2008 Argentine Congress on Computer Science
(Congreso Argentino en Ciencias de la Computación - CACIC 2008)

Transmission voice over 802.11

Jorge García Guibout and **Carlos García Garino**
Instituto Tecnológico Universitario, Universidad Nacional de Cuyo, Mendoza, Argentina,
jgarcia@itu.uncu.edu.ar, cgarcia@itu.uncu.edu.ar

and

Antonio Castro Lechtaler and **Rubén J. Fusario**
Universidad de Buenos Aires and Departamento Sistemas, Facultad Regional Buenos Aires,
Universidad Tecnológica Nacional, Buenos Aires, Argentina
acastro@urn.edu.ar, rfusario@speedy.com.ar

Abstract

Developing countries are pervaded with scarcely populated rural areas. Under those conditions, providing broadband services with an efficient internet access at reasonable costs becomes a difficult endeavor. Thus, the answer lies on finding simple alternatives but different from those implemented in more developed countries. Some solutions applied in these cases involve the use of long range wireless technologies, such as: microwave, 802.11, WiMax, CDMA450, among others. Some of the features fostering these technologies include speed, simple installation, use of frequencies which do not require previous authorization, and, furthermore, the possibility to override local telecommunications operators. This article argues that 802.11 technologies are appropriate in those areas. It also analyzes their behavior when used over areas involving significant distances, with different requirements from those needed to cover populated cities.

Keywords: WLAN, 802.11, CSMA/CA, VoIP, TCP.

1. INTRODUCTION.

The current trend for increasing mobility has favored the appearance of technologies promoting user freedom of movement in any network. In this sense, for example, cellular phones constantly offer additional services such as SMS, MP3 downloads, Internet access, TV, and others.

Wireless users can move freely having the same services which are offered in wired networks. They can also connect to existing networks and travel freely through them. All of this is possible while maintaining upper-layer connectivity.

Currently, connectivity is accomplished even in situations as diverse as closed environments, offices, homes, campuses or even in remote places away from main or central buildings. If the signal received is greater than the associated noise, the range reaches over several kilometers. Frequently, the most relevant constraints have a direct relationship to the capabilities of the technology and infrastructure.

Once a wireless network is built, setting up the necessary base stations and external antennas, user growth becomes merely a configuration problem. The existing network does not need to be modified and there is no need for additional investment in equipment, as would be the case in traditional networks.

Wireless networks transmit signals using electromagnetic waves. The differences among the different technologies involve the wavelength of the signals. The most common operate in the range of infrared light and radio waves.

Infrared ports are common in current personal computers. However, an important constraint is a small coverage area and their tendency to suffer from blockage from obstacles like walls and furniture. In addition, solar radiation prevents their use in open spaces. On the other hand, radio waves are effective in wider areas, even in open spaces, and are not easily undermined by obstacles.

Thus, wireless products have shifted towards the use of radio waves, over products previously standardized by IEEE in its Work Group 802. This article will focus particularly in the 802.11 standard [1]. Currently, in developing countries such as India and Ghana [2], this technology provides Internet, data and voice services in remote populations, away from urban centers, with scattered population.

The framework of this article is based on *Community Private Networks* [3] in which last mile technologies for areas with low population density are studied, particularly broadband services.

The main objective is to integrate these communities to society by the provision of elementary communication services (telephone and data transmission) which would grant access to medical attention, education, internet and other services available in urban centers.

This article analyzes the behavior of this technology with a greater latency and heading if compared to wired networks standards for telephony and data transmission. In addition, signal propagation time problems are addressed, which tend to be greater to the waiting times for retransmissions.

Consequently, recommendations relating VoIP and associated protocols are studied. These protocols enable voice transmission over general data networks and over the 802.11 standard in particular.

MAC sub layer of the 802.11 standard is also explored to reference time recognition. Later, laboratory work and its results are presented. Finally, conclusions are laid out.

2. VOICE OVER IP (VoIP).

VoIP is not a service in itself, but a technology which encapsulates voice in packets to be transmitted over data networks, enabling communication with telephones. Furthermore, it can incorporate these packets to a single converging network used to transmit all types of communication data: voice, video, text, or any other type.

Networks must be able sustain all the features pertaining to telephony to be able to transmit VoIP, such as addressing, routing, and signaling. Addressing identifies the origin and destination of the call. Routing finds the best path from source to destination, making transmission efficient to obtain low latency. Signaling reserves and/or associates terminals and network elements to establish communication.

VoIP can work under several protocols. Two of them are Recommendation H 323 [4] from ITU and the Session Initiation Protocol – SIP [5], established by Internet Engineering Task Force (IETF).

H 323 enables not only VoIP, but also data and video exchange. This protocol, which can be placed in the application layer of the TCP/IP model, includes a series of standards for voice and video transmission. It relies on low level layer protocols from the TCP/IP model as shown in Table 1.

TCP/IP LAYER	ITU RECOMMENDATION H.323			
Application	Voice G.711, G.729, Video H.263.		Control Call	
	RTP	RTCP	RAS (H.225)	Q.931, H.245, (H.225)
Transport	UDP			TCP
Network	IP, RSVP, WFQ.			
Link	Ethernet, 802.11, etc.			

Table 1: Comparison between TCP/IP and H.323

Addressing: Registration, admission, and status – RAS communications protocol, Domain Name Service – DNS, resolution name in IP address.
Signaling: Q.931 initial calling signaling, H.225 call control (signaling, registration, and admission). H.245 control protocol for stream voice channel opening and closing.
Voice Transmission: Transmission over UDP packets with greater efficiency in bandwidth use than with protocols TCP or RTCP (Real Time Control Protocol) when considering packet timing.
Transmission Control: RTCP (Real Time Control Protocol) to detect network congestion and to take corrective measures.
Voice Compression: G.711 y G.723, and optional G.728, G.729, G.726

Both recommendations share protocols at the application layer (RTP, CRTP, RAS, Q.931), the transport layer (TCP, UDP), and layer 3 protocols (IP, RSVP). They also share digitalization and compression standards (codec), as depicted in Table 2.

CODEC	DIGITALIZATION AND COMPRESSION ALGORITHM	RATE IN KBPS
G.711	PCM	64
G.726	ADPCM	40, 32, 16
G.728	LD-CELP	15
G.729	CS-ACELP	8
G.729[a]	CS-ACELP	8
G.723	MP-MLQ	6, 3

Table 2: Codec used in VoIP [5]

Codec G.711 is used in public and private telephone communications and involves the delivery of a digitalized sample every 125 µs; thus having a low sample latency. In G.729 and G.723 codec’s, samples are stored for 10 ms and, only then, mathematical algorithms are applied to obtain the desired compression. Thus, it requires greater resources and processing time, deteriorating voice quality.

The laboratory experience sought to test the behavior of 802.11 equipment under requirements of data and voice transmission. With this purpose, in the case of VoIP, the codec's used were G.711, requiring significant bandwidth and compromising connection response speed, and G.729, which although requiring less bandwidth, relies on sample jitter for voice quality.

3. LINK LAYER: 802.11.

Standard 802.11 operates over several types of physical layers and controls user data transmission in the wireless media. It provides the operating framework and the interaction with the cable network. Furthermore, different physical layers offer different speeds. Sub layer MAC should be able to sustain them to allow interaction of the different technologies and/or physical media.

802.11 use ***Carrier Sense Multiple Access – CSMA***. However, it does not use collision detection (CSMA/CD). Conversely, it employs a protocol to avoid collisions named CSMA / Collision Avoidance.

The MAC sub layer delivers data units asynchronously, under a **best effort** method because it is a protocol not oriented towards the connection. Thus, it does not guarantee delivery. Broadcast and multicast transmission is part of the asynchronous transport service of the MAC sub layer. However, they can experience a lower quality service when compared to unicast data units due to the character of the wireless media.

The main access method of 802.11 is called ***Carrier Sense, Multiple Access, Collision Avoidance - CSMA/CA***. It is implemented in all stations: not only in LAN networks, but also in *ad hoc* topologies. The CSMA/CA protocol establishes that once the medium is confirmed available at a certain time, in this case equal or greater to DIFS (DCF Interframe Space), stations are to wait a random period of time, called ***Contention Window***, before initiating transmission. During this window, the medium remains available. Thus, it attempts to avoid collisions.

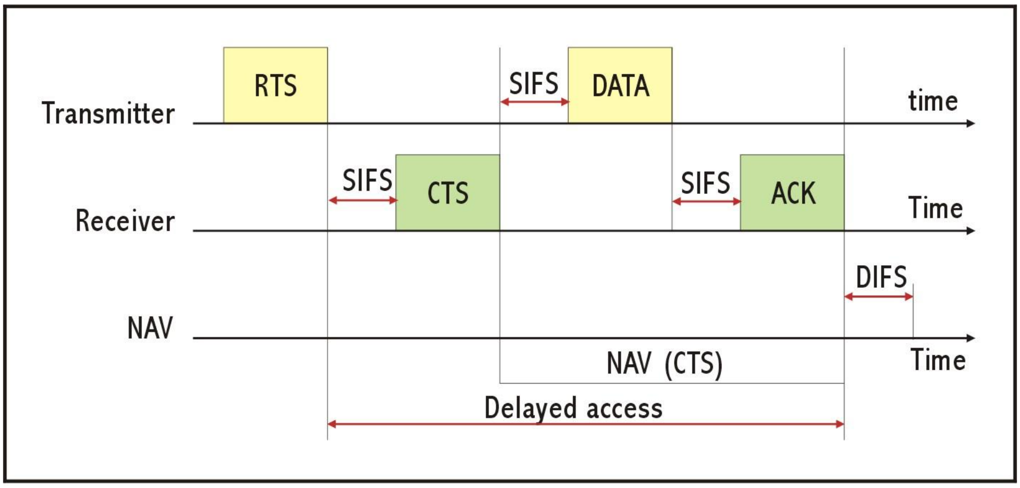

Figure N° 1: Virtual Census for NAV Carrier

Another way to avoid the possibility for collisions is to exchange short *frame of control* between transmitting and receiving stations, ***Request To Send – RT, and Clear To Send – CTS.*** When the medium is noisy, due to its own noise and the interference of other devices in the operating frequencies, the protocol establishes a positive recognition through an ACK frame to all traffic.

The only exceptions are multicast and broadcast messages which will not be required positive recognition.

Figure 1 shows that time periods between frames (the standard indicates them as the space between IFS frames) play an important role in the access to the transmission medium. As we have seen, stations delay transmission until the availability of the medium is ensured to avoid collisions.

If we vary times between frames, we can create different priority levels for different types of traffic. High priority traffic should not be delayed for long periods in securing medium availability. They are observed even among different transmission speeds.

With the use of RTS / CTS, if frames do not have the same length, congestion will be significant every time that a short frame is transmitted. Therefore, a frame size limit needs to be established. Beyond this threshold, RTS / CTS frame controls are used.

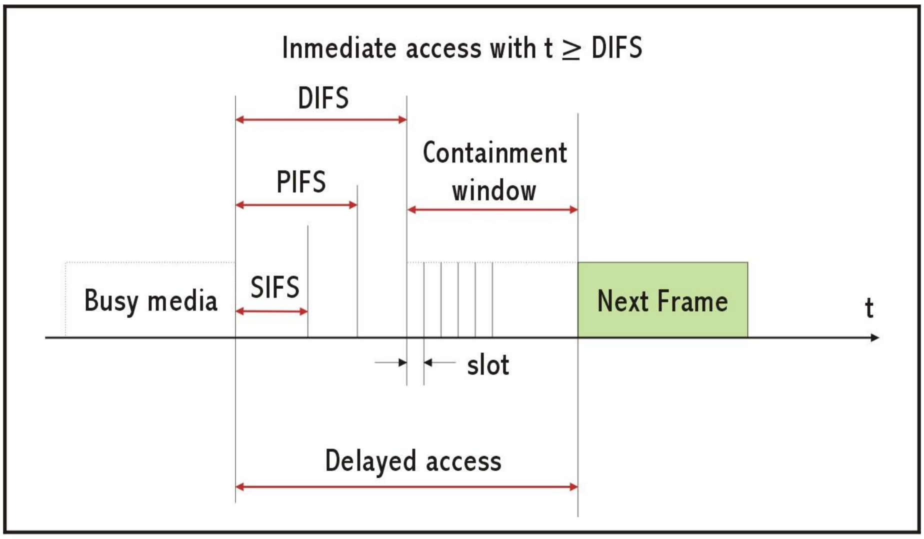

Figure N° 2: Interframe time relation

This technique is known as ***RTS threshold***. Although it can vary with each application, a standard value of 2346 bytes is the convention when using RTS / CTS. The possibility for transmitting two frames, one long and the other short, requires two counters which will increase every time transmission is attempted while the medium is busy.

Consequently, we must analyze two important aspects when links need to cover vast distances:

- ✓ ¿Could this technology be used for a VoIP service, given that 802.11 is not efficient for small packets and it also needs low latency for the service to provide good quality?
- ✓ ¿Which is the throughput of these connections if the ACK which must confirm the proper reception of the transmitted frames in 802.11 does not arrive at the expected time?
- ✓ ¿How does link 802.11 throughput affect the TCP packet transmission which must be identified by ACK, in this case?

In order to answer these questions, controlled tests were carried out in a laboratory where the conditions of a link using standard 802.11 were simulated.

4. LABORATORY TEST BANK.

A test bank was designed to perform the experiments.

The network architecture used is shown in Figure 3. The core of this architecture is a wireless network consisting of two Access Points, working under the 802.11 b/g standard. One of these points is configured as a bridge to the other. Connected to those AP, equipment and auxiliary networks complementing the test bank are placed. Both AP are D´Link, model DWL-2000 AP.

A Cisco 6000 Router is connected using Ethernet on the AP end that works as a bridge. The device has a Foreign Exchange Station plate – FXS, VoIP with two outlets where two analog phones are connected. The telephones are identified as extensions 54 and 56.

The other AP is connected to a LAN network, also using Ethernet. It includes a Cisco router model 1700 with a VoIP FXO plate.

Another analog telephone is connected to this card, identified as extension 24 of a central Eriksson switchboard, model BP 8/4.

A notebook with a telephone software emulator is used to study the use of mobile devices. It is also assigned an extension number.

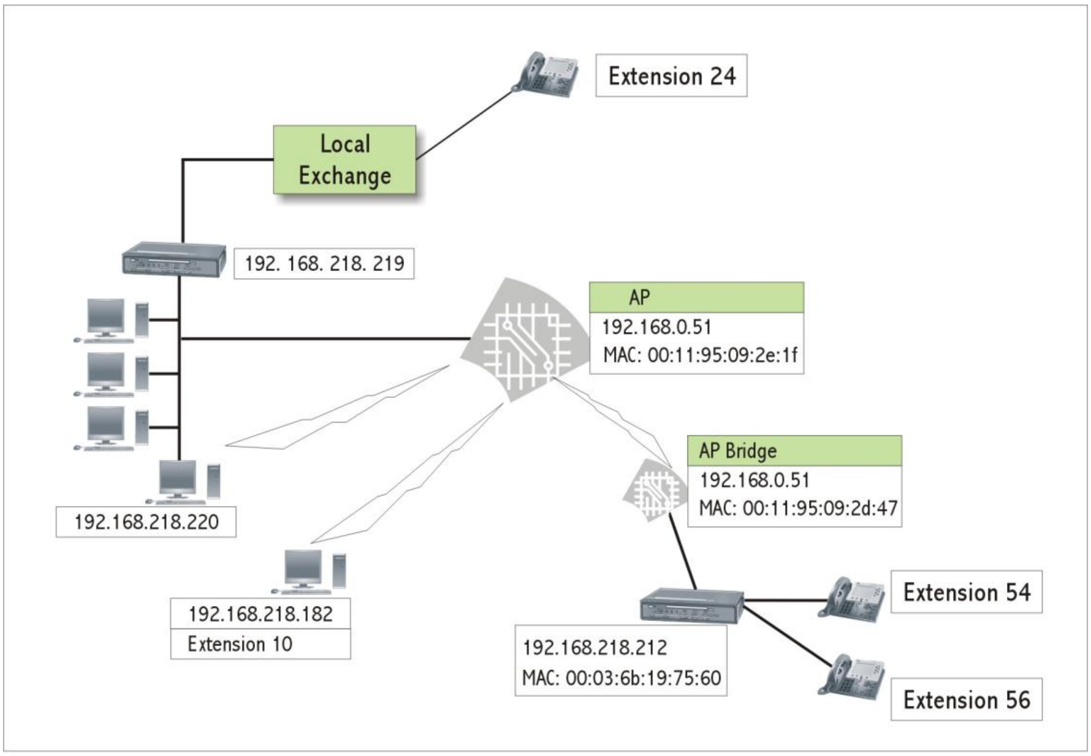

Figure N° 3: Diagram of Network 802.11 Assembled in the Laboratory

The notebook has a Linux OS and a D´Link DWL - 650 wireless card with all the requirements of standard 802.11b.

A PC with a WL-200 Compaq wireless network plate, configured in promiscuous mode, is used to capture traffic.

Its OS is Linux and Wireshark software, Version 0.99.6, is installed to capture traffic. With the appropriate configuration and software, wireless traffic was captured and analyzed during phone conversations and data transmission.

From the viewpoint of configuration and connectivity, the following IP addresses and configurations were assigned:

- ✓ *AP in mode AP*: original configuration, open authorization system. IP 192.168.0.50, RTS threshold in 2432, channel 6.
- ✓ *AP in mode Bridge:* Original IP address was replaced by 192.168.0.51 to configure a bridge through the IP protocol and to register adequately the MAC from the AP.
- ✓ *Router Cisco 1700*: address IP 192.168.218.219.
- ✓ *Router Cisco 2600*: address IP 192.168.218.212.
- ✓ *Notebook Compacq*: address IP 192.168.218.182
- ✓ *PC to capture traffic*: address IP 192.168.218.220.

5. TEST DESIGN AND RESULTS.

This section outlines the VoIP tests with the architecture laid out in section 4. Results are analyzed.

The tests used Codec G.711, detailed in section 5.1. The behavior of the MAC sub layer of 802.11 technology under VoIP traffic is analyzed in section 5.2. The next section studies the load introduced by the transmission layer.

5.1. Voice Tests.

Two simultaneous phone calls were established for the tests. The first one involved extension 54 of the Cisco 2600 router to extension 24 of the central switchboard. The second call connected extension 56, linked to Cisco 2600 router and extension 10 assigned to the notebook. Both cases used codec G.711.

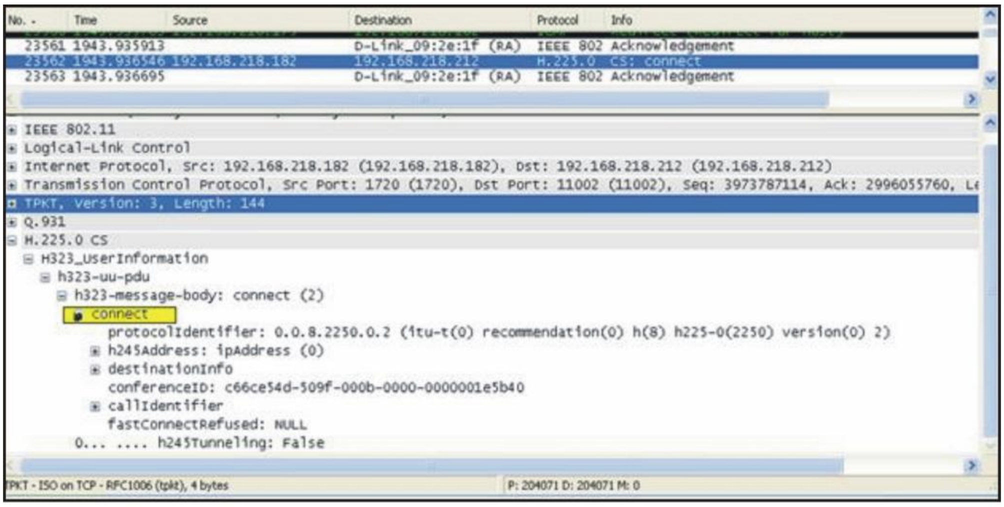

Figure N° 4: Obtaining H.225 Traffic VoIP in Extension 10 and 54

In both cases, the calls had excellent quality of voice.

The screen capture in Figure 4 details the traffic established between extension 10 (192.168.218.182) and extension 54 (192.168.218.212), and especially the H.225 protocol with the use of standard Q.931. Indicating the protocol as H.225.0 implies the call acceptance, confirmed by the term **connect,** highlighted in yellow.

The figure also shows that protocol H.245 is included which is informing the TCP port where the negotiation between the codec and ports UDP for RTP and RTCP is taking place.

Figure 5 is another traffic capture of the same communications. In this case, the RTP protocol works on UDP. In this packet, the codec corresponding to the usable load that transports, *Payload type: ITU-T G.711 PCMA*, is informed, making reference to the type of digital modulation and the data compression (in this case is Law A).

Timestamp can also be observed. It is the reference used to calculate the packets phase fluctuation, or jitter, due to network delays and the order of RTP packet arrival.

The figure also shows at the top of the image, in capture # 38625, the identification, ACK, by extension 10, identified by the notebook´s MAC of the wireless plate. There are no RTS and CLS packets because it exceeds the established limit by the KTS *threshold in 243*2 bytes.

A complementary test carried out consisted in making calls in the inverse path. The voice quality in this case was also excellent. At no time the voice broke off or the call got interrupted. It should be noted that signal levels were significantly above the AP sensibility levels.

During the voice experiments, a traffic overload was introduced, simulated through Ping packets between network machines, while maintain the call under the G.711 standard. At no moment a reduction in voice quality was noticed.

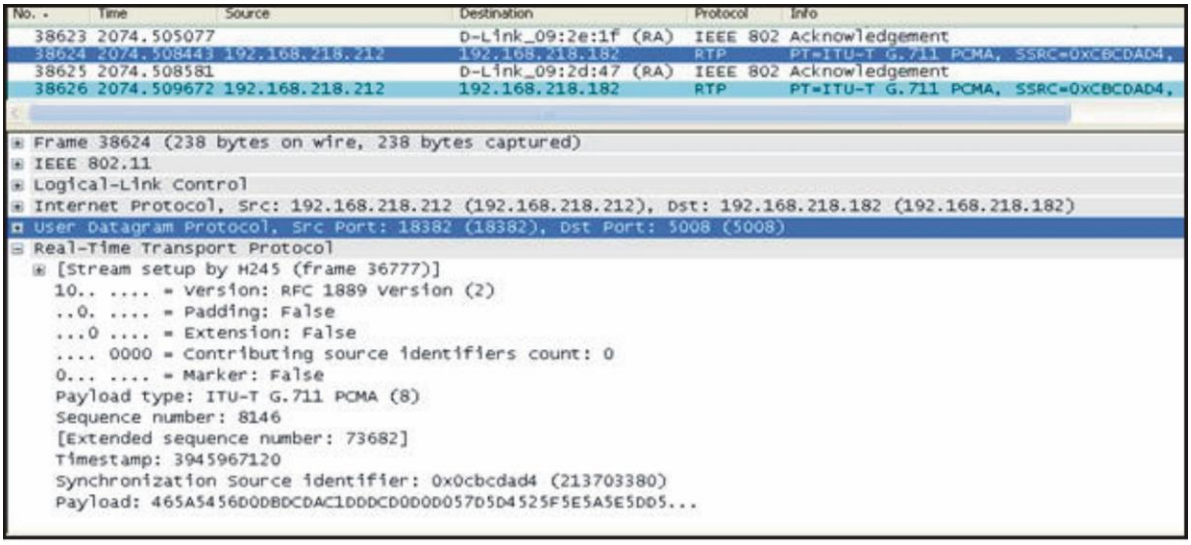

Figure N° 5: Obtaining Protocol RTP in Extension 10 and 54

The G.729 standard was used to analyze alternative codec behavior. A priori, good quality should be expected as the codec requires lower transference rates.

Communication between phones connected by router and switchboard, extensions 54 and 24 respectively, were of acceptable quality, taking into account the natural degradation from voice compression.

Incompatibilities between G.729 versions of the Cisco router OS and the phone emulator prevented from repeating the test of communicating the software emulator with the conventional phone. Future work in this area is intended.

5.2. Behavior of MAC sub layer of 802.11

As mentioned in the introduction, an area of interest is link behavior when distance delays ACK of the 802.11, originating retransmission and lowering the link´s throughput.

This task could not be carried out in the laboratory because lowering signal quality, with obstacles or dampeners, did not necessarily imply an increase of the signals´ traveling times or their identification. In order to further advance in this area and set up new test designs in this field under the framework of *Community Private Networks* [3] some features of the MAC sub layer are discussed.

Notice that ACK are transmitted after a period of time known as SIFS (Short Interframe Space). SIFs are the sum of other times which according to the 802.11 standard [1] are determined by the physical layer, depending also on the standards under use, 802.11b [7] or 802.11g [8], and defined by:

SIFS = RxRFDelay + RxPLCPDelay + MACProcessingDelay + RxTxTurnaroundTime.

Where,

- ✓ **RxRFDelay**: Nominal time (in µs) of the period between the end of a symbol received and the delivery of the data reception notice to the sub layer PLCP.
- ✓ **RxPLCPDelay**. Nominal time (en µs) taken by the PLCP physical sub layer to send a received bit from PMD to the MAC sub layer.
- ✓ **MACProcessingDelay**. Nominal time (in µs) taken by the MAC sub layer to treat and prepare a response for a frame.
- ✓ **RxTxTurnaroundTime**: Maximum period of time (in µs) that the physical layers require to change from reception to transmission at the beginning of the first symbol of the stream to be transmitted.

The terms of the SIFS time sum constitute primitives which define the standard and correspond to the communication times of the MAC and Physical layers, and RX and TX commutations times. The value varies between 10 µs y 30 µs in the different standards and according to the transmission speed. Thus, it indicates a maximum distance of approximately 5 kilometers considering the speed of light in free space.

Therefore, critical behavior is reached for distances greater than 5 kilometers. Field trials have been designed over links with a length ranging from 10 or 20 kilometers to test this conclusion. References have been found in the field to similar experiences carried out in other countries [2], yielding satisfactory results for links within the range of 5 to 20 km.

5.3. Results of the TCP layer.

A NetPIPE protocol (Network Protocol Independent Performance Evaluator) [9] was used to determine the behavior of the transmission layer, particularly the TCP protocol. NetPIPE is a tool developed to measure the communication performance between two network devices regardless of the protocol employed.

Size of Packet in bit	Thoughput in Mbps	Time of transfer in seconds
128	0.335721	0.00290885
512	1.248427	0.00312894
1021	1.028457	0.00757408
12285	2.224141	0.04214082
65533	4.900711	0.10202134
131075	5.000376	0.19998952
524285	2.166759	1.84606449

Table 3: Resulted of NetPIPE with Protocol TCP

NetPIPE sends a message which bounces several times between two nodes. In this way, the transmission time is determined for each message size. The size varies at regular intervals. Small disturbances are applied to complete the evaluation of the communication, including hardware and software.

Latency of small messages is obtained with this process, calculated as half the round trip time (RTT) for messages of up to 8 bytes and the throughput of a wide range of message sizes. Table 3 displays the results obtained for sent packets of different sizes. The link TCP level yielded a significant overload.

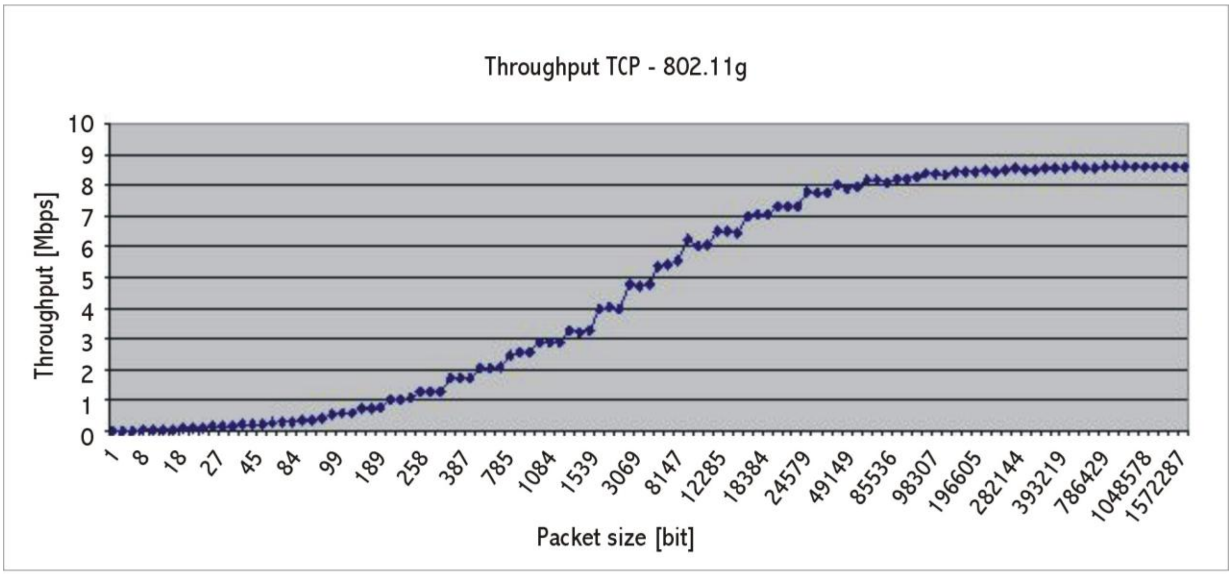

Figure Nº 6: Throughput in network laboratory

Figure 6 represents the results of Table 3. Protocol overload on the 802.11 bandwidth arises from the TCP ACK and the 802.11 headings.

6. CONCLUSIONS.

- ✓ Test results yield that 802.11 technology is suitable for, besides data transmission, the implementation of voice communication without quality degradation.
- ✓ In particular, favorable results were obtained with a low compression codec – G.711 – even with simultaneous traffic of voice and data. Future work should aim towards the analysis with greater depth of the use of other codec's, such as G.729.
- ✓ Link layer, due to the presence of ACK acknowledgements, significantly affect the throughput of the links, reducing effective transmission speeds to low levels in long distance cases, above 20 km.
- ✓ In this sense, field trials need to be carried out to determine the influence of other parameters; for example, the S/N relationship. It is also necessary to test in situ the performance between the endpoints of wireless links at different distances.
- ✓ Transmission layer penalizes significantly the theoretical throughput in 802.11 links. This result is valid not only to TCP but also UDP protocols.
- ✓ At the production links, transmission and link overloads are to be expected. They can even be simultaneous. Thus, further field tests and work proposals in the area become relevant.

7. ACKNOWLEDGEMENTS.

The financial support provided by Agencia Nacional para la Promoción Científica y Tecnológica and CITEFA (Project PICTO 11-0821, Préstamo BID 1726 OC-AR) are gratefully acknowledged.

8. REFERENCES.

[1] ANSI / IEEE Std. 802.11, Edition 1999. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification

[2] Lakshminarayan Subramanian, Sonesh Surana, Rabin Patra, Sergiu Nedevschi, Melissa Ho, Eric Brewer and Anmol Sheth, Rethinking Wireless for the Developing World.

[3] Proyecto PICTO 11-18621 *Redes Privadas Comunitarias*, FONCyT, ANPCyT. Director Antonio Castro Lechtaler, work in progress.

[4] Implementors' Guide for Recommendations of the H.323 System (Packet-based multimedia communications systems): *H.323, H.225.0, H.245, H.246, H.283, H.341, H.450 Series, H.460 Series, and H.500 Series*, July 2007

[5] Session Initiation Protocol RFC 3261, 2002. http://tools.ietf.org /html/rfc3261

[6] Jonathan Davidson and James Peters, Fundamentos de voz sobre IP, Cisco Press Publishers, 2001, ISBN: 84-205-3190-1

[7] ANSI / IEEE Std 802.11b-1999. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

[8] ANSI / IEEE Std 802.11g, Edition 2003. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

[9] Quinn O. Snell, Armin R. Mikler and John L. Gustafson, NetPIPE: A Network Protocol Independent Performance Evaluator, Ames Laboratory / Scalable Computing Lab, Ames, Iowa 50011, USA, http://www.scl.ameslab.gov/netpipe/paper/full.html

[10] Matthew S. Gast, 802.11 Wireless Networks, The Definitive Guide, O´REILLY Publishers, First Edition, 2002.

[11] Taif Everts, The Wireless LAN Book for Enterprise, editorial Trapeze Networks

[12] SDP (Session Description Protocol): RFC 4566, July 2006. http://tools.ietf.org/html/rfc4566
[13] Scott Keagy, Integración de Redes de Voz y Datos, Cisco Press Publishers, 2001, ISBN: 1-57870-196-1.