"ADMINISTRATION AND MANAGEMENT OF THE LOCAL AREA NETWORK OF THE MUNICIPALITY GADIP OF CAYAMBE, BASED ON FUNCTIONAL MODEL OF NETWORK MANAGEMENT FOR ISO/OSI PROTOCOL SNMP AND USE OF FREE SOFTWARE TOOLS" (DECEMBER 2015)

Sandra K. Narváez, Cyntia M. Inuca.

***Abstract* -This project has been developed with the aim of helping to improve the availability of the network of local area, the municipality of Cayambe GADIP, through functional model ISO/OSI network management, and the management areas; configuration, security, fault, performance, and accounting, which allows you to manage the network in an organized fashion, and indicates functions that you must manage.**

For the administration of the network deal free software tools, such as Zentyal and Zenoss, which help to monitor the areas of management of the above mentioned model, Zenoss acts as Station Manager, which collects information from the devices that is part of the network, the performance of its resources, inventories, notification of events and faults produced by email in terms of security, Zentyal provides a platform for various services in a single operating system, applies functions of firewall, IDS/IPS, control of users with OPEN LDAP with a captive portal. This project uses the concept of the Management Protocol simple NET, SNMP version 2, which are enabled to all managed devices, so they can send the Manager information from the operation of their resources, and so the administrator can control the activities of the network.

This is all part of a system of management of network, which operates on a center of monitoring and managing network located in the Department of TIC of the institution, which is rigue by means of policies and procedures to manage the network. He has been raised also a design of the network segmentation, as an alternative to improve the administration of the network.

***Indexed Term*—LAN, ISO, OSI, SNMP, IETF, TCP/IP, ITU, SMI, MIB, OID.**

I. INTRODUCTION

The Cayambe municipality is a public entity that provides services to citizenship, along with the Department of information technology and communication (ICT) work to improve the provision of services of communication within the institution, through the improvement of the infrastructure of the data network, and implementation of technological resources.

Department of ICT must be aware of the availability of the network, but its role has been complicated, given the large amount of users and additional installed equipment so that it has grown in an unplanned and unstructured way. The lack of adequate monitoring network, causes when there is a problem is difficult to identify the cause, so it must go personally to verify the operation of equipment, configurations, and network infrastructure to detect the problem. Either take control of State of the resources of the network and traffic flowing through it, which will allow to take preventive measures that control and solve any eventuality that detrimental to the performance of the network. The network of local area (LAN) of the institution does not have segmentation, enabling a correct management, all computers and servers are located under a same IP, the increase in new users of network addressing scheme and need for services required by the municipality require scalability.

Due to these drawbacks this project proposes the Administration and proper management of LAN based on the functional model ISO/OSI network management using SNMP protocol and free software tools, which have the characteristics of monitoring.

This research was performed as the previous project for the title Engineer in Electronics and Communication Networks race of the Faculty of Engineering of Applied Science (FICA) from the Technical University of the North. S.K. Narvaez, Professor at the Technical University of the North, in the Engineering in Electronics and Communication Networks, industry Av July 17 El Olivo, Ibarra-Ecuador (e-mail: sknarvaez@utn.edu.ec).. CMInuca, a graduate of the School of Engineering in Electronics and Communication Networks (e-mail: mab_c6@yahoo.es).

II. THEORETICAL FOUNDATIONS

A. Fundamental concepts.

The same, is not to manage to manage, but they are concepts that complement each other to ensure the correct operating a network, as well as some more concepts.

1) Administration.

Means organizing, directing, and controlling the resources of an entity, whether human, financial, technological, or knowledge, to ensure a level of service and keep the network operational.

2) Manage.

It means to assign actions or activities to each resource that has to meet a goal, as is the improvement of the operation of the network, efficient use of the network and its resources, make it more secure and control the changes that occur.

According to Saydam in his article of the Magazine Journal of Network and Systems Management "network management includes deployment, integration and coordination of hardware, software and human elements to monitor, test, probe, set up, analyse, evaluate and control the resources of the network and the elements necessary to meet the requirements of real-time response, operational performance and quality of service at a reasonable price." [1]

3) Network planning.

Network planning consists of activities that anticipate the needs of the network, is taken criteria from a new installation of network or modification of the existing network, according to the situation that arises.

4) Network control.

Networks control involves the daily monitoring of the network to ensure that it maintains the desired operation. Networks control includes procedures such as the detection of failures, fault isolation and restoration of the network. [2]

5) Monitoring network.

It is the monitoring, observation and analysis of the state of network components, aimed at obtaining information from the network traffic flowing through it, for preventive detection of problems, speeding up the process of efforts for solving future problems.

B. Why manage the network?

The need to manage networks stems for different causes such as:

- Growth of networks.
- Heterogeneous network environments.
- Increase in network traffic.
- Difficult diagnostic problems in large environments.
- Need network management tools.
- Necessity of a set of standardized rules governing identification and address actions automated for various common situations that occur on the network.
- Increase in expectations of a reliable, safe, fast and operational network users.

C. Objectives of management.

- The main objectives of the network management consist in improving:
- The availability
- The performance of the elements of the system,
- and increase its effectiveness.

D. Network management models.

- **Internet management** defined by the IETF[1], SNMP[2]-based TCP/IP[3] networks.
- **TMN[4] architecture** defined by the ITU[5] for telecommunications network management.
- **Management of OSI network** defined by ISO[6] as a general reference for environments of OSI network model.

1) Functional model of OSI network management.

The OSI network management model, presented their functional model, better known as FCAPS model, this is a well structured model that divides the functions of network management, in five areas of management.

Configuration management.

The goal of configuration management is obtaining data from the network and use it to add, maintain, and remove components and resources to integrate. Consists of three fundamental tasks:

Automated collection of data, on inventory and State of the network, such as the dist hardware and software versions.

[1] IETF Internet Engineering Task Force is an open international standards organization.

[2] SNMP, Simple Network Management Protocol, is a protocol for network management.

[3] TCP / IP Transmission Control Protocol / Internet Protocol, is a network architecture model, with a family of protocols.

[4] TMN Telecommunication Management Networks, is a protocol for administration of open systems.

[5] ITU, International Telecommunication Union, in charge of regulating telecommunications worldwide.

[6] OSI Open System Interconnection, is a model of OSI, created by the ISO to troubleshoot hardware and software compatibility, so that helps network designers to deploy networks that can communicate and work together, compatible and inter operable.

Fault Management.

Fault management involves the detection, isolation and correction of failures as well as correction of abnormal operation. It includes features for:

- Maintain and examine records of error (error logs);
- Accept notifications of detection of error and react to them.
- Track and identify failures;
- Perform diagnostic tests sequences;
- and Eliminate faults.

Accounting management.

Accounting management is to measure network utilization parameters allowing his Manager to prepare the corresponding invoices to their customers. The tasks to be performed in this area, include:

- Collection of data on the use of resources.
- Establishment of quotas.
- Charging the users with the rates derived from the use of resources.

Management of performance.

Management of performance or benefits. Performance management allows you to evaluate the behavior of resources that make up the network, its main objective is to maintain the level of service offered by the network to its users, making sure that it is operating efficiently at all times. Performance management is based on four tasks:

- Collection of statistical information, such as the troughput of the network, response, or latency times, etc.
- Analysis of data to determine the normal levels of performance. • Establishment of thresholds, as indicators that set minimum standards of performance that can be tolerated.
- Determination of a system of processing daily data for the provision of the different teams, for their continued study.

Security management.

Safety management aims to establish mechanisms and security policies to protect your network against attacks of intruders. The functions performed by security management systems, include:

- Identification of sensitive resources on the network, such as files or communications devices.
- Determination of the relationship between the sensitive network resources and user groups.
- Monitoring of points of access to sensitive network resources.
- Storage of the unauthorized attempts to access these resources, for further analysis. [3] [4]

E.Network management system.

A network management system is a set of tools to monitor and control the network, in an integrated way. It consists of additional hardware and software implemented in the existing network components, it is designed to view the network as a unified architecture.

1)Elements of a network management system.

Station Manager or management.

It is the main equipment which monitors the activities of the network and their behavior, allows the collection, processing, analysis or visualization of the network management information. The Manager sends messages or applications to perform certain actions and interacts with the devices that make up the network.

Managed device.

It is the team that answers to those messages with information on their operating current or indicating if the requested operation has completed successfully. Example: Router, switch, hub, PC, printers, etc.

Managed devices include:

- **Managed objects:** Are elements hardware such as a network interface card, each managed object has an identifier (OID), and this are identified within a MIB tree.
- **Agent:** Is residing on the managed device and software that communicates with the Manager, taking local action on the device run under control of the management station.
- **Network Management Protocol:** Protocol runs between the entity manager and managed devices, lets you check the status of managed devices and carry out actions in an indirect way in these devices through its agents. [5] [6]

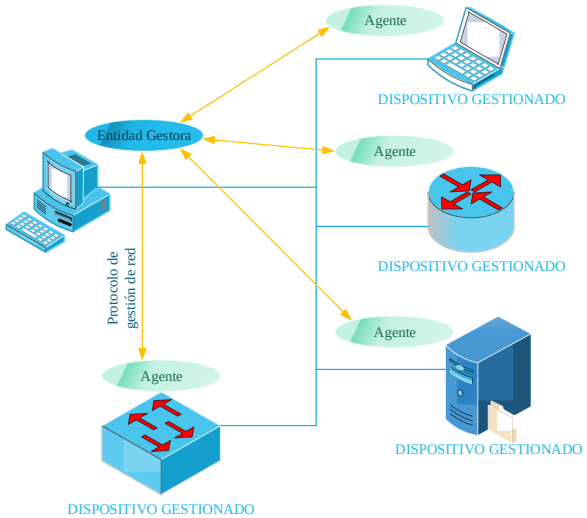


Fig. 1. Elements of a network management system
Source: James Kurose. (2013).Redes de Computadoras. Editorial: PEARSON. Estados Unidos.

F.SNMP simple network management protocol.

SNMP (Simple Network Management Protocol) is an application protocol, that allows to manage the network through exchange of management information network among management (Manager/Agent), based on request/response bodies. Along with the SNMP protocol, are also defined the structure of information management (SMI) and information management (MIB).

1)Structure of Management Information (SMI).

For information management method object identifier (OID, Objetc Identifier), which allows to reach objects in the sequence of a tree, getting the type of data used in the MIB is used.

The management information is communicated through the SNMP protocol, represented with ASN.1 language.

2)Management Information Base (MIB).

It is hosted virtual information on managed objects, whose values collectively reflect the current state of the network.

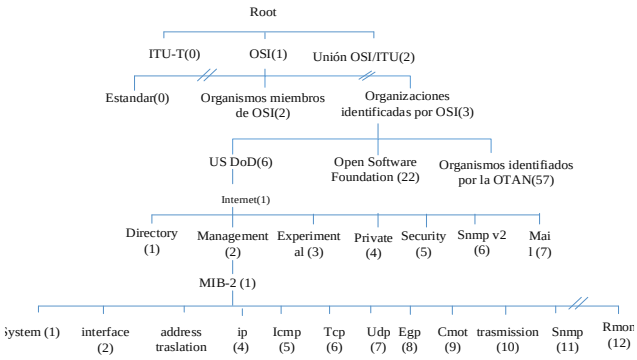


Fig. 2. MIB-II Tree.
Source: James Kurose. (2013).Redes de Computadoras. Editorial: PEARSON. Estados Unidos.

3)Operation of the SNMP architecture.

Network management station running management applications, which monitor and control network elements. Network elements are devices such as: host, gateways, servers, etc., where it has hosted software agent responsible for carry out management functions requested by the Station Manager. The Simple Network Management Protocol (SNMP) is used to communicate management information between network management station and the agents in the network elements.

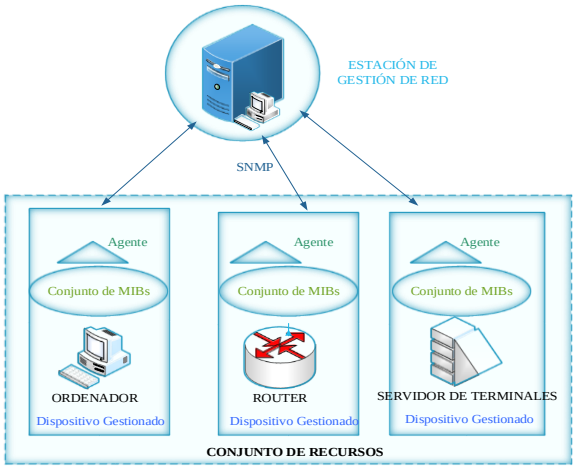


Fig. 3. SNMP management architecture.
Source: Antoni Barba. (1999). Gestión de red. Ediciones UPC.

Communication between management entities.

Communication of information among management entities management is performed through SNMP messages. It uses the UDP Transport Protocol, messages are sent via a UDP datagram. The Manager sends a message per UDP port 161, and the agent receives the message by the port 162.

SNMP Operations.

The management station can send the following messages:

- **GetRequest:** Gets the value of one or more MIB objects.
- **GetNextRequest:** Gets the value of an object MIB can move in a list or table MIB.
- **GetBulk Request:** Gets the value in a large block of data. The manager gets an answer that is as large as possible.
- **InformRequest:** a Manager provide management (values MIB) information to another entity manager.
- **SetRequest:** assigns or sets the value of one or more MIB objects.

The agent can send the following messages:

- **GetResponse:** returns the values requested by previous operations.
- **Trap (notification):** allows an agent to send to the management station notifications unsolicited on important events.

SNMP management relations.

- **SNMP Community:** community is called to a group of managers and the managed devices. The communities are assigned names, so this name with some additional information serves to validate an SNMP message and the issuer.
- **Authentication Service:** the agent can limit access to the MIB to authorized operators.

- **Access Policy:** The SNMP community association, access mode, and a MIB view. The agent could apply different access privileges to different managers.
  - **Access mode:** Specifies how to access the devices in the community, access modes are: read-only, read-write or write-only.
  - **MIB view:** defines one or more MIB subtrees to which a specific SNMP community can access.
- **Proxy services:** an agent may act as a proxy to another agent.

4)SNMP versions.

SNMP v1.

It is the first standard version of SNMP protocol defined by the IETF in RFC 1157.1155, y1212. SNMP defines the architecture formed by the management station and management elements or managed devices. For the transmission of messages using connectionless UDP protocol service, messages are sent in a UDP datagram, used ***GetRequest, GetNextRequest, GetResponse, SetRequet and Trap*** operations. Its operation is based on communities as a security method. Its use has expanded enormously, and began to notice some shortcomings, which arises SNMP v2.

SNMP v2.

It is an improved version polishing the shortcomings of the first version defined in RFC 1905, 1906.1907. Its operation is still based on community improvements gaps protocol operations are performed with respect to the structure of management information SMIv2, which extends the object tree by adding the hive SNMPv2 Internet also has the capability of manager-manager interaction, this version can handle seven types of operations SNMP PDU, GetRequest, GetBulkRequest, GetNextRequest, GetResponse, SetRequet InformRequest and Trap. Undoubtedly one of the most important improvements in SNMP v2 is GetBulkRequest is to minimize the number of exchanges of the protocol required to get lots of information management allows a SNMPv2 manager to request that the response be as large as possible, given the constraints message size, and transmits InformRequest unsolicited information between stations managers.

SNMP v3.

SNMP v3, eliminates the concept of community has its primary focus on safety, providing three important services: authentication, privacy and access control, which work on a modular architecture. The first two are part of the security model based on the user (USM, User-Based Security) uses algorithms like MD5 or SHA1 and DES, and the latter is defined in the access control model based on views (VACM, View - Based Access Control Model), is responsible for controlling access to the MIB objects.

It maintains its principle of architecture, with new textual conventions, concepts and terminology. Managers and agents are called SNMP entities, each entity consists of an SNMP engine and one or more SNMP applications. [7] [8]

5)SNMP Advantages.

- You can take as an advantage that SNMP is currently the most widely used network management protocol becoming a market standard.
- Currently the manufacturers of communication equipment support for all versions of SNMP.
- It has a simple design, easy to implement and understand for developers.
- Does not consume many resources.
- It has general monitoring and control capabilities.

6)SNMP Disadvantages.

- Consumption increased bandwidth in large network environments, not allowing optimization of network traffic. (version 1)
- The original version will not allow the transfer of large amounts of data, which is improved in version 2, allowing greater efficiency in traffic.
- One of the main disadvantages of snmp is having limited functionality and security level very low in versions 1 and 2, which has been already fixed in the latest version, SNMP v3, giving rise to concepts: authentication, privacy, and access control, but increases its complexity of configuration.

G.Administrator functions in a LAN environment.

The work of a network administrator is very important because it determines the proper functioning of the network, often the work is divided among a group of people, however, the designation of a responsible, who knows the network is necessary full.

The tasks to be performed by the network administrator are:

- Network planning.
- Preparation network.
- Organization and configuration.
- Change management.
- Problem Management.
- Security.
- Optimization.
- Maintenance of documentation.
- Maintenance documentation.
- Monitoring and control of traffic. [9]

III. Analysis of the current situation.

Information is gathered about the current conditions in which there is the local area network (LAN) Decentralized Autonomous Government Interculturaland Plurinational Municipality of Cayambe (GADIPMC), in order to know their needs and requirements to enhance network management.

A.Gobierno Autónomo Descentralizado Intercultural y Plurinacional Municipio de Cayambe (GADIPMC).

The GADIPMC is located in Canton Cayambe, Pichincha province, is a public entity, which aims to serve the cayambeña community, promoting equitable, solidarity and sustainable development of the territory, integration and citizen participation and social development and economic development of the population.

Manages and administers funds, property and public resources, undertakes, plans, manages and executes projects in order to improve the quality of life of citizens, fulfilling its slogan "Together for a good life."

1)Dirección de Tecnologías de la Información y Comunicación.

The address GADIPMC TIC is in charge of the development and growth of the technological area of the institution.

Estructure.

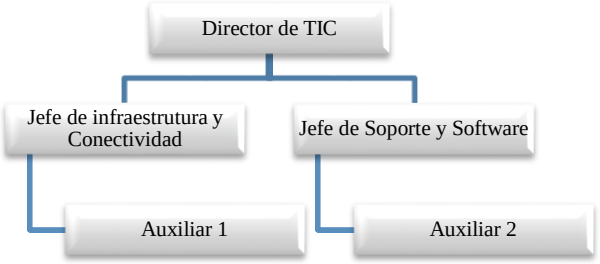


Fig. 4. Structure of the Directorate of TIC-GADIPMC
Source: Dirección de TIC del GADIPMC.

2) Municipal interconnected to the LAN.

The Municipality of Cayambe various functions through departments located in:

- Main building;
- Building Jarrin Espinoza;
- Units located elsewhere in the city.
- Independent entities.

These units are part of the LAN, through which users are interconnected, with access to network services and the Internet, shared files, printers, etc.

There are about 230 users belonging to the internal network of the municipality, which have assigned an IP address, without even considering computers using IP address.

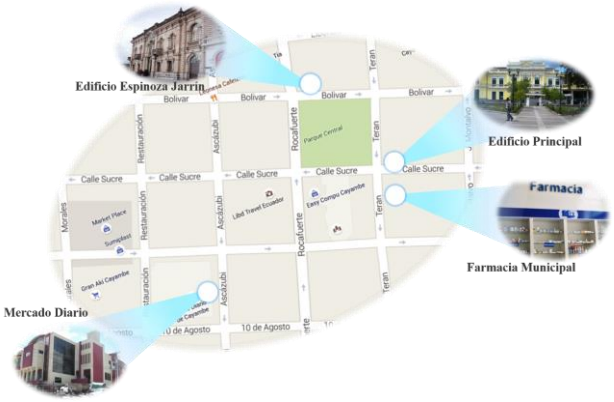


Fig. 5. Location GADIPMC agencies.
Source: Adapted from Google Maps.

B.Physical Infrastructure LAN.

The physical infrastructure of a network is the foundation on which all networks formed by different means of transmission, communication devices (routing / switching) equipment end users, constitute etc.

1) General Characteristics.

Then the physical elements of the local network GADIPMC described

- It has a Data Center where are located the following items:
  - Switches.
  - Firewall.
  - Servers.
  - Air conditioning.
  - Power distribution board.
  - UPSs.
- Several racks house the switching equipment.
- Manages a star topology.
- The means of transmission used include:
  - Twisted pair cable UTP Cat 5e and Cat 6A.
  - Fiber optics.
- The main building has 140 points respectively network of certified and labeled data.
- The building Jarrin Espinoza, and other dependencies lacks a good sizing structured cabling.

C.Logical Network Status

To review the logic state of the network aspects such as IP addressing, a diagram of the network topology is detailed, and the network is monitored to know what state you are in and identify their shortcomings.

1)IP Address.

Now a private IPv4 Class C address, which is distributed to users on the LAN statically, the staff of the Directorateof ICT are responsible for this work and to maintain control of the range of available IP addresses is used.

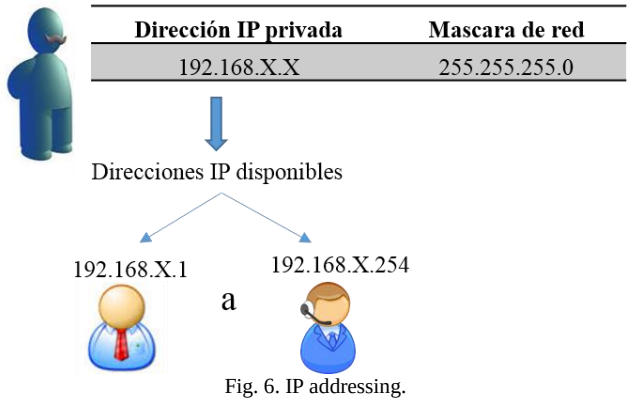


Fig. 6. IP addressing.
Source: Obtained from http://www.marbit.es/index_ip.html.

2)Topología lógica de la LAN logical LAN topology.

A star topology is handled, the central computer the firewall, from which the local network is formed, with connecting multiple switching equipment to reach end users

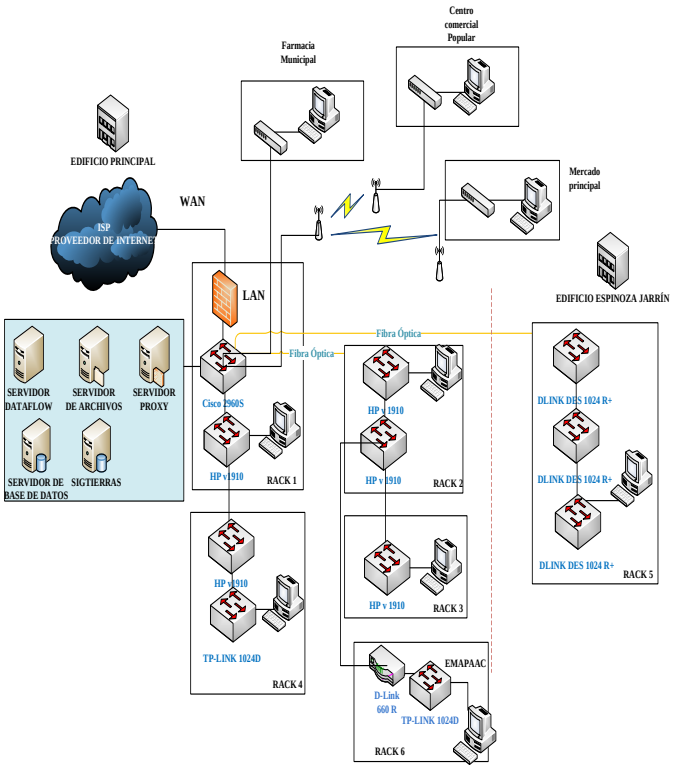


Fig. 7. Topology logic of the LAN GADIPMC.
Source: Server Zenoss.

3)Network monitoring.

To remove the information from the current network status is monitored network through a free management software chosen by the IEEE 29148.

Zenoss.

Zenoss on software that allows monitoring of network infrastructure, its features are:

- Discoveries and configuration.
- Performance and availability.
- Fault and event management.
- Alerts and remediation.
- Reports.

To monitor the current network has not made any configuration of SNMP, using the auto discovery range of IP network addressing is entered, then detail that results obtained following functionality Zenoss.

Discovered Devices.

Zenoss allows the auto discovery of the network by entering the IP address range of the local network was learned about how many users are connected in real time and the IP address assigned to each of them.

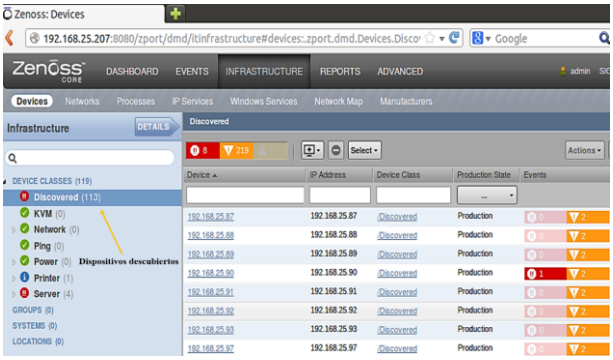


Fig. 7. Auto-discovery of the LAN.
Source: Server Zenoss.

Networks.

Network and discover devices and subnets interconnected to the local network, a subnet which found that belongs to EMAPPAC, independent institution to which the municipality provides Internet is observed.

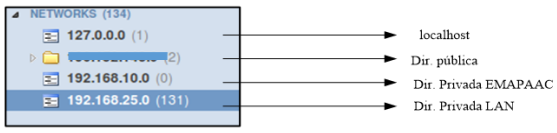


Fig. 8. Discovered networks.
Source: Server Zenoss.

Events and reports.

In the area of events and reports, it indicates that the software is not enabled SNMP devices discovered in which, to improve the administration of the LAN and obtain data on managed computers must be enabled.

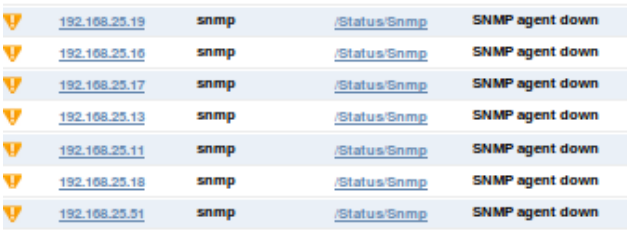


Fig. 9. State of the Protocol SNMP.
Source: Server Zenoss.

Network topology.

Automatically topology of the equipment that had enabled SNMP protocol, public community, these are some of the network printers that are used on the premises of the municipality is obtained.

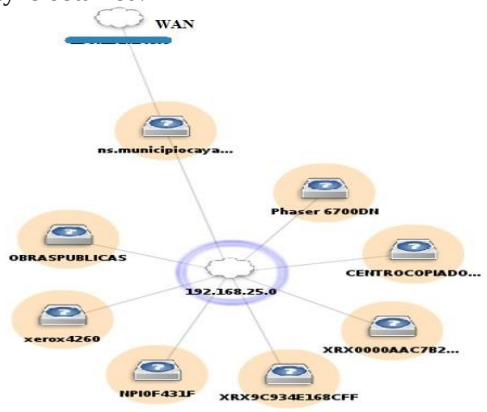


Fig. 10. LAN topology.
Source: Server Zenoss.
.

The Firewall is enabled by default SNMP with the public community, which could make an important observation status interfaces firewall visualized, the assigned LAN GADIPMC, interface has 7.92 MB maximum of bandwidth which is distributed to users for internet access, but you can see that full capacity is not occupied, making sure that does not exceed 2 MB.

TIC management is not aware of configurations to limit the bandwidth which is disturbing to know the cause of this result.

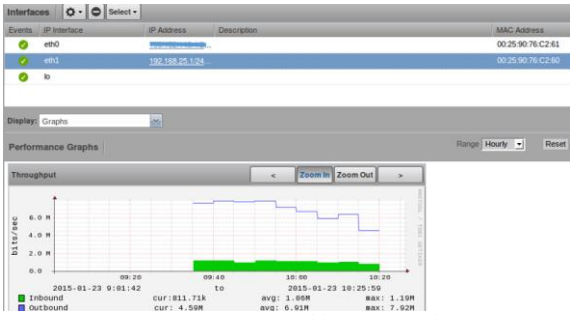


Fig. 11. Status of firewall interfaces.
Source: Server Zenoss.

D.Analysis of surveys of users.

To know the level of user satisfaction survey network was applied to a group of people, officials of the municipality, environment questions applies to the areas of:

Fault management, for the ICT department provides technical support to users, which communicate any issues related to internet, applications servers, equipment problems, etc. The questions are carried around:

- Attention to the problem reported.
- Detection of the problem.
- Problem resolution

Performance management, users are the ones who assess speed internet, and functionality of the various applications that are provided through the network. The questions are carried around:

- Speed internet connection; Y
- Network server applications.

1)Results and analysis.

A brief summary of the statistical results and an analysis of the answers given by the users is done.

Attention problems.

This item need to improve attention to the problems that users see, as there is a 47% majority stake it is sometimes said that the ICT department meets their requirements.

Detection and troubleshooting.

The staff responsible for solving the problem must diagnose the problem and find the cause, several times depends on the type of problem that may arise.

If problems are easy was the resolved quickly, 49% said that if the rapid detection is performed when the issues raised are complex, take time to resolve for the 34% who state that takes forever, and if it is not possible to identify it take the time necessary to resolve the issue.

Speed Internet.

Is required to improve the speed of Internet connection, 40% say it is slow so we must take measures to control the bandwidth and improve speed.

Network Services.

It is important that the services provided for through the local network, are always available, there is a 78% say they do not have any problem, showing that they are working well.

User satisfaction.

Several users surveyed are satisfied with the work performed by the ICT department, but there are also users who report being dissatisfied (30%) and dissatisfied (30%), the ICT department should verify that everyone network services

necessary according to the work of staff, providing internet and keep constantly available, so that percentage is reduced

E.Needs and requirements of the LAN.

Table 1. Needs and requirements LAN GADIPMC.

Problem	Needs	Requirements	Solution
Increase in the number of users.	More network points.	Restructuring the system wiring structured for the town of Cayambe.	Segmentation of the network.
Saturation of the range of available IP addresses.	Increase the range of IP addressing.	Sizing IP addressing, with scalability.	
Limited firewall.	Have control over the firewall settings.	Improve the firewall, that the administrator has full control over your settings.	Zentyal server.
	Transparent proxy	Restriction of https web pages.	
The network will become sluggish, and this sub occupied bandwidth.	Prevent the misuse of the internet and controlling the bandwidth of the network.	Improve the speed of internet connection and control the use of bandwidth.	
Too much time troubleshooting.	Meet the requirements of users in the shortest possible time.	Prevent and detect problems in the network.	Server for network monitoring.
Lack of information about the operation of the network.	Collection of information concerning the use of network resources.	Monitoring of the network, through a management software,	
	Carry documentation of the network and its infrastructure.	Manual configuration, and use of computers and servers. Take inventory.	Manual configuration and use of servers.(Zentyal and monitoring)

Source: Prepared by Cyntia Inuca.

IV. Administration And Management Of The Local Area Network Of The Municipality Of Cayambe GADIP

In this chapter the project is displayed, after analyzing the current situation of the local network management policies and procedures of local network, based on the functional management model ISO / OSI network is defined, to work through a network management system, a central network management and monitoring. Finally it presents a design network segmentation to improve network management.

A.Administration Center and network monitoring

It is a physical space, located in the department of ICT, which involved human resources, software and hardware to allow control and data visualization of network resources by monitoring applications, showing the network administrator a friendly graphical interface.

Fig. 12. Network monitoring and Management Center.
Source: Obtained from: http://iteigo.net/archives/2109

Objectives.

- Anticipate needs and network requirements.
- Monitor and control the operations of network resources.
- Provide technical support to network users.
- Maintain network information.
- Make good use of the Internet by users, and;
- Provide security across the network.

Functions.

The functions to perform in the center of administration and network monitoring are set according to each area of the functional model of the ISO/OSI network management.

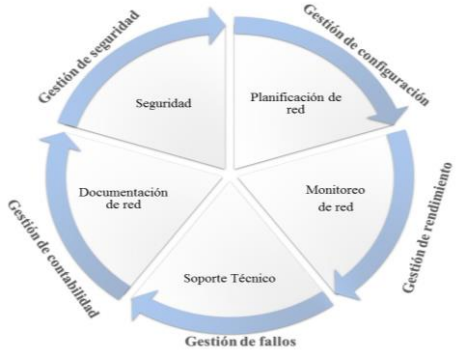


Fig. 13. Functions of the center of administration and monitoring network.
Source: Adapted by Cyntia Inuca.

(1) Network planning.

- Anticipate needs of the network, such as:
  - Growth of users.
  - Growth of technological equipments.
  - Update and implementation of new technologies and network services
- Plan local network infrastructure changes.
  - Mobility of staff and workstations.
  - Changes of settings on the computers in network.
  - Relocation, renovation or network equipment changes.
- Constantly review the network infrastructure and backbone links to work correctly.

(2)Monitoring network.

- Display of the active devices that are connected to the local network.
- Continually check the operational status of network resources.
  - Use of RAM.
  - HDD use.
  - Use network interfaces.
  - CPU (processor) usage
- Failure detection.
- Control users.

(3)Technical support.

- See, detect, and resolve bugs.
- Provide technical support to the users needs.
  - Hardware support.
    - Maintenance of communication equipment.
    - Maintenance of computers.
  - Software support.
    - Installation of operating systems, programs, and applications.
    - Update of operating systems, programs, and applications.
    - Handling and functions of systems, programs, and applications.

(4)Network documentation.

- Inventory of IP addresses.
- Inventory of elements of network infrastructure.
  - Switch.
  - Routers.
  - Servers, etc.
- Inventory of user terminal equipment.

(5)Provide security

- To internal and external network attacks.
- Control user access to the network and its resources.

B. Policies and procedures for network management.

The Administration and management of networks is a broad field in which involved elements; human, hardware and software, to evaluate the performance of network resources, based on policies and procedures is established the development of functions and processes to follow, describing a logical sequence to the activities to be held, with one goal in common.

Policies based on functional network ISO/OSI (FCAPS) management model, which comprises five functional areas are structured:

- Management Configuration
- Fault management
- Performance management
- Accounting management, and;
- Security management.

Through these manage the network by parties and improve the service provided to the municipality, ensuring the availability of the network will be achieved.

1)Establishing policies.

1. Policies for the management of local network.
- 1.1. Network management policy objectives.
- 1.2. Network management policy document.
- 1.3. Review of network management policies.

2. Policy for configuration management.
- 2.1. Network planning
- 2.2. Equipment configuration.
- 2.3. Entry of equipment.
- 2.4. Documentation of configuration.

3. Policy for the management of failures.
- 3.1. Fault management.
- 3.2. Notification of failures.
- 3.3. Documentation bug.

4. Policy for performance management.
- 4.1. Planning and acceptance of the system
- 4.2. Establishment of thresholds.

5. Policy for management of accounting.
- 5.1. Handling of reports.
- 5.2. Inventory management.

6. Policy for security management.
- 6.1. Equipment access controls.
- 6.2. Control access to management application.
- 6.3. Firewall access control.
- 6.4. Internet access control.
- 6.5. User control.
- 6.6. Protection against intruders.
- 6.7. Management of Backups.

C. Implementation of the functional model of ISO/OSI in the LAN network management.

The Administration and management of the local network of the GADIPMC is based on the functional model of network management ISO/OSI, in presenting its five functional areas, configuration management, management of security, fault management, performance management and management accounting.

For the fulfilment of these areas is implemented a network management system based on the gestor-agente paradigm that enables the monitoring of the resources that belong to the network, as well as also implemented a security system that has functions of firewall, IDS/IPS, and lets users control. Finally, it presents a design of network segmentation to improve the Administration and management of the network.

1)Configuration management.

This area is all about settings, which allows you to monitor the network, identify the devices connected to the LAN and information of its operation. This is configured a network management system, as well as also a security system.

Configuration of the network management system.

Network management system is composed by: a Manager, to manage devices and the network management protocol.

(1) Manager.

The Manager or Station Manager is nothing more than the server that allows the monitoring of network resources, network management tools.

This tool is chosen by the standard IEEE 29148, laying down requirements that must be met by the software of monitoring between the purchaser and the vendor of the application.

An analysis of the herramienstas of management most known being Zenoss the best alternative, as shown in table 3.

Zenoss allows the monitoring of the local network, unifies several capabilities, which allow you to manage the functional areas of management of fault, performance, and accounting, in a simple and modern, System interacting with the network through a web interface administrator.

Table 1. Choice of a tool for network monitoring.

Features		Zabbix	Nagios	Zenoss	Pandora FMS	Open NMS
Free Software	Free	✓	✓	✓	✓	✓
	Comercial	x	✓	✓	✓	✓
Software management		Dificulty down	Dificulty hight	Dinamic	Dificulty media	Dificulty media
Hardware resources		Down	Hight	Media	Media	Media
Functions	SNMP v2	✓	✓	✓	✓	✓
	Network auto-discovery	x	x	✓	x	x
	Auto-topology discovery	x	✓	✓	x	x
	Performance graphs	✓	✓	✓	✓	✓
	Reports	✓	✓	✓	✓	✓
	Database	Oracle MySQL, PostgresSQ.	Programado en C MySQL Postgres SQL.	MySQL PostgreSQL.	MySQL	PostgreSQL
	Management of alarms and notification of events by email	✓	✓	✓	✓	✓
Security		✓	✓	✓	✓	✓

Source: Official website of each software pages.

The administrator can auto descovery the network or enter each device to manage manually, to then obtain information of its operation.

Fig. 14. Discovery of devices.
Source: Application Zenoss.

But it is important before you start monitoring devices enable the SNMP protocol.

(2) Managed devices.

So that the network device is managed should be verified to have SNMP support. Managed servers and computers of the users of the GADIPMC network.

(a) SNMP protocol.

To enable the Protocol SNMP takes into account three aspects:

Version: Uses the version of SNMP v2c, community-based.

Community: Acts as a password used for authentication between the management station and the managed device.

Permissions: Through read-only permissions can monitor the network resources and observe its performance information.

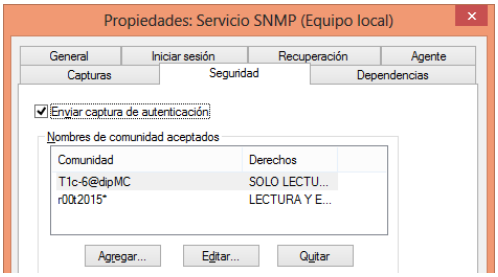


Fig. 15. Enabling SNMP protocol.
Source: Operating system Windows 7.

Configuration of the **security system.**

To provide security to the local network of the municipality of Cayambe is implemented a platform that integrates several services, Zentyal is a system based on Ubuntu, operative provides firewall, IDS/IPS, and control of users via Open LDAP, and administrator can have total control of the network through the configurations of those functions.

(1) Zentyal roles to manage the network of GADIPMC.

Table 3. Installation packages required for Zentyal.

ROLE	PACKAGE	REQUIREMENT
GATEWAY 	HTTP proxy Firewall IDS/IPS Captive portal	Limit access to web pages Protect your network from intruders Controlling user access
INFRASTRUCTURE 	DNS DHCP	Give a network domain name. Access to the network automatically.
OFFICE 	User and Computers Backup	Control user access to the network Back up the server configuration information.

Source: Derived from https://wiki.zentyal.org

DNS service: allows a domain name to the server Zentyal.
DHCP service: Automatically assigns ip addressing to the users of the network.

Fig. 15. DHCP service of Zentyal.
Source: Server Zentyal.

User and Computers Service: this service allows you to create users and user groups which are within a domain, this service is complemented by the **Captive Portal** that is applied to the LAN network interface, users must enter username and contarsena for access to the services that the network provides. The administrator can check how many users are connected in real time, in addition you can also set free enter by the captive portal users.

Fig. 16. Creation of user groups.
Source: Server Zentyal.

Backup: Allows to get a backup of the settings made on the server Zentyal, as support for emergent use.

Fig. 17. Backup of Zentyal.
Source: Server Zentyal.

Firewall/proxy service: Through this service is the filtering of web pages transparently, apply a black list of contents of domains and establish rules that deny access to web pages of obscene content, videos, downloads, music, which conseemen many network resources.

Fig. 18. Transparent proxy settings.
Source: Server Zentyal.

For https web pages, allows the creation of services and objects, which are small files that allow the creation of filtering rules that allow or deny access of an object to a service specific.

Fig. 19. Deny domains.
Source: Server Zentyal.

IDS/IPS Service: This service is activated to protect the network against attacks by intruders, are enabled to mode interfaces listen and apply rules that permit block and register access by an attacker on the network.

Fig. 20. Captive interfaces.
Source: Server Zentyal.

Fig. 21. Rules for IDS/IPS
Source: Server Zentyal.

2) Security management.

Security management is responsible for protecting the network and its components, this is based on the logical security, applying mechanisms for access control, firewall, and intrusion detection, and policy compliance.

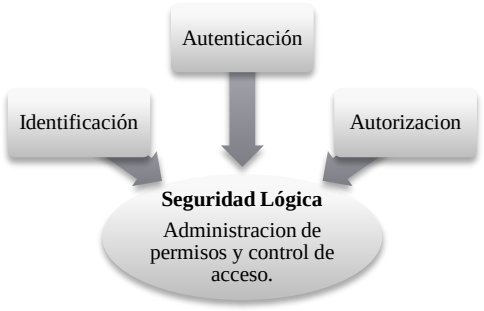


Fig. 22. Logical security.
Source: Saints. J (2011). Security and high availability. Publisher: RA-MA

Access control to the network management system.

Zenoss allows the configuration of users to manage the network, the administrator user has access to all kinds of settings and monitored information, and assign to another user so it can also monitor the network, and assign permissions equal or limited access to network information.

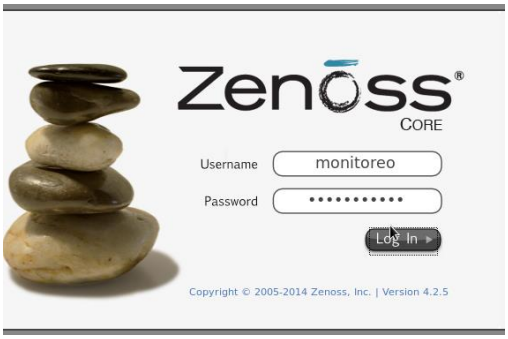


Fig. 23. Entrance to the Zenoss application.
Source: Application Zenoss.

Control of access to the security system.

Zentyal security system access will be only through the administrator user.

Access as Administrator this can enter through the web interface of the server, or through ssh.

Fig. 24. Income from administrator user to Zentyal.
Source: Server Zentyal.

For ssh access, it is necessary that you access through a computer belonging to the direction of ICT, that is set to rule the access through one of them.

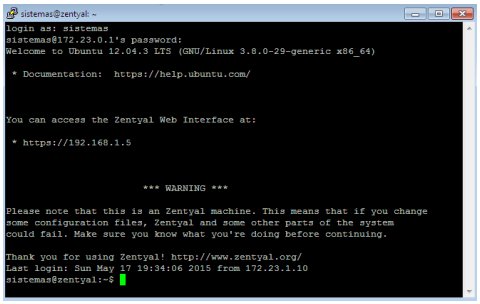


Fig. 25. Income from administrator user through ssh.
Source: Application Putty.

Control of access to computers.

Agreed to serious of console switching teams to find out your have some kind of configuration, the ip address is checked by default which is can access by web interfza.

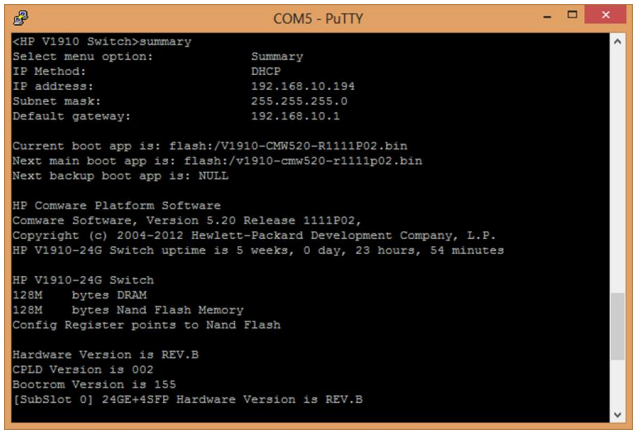


Fig. 26. Access to the console switch HP-1910.
Source: Application Putty.

Control of network users.

Users of the GADIPMC network, must enter a username and password to access the services provided by the network of the GADIPMC, is the only responsible of the use that is you of this, the administrator has the authority to register or unsubscribe from a user, can also handle users with privileges and without privileges allowing or denying access to certain services.

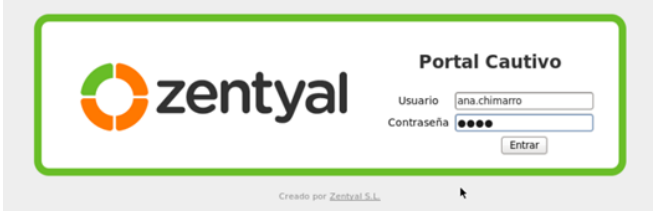


Fig. 27. By captive portal user access.
Source: Mozilla browser.

3) Fault management.

Fault management, enables constant monitoring network in order to identify faults in the same, fault management is not only limited to the monitoring if that fails with a life cycle of incidents of failure process, making it easy to keep track of the fault, to resolve it.

Fig. 28. Life cycle of incidences of failures.
Source: Adapted by Cyntia Inuca.

Zenoss allows you to follow the process of lifecycle impact of a failure in the network, detecting, isolating and diagnosing faults, through which the administrator may determine the solution to the bug occurred.

To detect faults in the network it does is proactive and reactive, acting before that happens the decision and after an unexpected failure from happening.

Zenoss has integrated essential tools such as:

- Ping.
- Traceroute.
- Snmpwalk.

Which are essential tools for preventive test connectivity and verify if a destination is reached.

Zenoss enables detect, isolate, and diagnose faults in the network, providing the Administrator information which would enable it to provide a solution to the problem. The network administrator can check the status of the bug in the console events and can also receive notifications by email.

Zenoss manages a color code to display the State or severity of the failure, and hence its priority, and identifies the device by its IP address and sums up the type of failure.

For the troubleshooting involved much the experience of the human element, same that will follow a process to solve the problem.

Fig. 29. Detection of Zenoss.
Source: Application Zenoss.

4) Performance management.

Performance management allows you to monitor the operation of the network resource information, and view it through graphs and statistical data.

Zenoss.

Using the software Zenoss verifies availability, displayed data and use of hard drive performance graphs, network, RAM, and CPU interfaces.

(1)Hard disk usage

You can review the capacity of the disk, and your partitions, size assigned to each partition, as that capacity is being used and how much is free, as well as its usefulness in percentage.

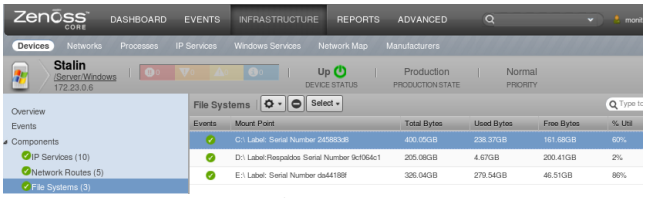


Fig. 30. Use of hard drive monitoring.
Source: application Zenoss.

(2)Monitoring of network interfaces.

All interfaces of the managed device, you will discover among them you can see the network, with the assigned IP address, and your MAC interface, and reports whether this active or not, also shows a graph about his performance with the amount of traffic that is using.

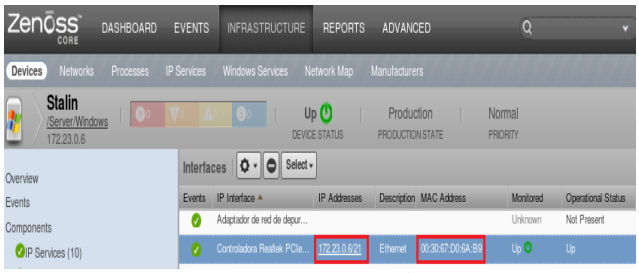


Fig. 31. Monitoring Interfaces.
Source: Application Zenoss.

(3) Monitoring memory usage.

It is important the monitoring since it is a key component for a computer to perform efficiently, and applications that make use of this resource, user flow quickly, Zenoss allows the visualization of graphs for memory usage, where the administrator can evaluate, the use that you are giving to this resource through the monitoring can make suggestions for change or increase in memory to the user's computer.

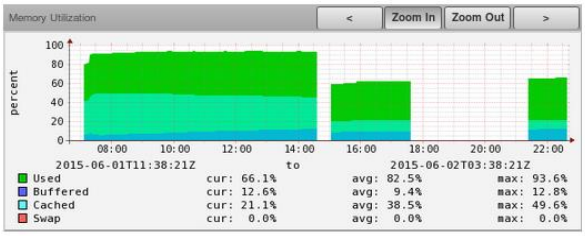


Fig. 32. Monitoring memory usage.
Source: Application Zenoss.

(4) Monitoring of CPU (processor) usage.

This resource is the core of the operation of a computer, which executes instructions, Zenoss shows the type of processor used by the team and a chart on the use that is being made of this resource.

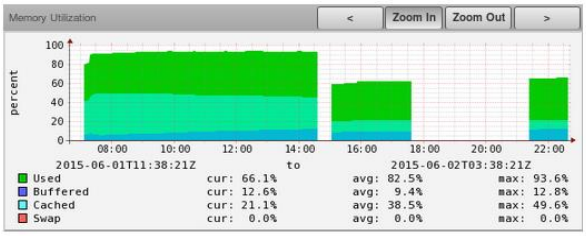


Fig. 33. Monitoring CPU usage.
Source: Application Zenoss.

Zentyal.

Zentyal displays information of the use of its resources; hard disk, RAM, CPU memory, so that the network administrator can check how is working. Also allows also to monitor the use of bandwidth.

(1) CPU (processor) usage.

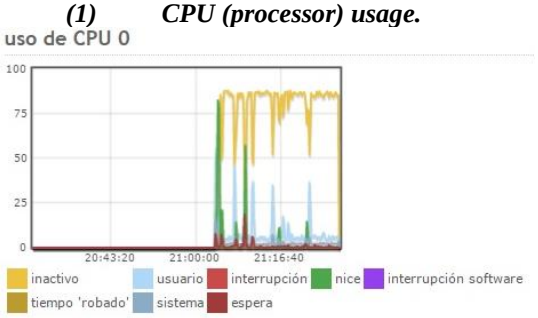


Fig. 34. CPU usage of Zentyal.
Source: Server Zentyal.

(2)Memory RAM.

Fig. 35. Use of RAM.
Source: Server Zentyal.

(3)Hard disk.

Fig. 36. Use of hard disk of Zentyal.
Source: Server Zentyal.

(4)Bandwidth.

Zentyal through you can see the use of bandwidth for each user on the network, through which the administrator can identify the user that this exceeding of this resource.

Fig. 37. Monitoring bandwidth.
Source: Server Zentyal

5) Accounting management.

Accounting management allows you to keep track of the information from the network, by means of inventories, records and reports.

The administrator must take inventory of device belonging to the local network, and complement this information with the application of network management Zenoss, which provides the administrator the monitored device performance reports.

Zentyal also provides records of HTTP Proxy, IDS, and you can also verify the users that are connected to the network.

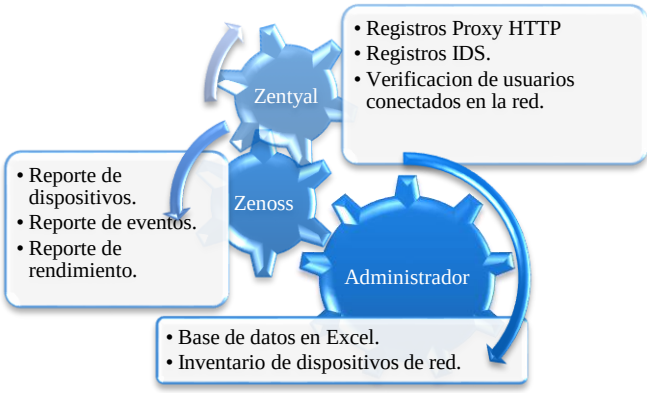


Fig. 38. Accounting management.
Source: Adapted by Cyntia Inuca.

Reports of Zenoss.

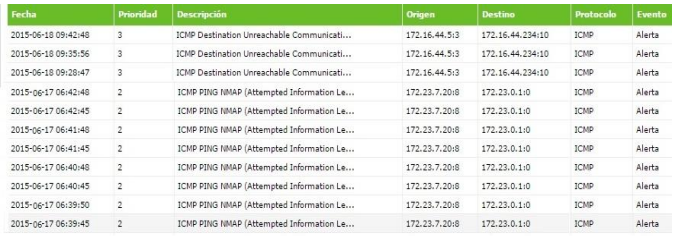
Zenoss provides several reports placed in the Reports tab, and reports of all managed devices, will be shown information like IP, MAC address, reports of events, report performance, etc.

Fig. 39. Reports of all devices being monitored.
Source: Application Zenoss.

Zentyal reports

Zentyal provides records of:

- **Proxy HTTP,** records made access to web sites, where the administrator can check the users use the Internet. The administrator can identify whether a user are trying to access a denied domain several times and track using the IP address.
- **IDS:** contains records of any suspicious activity in the network such as network information extraction, same that are recorded with an alert.



Fecha	Prioridad	Descripción	Origen	Destino	Protocolo	Evento
2015-06-18 09:42:48	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-18 09:35:56	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-18 09:28:47	3	ICMP Destination Unreachable Communicati...	172.16.44.5:3	172.16.44.234:10	ICMP	Alerta
2015-06-17 06:42:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:42:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:41:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:41:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:40:48	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:40:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:39:50	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta
2015-06-17 06:39:45	2	ICMP PING NMAP (Attempted Information Le...	172.23.7.20:8	172.23.0.1:0	ICMP	Alerta

Fig. 40. Record IDS.
Source: Server Zentyal.

6) Segmentation of local area network design.

There is a design for the segmentation of the network into vlans, under a hierarchical model with scalability, for the improvement of the Administration and security of the same.

Hierarchy of the network.

A hierarchical network is based on three-layer core (core), distribution, and access, each layer has its function.

Core layer: will link backbone, enabling internet connectivity, and add traffic to the distribution layer, this layer requires a switch to Core, to always be available and do rapid convergence, for the different services which can be implemented in the network.

Distribution layer: in this layer is where you can do configurations of routing between vlans, requires a switch layer 3, traffic will flow the switch of distribution and will be delivered to the layer core.

Layer access: this layer will be teams from end user, that they will be connected through a switch access, this may be a layer 2 switch not manageable, the access switch will be connected to the switch of distribution.

To rank a network gets benefits such as ease of expansion of the network, since it is more scalable and more users to the network can be included in any time, increased performance, ease of identification of problems and quickly to give a solution, improves management and network security.

Approach to the network segmentation.

Raises the segmentation of network into vlans, that allows to have several logical networks within a physical network, every direction that it plays within the municipality, it belongs to a vlan, each vlan will be assigned a range of IP addressing,

enough to cover the number of users of its dependence, according to these observations arises the segmentation of the network, in the following manner:

Table 4. Network segmentation approach.

VLAN	DIRECTIONS	HOST RANGE	SUB-MASCARA
10	GESTION DE TIC	172.23.0.1 - 172.23.0.126	255.255.255.128
11	FINANCIERO	172.23.0.129 - 172.23.0.190	255.255.255.192
12	AVALUOS Y CATASTROS	172.23.0.193 - 172.23.0.254	255.255.255.192
13	ALCALDIA	172.23.1.1 - 172.23.1.62	255.255.255.192
14	ADMINISTRATIVO	172.23.1.65 - 172.23.1.126	255.255.255.192
15	CONCEJO MUNICIPAL	172.23.1.129 - 172.23.1.190	255.255.255.192
16	CONCEJO DE LA NIÑEZ	172.23.1.193 - 172.23.1.254	255.255.255.192
17	DESARROLLO AMBIENTAL	172.23.2.1 - 172.23.2.62	255.255.255.192
18	DESARROLLO ECONOMICO	172.23.2.65 - 172.23.2.126	255.255.255.192
19	DESARROLLO FISICO	172.23.2.129 - 172.23.2.190	255.255.255.192
20	DESARROLLO INTEGRAL DEL TERRITORIO	172.23.2.193 - 172.23.2.254	255.255.255.192
21	DESARROLLO SOCIAL	172.23.3.1 - 172.23.3.62	255.255.255.192
22	COMUNICACIÓN	172.23.3.65 - 172.23.3.126	255.255.255.192
23	PARTICIPACION CIUDADANA	172.23.3.129 - 172.23.3.190	255.255.255.192
24	PLANIFICACION URBANA Y RURAL	172.23.3.193 - 172.23.3.254	255.255.255.192
25	PROCURADURÍA SÍNDICA	172.23.4.1 - 172.23.4.62	255.255.255.192
26	PROTECCION DE DERECHOS	172.23.4.65 - 172.23.4.126	255.255.255.192
27	SEGURIDAD, RIESGOS	172.23.4.129 - 172.23.4.190	255.255.255.192
28	TALENTO HUMANO	172.23.4.193 - 172.23.4.254	255.255.255.192
29	TRANSITO, TRANSPORTE	172.23.5.1 - 172.23.5.62	255.255.255.192
30	GESTION DE PROYECTOS	172.23.5.65 - 172.23.5.126	255.255.255.192
31	EMAPAAC	172.23.5.129 - 172.23.5.190	255.255.255.192

Source: Prepared by Cyntia Inuca.

Segmentation of the network diagram.

To distribute the network segment of vlans, administrator will maintain an ordered structure of the network, the distribution switch will have configured vlans and through trunk links you can replicate all vlans, it made the other switch, so from the different locations of the facilities of the municipality user's access through the segment to which they belong.

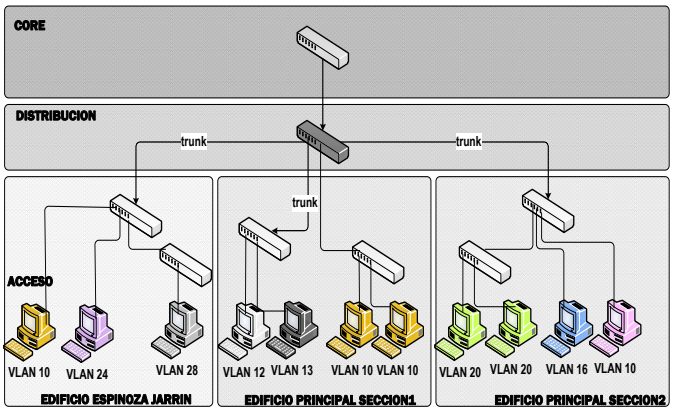


Fig. 41. Segmentation of the network under a hierarchical model.
Source: http://sistemasumma.com/2012/02/19/redes-jerarquicas/

V. ANALYSIS COST BENEFIT

This chapter is developed in order to meet expenditure involving the implementation of the project and the benefits obtained. For this chapter two aspects, first discussed in relation to the software and second hardware.

A. Software.

The project proposes free software tools, same that were chosen to meet the needs of the local area of the GADIPMC network, and these tools do not represent any cost relating to licensing.

You are currently available free software tools in multiple versions, the version of Core is free and Enterprise version. This project is made use of versions Core, since the Enterprise versions are based on capabilities that have the version of Core.

Table 5. Comparison of costs of free software tools.

Software	Annual cost	
Version	Core	Professional/Enterprise
Zentyal	$0	$1280,00
Zenoss	$0	$32.500,00
Total	$0	$34.495,00

Sources: mail electronic staff and https://store.zentyal.com/ so3137.html? _store = euro_es & _from_store = global.

Analysis of cost: The payment of annual license turns out to be a high investment, using versions Core, the institution saves money that can be invested in works for citizenship.

Analysis of benefits in using totally free software: features presenting versions Core are the basis for versions Enterprise, using the versions of Core, takes advantage of these features, and can be adapted to our needs.

Versions of Core are contributions from the community, free of charge, and are also updated.

In terms of support, the communities have forums where you can get information, ask, and contribute.

B. Hardware.

The advantage of using free software is that they can operate in teams of low hardware requirements, the municipality had computers that meet acceptable characteristics for its proper functioning, so it was not necessary to the acquisition of servers.

Then reviewed the characteristics of the hardware required for installation of softwares, available computers, and characteristics of the equipment in the event that the acquisition will be held.

Table 6. Features required by the software.

Server Features	Zentyal 3.2.	Zenoss Core.
Processor:	Xeon Dual Core	4 core
Memory:	4 GB	8 GB
Hard drive:	160 GB	300 GB
Network cards.	2 or more	1

Source**:** Es-3.2-images-intro-zentyal-install-tabla-installation-ES.png https://wiki.zentyal.org/wiki/File

The computers available in the area of ICT, meets the characteristics suitable for the correct functioning of the software, the management system, taking advantage of these features was the use of them.

Table 7. Characteristics of used hardware.

Servers	Zentyal	Zenoss
Features	Processor: i7. Memory: 4 GB Disk duro:500 GB Red cards: 2.	Processor: Intel Core i3. Memory: 4 GB. Hard disk: 300 GB. Network card: 1.
Cost:	$0	$0

Source: Computers available in the area of ICT.

To estimate the cost associated with the purchase of servers, which comply with the characteristics of the software, you have the following table, where sample value for purchase, characteristics which are attached to the requirements, these values are based on a proposed proforma.

Table 8. Cost of hardware for servers equipment.

Servers	Zentyal	Zenoss
Processor: **Memory:** **Disk:** **Network card**	Intel Xeon. 8GB 500GB 2.	Intel Core i5. 8GB. 1 TB. 1.
Cost for acquisition of hardware	$3377,70	$956,48
Total cost	$4.334,19	

Source: Pro forma TECNIT.

(This value can be used for other purposes of the municipality).

C. Benefits

The use of free software and the availability of equipment with features for the correct functioning of the software, did not represent costs, but if it was obtained benefits both for the network administrator as user.

1) Benefits of the administrator:

- ✓ Improvement of the security of the network against attacks.
- ✓ Has control of network users.
- ✓ Can review any failure in the network and respond quickly to the requirements of the users.
- ✓ Has largest number of IP addresses, to assign users.
- ✓ Obtains reports on computers that are connected to the network, and its operation.
- ✓ Can take inventory more easily since the user, IP, equipment characteristics, can be identified and;
- ✓ Monitor the use that is making the resources of the computer and the network.

2)User benefits:

- ✓ Efficient attention to the problems of the user.
- ✓ You have a network more secure and stable, with connection to the internet via a username and password,
- ✓ Administrator may suggest to the user upgrades to the good performance of your computer, equipment without that user obtaining endorsements, etc. requests it, such as expansion of hard disk, memory, network, cards

VI. Conclusions

The ISO/OSI network management functional model and the SNMP protocol, are the bases on which is based this project, since they pose guidelines for the Administration and management of a network in an organized manner, allowing you to have total control of the network.

The use of free software for network management tools plays an important role in the administrator as is presented to him as a friendly graphical interface which allows you to view the required performance data of resources which are connected in the network.

There are a wide variety of tools for network monitoring, each has its features, some complex and others simple. When searching a tool perform the management of the local network, the Administrator seeks to ease of use of the software, clear that there are very good tools but it has its level of complexity, while more functions like to make it more complex is, the choice of free software for network management tools made it through the standard IEEE 29148 It allows to establish agreements between the supplier and the purchaser of the functionalities or features that it must comply with the software, a feature important to comply was AutoDiscovery of the network.

In the analysis of the current situation was reviewed teams that has the GADIPMC LAN infrastructure, being these switch layer three and two layer, used only in mode for the interconnection of users access the network. For the segmentation of the network they should have the capacity for management of multiple vlans and enable routing between them, to act as a distribution switch, but they allow maximum

8 vlans routing, so are not suitable for the creation of vlans for directions.

Teams that work in access mode do not have any configuration that includes an ip addressing, therefore access is not enabled for ssh, the administrator can enter only console should occur any configuration.

To monitor the current state of the network, device information which had enabled snmp community public, including the firewall is detected, this shows the risk that any other user can see management information, why then carried out the monitoring network through a community to which they belong all teams the Community acts as a password for the exchange of information of management between the managed device and the Manager, this community is defined such that a password is set.

The firewall is the most important equipment within any institution network, the network administrator must have complete control over this case that it was not fulfilled in the municipality, because this was very limited to perform specific functions, this raises a security system that improves this firewall, same that allows you to manage various services and functions in a single platform, Zentyal, adding functions of firewall, IDS / / IPS, as well as allowing the control of users.

Whole process analysis of the current situation allows the compilation of needs and requirements of the local network, for which defined management policies as a guide to improve the administration of the network, being a tool of administrative support to the Manager of the network, in this defined rules to be met, that solvent these needs and requirements.

The creation of a system of network management, with tools that allow monitoring and display data of resources managed, based on a model, governed by policies, allows the administrator to make decisions and react to an unexpected event in the network, to maintain the level of network availability in a stable form.

To manage the network not only involves the snmp Protocol and management model that relies to carry out the management of network, but is also important the role played by the human resource model will be fulfilled as well as the proper functioning of the management system.

Zenoss monitors the network and handles the management of fault, performance, and accounting areas, to detect a fault allows sending notifications by e-mail, through the use of a server postfix as well as Gmail, for the project initially arose testing using a postfix server, but in the view of the functionality notifications via Gmail this medium, takes advantage of Gmail is available at all times and in every place that has connectivity to the internet, compared to the server postfix which was a local means to perform the relevant tests.

The realization of this project has provided the Manager, have control over the information of the network and its operation, no longer necessary to perform a manual inventory which was used IP addresses, the characteristics of the equipment, and the name of the user, since the equipment information obtained it through of the monitoring, and you can see the users that make use of the network through the captive portal.

The work of the network administrator or the technician in charge of the area of ICT, is to meet the requirements of the users, in the case of troubleshooting, should go to verify the problem that occurred, look for possible causes, and see alternative solutions, but now there are tools that allow you to diagnose problems, and through this provide faster solutions.

There are several versions of Zentyal, with several features, which help to improve the administration of a network, with an all in one, network administrator must be very well defined capabilities that requires your network, to implement them. Zentyal generates rules by default, why is important to know the settings that will be performed on the firewall (Zentyal), one of the important aspects are the ports that must necessarily be open.

To segment the local network under a hierarchical model, you'll get benefits such as ease of expansion of the network, since it becomes more scalable, increased performance, ease of identification of problems and speed to give a solution, since this is handled by layers, allowing the improvement of the Administration and security of the network.

The analysis of cost benefit of the project, in terms of software, settle differences that has a free software (business) license and non-license free software (core), being the version of core the best solution, since the licensed version is based on the version of core, differentiated by adding improvements, provide technical support , queries and maintenance, which version of core can get it through forums of communities of free software as well as the improvements that give you the version of core.

The benefits of the project are reflected in the network administrator and the users, since the administrator has control over the operation of the network and the users have a more stable, secure, and available network.

The use of free software tools, is beneficial since it avoids high costs in licensing, and gets the same benefits that provides a paid software.

VII. REFERENCIAS

[1] T. Saydam, «From Networks and Network Management Into Service and Service Management,» *Journal of Network and Systems Management*, 1996.

[2] R. McLeod, «Sistemas de información gerencial,» Mexico, Pearson Educación, 2000, p. 289.

[3] I. T. Union, «International Telecomunication Union,» 1992. [En línea]. Available: http://www.itu.int/rec/T-REC-X.700-199209-I/en.

[4] R. J. Millan Tejedor, «Gestion de Red,» *Windows NT/2000*, 1999.

[5] J. Kurose y K. Ross, Computer Network, PEARSON.

[6] IETF, «Simple Network Management Protocol (SNMP),» 05 1990. [En línea]. Available: https://www.ietf.org/rfc/rfc1157.txt.

[7] D. Mauro y K. Schmidt, Essential SNMP, Estados Unidos : O'Reilly Media, Inc., 2005.

[8] W. Stallings, Fundamentos de seguridad en redes, Aplicaciones y estandares., Madrid: PEARSON, 2004.

[9] Comunidad Autonoma de Castilla y Leon, Tecnicos de Soporte Informatico, Sevilla: MAD, S.L, 2006, p. 285.

[10] S. Untiveros, «METODOLOGIAS PARA ADMINISTRAR REDES,» JULIO 2004. [En línea]. Available: http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf.

[11] W. Stallings, Comunicaciones y Redes de Computadoras, Madrid: PEARSOON EDUCACIÓN, 2004.

[12] M. d. C. Romero, «Sistemas Avanzados de Comunicaciones - Gestion de Redes,» [En línea]. Available: http://www.dte.us.es/personal/mcromero/docs/sac/sac-gestionderedes.pdf.

[13] F. J. M. Robles, «Planificacion y Administacion de Redes,» Madrid-España, RA-MA, 2010, p. 605.

[14] L. R, «IP Reference,» [En línea]. Available: https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/.

[15] A. Perpinan, «ADMINISTRACION DE REDES GNU/LINUX,» de *ADMINISTRACION DE REDES GNU/LINUX*, Santo Domingo-República Dominicana, GAMMA, 2004, p. 9.

[16] R. J. Millan Tejedor, «Tendencias en gestión de red,» *Comunicaciones World*, pp. 54-56, 2004.

[17] R. McLeod, «Sistemas de información gerencial,» de *Sistemas de información gerencial*, Mexico, Pearson Educación , 2000, p. 298.

[18] A. B. Martí, Gestión de Red, Barcelona: Universidad Politecnica de Cataluña, 1999.

[19] T. Magazine, «Optimización del rendimiento de la CPU de SQL Serve,» 2008. [En línea]. Available: https://technet.microsoft.com/es-es/magazine/2007.10.sqlcpu.aspx.

[20] J. Lázaro Laporta y M. Miralles Aguiñiga, Fundamentos de Telemática, Universidad Politecnica de Valencia, 2005.

[21] I. Hoy, «Como optimizar la memoria RAM,» 2012. [En línea]. Available: http://www.informatica-hoy.com.ar/.

[22] P. Gil, J. Pomares y F. Candela, «Redes y Trasmision de Datos,» de *Redes y Trasmision de Datos*, 2010.

[23] J. Curry, «Gestión de Eventos para Zenoss Core 4,» Enero 2013. [En línea]. Available: http://www.skills-1st.co.uk/papers/jane/zenoss4-events/zenoss_Core4_event_management_paper.pdf.

[24] Zenoss Community, «Zenoss Documentation,» 2005-2015. [En línea]. Available: http://www.zenoss.com/sites/default/files/documentation/Zenoss_Core_Administration_02-022014-4.2-v08.pdf.

[25] ZABBIX, «ZABBIX,» 2001-2015. [En línea]. Available: http://www.zabbix.com/features.php.

[26] Artica Soluciones Tecnologicas, «The monitoring wiki PANDORA FMS Enetrprice,» 2006-2012. [En línea]. Available: http://wiki.pandorafms.com/index.php.

[27] Comunidad Autonoma de Castilla y Leon, «Tecnicos de Soporte Informatico,» de *Tenicos de Soporte Informatico*, Sevilla, MAD, S.L, 2006, pp. 286-287.

[28] Diego Borja, «PROYECTO DE CABLEADO ESTRUCTURADO DEL GAD MUNICIPAL DEL CANTON CAYAMBE,» 2012.

[29] Zentyal Community, «Documentacion oficial de Zentyal.,» [En línea]. Available: https://wiki.zentyal.org/wiki/Es/3.2/Zentyal_3.2_Documentacion_Oficial.

[30] Zenoss Own IT, «¿Por que Zenoss?,» 2005-2015. [En línea]. Available: http://www.zenoss.com/solution/why-zenoss.

BIOGRAPHIES

Cyntia M. Inuca G. Is born an April 8, 1990 on Gonzales Suarez - Otavalo - Ecuador. He completed his primary studies at the school of practice teaching "Juan Montalvo", high school ends them in the "Otavalo" Technological Institute in 2007 in specializing in mathematical-physical, is currently finishing his studies at the Technical University in the city of Ibarra North, to obtain the title of engineer in electronics and communication networks.

He made his preoccupational work practice in the town of Cayambe in the Department of information technologies and communication, where performance tasks of technical support around the infrastructure of internal data network of the municipality; installation of new points of network, configurations of communication equipment, inventories of computers interconnected to the network and IP addressing, design wiring structured for building Espinoza Jarrin, the municipality also is responsible for the wireless network of the educational institutions of canton of Cayambe, where is endowed with several schools internet service, installation activities , maintenance and configuration of antennas, wireless routers, to the formation of the network of institutions.