SATSIX : A Network architecture for Next generation DVB-RCS Systems

L. Fan[1], C. Baudoin[2], F. Rodriguez[3], A. Ramos[4], J.A. Guerra[5], B. Cuesta[6], G. Fairhurst[7], A. Sathiaseelan[7], P. Berthou[8], T. Gayraud[8], L. Liang[1], A. Yun[9], E. Callejo[9], I. Melhus[10], S. Iyengar[1], H. Cruickshank[1], Z. Sun[1]

[1] *University of Surrey, Guildford, Surrey, GU2 7XH, UK*

[2] *Thales Alenia Space, 26, Avenue J-F Champollion, 31037 Toulouse Cedex 1, France*

[3] *Telespazio, Via Tiburtina 965, 00156 Rome, Italy*

[4] *Telefonica I+D, Parque Tecnológico de Boecillo, 47151 Boecillo Valladolid, Spain*

[5] *Hispasat SA, Spain*

[6] *University of Valladolid, Calle del Cementerio s/n, 47011 Valladolid, Spain*

[7] *University of Aberdeen, Department of Engineering, Fraser Noble Building Kings College, Aberdeen AB24 3UE UK*

[8]*CNES/LAAS, Toulouse University of Science, France*

[9] *Thales Alenia Space Espana, 7 calle Einstein (PTM) 28760 Tres Cantos, Madrid, Spain*

[10] *SINTEF ICT - Communication Systems, O.S Bragstads plass 2C, Norway*

Abstract

Broadband satellite will play an important role to provide universal broadband access for the users. In order to lower the cost, the next-generation satellite systems should support IPv6 and seamlessly integrate with terrestrial networks, including wireless local loops. Based on the studies on the requirements and design constraints, in this paper, a novel network architecture has been proposed as a potential solution to the above problems. The proposed network architecture supports both transparent and regenerative topologies and can seamlessly interworking with WLL. It also integrates QoS, multicast, security, and mobility functions to support a range of transport requirements. How to apply this network architecture to support three different scenarios, namely corporate application scenario, residential application scenario and collective access terminal scenario, are also described.

Introduction

Current broadband satellite services are regarded as a niche market due to the cost of launching a satellite system, and the relatively limited available bandwidth compared to terrestrial counterparts. Cost-effective solutions are essential to improve up-take of broadband satellite and to efficiently accommodate new multimedia applications, integrating satellites into next generation networks. These issues are being addressed in the SATSIX, which will implement innovative concepts and for broadband satellite systems and services.
This paper describes the design of the SATSIX network architecture, with particular reference to support for IPv6 and thw integration of hybrid satellite and wireless local loops (WiFi and WiMAX), which together will enable low-cost universal broadband access. Three network architectures have been identified that use this reference network architecture to support three different scenarios, namely corporate application scenario, residential application scenario and collective access terminal scenario. In each case the related protocol stacks are presented.

1 Requirements and Constraints

This section focuses on the requirements and design constraints that were faced in the design of the network-layer of the SATSIX system utilising the IP protocol suite.

TCP provides a reliable byte-stream interface to the IP protocol suite. It is used by many popular applications, including web transfer (http, shttp), terminal access (telent, ssh, rlogin), file transfer (ftp, nfs) and email (smtp, pop, imap). TCP may also be used for multimedia services (e.g. streaming over RTP). Although TCP is the most widely used transport protocol and contributes the majority of traffic seen on the Internet backbone, most current Internet multimedia applications use UDP as the transport protocol (e.g. video and audio streaming, gaming). UDP is also used for many signaling applications (e.g. SIP, routing protocols, network management) and for IP multicast (e.g. IPTV).

Multimedia traffic may be associated with an explicit resource reservation, a DiffServ (DS) class, or the Best Effort (BE) service. Each of these approaches has merit. When the entire transmission path is under the control of a network operator, explicit QoS may be configured and used to provide a service guarantee for each configured session. This is the approach favored in many current IPTV deployments. It is however difficult to manage when the traffic has unknown or highly variable characteristics. An alternative is to use a DiffServ class provisioning capacity to the service as a whole (rather than individual sessions). This can be significantly better than the unrestricted behavior offered by a Best Effort service, particularly when traffic patterns are well understood. However, in both the BE and DS approaches, several traffic flows can share common capacity, and it is highly desirable to provide a method to fairly distribute the available capacity between the various flows, known as congestion control.

Although for many years TCP and IP offered the only transport protocols within the Internet Protocol Suite, the Internet Engineering Task Force (IETF) has more recently added three new protocols to supplement these specifications: UDP-Lite (a variant of UDP for multimedia optimised for wireless enviroments), the Stream Control Transport Protocol (SCTP, for transaction-based signaling protocols), and the Datagram Congestion Control Protocol (DCCP) transport protocol as an alternative to UDP for unicast multimedia applications. The features of the various transport protocols are summarised in the table below.

Current UDP-based applications can (and often do) transmit at a constant rate, irrespective of available capacity. Although congestion control is a standard feature of TCP, it is not provided by most current applications that use UDP for multimedia. Growth of such long-lived non-congestion-controlled traffic poses a threat to the overall health of the Internet. Congestion control is particularly desirable for sessions that need to operate over the dynamically changing properties that may result from Internet paths that combine both wired networks and wireless (e.g. satellite broadband). Standards-based Congestion-Control and NAT-traversal are key features of the new DCCP protocol, while supporting the flow-based semantics of TCP, but not the in-order delivery and reliability of TCP. DCCP is designed to operate with any QoS, including the best-effort service, however it can not effectively deliver real-time multimedia flows over highly variable network paths, since like TCP, it utilizes transport layer feedback to determine an appropriate transmit rate, and will result in penalizing flows that see abrupt changes in delay and/or capacity.

While the IP transport protocols are designed to operate over any IPv4 or IPv6 network service, there are important network characteristics (network QoS, support for multicast and mobility, security and wireless constraints) that can significantly impact performance when used in a satellite environment. It is therefore important to asses the requirements for each individual application using the network service.

1.1 QoS requirements

Managing bandwidth allocation is a difficult task because different applications, and their associated network traffic, do not usually share the same requirements. This becomes even tougher when we take different users profiles into account. Bandwidth requirements refer to traffic volume/intensity and they will have impact on the configuration of the node mechanisms; they are also important for traffic engineering and/or overall network dimensioning.

The other performance parameters can be directly associated with service categories. Different services exhibit different sensitivities to packet losses, delay and delay variations, from low to medium to high. Some requirements (or performance parameters) are not relevant to some services. The most difficult applications to deal with are those with variable performance requirements. They may lead to either inadequate service or waste of resources.

The degree of symmetry is not considered criteria for class definition, as QoS is in general independently provided on the forward and return links. However, for strongly asymmetric applications (such as broadcasting, VoD, cinema distribution) QoS would make sense only on the forward link. Nevertheless, the degree of asymmetry is considered a factor in network dimensioning on the forward and return links.

To fully understand the different applications requirements and the constraints on bandwidth and delay associated, we will consider the applications behaviour with respect to five characteristics:

- Delay sensibility: Interactive applications are especially sensitive to delay issues, in a scenario like ours, where delay is already high due to the satellite link propagation time (≅270ms), delay plays an important role in the link quality. If the end-to-end delay is too high, an interactive communication is difficult or impossible. Applications including gaming, videoconference, or VoIP are the services directly affected by this issue and therefore are the most restrictive applications.
- Jitter: Jitter is usually tied to delay, in the sense that applications requiring small delays will also require small delay variation or jitter. But not only applications requiring small delays (the ones specified earlier) request small values of jitter, also applications like TV Broadcast or VoD need small delay variation to offer really competitive video. A way to compensate for excessive jitter is to increase the size of the jitter buffer which is responsible for reassembling packet streams. When there is an issue with packets, such as arriving out of sequence or too late, the buffer will try and adjust to compensate or fill in with white comfort noise if necessary. Adjusting the buffer can minimize jitter problems, but it can also introduce other issues such as latency, which can cause conversations to be clipped.
- Packet loss sensibility: Packet loss can be caused by many different reasons. Normally, packet loss starts to be a real problem when the

percentage of lost packets exceeds a certain threshold, or when packet losses are grouped together in large packet bursts. When a packet is does not arrive the receiver correctly and if TCP is being used, retransmission takes place, making delay and jitter greater and forcing a larger use of bandwidth, but assuring that no packet will be lost. That is the reason that makes us set as a constraint no packet loss for applications like email, web-browsing, ftp, p2p and those using TCP.

- Bandwidth: Bandwidth is by far the most common parameter in users mind thanks to the proliferation of bandwidth consuming applications like p2p, streaming or services like iTunes. This forces us to consider bandwidth as the most important requirement for our network. Some of the applications mentioned above would use as much bandwidth available as possible, and maybe the more the user gets, the more they are going to use, and therefore to demand. It is necessary to take into account that allocating a certain amount of bandwidth (higher than the actual needs of the user) will allow the transmission of higher definition videos, larger files, etc.,... driving us to a higher bandwidth consumption.
- Burstiness: A traffic session that tends to swell to use increasing amounts of bandwidth and produce large surges of packets is said to be “bursty.” TCP’s slowstart algorithm creates or exacerbates the traffic tendency to burst. As TCP addresses the sudden demand of a bursting connection, congestion and retransmissions occur. Applications such as P2P, FTP, multimedia components of HTTP traffic, and the graphics portion of HTTP traffic (*.gif, *.jpg) are considered bursty since they generate large amounts of download data.

1.2 IPv6 Network architecture requirements

IPv6 solves the Internet scaling problem, provides a flexible transition mechanism for IPv4 which reduces the risk of architectural problems, and it has been designed to meet the needs of new markets such as nomadic personal computing devices, networked entertainment, and device control.

IPv6 provides a platform for new Internet functionality. This includes support for real-time flows, provider selection, host mobility, end-to-end security, auto-configuration, and auto-reconfiguration. And it is designed to run well on high performance networks and at the same time is still efficient for low bandwidth networks (e.g., wireless). Therefore, the use of IPv6 in SATSIX will solve the problem of the shortage of IPv4 addresses, which are needed by all new machines added to the Internet, adding also many improvements to IPv4 in areas such as routing and network auto configuration.

For IPv6 support by the terminals it is required that the terminal network and air interfaces support IPv6, both the terrestrial and satellite networks can use IPv6 packets. The terminal should also include an IPv4 / IPv6 gateway. The "calling" terminal network interface receives the IPv6 packets, they are translated to IPv4 and sent to the air interface. The "called" terminal receives the IPv4 packets and translates them to IPv6 to send them to the network interface.

- Multicast: Multicast is intended to allow a single device to send datagrams to a group of recipients in the most efficient way and without requiring sending several identical packets to each of the receivers. IPv6 uses a new protocol called Multicast Listener Discovery (MLD), which is embedded in ICMPv6 instead of using a separate protocol. IPv6 multicast supports three service modes, SSM (as in IPv4), ASM (in IPv6, constrained to a single administrative domain) and embedded RP (offering services that would otherwise require MSDP in IPv4).
- Mobility: Mobile Ipv6 is a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. To reduce the amount of signalling required by MIPv6 a new Hierarchical Mobile IPv6 (HMIPv6) protocol was designed by the Internet Engineering Task Force (IETF). It also improves handoff speed for mobile connections. The main

problem of MIPv6 is its inefficient use of resources in the case of local mobility, since it uses the same mechanisms in both global al local cases. HMIPv6, on the other hand, separates local from global mobility and the later one is managed locally.

- Security: IP Security (IPSec) is a mandatory feature in terrestrial IPv6 networks. IPSec offers strong and complete security services. In theory, it can be used in point-to-multipoint scenarios: in such a case, IPSec Security Associations (SA) have to be shared by the source and the concerned receivers. However, the Internet Key Exchange (IKE) protocol, which is always used with IPSec for key exchange and SA establishments, is a point-to-point oriented protocol. It does not allow establishing shared Security Associations between multiple network equipment. SAs have to be configured statically and manually in the source and in each receiver. This is not scalable for large groups.

2 Overall Network Architecture Definitions

The SATSIX system presents an integrated architecture that has been applied to both a transparent star and regenerative mesh topology using a DVB-RCS satellite link. The link layer is provided by the DVB-RCS standard [DVB-RCS], is derived from the highly successful Digital Video Broadcast (DVB) standard for Satellite [DVB-S]. In DVB-RCS, the Forward Link Subsystem (FLS) is provided by DVB-S, and the Return Link Subsystem (RLS) uses Multi-Frequency TDMA. The Time-Division Multiplexed (TDM) FLS is also used to transmit control tables that configure and control the operation of each RCS Terminal (RCST). SATSIX also considers systems that use the DVB-S2 [DVB-S2], a second-generation standard, (designed to replace DVB-S, and recently incorporated into the DVB-RCS specification) as an alternate technology on the FLS, and can employ Dynamic Rate Adaptation for the RLS link. These new waveforms offer higher efficiency for transmission and also introduce more flexibility when designing the network service.

DVB-S utilises the ISO MPEG-2 Transport Stream [MPEG2]. It defines the physical and link layers that together provide a fixed rate simplex transmission of data by fragmenting data into fixed-sized frames (known as TS Packets) [RFC4259]. The most widely deployed method for transmission of IP data over

DVB-S uses the Multiprotocol Encapsulation (MPE) [DVB-D]. An alternative, the Unidirectional Link Encapsulation, ULE [RFC4326], provides a more simple and flexible interface to the IP layer. Both are supported over the SATSIX air interface.

The DVB-S2 standard defines a set of advanced coding and modulation waveforms that offer a significant improvement in efficiency over that provided by DVB-S. S2 specifies two adaptive methods: the pre-provisioned Variable Coding/Modulation (VCM) method and a more sophisticated dynamic method called Adaptive Coding/Modulation (ACM). To take full advantage of the adaptive VCM and ACM methods requires using new methods based on the Continuous Generic Stream. A new Generic Stream Encapsulation (GSE) [DVb-GSE] allows a transmitter to directly transport IP packets without using TS Packets. The interface to IP resembles that offered by ULE. The most significant benefit is the flexibility that it will allow for operators to change the waveform on a frame-by-frame basis. This method is particularly appropriate to the two-way service provided in DVB-RCS systems. In these systems, the reduction in operational cost offered by flexible use of ACM is seen as crucial to successful competition with other satellite and terrestrial Internet services. The remainder of this section describes the architectural components required to design an RCS system that is able to offer QoS and other IP services over the S2 physical layer.

2.1 Network Architecture Overview

The SatSix network architecture is derived from the ETSI Satellite-Independent Service Access Point (SI-SAP) reference model for IP-based satellite systems, and introduces a satellite-independent QoS architecture [BSM]. In this section, the overall reference network architecture is described, and then applied to two specific DVB-RCS topologies, namely transparent star [BSM-TSS] and regenerative mesh [BSM-RSM].

Fig. 1

Figure 1 shows the physical elements of the network reference architecture. These are described below:

- RCST: Return channel satellite terminals act as an interface between the system and external users providing bi-directional services through the satellite network. It can operated in is the interface between DVB-RCS and external users/networks, such as WiFi and WiMAX.
- Satellite: It provides the backhauling link between the RCST and the hub or other RCSTs. This can use either a transparent satellite or one that has OBP capability.
- NCC: Network Control Center provides session control, routing and resource access to the RCSTs and manages the OBP configuration [BSM-RSM] and DVB control tables.
- NMC: This controls the management of all the system elements. The AmerHis NMC is split in two subsystems:
- The Element Manager (EM): It is responsible for the management of the redundant NCC (including NCC-RCST) and of the GWs.
- The Network and Service Manager (NSM): It is responsible for the management of the VSNs, Service Providers, RCSTs, and telecom services and NCC-initiated connections.
- Gateway (GW): This provides the interconnection with terrestrial networks (ISDN/POTS, Internet, and Intranet). The GW is comprises the following subsystems:
    - NMS: Interfaces between ISP/operator and Hub to manage user traffic and service provision. The NMS also performs control and supervision of HUB equipment, the network, and the RCSTs.
    - FLS: Encapsulates IP packets in MPEG-2 frames and transmits these frames on a TDM carrier, base-band modulated. In the RF equipment, the modulated bitstream is upconverted and sent to the antenna, which transmits it up to the satellite at frequencies in the Ku band.
    - RLS: The Gateway antenna receives the downlink signal at Ku band and downconverts it to the 950-1450 MHz IF band. Thereafter, RLS filters the different return channels that compose a superframe, demodulates the signal, decodes the TDMA bursts

form the terminal and extracts and forwards the frames containing the IP packets.

    - Reference and Synchronization Subsystem (REFS). Receives time signals from GPS and provides synchronization and timing for the different Gateway subsystems.

- Access router/Switch: This provides the access point with terrestrial networks.
- WiFi Access point: A wireless access point (AP) is a hardware device that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs extend the physical range of service a wireless user has access to. An AP is identified by the broadcast SSID (Service Set Identifier) and must provide wireless security.
- WiFi user: Terminal or end user who accesses the network through WiFi connection.
- WiMAX BS: A WiMAX base station connects the terrestrial networks to the WiMAX subscriber station.
- WIMAX SS: A WiMAX subscriber station provides service through a wireless connection.

Fig. 2

Figure 2 shows the network architecture for the transparent star topology. The main features are: the satellite does not have OBP and RCSTs can only communicate with the gateway/NCC via the satellite. WLLs are connected to the DVB-RCS via RCSTs.

Fig. 3

Figure 3 shows the network architecture for the regenerative mesh topology. It main features are: the satellite has OBP, and a RCST not only can communicate with the gateway/NCC via the satellite, but also can communicate with other RCSTs.

2.2 Interworking with WLL

2.2.1 Interworking with WiFi

The complexity of a Wi-Fi network depends on the user scenario. For personal use, it can be limited to a Basic Service Set (BSS), i.e. a collection of Wi-Fi end terminals associated to a single Wi-Fi access point (AP). For companies or service providers, it is likely to be an Extended Service Set (ESS), i.e. a collection of access points (with their associated terminal stations) interconnected by means of a distribution system. This latter can be based on a wired technology, typically Ethernet, or on a wireless technology (Wi-Fi or WiMAX). In the former case, the RCTS could simply integrate a Wi-Fi interface configured as an access point or could be connected to an access point by means of an Ethernet link. In the second case, the RCTS is connected to the distributed system by means of a switch/router as shown in Fig. and Fig. . Note that, as with some commercial solutions, the above-cited switch/router can be a wireless switch controller which centrally manages all access points. By so doing, QoS provision, security, mobility is managed by the wireless switch controller and not fully deported in the access points.

Wi-Fi stations (access points and end terminals) should support some QoS functionalities at the Medium Access Control (MAC) Sublayer in order to support SATSIX classes of services. This is the case of many recent Wi-Fi products that are already available on the market and that are labelled with Wi-fi MultiMedia (WMM).

Fig. 4

2.2.2 Interworking with WiMax

The WiMAX base station has two interfaces and is connected to a RCST. It is noted that the WiMAX users (i.e. Subscriber Station) can only communicate with the WiMAX base station, and the WiMAX base station is connected to the DVB-RCS system via a RCST. The backbone of the DVB-RCS system is the IPv6-based Internet. In this way, there is no modification on the DVB-RCS system, and the main modification is on the MAC scheduler of the WiMAX base station. Since the design of WiMAX MAC scheduler is not standardised the IEEE 802.16 and is up to the operators, this approach adds flexibility.

The enhanced functionalities of the MAC scheduler in the WiMAX base station is as follows:

- Map the WiMAX QoS category onto the DVB-RCS SATSIX traffic classes.
- Provide end-to-end IPv6 communications over both DVB-RCS and WiMAX air interface. It includes how to perform segmentation and reassembly of IP packets at the WiMAX base station, which is connected to the satellite terminal, and how to perform address mapping/translation. The end-to-end protocol stacks are also described.
- Contact the DAMA Manager in NCC for admission control.

The negotiation of the SLA is realised through the SIP signalling protocol. By exploiting the Session Description Protocol, the SIP client located in the end user declares the session parameters (user address, type of media, bandwidth) to the stateful proxy SIP present in the satellite terminal. At this point the satellite terminal, which represents the edge router of SATSIX domain, makes classification and marking of the incoming flows according to each associated Per Hop Behaviour. Once the user has sent with the SDP application information about its traffic to the Proxy SIP in the RCST, the DAMA agent can read these parameters directly in the stateful proxy, and on the basis of the traffic is going to enter network, it can forward the requests of resources reservation before the flow start to fill the queue, and monitor continuously the state of the buffers in order to dynamically change the bandwidth requests. Mobility management is another interesting topic in the interworking between DVB-RCS and WiMAX.

Fig. 5

3 Functional architecture definition

Based on the overall network reference architectures, Figure 6 and 7 shows the overall reference functional architectures for transparent star [BSM-TSS] and regenerative mesh [BSM-RSM] topologies, respectively. These functional architectures have integrated QoS, multicast, security, mobility and transport functions.

Fig. 6

The main elements of the functional architectures are:

- This functional architecture not only support end-to-end QoS, but also support dynamic QoS according to applications and users needs. The satellite segment can interwork with Internet QoS DiffServ in order to provide end to end QoS at network level. The terminal model can perform this interworking in terms of signalling and QoS parameters mapping. The involved entities are SIP proxy, QoS agent, QoS server, PEP, IP compression, IP QoS, MAC QoS, RRM, C2P agent and C2P server.
- This functional architecture can provide up-to-date multicast management for both IPv4 and IPv6. The RCSTs should act as an MLDv2 multicast router proxy to forward the MLDv2 messages between listeners and the remote multicast router in the NCC.
- This functional architecture support security at application level such as TLS, SSL, and DTLS, key management protocols such SATIPSec and GSAKMP, key distribution systems like LKH and layer 2 security enhancing security level provided by L3 solutions such as SatIPSec. The Group controller/key Server will be co-located within the NCC and all the key management group members will be co-located within user terminals. All key management messages will flow between the Group controller/Key server/NCC and all the secure data will be between the user terminals in mesh and user terminals and Gateway in a star configuration.

- This functional architecture has enhanced standard IPv6 mobility in a satellite system, with the use of Mobile IPv6. Mobility Anchor Point (MAP) is located in RCSTs and Home Agent (HA) is co-located in gateway. This design can reduce the signalling message during intra-domain movement and handover.
- This functional architecture supports PEP enhancement.

4 Applying the Network architecture

In this section, the proposed network and functional architectures are applied to three different scenarios, namely corporate application scenario, residential application scenario and collective access terminal scenario.

4.1 Corporate application scenario

This type of scenario and architecture can concern a company having distant offices, warehouses, manufactures, subsidiaries or individual workers located in rural or hardly reachable areas by wired backbone.

It composed of different subnetworks belonging to the Headquarters and to “distant offices”. The interconnections among the subnetworks is based on VPN end-to-end. It also includes tunnelling between the distant offices located beyond the satellite access on the local loop and the Headquarters located on the terrestrial backbone.

The scenario covers the following main categories:

- Intranet: provides internal site-to-site or LAN-to-LAN connectivity over public network.
- Internet: provides access to the internet.
- Extranet: allows secured connections with business partners, suppliers and customers of e-commerce. It is an extension of Intranet VPNs completed with firewalls & protections.

In the framework of each category different traffic types are allowed:

- Internet protocols: TCP (ftp, http, …), DCCP (VoIPO, VoD, …), UDP (IPTV, …)

- Control protocol (SIP, H323)
- Applications protocols: Video conferencing,VoIP
- Applications-signalling based on frameworks like SAP or web services

The distant offices do not have direct access to the Internet. Their only entry point is the Headquarters.

The distant offices which are not located in the same spot can however “talk” to each other without passing through the Headquarters, provided they are using their Intranet facilities only.

The network architecture shall be composed by the following elements

- Distant offices: user equipment with wireless capabilities (Wifi or WiMAX), WiFi AP or WiMAX BS, Router/switch, and Firewall with VPN capabilities (if not provided by the router)
- Headquartes: Gateway, Router/switch, Firewall with VPN capabilities, WiMAX BS (optionally also WiFi AP), Content/application servers (es SAP), DHCP server, Proxy server, and Firewall for the access to the Internet

Fig. 8

The protocol architecture takes into account the different types of applications and control protocols at user level; considering the presence of a wireless connection the simplest architecture foresees the interconnection of a Access point in the WiFi case, or a base station, in the WiMAX case, with routing capabilities (so with the presence of the IP layer) in order to implement the interworking strategy, basically classifying the traffic at IP level and creating a mapping between the wifi/WiMAX classes and the SATSIX one.

Fig. 9

4.2 Residential Application Scenario

Nowadays the principal residential application of satellite network is the provision of triple play services. The principle of the ‘Triple Play’ concept is to provide the three basic access services (Television, Internet access and Telephony) through one single satellite communication network. The services considered in this scenario are:

- Digital TV.
- Video broadcasting.
- Interactive television.
- Web Browsing.
- VoIP Telephony & Videoconference.
- P2P applications.

Residential application scenario uses both transparent and regenerative satellite systems.

In order to provide Triple Play, IP connectivity must be used on top of a layer-2 adaptation layer based on DVB Standards. The uplink channel specification has been defined by ETSI in the DVB – Return Channel via Satellite (DVB-RCS) standard, and the downlink channel, also defined by ETSI, is the DVB by Satellite (DVB-S2) standard.

Fig. 10

Television broadcasting, video and audio broadcasting are ideally suited to the broadcast nature of satellite networks and become more cost effective the larger the end user population is, assuming that the same pieces of content need to be delivered to all (or large groups of) end users. Others triple play services as web browsing, VoIP and P2P applications involves a mixture of terrestrial and end users.

The satellite system architecture is compound by:

- On-Board Processor (regenerative system): The OBP combines DVB-RCS and DVB-S standards into a single multi-spot satellite system allowing cross-connectivity between different uplink and downlinks thanks to the signal processing.
- Network Management Center: in charge of the management of all the system elements.
- Network Control Center: controls the network, provides session control, routing and resource access.
- Satellite Terminal: is the interface between the system and external users.
- Gateway: provides interconnection with terrestrial networks.

In order to provide complete Triple play services, some equipment is needed:

- Home Gateway: It interconnects and integrates all kind of products in the home.
- IP Set-Top Box: A set-top box is a device that enables a television set to become a user interface to the IP world.
- Video on Demand Server.
- Streaming Server.
- Video service Provider.
- Television Broadcast centre.

The proposed protocol stack for the residential application scenario is shown in next figure. The proposed protocol stack differs from different services depending upon service need. The presence of wireless technology has been considered in the protocol stack.

Fig. 11

4.3 Collective access terminal scenario

The collective scenario aims to provide a high level of connectivity to citizens and small companies (or distant offices of bigger companies) belonging to rural communities that are not ADSL eligible. This solution is based on hybrid network combining a satellite segment and terrestrial wired as well as wireless access such as WiFi, WiMAX or Ethernet.

It is considered that the final users do not have to take care of the technology used for transmission of the traffic. The connection to satellite on the WLL side is single for the whole community that shares the satellite segment.

So the collective scenario is represented by all these public places in which any kind of people can access to the service without any specific requirements but only with a subscription that allows access to the broadband wireless network and applications.

Examples of this scenario are: Hotel, public places, mountain hut, islands harbours, emergency istuations (war or natural disasters).

Three types of interconnections may be provided on the local loop and may be used simultaneously:

- Wired access: the Return Channel Satellite Terminal (RCST) interfaces with Ethernet wiring providing access in a building.
- WiFi: the RCST interfaces with WiFi Access Point, which spreads and collects the traffic over the local area. The PCs are equipped with WiFi cards that allow them to move within or at a short distance from the premises.
- WiMAX: the RCST interfaces with a WiMAX Access Point, which spreads or collects the traffic over the local area. This may concern users close to the AP that are equipped with WiMAX cards, as well as users far from the AP, depending on the legally allowed transmission power. WiMAX may also be used a backhaul for WiFi, where a 802.11 network is connected to the 802.16 Subscriber Station (SS). These solutions can be put in place for quite big local areas, as dock for instance.

In this type of scenario, the link between the RCST and the Satellite Access Provider's Gateway is seen as a LAN. The local loop can be seen as a sub-LAN. All the traffic passing over the satellite must pass through the Satellite Access Provider's Gateway. This means that no direct Internet flow is possible between two RCSTs connected to a local loop.

The baseline network is composed mainly by the following elements:

- User equipment with wireless capabilities (Wifi or WiMAX)
- Hot spots composed by Wifi access point (switch) with WPA capabilities as minimum or WiMAX BS
- Satellite access subnetwork: Router (to the RCST) with embedded firewall, and RCST
- Service provider: Satellite HUB/Gateway, and Router (to external internet network) with embedded Firewall

Fig. 12

Fig. 13

The protocol architecture takes into account the different types of applications and control protocols at user level; as in the case of the Corporate scenario, considering the presence of a wireless connection, the simplest architecture foresees the interconnection of a Access point in the WiFi case, or a base station, in the WiMAX case, with routing capabilities (so with the presence of the IP layer) in order to implement the interworking strategy, basically classifying the traffic at IP level and creating a mapping between the wifi/WiMAX classes and the SATSIX one.

5 Conclusions

The SATSIX system presents an integrated architecture that has been applied to both a transparent star and regenerative mesh topology using a DVB-RCS satellite link. This paper focuses on the requirements and design constraints that were faced in the design of the network-layer of the SATSIX system. The reference functional architecture integrates QoS, multicast, security, and mobility functions to support a range of transport requirements. Issues impacting integration of wireless local loop and network-layer QoS have been highlighted and solutions have been briefly outlined. Three network architectures have been identified that use this reference network architecture to support three different scenarios, namely corporate application scenario, residential application scenario and collective access terminal scenario. In each case the related protocol stacks are presented.

Acknowledgement

This work is supported by the IST FP6 SATSIX project, funded by European Commission (EC). The financial contribution of the EC towards this project is greatly appreciated.

References

[DVB-S] EN 301 421,"DVB Modulation and Coding for DBS satellite systems at 11/12 GHz", ETSI.

[DVB-RCS] EN 301 790, "DVB Interaction channel for satellite distribution systems", ETSI.

[RFC4259] Montpetit, M.-J., Fairhurst, G., Clausen, H.,Collini-Nocker, B., and H. Linder, "A Framework for Transmission of IP Datagrams over MPEG-2 Networks", RFC 4259, 2005.

[DVB-D] ETSI/EN 301 192, "DVB Specifications for Data Broadcasting", European Telecommunications Standards Institute, 1999.

[RFC4326] Fairhurst, G. and B. Collini-Nocker, "Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)", IETF RFC 4326, 2005.

[DVB-S2] EN 302 207, "Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services,News Gathering and Other Broadband Satellite Applications", [MPEG2] ETSI.ISO/IEC 13818-1, "Generic Coding of Moving Pictures and Associated Audio Information Systems”.

[DVB-GSE] “Digital Video Broadcasting (DVB); Generic Stream Encapsulation (GSE) Protocol For Interactive and Professional Applications”, ETSI Work in Progress, 2007.
[BSM] TS 102 462, “Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) Services and Architectures: QoS Functional Architecture”, ETSI.
[BSM-TSS] TS 102 352, “Broadband Satellite Multimedia (BSM); Transparent Satellite Star - A (TSS-A); DVB-S/DVB-RCS for transparent satellites”, ETSI, 2005
[BSM-RSM] “Broadband Satellite Multimedia (BSM); Regenerative Satellite Mesh B (RSM-B); Profile of DVB-RCS and DVB-S Standards”, ETSI, 2006.

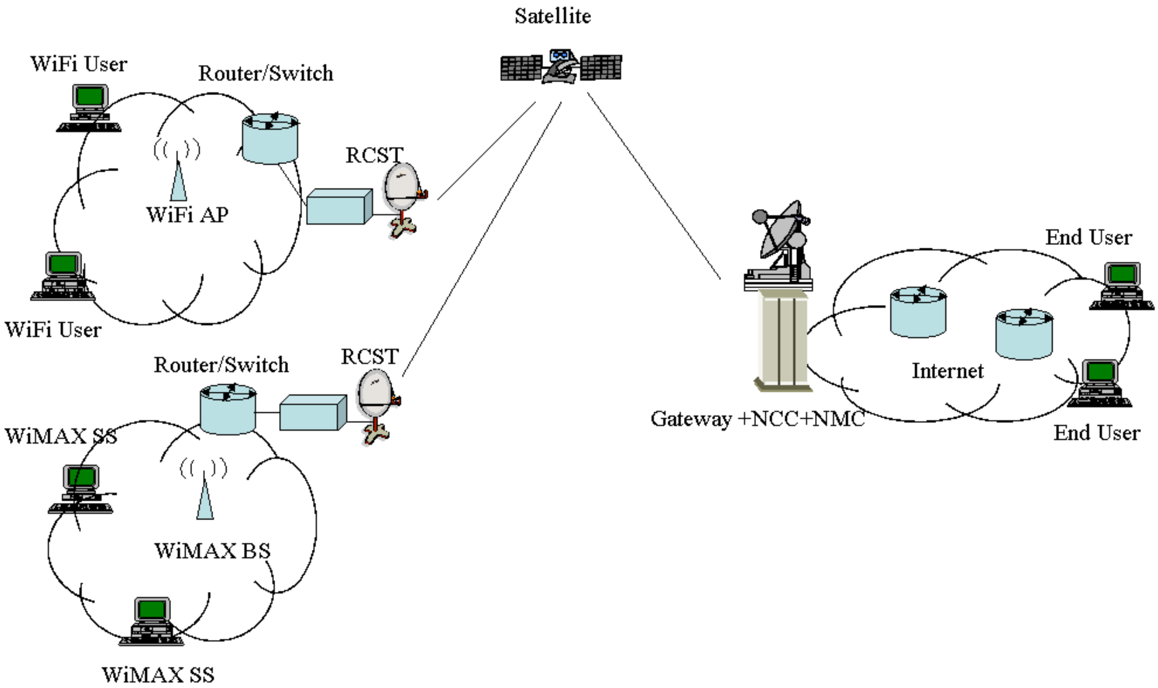

Fig. 1 Reference Network Architecture

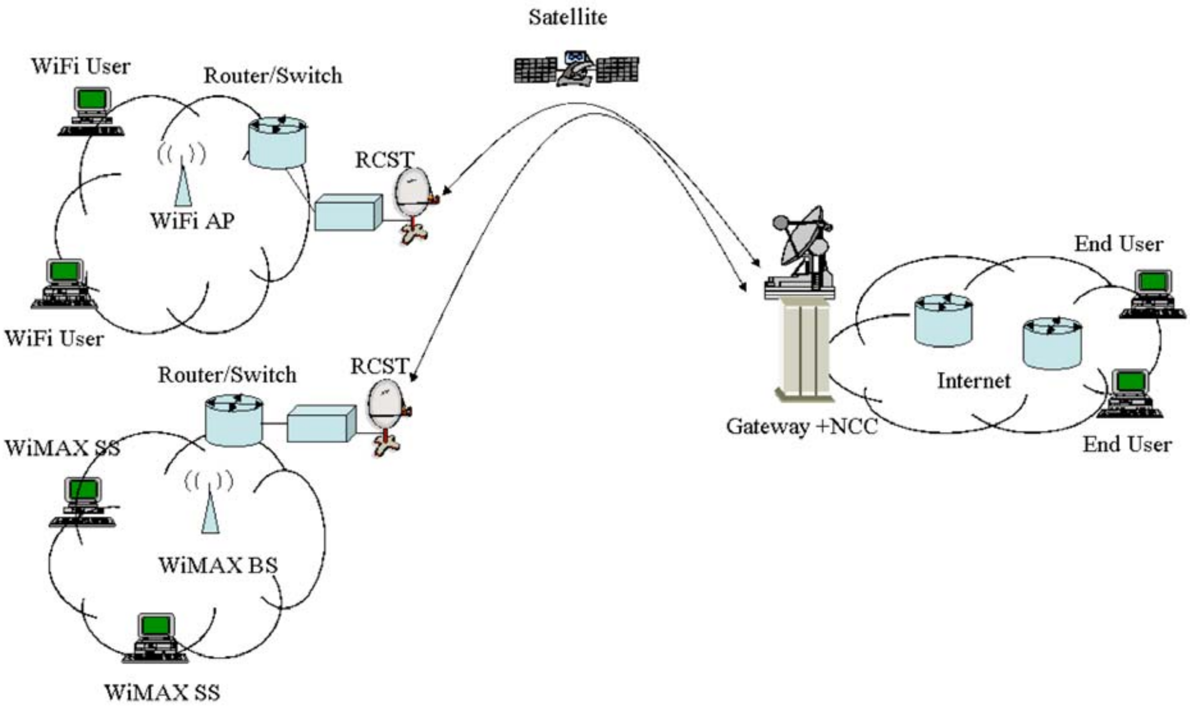

Fig. 2 Network Architecture for the Transparent Star Topology

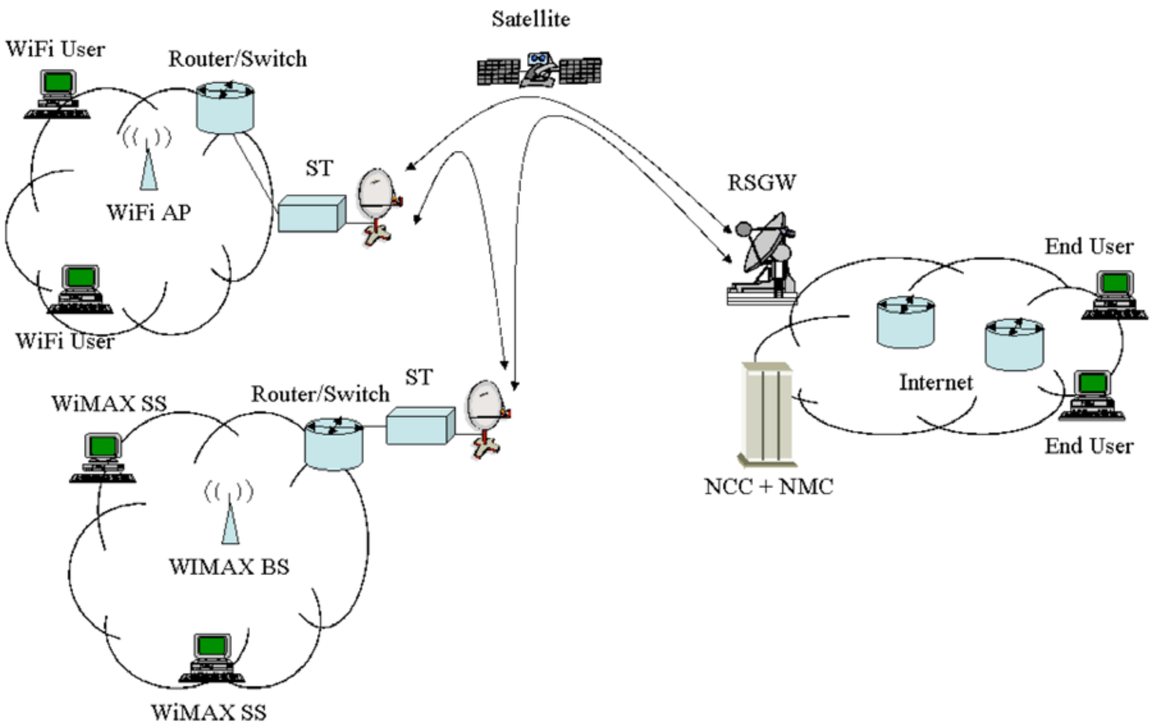

Fig. 3 Network architecture for the Regenerative Mesh Topology

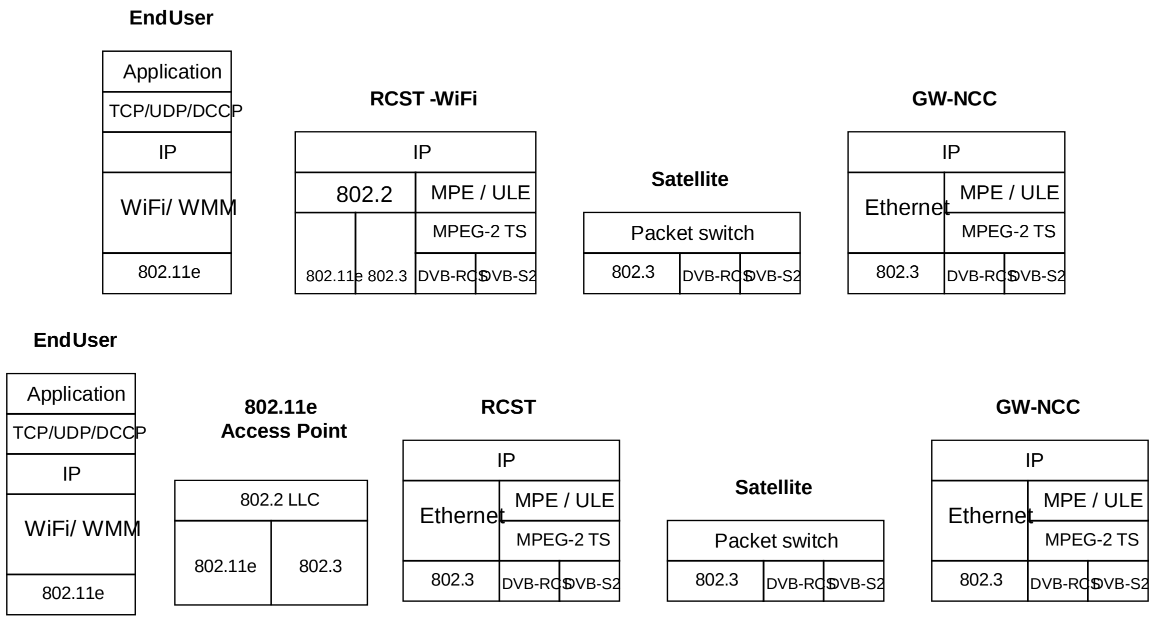

Fig. 4 Protocol stack of Interworking between DVB-RCS and WiFi or WMM

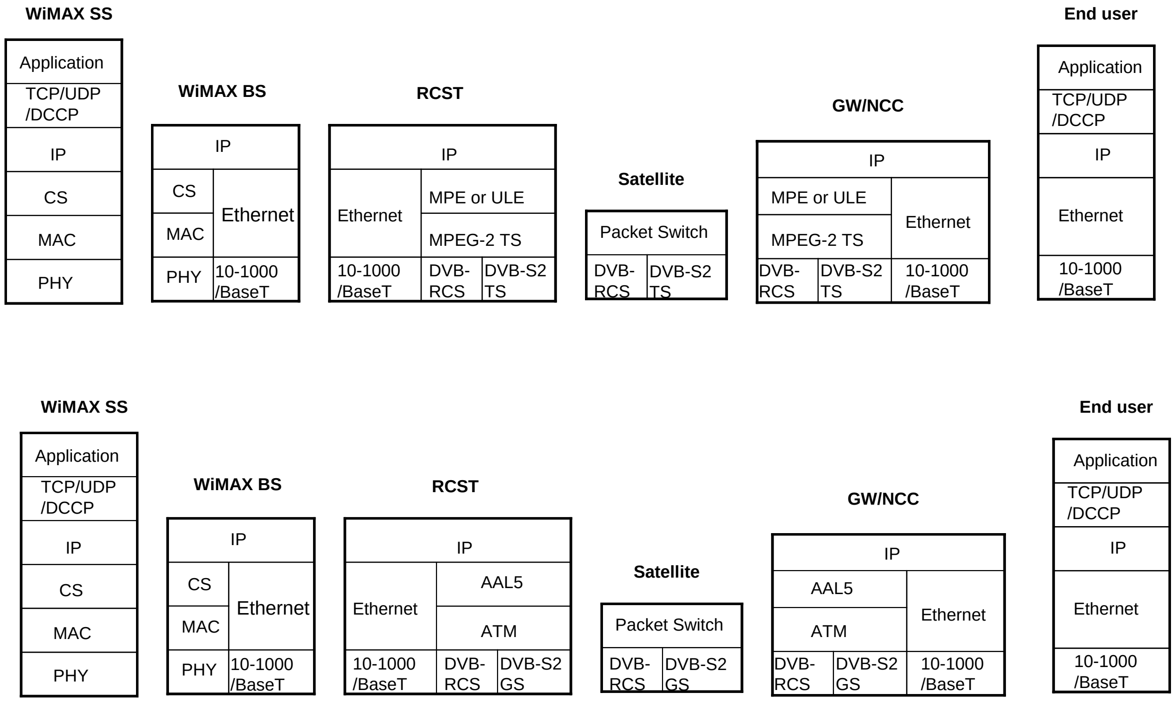

Fig. 5 Protocol stack of Interworking between DVB-RCS and WiMAX

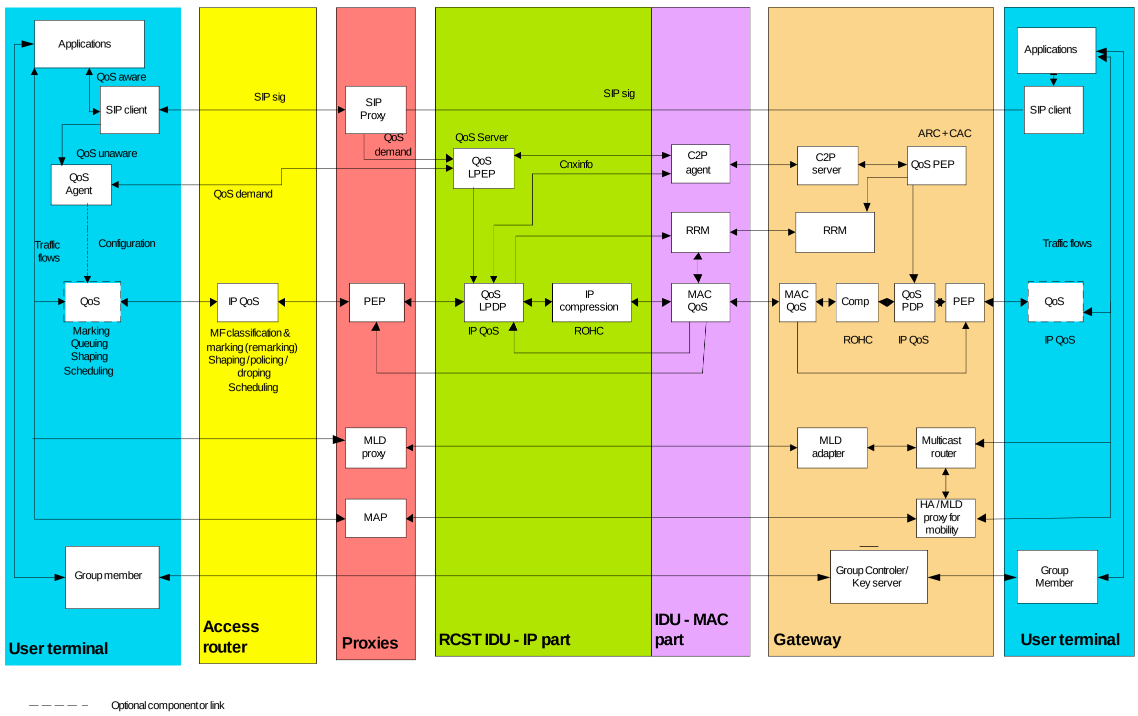

Fig. 6 SATSIX overall reference functional architecture for the Transparent Star Topology

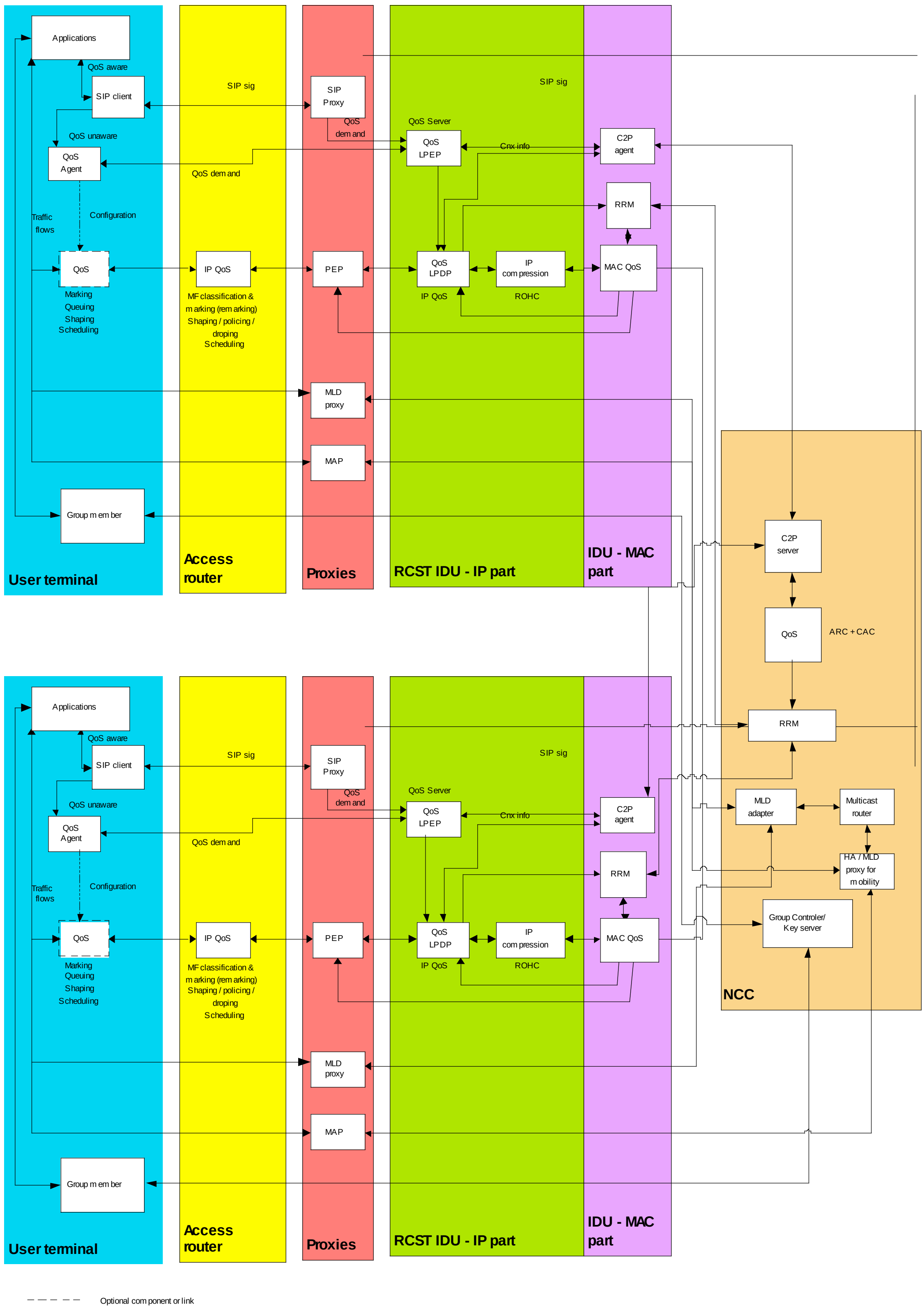

Fig. 7 SATSIX reference functional architecture for the Regenerative Mesh Topology

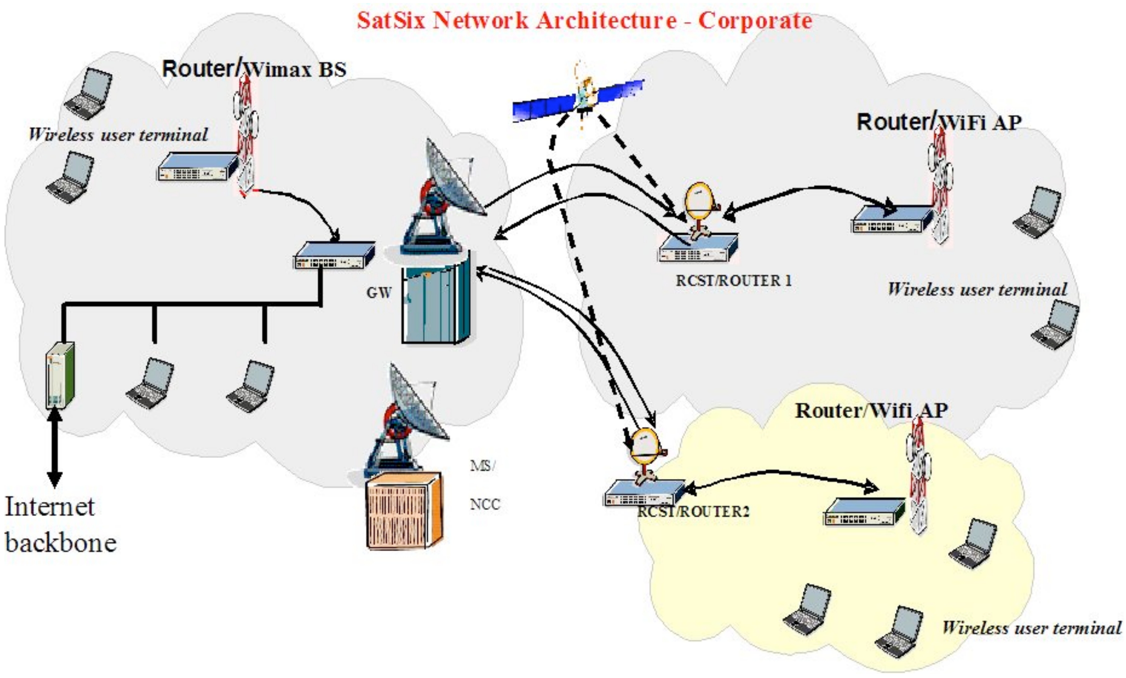

Fig. 8 Corporate Application Network Architecture

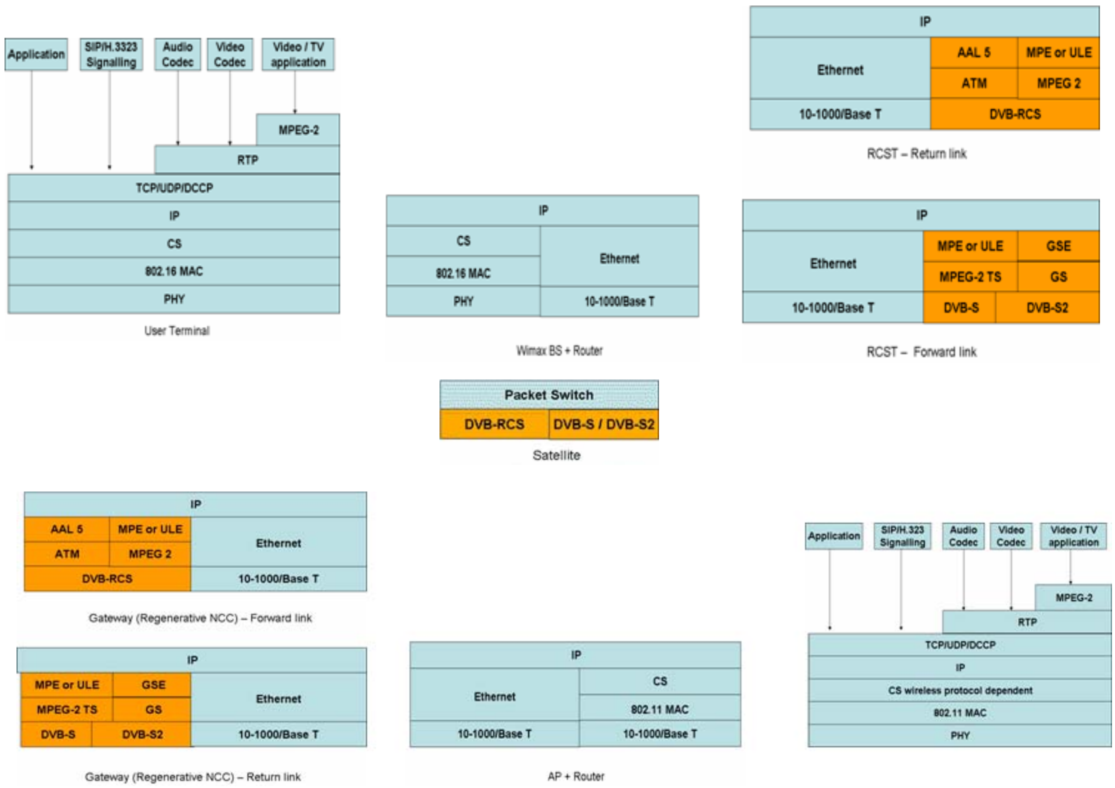

Fig. 9 Corporate application Protocol stack (Regenerative payload)

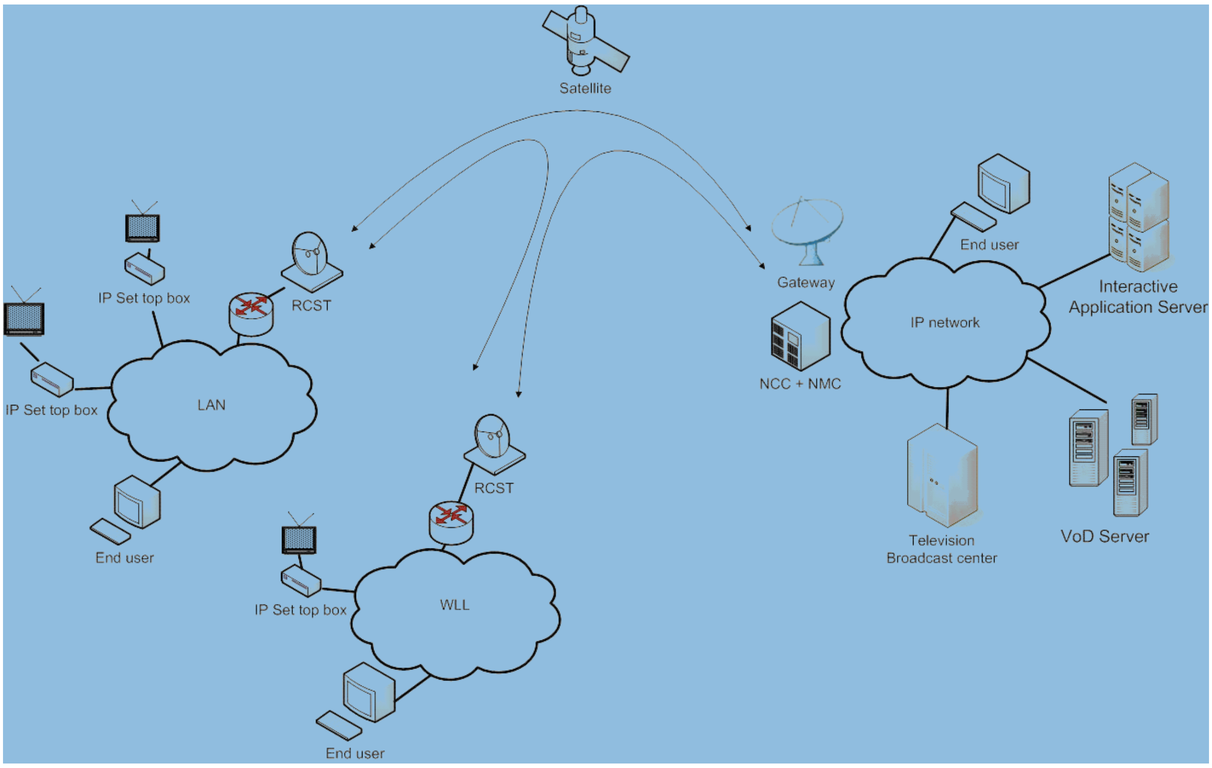

Fig. 10 Residential Application Network Architecture

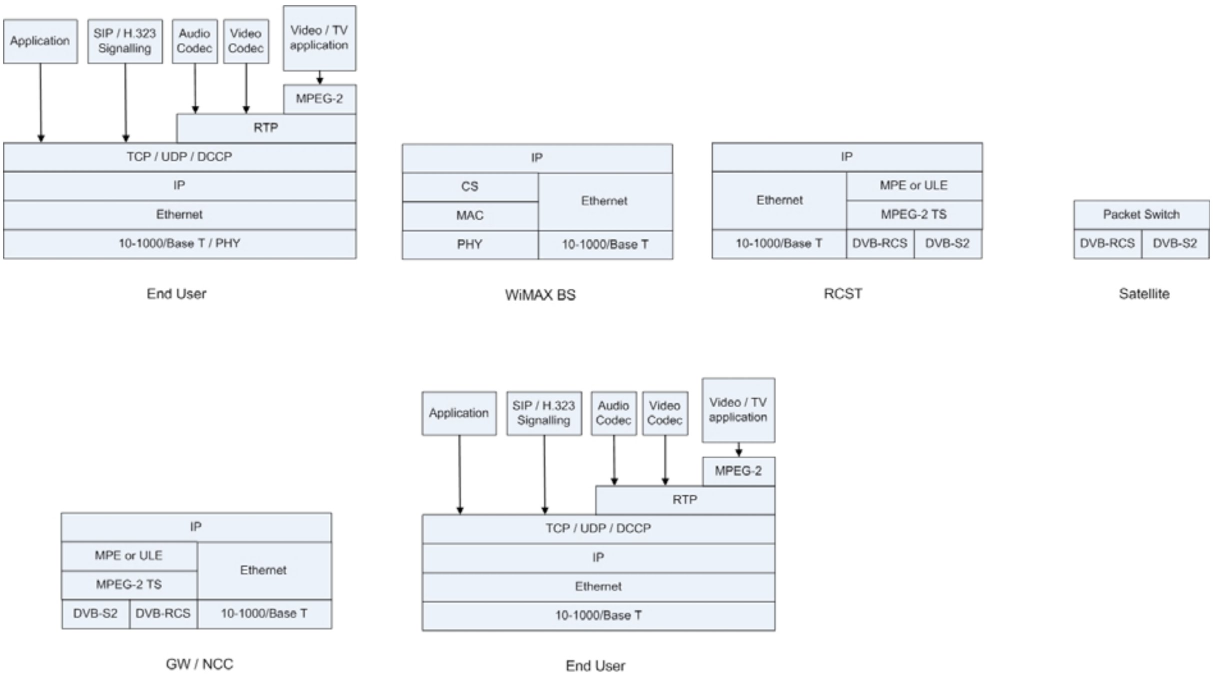

Fig. 11 Residential application Protocol stack

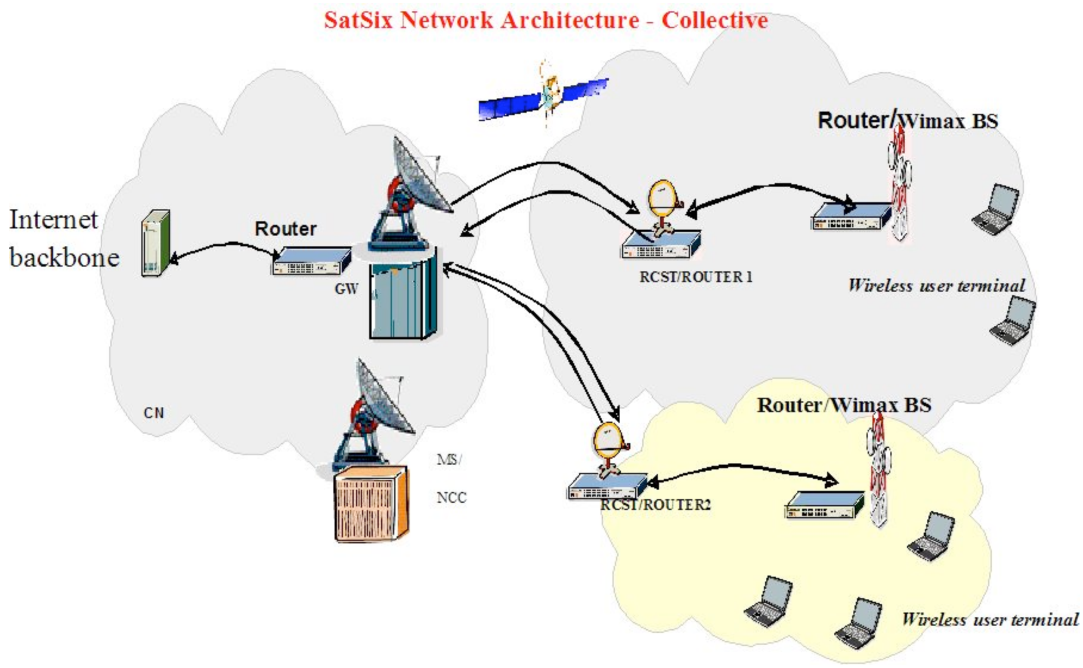

Fig. 12 Collective Access Scenario Network Architecture

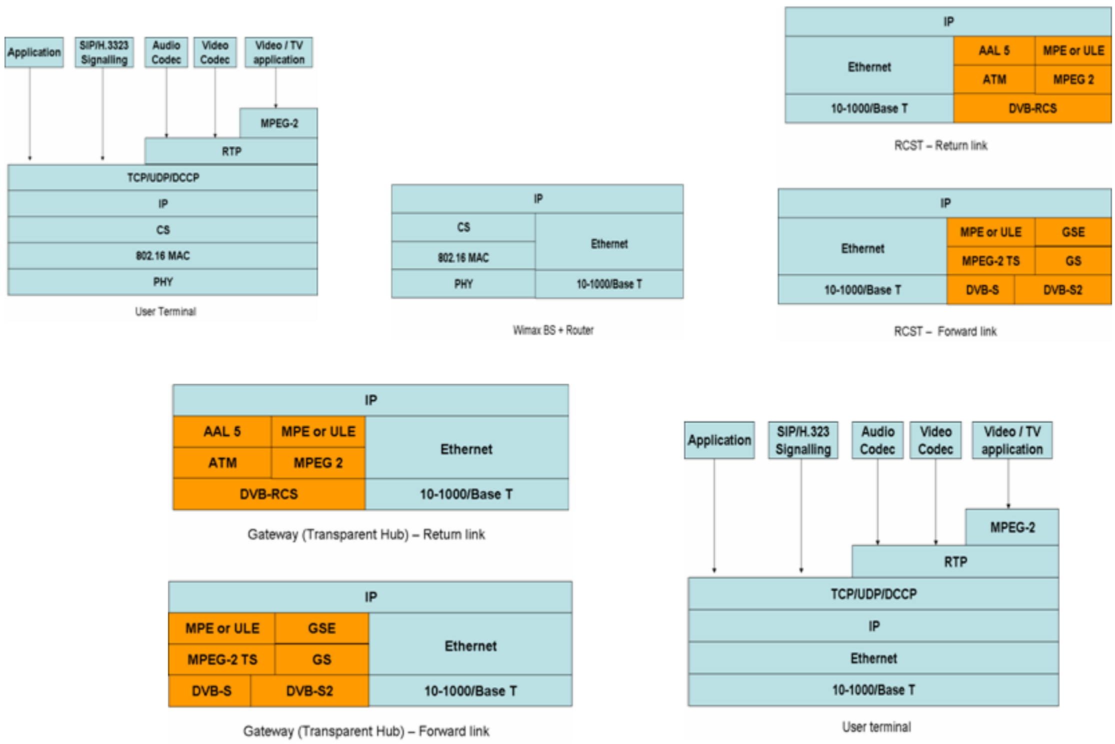

Fig. 13 collective access scenario Protocol stack (Transparent payload)