Network Communications Design to the Caranqui´s Parish Government´s Benefit

Carlos A. Vásquez, Edwin G. Túquerrez

Abstract—**This actual document discloses a communication network´s design process that provides wireless connectivity and computer services to the Caranqui´s Parish government, defining strategic places capable of covering the entire parish in order to provide internet services, computer security, voice and video transmission and most of all to reduce the digital gap in the Caranqui´s Parish.**

The study is based on a network consistent with a wireless technology WIMAX and available software alternatives to provide services such as: Firewall, VoIP, Video Streaming and Captive Portal.

Indexed Terms—**WIMAX, VoIP, WISP, MINTEL**

I. INTRODUCTION

Caranqui´s parish actually counts with 6 urban neighborhoods, 11 marginal urban and 7 communities. Within its entire territory 15 educational units, 2 private units and 13 public units have been established, besides having 13000 habitants or 3250 families approximately.

The parish has limited access to a network data base and internet due to the lack of infrastructure by the companies which provide these services through wired networks, lack of coverage from local WISP belonging to the city of Ibarra and high costs by the cellular companies.

The telecommunications ministry together with the Information society (MINTEL) through the Consejo Nacional de Telecomunicaciones (CONATEL) has current the TEL-534-CONATEL-2011 resolution to the legalization and implementation of *Redes de Acceso Universal de Internet* that provides a model allowing the fulfillment of the actual connectivity and computer services in need of the Caranqui parish.

II. BASIC CONCEPTS

A. WIMAX

The worldwide Interoperability technology to access by microwave defined by the acronym WIMAX is standardized by the IEEE 802.16-2009 in its accumulative document version. Its objective is to implement high-end fixed access wireless networks that allow a 70 Mbps transfer rate and a 50k coverage. [1]

Characteristics:
- It works with an adaptive modulation and codification (ACM) with the following medthos: BPSK—QPSK—16QAM—64QAM
- It supports TDD—FDD Duplexing
- Sets a médium Access protocol TDMA
- Multiplexing: OFM—OFDMA—SOFDMA
- It supports MIMO antennas
- It provides quality and service
- The frequencies used are defined according to the region / country where the technology is applied (see Table 1)

Table 1: Frequency distribution by region or country

Region or Country	Frequency bands for WiMAX
EE.UU.	2.3, 2.5 y 5.8 GHz
South and Central America	2.3, 2.5 y 5.8 GHz
Europe	3.5, 5.8 y 2.5 GHz
Southeast Asia	2.3, 2.5, 3.3 y 5.8 GHz
Middle East and Africa	3.5 y 5.8 GHz

Architecture
WIMAX Technology is based on the OSI reference model represented in 7 layers, it functions on the physical layer divided by 4 sub-layers and the MAC sub-layer coming from the data link is divided in 3 sub-layers (see figure 1).[1]
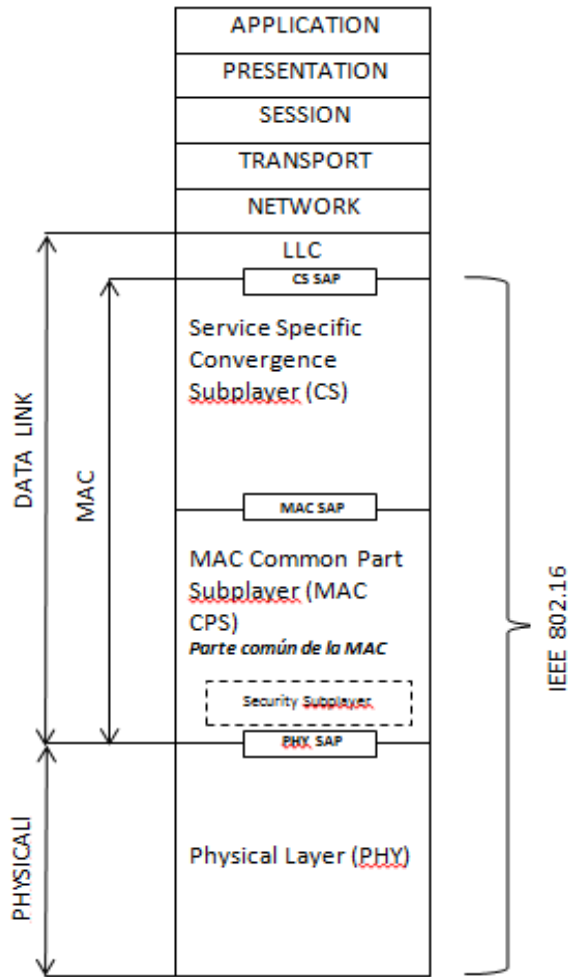
Figure 1: Architecture of IEEE 802.16 layers.
Source: IEEE Std 802.16 ™ -2009, IEEE, 29 May 2009.

Format weft MAC

IEEE standard 802.16 defines two types of wefts, GMH which is generic and the second one which is the headlong MAC without payload mainly used to favor broad band (BR).
WIMAX technology works mainly in the wefts´ headlong to provide the mentioned benefits by this standard (see Figure 2).[1]
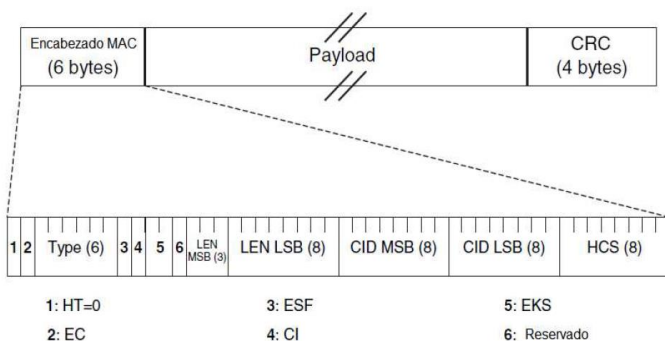

Figure 2: Format of the WiMAX frame.
Source: IEEE Std 802.16 ™ -2009, IEEE, 29 May 2009.

Description of each field from wefts heading (see Table 2)

Table 2: Description of the bits contained in the header of the WIMAX frame.

Bit	Description	Functions
1	HT (Header Type)	Indicates the frame type: 0 = (GMH) Generic Mac 1 = (BR) request bandwidth or Mac without payload
1	EC (Encription control)	0 = payload encrypted 1 = not encrypted payload
6	Type	Indicates whether special type of payload and subheadings
1	ESF (Extended Subheader)	0 = no sub header 1 = contains subheadings and activated GMH
1	CI (CRC Indicator)	0= no CRC 1= CRC
2	EKS (Encription Key Squence)	It is responsible for encrypting the payload of the frame only active if EC is 1
11	LEN (Lenght)	Length in bits of MAC PDU including the header and CRC
16	CID (ID Connection)	Shows connection identifier of frame header
8	HCS (Header Check Sequence)	detect errors in the frame header

B. Firewall

It is a tool that can be implemented in hardware or software or both which can allow, block, limit or decipher traffic within a computer network according to the implemented policies in its norms. [2]
There are two types of firewall which differ from filtering resources and the layer that works with the OSI reference:

- Packet filtering firewall
- Application layer firewall

Packet filtering firewall
This type of firewall works in network layers and transport through the filtration of networks and ports. According to the computers network's policies the needed norms and filters must be designed for its implementation. In order to design filters of this kind of firewall one must consider the two types of general policies:

- *Restrictive policy:* Everything is allowed only through the firewall rules
- *Permissive policy:* Everything is permitted except denials imposed by firewall rules

Application layer firewall
This kind of security works in layer seven named OSI Application model, which is commonly called Proxy. It main function is to filter content and applications throughout URL directions and Web sites within this layer's protocol rules and level.

C. Proxy

This is a network's element in the form or hardware or software which in Spanish is called "punto intermedio". Its functions vary depending on the network:

- Access control
- Traffic record
- Cache management

The web proxy's server main function is to filter HTTP AND HTTPS content in the www with a URL according to internal network's policies. At the same time there are external policies that form two basic web proxy servers:

Local Proxy: Servers are configured with internal policies and its application used for internal network requests. [2]

External Proxy: Policy servers for filtering external content to the intranet used especially for output Internet as external traffic to be filtered on their requests to internal servers. [2]

D. VoIP

This technology encompasses resources for the transmission and reception of voice signals through internet protocol. It starts by the sampling and modulation of a signal in order to switch from analog to digital. For the transmission of IP packets compression Codecs already specified for this technology are used and decompressing occurs when the packet gets to its final destination.

VoIP Standards

They are norms for the use of VoIP technology. Among the main ones are H.323 defined by IETF, the standard selection based on its own characteristics, function forms and mainly by the use of the service providing software.

VoIP Protocols
These are protocols created for voice transmission over data networks. They were made to minimize costs and optimize resources for this technology and to provide its main telephony service. The predominant protocol services at present are: H.233, SIP and IAX2. Both protocols H.323 and SIP are also considered standard in this technology. [4]

IAX2
(Inter-Asterisk exchange Protocol) this protocol is developed to work in IPBX centrals by the Digium company, and to work for Asterisk and its interconnection.

VoIP Architecture
In order to implement this service, the following items are necessary: terminals, VoIP servers and Gateway. These are also used in similar technologies.

Codec for VoIP
Its objective is to transform analog waves to digital. This method is useful to decrease broad band consumption due to information compression.

Most used Codecs in VoIP are (see Table 3). [4]

Table 3: Features for VoIP codec.

Codec	Bandwidth (Kbps)	License
G.711	64	No need
G.711.1		
G.722	64	No need
G.722.1	24, 32, 48	
G.726	16, 24, 32, 40	No need
G.729	8	No need
G.729 A		
GSM	13	No need
Speex	2.15 − 22.4	No need

E. Video Streaming

Streaming technology consists on web content diffusion in both voice and video throughout the content´s download and at the same time the reproduction of the same. These applications use a memory space in the local disk where the content gets stored. Applying live transmissions through web applications, radios and television are used as internet platforms and computer networks.

Streaming Protocols
To administer streaming, two protocols are considered: UDP utilized to avoid error correction because these are unpredictable and RTSP that distributes data control with TCP, voice data and video with UDP.

Codec for video streaming
Compression and decompression technologies is known by codec being that it is composed by two processes, one in the streaming and video transmission as well as voice transmission. [5]

Top codec in video transmission are characterized by:

H.264: It was developed by UIT-T, also known as MPEG1-4 Part 10 7AVC a licensed open standard which offers vast broad band efficiency compared to its predecessors and better error correction capacity. It allows faster speed and resolution. Its distribution is global due to gadgets´ developers have joined this protocol.

VP8: this is a codec developed by the On2 Technologies Company affiliated to Google Inc. It is applied to free software since its licenses are free. Its main characteristic is high interpolation performance in Sub-Pixels and to adaptive bucle filter to reduce broad band and speed video transmission.

F. Captive Portal

It is a web page predesigned and isolated in a server with the purpose of bringing computer network safety. It interacts directly with the user providing a user name and password. It supplies a view of the page initial content according to

network policies. It can also administer navigation times within the network and broad band for each user. [6]

This application is widely used in wireless networks or Hotspot which need open networks control to the general public. Its implementation can be in both software and hardware due to the varying functions and performance elements pertaining to the network.

III. REGULATORY ANALYSIS

Currently in Ecuador the administrative entities that regulate telecommunication sectors count with an organizational structure that answers to the Telecommunications Ministry and Information Society (MINTEL) and its annexes as showed in Figure 3. [7]
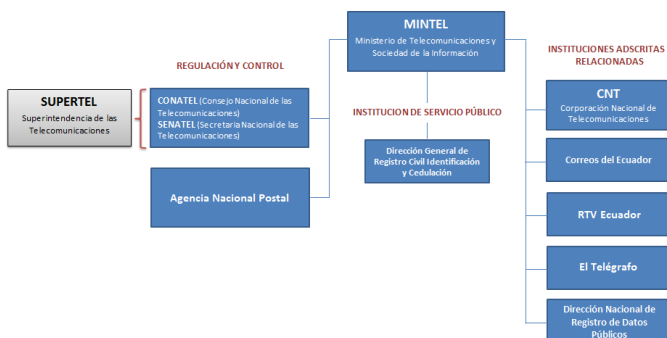

Figure 3: Organizational Structure of telecommunications in Ecuador.
Source: Ministry of Telecommunications (Mintel).

CONATEL is the entity that approves norms and regulations for the telecommunications sector and for this project Resolution TEL.534-CONATEL 2011 which provides an implementing model that regulates networks like the ones set in this project.

A. Resolution TEL-534-CONATEL-2011

This is a resolution that provides norms and regulations to Universal Access Internet Networks, its beneficiaries and entities that are able to implement these types of networks according to its definitions: [8]

B. Modulation digital broad band norms in Ecuador

For this study's implementation is necessary to exercise current laws in order to use the radio-electric spectrum in Ecuador. Its normalization is current according to Resolution TEL.560-18-CONATEL-2010 where the *norm for the systems implementation and operation modulation of digital broad band* exists.

C. Resolution 163-06-CONATEL-2009

This resolution presents a regulation over the shared use of both physical infrastructure and public and private businesses. It seeks to provide an administrative and technical procedure for the use of telecommunication towers through the compliance requirement by the company´s owner and this resolution.

IV. DESIGN

The proposed design for the Caranqui´s parish contemplates wireless coverage of all its geographical extension and the selection of points called computer centers where desktop computers and networking equipment is set up.

A. Computer centers selection

The 22 computer centers are based on the actual physical and electronic infrastructure capable of installing proper equipment. These have been strategically selected to prove services and coverage to all educational units, neighborhoods and parish´s communities. (see Figure 4).
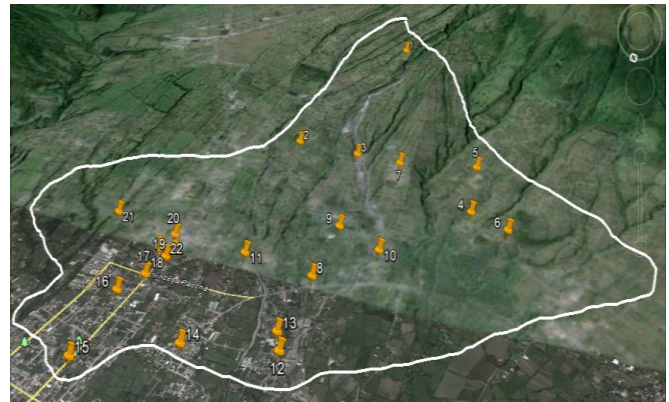

Figure 4: Points considered computer centers.
Source: Digital Maps Google Earth edited by Edwin Túquerrez.

Computer centers definition

The model for these centers is based on info centers that MINTEL installs. They feature 6 desktop computers, an IP telephone, a computer exclusively used to teleconferencing, additional computers, printer and whiteboards.

For the parish´s entire wireless coverage a strategic point was selected, it feeds the technical characteristics to set up network equipment. This point is the telecommunications tower belonging to CNT public enterprise located at Juana Atabalipa and Princesa Cory Cory (see Figure 5).

Figure 5: Structural CNT Tower.
Source: Caranqui's Parish

To demonstrate coverage from CNT´s telecommunications tower a simulation was made through software Radio Mobile to visualize such coverage from both the 22 points and from Caranqui´s Parish. This simulation is interpreted based on colors and dBm intensity that leads transmission signal. (See Figure 6).
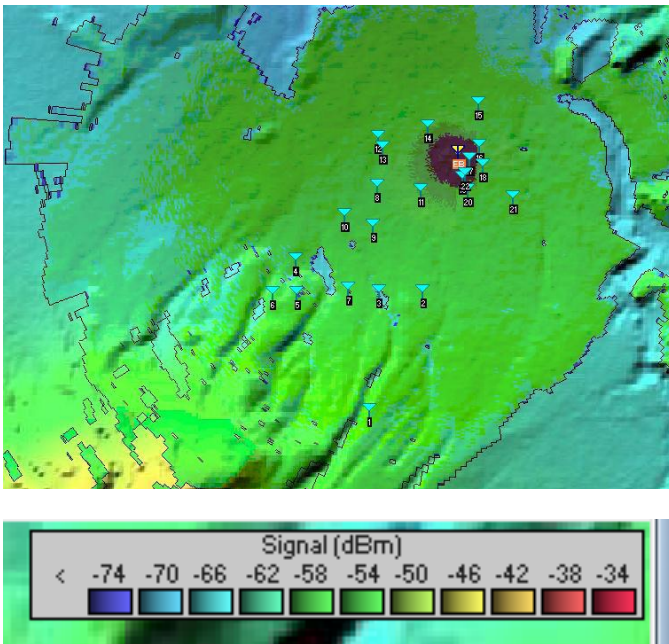

Figure 6: Simulation coverage CNT tower.
Source: Radio Mobile Simulator edited by Edwin Tùquerrez.

B. Design`s Architecture

Design´s planning is supported by a layered structured architecture (see Figure 7).

Figure 7: Architecture of the proposed design.
Source: Material Course Design of communication ninth level.

Electricity

In this sub-layer the characteristics and requirements that design demands were analyzed in order to improve the equipment´s functioning. This analysis was made in the 22 points harboring desktop PCs and networking equipment in addition to the place where servers are found.

Electronic requirements for the computer centers:

- Electrical Systems that provide a 110 VCA /220 VCA network averaging 10 percent with a 60Hz frequency approximately.
- Electric rush protection through finish boxes with a minimum taco braker of 20 amperes that hold up to 10 computers and communications equipment.
- Ground system through ANSI/TIA/EIA-607 norm under 5 Ω sizes.

For the center that will house servers, a UPS implementation must be included to the previous requirements depending on the number of equipment to be used and to the ground system. A galvanized tube destined to work as a pole to support antennas from each computer center must be included.

Furthermore, some civil works recommendations were suggested since certain issues were present that interfered with equipment installation. (see Figure 13).

Recommendations were:

- Ceiling installation
- Installation of glasses to Windows
- Lock installation for entering
- To do civil works and painting if necessary

Passive

Passive sub-layer covers infrastructure which will prove access to proposed services from the 22 computer centers. For its design speed transfer is required in each point and the distance between the tower and the distribution from each other.

To calculate transfer speed demand required by each point, the sum of transfer speed consumption of each destined device was made in the following way (see Table 4)

Table 4: Transfer Rate Requirement.

Description	Upstream	Downstream
5 PC = Internet	128 Kbps x 5 =640 Kbps	128 Kbps x 5 = 640 Kbps
1 IP Phone	64 Kbps	64 Kbps
1 videoconference	384 Kbps	384 Kbps
5 PC (Captive Portal)	128 Kbps x 5 =640 Kbps	128 Kbps x 5 =640 Kbps
TOTAL	1.728 Kbps	1,728 Kbps

Required speed by each computer center is 1.728 Kbps considering desk top computer traffic if the computer center is located within an educational unit, then its total networking demand would be of 21 Mbps.

Once distance and transfer speed is represented in a preliminary network design (see Figure 8), the equipment selected is to be used as clients Access Points in agreement with:

Access Points Requirements:

- It supports IEEE 802.16-2009 protocol and beyond
- Works with free bands 5.725—5,850 GHz
- Irradiated potency must not be over 1W (<=30dBm) in accordance with the country's regulations.
- It allows broad band channels of 20 MHz
- It allows scalability to add new users
- It allows transfer sped up to 21 Mbps symmetric
- TDD,FDD Duplexing
- OFDM (BPSK, QPSK, 16 QAM, 64 QAM) Modulation
- It can include an antenna or an N connector to sum sectorial 120º coverage

Client Stations requirements:

- It supports IEEE 802.16d protocol and beyond
- It works in free band 5.725—5,850 GHz

- Irradiated potency does not exceed 1W(<=30Bm) according to country's regulations
- It allows broad band channels of 20Mhz
- Duplexing TDD, FDD
- Modulation OFDM (BPSK, QPSK, 16 QAM, 64 QAM)
- It allows transfer speed up to 5 Mbps symmetric
- It can include an antenna or proved an N connector to sum a directive antenna
- It can work with other brands at the Base station.

With these requirements a device was selected from the Albentia firm, with PRO-BS 1150 model at the base station and model PRO-SU 1150 for client's stations. The same equipment was used for the Back haul link adding a directive antenna from the Ubiquiti company model RD-5G-30.

With equipment selection and network characteristics a 22 link simulation was made to software radio Mobil (see figure 9). Results were verified (see figure 10) to certify each link´s viability. Main results were: Fresnel first zone sensibility reception, antennas heights and links potency margin.
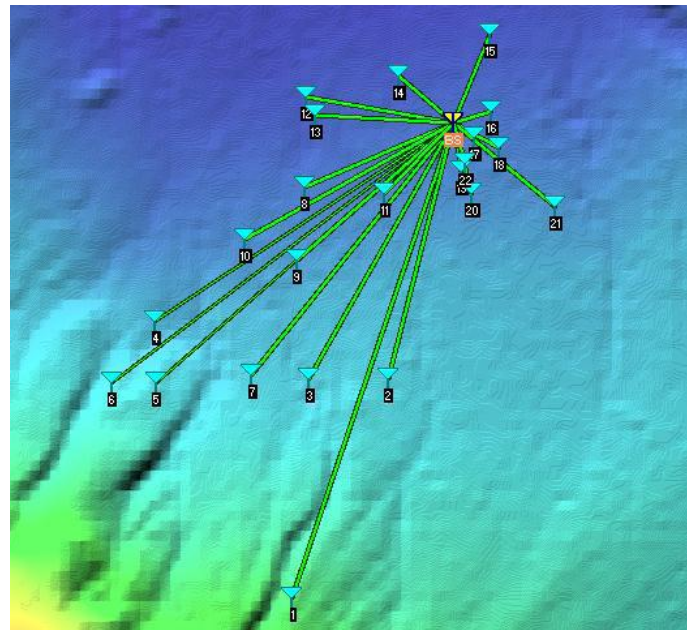

Figure 9: Simulation preliminary design.
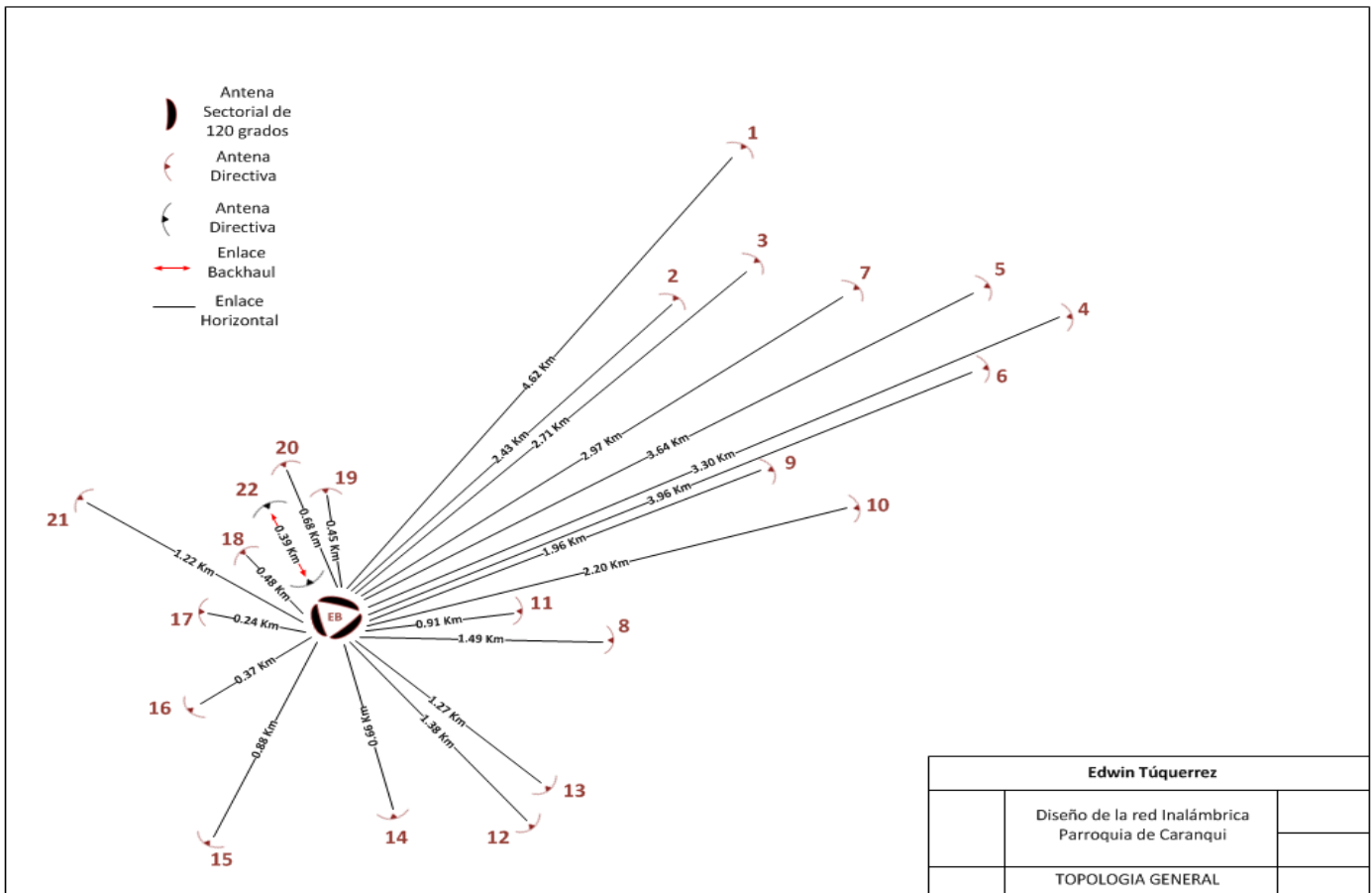Source: Radio Mobile Simulator edited by Edwin Túquerrez.

Figure 8: Preliminary design of the wireless network.
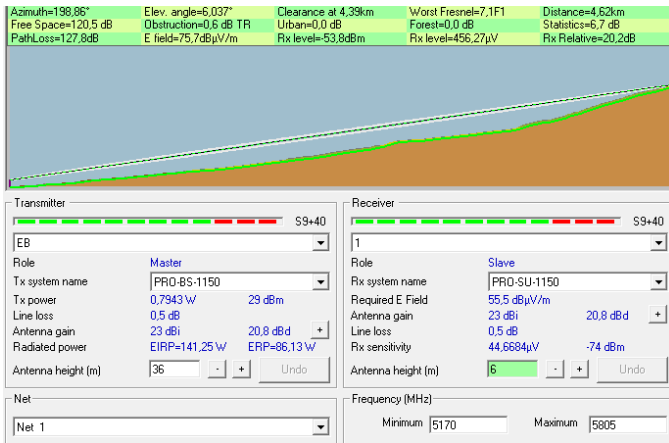Source: Compiled by Edwin Túquerrez.

Figure 10: Simulation results.
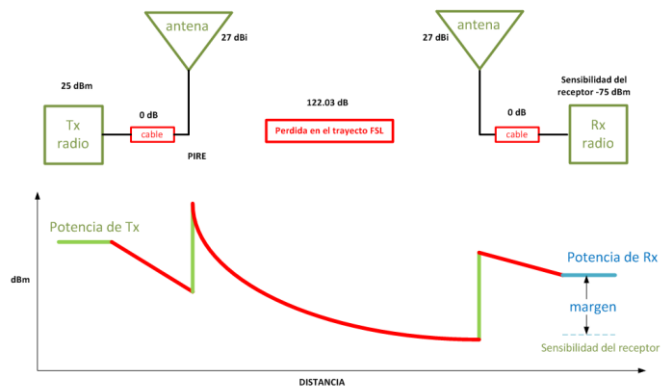Source: Radio Mobile Simulator edited by Edwin Túquerrez.

Figure 11: General scheme of power link budget calculation.
Source: Compiled by Edwin Túquerrez from link budget calculation.

For each links viability, the best results were verified which consists of reception sensibility through a mathematical model set up to the link, where the a loss and gain system sum was made (see Figure 11). It is then where the result is guaranteed not to be higher that the radio data receptor previous exposure to the link.

Active
During this sub-layer a network equipment distribution was made according to a ranking model implemented with the following layers: Nucleus, Distribution and Access

Nucleus

Equipment that shapes this stage will house services being that internet output and the Backhaul link. Such equipment is located at the Caranqui Parish board. This center has been assigned as a computer center as additional equipment has been stored to the end users. (see Figure 12).

Distribution

At this set sub-layer radio-linked equipment has been set to Access Point mode and are located at the distribution tower interconnected through a layer 3 switch. It also accounts for the radio-link equipment found at the 22 computer centers set on router mode (see figure 12).

Access

Access sub-layer is designated to end-users. The following design contemplated services for 6 desktop computers assigned by a layer 2 and an access point for reaching wireless equipment where captive portal service will be provided. (see Figure12).
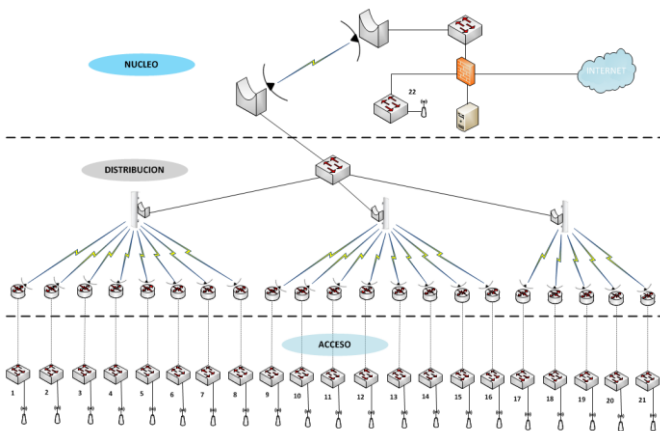

Figure 12: General diagram of the proposed network hierarchy.
Source: Compiled from design considerations..

Logical Addressing

Once equipment has been distributed and sub-networks are ready to be used, a sub-network assignment takes place within each computer center. Also a proper radio and services administration must take place (see Table 5). Consistent with the addressing:

- IPv4 Protocol
- Private Network 192.168.00
- Class C (255.255.255.0)
- Type of Logical addressing: without VLSM

With the sub-network distribution, an IP is added to each device for its set up and administration. General topology shows equipment and their IP assignation (see Figure 13).

Table 5: Distribution of subnets for each computer center.

	Networks	Subnet
1	Administration	192.168.1.0/24
2	Servers	192.168.2.0/24
3	Juan de dios Navas -Naranjito	192.168.3.0/24
4	Leopoldo N Chávez - San Cristóbal Alto - San Cristóbal de Caranqui	192.168.4.0/24
5	Manzanal	192.168.5.0/24
6	Turupamba – San Francisco de Chorlavi	192.168.6.0/24
7	Catzoloma	192.168.7.0/24
8	San Francisco de Chorlavisito	192.168.8.0/24
9	19 de Enero	192.168.9.0/24
10	Oscar Efrén Reyes - Ejido de Caranqui – Unión y Progreso	192.168.10.0/24
11	Chamanal	192.168.11.0/24
12	20 de octubre	192.168.12.0/24
13	Guayaquil de Caranqui	192.168.13.0/24
14	Agustín Cueva Dávila - Vista Hermosa – 10 de Agosto	192.168.14.0/24
15	El Naranjal	192.168.15.0/24
16	Yuyucocha	192.168.16.0/24
17	Olimpia Gudiño Vázquez - Cuatro Esquinas	192.168.17.0/24
18	Colegio Atahualpa – La Candelaria	192.168.18.0/24
19	José Nicolás Vacas	192.168.19.0/24
20	Avelina Lazo de Plaza – Simón Bolívar	192.168.20.0/24
21	Juan Miguel Suarez	192.168.21.0/24
22	Medardo Proaño Andrade - Unidad Artesanal de Caranqui - Bellavista de María	192.168.22.0/24
23	Santa Lucia del Retorno	192.168.23.0/24
24	Central	192.168.24.0/24

Once general topology is made, equipment comparison of technical characteristics and cost, the following bands are assigned for the design´s usage (see Table 6)

Table 6: Selected equipment to general design

| #	Hardware selected for the design
22	Access Point Ubiquiti Unifi AP (UAP)
22	Switch Mikrotik RB2011iL-RM
22	Radio y antenna Netkrom ISPAIR CPE 510
22	Phone IP GXP-2160
3	Radio y antenna Albentia (ARBA Pro)
1	Switch Ubiquiti EdgeRouter PRO ER-8
2	Radio Albentia (ARBA Pro)
2	Antennas Ubiquiti Rocket Dish Airmax
1	Switch Ubiquiti EdgeRouter PRO ER-8
1	Server IBM X3250M4
1	Server ML10HP Proliant
1	Rack Floor Beaucoup
22	Rack de Beaucoup
1	UPS APS APC Smart-UPS 750VA USB
22	UPS CDP G-UPR-506
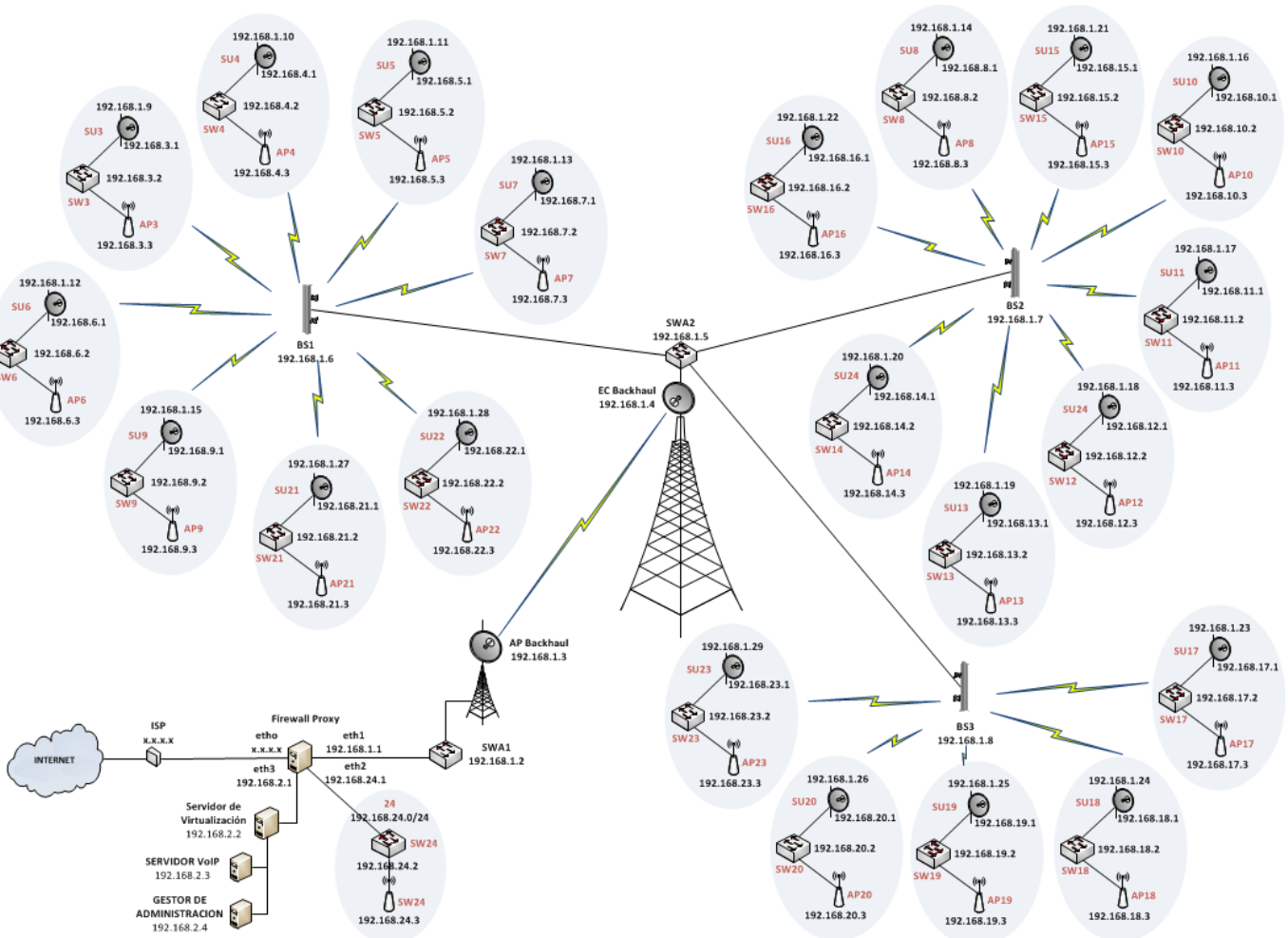
Figure 13: General Topology.
Source: Compiled from design considerations.

Applications

Firewall and Proxy

This project´s proposal is to have basic port input and output safety traffic control between internal sub-networks. As for inadequate or undue web pages access control is also included. The implementation of such services was made with Firewall and Proxy architecture (see figure 14). This model uses internal network devices LAN and Internet service to control ports and web content.

These services are based on network control internal policies, port control, and restricted configuration policies, denying access to all ports and opening only the necessary ones which Firewall is in charge of doing.

Traffic control from internal network to internet access is determined by the authorization of basic navigation ports (see Table 7), authorized traffic by user end is made by a firewall device that must be set up in this mode.
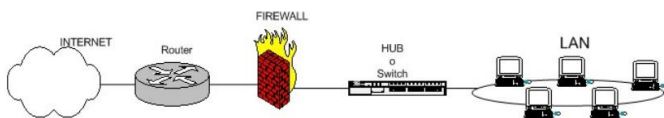

Figure 14: Architecture of firewall and proxy selected.
Source: Altadil P. (2008). IPTABLES Practical Manual. retrieved from http://www.pello.info/filez/firewall/iptables.html

Table 7: Traffic allowed from the internal network to external networks and internet.

Ports	Protocolo	Action	Description
443	HTTPS	Allow	The encrypted web browsing traffic is allowed.
80	HTTP	Allow	Web browsing traffic is allowed.
21	FTP	Allow	The file transfer is allowed
25	SMTP	Allow	Email transference is allowed.
110	PoP	Allow	Email transference is allowed.
143	IMAP	Allow	Email transference is allowed.

995	PoP3s	Allow	Email transference is allowed encrypted
993	IMAPs	Allow	Email transference is allowed encrypted
53	DNS	Allow	Traffic is allowed to resolve domain names
8 y 30	ICMP	Allow	Test traffic allowed basic connectivity table
Any	Any	Deny	Deny all other ports

Moreover implemented traffic control ports subnet from the server to the application of the proposed services (see Table 8).

Table 8: Traffic allowed from the server subnet.

Ports	Protocol	Action	Description
161	SNMP	Allow	Snmp traffic is allowed to manage network devices
5060	SIP	Allow	SIP traffic for the use of VoIP and Video Streaming is allowed
8 y 30	ICMP	Allow	Test traffic allowed basic connectivity table
Any	Any	Deny	Deny all other ports

For control of web content rules is performed based on a permissive policy which allows everything except content that does not bring to the community (see Table 9), these functions requested in the Proxy design handles.

Like the firewall proxy server must be configured in transparent mode for the user.

Table 9: Control of Web content.

Content	Action	Description
Adult	Deny	Inappropriate content
Quotations	Deny	Inappropriate content
Entertainment	Deny	Inappropriate content
Games	Deny	Inappropriate content
Ads	Deny	Inappropriate content
Violece	Deny	Inappropriate content
Drugs	Deny	Inappropriate content
Piracy	Deny	Inappropriate content
Any	Allow	Appropriate content

In order to satisfy the needs of these type of settings, a hardware and software comparison was made to include the use of a ML10HP Server Poliant with Endian Firewall Software 2.5.2 that contains two functions from Firewall and Proxy requirements.

VoIP Service

This VoIP service provides voice service through IP network to all computer centers already defined. For the implementation of this system will be used with SIP port 5060 TCP and UDP because it is highly modular and flexible.

For is architecture an extension of this service has been assigned for each computer center. To provide this service is necessary to use a codec G.729 due to its better performance and low broad band consumption.

Once the previous characteristics have been approved, a general diagram (see figure 15) regarding server´s position designated to provide VoLP and final user device.
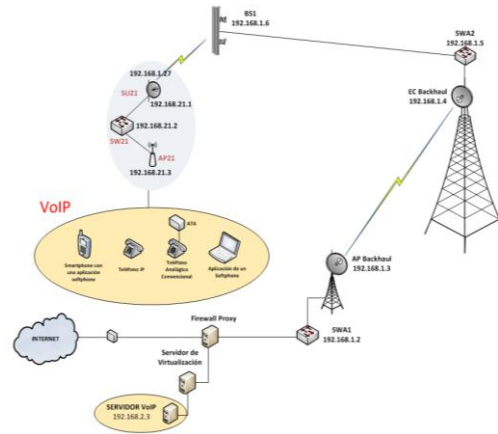

Figure 15: Architecture of the VoIP service.
Source: Compiled from the design requirements.

Hardware and software selection was based on design demand. IBM X3250M4 server hardware was established to virtualize services. The software that qualifies is Elastix 2.4.0 which provides this service through selected protocols and codecs specifications, even an IP GXP-2160 telephone was assigned to each computer center.

Streaming Video Service

This type of service was planned and its main purpose is the video transmission between computer centers. Applying the architecture and VoIP service the extensions had already been designated.

SIP protocol will be used complying with RTP protocol to perform Streaming technology. H.264 codec is selected because of its free software applications required by its design.

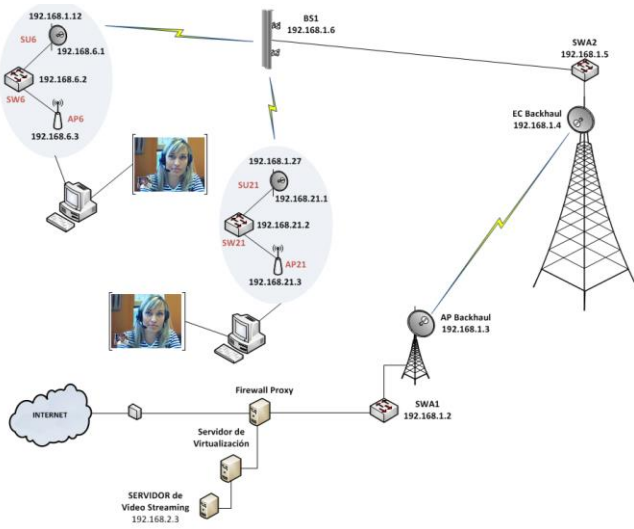In order to perform this service a server is shown in the following diagram (see Figure 16)

Figure 16: Video Streaming service architecture.
Source: Compiled from the design requirements.

The server will be virtually implemented and the software that provides VoIP server Elastix2.4.0 complement themselves. Both hardware and software will be utilized between both services, final computers will be implemented with multimedia peripherals such as microphones and web cameras

Captive Portal

This service will provide user information at the final WiFi zone that has been already implemented in each computer center. The architecture to be set up for this service at the computer switch access (see Figure 17)
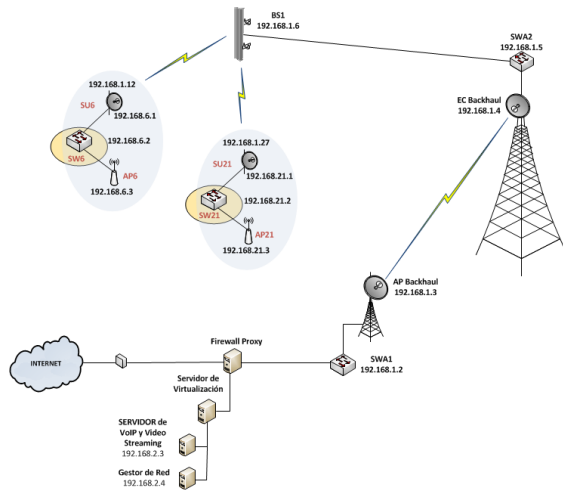

Figure 17: Architecture of the service of the captive portal.
Source: Compiled from the design requirements.

Hardware such as Mikrotik RB2011 iL-RM and internal Router OS system will be used where the Portal captive will be set up.

Presentation design belonging to the captive portal was made in KompoZer software version 0.710 where an information page will be implemented. One can look at the network security policies, its functions and administrator network information for user recommendations and suggestions. (see Figure 18)

Figure 18: Information Page for the Captive Portal service.
Source: Compiled from the design requirements.

I. COST BENEFIT

A cost benefit analysis was made with a total cost of 48.479 of the proposed equipment according to local enterprises estimate. A second cost analysis was made that would include only internet service based on the SAITEL company including design requirements. The final result from only internet service for each computer center was 195,000 USD for a 5 year service.

The following data analyses a cost benefit formula:

$$CB = \frac{Beneficio - Contrabeneficios}{Costo}$$

Equation 1: Formula cost benefit
Source: Leland Blank, Anthony T. (2006). Economic Engineering. McGrawHill. Mexico.

Internet –only payment service from a private institution: 195,000 USD
Cost (Propose expense): 48,479 USD
Against: 0 dollars
Benefits: 195,000-48,479,521 USD

$$CB = \frac{146,521}{48,479}$$

$$CB = 3,02$$

It was determined that a 3.02 positive benefit cost is considered acceptable being that the benefits to be obtained are greater that the cost if only internet service installation is provided by a private company.

Beneficiaries

Direct and indirect beneficiaries are students from a variety of schools with 2595 students from a pre-primary level, primary and secondary levels within urban and rural zones. Services to 228 students will be provided for the urban area and 11 in the rural zone according to official Ministry of Education data.

Computer centers assigned to provide services to the parish will cover in their totality all habitants, Caranqui counts with an estimated 13000 people or 3250 families who will use the predicted networks directly and indirectly.

II. CONCLUSIONS

Caranqui's Parish is composed by 6 urban neighborhoods from which only the central neighborhood has access to an internet unit and out of 11 marginal urban neighborhoods do not count with any internet access at all. Besides the 11 government schools, 7 of them already count with internet access, but 4 of them do not have this service.

WIMAX Technology 802-16-2009 standard complies with requirements demanded by the network´s design at the Caranqui's Parish since it supports transfer speed of 70 Mbps and has a 50 km coverage which utilizes 5.8GHz frequencies appropriate for Ecuador.

The TEL-534-CONATEL-2011 resolution allows the implementation and legalization of the network´s model adequate and proposed by the parish, it also utilizes TEL-560-18-CONATEL-2010 resolution for equipment selection. For working frequencies resolution 163-06-CONATEL-2009 refers to the communications tower from the public company CNT which is already installed was a coverage point to the entire Caranqui's Parish.

The 22 points are contemplated in the design count on defined computer centers for each point. Only one distribution point for wireless networks and the brand used for the proposal is Albentia with its ARBA Pro. Line. Proposed services use free software in the case of Firewall. Proxy uses Endian Firewall 2.5.2 VoIP and Video Streaming applies Elastix 2.4.0 software, finally captive portal was tested and used Mikrotik Router OS.

The suggested services look at scenarios where firewall with input and output port traffic control among networks and sub-networks, web control using proxy, voice and video transmission and captive portal set up to supply a user information webpage from the 22 points of the design.

Cost-benefit analysis yields positive value of 3,02 according to its formula that shows the project's economic viability. Moreover, the network will furnish services to 11 schools including 2595 students, 228 teachers in the urban zone and 11 in the rural area, again it benefits 24 neighborhoods and communities that include 13,000 habitants or 3,250 families approximately.

REFERENCES

[1] IEEE Standards Store. (2013). Estandar IEEE 802.16-2009. Recuperado de: http://www.techstreet.com/ieee/products/vendor_id/4184.
[2] Tanenbaum A. S. (2011). Redes de computadoras quinta edición. Estados Unidos. Pearson.
[3] Altadil P. (2008). IPTABLES Manual Práctico. Recuperado de http://www.pello.info/filez/firewall/iptables.html.
[4] Foro VoIP. (2014).Comparación de Códec y protocolos para VoIP. Recuperado de: http://www.voipforo.com/codec/codecs.php
[5] Enseñar es aprender dos veces. (2013). VP8 Vs H.264. Recuperado de: http://aprendiendo2veces.blogspot.com/2013/05/vp8-vs-h264.html
[6] Slideshare. (2014). Trabajo de investigación: "Portal Cautivo". Recuperado de: http://www.slideshare.net/valericio1/portal-cautivo
[7] Ministerio de Telecomunicaciones y Sociedad de la Información. (2014). Valores, Misión, Visión. Recuperado de: http://www.telecomunicaciones.gob.ec/
[8] Consejo Nacional de Telecomunicaciones. (2011). Resolución-TEL-534-14-CONATEL-2011.
[9] Consejo Nacional de Telecomunicaciones (2010). Resolución-TEL-560-18-CONATEL-2010.

Carlos A. Vásquez A.

Born in Quito - Ecuador, on September 19, 1980 Engineer in electronics and telecommunications form the School Polytechnic National (2008), Currently, teacher of the Electronics and Communication Network Engineer Career Universidad Técnica del Norte Ibarra - Ecuador, graduate master degree in communication network of the Pontifica Universidad Católica del Ecuador, Quito-Ecuador.

Edwin G. Túquerrez I.

Born in Ibarra, Ecuador, on December 31, 1987. Daughter of María Elena Túquerrez Ipiales. She studied in "technological institute 17 de July". She studied Electronics and Communication Network Engineer at the "Universidad Técnica del Norte", Ibarra-Ecuador.