TECHNICAL UNIVERSITY OF NORTH

ENGINEERING CAREERS IN ELECTRONICS AND COMMUNICATION NETWORKS

THEME:

REDESIGN AND OPTIMIZATION DATA NETWORK SECURITY PERIMETER FOR SELF-GOVERNMENT DECENTRALIZED SAN MIGUEL DE URCUQUÍ

SCIENTIFIC REPORT IEEE

AUTHOR: MORÁN VELASCO JONATHAN MARCELO

DIRECTOR: ING. FABIÁN CUZME

IBARRA, 2016

REDESIGN AND OPTIMIZATION DATA NETWORK SECURITY PERIMETER FOR SELF-GOVERNMENT DECENTRALIZED SAN MIGUEL DE URCUQUÍ

J.M. Morán
jonathanmarcelomoran@gmail.com

Abstract- This paper titling is redesigning the data network and optimizing the security perimeter "Decentralized Autonomous Municipal Government of San Miguel de Urcuquí" (GADMU), was started gathering information on building infrastructure main (GADMU) on the horizontal wiring, vertical wiring, telecommunications room, work areas, grounding in order to determine the status of the network. access and core collapsed with which the new network structure, each layer with the respective configurations for troubleshooting issues: broadcast domains, failures physical link, traffic control between a hierarchical model based on two layers was then used departments, the use of these switches (CISCO WS-C2960-24-TD / C2960-48-TD) and (WS-C3750X-24-PS) was determined. In addition to microsegmentation it was made by VLANs and VLSM was used to distribute based on the number of users, which is intended to improve network management IP addresses. To verify operation GNS3 the respective simulations with which it is intended to validate the settings made demonstrating its operation is performed. An analysis of risks and vulnerabilities was conducted by MARGERIT JUNIPER methodology and equipment for perimeter security was determined. By ISO / IEC / IEEE 29148 standard operating system for FTP and SQUID PROXY servers is determined. In the benchmark cost-benefit analysis, a recovery period of 6 months and approximately 5 days was determined.

I. BACKGROUND

A. Problem

There have been problems of certain officials accessing files that do not correspond departments and review the information and manipulate important documents; the finance department is the most committed because of information that should be confidential.

In GADMU data network, you have a delay in solving problems, such as in the search for a point of damaging network; due to poor record of them, it occurred because of the lack of a physical mapping; thus causing dissatisfaction not only the workforce in the GADMU, but also to the citizens of San Miguel de Urcuquí Canton, visiting the premises in search of a service and is not available.

Likewise, the lack of a scheme of IP (Internet Protocol) address, has caused that services and network resources are in the same range and anyone entering the internet service to access restricted resources such as printer, scanner among others.

Similarly, the growth of the network has resulted in a low yield due to the infrastructure of switches cascade that have been placed to solve the problem of scalability, this has resulted in low availability, waste of resource bandwidth, storms broadcast, among others.

Another issue is the sharing of information; it takes through the network, so employees of the company with a broader knowledge networks, easily manipulate this information, replacing the IP of your personal computer by IP who want to hurt gained easy access to resources for these reasons disruption of the network is very easy for both internal people and external conduct tampering.

And finally the social entertainment networks by civil servants during working hours causes an inadequate underperforming in their business activities.

B. Justification

The realization of this project will be done in order to contribute to the social development of the company's San Miguel de Urcuquí Canton, making the direct beneficiary is the citizen, to receive an improved and efficient service from the areas that are linked directly with them, thus fulfilling the mission and vision of the Technical University of the North.

The logical project redesign and implementation of servers based on free software, will help the GADMU to decreased time on solving problems in case of failure, with the help of labeling and physical mapping; plus security flaws on stored data is correct, so the chances of damage occurring information will decrease, perimeter security will be optimized according to the needs of departments, avoiding excessive use by unauthorized personnel setting pages; problem of network downtime will be corrected by a hierarchical model, meaning that damage to a part of the network does not cause damage to the entire network. Performance will be improved by eliminating unnecessary traffic on the network, ensuring that employees and citizens are satisfied with the service offered to the provision of efficient services.

In the project by using a diagram of the network will help to solve as quickly as possible when a problem arises network downtime, VLAN'S also be held so that the data do not cross between departments, preventing eliminate important information. In addition to separate networks into 3 levels, the network will be easier to design, implement, maintain and scale the network, makes it more reliable.

Implementing a Squid proxy server help manage access from the Internet to the private network, blocking websites that distract employees of the institution, allows the network administrator to keep out of the private network to non-authorized users. The FTP server is a protocol for file transfer between computers connected to a TCP (Transmission Control Protocol Transmission) based on client-server architecture so that from a client computer we can connect to a server to download files from the system or to send our own files regardless of operating system used on each computer,

with the knowledge gained in the race solution to the problem will, facing obstacles and problems that this presents to us, in addition to acquiring new experiences and knowledge that will enhance my skills and job performance.

II. THEORETICAL FOUNDATION

A. What is a network

[1] He states that "A telecommunications network is installed a set of technical means, organized, operated and managed in order to provide remote communications services" .

B. Network topology

“A topology is defined as the physical or logical map of a network to exchange data “[1]. The physical topology is based on the way how the computers are connected, including some types are: bus topology, star topology, ring topology type, among others. The logical topology of a network is the way computers communicate through the media, the two most common types of topology are broadcast topology, topology by transmitting tokens.

C. Transmission method

“The transmission medium is the channel for transmitting information between two or more terminals. The transmission is performed by means of an electromagnetic signal propagating through the channel. Sometimes for transmitting a physical channel is used or guided and sometimes that is not unguided. “[2].

D. OSI reference model

The ISO (International Standards Organization) proposed a model reference adaptive to all computer systems, systems hosting this architecture "open systems" are called, and these allow communication with other systems. In Figure 1 it is shown as OSI reference model is divided into seven layers.

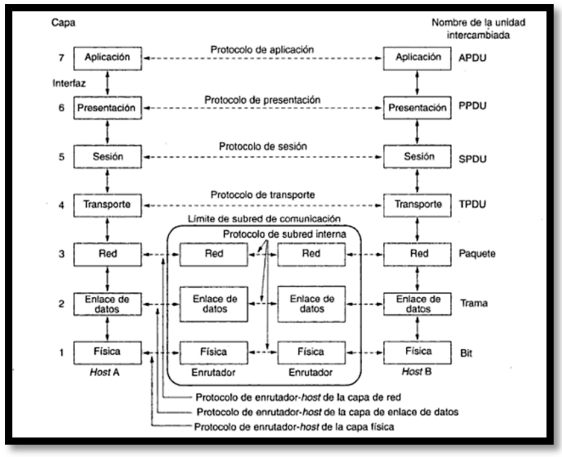


Figure 1. OSI Reference Model

Reference: [3]

E. TCP/IP MODEL

This model is the most commonly used today, the same logic handles the OSI model, in Figure 2 the layers of the two network model is displayed.

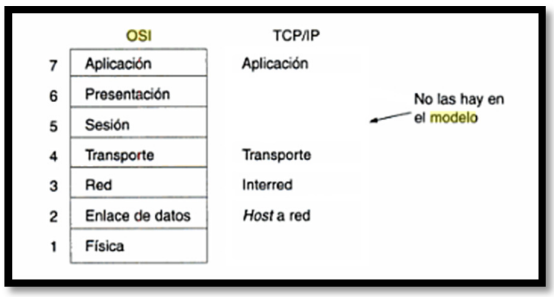


Figure 2. Reference models TCP / IP

Reference: [3]

F. Fundamentals of building a LAN

A structured cabling system is one of the fundamental parts of any building as it supports applications like voice, video and data, becoming the basis for the operation of all systems, being one of the vital parts of the network. It is important to note that the structured cabling systems have an approximate duration of 10 years so its design must allow and facilitate future changes or additions to the network, taking into account a proper planning for growth on the current network.

G. Perimeter Security

[4] Mentions that the data security are studied within, to and from a computer network is the main concern of a network administrator, so you should implement security methods to prevent attacks, intruders and information can disrupt the proper functioning of the network, perimeter network security.

H. Definition of perimeter security

“The perimeter security bases its philosophy on the protection of all computer system of a company from" outside " that is composing a shell that protects all sensitive elements of attack within a computer system. This implies that each transmitted packet traffic must be dissected, analyzed and accepted or rejected based on their potential security risk to our network. “[5]

I. Types of vulnerabilities

Vulnerabilities, are also referred to as weaknesses that can affect or cause risks regarding safety concerns among some vulnerabilities are: natural, physical vulnerabilities of hardware and software, storage media, human, among others.

J. UTM (Unified Threat Management)

[6] Claim that “UTM or Unified Threat Management is a set of features designed to provide application-layer inspection of traffic across a network. As in the intrusion detection and

prevention (IDP for its acronym in English), the safety devices that support features UTM decrypted and inspected the upper layer protocols to detect malicious traffic or simply not recognized. "

III. ANALYSIS OF THE CURRENT SITUATION

This chapter provides the information gathering network in the Autonomous Municipal Government Decentralized San Miguel de Urcuquí (GADMU) with its topologies (logical and physical) and current teams to have a clear idea of the current state of the network, they should be considered in areas such as: structured cabling, network equipment status, among others.

A. Survey of information telecommunications room

In Figure 3, the cable is displayed on the ground without any protection, in addition to these energy sources are in operation, causing performance degradation of the network.

Figure 3. Room structure telecommunications cabling

Reference: Own Photography.

In Figure 4, two patch panel 48 ports, these distribute structured to different departments GADMU wiring, is observed this indicates how the cables are accumulated without complying with the ANSI / TIA / EIA -569 -A standard , indicating how to structure the cables in a telecommunications room .

Figure 4. Patch panel 48 ports located in the telecommunications room

Reference: Own Photography.

In Figure 5, the state of the rack, which is located in the telecommunications room and contains two patch panels, a cisco router 881 and network cables (Category 5e) accumulated on the floor, without any protection indicated affecting availability of the network.

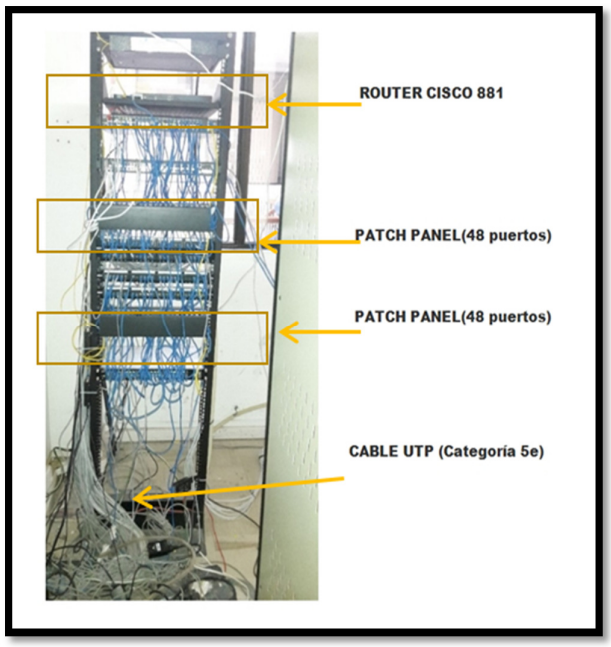


Figure 5. Rack located in the equipment room front view

Reference: Own Photography.

In Figure 6, the network cables is observed without plastic cover and tangled with power lines, causing instability network service in the department of drinking water.

Figure 6. Structured cabling in the department of drinking water

Reference: Own Photography.

B. Gathering information for structured cabling

The horizontal subsystem, vertical subsystem, equipment room, work areas, grounding system: gathering information in structured cabling for the following items were considered.

1. Information gathering horizontal subsystem

The horizontal subsystem runs from the work area to the telecommunications closet. In the GADMU the following information was obtained:

- The building does not have a horizontal subsystem.
- The installation was performed by drilling the floor to give internet service to each work area.
- The vast majority structured cabling is Category 5e UTP cable. Departments in revenue, income and computer systems, installed category is.
- Do not use products to guide the network cable to the respective work areas.
- No metal trays to prevent damage to network cables.

2. Lift the vertical subsystem information

The main function of telecommunications closet is to concentrate all terminations horizontal recognized by the standard cable. In the GADMU the following information was obtained:

- In the building does not have a vertical subsystem.
- The cable is crossed to other departments through holes drilled in the wall.
- The vertical subsystem was installed Category 5e cable.
- The backbone links do not have any protection along its route.
- No vertical ladders is used to guide the network cable to the telecommunications room.

3. Lift telecommunications room information

The telecommunications room should be able to accommodate telecommunications equipment, cable terminations and associated interconnecting wiring in the GADMU the following information was obtained:

- National Telecommunications Corporation provides Internet service, which arrives via fiber optics to the telecommunications room.
- has a main rack containing two patch panel to accommodate data cables, also contains an ODF (optical fiber organizer) which provides internet service to CISCO 881 router and router Mikrotik routerboard 750, which is connected to two cisco switch SG 200-50.
- Contains a cabinet where two HP PROLIANT nonoperating E5649, each computer servers are housed with their UPS (Uninterruptible power supply) these are locked and administered only by the head of systems area.
- It has no security for access to telecommunications room, it is handled only by a simple lock.
- has a ventilation equipment is damaged.
- Contains a case for housing electric cables and is in poor condition. It has two fluorescent lamps, not suitable for work.

4. Gathering information from workspaces

Are the spaces where users' desktops are located and are common places for employees. In the GADMU the following information was obtained:

- In 40% of the work areas, the network points are in poor condition. For installation of network points in the work areas ANSI / EIA / TIA 568B standard and labeling thereof is in most areas of work, except in the new network points that were recently installed dealt.
- In the departments of audit, finance, public works network points are not flaceplate.

5. Gathering information network Internet

The transmission speed is 12 MHz upstream and 16 MHz downstream.

CNT provides active network equipment such as cisco router routerboard 881 and 750 that route data to the respective departments which are connected to the switch SG 200-50 and distribute these internet service departments operating in the GADMU.

6. Information gathering subsystem grounding

It has a centralized system grounded by a copper rod which is located buried in the outer building GADMU.

C. Active teams

Then the active equipment found on each floor of the facility, of which some are in use and others are not presented.

1. First floor

In Figure 7, the existing equipment specified on the first floor detailing: their brand, description and status.

QUANTITY	ACTIVE TEAM	BRAND	DESCRIPTION	STATE
2	SWITCH	D-LINK DES-1024D	24 ports 10/100 Mbps	OPERATIVE
1	WIRELESS ROUTER	TP-LINK	2,4 Ghz - 802.11 a/g	OPERATIVE
1	BIOMETRIC	WALDSO		OPERATIVE

Figure 7. Active teams on first floor

Reference: Prepared

2. Second floor

In Figure 7, the existing equipment specified on the first floor detailing: their brand, description and status.

QUANTITY	ACTIVE TEAM	BRAND	DESCRIPTION	STATE
1	SWITCH	D-LINK DES-1024D	24 ports 10/100 Mbps	OPERATIVE
1	SWITCH	CISCO	SG 200-50	OPERATIVE
1	ROUTER	CISCO	CISCO 881	OPERATIVE
1	TRANCEIVER	HUMANITY	10/100 BASE –TX & 100 BASE FX CONVERTER	OPERATIVE
1	ROUTER	TRENDNET	TK-409	OPERATIVE
1	ROUTER	MIKROTIK	ROUTERBOARD 750	OPERATIVE
1	SWITCH	HP 5130	SERIES SWITCH JG934	NO OPERATIVE
3	UPS	TRIPP-LITE	APC 1500VA 120 W	NO OPERATIVE
1	UPS	SMART UPS	APC 1500VA 120 W	OPERATIVE
1	ROUTER	D-LINK	2,4 Ghz - 802.11 a/g	OPERATIVE
1	UPS	APC	BACK UPS PRO 1500	OPERATIVE

Figure 8. Active teams on first floor

Reference: Prepared

With the gathering of information on the second floor information it was obtained servers in Figure 9, each team explains its mark and its function meets in the Municipal GAD of San Miguel de Urcuquí.

QUANTITY	ACTIVE TEAM	OS	DESCRIPTION	STATUS	FUNCTION
1	HP	CENTOS 5.5	PROLIANT E5649	NO OPERATIVE	PROXY
1	HP	CENTOS 6.5	PROLIANT ML170	OPERATIVE	EMAIL
1	HP	CENTOS 6.5	PROLIANT ML170	OPERATIVE	WEB

Figure 9. Servers in the equipment room

Reference: Prepared

3. Third floor

In Figure 7, the existing equipment specified on the first floor detailing: their brand, description and status.

QUANTITY	ACTIVE TEAM	BRAND	DESCRIPTION	STATE
1	SWITCH	D-LINK DES-1024D	24 ports 10/100 Mbps	OPERATIVE

Figure 10. Active teams on third floor

Reference: Prepared

D. Network topology scheme

The scheme of network topology, is divided into two parts: physical and logical.

1. Logical topology

The logical topology is GADMU Ethernet bus type, since all devices are connected by the same means.

In Figure 11, logical features that was obtained from the collection of information is explained.

TECNOLOGIA	VELOCIDAD DE TRANSMISION	TIPO DE CABLE	DISTANCIA MAXIMA	TOPOLOGIA
100BaseTX	100 Mbps	Par trenzado(Cat. 5e UTP)	100 M	Estrella-Full Dúplex(Switch)

Figure 11.Logical characteristics

Reference: Prepared

2. Physical Topology

It is based on extended star topology since all switches are connected to a central node in Figure 12, GADMU physical topology is displayed.

.

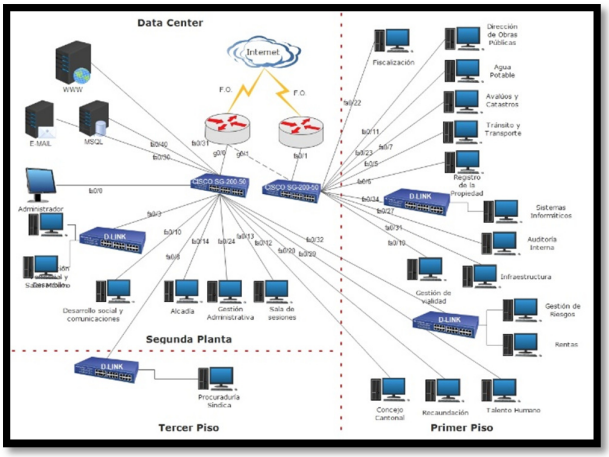


Figure 12. *Physical topology diagram*

Reference: Prepared

E. Buildings plans

To get an idea of the location of departments and network points, the planes was developed in AUTOCAD. In Table 1, the symbols used specified points corresponding to network and structured cabling.

Table 1. Symbols used in structured cabling

SYMBOL	MEANING	# OF POINTS NETWORK
△	POINTS NETWORK	100
|	STRUCTURED CABLING (Cat. 5e)	

Reference: Prepared with information obtained from the main building GADMU

In Figure 13, the plane of the first floor is shown with its respective location of network points.

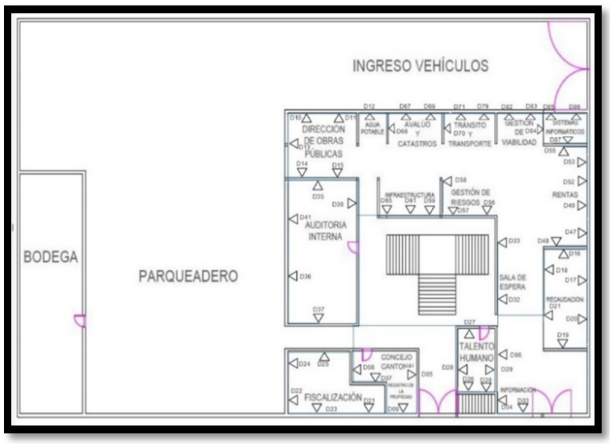


Figure 13. Flat on the first floor of the main building

Reference: Prepared with information obtained from the main building GADMU

In Figure 14, the plane of the second floor is shown with its respective location of network points.

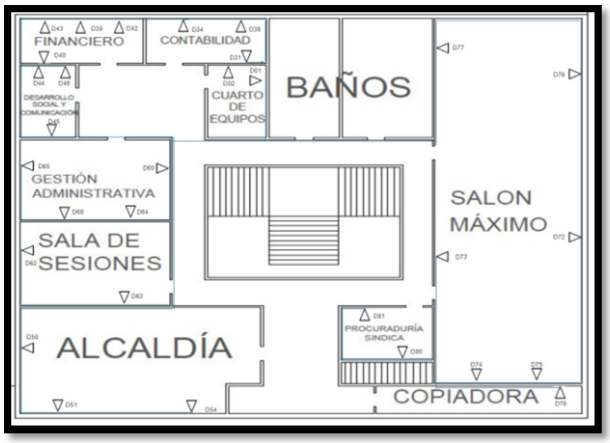


Figure 14. Flat on the second floor of the main building

Reference: Prepared with information obtained from the main building GADMU

In Figure 15, the plane of the second floor is shown with its respective location of network points.

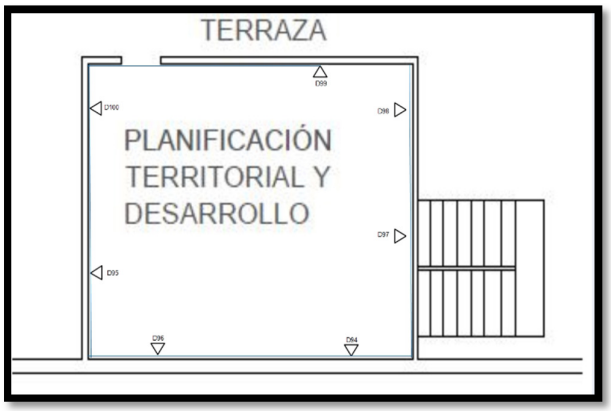


Figure 15. Flat on the third floor of the main building

Reference: Prepared with information obtained from the main building GADMU

IV. REDESIGN LOGICAL DATA NETWORK

In this chapter the logical network redesign data GADMU is made by important aspects such as:

- The projection of growth of the network.
- Access to applications for each network point.
- Sizing of network equipment and the new proposal.
- Topologies logical and physical.

It's based on the hierarchical model and jointly for checking the simulation tool is used GNS3 networks as it complies with similar functionality to switches to choose respective settings are then performed.

1. Block diagram

In Figure 16, the process is indicated for the redesign of the data network, in which the steps for the development of the project indicated.

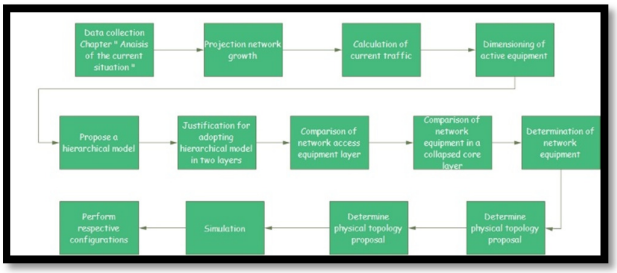


Figure 16.Block diagram to follow

Reference: Prepared

2. Study of the growth forecast

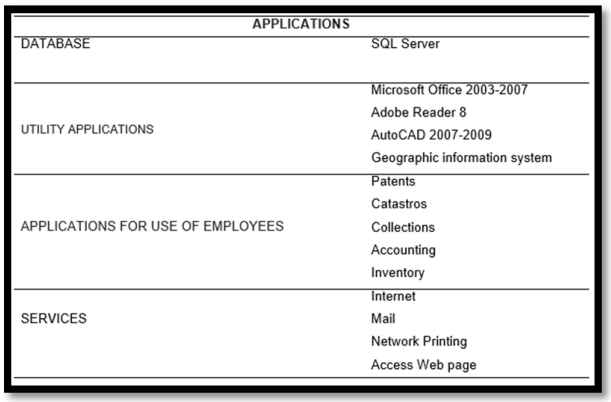
According to information provided by the Department of Systems , through the network administrator the engineer in charge of systems, in the GADMU there is no staff growth , as the number of jobs is fixed and most workers have been fixed passing of the years. But the use of TIC`s demanded installation has points without any network planning, infrastructure GADMU affected.

It is estimated that next year an increase of approximately 148 network points, this growth is for network equipment:

- Servers
- Computers
- Printers,
- Scanner, etc.

3. Access Application

Each new point network is installed in the institution, should have access to each application that the institution provides, in Table 17 applications that are operating in the GADMU is displayed .



APPLICATIONS	
DATABASE	SQL Server
UTILITY APPLICATIONS	Microsoft Office 2003-2007
	Adobe Reader 8
	AutoCAD 2007-2009
	Geographic information system
APPLICATIONS FOR USE OF EMPLOYEES	Patents
	Catastros
	Collections
	Accounting
	Inventory
SERVICES	Internet
	Mail
	Network Printing
	Access Web page

Figure 17. Applications for each employee

Reference: Prepared

A. Calculation of traffic and internal external services provided by GAD Municipal Urcuquí

For calculating traffic it is considered the following services provided by the GADMU: email, database, file downloads, web pages. In Table 2, all data obtained from earlier estimates for traffic (internal) for each user is explained.

Table 2. Current traffic demand

INTERNAL SERVICES	INDIVIDUAL CAPACITY (KBPS)	CAPACITY 125 USERS (KBPS)
Email	0,22	22,20
Database	0,11	11,11
Internet downloads information	62,27	6.226,60
Access to web pages	45,55	4.555,10
Total	108,15	10.815,01
Mbps total	0,11	10,56

Reference: Prepared

In Table 3, all calculations performed above, which indicates a (external) traffic for each user is explained.

Table 3. Total calculation of internal services

INTERNAL SERVICES	INDIVIDUAL CAPACITY (KBPS)	CAPACITY 125 USERS (KBPS)
Email	0,89	111,00
Internet downloads information	68,27	8.533,25
External total	69,15	8.644,25
Internal total	108,15	10.815,01
Total	177,30	19.459,26
Mbps total for each employee	0,17	19,00

Reference: Prepared

B. Dimensioning of active equipment

Active equipment sizing determines us the amount of network equipment to be used in the access layer, then a summary is:

Table 4. Requirements for access layer

REQUIREMENTS	VALUES
48-port switches	1
24-port switches	1
Switches for reasons of contingency	
Speed to workstations	100 Mbps
Speed up -link ports to the core layer	
Switching capacity	1 Gbps
	13,6 Gbps

Reference: Prepared

C. Network Redesign

This item redesigning the data network for the City of San Miguel GAD Urcuqui, which is divided into two parts explained: physical and logical; for the physical model involves two layers (collapsed core and access), which will be outlined indicating the function of each layer; and the logic part scheme creating VLANs with their respective addresses for each arises.

To determine the type of network equipment used, an analysis of current traffic calculation with which the bandwidth needed by each employee of the institution which is [0.17 Mbps] is determined is performed. With these calculations dimensioning for access layer, thus the number of switches each access layer, in Table 22 minimum requirements (a summary that must meet each access switch to be used detailed) needed is determined is performed. After analyzing all these parameters we proceed to choose network equipment to be used, making a frame where brands that offer network equipment are compared.

Finally, the design is simulated in the GNS3 program in order to verify the operation.

D. Justification of the model in two layers

(Domíguez Limaico & Gordillo Pasquel, 2006) has mentioned: "The structure of interconnection network to be designed, based on the hierarchical model proposed by CISCO Systems, so the teams that make up the section of" backbone "or" Core "they must have sufficient switching capacity (backplane) able to support the requirements of the network to be designed also provide redundancy options.

In the distribution section, it controls and monitors the network traffic, plus security and authentication of registered users is implemented; depending on the size of the network, he can integrate with section backbone in one team. "

The model will host two layers (access and collapsed core) as the number of employee with the City of San Miguel de GAD Urcuquí is small.

By mixing the two layers of a layer is removed in the hierarchical model, this layer called the collapsed core is compacted into a single robust equipment, which will solve all the problems of the poor performance of the network referred to in Chapter 3; it is considered that the institution's main

disadvantage is the economic deficit, so this model is perfectly suited to the needs of GADMU.

"There are now switches high capacity which integrate Ethernet, Fast Ethernet, 1 Gigabit Ethernet UTP and fiber interfaces and 10 Gigabit Ethernet optical fiber, the same that achieve switching at high speed." (Domíguez Limaico & Gordillo Pasquel, 2006).

For the project FastEthernet switches (100 Mbps), this analysis is in this chapter in item (4.3) sizing for access layer switches need. And a summary of the parameters that need access layer shown in Table 4.

(Domíguez Limaico & Gordillo Pasquel, 2006), mentions: "Currently there are switches that handle layer 2 and layer 3 to layer 4 (transport layer) called multilayer switches. With this type of equipment can be deployed securities such as restricting MAC addresses, IP addresses and logical port's transport layer, by way of a cortafuegos (firewall). To redesign switches layer 2 and layer 3 is used.

In Figure 18, a physical topology proposed in which it is divided into two layers (access and collapsed core), one can see that in the layer of collapsed core two network equipment, a main computer and a secondary are indicated (redundancy), it is recommended to use the computer a redundant institution if the main computer fails, the other team comes into operation and the network remains operational.

In addition it is observed that access switches are connected to the collapsed core switches through interfaces 1 Gigabit uplink so these teams will need: 2 Gigabit uplink ports to 1 for each of these for future applications.

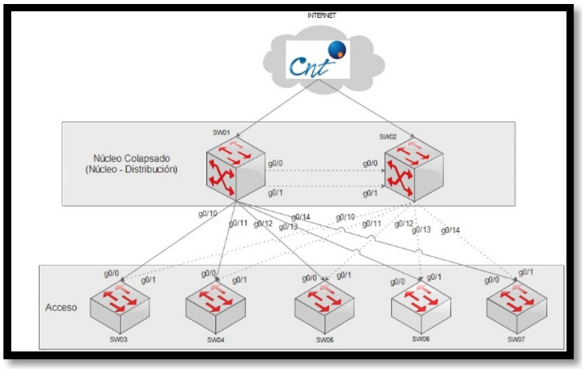


Figure 18. Proposed for the physical network

Reference: Prepared

1. Configuration collapsed core layer

For the collapsed core layer configuration is done to create the VLANs, these were grouped according to the functions of the departments in the Municipal GAD Urcuquí together these routing between VLANs used for conveying information such Vlans configured .

VTP (VLAN Trunking Protocol) protocol server mode thereby creating VLANs on the access switches in manual mode, avoiding problems with writing errors when creating a Vlans be avoided is set.

It is very important to consider aspects of failures (equipment), so HSRP, its basic operation is to be enabled: when a switch is placed in active mode and a standby if the switch active fault which is awaiting plays it functions.

Access lists with which will be prevented and largely accepted communication between departments grouped by Vlans through rules, for example communication between finance department and administrative department is allowed, these rules were chosen by the IT department is set.

Ports connected to access switches layer is set trunked to transport many Vlans by a single link. In Figure 19, it is seen as switches must be connected in the collapsed core layer.

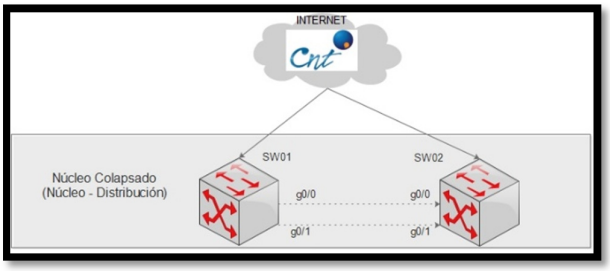


Figure 19. Hierarchical model - collapsed core

Reference: Prepared

1. Level access

In the access layer is essential configure MAC authentication for each computer that existing in the main building of the Municipal GAD Urcuquí, this will prevent access to resources (printer, internet, database, corporate mail).

Configuring VTP (VLAN Trunking Protocol) in client mode is done to prevent Vlans set manually. The ports connected to end users, will be configured for access to transport traffic of each user connected to that VLAN mode.

The protocol VPC (Virtual port channel) this allows links that are physically connected to different switches appear as a single link, this provides rapid convergence if the link failure is set. In Figure 20, we see how they should be structured in access layer switches providing connection to all the existing departments.

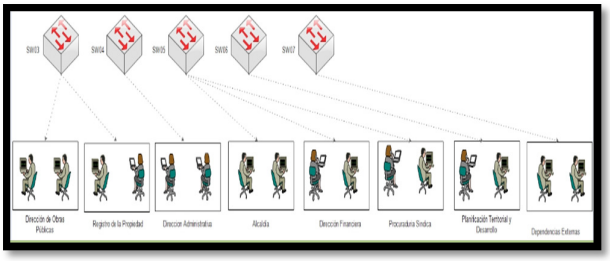


Figure 20. Hierarchical model - access

Reference: Prepared

E. Proposal for logical network model

For the logical part microsegmentation based on VLANs is done jointly IP addressing calculation is performed using VLSM, the calculation is based on number of users that each VLAN. The procedure for the logical part is explained.

1. Network Segmentation

In Figure 21, the VLANs is observed with different images which are located on different floors; It proposes creating a total of 14 Vlans.

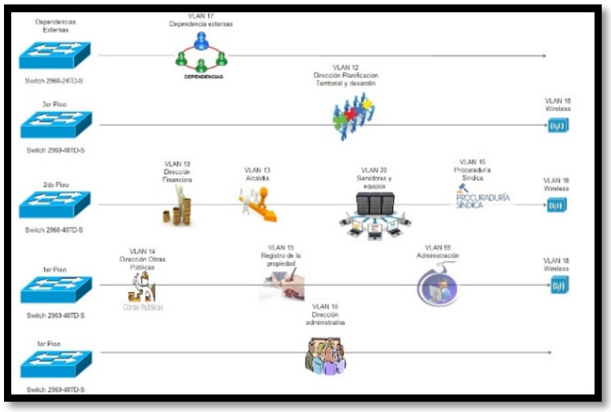


Figure 21. Distribution of VLANs

Reference: Prepared

By creating VLANs have a logical schema in an orderly fashion, with a great advantage of providing more control to the administrator as are assigned locally, departments grouping is based on Table 5.

Table 5. Grouping departments

VLAN	GROUPING DEPARTMENTS	DEPARTMENTS
10	Administrative Management	Human talent
		Information systems
		Cellar
		Government procurement
		Maintenance
11	Financial Management	Budget
		Accounting
		Treasury
		Rents
12	Territorial planning and development	Urban regulation
		Appraisals and Catastros
		And project management
		Traffic and Transportation
13	Mayoralty	Communication
		General Secretary
		Advisory
		Audit
		Internal audit
		Mayoralty
		Municipal Council
14	Public Works Department	Drinking water
		Infrastructure
		Risk management
		Environmental management
15	Property registration	
16	Attorney Sindica	Municipal Commissioner
17	External dependencies	Place of good living
		Social Development Unit
		library
		Maintenance

Reference: Prepared

In Table 5, the complementary create VLANs proposed in GADMU for management and monitoring are indicated.

Table 6. Additional Vlans in GADMU

VLAN	USO
18	Wireless
19	Servers and Equipment
20	Systems area
99	Administration
22	Voice
23	Video surveillance

Reference: Prepared

2. IP Addressing

To assign IP addresses VLAN groups more users and users also lower, in our case the group (External Dependencies) has increased influx of users and Attorney Sindica group with lower number of users was considered. With the following data collected described in the following subnets:

- A subnet host 24 to be assigned to administrative management VLAN.
- A 24 host subnet to be assigned to the VLAN financial management.
- A 24 host subnet to be assigned to the VLAN territorial planning and development.
- An 18 host subnet to be assigned to the VLAN Hall.
- An 18 host subnet to be assigned to the VLAN address public works.
- An 11 host subnet to be assigned to the VLAN property registration.

- A 7 host subnet to be assigned to the VLAN Attorney Síndica.
- A subnet host 29 to be assigned to the management VLAN External dependencies.
- A 240 host subnet to be assigned to the VLAN Wireless.
- A 40 host subnet to be assigned to the VLAN Servers.
- A 20 host subnet to be assigned to the VLAN area systems.
- A 10 host subnet to be assigned to the VLAN Administration.

For future applications: A 150 host subnet to be assigned to the Voice VLAN, one 50 host subnet to be assigned to the VLAN Video surveillance.

Table 7, based VLANs, along with their respective network mask, gateway and location, with the 172.16.0.0/24 IP address specified proposes the following networks:

Table 7. *VLANs based routing*

VLAN	DEPARTMENT	ACRONYM	# RED POINT	RED MASK	NETWORK ADDRESS	1ST IP UTILIZABLE	LAST BROADCAST IP	BROADCAST	LOCATI - ON
18	Wireless	WIRELESS	240	/24	172.16.0.0	172.16.0.1	172.16.0.254	172.16.0.255	P1,P2, P3
23	Voice	VOZ	150	/24	172.16.1.0	172.16.1.1	172.16.1.254	172.16.1.255	P1,P2, P3
24	Video surveillance	VIDEOVIG	50	/26	172.16.2.0	172.16.2.1	172.16.2.62	172.16.1.63	P1,P2, P3
19	Servers and Equipment	SRVEQU	40	/26	172.16.2.64	172.16.2.65	172.16.2.126	172.16.2.127	Cuarto de equipo s
17	external dependence	DEPEXT	29	/27	172.16.2.128	172.16.2.12 9	172.16.2.158	172.16.2.159	EXTER IORES
10	administrative management	DIRADMIN	24	/27	172.16.2.160	172.16.2.16 1	172.16.2.190	192.16.2.191	P1
11	Financial Management	DIRFINAN	24	/27	172.16.2.192	172.16.2.19 3	172.16.2.222	172.16.2.223	P2
12	Territorial Planning and Development	PLANDES	24	/27	172.16.2.224	172.16.2.22 5	172.16.2.254	172.16.2.255	P3
20	Systems area	ARSIST	20	/27	172.16.3.0	172.16.3.1	172.16.3.30	172.16.3.31	P1
13	mayoralty	DEPALCD	18	/27	172.16.3.32	172.16.3.33	172.16.3.62	172.16.3.63	P1,P2, P3
14	Address Public Works	DIROBPUB	18	/27	172.16.3.64	172.16.3.65	172.16.3.94	172.16.3.95	P1
15	Property registration	REGPRO	11	/28	172.16.3.96	172.16.3.97	172.16.3.110	172.16.3.111	P1
99	Administration	ADMIN	10	/28	172.16.3.112	172.16.3.11 3	172.16.3.126	172.16.3.127	P1
16	Attorney Sindica	PROSIN	7	/28	172.16.3.128	172.16.3.12 9	172.16.3.142	172.16.3.143	P2

Reference: Prepared

F. Access Control Lists

These checklists are implemented in the switch core collapsed to limit traffic, these were given by the department to improve traffic between Vlans. The rules are as follows:

- The user with the IP 172.16.3.34 (Mayor) have access to the Vlans of : Administrative Management, Financial Management , Planning and Development , Department of Public Works , Land Registry , Attorney Sindica , External Dependencies .
- Users with network 172.16.2.160 (Administrative Management) will have access to financial resources management VLAN.
- Users with network 172.16.2.192 (Financial Management) will have access to resources Administrative Management VLAN.
- The user with the IP 172.16.3.2 (System Area) will have access to all network resources.

G. Network Topology Diagram

Table 4 shows the parameters for access layer are presented are: number of ports (48-24 ports), speeds toward work areas (100 Mbps) speeds ports up-link (1 Gbps) switching capacity (13, 6 Gbps). Another important point is the number of ports and types of interfaces that must have switching equipment for collapsed core layer. We must consider capacity for future growth while integrating on a single computer (distribution and core), so it is recommended an amount of at least 24 Gigabit Ethernet 1 [Gbps] and 4 interfaces 10 Gigabit Ethernet Fiber Optic, of which 2 are used to having redundant connection between nodes. Access layer switches and core layer should work with the following protocols.

• IEEE 802.3x for simultaneous reception and transmission (full duplex).

• IEEE 802.3u for connection of terminal devices via 10/100 Mbps cards via CAT6 UTP cable.

• IEEE 802.3ab for connection of end computers using cards 10/100/1000 Mbps over UTP cable and the standard CAT6.

• IEEE 802.3z for connecting optical fiber links at 1 Gbps.

• IEEE 802.1q allows multiple networks sharing the same physical space, using this alternative logical network segments are generated in the GADMU this protocol allows you to create Vlans.

• It is necessary to ensure network redundancy, that links are available so set using protocols such as IEEE 802.1d and 802.1w.

• For future applications the main switch must provide quality service and label the differentiating traffic if they are data or voice. For which you need to have the IEEE 802.1p protocol, and differentiate the traffic generated by the Vlans.

• Both access switches as the core should provide the dynamic mapping service hosts.

• A security level required to switch ports support the IEEE 802.1x protocol for authentication and access lists with permissions to provide user's access lists should be standard and extended.

• Even team management must provide security through SSH protocol, remote access with the Telnet protocol and SNMP protocol support management in their current versions. And switching equipment must support both GUI administration as command line.

H. Design Overview

For operation of the network redesign it is important that the structured wiring is in good condition, in the Municipal GAD of San Miguel de Urcuquí not have any standards, therefore considerations should solve the GADMU structured cabling.

By calculations in this chapter was determined that four access switches 48 ports and a switch 24 ports are required, they must have speed to the work areas of 100 Mbps and up-link of 1 Gbps, with a capacity of 13.6 Gbps switching and core portion takes two switches with 24 ports Fast Ethernet to 1Gbps with 8 up-link ports to 1Gbps connection with equipment for access layer, with a switching capacity of 160 Gbps. Selected for each layer devices are Cisco Catalyst WS-C2960 and WS-C3750X-24-PS that fit the proposed In order to verify the operation of the redesign the GNS3 program was used redesign, in which all protocols configured above.

I. Design Overview

For operation of the network redesign it is important that the structured wiring is in good condition, in the Municipal GAD of San Miguel de Urcuquí not have any standards, therefore considerations should solve the GADMU structured cabling.

By calculations in this chapter was determined that four access switches 48 ports and a switch 24 ports are required, they must have speed to the work areas of 100 Mbps and up-link of 1 Gbps, with a capacity of 13.6 Gbps switching and core portion takes two switches with 24 ports Fast Ethernet to 1Gbps with 8 up-link ports to 1Gbps connection with equipment for access layer, with a switching capacity of 160 Gbps. Selected for each layer devices are Cisco Catalyst WS-C2960 and WS-C3750X-24-PS that fit the proposed In order to verify the operation of the redesign the GNS3 program was used redesign, in which all protocols configured above.

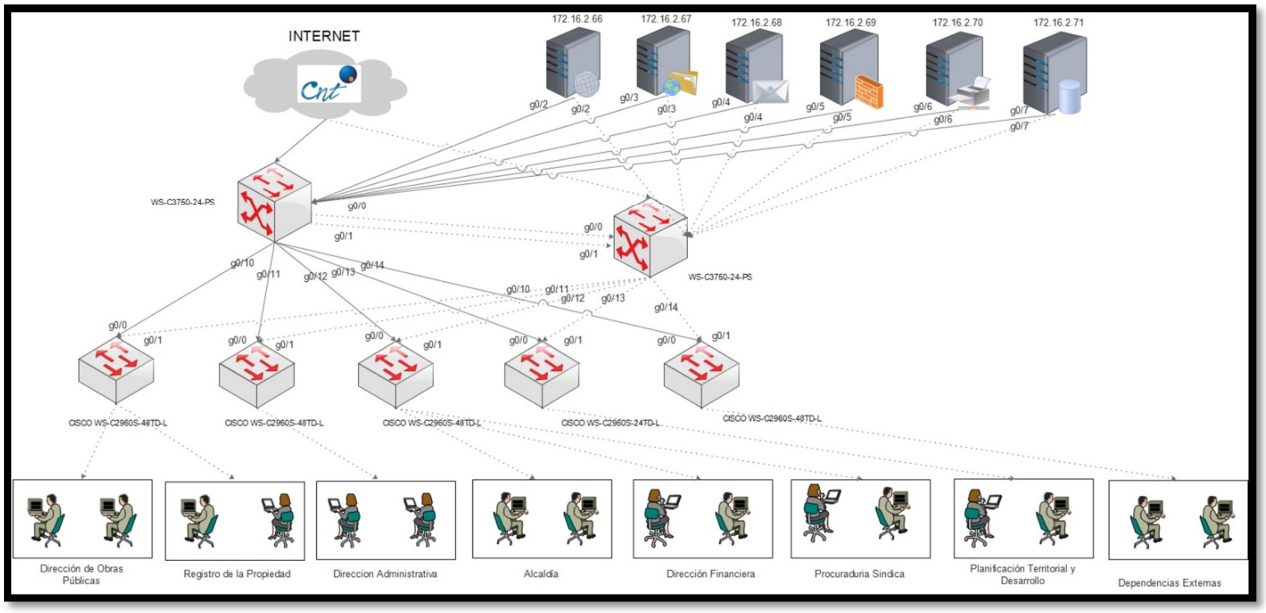


Figure 22. Distribution of VLANs

Reference: Prepared

In Figure 23, the topology shown in operation switch has two core collapsed to their respective redundant links, besides these VLANs each configured with its respective IP address and a virtual machine (Ubuntu) is observed.

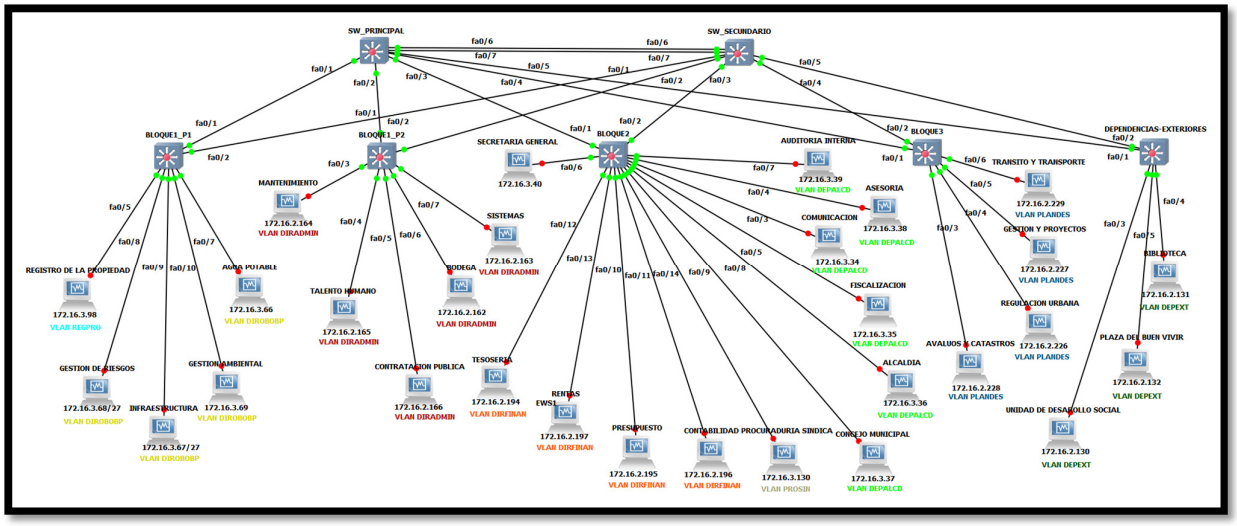


Figure 23. Distribution of VLANs in GNS3

Reference: Prepared

v. PERIMETER SECURITY OPTIMIZATION

This chapter MARGERIT methodology adopted to determine a risk analysis thereby is to distinguish vulnerabilities in the Municipal GAD Urcuquí; be held together a comparison between two proposals with the marks (JUNIPER and CISCO) and a team to be chosen perimeter security, managing assets der protect network and important information.

After the election of the operating system used on servers (FTP and PROXY SQUID) ISO / IEC / IEEE 29148 standard is used.

With the methodology MAGERIT a risk analysis of the network security of the Autonomous Government Decentralized Municipal of San Miguel de Urcuquí be performed, such analysis will identify threats that affect the vulnerability of information and finally able to propose a team to optimize perimeter security.

In this way network administrators can easily identify threats and to make better decisions when some threats.

A. Justification of the methodology MARGERIT

In Figure 24, the main methodologies of analysis and risk management systems commonly used in the market for information security are observed are : MAGERIT, OCTAVE, CRAMM, IRAM, to determine the methodology that generates confidence in mitigating risk was made the following comparison table.

		MAGERIT	OCTAVE	CRAMM	IRAM
ALCANCE CONSIDERADO	Análisis de Riesgos	●	●	●	●
	Gestión de Riesgos	●	●	●	●
TIPO DE ANÁLISIS	Cuantitativo	●	◑	●	●
	Cualitativo	●	◑	●	●
	Mixto	●	◑	○	○
TIPO DE RIESGOS	Intrínseco	●	○	●	●
	Efectivo	●	●	●	●
	Residual	●	◔	○	◔
ELEMENTOS DEL MODELO	Procesos	●	●	○	○
	Activos	●	●	●	●
	Recursos	●	●	○	○
	Dependencias	●	●	●	●
	Vulnerabilidades	●	●	●	●
	Amenazas	●	●	●	●
	Salvaguardas	●	●	●	●
OBJETIVOS DE SEGURIDAD	Confidencialidad	●	●	●	●
	Integridad	●	●	●	●
	Disponibilidad	●	●	●	●
	Autenticidad	●	○	○	○
	Trazabilidad	●	○	○	○
INVENTARIOS	Tipos de Recursos	●	●	●	○
	Vulnerabilidades	●	●	●	●
	Amenazas	●	●	●	●
	Salvaguardas	◕	●	○	●
AYUDAS A LA IMPLANTACIÓN	Herramienta	●	○	●	●
	Plan de Proyecto	●	●	◔	○
	Técnicas	●	●	○	○
	Roles	●	●	●	○
	Comparativas	●	○	●	○
	Otros	○	Cuestionarios	Cuestionarios	Soporte Del ISF

Figure 24. Comparison of methodologies

Reference: Based on (Álvarez, 2014)

From the above comparison chart developed it can conclude that MAGERIT is a complete methodology because it processes, activities. A key part of managing information security is to know and control the risks to which it is exposed Municipal information Urcuquí GAD.

Precisely MAGERIT is based on analyzing the impact it can have for the institution, seeking to identify threats that may affect the institution and vulnerabilities that can be used by these threats, achieving have a clear identification of preventive and corrective measures more appropriate.

This methodology is very useful for companies that start with the management of information security, allowing focus efforts on the risks that may be more critical to a company.

B. Preparation of risk analysis in the GADMU

Risk analysis to analyze these elements methodically to reach conclusions on the basis, for the risk analysis process the following steps are performed as shown in the following figure.

TAREAS DELANÁLISIS DE RIESGOS
Paso 1. Caracterización de los activos
1.1 Identificación de los activos
1.2 Dependencias entre activos
1.3 Valoración de los activos
Paso 2. Caracterización de las Amenazas
2.1 Identificación de las amenazas
2.2 Valoración de las amenazas
Paso 3. Caracterización de las salvaguardas
3.1 Identificación de las salvaguardas pertinentes
3.2 Valoración de las salvaguardas.
Paso 4. Estimación del estado de riesgo
4.1 Estimación del impacto
4.2 Estimación del riesgo

Figure 25. Table for risk analysis

Reference: Based on (Álvarez, 2014)

In Figure 25 the steps outlined 4 steps to be met to determine the risks and vulnerabilities.

1. Identification and classification of assets on the network

Identifying assets is important because it allows to capture precisely the scope of the project, it can accurately value assets and identifying and assessing the threats they are exposed to such assets.

The respective collection of asset information was performed.

The description of all the information collected already mentioned above in Chapter 3 "Analysis of the current situation," through Tables 5, 7, 8. As a result of previous interviews with manager's Municipal infrastructure Urcuquí GAD, we have identified the following set of assets LAN:

- Data / information: Data is the main part that allows an organization to provide services. Information is inaccurate asset that will be stored on computers. Within the GADMU they have identified the need to protect citizen's information stored in the database

- Computer equipment (hardware): These are media material, physical, intended to directly or indirectly support the services provided by the institution, be it temporary or permanent repositories of data, runtime support computer applications or responsible for processing or transmission of data. Within this type of network assets owned by the GADMU, we have the following: Mail Servers, Database Server

- Facilities: Among the places where information and communication systems are hosted. In the GADMU has a telecommunications room.

- Personal: In this type of asset the people related to communications systems appear. In addition this type of asset (Personal) no dependencies are identified. GADMU in the area have been identified that are Administrators Network.

2. Asset valuation equipment

It can be concluded that the assets more high value for the organization in availability security dimension in descending order are:

- Telecom Room
- Database Server
- Mail Server

3. Identification of threats

After identifying the assets must identify threats that may affect each asset, so that a threat can trigger many more.

Valuing threats

	ASSETS	THREATS	FREQUENCY	DEGRADATION
Facilities	Telecommunications room	Fire Water damage Natural disasters industrial disasters mechanical contamination electromagnetic pollution Damage from physical and logical Power Outage inadequate conditions of temperature or humidity Administrator errors Update maintenance errors programs Loss of equipment Alteration sequence Unauthorized access Unforeseen use Handling equipment electromagnetic emanations Program Manipulation	2	75%
Personal	Network administrators	Unavailability of staff Deficiencies in the organization Information leaks Extortion Social engineering	12	75 %

Figure 26. Valuing threats

Reference: Prepared

	ASSETS	THREATS	FREQUENCY	DEGRADATION
Equipment	Server	Fire Water damage Natural disasters Industrial disasters Mechanical contamination Electromagnetic Pollution damage from physical and logical Power Outage Inadequate conditions of temperature Humidity Administrator Errors update maintenance Errors programs Loss of equipment Alteration sequence Unauthorized access Unforeseen Handling equipment Disclosure of Information Program manipulation	2	25 %
Data	Citizens information stored in the database	Administrator errors Accidental alteration of information Destruction of information Information leakage User Impersonation Abuse of access privileges Unauthorized access deliberate modification of information Destruction of information Disclosure of Information	12	75

Figure 27. Valuing threats

Reference: Prepared

In the following tables 26, 27 the frequency and degradation of the active devices shown.

4. Identification safeguards

Once identified threats, safeguard mechanisms implemented in those assets are identified, describing the dimensions of security they offer (Availability, Integrity, Confidentiality, and Authenticity).

	ASSETS	SAFEGUARDS
Facilities	Telecommunications room	Physical access control Ensuring availability alarms Ventilation Fire extinguishers Ups
Personal	Network administrators	Training and awareness Ensuring availability
Equipment	Server	Keys. Protection team within the organization. It applies security profiles Authentication channel Protecting the integrity of the data exchanged
Data	Citizens information stored in the database	Information protection

Figure 28. Identification safeguards

Reference: Prepared

C. Study of the UMT technology

Today the threats are becoming more dangerous and complex, therefore to implement a security system required several different control systems services on the network, proxy, firewall, antivirus, anti -spam.

The solution is to centralize services and an excellent choice is the unified threat management. Manufacturers for perimeter security increasingly draw new features, the most common manufacturers are: Juniper Networks, Astaro, SonicWall, WatchGuard, Netgear, Crossbeam among others, in this case the CISCO and JUNIPER solution will be analyzed as mass characteristics have to they adapt the project. For the election you must meet these minimum requirements for the firewall (firewall) team , these were determined by the relationship with the characteristics of existing servers in the Municipal GAD of San Miguel de Urcuquí which are as follows:

1. Memory 1024 MB RAM minimum.
2. Interfaces at least six with capacity of 10 /100/ 1000 Mbps.
3. Ability to manage bandwidth interfaces.
4. Simultaneous sessions at least 400,000 connections.
5. Service capacity for 150 users.
6. Hard disk at least 20 GB.
7. Support for Vlans (802.1Q) in their interfaces.
8. Include training at least two people.
9. Warranty team at least two years.
10. Support mechanisms for secure access (SSH, HTTPS, etc.)
11. Support 802.1X authentication certificates.
12. Interface for configuration and management via web, telnet and / or CLI.
13. Automatic update of security services: IDS / IPS, Anti-Spam, Antivirus (minimum hourly) and the list of URLs.

.

14. Annual cost of subscriptions to security services.
15. Monthly Support .

Figure 29.Features Cisco equipment

Reference: Prepared

D. Proposal for perimeter security

With the risk analysis and the choice of equipment for technology UTM equipment such as firewall (firewall) for the Municipal GAD of San Miguel de Urcuquí , which will allow solve problems for vulnerabilities by MARGERIT methodology discussed above is determined.

In Figure 31, a proposed perimeter security scheme, which uses a computer Juniper Networks SSG 550M with a team firewall (firewall) to restrict traffic entering and leaving is observed.

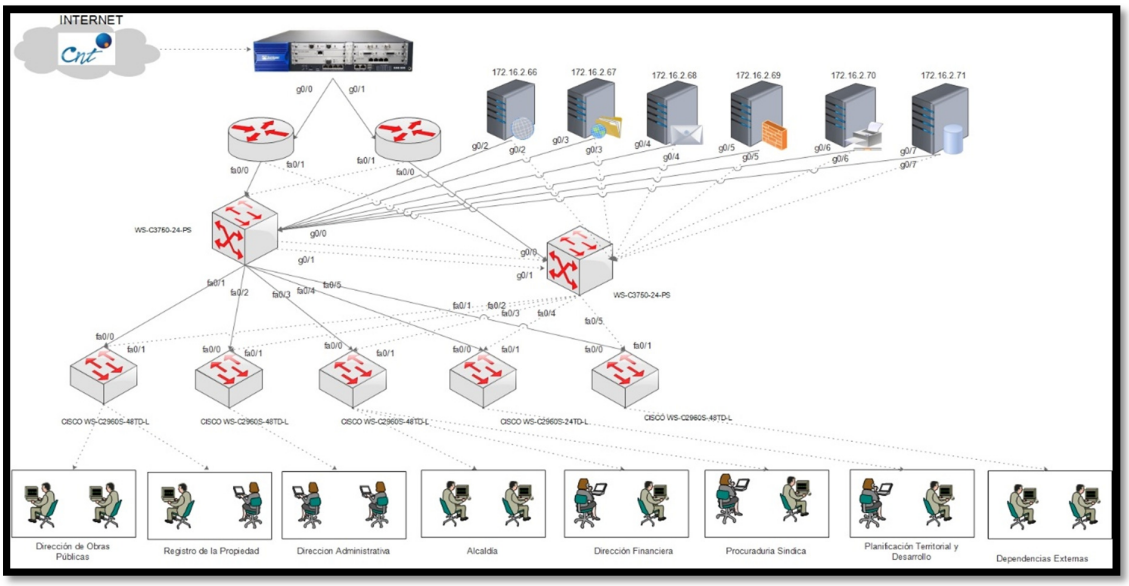


Figure 30. Features Juniper equipment.

Reference: Prepared

VI. COST BENEFIT ANALYSIS

This chapter is made known all costs to be used for the redesign of the data network and perimeter security optimization for future implementation for the data network.

A. Costs of equipment and materials

Benchmark costs if you want to implement, are taken from pages: free market, suppliers of network equipment, companies from the same manufacturers, among others.

1. Cost of equipment for the redesign of the internal network of GAD Municipal Urcuquí

In Table 8, the teams that exist in the institution and for the benefit of the redesign shown. In Table 8, the teams observed in reused for the system.

Table 8. Equipment reuse for the System

TEAM		CANT	UNIT VALUE	TOTAL VALUE
PROLIANT SERVER	E5649	1	2.730	2.730
PROLIANT SERVIDOR	ML170	1	1.880	1.880
TOTAL				4.610

Reference: Prepared

Costs of equipment that must be purchased by the institution, for the redesign of the internal network are detailed in Table 9.

Table 9. Cost of equipment der redesigning the GAD

TEAM	CANT	UNIT VALUE	TOTAL VALUE
Switch (CISCO WS-C2960S-48TD-L)	4	2.278	9.112
Switch (CISCO WS-C2960S-24TD-L)	1	1.629	1.629
Switch (CISCO WS-C3750X-24-PS)	2	3.024	6.048
TOTAL			16.789

Note: The values shown in the table are for reference and are obtained from the website of each brand.

Reference: Prepared

2. Cost of equipment for perimeter security

Table 10. Cost of equipment for perimeter security

TEAM	CANT	UNIT VALUE	TOTAL VALUE
SSG 550M	1	10.500	10.500
Anti-Virus Juniper-Kaspersky, NS-K-AVS-SSG550	1	3.150	3.150
Anti-Spam, NS-SPAM-ISG1000	1	5.000	5.000
Web Filtering, NS-WF-SSG550	1	2.300	2.300
Deep Inspection, NS-DI-SSG550	1	1.000	1.000
J-Care Support Services, SVC-COR-SSG550M	1	750	750
TOTAL			22.700

Note: The values shown in the table are for reference and are obtained from the website of each brand.

Reference: Prepared

Equipment costs for perimeter security must be purchased by the institution if the implementation is desired in Table 10.

3. Cost of net material

Material costs network must be purchased by the institution, to the internal wireless network is detailed in Table 11.

Table 11.Costo de materiales de red

DESCRIPTION	CANT	UNIT VALUE	TOTAL VALUE
Cable UTP Cat 6A(305m)	2 roll	350,00	700,00
Connector RJ-45	1 box	8,50	8,50
Plastic gutters 32x12	10	2,10	21,60
TOTAL			730,1

Reference: Prepared

4. Cost of electrical equipment

Costs of electrical materials to be purchased by the institution are detailed in Table 12.

.

Table 12. Cost of electrical equipment

DESCRIPTION	CANT	UNIT VALUE	TOTAL VALUE
Electric socket	30	0,20	6,00
12AWG power cord	2 rollo 100mts c/u	40,00	80,00
TOTAL			86,00

Note: The values shown in the table are for reference and are obtained from the website of each brand.

Reference: Prepared

5. Cost of labor

Costs of labor which must be employed by the institution, for installations of equipment for perimeter security, structured wiring portion corresponding to network redesign and network equipment configuration are detailed in Table 13.

The number of people required for the job is 2 people.

Table 13.*Costo de mano de Obra*

DESCRIPTION	# PERSON	COST/DAY	#DAY	TOTAL
Skilled labor	2	250	4	$ 1000

Note: The values shown in the table are for reference and are obtained from the website of each brand.

Reference: Prepared

A. Determination of total cost of redesigning the data network and perimeter security optimization

Table 14, shows that the sum of expenses for the part of the redesign of the network and perimeter security.

Table 14. Total costs of the redesign of the network and perimeter security

DESCRIPCIÓN	COSTO
Cost of equipment for the redesign of the internal network of GAD Municipal Urcuquí	16.789,00
Cost of equipment for perimeter security	22.700,00
Cost of net material	817,71
Cost of electrical equipment	96,32
Cost of labor	1.000,00
SUBTOTAL	40.722,49
IVA 12%	4.886,69
TOTAL	45.609,18

Referencia: Elaboración Propia

B. Determination of profit

Municipal GAD in San Miguel de Urcuquí currently employed 125 employees, distributed between the main building and external dependencies. The monthly payment that disburses the institution is $ 156,748.75, a table is shown with detailed values wages of each employee.

To determine the average salary of each worker, equation 1 applies.

$$Amount\ to\ be\ paid\ monthly\ to\ each\ employee = \frac{Salary\ disbursed\ monthly}{Total\ number\ of\ employess}$$

Equation 1. Calculation of average salary

Reference: Prepared

$$Amount\ to\ be\ paid\ monthly\ to\ each\ employee = \frac{156.748{,}75\ dólares}{125\ empleados}$$

$$Amount\ to\ be\ paid\ monthly\ to\ each\ employee = \$\,1.253{,}99$$

Monthly, daily, hourly and minute to object calculation: Table 15, the amount payable to each employee so detailed.

Table 15. Monetary values received by each employee

DESCRIPTION	VALUES
Amount to be paid monthly to each employee	1.253,99 dólares
Daily amount payable to each employee	41,79 dólares
Amount to be paid per hour for each employee	5,22 dólares
Value to pay per minute for each employee	0,08 ctvs.

Reference: Prepared

Employees of that institution, working 8 hours a day established by law. Nevertheless; due to problems in the current network is not working continuously, causing distractions of officials and generates losses to the institution. A survey was conducted to raise 25 people chosen to determine an average time in which the network is not available, obtaining as a result an average of 5%. Using Equation 2 determines the time (hours) without service in the San Miguel Municipal GAD Urcuquí.

$$5\%\_en\_hours = (8\ hours)x\ 0{,}05 = 0{,}4\ hours$$

Equation 2. Determination of time without service for hours

Reference: Prepared

Together with the above equation the calculation of loss in minutes, specified in equation 3 is determined.

$$5\%\_en\_minutes = \ 0{,}4\ x\ (60\ minutes) = 24 minutes$$

Equation 3. Determination of time without service for minutes

Reference: Prepared

With these values we can conclude that 5% of unavailability of network service corresponds to 24 minutes a day, in equation 4, this time is multiplied by the average value of each worker earns per minute, yielding a value of $ 2.08.

$$Profit\ per\ employee = \ 24\ minutes\ x\ 0{,}08\ ctvs = 2{,}08\ dólares$$

Equation 4. Total profit per day

Reference: Prepared

In Equation 5, the daily total profit, the GADMU saved if the network was in good condition is determined.

$$Total\ profit\ per\ day = \ 2{,}08\ dólares\ x\ 125\ employee = 261{,}25\ dólares$$

Equation 5. Total benefit

Reference: Prepared

In Table 16, the benefit is described for daily, weekly, monthly and yearly.

Table 16. Summary calculation of benefit

DESCRIPTION	BENEFIT
Value of total profit per day	261,25 dólares
Value of total profit per week	1.828,75 dólares
Value of the total benefit per month	7.837,43 dólares
Value of total profit per year	94.050,00 dólares

Reference: Prepared

C. Calculation cost / benefit

After analyzing the costs and benefits generated by the project, we apply equation 6, to determine the benefit / cost, for which the following parameters were used:

- If B / C is greater than 1 the project is accepted.
- If B / C is equal to 1 the project is indifferent.
- If B / C is less than 1 the project is rejected.

$$\frac{B}{C} = \frac{\Sigma\ \text{BenefiT}}{\Sigma\ \text{Cost}}$$

Equation 6. Calculation cost / benefit

Reference: [4]

$$\frac{B}{C} = \frac{94.050{,}00}{45.609{,}18} = \mathbf{2.06}$$

By applying the equation the value is 2.06; so it is determined that the project is acceptable.

D. Period will accrue to the project

Table 17, is applied to determine which month the investment is recovered, however, to have a more precise time period equation applies.

Table 17. *Period will accrue to*

MOUNTH	PROFIT/ MOUNTH	ACCRUED BENEFIT
		- 45.609
1	7.837,44	7.837
2	7.837,44	15.675
3	7.837,44	23.512
4	7.837,44	31.350
5	7.837,44	39.187
6	7.837,44	47.025

Note: The value of 45.609 is the total cost specified in Table 46 and the value of 7837.44 is the calculation of earnings per month specified in Table 48.

Reference: Prepared

$$\text{Period will accrue to} = 6\ mounth + \left(\frac{Total\ cost - \ \Sigma\ de\ 6\ mounth}{Monthly\ benefit}\right)$$

Equation 7. *Period Payback*

Fuente: [5]

$$\text{Period will accrue to} = 6\ mounth + (\frac{45.609 - 47.025}{7.837{,}44})$$

$$\text{Period will accrue to} = 6\ mounth + (0{,}18\ x\ 30\ day)$$

$$\text{Period will accrue to} = 6\ meses + 5\ dìas$$

These calculations show that a period of investment will accrue to 6 months and 5 days will.

VII. CONCLUSIONS

- Using books, articles and theses related to the topic, essential criteria for the development of the theoretical basis of the components involved in the investigation was established.

- As a result of gathering information on the current status of the network, it was determined that the physical state of the network and does not meet any standard structured cabling; causing discomfort for

employees, and this is consistent with the logic state of the network; the same is not properly configured and that computers are unmanaged and are spreading broadcast domains causing saturation of these, affecting network performance.

- By calculating the internal and external traffic that each user is generated, and in conjunction with the analysis of sizing active equipment network equipment was determined to be used and the Cisco brand was chosen because it provides an adaptable solution to the project and with the advantage in monetary savings for Municipal GAD of San Miguel de Urcuquí also these teams are excellent in areas of production, and offers a wide range of products available to the company prices, with profit in the following aspects reliability, scalability and reliability.

- For network redesign GADMU data layers based on a hierarchical model that will improve availability features, scalability and flexibility is implemented; this way you can optimize network performance, level of physical links and active equipment, ensuring continuity of service.

- The FTP server allows better access to the files of employees, and the Squid proxy server access to entertainment sites not authorized by the GADMU, helping to improve employee performance and reducing unnecessary traffic will be limited net.

- To select the requirements that have the FTP software and SQUID Proxy servers, an analysis with IEEE-STD-830-1998 standard was proposed but development was concluded that this is not in effect, therefore used ISO / IEC / IEEE 29148; the same one that provides a solution for operating system right choice by choosing essential characteristics such as robustness, stability, with which it was determined that Centos 6.3 (32 bits) text mode is the most feasible option for deploying servers.

- To simulate network was proposed GNS3 1.3.0 was used because perform similar to the chosen with switches 2960 and 3560 the equipment characteristics.

- By analyzing the UTM technology, it was determined that the best option for implementing perimeter security is Juniper, as compared to other brands, is economically priced within reach of the enterprise; improving the protection of personal information, intrusion prevention, control user access, security, management and entry applications so safe.

- The project is profitable according to the calculations of cost / benefit, thus recovering the investment over a period of 6 months and 5 days

VI. RECOMMENDATIONS

- It is recommended that the staff in charge of data network GADMU continually be undergoing the training and learning, which would help solve problems quickly.

- You must keep a log stating all events that occur on the network and incidents with the actions that were performed in this way if the personnel changes, the new head of network, can understand the current state of the same and easier administration.

- It is proposed to implement security policies in the institution to establish security levels, aimed at the organization, technology and users, so that regulates and controls the use and access to the network.

- It is advisable to restrict access using biometric and include cameras to record the malicious events that can occur in this. It is suggested to change passwords periodically, they must contain uppercase letters, lowercase letters, numbers and special characters for added security.

- It is essential to have a backup configurations in equipment, because if one botched configuration can be restored without affecting the system.

- The use of monitoring tool is recommended to determine the incidents or events that arise in the network.

- You should take note that no team provides complete security, so you must purchase additional safety equipment to have more confidence in the system.

VI. REFERENCES

[1] W. Stalling, FUNDAMENTOS DE SEGURIDAD EN REDES, APLICACIONES Y ESTÁNARES, España: Pearson, 2011.

[2] J. NOGUERA y A. VÁSQUEZ, Diseño eimplementación de un circuito cerrado de televisión con cámaras IP inalámbricas y monitoreo remoto, notificaciones de eventualidades mediante el uso de un servidor para la grabación de video bajo la plataforma Linux usando zonemider para el labora, Quito, 2011.

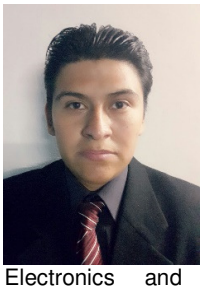
[3] A. Tanenbaum, Redes de computadoras, México: Pearson, 2011.

[4] D. Aulema, «Estudio y diseño de un sistema de seguridad perimetral utilizando tecnologia UTM,» 14 Junio 2011. [En línea]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/618/1/CD-1580%282008-06-30-03-34-00%29.pdf.

[5] S. Villalba, «Diseño de un esquema de seguridad para la intranet y extranet del CONESUP,» 2013. [En línea]. Available: http://biblioteca.epn.edu.ec/cgi-bin/koha/opac-detail.pl?biblionumber=8165&shelfbrowse_itemnumber=8533.

[6] V. G. B. &. Q. Cameron, Fundamentos de sistemas operativos, Editex, 2011.

Jonathan M. Morán



He was born in Ibarra on January 1, 1990, it conducted its secondary studies in the "Teodoro Gomez de la Torre "where he graduated Bachelor of Physical Technical Mathematical Experimental Unit. In 2008 he joined the North Technical University where he studied at the Faculty of Engineering of Applied Science. He is currently a graduate of the engineering degree in Electronics and Communication Networks Technical University North.