Signalling Extensions for QoS Support in a IEEE 802.16d/e Domain

Fausto Andreotti\(^1\), Nicola Ciulli\(^2\), Marilia Curado\(^3\), Giada Landi\(^2\), Cristina Nardini\(^4\)

\(^1\) Italtel (IT)  
\(^2\) Consorzio Pisa Ricerche (IT)  
\(^3\) University of Coimbra (PT)  
\(^4\) University of Rome “La Sapienza” (IT)

Abstract: - The IEEE 802.16 standard (WiMAX) provides a specification for fixed and mobile broadband wireless access system, offering high data rate transmission of multimedia services with different Quality-of-Service (QoS) requirements through the air interface. The WiMAX Forum, going beyond the air interface, has defined an end-to-end WiMAX network architecture, based on an all-IP platform. This paper focuses on the signalling needed in a WiMAX domain to support Session Initiation Protocol (SIP) applications with particular QoS requirements. The choice to use SIP-based applications is due to the fact that this protocol is the de-facto standard in NGN architecture, like the IP Multimedia Subsystem (IMS) proposed by the 3GPP2 consortium. Our studies aim at integrating the IMS vision (SIP-based) with the emerging IEEE 802.16 standards in order to guarantee end-to-end QoS for multimedia applications. Besides SIP at the application layer, other lower-layer protocols shall be considered in order to provide a complete end-to-end QoS support. The Next Step In Signalling (NSIS) protocol suite is used to reserve resources in the access and core wired segments. NSIS was chosen due to its usability and adaptability to multi-domain and QoS contexts. In detail, the integration among SIP signalling, resource allocation in the WiMAX wireless link and NSIS signalling is investigated. Results presented in this paper are the summary of the work performed within the framework of the European IST project WEIRD (WiMAX Extension to Isolated Research Data networks).

Key-Words: - SIP, NSIS, QoS, WiMAX

1 Introduction

IEEE 802.16 WirelessMAN supports multiple types of communications services, like data, voice and video, with different QoS requirements; it provides high data rate, large coverage and, in the e-version also mobility. The objective of WEIRD project is to develop an End-to-End architecture WiMAX compliant with the WiMAX Forum architecture and able to support SIP application with QoS requirements. To achieve this purpose is necessary a complete integration between the signalling mechanisms at application level and the signalling mechanisms at control plane level. The control plane signalling allows resource allocation in the WiMAX segment and the request for resource reservation in the wired segment of core network. The signalling protocol used is the IETF Next Steps In Signalling (NSIS) [1], for its usability and adaptability to multi-domain contexts and the possibility to support end-to-end, end-to-edge and edge-to-edge reservations. The concepts presented in this paper address the solutions to provide a scalable end-to-end QoS architecture, more specifically with integrated signalling, linked with a real time monitoring sub-system, and with support of multimedia and SIP applications, multicast and broadcast services. The applications adopted are those that use the IETF protocols and the IP Multimedia Subsystem (IMS) model for service provisioning being developed by 3GPP [2].

The remaining part of this paper is organized as follows. The state of the art in networks based on IEEE802.16d is described in section 2, a general overview of the standards with focus on QoS support and on the architecture proposed are also given in such section. The innovative proposed solution, implemented in the WEIRD project, with its protocols extensions and architectural issues is described in section 3. Signalling scenarios used to validate the work described in the previous section are described in section 4. The conclusions are given in section 6.

2 State of the art

Standards for Broadband Wireless Access (BWA) are being developed within the IEEE Project, working group 16. The IEEE Std 802.16-2004 [3] d-version, specifies the air interface of fixed BWA systems supporting multiple services and includes Medium Access Control (MAC) and multiple physical layer (PHY) specification. The MAC supports a primarily point-to-multipoint architecture, with an optionally mesh topology. The IEEE Std 802.16-2005 [4] e-version, allows mobile subscriber stations. These standards offer different level of QoS, specifying a variety of scheduling classes in order to support different kinds of applications. In particular, the 802.16d/e QoS framework is based on a connection-oriented (CO) approach: each packet transmitted over the air interface belongs to a Service Flow (SF) that defines the transmission ordering, scheduling and some QoS parameters, like throughput, jitter and latency. The 802.16d standard scheduling services are:
• **Unsolicited Grant Service (UGS)** - for real time uplink SFs with fixed size data packets on a periodic basis, such as VoIP without silence suppression and T1/E1 emulation.

• **Real-Time Polling Service (rtPS)** - real time uplink service flows with variable size data packets on a periodic basis such as MPEG video.

• **Non-Real-Time Polling Service (nrtPS)** - supports delay-tolerant data streams with variable sized data packets for which a minimum data rate is required, such as FTP.

• **Best Effort (BE)** - supports data stream for which no minimum service level is required.

The 802.16e standard provides additionally Extended Real Time Polling Service (ErtPS) in which the BS provides unicast grants in an unsolicited manner like in UGS, but where allocations are dynamic. These service flows can be created, changed or deleted through the exchange of different MAC messages: Dynamic Service Addition (DSA), Dynamic Service Change (DSC) and Dynamic Service Deletion (DSD). The standard defines two models to activate service flows: a SF is directly activated using the single-phase model, while it is first admitted and then activated using the two-phase model. In WEIRD system the two-phase activation model is adopted, because it is suitable for real-time applications that require a first signalling phase to establish the session, like SIP applications.

The WiMAX Forum [5] is working to facilitate the deployment of broadband wireless networks based on the IEEE802.16 and ETSI HiperMAN standards by ensuring the compatibility and interoperability of broadband wireless equipment. In order to support the integration of the WiMAX segment in an end-to-end scenario, the WiMAX Forum has defined a Network Reference Model (NRM) that describes a logical representation of the network architecture. The NRM, shown in Figure 1, identifies functional entities and normative reference points (RP) over which interoperability is achieved between functional entities. The NRM consists of Mobile Stations (MS), Access Service Network (ASN), and Connectivity Service Network (CSN). The ASN provides radio access to WiMAX subscribers. It consists of Base Stations (BS) and one or more ASN Gateways (ASN-GW). The BS embodies a full instance of the WiMAX MAC and PHY in compliance with the IEEE 802.16. The ASN Gateway represents an aggregation of control plane functional entities. The IP connectivity services to the WiMAX subscribers are guaranteed by CSN, a network infrastructure having a set of network functions.

The WiMAX Forum defines groups of functions that can be realized by each entity, but the distribution of these functionalities in the physical devices is not detailed. This choice depends on the system to develop. The WEIRD system provides specific support for SIP applications with QoS requirements, through the introduction of a SIP Proxy in the CSN and the development of mechanisms for the direct interaction between the SIP Proxy and the ASN-GW. This interface is used to signal the required QoS parameters, request the resource allocation in the WiMAX segment through the ASN-GW and trigger the NSIS signalling towards the CSN and the core network.

![Fig. 1 - WiMAX Forum Network Reference Model](image1)

### 3 WEIRD Solutions for SIP applications in WiMAX

The WEIRD system is designed in order to provide end-to-end QoS guarantees to a large set of applications for WiMAX relevant scenarios: legacy applications, without QoS signalling capabilities, and applications with signalling capabilities based on different protocols. This section describes a new architectural solution, designed within the WEIRD project [6], aimed at providing end-to-end Quality of Service (QoS) guarantee for SIP applications in WiMAX access networks.

The WEIRD infrastructure, depicted in Figure 2, includes three main entities: Customer Premises Equipment (CPE), Access Service Network (ASN) and Connectivity Service Network (CSN).

![Fig. 2 WEIRD infrastructure for SIP support](image2)
The CPE may be composed by IEEE802.16 single user or multiple users SSs. An ASN may control and aggregate several BSs, based on a wireline or wireless IP infrastructure which is linked through an ASN Gateway (ASN-GW) to the CSN. The ASN-GW plays here both the role of gateway and of control entity for ASN. In a mobile environment the CSN may be either the Home or Visited CSN. Connectivity with other networks may be realized via an IP backbone.

The Connectivity Service Controller (CSC) located on the ASN-GW (CSC ASN) acts as the main coordination point for dynamic resource allocation, admission control, and QoS authorization. It receives requests for resource reservation from the SIP-Proxy located in the CSN and coordinates the creation of the Service Flows (SFs) in the wireless link, the resource allocation in the wired ASN segment and the signalling towards the CSC located on the CSN (CSC CSN) and the core network. The interactions between the CSCs located on the different entities of the WEIRD architecture (i.e. ASN-GW and CSN) are based on the IETF NSIS protocol.

2.1 Objectives

The WEIRD architecture is responsible of QoS control in WiMAX and ASN segments only, i.e. it reserves resources in the access network, including the WiMAX channel and coordinates the QoS signalling towards the CSN and the core network without considering the actual resource reservation in these parts. The resource allocation is done on the following segments: SS – BS and BS – (ASN-GW). The resource control and allocation in the (ASN-GW) – CSN and CSN – far-end segments is outside the WEIRD scope. In fact, WEIRD may consider CSNs in order to have complete picture of the end-to-end chain and the end-to-end signalling, but it will not innovate in the CSN resource allocation area assuming that the QoS is controlled via appropriate technologies.

Starting from the Network Reference Model proposed by WiMAX Forum, in which a logical representation of the network architecture is designed, new software modules should be introduced in the Application Service and Control Plane: the target is to guarantee end-to-end QoS to data flows crossing a WiMAX access network for SIP-based applications. Dedicated blocks have been included in the CSN, namely a SIP-Proxy and an AAA server, together with other functions necessary for domain name resolution and IP address allocations (DNS, DHCP).

The AAA server is used to store user credentials and profiles and it will provide security at three different levels:

- network level - only authorized devices can use the WiMAX access channel, preventing unauthorized wireless devices to enter the network by connecting the BS;
- application level - only authorized customers can activate applications and then use signalling for it;
- service level - only authorized users can use network resources and then activate available services.

AAA may include mechanisms for secure exchange and distribution of authentication credentials and session keys for data encryption.

An enhanced SIP-Proxy supports both application and resource control signalling in a similar way as the x-CSCF in NGN architectures thus giving to WEIRD an IMS compliance (IMS-WiMAX).

An important issue is related to the triggering of service flows (SFs) in a WiMAX network. According to the relevant standards, ASN-initiated creation, modification and deletion of service flows must be supported, while an MS may, but is not required to, have this capability. For SIP-based applications, like peer-to-peer VoIP and videocommunication, it is used a network triggered and network initiated service flow creation approach, i.e. the triggering from the ASN side is operated by a suitable Application Function (AF) module included in the SIP-Proxy. This module communicates with the Connectivity Service Controller inside the ASN-GW through an appropriate interface (ETSI/TISPAN Gq’-like [7]) based on Diameter protocol, providing information about the codecs (for QoS parameters, i.e. bandwidth) and the destination IP address and ports (for subconvergence layer classifiers).

Several commands (AAR/AAA and STR/STA) have been implemented in order to support establishment, modification and deletion of sessions through this interface. Moreover, resource control triggering from the ASN-GW side implies the cooperation with resource reservation protocols, like the IETF Next Step In Signalling (NSIS) protocol, in order to propagate the QoS requirements along the end-to-end path. The use of NSIS on the different entities of the WEIRD architecture will be described in a dedicated paragraph.

2.2 Integration of the SIP architecture with the WiMAX e2e architecture

The proposed framework has the capability to support different end-to-end signalling scenarios, like intra-domain and inter-domain SIP communication. In any case, a SIP-Proxy will be used in each CSN domain, in order to manage application layer signalling. In addition, the proxy can use different modes of interaction with the resource control (i.e. the Service Controller in the ASN-GW), according to the network topology and the adopted QoS model.

Before SIP services are deployed on the system, there is a need for authentication, authorization and accounting of SIP sessions [8]. It is typically more convenient for SIP entities to communicate with an AAA server than to attempt to store user credentials and profiles locally. For this purpose, a Diameter SIP application [9] has been specifically designed including a client co-located with the SIP-Proxy, with the ability to request the authentication of users and
authorization of SIP resources usage from a Diameter server. The most basic level of security, required to be implemented by all SIP clients and SIP-Proxy servers, is Message Digest (MD5) authentication [10]. The SIP-Proxy interacts with the AAA server via an appropriate interface (ETSI/TISPAN Cx/Dx-like [11]) using Diameter messages (MAR/MAA) for authentication and authorization of users during the SIP registration and session setup. It also records accounting information in each SIP session.

In the process of QoS provisioning the call session layer cooperates with resource control layer in order to reserve and commit resources for a call. The MS client communicates with the SIP-Proxy for initiating a session: after user authentication, the SIP-Proxy uses the Gq-like inter face for transmission of the service description information (SDI) to the rest of the WEIRD control plane entities. The QoS information is extracted by the AF located in the SIP-Proxy, then a resource reservation request is made toward the control plane on behalf of the application. The outcome of this process is the reservation of network resources (i.e. WiMAX SFs) for the current SIP session. Suitable protocol extensions (SIP/SDP) could be adopted in order to support QoS provisioning, as it will be shown in the next paragraph. Moreover, the same interface could be used to get informed of events occurred in the network, thus making aware the SIP application layer by event subscription/notification procedures [12].

2.3 QoS Model for SIP Applications

This section presents the models that can be used for providing QoS to SIP-based applications. The WEIRD architecture should allow different levels of QoS to high level services and applications by using the classes of service supported by IEEE 802.16 (i.e. UGS, r-t-PS, er-t-PS, nrt-PS and BE).

Regarding SIP applications, it is generally easy to extract the necessary SDI information from the SDP payloads [13] exchanged during session setup [14], and then to define the mapping to the WiMAX service class (UGS, etc). In any case, a default value can be assigned for providing at least BE quality. The SIP-Proxy is able to understand the QoS requirements for both legacy and customizable applications, and operates in a suitable way toward the resource control. The WEIRD architecture aims to support two different QoS models: QoS assured and QoS enabled.

In both cases, the reservation process is driven by a SIP-Proxy, leaving the SIP endpoints (UAs) to participate in the precondition verification mechanism (if used). Table 1 gives a very simplified overview of the above mentioned QoS models.

In a QoS enabled model, the availability of QoS resources does not affect the success of a call, it only affects the effective level of QoS associated to the call. Thus, call setup and resource reservation are decoupled and may proceed concurrently: in case of resource reservation failure, the caller could be notified and given the option of continuing the call with BE quality.

According to the QoS assured model, a call can be established only if the required QoS can be set; in other words the QoS setup becomes a precondition for calls. In SIP-based applications, QoS preconditions are media stream specific, therefore they can be specified in SDP messages as attributes of the media. In the following, two sub-cases are considered, i.e. preconditions required and preconditions not required.

Preconditions required - preconditions are a set of rules used for coordinating the session signalling and the establishment of end-to-end resource reservations. A precondition is a condition that must be verified by one or more entities: the progress of the signalling in the session can be made dependent on the success of this condition, i.e. the session establishment is suspended until required resources have been allocated to that session.

It is worth noting that, although the SIP endpoints are required to participate in the precondition verification mechanism, they are not involved in the QoS reservation procedure. This approach requires the SIP endpoints to support some protocol extensions (15, 16 and 17) which imply modifications of the client application.

No preconditions required - in WEIRD this hybrid approach is proposed, in which a QoS assured model is assumed with no need of preconditions, thus making it possible to deploy SIP legacy equipment. This is a two phase method, which is compatible with the service flow admission and activation phases used in WiMAX standard. In real deployments this solution usage depends on the 802.16 hardware capability to accept this two-phases scheme for SF management and control.

In the first phase the calling proxy extracts the QoS parameters from the SDP payload and requests resource reservation for the worst-case (e.g. max bandwidth). In the second phase, when the session setup is nearly completed (all parameters are known), the proxy issues a new command, thus activating the service flows with the correct parameters (including IP port numbers).

Table 1 – WEIRD QoS Model for SIP Applications

<table>
<thead>
<tr>
<th>Enabled QoS model</th>
<th>Preconditions</th>
<th>Assured QoS model</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP request (INVITE)</td>
<td>Trigger SF activation</td>
<td>Suspend SIP session</td>
</tr>
<tr>
<td>SIP response (200 OK)</td>
<td>Suspend SIP session</td>
<td>Trigger SF activation</td>
</tr>
<tr>
<td>SIP request (INVITE)</td>
<td>Trigger SF activation</td>
<td>Resume SIP session</td>
</tr>
<tr>
<td>SIP response (200 OK)</td>
<td>Resume SIP session</td>
<td>Trigger SF activation</td>
</tr>
</tbody>
</table>

According to the QoS assured model, a call can be established only if the required QoS can be set; in other words the QoS setup becomes a precondition for calls. In SIP-based applications, QoS preconditions are media stream specific, therefore they can be specified in SDP messages as attributes of the media. In the following, two sub-cases are considered, i.e. preconditions required and preconditions not required.

Preconditions required - preconditions are a set of rules used for coordinating the session signalling and the establishment of end-to-end resource reservations. A precondition is a condition that must be verified by one or more entities: the progress of the signalling in the session can be made dependent on the success of this condition, i.e. the session establishment is suspended until required resources have been allocated to that session.

It is worth noting that, although the SIP endpoints are required to participate in the precondition verification mechanism, they are not involved in the QoS reservation procedure. This approach requires the SIP endpoints to support some protocol extensions (15, 16 and 17) which imply modifications of the client application.

No preconditions required - in WEIRD this hybrid approach is proposed, in which a QoS assured model is assumed with no need of preconditions, thus making it possible to deploy SIP legacy equipment. This is a two phase method, which is compatible with the service flow admission and activation phases used in WiMAX standard. In real deployments this solution usage depends on the 802.16 hardware capability to accept this two-phases scheme for SF management and control.

In the first phase the calling proxy extracts the QoS parameters from the SDP payload and requests resource reservation for the worst-case (e.g. max bandwidth). In the second phase, when the session setup is nearly completed (all parameters are known), the proxy issues a new command, thus activating the service flows with the correct parameters (including IP port numbers).
Using this method, the session is setup with the desired degree of QoS, but it could be aborted if the preliminary worstcase requirement (which is sometimes unnecessary) is not met.

An alternative method could be to admit the service flows with an initial request for BE quality and then adjust the QoS parameters upon activation. In this case, the session is always setup with at least BE quality.

2.4 Resource Control Signalling

Next Steps In Signalling (NSIS) is a signalling framework being developed by the IETF in the context of the NSIS Working Group, with the objective of installing and maintaining flow state in the network. By using a two-layer signalling architecture, signalling transport is separated from signalling applications, which makes easier the development of several applications, including quality of service signalling. With NSIS it is possible to perform perflow signalling as well as flow aggregates signalling, based, for instance, on the Differentiated Services Code Point (DSCP) field.

NSIS is being developed as a two-layer modular approach, comprising an NSIS transport layer and an NSIS signalling layer. The NSIS transport layer protocol, known as General Internet Signalling Transport (GIST), is responsible for the transport of signalling messages between network entities. The signalling layer contains specific functionality of signalling applications and may comprise several NSIS signalling layer protocols (NSLP). With this two-layer scheme, the same signalling transport protocol is used for the support of all signalling applications. Examples of signalling protocols are the QoS-NSLP [18] and the Network Address Translation (NAT)/Firewall-NSLP [19].

In a communication system which aims at providing QoS, as well as to provide security capabilities and mobility support, there is the need to use a signalling protocol. The NSIS protocol was chosen as the main signalling protocol for the WEIRD system due to its flexibility, independence of the application and lower layers, as well as its applicability to different QoS models and to mobility environments.

In the WEIRD project, NSIS is used for QoS signalling in order to verify the resource availability or request dynamic resource allocation in the CSN and in the core network, along the full path, across heterogeneous domains which support NSIS.

NSIS signalling is triggered in the ASN-GW, where a QoS Specification (QSpec) object is created with the QoS parameters requested by the SIP application. The QSpec is sent in a QoS-NSLP message to the core IP network until the access network of the destination. If the routers in the domains traversed are NSIS aware, NSIS signalling may be performed, and the required resources allocated.

4 Signalling Scenario

The WEIRD architecture provides support for SIP applications with QoS requirements through a direct interaction between the SIP Proxy located on the CSN and the ASN-GW. This approach allows the SIP Proxy to ask for the resource allocation to satisfy the QoS requirements signalled via SDP protocol. Additional functionalities, such as authentication and QoS authorization, are supported: a specific AAA server, based on the Diameter protocol [20], is located in the CSN and interacts with both the SIP Proxy and the ASN-GW.

Two different scenarios can be distinguished depending on the location of the SIP User Agents (UA) involved in the communication, as showed in Figure 3. In the first case both the caller and the callee are located in the same ASN, so they can be served by MSs connected to either a single BS or different BSs under control of a single ASN-GW. In such situations, resources are allocated only in the wireless segments through the creation and the activation of a set of WiMAX Service Flows. The entire resource reservation is handled by a single ASN-GW and the QoS signalling towards the CSN and the core network is not performed.

![Fig. 3 – SIP Scenario](image)

In the second case, caller and callee are served by MSs located in different ASNs. In this scenario, two SIP Proxies and two ASN-GWs are involved. Resources are allocated in both the wireless segments and the NSIS protocol is adopted to signal the QoS requirements in the multi-domain wired network between the ASN-GWs. Two distinct types of signalling are involved: the end-to-end application-layer signalling, processed by the SIP Proxies and used to establish the session, and the edge-to-edge NSIS signalling between the ASN-GWs, used to request the resource allocation in the CSN and in the core network.

Both scenarios adopt the two-phase SF activation mechanism, where a SF is firstly admitted and then activated. Such mechanism is defined in the IEEE 802.16 standard.
d/e specification in order to be used with applications that first require a specific signalling process to establish the session and then can transmit and receive the data traffic, therefore this approach is especially suitable for voice or video applications based on the SIP protocol. This choice allows the WEIRD system to provide a more efficient resource utilization: in the first phase SFs are only admitted, but not activated, they cannot carry data traffic and radio resources are not spent. This is a great advantage because in this first stage the codec negotiation between the UAs is still in progress, so only the maximum requested bandwidth can be considered.

The WEIRD system makes use of a similar two-phase approach also in the wired network between the CSNs, exploiting the related functionalities of the NSIS protocol. In particular, in the first admission stage the NSIS signalling aims to verify the resource availability in the core network, without any actual allocation. In the second phase, when the codec negotiation is terminated and the correct bandwidth value is available, the NSIS signalling demands the resource allocation via the NSIS RESERVE messages. Figure 4 shows the overall signalling between the different involved entities for a scenario where both the MSs are located in the same ASN. First of all, the SIP request is authenticated and authorized [21] through a Diameter message exchange between the Diameter client included in the SIP Proxy and the AAA server (Figure 5).

The caller SIP UA initiates the signalling with a SIP INVITE to its outbound SIP Proxy, without any credentials. In order to authenticate the user and authorize the service, the SIP Proxy sends a Multimedia Auth Request (MAR) message to the Diameter server, that replies with a Multimedia Auth Answer (MAA) including a random-generated nonce. This message allows the SIP Proxy to challenge the user with the HTTP Digest Authentication, so it sends a SIP 407 (Proxy Authentication Required) to the SIP UA with the challenge. The second INVITE contains the credentials that are included in the new MAR message and sent to the Diameter server to be validated, so that the SIP transaction can be finally authorized via the second MAA message.

If the authentication is successful, the SIP Proxy requests the resource allocation interacting with the ASN-GW, through the Gq’ interface [22]. As explained before, the resource allocation consists of two distinct phases: the SF admission considering the worst-case bandwidth requirements and the SF activation using the negotiated bandwidth. The SIP Proxy includes an Application Function (AF), in charge of processing SDP messages and extracting valuable data, such as IP addresses, ports, media types and QoS parameters (bandwidth and priority). This information are transmitted to the ASN-GW using the Diameter Authorize Authenticate Request (AAR) message, with the AVPs (Attribute Value Pairs) described in Table 2.

The ASN-GW contains a module, called Connectivity Service Controller, that processes the dynamic requests and acts as a coordinator of the signalling for the resource allocation. The CSC translates the session description included in the AAR message into a set of parameters for the configuration of the WiMAX SFs. In particular, it uses the network topology description stored in the internal database to determine the MAC addresses of the BS and SS involved in the communication and the direction of the SFs (uplink or downlink). The scheduling class for each SF is chosen according to the media type as defined in Table 3.
Table 2 – AAR message AVP

<table>
<thead>
<tr>
<th>AVP Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>263</td>
<td>Session Id: Globally unique identifier for the session</td>
</tr>
<tr>
<td>264</td>
<td>Origin-Host: The endpoint that originated the Diameter message</td>
</tr>
<tr>
<td>296</td>
<td>Origin-Realm: The realm of the originator of the Diameter message</td>
</tr>
<tr>
<td>283</td>
<td>Destination-Realm: The realm of the destination of the Diameter message</td>
</tr>
<tr>
<td>517</td>
<td>Media-Component-Description: Grouped AVP - see Media-Component-Description</td>
</tr>
<tr>
<td>518</td>
<td>Media-Component-Number: Used to identify the ordinal number of the media component</td>
</tr>
<tr>
<td>519</td>
<td>Media-Sub-Component (one or more): Grouped – see Media-Sub-Component</td>
</tr>
<tr>
<td>520</td>
<td>Media-Type: AUDIO (0) - VIDEO (1) - DATA (2) - TEXT (5)</td>
</tr>
<tr>
<td>515</td>
<td>Max-Requested-Bandwidth-DL: The maximum requested bandwidth in bits per second for a downlink flow</td>
</tr>
<tr>
<td>516</td>
<td>Max-Requested-Bandwidth-UL: The maximum requested bandwidth in bits per second for an uplink flow</td>
</tr>
<tr>
<td>458</td>
<td>Reservation-Priority: A value in the range 0-7.</td>
</tr>
<tr>
<td>509</td>
<td>Flow-Number: Identifier for the ordinal number of the IP flow</td>
</tr>
<tr>
<td>507</td>
<td>Flow-Description: ENABLED-UPLINK, ENABLED-DOWNLINK, ENABLED (both directions)</td>
</tr>
</tbody>
</table>

Table 3 – Mapping between Media Type and SF scheduling service

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Scheduling service</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIO</td>
<td>UGS</td>
</tr>
<tr>
<td>VIDEO</td>
<td>rtPS</td>
</tr>
<tr>
<td>DATA</td>
<td>nrtPS</td>
</tr>
<tr>
<td>TEXT</td>
<td>BE</td>
</tr>
</tbody>
</table>

Table 4 – QAR Message AVP

<table>
<thead>
<tr>
<th>QoS Authorization Data</th>
<th>Diameter QoS AVPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization entity ID</td>
<td>Destination-Host</td>
</tr>
<tr>
<td></td>
<td>Destination-Realm</td>
</tr>
<tr>
<td>Application session ID / Credentials of the QoS requesting entity</td>
<td>QoS-Authorization-Data / User-Name</td>
</tr>
<tr>
<td>QoS parameters</td>
<td>QSPEC</td>
</tr>
<tr>
<td>Signalling session ID</td>
<td>Signalling-Session-Flows</td>
</tr>
</tbody>
</table>

The resource utilization for each request must be authorized, using the Diameter Quality of Service Application [23], through a QAR/QAA (QoS Authorization Request / Answer) message exchange between the QoS Diameter client of the CSC and the AAA server. The QAR message consists of the AVPs shown in Table 4. The QSPEC AVP carries a particular NSIS QSPEC [24], defined for a WiMAX QoS model in order to define all the WiMAX specific QoS parameters (Maximum Sustained Traffic Rate, Maximum Latency, Tolerated Jitter, Traffic Priority and Minimum Reserved Traffic Rate). When authorized, the request is processed by the Admission Control module that accepts or rejects it according to the current load of the network. If the request is accepted, the ASN-GW configures the BSs via SNMP protocol in order to create and admit the set of SFs and a successful response (Diameter AAA) is notified to the SIP Proxy. The SIP signalling proceeds and when the SIP Proxy receives the 200 OK message the negotiated QoS parameters are available in the SDP message. The ASN-GW extracts the AAR parameters and activates the SFs with the correct values.

Figure 6 shows the interaction between the SIP signalling and the NSIS signalling in case of SIP UAs located in
different ASNs. The authentication, the QoS authorization and the SF admission and activation is very similar to the previous ones, but in this scenario resources need to be reserved also in the CSN and in the core network. During the admission phase, the ASN-GW 1 (located in the ASN that serves the caller) verifies the resource availability in the core network sending an uni-directional NSIS QUERY message, that will be processed by all the NSIS nodes (not represented in the figure) on the path until the ASN-GW 2. An analogous NSIS QUERY message will be used at the ASN-GW 2, triggered by the received AAR message, to verify the resource availability in the opposite direction.

The ASN-GW acts as a QoS NSIS Initiator (QNI) and creates the Initiator QSPEC according to the WiMAX QoS model. The next NSIS peer, located in the CSN, is an edge node situated between two different domains, a WiMAX domain and a different domain X, and thus supports both the QoS models. This module is in charge of the translation of the WiMAX QSPEC into a new QSPEC supported by the domain X. The new Local QSPEC is added on the top of the stack and forwarded together with the Initiator QSPEC, so that the following NSIS peers of the domain X process only the Local QSPEC. This approach allows to reduce the processing of the internal nodes and to enhance the interoperability between different domains.

During the activation phase, the ASN-GWs utilize NSIS RESERVE messages to ask for the actual resource allocation. The QSPECs included in the RESERVE messages contain the correct values for the bandwidth, as negotiated between the two agents with the SIP signalling, so only the strictly required bandwidth is actually allocated.

In order to show the validity of the QoS signalling scheme proposed, two signalling scenarios, one with a single Access Service Network and the other involving different Access Service Networks were described, using the sequence messages of the involved protocols, according to the components of the WEIRD architecture.

The proposed scheme has been developed and functionality tests of the integrated WEIRD system were successfully performed on a prototype deployed at two test-beds.

## 6 Conclusions

Acknowledgments

Authors would like to thank all the partners of the WEIRD consortium for their valuable contributions.

Disclaimer: The work described in this paper is based on result of IST FP6 Integrated Project WEIRD. WEIRD receives research funding from the European Community’s Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

### References:


[7] ETSI TS 183 017 V1.1.1 (2006-03) - Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF) - Protocol specification

[8] Loughney J., Camarillo G., “Authentication, Authorization, and Accounting Requirements for the
Session Initiation Protocol (SIP)


[22] ETSI TS 183 017 V1.1.1 (2006-03) - Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF) - Protocol specification
