Dynamic Traffic Regulation for WiFi Networks

Domingo Marrero, Elsa M. Macías, *Member, IAENG*, and Alvaro Suárez, *Member, IAENG*

***Abstract*— Multimedia applications require high bandwidth in order to assure certain level of *Quality of Service* (*QoS*). It is well known that the characteristics of the traffic for multimedia applications are very different from the traditional data traffic that only requires a best effort service. In a network in which terminals communicate multimedia and also traditional data traffic, another important effect is produced: if a bad set of priorities is used neither the data traffic nor the multimedia ones obtain good performance. Sometimes is better to give higher priority to a short traditional data transaction, because it will finish soon leaving free the channel for the multimedia application. This is a hard problem to solve that requires a combination of well known methods.**

On the other hand, *Wireless Fidelity* (*WiFi*) networks have experimented an spectacular growth in last recent years. As a result, they are being used to access multimedia servers allocated in wired networks. Nevertheless, the availability of real bandwidth in current commercial WiFi networks is limited. Therefore, admission control becomes very important to increase the overall system performance. To get real value of this, we combine the admission control with a traffic regulation mechanism. Depending on the requested service, the *Access Point* (*AP*) could deny the network access if the required bandwidth is not guaranteed or on the contrary, the access is allowed by reducing the rate of the newly associated station or the rate of some current associated ones.

***Index Terms*— WiFi networks, admission control, traffic regulation, limited bandwidth.**

I. Introduction

The maximum *Phisycal Level* (*PHY*) data rate targeted by a current WiFi network is 54 Mbit/s [1] [2]. This data rate is theoretical since actual data throughput will vary because of network conditions and environmental factors. Some studies show that with *International Electric and Electronic Engineers* (*IEEE*) 802.11b [3] users will get between 4 and 5.5 Mbps. IEEE 802.11a/g users can expect about 25 Mbps [4][5]. Some vendors offer products with higher data rate [6] that only work at that rate for products from the same family. IEEE 802.11n work group [7] is investigating the possibility of improvements to the IEEE 802.11 standard to provide high throughput. In our days this standard is only used commercially in certain proprietary kind of *set-top-boxes* [8] to forward TeleVision (TV) signal from this set to the PC or TV set, although this standard is not ratified.

The *Medium Access Control* (*MAC*) for these wireless networks is usually a contention based mechanism. Therefore, wireless stations have the same opportunity to transmit data. Since this approach is not optimal for priority traffic, e.g. transport of voice, audio and video, video conferencing, media stream distribution and so on, the IEEE 802.11e work group [9] is improving the IEEE 802.11 MAC to manage Quality of Service (QoS), provide classes of service, and enhanced security and authentication mechanisms. These enhancements, in combination with improvements in PHY capabilities from IEEE 802.11a/g/n, will increase overall system performance.

Apart from using a higher PHY data rate and a MAC that manages QoS, we think that providing different throughput depending on the application will even improve the overall system performance. For example, consider two stations contending to send data coming from a video streaming session and a *File Transfer Protocol* (*FTP*) application respectively. It is expected that the MAC solves this contention giving the opportunity to transmit to the first station most of the time, if IEEE 802.11e is used, or a random access if a MAC without QoS provision is used. Whatever MAC is used, when the second station gains the channel, it would be desirable that the wireless channel were free as soon as possible. For doing that, the FTP data must be sent at the maximum available PHY data rate and the amount of data that the application passes to the MAC algorithm should be regulated to be minor than the video streaming data rate.

More precisely, if the real available bandwidth in an IEEE 802.11a/g network were 25 Mbps, and the access to the channel were fair, the wireless station with priority traffic could fix, as a first approach, 18.75 Mbps as the data rate (the 75% of the capacity) and the other station will fix the data rate at 6.25 Mbps for the FTP application (the remaining 25%). That is to say, regulating the rate on the wireless stations will improve the overall system performance since the FTP traffic does not need high throughput and reducing the MAC data rate for the FTP application will not penalize the user experience. Obviously,

Manuscript received March 22, 2007. This work was supported in part by the Spanish CICYT (MEC) and European Research Development Fund (FEDER) under Grant TSI2005-07764-C02-01, and FEDER and The Canaries Regional Education under contract PI042004/164.

Domino Marrero is with GAC (Grupo de Arquitectura y Concurrencia), Departamento de Ingeniería Telemática, Universidad de Las Palmas de G. C., Campus Universitario de Tafira, 35017 Las Palmas de G.C., SPAIN. (phone: 34 9 28 451250; fax: 34 9 28 451380; e-mail: dmarrero@dit.ulpgc.es).

Elsa Macias, is with GAC (Grupo de Arquitectura y Concurrencia), Departamento de Ingeniería Telemática, Universidad de Las Palmas de G. C., Campus Universitario de Tafira, 35017 Las Palmas de G.C., SPAIN. (e-mail: emacias@dit.ulpgc.es).

Alvaro Suarez, is with GAC (Grupo de Arquitectura y Concurrencia), Departamento de Ingeniería Telemática, Universidad de Las Palmas de G. C., Campus Universitario de Tafira, 35017 Las Palmas de G.C., SPAIN. (e-mail: asuarez@dit.ulpgc.es).

the optimal data rate will be dynamically recalculated according to network changes. For example, if more than two stations are contending to send data and there is the same real bandwidth available.

At present there are solutions aimed at solving the problems derived from the limited wireless bandwidth. In [10] is presented a solution to extend the reservation based end-to-end QoS for WiFi networks. Others solutions pretend to modify the current MAC distributing the access among the participating stations into time slots or different frequencies. Obviously, this solution is not compliant with the standard. There are other solutions to regulate the bandwidth from the wired network [11] or from the AP. In this case, the wireless station could reduce the overall system performance if the throughput of its applications were high.

We have implemented a solution that consists of an admission control in the AP and a traffic regulation mechanism on source, i.e. on the wireless station. Briefly, the AP allows or denies the access to a newly wireless station depending on the type of traffic that the station will generate and the wireless channel state in terms of the available wireless bandwidth. The associated wireless stations will dynamically readjust its MAC data rate according to the information provided by the AP which broadcasts all the necessary information about the type of traffic in the wireless stations. This information is sniffed from the AP due to its strategic location in the infrastructure network. The main benefit of our approach is that it is more efficient to manage the wireless bandwidth in comparison with other solutions based solely on admission control.

The rest of the paper is organized as follows. Section 2 is devoted to present our proposed software solution. In section 3 is presented some preliminary experimental results. Finally, we summarize our conclusions and present directions for further research.

II. ADMISSION CONTROL AND TRAFFIC REGULATION MECHANISM

The mechanism we propose is basically composed by two different entities: The manager allocated in the AP and the agents allocated in the wireless stations.

In Fig. 1 we show a graphic representation of the overall software we propose. It basically consists of the following elements:

- When an incoming wireless station enters the coverage area of the AP, the user must request to a standard *Web Server*, via a standard *Web Browser* some basic parameters, in order to be authorized to communicate. Basically, once the wireless station is associated its user must specify the type of traffic that it will generate after the association process. This information is sent via the user interface.

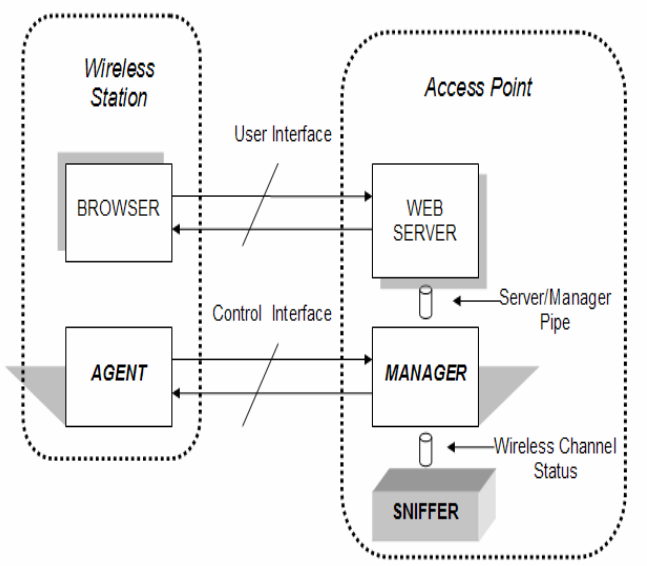

Fig. 1. Software architecture.

- A *Manager/Agent* based model to set up dynamically the traffic rate for all the associated wireless stations. The only manager runs on the AP (we suppose that the AP is programmable, in other case we can arrange a PC with a *Wireless Network Card Interface* (*WNIC*) and *Fixed NIC* (*FNIC*) in charge to interconnect both networks). There are as many agents as wireless stations and therefore one agent running on each wireless station (Fig. 2). The manager and each agent communicate themselves via the control interface sending messages that contain useful information for our mechanism such as the data rate the agent must set up at any time.
- A *Sniffer* daemon to monitor the communications using the *libpcap* library [12]. In particular, the gathered information includes the number of packets injected into the wireless network during the last second and the last 5 seconds, and the average latency

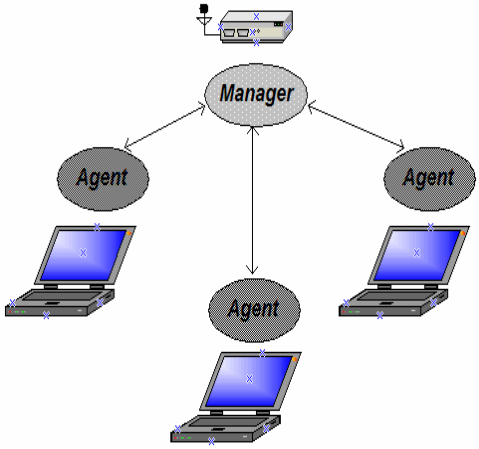

Fig. 2. Manager/Agent based model.

among packets during the last second and the last 5 seconds. This information is used by the manager to set up the data rate for each station, including the newly associated wireless ones. The sniffer also monitors the ports used for each wireless station and the stations transmitting, blocking the communications coming from stations not associated or associated stations that use ports not allowed (e.g. stations doing ping can flood the network if the AP forwards the *Internet Control Message Protocol* (*ICMP*) messages). Besides, it checks if there is one or more wireless stations not associated but sending data in the same radio channel than the AP or in a different one overlapped with that channel (remember that for IEEE 802.11g networks there are only three non-overlapped PHY channels). With this last consideration, the AP is also aware of the presence of stations that can reduce the overall performance system because their communications can collide with the communications of the wireless stations associated to the network.

Fig. 3 shows the different steps since a wireless station requests the association until its request is allowed or denied by the AP. As it is shown in Fig. 3, the different steps are the following:

1. The web browser of the user connects with the web server. The response of the web server, a window that appears in the browser, requests the user to type the username, password and the selection of the type of service. In our implementation, the user can select one of the following applications: peer to peer, FTP, telnet, *Secure Shell* (*SSH*), chat, *Real Time Streaming Protocol* (*RTSP*) and *Real Time Protocol* (*RTP*)/*Real Time Control Protocol* (*RTCP*).
2. The above identification values typed by the user are checked by the web server to be well formed and be semantically correct.
3. The sever will deny the access if the username or password are not valid.
4. On the contrary, the server conveys the manager the type of service requested by the new wireless station.
5. The manager consults the state of the channel to the sniffer.
6. The sniffer returns the requested information, and the manager decides if the requested service can be guaranteed or by the contrary, some type of traffic regulation should be applied for the new wireless station or for the current stations in the network. For example, if the chosen service is one of higher priority in comparison with the type of traffic that is being transmitted by the current wireless stations, then the data rate for these stations will be reduced. This will be communicated by the manager to each agent using special control packets of our mechanism.

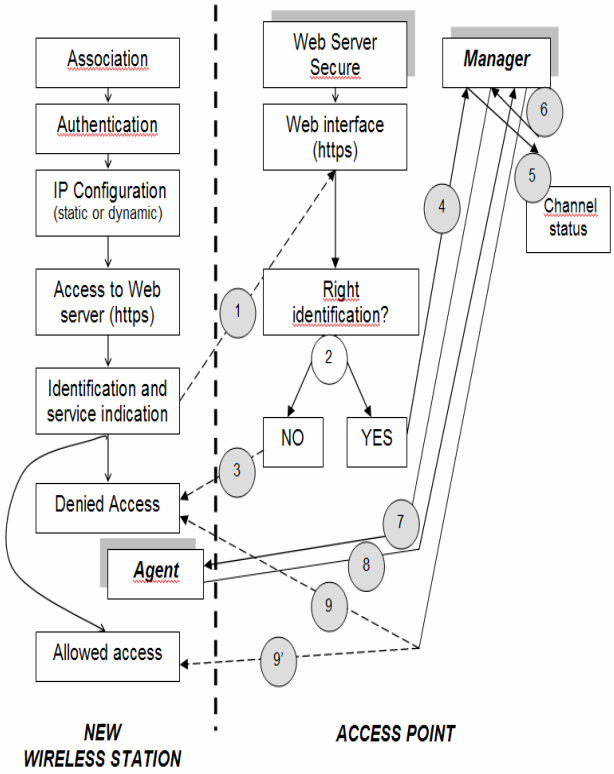

Fig. 3. Steps to regulate the traffic for a new wireless station.

7. The manager sends the data rate that the agent must pass to the MAC level.
8. The agent replies accepting or not the imposed data rate.
9. If the agent does not respond, the manager will block the access to the wireless station specifying this fact through the Web browser to the user.

9'. On the contrary, the access will be allowed only for the requested service using the iptables [13].

Once the wireless station starts the data communication, the manager regularly will check that the agent is running and that the imposed data rate for the chosen service is carried out. If not, then the data communications are not forwarded by the AP.

The agent set up the MAC data rate for its station using the *Traffic Control* functions [14] implemented for Linux operating system that allow defining different types of policy, traffic classification, rates regulation and so on. In our preliminary version, we have used only *Token Bucket Filter* (TBF) [14] to restrict the MAC data rate.

In order to calculate the optimal data rate for each station, it is necessary to know the wireless bandwidth available. As we stated in the introduction, it will be minor than the theoretical PHY data rate defined by the standard. We use *iperf* [15] application to obtain this value. Let us note that the bandwidth we calculate is estimated since network conditions and environmental factors can reduce the real value. Once the manager has this value (we termed it as *B*), *B* will be split among the current stations as follows: *B/3* will be distributed among the stations with non priority traffic and the remaining,

i.e. *2B/3*, will be distributed equally among the stations with the priority traffic. Obviously, *B* should be recalculated periodically. Besides, other dynamic distribution techniques should be considered.

III. Preliminary Experimental Results

The hardware architecture we used to test our software is presented in Fig. 4. Instead of using a conventional AP, we decided to use a *Personal Computer* (*PC*) that behaves as a router to the wired network with the operating system Linux and two NIC: an *Ethernet* NIC for the connection with the wired network and an IEEE 802.11b/g NIC for the wireless network. Using a Linux router has several advantages for our aims: open source (kernel and applications), support for database to register our users, management of forwarding, filtering and masquerading (iptables [13]), web server secure: *Hiper Text Transfer Protocol Secure* (*HTTPS*) and Traffic Control functions.

Table 1 shows the technical characteristics of the two wired stations (PC), the two wireless stations (portable computers) the PC that implements the router and the hub used in our equipment. We deliberately used low performance PC and portable computers (except one) because, in general, *Personal Digital Assistants* (*PDA*) and mobile phones with WiFi have also low performance hardware. In this way we can obtain relative results that can be used with these kinds of wireless stations. The WNIC of wireless stations is configured in ad hoc. Nevertheless, our software will work at the same manner as for an infrastructure network.

Firstly, we evaluated the real available wireless bandwidth. We obtained an average value of 5 Mbps.

Secondly, we introduced traffic from the wireless station 1 to the wired station 1 using iperf application. The former acts as the iperf client and the latter as the server. We repeated the experiment with the wireless station 2 and the wired station 2. The aim of this experiment is to calculate the maximum rate we obtain when there is only one communication in the network coming from wireless station 1 or wireless station 2 respectively.

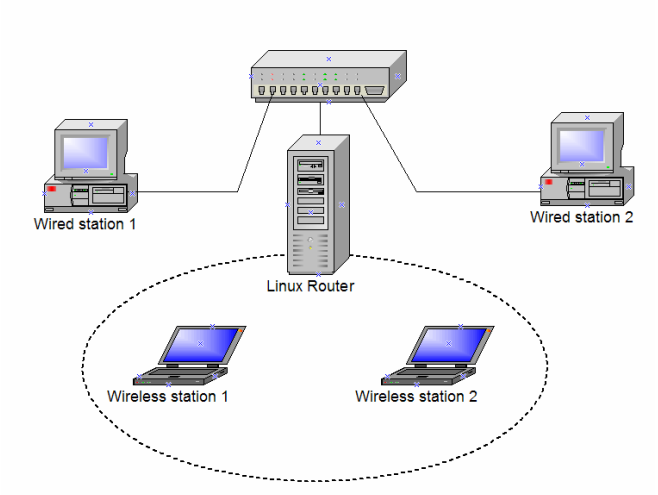

Fig. 4. Test-bed architecture.

Table 2 summarizes the results: the second column shows the data rate and the third column is the quantity of transmitted information. The differences obtained in both experiments are due to the different WNIC used for both tests (the wireless station 1 used a IEEE 802.11b WNIC and the other a IEEE 802.11g one).

Table 1. Technical characteristics of the hardware of the experimental platform.

Station / hub	***Hardware***	***NIC***
Wired station 1 (Linux Fedora Core 3 operating system)	PC, Pentium III 1Ghz, 512K RAM[1]	Ethernet /Fast Ethernet 10/100BaseT
Wired station 2 (Linux Fedora Core 2)	PC, Pentium II, 400Mhz, 128M RAM	Ethernet /Fast Ethernet 10/100BaseT
Wireless station 1	Pentium III 1Ghz, 256M RAM	*PCMCIA*[2] Compaq[3] IEEE 802.11b
Wireless station 2	Pentium IV 3Ghz, 1G RAM	PCMCIA Dlink[4] IEEE 802.11b/g
Linux router (Fedora Core III)	PC, Pentium II 400Mhz, 196M RAM	PCMCIA Compaq IEEE 802.11b
Hub	Genius 8 Ports	Ethernet /Fast Ethernet 10/100 Mbps

[1] *RAM stands for Ramdom Access Memory,* [2] *PCMCIA stands for Personal Computer Memory Card International Association.* [3] *Compaq is a registered company.* [4] *DLink is a registered company.*

Table 2. Maximum rate for isolated communications between one source (wireless station 1 or 2) and one destination (wired station 1 or 2).

Source→Destination	***Rate***	***Information***
Wireless station 1→Wired station 1	3.89 Mbps	4.71 Mbytes
	3.95 Mbps	4.74 Mbytes
	3.95 Mbps	4.73 Mbytes
	3.94 Mbps	4.70 Mbytes
	3.93 Mbps	4.70 Mbytes
	3.95 Mbps	4.70 Mbytes
Wireless station 2→ Wired station 2	5.44 Mbps	6.52 Mbytes
	5.48 Mbps	6.58 Mbytes
	5.44 Mbps	6.52 Mbytes
	5.47 Mbps	6.58 Mbytes
	5.47 Mbps	6.55 Mbytes

Next, we repeated the experiment considering both wireless stations transmitting. As a result the rates are reduced for both stations due to PHY channel competition between the two stations and no traffic regulation as it is shown in Table 3. Let

us note that the rate and the quantity of information for wireless station 1 are now reduced by a factor of 2 approximated. For wireless station 2 this factor is approximately 1,4.

Table 3. Maximum rate for communications between two sources (wireless station 1 and 2) and two destinations (wired station 1 and 2).

Source→Destination	***Rate***	***Information***
Wireless station 1 →Wired station 1	1.73 Mbps	2.08 Mbytes
	1.75 Mbps	2.11 Mbytes
	1.73 Mbps	2.08 Mbytes
Wireless station 2 →-Wired station 2	3.66 Mbps	4.39 Mbytes
	3.69 Mbps	4.44 Mbytes
	3.68 Mbps	4.43 Mbytes

To evaluate our traffic regulation mechanism, the manager forced the wireless station 1 to set up its data rate at 125 kbps. In this experiment, the regulation is not applied to the wireless station 2 to mimic that this station has higher priority traffic. The results are shown in Table 4. As it is shown, with the regulation, the wireless station 2 can transmit at a higher data rate and it runs at very close to the maximum data rate shown in Table 2.

Table 4. Maximum rate with our traffic regulation mechanism for communications between two sources (wireless station 1 and 2) and two destinations (wired station 1 and 2).

Source→Destination	***Rate***	***Information***
Wireless station 1 →Wired station 1	125 Kbps	168 Kbytes
	125 Kbps	168 Kbytes
	125 Kbps	168 Kbytes
	125 Kbps	168 Kbytes
	125 Kbps	168 Kbytes
Wireless station 2 →Wired station 2	5.27 Mbps	6.32 Mbytes
	5.24 Mbps	6.28 Mbytes
	5.26 Mbps	6.30 Mbytes
	5.31 Mbps	6.38 Mbytes
	5.27 Mbps	6.33 Mbytes

The last experiment consisted of testing the effects of injecting FTP traffic from wireless station 2 to wired station 2 (traffic not priority), and RTSP/RTP traffic from wireless station 1 to wired station 1 (priority traffic). We made the experiments twice: the former without traffic regulation mechanism , and the latter with it. To transmit the *Moving Picture Expert Group 4* (*MPEG4*) video with 2.992 KB size and 17 seconds duration, we used VideoLAN [16] as player and also as server. With both tests, we were concerned about the user experience.

When no traffic regulation was made for the FTP traffic, many video frames were lost and as as result, the user experimented intermittent playback and pixellation. On the contrary, when traffic regulation was applied, the reproduction quality improved a lot. Obviously, the duration of the FTP transmission was increased but it was worth.

IV. Conclusions and Future Work

In this paper we were concerced with the limited real bandwidth in WiFi networks. This is a handicap for multimedia applications that demand high throughput, e.g. video on demand. Our solution is based on an admission control mechanism in the AP and a traffic regulation technique via a manager/agent model among the AP and the wireless stations.

With our preliminary experimental results, we demonstrated that regulating the traffic of services with low priority for the benefit of the applications with higher priority such as the transport of video, it improved the user experience.

Many things remain to be done. We are thinking in developing a dynamic distribution technique for the bandwidth instead of being fixed to *B/3* for the not priority traffic and *2B/3* for the priority one, as we mentioned in section 2. On the other hand, the manager/agent model could be extended to consider agents in the wired network. With this approach, the source could be also in the wired network so under this scenario it is suitable to apply our traffic regulation mechanism. Finally, we are planning to consider a station with more than one type of traffic to transmit. In this case, the manager must fix different data rates for this station.

An important design element of our technique that must be improved is that any station can flood the PHY wireless channel scanning for the channel in which the AP is transmitting. A wireless station also can interfere trying to transmit although the AP limits its bandwidth. If a lot of wireless stations does this, a poor performance can be obtained. We think that it can be solved extending the number of elements of our software architecture. We can include a new element in the AP that will be in charge of detecting stations interfering in one particular channel. The AP then changes its channel to other non-overlapped one, but before doing it, it warms to particular agents to do it also. These agents are the only ones that are authorized to transmit, with the before assigned priority. The manager also informs the agents that are not authorized to change to the new channel, that the AP is communicating in the old channel. In this simple way the AP is not disturbed by the wireless stations that are not authorized to transmit.

References

[1] IEEE 802.11a-1999 (8802-11:1999/Amd 1:2000(E)), IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band.

[2] IEEE 802.11g-2003 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

[3] IEEE 802.11b-1999 Supplement to IEEE 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band.
[4] Jangeun Jun, Pushkin Peddabachagari, Mihail Sichitiu, "Theoretical Maximun Throughput of IEEE 802.11 and its Applications", *IEEE International Symposium on Network Computing and Applications (NCA)*, 2003, pp. 249-256.
[5] D. Marrero, A. Suárez, E. M. Macías, "Dynamic Interconnection of Ad-hoc Nodes Based on the Type of Service to be Accessed", *International Conference on Wireless Networks (ICWN)*, June 2005, pp. 539-545.
[6] D-Link Homepage, Available: http://www.dlink.com/
[7] PIEEE 802.11N (D2) Draft STANDARD for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications:Amendment : Enhancements for Higher Throughput.
[8] AppleTV, Technical specification, Available: www.apple.com/appletv/specs.html.
[9] IEEE 802.11e-2005, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements.
[10] CSWL: Extending End-to-End QoS to WiFi based WLAN, Available: http://www.cswl.com/whitepapers/qos-wireless-lan.html.
[11] Eduna, Available: http://www.e-duna.com/.
[12] Programming with pcap, Available: http://www.tcpdump.org/pcap.htm.
[13] Netfilter/Iptables Project Homepage, Available: http://www.netfilter.org/
[14] Linux Advanced Routing & Traffic Control, Available: www.lartc.org, http://tcng.sourceforge.net/.
[15] NLANR/DAST: Iperf 1.7.0 - The TCP/UDP Bandwidth Measurement Tool, Available: http://dast.nlanr.net/Projects/Iperf/.
[16] VideoLAN - Free Software and Open Source Video Streaming Solution for Every OS!, Available: www.videolan.org.