Quality of Service Solution for Open Wireless Access Networks

G.J. Hoekstra, O. Østerbø, R. Schwendener, J. Schneider, F.J.M. Panken, J. van Bemmel

***Abstract*—Specific network environments may require tailor-made solutions to solving Quality of Service (QoS). This is valid for the Open Access Networks (OAN) considered in this paper, where network access is provided by access points installed in homes and where different types of users need to be distinguished: residential users and users that pass the home where the access is offered. Residential users enjoy a certain broadband subscription; the casually passing users can use broadband access line's surplus capacity. As this concept enables formidable business opportunities, it imposes stringent constraints to the security, mobility and QoS solutions chosen. This paper concentrates on the QoS solution for the wireless OAN described, where casually passing users may receive a certain network capacity without affecting the residential user's broadband subscription. This brings forward specific requirements to the QoS solution, which is addressed after introducing the envisioned wireless OAN. In subsequent sections, the architectural, traffic mapping and capacity distribution details of the QoS solution are revealed to suit various capacity sharing scenarios.**

***Index Terms*—Wireless LAN, Quality of Service, Open Access Networks, OBAN**

I. Introduction

The concept of Open Access Networks (OANs) is extensively studied and demonstrated in the OBAN project [1], which aims at realizing the Open Broadband Access Network (OBAN) vision. This vision embraces a future network that enables people to roam through a WLAN and 3G communication landscape while maintaining their communication and agreed QoS.

The added value of the OBAN vision originates from the fact that the fixed access lines of ordinary *residential users* will be tuned to the maximum achievable capacity, rather than what the residential user has subscribed for. Capacity that is available to the Residential Gateway (RGW) in excess of the residential user's subscribed capacity, called *the surplus capacity*, is made available through a Wireless LAN (WLAN) Access Point (AP) to casually passing users (referred to as *visiting users*).

This forms the basic outline of the OBAN concept of having many of these, so called, home-spots forming one large wireless access network where visiting users can seamlessly roam through. Fig. 1 illustrates the basic concept of sharing the access network between the two types of users.

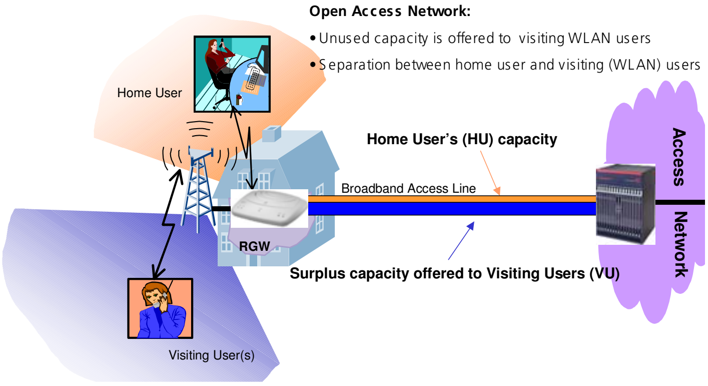
Open Access Network:
• Unused capacity is offered to visiting WLAN users
• Separation between home user and visiting (WLAN) users
Home User
Home User's (HU) capacity
Broadband Access Line
RGW
Surplus capacity offered to Visiting Users (VU)
Access Network
Visiting User(s)

Fig.1. The Open (Broadband) Access Network Concept of making surplus capacity of residential (broadband) access subscriber lines available to (casually passing) visiting users.

For applying this concept in practice, a certain degree of security, mobility and QoS should be offered. In addition, a strict division between residential and visiting users, in terms of security and Quality of Service (QoS), is necessary. For instance, users should be unable to infringe on other user's security, i.e., gain access to appliances or information. QoS degradations for the residential user should be manageable and should not drop below a predetermined and agreed threshold.

Parties that may be involved for providing the services to these users are:

- *An Internet Service Provider* (ISP) is involved for offering services to the residential and visiting users. This ISP offers, additionally, the services of a wireless overlay network, formed of all home-spots.
- *An Access network provider* (ANP) that operates the fixed access network, i.e. the equipment that connects the RGW to the ISP.

A crucial aspect for realizing the OAN is the incentive for the residential user to collaborate. Chapter 3 illustrates three possible scenarios. These scenarios also indicate more clearly the resulting responsibilities for all users and involved parties. These responsibilities are decomposed into QoS elements and form the basis of the QoS architecture.

This paper illustrates how existing mechanisms can be applied for offering an acceptable QoS for all users in the envisioned OAN.

Manuscript received February 6, 2005. G.J. Hoekstra is with Bell Labs Europe, Hilversum, The Netherlands, (gjhoekstra@lucent.com). O. Østerbø, is with Telenor R&D, Oslo, Norway.R. Schwendener and J. Schneider are with Swisscom Innovations, Bern, Switzerland. F.J.M. Panken and J. van Bemmel are with Bell Labs Europe, Hilversum, The Netherlands.

II. BASIC TRAFFIC CLASSES FOR THE OAN CONCEPT

A. *Basic traffic classes & QoS mechanisms for the OAN concept*

The possibility to make distinction between traffic classes is essential to obtain QoS in the OAN architecture. The OAN consists of different access and edge technologies, including wireless, DSL, Ethernet at different parts of the network. Different standards by various organisations like IETF and IEEE adopt different QoS approaches at several interfaces or/and layers, e.g. IP DiffServ over the IEEE802.11e MAC layer. To get a consistent end-to-end QoS view it is beneficial to define a generic set of traffic classes, and to make the necessary translation between the protocol settings and parameters at different layers or interfaces.

A natural way of defining the basic traffic classes is to adapt the four UMTS classes [2]:

- Class-1, the conversational class
- Class-2, the streaming class
- Class-3, interactive class
- Class-4, background class

Class-1 and Class-2 are typically applied for real time traffic, using UDP as transport protocol, while Class-3 and Class-4 are the service classes for elastic traffic, applying TCP as the transport protocol. While elastic traffic easily adapts to changing network conditions and shares the available capacity equally among the ongoing sessions, the traffic using UDP as transport will not be able to adjust their rate to the current network situation. This explains why it is necessary to have a *Capacity Distribution Algorithm* (CDA) combined with Call Acceptance Control (CAC) on a per flow basis to ensure that QoS is maintained at least for real time services. In addition, there is a possibility to prioritize among the different traffic classes. This means that a two level QoS resolution can be defined:

- *Relative QoS differentiation*, by using different forms of scheduling among the traffic classes, and
- *Strict QoS*, on a per flow base, at resource management level by the CDA (combined with CAC).

Combining the basic traffic classes with the two types of users yields in total eight traffic types in the proposed OAN concept.

B. *QoS differentiation on WLAN*

To obtain QoS differentiation over the "air" interface the IEEE has standardised QoS in WLAN networks with the 802.11e standard. A subset of the IEEE 802.11e standard, called Wi-Fi Multimedia (WMM)[3], is defined by the Wi-Fi Alliance [4] for traffic prioritization. In WMM, traffic differentiation is based on the Enhanced Distribution Channel Access (ECDA) function where four Access Categories (AC) are defined based on differing the two timing parameters in the collision resolution algorithm:

- The minimum inter-frame space, or Arbitrary Inter-Frame Space Number (AIFSN)
- The Contention Window (CW)

Both values are smaller for high-priority traffic. For each AC, a backoff value is calculated as the sum of AIFSN and a random value, chosen between zero and CW. If a collision is detected, the CW is doubled until a maximum value is reached (also depending on the AC). Since the AC with highest AC tends to have the lowest backoff value, they are more likely to capture the "channel" when it is idle.

WMM defines four "priority" classes or ACs. It is therefore necessary to appropriately map the eight OAN traffic types onto the four ACs. One plausible way is to take real time traffic (Class-1 and-2) for the residential user as AC 1 (the highest "priority") and real time traffic (Class-1and-2) for visiting users as AC 2. In that case, elastic type traffic (Class-3 and-4) for the residential user can be mapped to AC 3 and finally elastic traffic (Class-3 and-4) for visiting users to AC 4. This mapping is given as alt. 1 in *Table 1*.

A second alternative (alt. 2 in *Table 1*) gives the residential user's traffic strict "priority" over all the visiting users traffic. Restriction of capacity usage is needed to avoid undesirable effects on the real-time traffic of the visiting users.

TABLE 1. BASIC MAPPINGS BETWEEN OAN TRAFFIC TYPES AND IEEE802.11E/WMM ACS (RU = RESIDENTIAL USER / VU = VISITING USER)

Traffic classes/types of users	Possible DiffServ classes	IEEE802.11e AC		Traffic type description
		alt. 1	alt. 2	
Class -1/RU	EF	AC 1	AC 1	Residential/ Conversational
Class -2/RU	AF1	AC 1	AC 1	Residential/ Streaming
Class -3/RU	AF2	AC 3	AC 2	Residential/ Interactive
Class -4/RU	BE	AC 3	AC 2	Residential/ Background
Class-1/VU	EF	AC 2	AC 3	Visiting/ Conversational
Class -2/VU	AF1	AC 2	AC 3	Visiting/ Streaming
Class -3/VU	AF2	AC 4	AC 4	Visiting/ Interactive
Class -4/VU	BE	AC 4	AC 4	Visiting/ Background

It could be desirable to have a direct mapping between the appropriate traffic classes onto DiffServ classes and, subsequently, a hierarchal mapping onto the QoS mechanisms at the different interfaces. This way, the DiffServ DSCP can be set by terminal and remains unchanged through the network, and the mappings of the traffic classes to the link layer QoS mechanisms can be based only on the DSCP value. This approach appears to be a difficult, as it requires up to eight DiffServ classes to be defined for the residential and visiting user's traffic classes. Furthermore, at the RGW the basic priority scheduling rules between the traffic classes for the residential and visiting users should be maintained as for the "air" interface.

Another approach could be to make the QoS mapping, dependant, not only on the DSCP value, but also on the knowledge of the user types as indicated in Table 1.

By such a method the basic DSCP values can be set at the terminal and maintained at the IP level end-to-end.

III. Capacity Sharing Scenarios and QoS Architecture

A. *Capacity sharing scenarios for Open Access Networks*

The capacity in the fixed access network part (e.g. Fibre or xDSL) assigned to the residential user must be shared with visiting users to realize the Open Access Network. Three scenarios can be distinguished:

1) *Scenario 1: Sharing of the residential user's network capacity*

In this scenario, the ANP just provisions the capacity ordered by the residential user. Visiting users are using a part of this capacity. The residential subscribers do not get a guarantee for the nominal capacity they subscribe to at the ANP. Visiting users can use all capacity of the residential user, if required. However, this is expected to happen rarely. Residential users may be ready to accept this, and even encourage the capacity usage of visiting users, e.g. if they get the service at a significantly reduced price, or get a discount for every visiting user.

From a business perspective, this scenario potentially allows to implement the OAN without cooperation of the ANP. This scenario is currently applied by certain ISPs, such as Boingo [5] and Linkspot [6].

2) *Scenario 2: Supplementary capacity for visiting users, no sharing of the residential user's network capacity*

In this scenario, the ANP provisions additional capacity for the visiting users. The residential user receives exactly the same service from the ANP as without the visiting users. The ANP makes sure, for network parts that he is responsible for, that the traffic of the residential and the visiting user do not disturb each other.

From a business perspective, this scenario involves the ANP. One business variant is that the ANP or the ISP of the residential user offers the same service to the visiting users. Another variant would be a cooperation of a fixed-and mobile operator, or possibly a future converged Fixed/Mobile operator.

3) *Scenario 3: Supplementary capacity for visiting users and sharing of residential user's capacity*

In this scenario, the ANP provisions additional capacity for the visiting users (as scenario 2). However, these users can, in addition, use a part of the residential user's capacity (this is where this scenario differs from scenario 1).

From a residential user's perspective, this scenario is identical to scenario 1. From an access network operator's perspective, it is the best solution, as this provides the maximum capacity (however, the additional capacity reserved in the fixed network will not be free of charge).

From a business perspective, the ANP is involved, as in scenario 2.

For general service oriented QoS support the architecture needs to handle different traffic classes, depending on the supported services. For OANs, the described capacity sharing scenarios have an additional influence on the needed QoS elements. The consequences of each scenario on the QoS architecture are as follows:

In Scenario 1 it is difficult to provide services with QoS to visiting users because the traffic cannot be distinguished from that of the residential user. As visiting traffic should not degrade the quality of the residential traffic, only very little visiting traffic can potentially have priority against residential traffic, even if the residential traffic is just best effort traffic. Thus, scenario 1 can mainly be used for best effort traffic offered to visiting users.

Scenario 2 is a static sharing approach and needs two fixed dimensioned pipes for the residential-and the visiting user, e.g. for ATM on layer 2 two ATM virtual circuits are needed. No additional QoS elements are needed in the fixed access network part to realize the sharing mechanism with two ATM virtual circuits.

With scenario 1 and 3 the traffic from the visiting users and from the residential user share common resources. Therefore traffic from residential users needs to be prioritized over that of the visiting user.

For the realization of scenario 3 an additional QoS entity is necessary. In order to restrict the residential user to his subscription with a corresponding monthly fee, the residential capacity needs to be limited. This can be done by the ANP by applying shaping and policing mechanisms.

With the implementation of scenario 3 enough flexibility and mechanisms are available to realize also scenarios 1 and 2. Therefore it is used here as a basis to determine the required QoS elements in the architecture. For the architectural QoS elements needed, scenario 3 forms a superset of the other scenarios. The other scenarios can be obtained by omitting functional QoS elements.

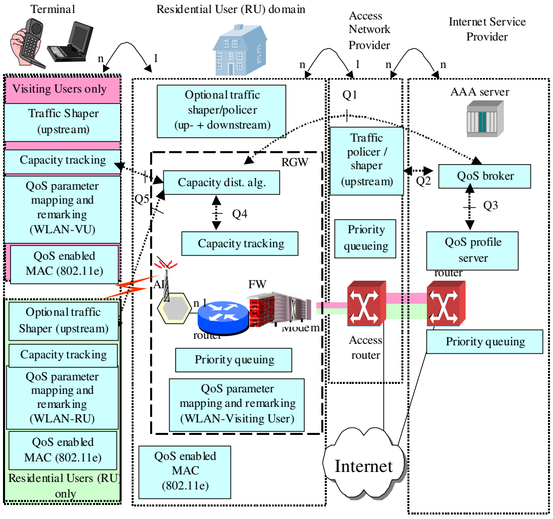
Terminal
Residential User (RU) domain
Access Network Provider
Internet Service Provider
n
1
n
1
n
n
Visiting Users only
Traffic Shaper (upstream)
Capacity tracking
QoS parameter mapping and remarking (WLAN-VU)
QoS enabled MAC (802.11e)
Optional traffic Shaper (upstream)
Capacity tracking
QoS parameter mapping and remarking (WLAN-RU)
QoS enabled MAC (802.11e)
Residential Users (RU) only
Optional traffic shaper/policer (up- + downstream)
RGW
Capacity dist. alg.
Q5
Q4
Capacity tracking
AP
n 1
router
FW
Modem
Priority queuing
QoS parameter mapping and remarking (WLAN-Visiting User)
QoS enabled MAC (802.11e)
Q1
Traffic policer / shaper (upstream)
Priority queueing
Access router
Internet
AAA server
Q2
QoS broker
Q3
QoS profile server
router
Priority queuing

Fig. 2. Functional QoS architecture for an Open Access Network (OAN) featuring different domains for Visiting Users (VU) and Residential Users (RU) in addition to the ANP and ISP. The arrows between these domains indicate the mutual relation, e.g. *n* terminals can be associated to one residential user domain.

B. QoS Architecture for Open Access Networks

The following subsections show how existing QoS elements and interfaces can be accommodated into a QoS architecture suitable for the considered OAN.

1) Architectural QoS elements

For each party (users, ISP, ANP) in the architecture an overview of QoS elements can be derived for accommodation in the QoS architecture of Fig.2.:

a) The Internet Service Provider

- QoS broker; determines the capacity for the ANP and instructs the policing functionality in the ANP.
- QoS profile server; stores the profiles of each user. This functionality could be integrated with the AAA server and is triggered after authentication was successful.
- Priority queuing; can be realized through e.g., Diffserv. or other techniques.

b) The Access Network Provider

- Traffic policer/shaper; monitors whether the sum of the assigned capacity is not violated by a RGW through policing. It has received the granted profile from the QoS broker. This could be realized through policies, where the QoS broker can control the policing mechanism.
- Priority queuing; can be realized through e.g., Diffserv. or other techniques.

c) The RGW in the residential user domain

- Capacity distribution algorithm (CDA); determines the network capacity that can be assigned to a terminal. This value is based on various parameters, including the visiting user's QoS profile, the capacity reserved for the residential user, the gross capacity of the medium and inefficiency of the medium (depending on using e.g., the wireless LAN's channel reservation mechanism). A typical entry in of the QoS profile would be the application characteristics.
- Capacity tracking; allows to track the capacity for each associated station, which may vary over time as a result of a greater distance from the RGW. The capacity tracking could be implemented as part of the entity that realizes traffic policing.
- Priority queuing; can be realized through e.g., IEEE 802.11e or WMM.
- QoS parameter mapping & remarking; checks the priority level and subsequently maps it to the QoS levels understood outside the context of the OAN.
- Traffic shaper and policing functionality, assuring that the terminals (and RGW) do not violate the granted capacity.

d) Terminal for Residential and Visiting User

- Traffic shaper; shapes the traffic such that it obeys the capacity value received from the RGW.
- QoS parameter mapping; maps the priority values of higher layers to the appropriate WLAN AC values.
- QoS enabled MAC; e.g., IEEE 802.11e or WMM.
- Capacity tracking; as the terminal moves, the capacity that can be used changes accordingly. The entity "capacity tracking" keeps track of this locally. It can also decide which capacity values can be used and can re-initiate WLAN admission control requests in the case the WLAN link rate drops below a certain threshold.

2) Interfaces between the QoS architectural elements

In the QoS architecture indicated in Fig 2., five QoS interfaces, namely:

a) Q1: communication between QoS broker and the capacity distribution algorithm.

Exchange of QoS profile information that belongs to the user that seeks connectivity. The information consists of a set of QoS profiles that is associated to the user and restricted by the QoS broker and/or the capacity distribution algorithm as a result of lack of capacity. The profiles consist of a set of name-value pair that can be exchanged by various protocols or by policy mechanisms. Since QoS is closely related to security and charging, value specific attributes of the AAA solution could also be used to exchange this information.

b) Q2: communication between QoS broker and the traffic policer entity

The QoS broker instructs the traffic policer entity regarding the newly admitted QoS profile such that this entity can verify whether the RGW violates the sum of the granted QoS profiles. SNMP, CORBA or other protocols used for management or the assigning of traffic regulation can be used.

c) Q3: communication between QoS broker and QoS profile server

The QoS profile server stores the QoS profiles for each user. Upon correct authentication, the QoS profile of the authenticated user is passed to the QoS broker. This QoS broker can subsequently admit or adjust the profile, depending on the result of negotiations with other network parts. A possible reason for adjustment is that there is limited capacity available in the access network. The QoS broker is aware of the capacity granted to each user and can be integrated with accounting mechanisms. Traffic monitoring functionality in the network can be instructed to count bytes for each of the AC and communicate this back to the QoS broker.

d) *Q4: communication between the capacity distribution algorithm and entity that tracks capacity*

Upon deciding the capacity that can be granted to an associated user, the capacity distribution algorithm communicates the value with the capacity tracking entity. The capacity tracking entity can determine the capacity associated with each user as a result of e.g., roaming.

e) *Q5: communication between the terminal and the capacity distribution algorithm*

The capacity distribution algorithm determines the capacity each terminal consumes. This value is communicated to the terminal. It is in the best interest of each terminal not to violate this value, since exceeding traffic will be discarded (or shaped until credentials are met) by the policing entity in the RGW. Various protocols are suitable for communicating the granted capacity, including SNMP and the beacon frames of the IEEE 802.11 protocol.

3) QoS Architecture Interoperation with mobility and security

With the QoS elements and interfaces defined for each of the domains, the next step is to allow this architecture to be integrated with security and mobility functionality. This subsection concentrates on an example of how the QoS functionality should interoperate with security for authenticating users.

Fig. 3. depicts the information sequences exchanged between the various functional elements. We assume the presence of a Radius AAA proxy in the RGW, relaying the authentication messages to the AAA server. After the Radius proxy receives an authentication request, it first communicates with the capacity distribution algorithm to verify whether the minimum amount of capacity is available. If not, the authentication request is not relayed and it decides locally that access cannot be granted. If the capacity distribution algorithm informs that the minimum capacity is available, the AAA proxy continues the authentication process by forwarding the request to the AAA server of the appropriate service or network provider. If the AAA service decides authentication is successful, it interrogates the QoS profile server with the profile and a pointer (URL, IOR,…) to the capacity distribution algorithm. The QoS profile server is a database that stores QoS profiles for each user and can ideally be integrated with the AAA server.

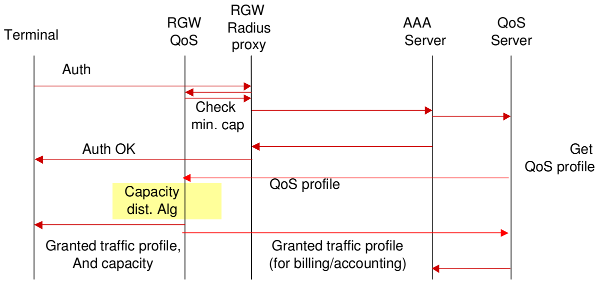

Fig . 4. Authentication and the interaction with the QoS modules

The authentication process can continue and the RGW informs the terminal that access is granted. In parallel, the QoS broker and the capacity distribution algorithm negotiate the QoS profile that can be granted. These processes are executed in parallel to ensure that the timing requirements for authentication can be met. Subsequently, the capacity allocation algorithm determines the capacity from all input parameters (including the selected profile, capacity reserved for residential user, type of WLAN, etc) and the terminal is informed about the value. The QoS broker is subsequently informed about the selected profile as it may be input for charging and also for the update of the policing mechanisms in the access network.

Alternatively, if policing in the access network is not needed, the QoS profile can be passed along with the information that access to the user should be granted.

When roaming between different home-spots occurs, re-authentication is required. In that case the same interactions will apply for obtaining the appropriate QoS at the new home-spot.

IV. Conclusion

Opening existing residential access networks for services to new mobile users yields appealing capacity sharing scenarios. This paper shows how QoS mechanisms can be applied to add and apply a predefined QoS level to these network services. It has been shown that existing traffic classes can be used. By applying contemporary traffic prioritization mechanisms visiting users can be offered a desired level of QoS. The capacity distribution algorithm can be configured such that the effects for the residential users can be manageable.

Acknowledgment

This is work performed in the context of the OBAN project. The OBAN project is partially funded by the European Commission with the participation of Swisscom Innovations partially funded by the Swiss Bundesamt für Bildung und Wissenschaft.

References

[1] The OBAN Project Website: http://www.ist-oban.org
[2] 3GPP; Quality of Service (QoS) concept and architecture (Release 6) TS 23.107 (2004-12)
[3] Wi-Fi CERTIFIED™ for Wi-Fi Multimedia (WMM™) - Support for Multimedia Applications with Quality of Service in Wi-Fi® Networks, http://www.wi-fi.org/OpenSection/pdf/WMM_QoS_whitepaper.pdf,
[4] Wi-Fi Alliance Website: http://www.wi-fi.org
[5] Boingo Website: http://www.boingo.com/
[6] Linkspot Website: http://www.linkspot.com/

G.J. Hoekstra received his Hon. M.Sc. degree in electrical engineering from the University of Twente, Enschede, The Netherlands, in 1999.

Gerard joined Lucent Technologies in 1999 and works as member of technical staff in the department of Bell Labs Europe, located in Hilversum, the Netherlands. He has been involved in several research projects, funded by the Dutch government and the European Commission. His research interests include performance analysis and modeling and simulation of communication networks.