals to keep communication while moving, even trough network boundaries. Link-layer mobility is fully supported in the IEEE 802.11 standard. This way, a station can transit from a BSS 1 to a BSS 2 if their respective access points are in communication through a distribution system, and hence can manage corresponding disassociation and association tasks. In order to achieve this, access points must not be interconnected through a router, since it is a network-layer boundary. Transitions from one ESS to another are not affordable either by IEEE 802.11 means, so higher layer techniques such as Mobile IP must be employed to accomplish them in a seamless manner.

4.5.3.10. Power saving support

Most of the power spent in a wireless station is destined to feed RF transceivers. 802.11 standard specifies support for power saving techniques that enable temporary disconnection of transceivers, which hence switch into a “sleep mode”. Unicast frames destined to a station in sleep mode are buffered in the Access Point, and finally delivered when the receiver station awakes and asks for it by means of a PS-poll message. In the case of group frames, more complex methods enable buffering when any of recipient stations is “sleeping”.

5. IP over DVB

5.1. Encapsulation

In the demonstrator, IP over DVB will be achieved by encapsulating IP packets over MPE and then over TS. We may do other experiments by using the BBFramer/LFFramer as described in Section 4.2.

5.2. Address resolution

The mobile DVB-RCT works as layer 2 bridge. The BST works as layer 2 bridge between the operator network and the wireless section. The IP addresses that BST or user terminal have are for management proposes only. The interface with the layer 3 switch/router is through Ethernet interface (in Runcom’s equipment using RJ45 connector).

The BST consist of one or more sector cards, each sector card implements one instance of the air interface (MAC & PHY). All sectors are synchronized in timing and frequency in order to synchronize the network operation.

5.3. Incorporation of DVB-S2 tools

As a main requirement, the DVB-T/H transmission system will use a TS. However, we will keep in mind the new features as discussed in Section 4.2 like:

- On-line ACM (Adaptive Coding and Modulation). Each receiver requests from a return channel, the level of protection to be applied to the traffic addressed to it (unicast). This feature can be tested by using the classical concatenation defined in DVB-T, RS+Conv. coding.
- The replacement of the concatenated code RS+Conv by BCH+LDPC is also under investigation in SUIT as well as the ACM capability.

Obviously, ACM is not an IP requirement, nevertheless, as discussed in Section 8, the modulator is part of a bridge and therefore SUIT will define a protocol to tell to the bridge which coder and modulator should be associated to a particular packet. Each packet sent to the bridge by the playout should be tagged with some extra information.

SUIT is investigating the performance of BCH+LDPC over RS+Conv under terrestrial channels. Once a decision comes up, IT with the collaboration of R&S intend to design specific hardware to support ACM.

5.4. DVB-RCT considerations

5.4.1. DVB-RCT system overview

The standard for DVB-RCT was defined originally for Digital Terrestrial TV with high performance of the return channel. On top of such considerations, the DVB-RCT (Return Channel Terrestrial) specifications provide an attractive solution.

In a Terrestrial environment, operation may include partial blockage by foliage that contributes to the signal attenuation and multi-path effects. The range of radius varies with transmit power, channel characteristics, availability requirement, local regulations and atmospheric conditions.

To facilitate description, DVB-RCT system consist of one base radio and one or more subscriber stations (Point to Multi Point system).

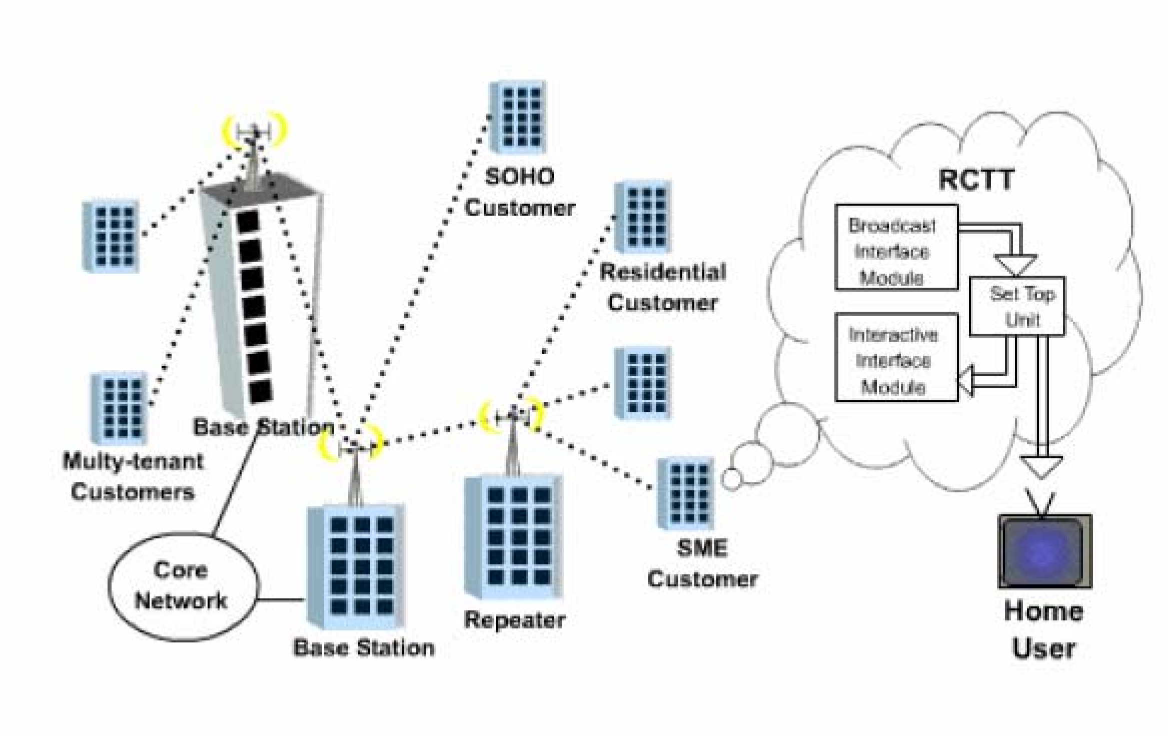


Figure -17 DVB-RCT System

5.4.2. Software building blocks

Runcom provides system on a chip (SoC) solution for the user terminal, a full user terminal solution based on the SOC and BST based on FPGA –all implemented the DVB-RCT modem and system PHY and MAC. The PHY and MAC are according to BS3 defined in the DVB-RCT standard. MAC software is divided into two software packages to shorten time to market for customers.

Runcom's DVB-RCT system building shown in the figure below and detailed below:

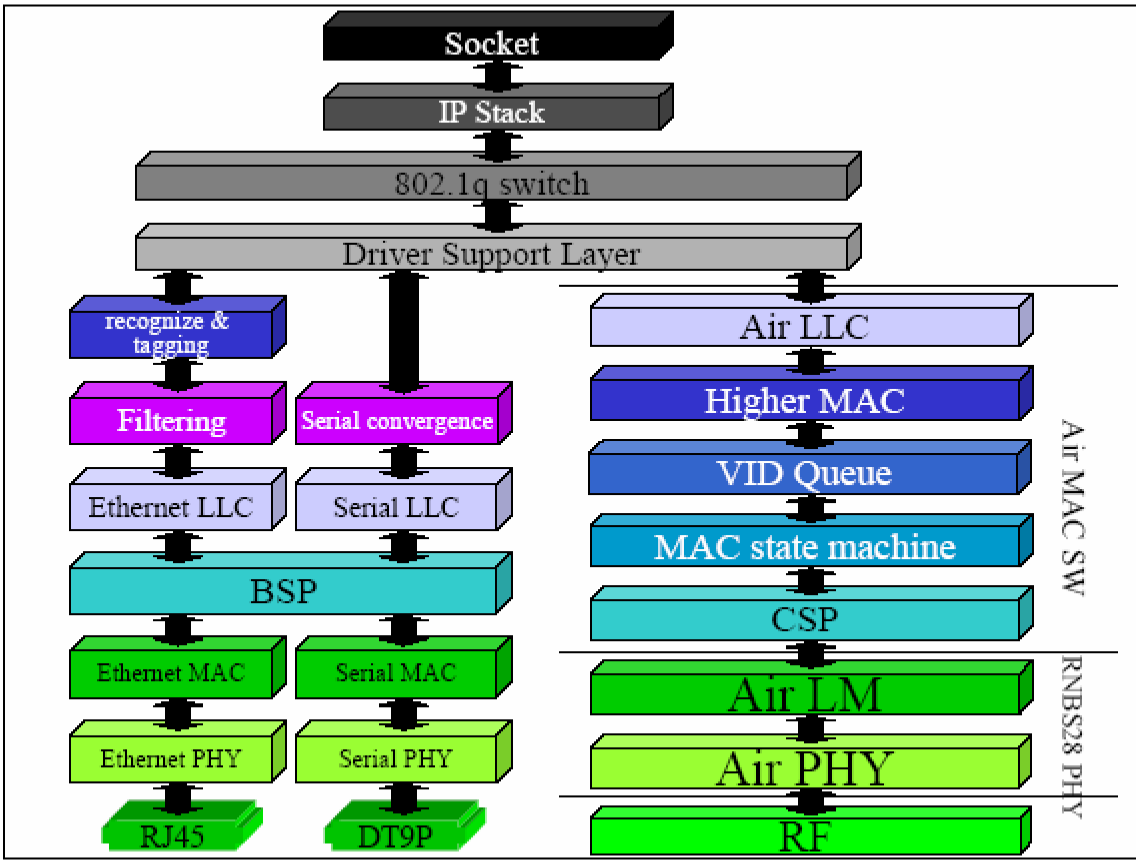


Figure -18 Runcom's DVB-RCT system building

PHY – Hardware implementation of the OFDMA modem

LM – Additional hardware packages allowing smaller CPU over load for MAC implementation including:

- BIU – CPU SDRAM bus interface, 6 counters, watch dog, interrupt controller, DMA interfaces to Rx and Tx FIFO etc.
- RF interface – SPI and I^2C interfaces, TR, power down etc.
- ATM frame building.
- MPEG packet assembly.
- Etc

CSP – Software package supporting all RN2821 (DVB-RCT Runcom's ASIC) hardware interfaces and initialisation.

LMDD – Software modules implementing all MAC time critical tasks usually frame depended.

HMAC – Software MAC implementation of DVB-RCT MAC.

LLC - Software package that implement ARQ error correction, QoS etc.

DSL – Drives Support Layers that switch all packets (traffic) between physical ports and/or higher applications.

Socket – Interface to higher applications.

Ethernet LLC – software module implement all Ethernet filtering, forwarding according to 802.1q or 802.3

Ethernet MAC – 802.3 MAC

Serial LLC – Software module implementing protocol over serial interface.

Serial MAC - Software module implementing serial MAC (if needed).

Serial PHY – RS232 converter or USB.

5.4.3. MAC board layer model and design consideration

Runcom's MAC package includes hardware board and package of software and firmware modules that support modem, RTOS and board hardware. MAC Hardware and Software Package (MHSP) designed to implement DVB-RCT standard at the user terminal and BST. BST MHSP has the same hierarchy as user terminal MHSP but with following differences.

1. CPE (Customer Premises Equipment) CPU support simple user applications. BST can support any user application by adding CPU.
2. Only BST QoS system supports bandwidth limitation feature (MIR- Maximum Information Rate and CIR- Committed Information Rate).
3. Only BST support broadcast and multicast messages.
4. CSP differences due to modem differences in CPE and BST.
5. BPS (Board Support Package) differences because CPE is SoC (System on Chip) and BST is SoB (System on Board).

MHSP designed to support the DVB-RCT standard, which is package-oriented protocol over OFDM/OFDMA air links. The MHSP was designed to provide good solutions for the following considerations:

1. Supports DVB-RCT modem and allow further extensions to other OFDMA standard (e.g IEEE802.16a/e) – Only small part of the firmware and some of the MAC features should be changed for each protocol.
2. Chips solution for CPE i.e SoC solution with minimum additional hardware.
3. BST MHSP is based on CPE MHSP i.e adding some more hardware/firmware/software to CPE design for BST to achieve faster implementation.
4. Modularity, i.e. different hardware/firmware/software component and combine to implement different set of features.
5. Easy to immigrate to different board design, CPU, and RTOS (Real Time Operating System) by adding interfaces layers to support different boards (BSP-Board Support Package), RTOS (shell) and modems (CSP-Chip Support Package).
6. RTOS response time is insufficient for firmware i.e. firmware is RTOS independent.
7. Maximum 4096 users.
8. Support up to 32768 packets/sec.

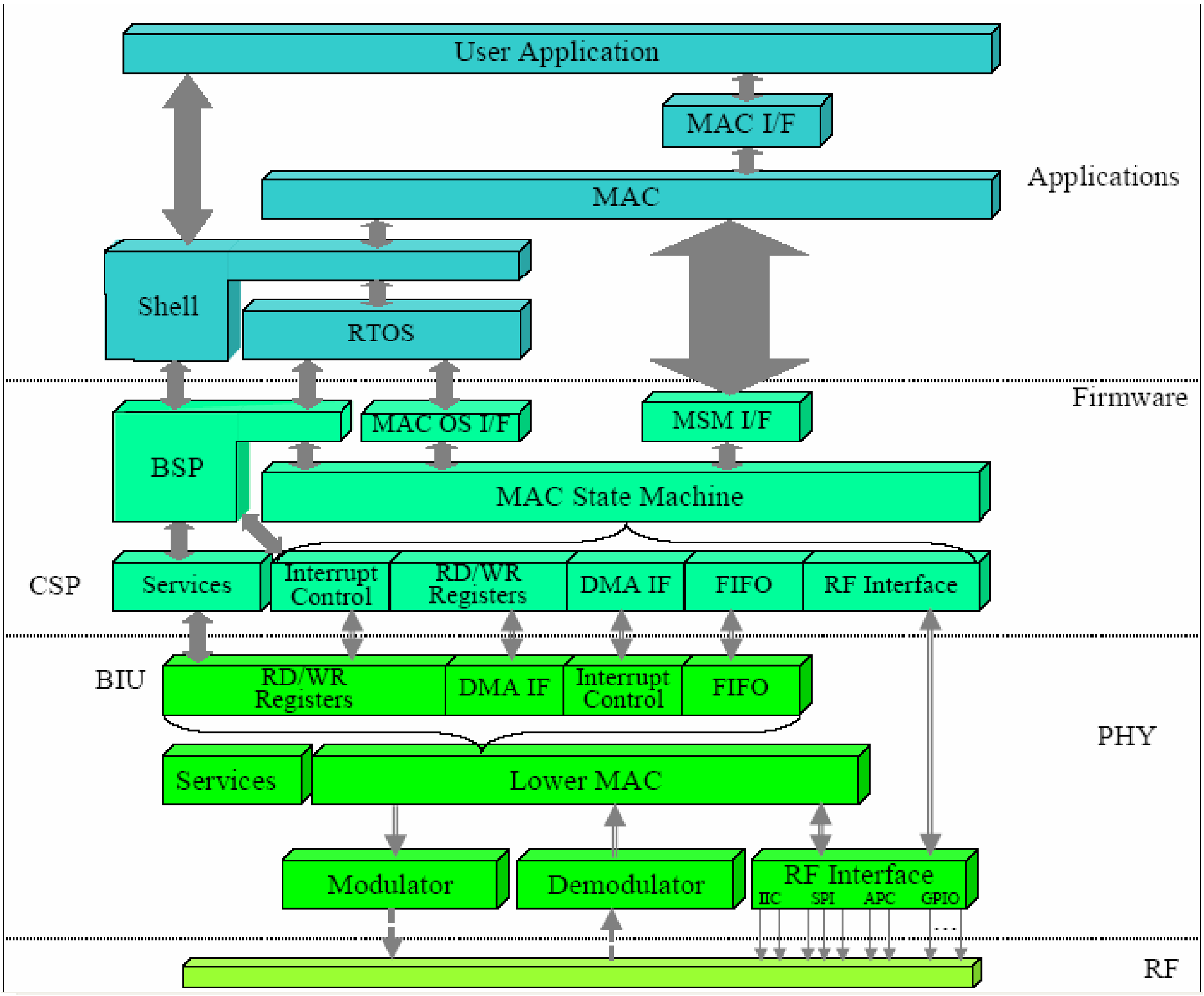


Figure -19 BST and User Terminal Layers model

The DVB-RCT MAC layer is usually referred as layer 2 in the OSI layers referece model. The scope of the DVB-RCT MAC layer protocol is to define the required massages between the BST and the user terminal for MAC. These areas are divided into three categories:

a. Initialization, Provisioning and Sign On Management

b. Connection Management.

c. Link Management

5.4.4. DVB-RCT access modes

The following rules define how to select access modes:

- MAC messages:

  MAC messages can be sent on contention access, reservation access, fixed rate access.

- Data connections:

  When the BST assigns a connection ID to the user terminal, it either specifies a slot list to be used.

There are four modes of the user terminal access to the BST listed below:

a. Contention Access

Contention Access indicates that data (MAC or bursty data traffic) is sent in the unreserved slots. It can be used either to send MAC messages or data. For modes with burst length smaller than ATM size only MAC messages (that fit in the burst) will be sent in contention. When the burst length is bigger than ATM size then ATM cells containing MAC or data messages shall be used for contention. The VPI, VCI of the ATM cells are then used to determine the type and direction of the data layers. Contention based access provides instant channel allocation for the CPE.

The contention based technique is used for multiple subscribers that will have equal access to the signalling channel. It is possible that simulations transmissions occur in a single slot, which is called a collision. The BST can send indication to the CPE when it has detected a collision. In case of a collision, the CPE shall perform truncated exponent back-off algorithm to prevent re-collision.

b. Ranging Access

Ranging Access indicates that the CPE performs synchronization of power and time with the BST. Ranging Access is performed on specially assigned slots (Ranging slots) that are used only for this purpose. The CPE shall use Ranging access when entering to the network, moving to a new upstream channel or instructed to do so by the BST. Also this mode shall be used for maintenance Ranging and fast bandwidth requests.

c. Fixed rate Access

The BST is also allowed to assign slots in fixed rate access to a connection. Those slots can be assumed as reserved to the CPE without explicit requesting for bandwidth.

d. Reservation Access

Reserved slots are uniquely assigned once to a connection by the BST. Requests are indicated via a request message in a contention slot, in a reserved slot, in a fixed rate slot or via the Piggybacking mechanism.

5.4.5. Grand system main layers –Up Link

The figure below shows the data flow in the Up link:

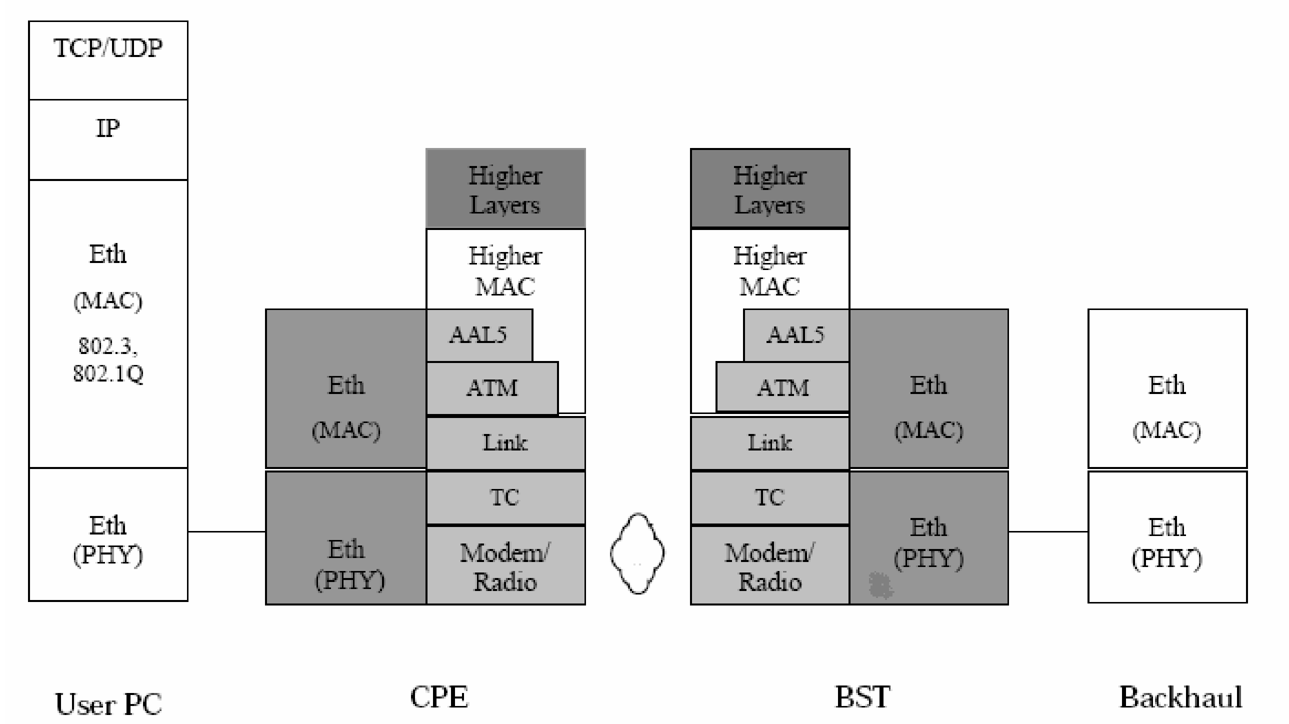


Figure 20 Data flow in the Up link

The following transactions are possible in this plane (transmits stand for the module that is the origin):

1. CPE MAC transmits MAC control message encapsulated in ATM cell(s) (VPI=0, VCI=0x21).
2. CPE MAC transmits MAC control message directly (not with AAL5, “direct message”).
3. CPE MAC transmits MAC control codes (e.g, Ranging, BW request) directly to the PHY layer.
4. CPE MAC transmits MAC control codes (e.g, Ranging, BW request) directly to the PHY layer.
5. CPE higher layers transmit Ethernet packets over AAL5.
6. CPE higher layers transmit management packets (e.g, SNMP) over AAL5.
7. CPE PHY transmits ATM idle cells. Idle cells are not delivered to the BST’s MAC layer.

5.4.6. Grand system main layers –Down Link

The figure below shows the data flow in the Down link:

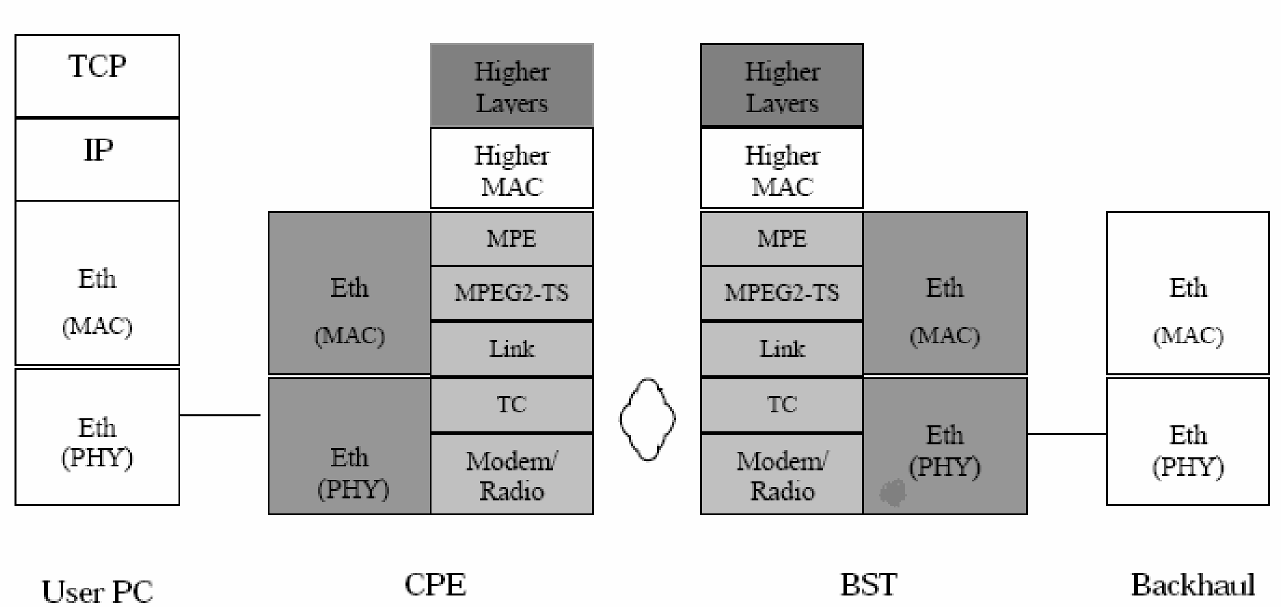


Figure -21 Data flow in the Down link

The following transactions are possible in this plane (transmits stand for the module that is the origin):

1. PHY transmits NULL packets (PID=0x1FFF).
2. BST MAC transmits MAC control messages (PID=0x1c, several MAC messages might be packed within a single MPEG).
3. PHY transmits Time stamp packets (PID=0x1c). Note that several MAC messages (including time – stamp) might be packed within a single MPEG.
4. Higher layers transmit service data (Ethernet traffic) packets.
5. Higher layers transmit management data (e.g, SNMP) packets.

6. IP over 802.16 (WiMAX)

This section specifies the frame format for transmission of IP packets and the resolution of IP addresses for WiMAX networks. It also addresses the issue of IP multicast packets over IEEE 802.16 networks.

6.1. Encapsulation

IEEE 802.16 [21][22] defines a new air interface and medium access control (MAC) protocol for the provisioning of high data rate services over large cell coverage. The architecture for WiMAX IP transmission is shown in Table 2- MAC packet components

The Radio Access Station (RAS) provides connectivity for the mobile station. The Access Control Router (ACR) is a generalized equipment set providing connectivity between the RAS and the IP network. Both RAS and ACR are parts of a base station in IEEE 802.16. The Edge Router (ER) is a device which routes the data packets between the I interface of the base station and the Internet. The I interface facilitates the connection between the ACR and the Internet. The IEEE 802.16 MAC consists of three sub-layers; service specific convergence sub-layer (CS), MAC common part sub-layer, security sub-layer. Multiple CSs are used for various protocols, including IPv4 and Ipv6 via their own specific CS.

The frame format for the MAC PDU (Packet data Unit), in the IEEE 802.16 U interface, consists of a 6-byte MAC header, various optional sub-headers, and an IP data payload as shown in Figure -23 (a). When the Ethernet CS is used (for A interface), an Ethernet header should be inserted between the MAC header and the IP header [26][28] as shown in Figure -23 (b). The meanings of the Generic MAC header are as follows:

HT: Header Type (1 bit). This should be set to zero indicating that it is a Generic MAC PDU.

EC: Encryption Control (1 bit). 0 = Payload is not encrypted; 1 = Payload is encrypted.

Type (6 bit). This field indicates the sub-headers (such as fragmentation, packing etc.) and special payload types (ARQ feedback) present in the message payload.

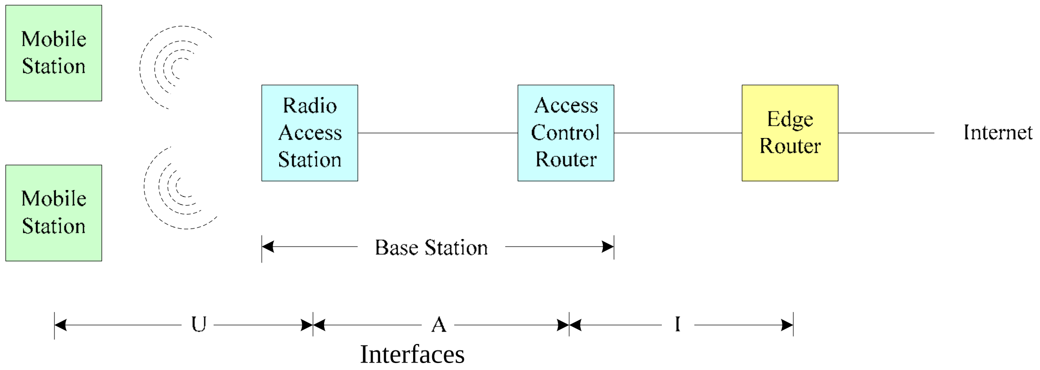


Figure -22 Elements of WiMAX Network

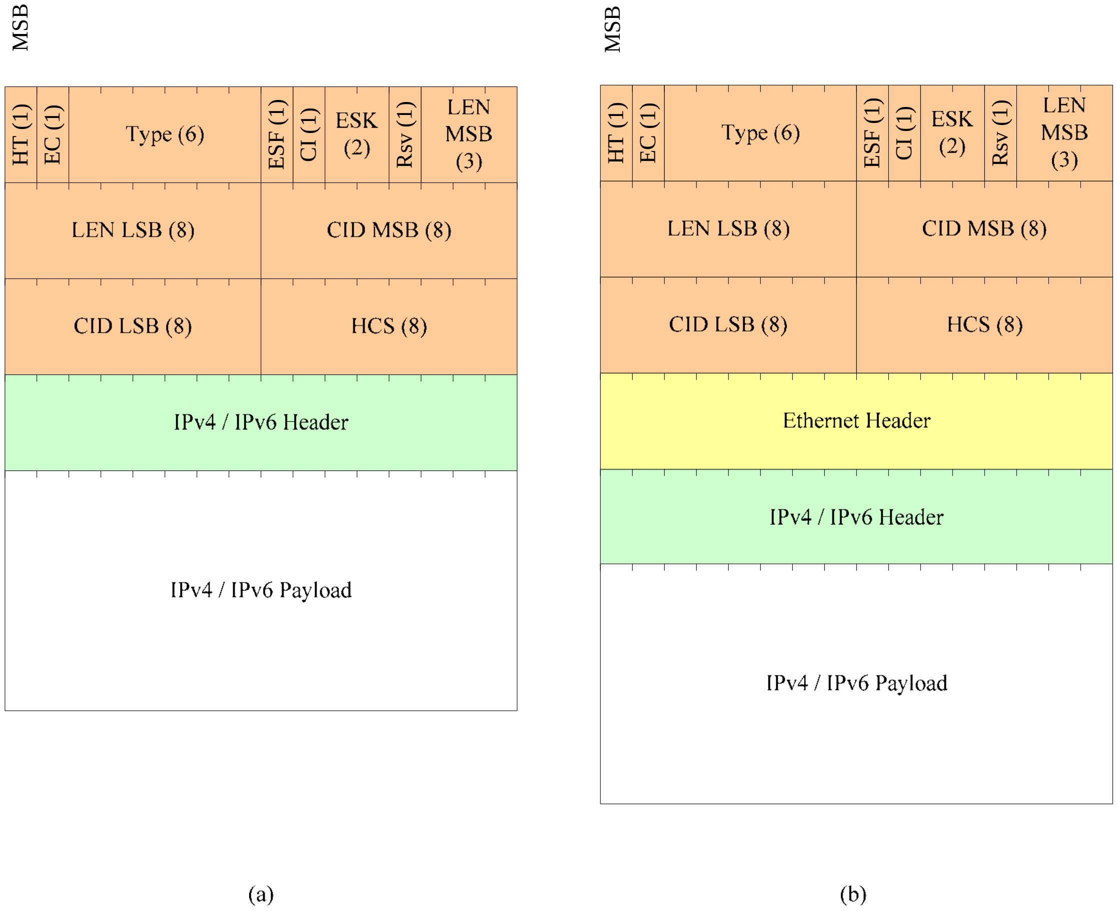


Figure -23 Frame format for (a) Reference point U (b) Reference point A

ESF: Extended Sub-header Field (1 bit). 0 = The extended sub-header is absent; 1 = The extended sub-header is present. The ESF is applicable both in the downlink and in the uplink.

CI: CRC Indicator (1 bit). 1 = CRC is included in the PDU by appending it to the PDU Payload after encryption, if any. 0 = No CRC is included.

EKS: Encryption Key Sequence (2 bit). The index of the traffic encryption key and initialization vector used to encrypt the payload. This field is only meaningful if the EC field is set to 1.

Rsv: Reserved (1 bit). It should be set to zero.

Length (11 bit). The length in bytes of the MAC PDU including MAC header and the CRC.

CID: Connection IDentifier (16 bit). The CID in the generic MAC header identifies a connection to equivalent peers in the MAC of the BS and SS (Subscriber Station).

HCS: Header Check Sequence (8 bit). An 8-bit field used to detect errors in the header. The transmitter shall calculate the HCS value for the first 40 bits of the IEEE 802.16 MAC header, and insert the result into this field. The HCS value is the remainder of the division by the generator polynomial that is g(x) = X8 + X2 + X + 1.

CRC: Cyclic Redundancy Check (32 bit). A MAC PDU may contain a CRC. Implementation of CRC capability is mandatory for OFDM. CRC = 1 indicates the presence of CRC in the MAC PDU. The generator polynomial is g(x) = X32 + X26 + X23 + X22 + X16 + X12 + X11 + X10 + X8 + X7 + X5 + X4 + X2 + X + 1. The CRC shall be calculated after encryption; i.e., the CRC protects the generic header and the ciphered payload.

6.2. Address resolution

The mobile WiMAX 802.16e works as 2 layer bridge. The BST works as 2 layer bridge between the operator network and the wireless section. The IP addresses that BST or user terminal defined are only for management and for exchanging Hand-Off information. The interface with the 3 rd layer switch/router is through Ethernet interface (in Runcom's equipment using RJ45 connector).

The BST consist of one or more sector cards, each sector card implements one instance of the air interface (MAC & PHY). All sectors are synchronized in timing and frequency in order to synchronize the network operation.

6.2.1. Downlink

6.2.1.1. Downlink allocations

Here are the downlink burst allocations (maximum configuration):

- **FCH:** is 4 subchannels over 1 time symbol (that is 4 slots), QPSK ½ CC.
- **DL-MAP burst**: QPSK 1/2 with repetitions (1, 2, 4, or 6 repetitions).
- **Management burst:** Include all MAC management broadcast messages such as UL-MAP, DCD and UCD.
- **Data bursts**: include several CID mode IEs.

The management and data bursts together consist of (normally) 30 x 11 slots (assuming PUSC reuse 1 and DL-MAP size of 4 time-slots).

6.2.1.2. DL-MAP size

Calculation
Assuming a single zone:

- DL-MAP payload size (not including IEs) is 13 bytes.
- Burst type IE (not including CID) size is 9 bytes.
- Burst type including CIDs size is 9 + 1 + n*2 where n is the number of CIDs.
- Cid_SWITCH_IE size is 12 bits, there is a need for 2 IEs so total 3 bytes overhead.
- DL-MAP system requirement is to use transmission of 6 repetitions (assuming PUSC, for PUSC 1/3 can be 2 repetitions).

Currently the implementation allocate a user per burst, that is all its' CIDs is using a single IE (CID type). Assuming a single CID per user then 12 bytes required per user. The DL-MAP overhead for N users is 13+9+3+N*(9+1+2) = 25+(12*N).

Let us define L Mbps as the UT maximum downlink burst size. Then an IE can include several CIDs with the same modulation and code-rate, not necessarily related to the same UT, which is size is equal or smaller then the UT (that at least has one of the CIDs) with the minimal L. Currently L is equal 10Mbps.

6.2.1.3. Data and management bursts throughput

When using 64QAM 5/6 in the user-data burst, the resulting rate is (assuming DL-MAP burst includes 4 time slots): 30sec * 11slots * 30bytes * 8bits * 200frames = 15.840000 Mbps. This is the over the air rate that includes all MAC level overhead including GMH, sub-headers, CRC32 (if attached) and management messages. If we add one time slot (total 30 * 1 = slots) then we can have

1.440000 more. The minimal allocation unit is a “line” – that all slots related to a sub-channel. That is, the waist of BW might be line size minus one slot. In QAM64 5/6 and line size of 11 slots this results in 10sec * 30bytes * 8bit * 200frames = 480 kbps per user for a second or 300 bytes per frame.

6.2.1.4. Downlink throughput

Based on current implementation. Throughput, in bps, is including all MAC overhead.

Number of Uts (up to)	Throughput (DL-MAP is using Repetition 6)
2 (2 time-slots)	15,840000
5 (3 time-slots)	14,.400000
7 (4 time-slots)	12,960000
10 (5 time-slots)	11,520000

Number of Uts (up to)	Throuput (DL-MAP is using Repetition 4)
3 (2 time-slots)	15,840000
10 (3 time-slots)	14,400000
13 (4 time-slots)	12,960000

6.2.1.5. Factors that affect throughput

Key factors that affect throuput per sector:

1. More DL-MAP Ies decrease throuput.
2. More Uts increase overhead (more DL-MAP IEs) and decrease throuput.
3. More repetitions on the DL-MAP decrease throuput.
4. More diversity of modulation/code-rate increases the number of IEs in the DL-MAP.
5. Use highest modulation (QAM64 5/6).
6. Use all available 30 sub-channels (PUSC-1K system) and time-slots.
7. Decrease MAC overhead:
    a. Use large PDU size - The packing rate increase and overhead decrease.
    b. Increase DCD and UCD intervals.
    c. CRC32 is/isnot attached

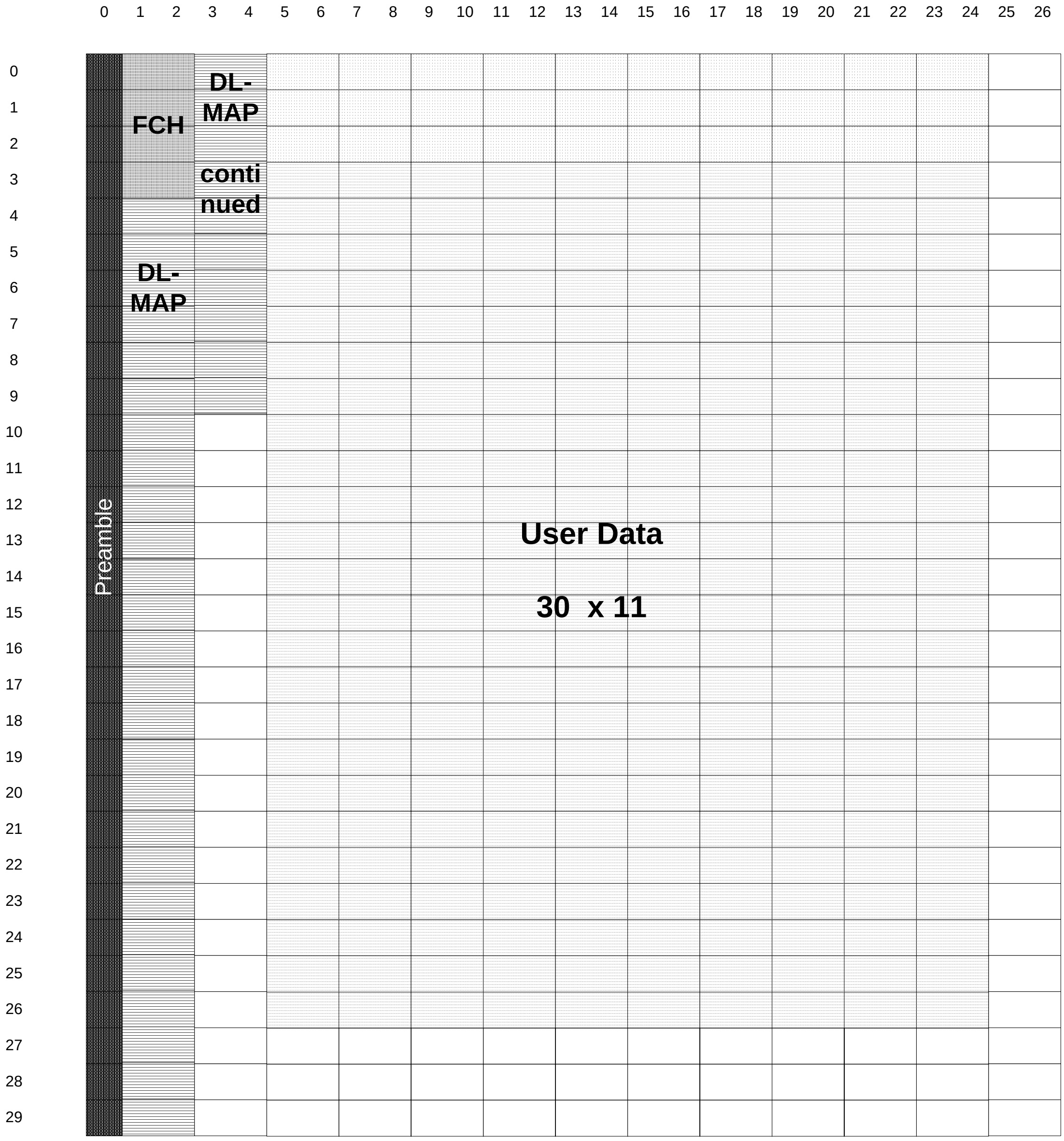


Figure -24: DL allocations

6.2.2. Uplink

6.2.2.1. Uplink allocations

Here are the uplink allocations (maximum configuration):

- **Ranging channel** is 6 subchannels over 3 time symbols (that is 1 slot).
- **Fast-feedback** is 29 (1K system), 64 (2K system) subchannels over 3 time symbols (that is 1 slot).
- **Data bursts**: the entire 4 time slots multiple 35 (1K), 70 (2K) subchannels.

  For QAM 16 ¾ it is 18 * 4slots * 35sec * 8bits * 200frames which is 4.032000 Mbps. On the uplink allocations are done on the time domain manner, that is, no fragmentation exist between users.

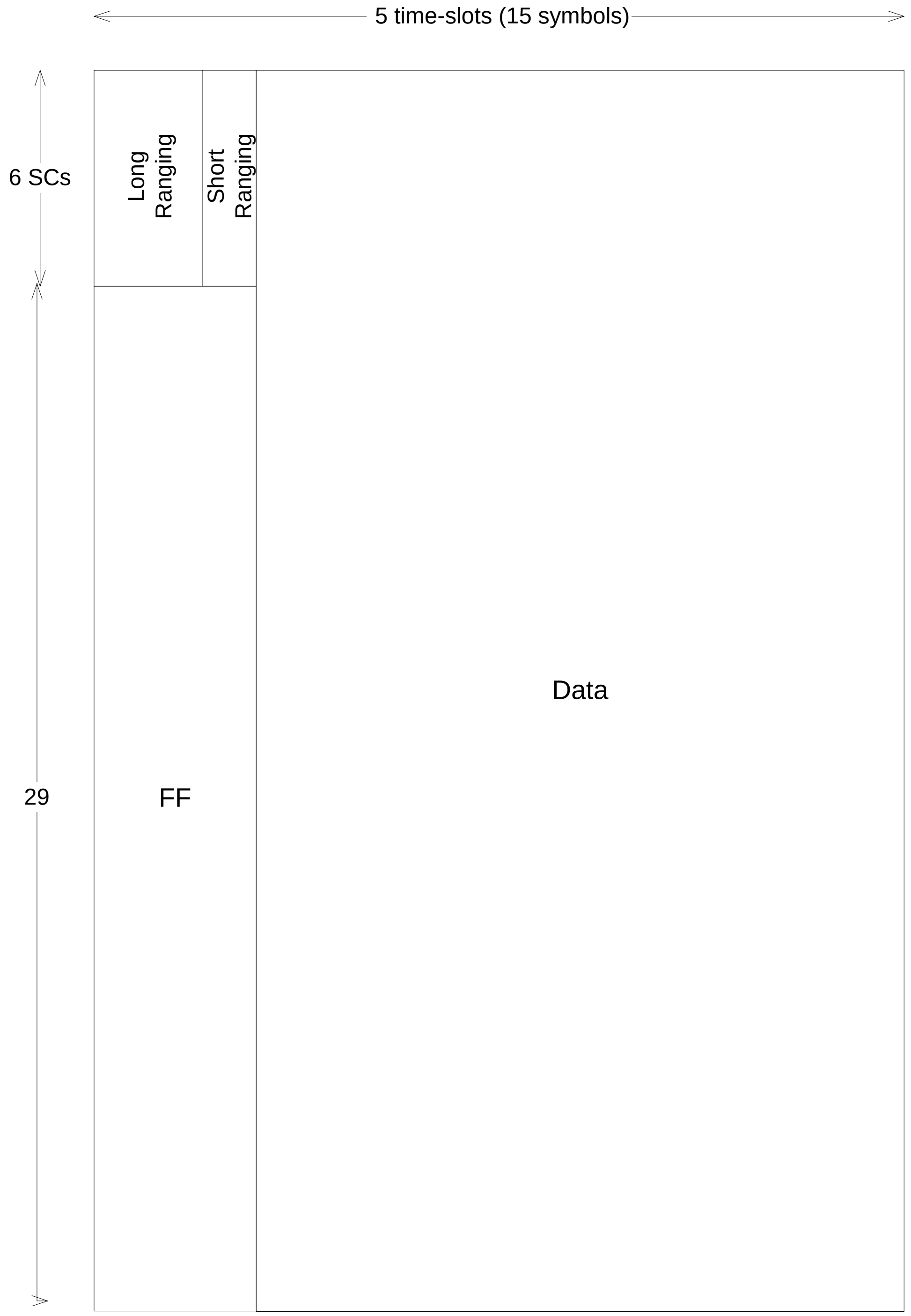


Figure -25: UL allocations (1K)

6.3. Multicast support

IEEE 802.16 networks do not provide link layer native multicast capability which restricts the adoption of protocols or applications based on IPv6 multicast functionality. This means that the point to multipoint connection oriented technology used in IEEE 802.16 air interface does not support bidirectional multicast transmission. Without the native multicast support, the IPv6 native discovery functions (such as on-link determination and address resolution) [25] do not operate properly. The multicast and broadband services provided by IEEE 802.16 use the MAC management addresses and not the IP multicast addresses. Furthermore, the standard does not provide a detailed description of IPv6 operation. The IEEE 802.16 connection always ends at the base station, while the IPv6 connection terminates at a default router. This leads to operation and limitation scenarios which are dependent on the given subnet model [26][27]. The four possible scenarios are now discussed briefly in this section.

6.3.1. Scenario A:

In this scenario, the base station is separated from the access control station and the connection between them is via Ethernet as shown in Figure -26. This scenario is highly relevant for the SUIT project, because of the support of multiple base stations and multiple mobile stations. Multicast packets are distinguished from unicast packets by using multicast CID (MCID). The MCID may be initialized during the establishment phase of the host IP connectivity.

When a link-local scope multicast packet originating from mobile station 1 in Figure -26, is received at base station 1, the base station multicasts the packet in the downlink direction by using MCID. Base station 1 then converts the IEEE 802.16 MAC frame format to an Ethernet frame and transmits the frame into the link connected to the access control station. Similarly, in the downlink direction, if an Ethernet frame sent from access control station is received in a base station, the base station examines the IPv6 destination address. If the destination address is a link-local scope multicast address, the packet is transmitted in the downlink direction with MCID.

When mobile station 1 sends a non-link-local scope multicast packet, base station 1 performs the same operation as for the link-local scope case. When the access control station receives the packet transmitted by base station 1, it searches the multicast routing table and forwards the packet to the access control station. The packet is then forwarded by the access control station and is delivered to base station 2 or the edge router according to regular IPv6 multicast packet transport procedures. If the packet is destined for mobile stations in the base station 2 subnet, then base station 2 transmits the received packet to its downlinks with a predefined MCID.

Similarly, when the access control station receives a packet from the edge router, it looks up the multicast routing table and checks whether a receiver of the packet exists in the access control stations subnets. If a receiver exists, the access control station sends the packet to appropriate base stations in the downlinks. When the base station receives the multicast packet sent from access control station, it checks the IPv6 destination address. If the destination address is a non-link-local scope multicast address, the base station multicasts the packet to its downlinks with MCID.

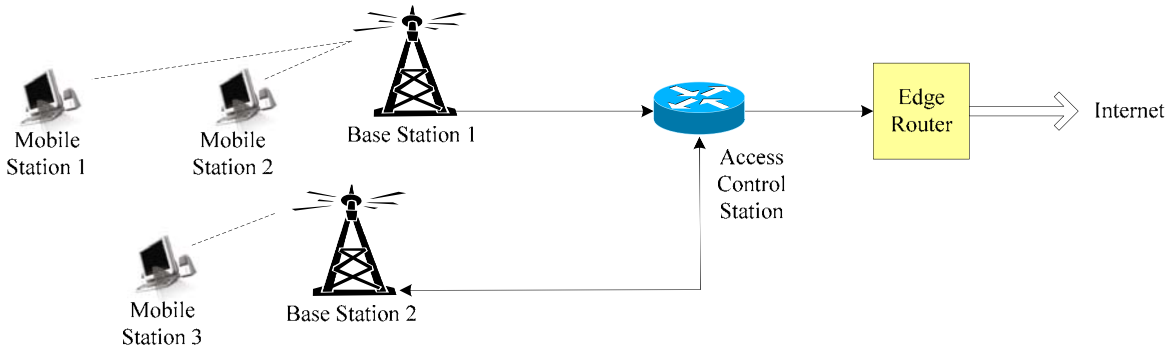


Figure -26 WiMAX multicast scenario A

6.3.2. Scenario B:

Scenario B represents the configuration shown in Figure -27, where the base station is separated from the access control station, and there are multiple access control stations. This means a subnet, attached to multiple access control stations, consists of multiple base stations and multiple mobile stations. This scenario is most suitable if IEEE 802.16 access networks are widely deployed similarly to WLAN hot-spot deployments.

Multicast packet transmission originating from a mobile station with link-local scope is similar to scenario A. The packet received at the base station is sent in the downlink direction using the MCID and is also sent on the wired link after de-capsulation of the IEEE 802.16 MAC header. In this way all the routers and base stations attached on a wired link get the multicast packet, which is then forwarded in the respected downlink direction using the MCID.

Similarly, if the base station receives a multicast packet with non-link-local scope from a mobile station, it forwards the packet in the downlink direction using MCID, and sends the packet to other base stations and routers linked by a wired Ethernet connection. However, in this case, the access control station will look up the IPv6 routing table for multicasting and will then forward the packet to the edge router for further transmission.

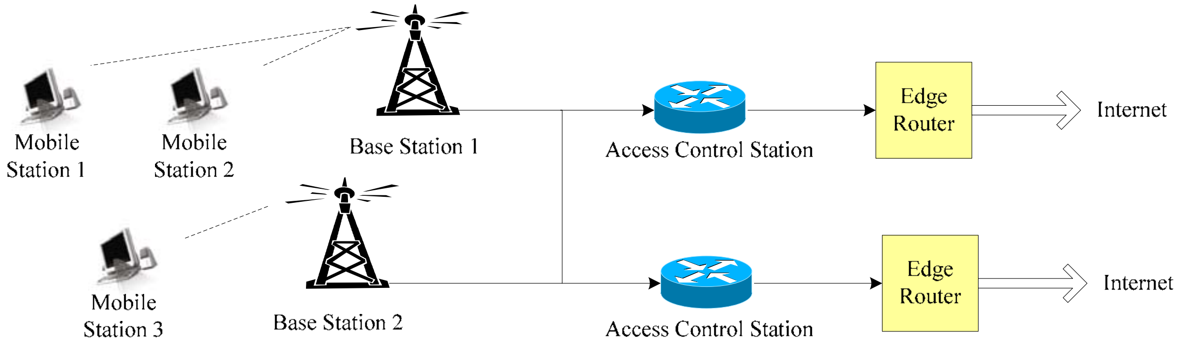


Figure -27 WiMAX multicast scenario B

6.3.3. Scenario C:

In this scenario, the base station is integrated with the access control station, and a subnet is composed of a single base station/access control station with multiple mobile stations as shown in Figure -28. Since each base station/access control station is connected directly via a single Ethernet connection to the edge router, no routing protocols are needed at the access control station. All outbound multicast packets from the mobile station with link-local scope are sent back in the downlink direction by the base station/access control station using the MCID. However, upon reception of multicast packets with non-link-local scope from the mobile station, the base station/access control station forwards the packets to the edge router after analyzing the IPv6 multicasting routing table.

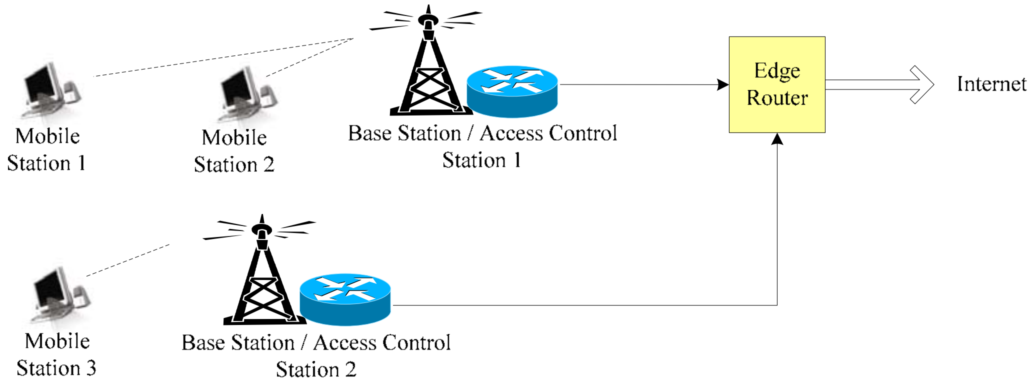

Mobile Station 1
Mobile Station 2
Base Station / Access Control Station 1
Edge Router
Internet
Mobile Station 3
Base Station / Access Control Station 2

Figure -28 WiMAX multicast scenario C

6.3.4. Scenario D:

This scenario is similar to scenario C, except that there is only a single mobile station for each base station/access control station as shown in Figure -29. This situation mimics the existing 3GPP IPv6 model because within 3GPP networks, hosts connect to their default routers via point-to-point links [29]. This means there are exactly two IP devices connected to the point-to-point link. Similarly to scenario C, the WiMAX connection and IPv6 termination point are the same due to integration of the base station and access control station. In contrast to scenario C, each mobile station can be on a different IPv6 link. This means many IPv6 protocols can be operated without specific consideration of the network implementation. Furthermore, since broadcasting is not desired in this scenario, IPv6 CS (Convergence Sub-layer) type should be used instead of the Ethernet CS type.

When a multicast packet with link-local scope is received from a mobile station, it is terminated without the need for forwarding anymore. However, in the case of non-link-local transmission of a multicast packet from mobile station, the base station/access control station looks up the IPv6 routing table and sends the packet to the edge router for further transmission.

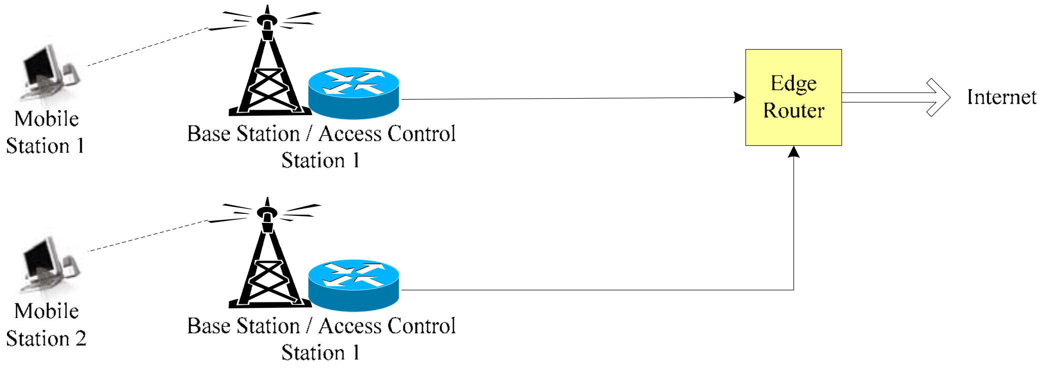

Mobile Station 1
Base Station / Access Control Station 1
Edge Router
Internet
Mobile Station 2
Base Station / Access Control Station 1

Figure -29 WiMAX multicast scenario D

7. IP over 802.11

The IEEE 802.11 family of wireless LAN standards offers a direct shared-medium replacement for Ethernet. Thus IP runs over the wireless LAN in much the same manner as over the wired Ethernet. The main differences are those of the wireless physical medium used which result in issues such as having a higher error probability in packet transmissions or different transmission rates depending on the distance and the channel conditions (see section 4.5). In the following sections, an overview of the main issues regarding the implementation of IP over WLAN is provided.

7.1. Address resolution

In order to find out the correspondence between an IP address and its associated device MAC address, an address resolution procedure is needed. Address Resolution Protocol (ARP) is widely employed to map IP (concretely IPv4) addresses into link-layer hardware addresses.

ARP executes locally at every host, closely related to the network interface card. When a machine needs to resolve which MAC address is associated to a concrete IP address and it does not have that information locally, it broadcasts an “ARP query” message (with MAC broadcast address as destination) asking for it. If destination host is not within the same LAN, this message will be redirected through the router to the destination network. Since ARP is running at the target device, it will recognize the call and send its hardware address to querying machine in an “ARP response” message.

Resolved addresses are commonly cached in an address resolution table for a certain period of time. For example, the set of MAC addresses linked to an IP multicast address can be found there. By the way, IPv4 broadcast address (255.255.255.255) is mapped into MAC broadcast address (FF:FF:FF:FF:FF:FF).

Sometimes it is needed to know which IP address corresponds to a MAC address. In those cases, protocols such as Inverse ARP (InARP) can be employed.

7.2. MAC framing and encapsulation

7.2.1. MAC frame structure

Figure -30 defines the format of an 802.11 packet, with the length in bytes of each field:

Frame Control	Duration ID	Addr.1	Addr.2	Addr.3	Sequence Control	Addr.4	Data	FCS
2	2	6	6	6	2	6	0 - 2312	4

Figure -30 802.11 packet structure

Some characteristic fields of 802.3 (Ethernet) frames have been removed, such as type, length and preamble. A more detailed view on MAC frame components can be found in the following table:

Field	**Bits**	**Description**
Frame Control	16	
- Protocol version	2	Equal to 0
- Type	2	Management, Control or Data
- Subtype	4	RTS, CTS, ACK, Data, Beacon…
- To DS	1	1 = To the Distribution System.
- From DS	1	1 = From the Distribution System.

- More Fragments	1	1 = More fragment frames 0 = Last or unfragmented frame
- Retry	1	1 = Re-transmission.
- Power Management	1	1 = Station in power save mode 0 = Active mode.
- More Data	1	1 = Additional frames buffered for the destination address
- WEP	1	1 = Data processed with WEP algorithm. 0 = No WEP.
- Order	1	1 = Frames must be strictly ordered.
Duration ID	16	Can be used to set up the NAV.
Address 1	48	Source address
Address 2	48	Destination address
Address 3	48	Receiver station address
Sequence Control	16	Fragment number (4 bits) + Sequence number (12 bits)
Address 4	48	Transmitter station address
Frame Body	0 - 18496	Data field
FCS	32	Frame Check Sequence (32 bit CRC)

Table 2- MAC packet components

7.2.2. IP encapsulation within 802.11

Encapsulation of network layer protocols within 802.11 relies in 802.2 LLC specifications. Two different though quite similar schemes are commonly used for this purpose: IETF encapsulation (RFC 1042) and tunnel encapsulation (802.1H). The only difference between them is the value of a field, as can be seen in the following figure:

802.11 MAC headers	SNAP DSAP 0xAA	SNAP SSAP 0xAA	Control (UI) 0x03	Ethernet Tunnel 0x00-00-F8	Type (IP) 0x0800	IP packet	FCS (4bytes)

Figure -31 802.11 encapsulation following 802.1H

802.11 MAC headers	SNAP DSAP 0xAA	SNAP SSAP 0xAA	Control (UI) 0x03	RFC 1042 Encapsulation 0x00-00-00	Type (IP) 0x0800	IP packet	FCS (4bytes)

Figure -32 802.11 encapsulation following RFC1042

SNAP stands for 802.2 Sub-Network Access Protocol. This protocol inserts specific one-byte headers for Destination Service Access Point (DSAP) and Source Service Access Point (SSAP). Then, a Control field describing category of delivery is set up. The adequate Control byte for IP best-effort is 0x03, denoting "Unnumbered Information" (UI). Finally, an Organizationally Unique Identifier (OUI) field is filled, depending on the encapsulation method used.

8. DVB-T/H/RCT / 802.16 / 802.11g interoperability issues

As discussed in Deliverable D1.1 about terminal requirements, we have three types of SUIT terminals, Wi-Fi, WiMAX/DVB-T/H/RCT and MHP-IPTV. The Wi-Fi terminal requires a gateway which has two interfaces on the local loop side, WiMAX and DVB, and Wi-Fi on the other side, that of WLAN. If we move most of the gateway functionalities to the terminal, we get the WiMAX/DVB-T/H/RCT terminal. This terminal will allow us to experiment vertical and horizontal handover. The MHP-IPTV will be a connected to WiMAX and will be used to test MHP applications as well as horizontal handover. The most complex network scenario is the one that includes Wi-Fi terminals. This case's requirements are explained in the following section.

8.1. Home network scenario

SUIT proposes the convergence between WiMAX and DVB as depicted in the figure below. Both networks feed a WLAN with Wi-Fi terminals. The example shown below, in the figure, includes two WLANs. Each WLAN connects to the local loop through a Gateway with DHCP (see Section 3.1.2.1) and NAT (see Section 3.1.2.1) capabilities. Therefore, Wi-Fi Terminals in a WLAN may use the same IP private addresses as other Wi-Fi Terminals placed in another WLAN. Each gateway has two input interfaces, we mean, two transceivers, one WiMAX and another DVB-T/H/RCT. On the Playout side, there are a real time encoder and a pre-recorded stream server. Each of them produces two different descriptions. Description 1 is always switched to VLAN A (DVB) and description 2 is always switched to VLAN B (WiMAX). Therefore, the switch is Layer 2 with VLAN capability. The terminals can access to the internet through the Router. The Gateway can inform the Playout (Controller-Return Channel) about the network or terminal characteristics. All transceivers act as Bridges, just copying packets at the link (MAC) layer. A bridge is like a hub but with MAC address filtering. In case the extractors will broadcast descriptions, it should use IP and MAC broadcasting address. Otherwise, in a unicast situation, they have to use the right gateway IP address. All wired connections use Ethernet protocols with RJ45 Connector 100baseT.

As an example, we use the IP Router address in IT which is 193.136.93.1. All other address, IPx, x=1,..,9, are public and can start on 193.136.93.18 and increment sequentially (18, 19,…26).

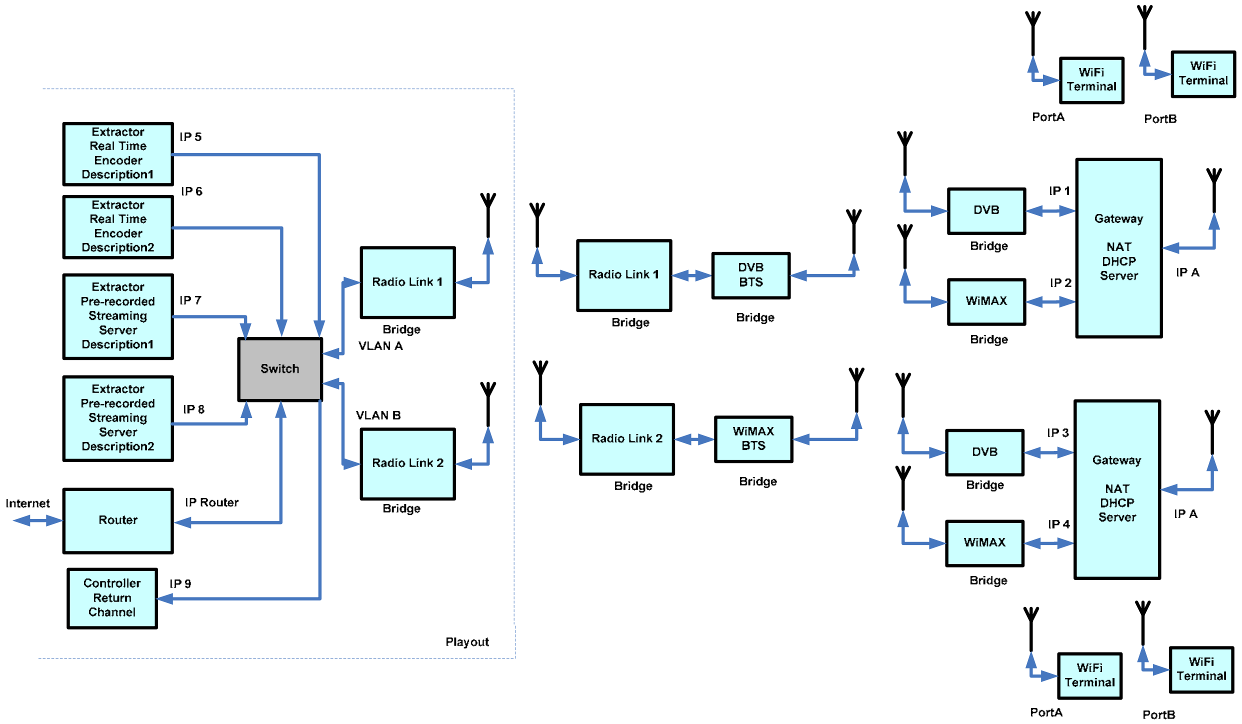


Figure -33 IP requirements for home scenario

8.2. Mobile network scenario

Once explained the home network scenario, the mobile network scenario is easy to understand. The Gateway is now replaced by the WiMAX/DVB-T/H/RCT terminal as shown in the figure below. In order words, some of the Gateway functionalities, like the combiner, have moved to the terminal. Now, the system has to handle with handover issues. The controller must be informed about the network characteristics in order to redirect the information from the Playout by acting on the Switch. Again, all wired physical connections are RJ45.

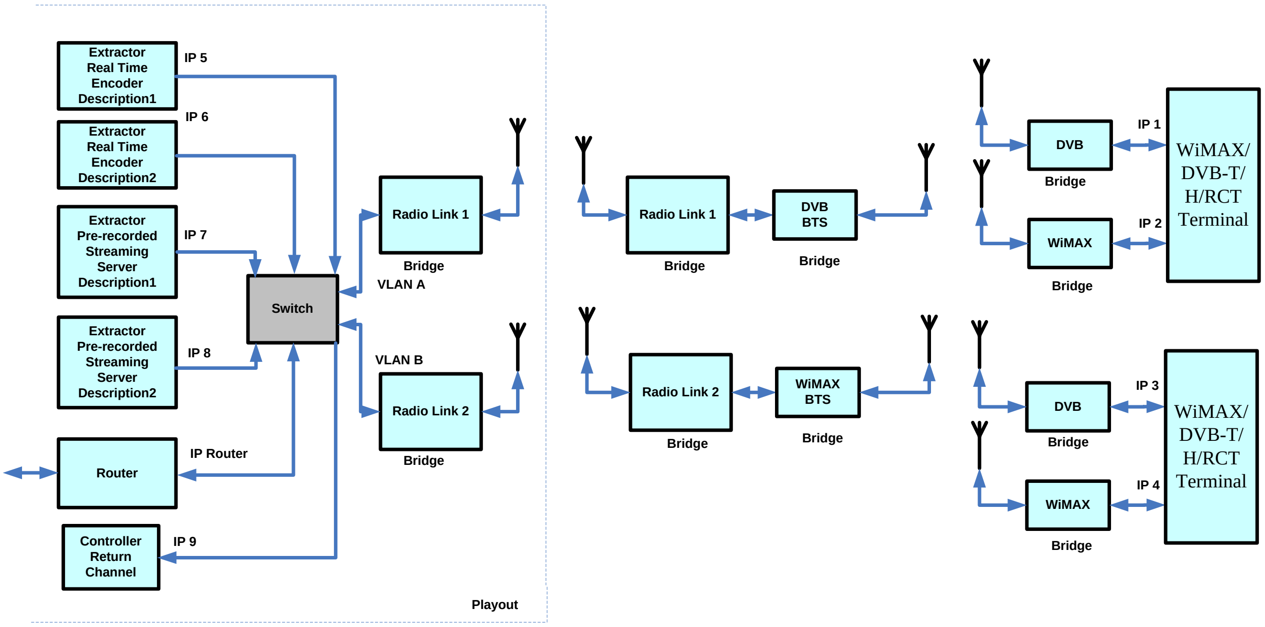

Extractor Real Time Encoder Description1
Extractor Real Time Encoder Description2
Extractor Pre-recorded Streaming Server Description1
Extractor Pre-recorded Streaming Server Description2
IP 5
IP 6
IP 7
IP 8
Switch
Router
IP Router
Controller Return Channel
IP 9
Playout
Radio Link 1
Bridge
VLAN A
VLAN B
Radio Link 2
Bridge
Radio Link 1
Bridge
DVB BTS
Bridge
Radio Link 2
Bridge
WiMAX BTS
Bridge
DVB
Bridge
WiMAX
Bridge
IP 1
IP 2
WiMAX/ DVB-T/ H/RCT Terminal
DVB
Bridge
WiMAX
Bridge
IP 3
IP 4
WiMAX/ DVB-T/ H/RCT Terminal

Figure -34 IP requirements for mobile scenario.

8.3. MHP-IPTV scenario

The MHP-IPTV scenario setup will comply with the standards DVB-IP 1.2 and DVB-MHP 1.1. DVB-IP phase 1 defines the interface between a HNED (Home Network End Device) – the terminal – and the service network. The terminal receives a live TV service by joining a multicast group. After joining the multicast group the terminal receives a DVB Transportstream over IP. The service location in DVB-IP is announced using a mechanism called Service Discovery & Selection (SD&S) which has been defined in DVB-IP. SD&S proposes a multicast and a unicast method for the delivery of SD&S information to the terminal. The terminal is required to support both methods, with the consequence that the service provider is free to choose one of them. There are a few possibilities how a terminal finds the SD&S information – also called the "Entry Point".

1. The network configures the terminal with DHCP (Dynamic Host Configuration Protocol).
2. The terminal uses DNS to resolve either _dvbservdsc._tcp.services.dvb.org or _dvbservdsc._udp.services.dvb.org into an IP address.
3. The terminal joins the multicast group 224.0.23.14 which has been assigned by IANA (Internet Assigned Numbers Authority) for DVB service discovery.
4. The end user is asked to enter the entry point manually.

The terminal has to check all 4 options in this order until it gets the entry point. The SD&S information is transmitted using the protocol STP (SD&S transport protocol) over IP multicast or being requested from an http server if the service provider has chosen the unicast delivery method. The port number for the SD&S service is 3937, as assigned by IANA.

DVB-MHP applications can be used in a DVB-IP network without any restrictions. The "built in" return channel of WiMAX can be used by an interactive application to request content on demand, but also the application itself might be retrieved on demand from a server. MHP 1.1 defines the application loading via the remote channel. The transport protocol again is http.

Note: IPv6 is not in the scope of DVB-IP Phase 1.2, but possible migration scenarios will be considered in DVB-IP Phase 2.

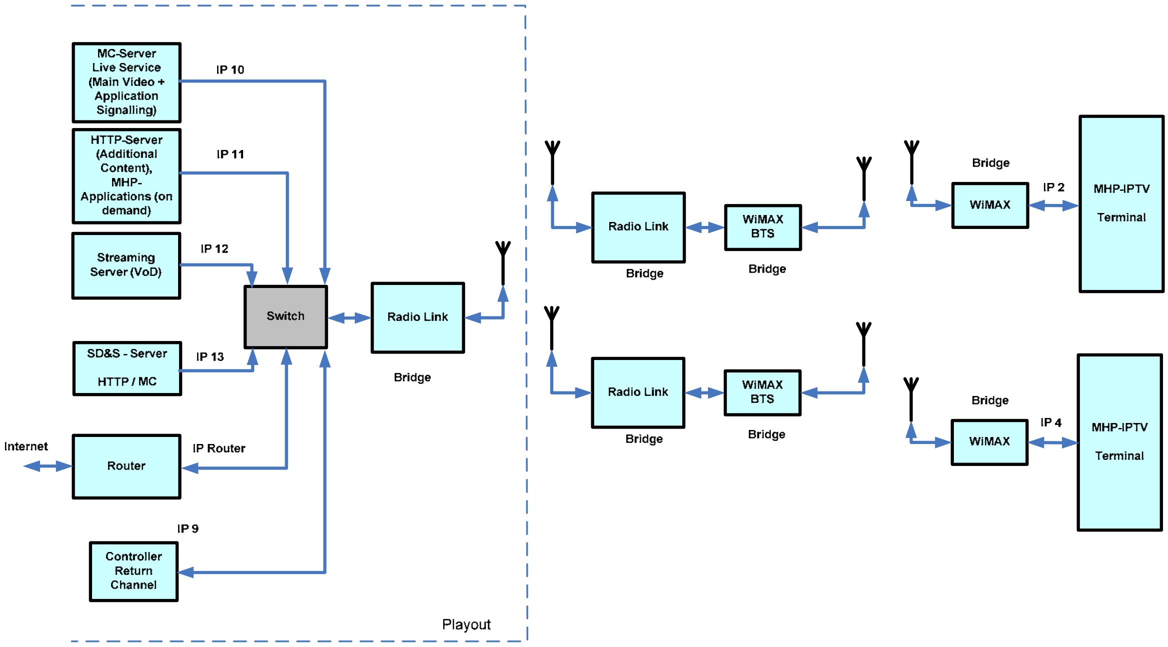


Figure -35 IP requirements for MHP-IPTV scenario.

In Figure -35 above, the MHP-IPTV scenario in case of horizontal handover is depicted.

In contrast to the SUIT terminal, the MHP-IPTV terminal receives its content solely via WiMAX. A server plays out the so-called Live Service using Multicast (IP10). This service contains the Main-Video and the signalling of MHP Applications belonging to that service. The MHP-Application as well as additional content will be retrieved from another server (IP11). A streaming server is foreseen to provide hyperlinked Video on demand content.

As above described, the SD&S –Server (either HTTP or MC) provides the information needed by the MHP-IPTV terminal to find the services in the network.

In respect to horizontal handover tests – WiMAX to WiMAX-, a return channel controller might be required.

9. Conclusions

A set of mechanisms and solutions at the IP level have been analyzed to allow interoperability among the wireless networks considered in the SUIT project (DVB, WiMAX and Wi-Fi), following the “all-IP network” paradigm.

In a first step, a review of the available Internet Protocol versions together with a description of the main characteristics and services offered by the wireless networks has been presented. In a second step and focusing on the available solutions to support IP over DVB, WiMAX and Wi-Fi networks, specific approaches for address resolution, encapsulation and multicast support have been identified. Finally, some implications at the different SUIT scenarios are derived from this research, resulting in a set of specific requirements at network, link, and physical layers for different scenarios according to the type of terminals being used, which can be summarized as:

- IPv4 will be adopted to ensure compatibility among all the components involved in the deployment of the SUIT project. Nevertheless, the possible migration to IPv6 will be considered along the development of the project.
- The playout and the SUIT Terminal/Gateway will be interconnected within the same IP network.
- Each SUIT Terminal/Gateway will be connected to the playout via two different links:
    1. A communication link with a DVB-T/H/RCT link.
    2. A communication link with a WiMAX link.

  Thus, each SUIT Terminal/Gateway will have two input interfaces, via two transceivers, one for WiMAX and another for DVB-T/H/RCT. All transceivers will act as bridges, just transferring packets at the link (MAC) layer.
- The connection between the playout and the MHP-IPTV terminal will rely only on a single link: that of the WiMAX channel.
- Two VLANs will be established over these physical links: one over the DVB channel (VLAN A) and the other over the WiMAX channel (VLAN B).
- Each SUIT Terminal/Gateway will use two different IP addresses to be able to manage separately the information coming from each VLAN.
- The Gateway will include a Wi-Fi interface to feed the Wi-Fi terminals. The Gateway will provide DHCP and NAT capabilities, thus Wi-Fi Terminals in a WLAN may use IP private addresses.

- Internal wired connections will use Ethernet protocols with RJ45 Connector 100baseT.

10. Acronyms

3GPP	3rd Generation Partnership Project
ACR	Access Control Router
AIPN	All-IP Network
AP	Access Point
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BS	Base Station
BSP	Board Support Package
BST	Base Station
BSS	Base Service Set
CC	Convolution Code
CCMP	Counter mode with Cipher block chaining Message authentication code Protocol
CI	CRC Indicator
CID	Connection IDentifier
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Convergence Sublayer
CSP	Chip Support Package
DCD	Downlink Channel Descriptor
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DIFS	DCF Inter-Frame Space
DL	Down link
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Inter-Frame Space
ER	Edge Router
ERP	Extended Rate Physical layer
ESS	Extended Service Set
EUTRAN	Enhanced UTRAN
FCH	Frame Control Header
FEC	Forward Equivalence Class / Forward Error Correction
FTP	File Transfer Protocol

GERAN	GSM Edge Radio Access Network
HCS	Header Check Sequence
HDTV	High Definition Television
HTML	HyperText Markup Language
IBSS	Independent Base Service Set
IE	Information Element
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
InARP	Inverse Address Resolution Protocol
ISO	International Standards Organization
LLC	Logical Link Control
MAC	Medium Access Control
MIR	Maximum Information Rate
MMS	Multimedia Messaging System
MPLS	Multi-Protocol Label Switching
MS	Mobile Station
NAT	Network Address Translation
OFDM	Orthogonal Frequency Division Multiplexing
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PUSC	Partial Usage Sub Channel
PIFS	PCF Inter-Frame Space
QoS	Quality of Service
RAS	Radio Access Station
RF	Radio Frequency
RFC	Request For Comments
RSVP	Resource reservation Protocol
RTOS	Real Time Operating System
SIFS	Short Inter-Frame Space
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
STB	Set-Top-Box
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol

UCD	Up link Channel Descriptor
UDP	User Datagram Protocol
UL	Uplink
UT	User Terminal
UTRAN	UMTS Terrestrial Radio Access Network
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VoIP	Voice over IP
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

11. References

[1] 3rd Generation Partnership Project (3GPP), “Technical Specification Group Services and Systems Aspects; All-IP Network (AIPN) feasibility study (Release 7)”, 3GPP TR 22.978 V7.1.0, 2006

[2] European Telecommunication Standards Institute, “Universal Mobile Telecommunications System (UMTS); Service requirements for an All-IP Network (AIPN); Stage 1 (3GPP TS 22.258 version 7.0.0 Release 7)”, ETSI TS 122 258 V7.0.0, 2005

[3] Information Sciences Institute, “Internet Protocol”, RFC 791, 1981

[4] Deering S., Hinden R., “Internet Protocol, Version 6 Specification”, RFC 2460, 1998

[5] Bradner, S. O., “IPng : Internet Protocol Next Generation”, Addison-Wesley, 1995

[6] Stephenson A., “DiffServ and MPLS: A Quality of choice”, Article in www.networkmagazine.com, 1999

[7] Rosen, E., Viswanathan, A. et al., “A Proposed Architecture for MPLS”, RFC3031, 2001

[8] Blake, S., Black, D., et al., “An Architecture for Differentiated Services”, RFC2475, 1998

[9] Perkins, C., “IP Mobility Support for IPv4 ”, RFC3344, 2002

[10] Soliman, H., “Mobile IPv6 : mobility in a wireless internet”, Addison-Wesley, 2003

[11] IEEE 802.3, “Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications”, 2000.

[12] ETSI EN 302 307: "Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering (DSNG) and other broadband satellite applications", Jan 2004.

[13] TM2977_r4, "Digital Video Broadcasting (DVB); DVB-H Implementation Guidelines”, Set 2004.

[14] Gallager, R., “Low Density Parity Check Codes”, IRE Trans. on Info. Theory, pp. 21-28, Jan 1962.

[15] ETSI EN 300 744, “Framing structure, channel coding and modulation for digital terrestrial television”, Nov 2004.

[16] ETSI EN 301 192: "Digital Video Broadcasting (DVB); DVB specification for data broadcasting", Nov 2004.

[17] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems", Nov 2004.

[18] ETSI EN 300 421, “Framing structure, channel coding and modulation for 11/12 GHz satellite services”, Aug 1997.

[19] ETSI EN 300 744, “Framing structure, channel coding and modulation for digital terrestrial television”, Jan 2001.

[20] Gast, M., “802.11 wireless networks : the definitive guide”, O'Reilly, 2002

[21] IEEE 802.16,“802.16-2004 Standard for Local and Metropolitan Area Networks Part 16: Air interface to fixed and mobile broadband wireless access systems”, 2004

[22] IEEE 802.16e, “Part 16: Air interface to fixed and mobile broadband wireless access systems”, 2004

[23] IEEE 802.11-1999, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, IEEE 802.11, 1999.

[24] IEEE 802.11g Part 11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further higher data rate extension in the 2.4 GHz band”, IEEE, 2003

[25] [RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[26] Shin, M and Han, Y "ISP IPv6 Deployment Scenarios in Broadband Access Networks", draft-ietf-v6ops-8012-16-deployment-scenarios-00 (work in progress), May 24, 2006.

[27] Shin, M. and Jang, H., "Transmission of IPv6 Packets over IEEE 802.16", draft-shin-16ng-ipv6-transmission-01 (work in progress), June 19, 2006.

[28] Kim, S., Paik, E., Jin, J.; “IP Deployment over IEEE 802.16 Networks”, draft-nam-ipv6-802-16e-01.txt (work in progress), June 24, 2006

[29] [RFC3316] Arkko, K., Kuijpers, G., Soliman, H., Loughney, J., Wiljakka, J., Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, April 2003.