

Management model of functional network in the local data network at San Miguel Ibarra Government Autonomous Decentralized based on the standard ISO

Carlos A. Vásquez, Viviana E. Ayala

Abstract- Nowadays the challenge of companies and organizations is that their services are available 365 days a year, this means that the network elements function effectively

Analyzing the reality San Miguel de Ibarra Government Autonomous Decentralized (Ibarra-GAD), this project proposes the implementation of a management model functional network in critical areas of the local data network, which is based on ISO standard, using free software tools in order to optimize network resources. Thus enabling timely action to any event that may happen

By implementing management software can be maintained monitored network devices, 24 hours a day, 7 days a week, which allow you to have a knowledge base on incidents that occur, enabling the network administrator take timely corrective action on the most devices sensitive to faults.

Indexed terms—ISO, NMS, ITU-T, UDP, SNMP.

I. INTRODUCTION

San Miguel de Ibarra Government Autonomous Decentralized It's located in Ibarra canton, Imbabura province. It is an entity of public law consists of a human community, which manages its own financial resources, whose purpose is the local common good and, in this and primarily, the attention to the needs of the city, the metropolitan area and the rural parishes of the respective locality

It is an organization that every day is committed to the widespread use of information and communications technology (ICT), forming an integrated all its units to toast connectivity services platform through hardware and software tools to satisfy requirements and demands of the canton users.

Document received in June 2015. This research was realized as a preliminary project to obtain the professional title in the Engineering Electronics and Communication Networks Engineering of Applied Science Faculty (FICA) North Technical University.

C.A. Vásquez, North Technical University professor, In the Engineering in Electronics and Communication Networks career, Av. 17 de Julio El Olivo sector, Ibarra-Ecuador (fhone: 5936-2955-413; e-mail: cava_6@hotmail.com).

V.E. Ayala, graduate in Engineering in Electronics and Communication Networks career (Phone: 5939-2054-723; e-mail: ayala_yandun@hotmail.com).

Therefore it is proposed to realize a management model functional network through based on free software tools that are capable of allowing a glimpse of the state of the devices in the network infrastructure in order to maximize efficiency, productivity and availability , which involves active and passive surveillance to detect and solve problems, thus improving the performance of the same.

II. FUNDAMENTALS OF NETWORK MANAGEMENT

A. Network Management

It's a process of planning and control of all activities that manage network performance data of an organization, in order to obtain the maximum benefit possible.

It has the capacity to ensure that the use of the network is carried out effectively, improving the continuity in the operation of the network by monitoring mechanisms that help solve problems and be monitored resources [1]

B. Network Management.

According to ISO (*International Organization for Standardization*) said network management as: The set of activities necessary for the control and monitoring of resources that help the exchange of information flowing through the data network, increasing its functionality and performance. [2]

C. Elements of a network management system.

According as specified in RFC documents from the Internet and distributed management system comprises the following elements in Figure 1 is indicated each of them:

Managed devices. - Equipment that communicate with the network, with the purpose to be monitored are called managed elements or network, such as routers, switches, servers, computers, printers, so on.

Manager.- It's the console through which the network administrator performs network management functions

generates management operations (commands, requests) and received (responses, notifications) agents.

Agents.- They are software modules that collect and store local information about managed devices in which you reside and then store this information in a database management, to provide it to entities management through a network management protocol network.

Network Management Station or Network Management Station (NMS).- They are independent devices that serve as an interface between the administrator and network.

Network management protocol.- It's used to convey management information between the agents and network management stations (NMS).

Base de Información de Gestión (MIB).- It's derived from the network management model OSI/ISO and It's a type of database used to manage the devices in a communications network. It consists of a collection of objects in a database (virtual).

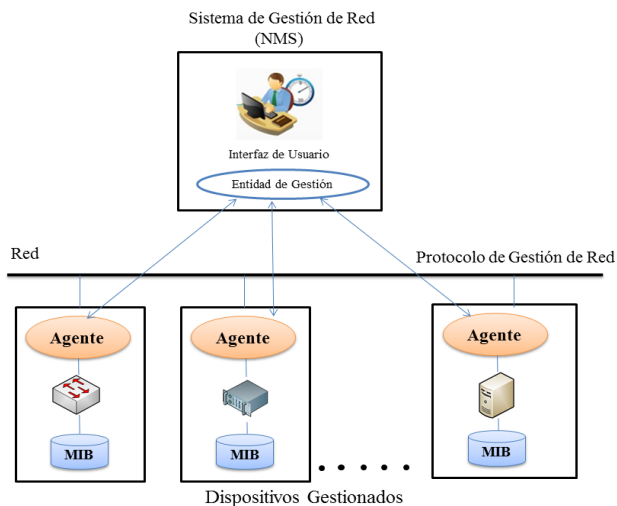


Figure 1. Elements of a network management model
Font: (Ding, 2010)

D. Functional model of network management based on ISO standard.

(ISO / IEC , 1989) and UIT-T (International Telegraph and Telephone Consultative Committee (CCITT-UIT), 1992) have defined a management model functional network which covers the five functional areas known as FCAPS is an acronym of faults(Fault), Configuration (Configuration), Accounting (Accounting), Performance (Performance), and security (Security) as indicates the Figure 2, areas that define the tasks of network management.

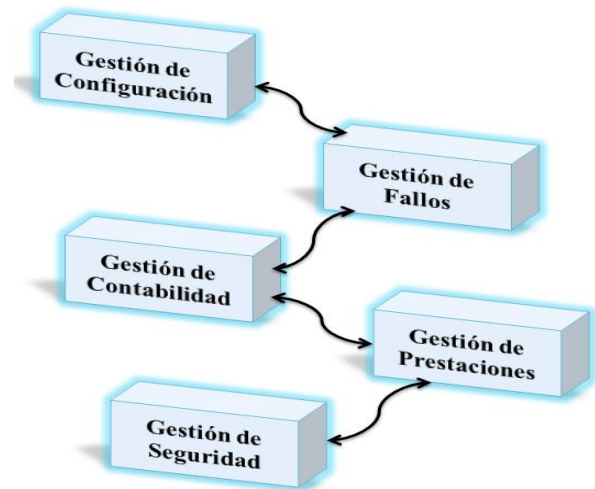


Figure 2. Functional Model Areas.
Font: (Jorquera, 2010)

Configuration Management.

Configuration management refers to keeping design information and current network configuration. This area is perhaps the most important network management because improper settings can cause the network does not work at all. [3]

This management area is related to the detailed operation of the hardware and software configuration as explained to continue:

- *Hardware configuration management*

It's objective is show what the infrastructure and illustrate the physical locations and linkages between each element, known as configuration as elements.

- *Gestión de configuración de software*

Inside of the process of software configuration management network includes:

- ✓ Configuration identification.
- ✓ Control configuration changes.
- ✓ Determining the status of settings.
- ✓ Authentication Settings.

Fault Management.

This area of management has as objective detect, isolate and fix abnormal behaviors that affect performance and availability of the managed network also performs maintenance, analysis of error logs sequences diagnostic tests and fault reporting.

Inside the functions of fault management is the following. [4]

Avoid the failure before it happens, here the proactive management and the management is preventive tests.

If the failure has happened, It's known as reactive where its find the following parameters:

- Detection of faults

Determines the cause of a fault is in the process of capturing directions as alarms (users or tools), about disorder in the networks provided by devices that bad functio.

- Fault Isolation

It's analyze a series of fault indications observed for an explanation of the alarms. This phase includes the identification of the cause leading to the spread of a fault and determine the root cause.

- Fault Diagnosis

It refers to the failure monitoring, observation of symptoms, making hypotheses based on the experience of the manager and the record of previous, hypothesis testing where realize a set of tests to approve or discard different hypotheses.

Management Accounting.

Management Accounting it's based on the record of the use of resources and services provided by network users. Inside this Management mentione the following:

Management accounting functions

To continue it's listed the main tasks and functions performed by the management accounting:

- Data collection about the use of resources.
- Maintenance of the registration user accounts.
- Maintenance of statistics to use.
- It helps to maintain network performance to an acceptable level.
- Definición Definition of procedures to tarification

Performance management.

It refers to evaluate the performance and ensure the correct operation of the managed devices and the effectiveness of certain activities also collects and processes the measured data to generate reports corresponding.

management functions of provide.

To continue it's pointed the functions or tasks of the management area:

- Capture the data or performance indicator variables, such as effective data rate of the network, response times to users, among others, resources (CPU utilization, available memory, disk utilization, ports) and compare this information with normal values or desirable for each uno. b
- Analyze the data to determine normal levels of performance.
- Generate reports and statistics.

Security Management.

Security management refers to the set of functions that protects networks from unauthorized access, so it is related to the generation, distribution and storage of encryption keys, passwords information. It is also responsible for protecting communications equipment, servers and workstations from attacks from third to maintain system integrity.

E. Simple Protocol Network Management (SNMP)

It's an application layer protocol based on the TCP / IP architecture, this makes possible the exchange of management information between network devices. SNMP enables network administrators to monitor network operation, configure computers, find and fix bugs, plan network growth, analyze performance of equipment, information access products from different vendors in the same way, developing a common tool monitoring.

SNMP components.

SNMP has the following main components were clarified below, which interact to establish its operation as shown in Figure 3:

- Network Management Station (NMS).
- Agent.
- Network Management Protocol.
- A management information base (MIB).

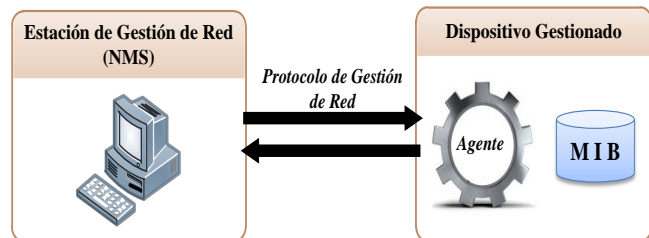


Figure 3. components involved in SNMP
Source:(Guerrero Pantoja, 2011)

These components interact with human operators and trigger the necessary actions to carry out the tasks they invoked or planned

F. Services offered GSM.

The GSM mobile phone standard facilitates the existence of a number of services, without need for an external modem via a card for connection to the computer's serial port. It offers a short alphanumeric messages (SMS) up to 160 characters and a all range of supplementary services.

G. ANALYSIS OF actual INFRASTRUCTURE OF LOCAL NETWORK DATA IBARRA- GAD.

H. Physical topology of the local data network.

In the diagram shown in Figure 4 the structure of the physical topology of the local network data Ibarra -GAD, where look at LAN connections in the links that go to the building of internal and external dependencies.

Besides it's can see the core switch connection via fiber optic link Telconet which deliver a bandwidth of 10 Mbps to the network entity, the connection of the physical servers in the data center is also observed and wireless links that go to the white city park area where citizen participation is and to the municipal cellar.

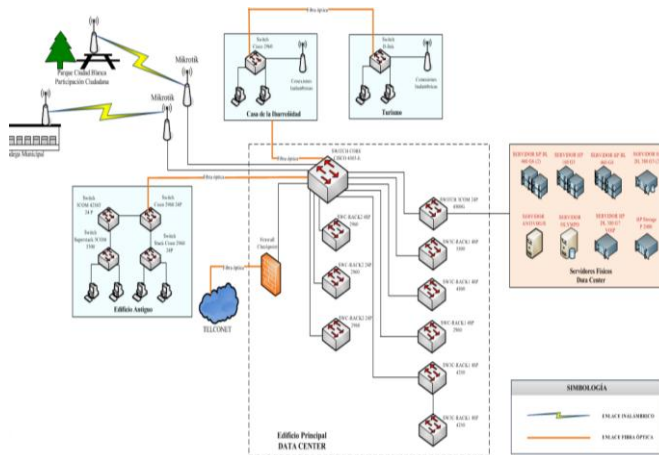


Figure 4. Physical network topology data
Source: (Hardware and Comunicaciotions unit, 2013)

I. Analysis of the infrastructure local network data to identify critical areas.

After obtaining the data of the physical and logical infrastructure of the local data network Ibarra-GAD it proceeds to an analysis in conjunction with the administrator of the network, which determines critical areas and equipment greater priority which will make object for subsequent implementation [5]

Analysis for choosing of switches.

It is determined that the primary critical area of the network is the data center, taking into consideration his unavailability would cause the collapse of the entire network of the entity, for this reason it is of paramount importance to implement a management model that can help prevent with they arriving to fail the active elements network.

It's determine the Network devices according highest priority to establishing a layered hierarchical model, with its respective port line diagram, as shown in Figure 5. It's structure into three

layers which are: nucleus, distribution and access which comply specific functions described below:

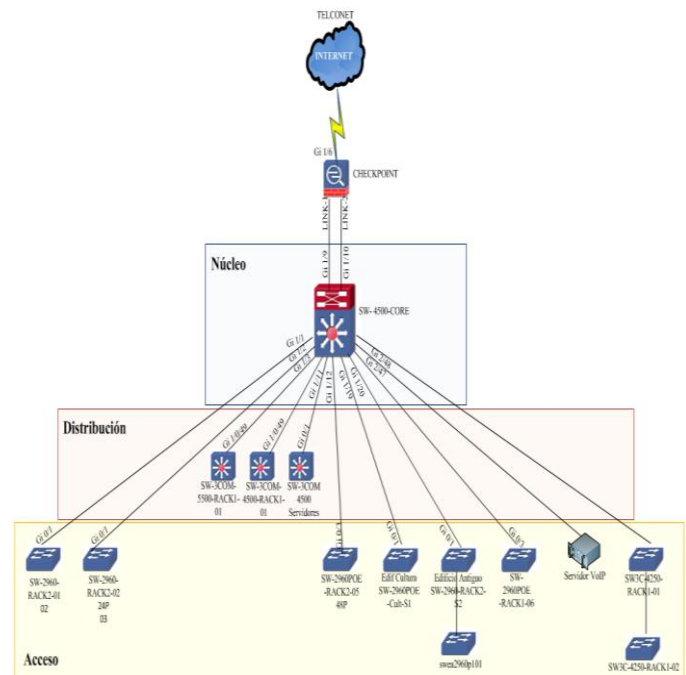


Figura 5. Modelo Jerárquico de la red del GAD-Ibarra
Fuente: (GAD-Ibarra, 2013)

Core

This layer is formed by a Cisco Catalyst switch 4503-E high performance is the Core or Core. This equipment is interconnected through one controller to the distribution layer, access layer and together with Check Point Firewall equipment; the same as in turn connects to the Internet network Telconet. And through controller two connected with a switch of the access layer and the VoIP server.

Therefore the functions has inside the network of the organization in this layer has been identified only 4503-E switch as critical priority and also meet the technical specifications to carry out the implementation of the management model.

Distribution

Inside of this layer three switches 3Com where; the switch 3Com, 4500G for being in charge of the operation of physical and virtual servers and priority is critical, because this device depends ensure delivery of services to users of the entity 24 hours a day. And the other switch are responsible of interconnect network segments of the main building therefore are considered as critical.

Access

This layer is responsible for establishing connectivity with end users of the entity as integrating network equipment; Network printers, computers, IP phones, Access Point, among others. The switches that form are layer have a management VLAN's that allow segmenting broadcast domains, and provide greater

security for the end node devices on the network, so that has been established as a critical area.

It was considered to manage the switch located in the department of Culture since this switch maintains connectivity for sending information to the main building, it is critical because here realize social activities and projects to be supervised by the authorities of higher order.

Moreover two switches that are in the old building which provide connectivity to the ground and first floor of the same. Together the switch chosen to manage this critical area are manageable and support enabling SNMP.

Analysis to choosing physical servers.

Servers involve highly relevant to the entity, so that the interruption of their services involve a high value of losses is why its functionality is essential. Among the most critical is the following:

- POSTGRESQL server.
- OLYMPO server.
- Antivirus server.
- HP server.

Analysis for choosing virtual servers.

The analysis to choosing virtual servers are made taking into account the availability of functioning of the services provided by each entity within the then points out each server is selected to monitoring:

- Mail server.
- DNS y DHCP server.
- Server Quipux documentary.
- Server repositories.
- Web Application Server.
- SRI Server.
- MAPSERVER server.
- WEBSERVICE server.
- POSTGIS database server.

J. MANAGEMENT LOCAL NETWORK OF DATA

IBARRA - GAD

Establishment Management Policy for Local Data Network Ibarra -GAD.

In this point management policies, based on the areas of management model functional network based on the ISO standard and are directed towards network administrators who are committed to fulfill to effectively maintain the availability of function of the devices critical network.

Organizational levels

- a) Director.- Authority upper level. Under his administration it is accepting management policies, in agreement with the manager of the Hardware and Communications Unit and Computer Unit.

- b) Unit Manager Hardware and Communications: Person in charge of the preliminary analysis of the state of the network entity through assessments of availability, maintenance and performance. Maintains reporting procedures performed together in coordination with computing Unit.
- c) Computing Unit. - Department inside the entity, which is responsible for the operation of the Data Center for the effectiveness of data processing and information with everything related to the installation of LAN and WLAN, use, maintenance and updating of computing equipment.

Validity

The documentation present with their management policies will take effect from the time it is approved as a technical document network management by the relevant authorities of the ICT department of the Ibarra GAD.

Reference

The present document is realized taking like reference the format the institution has a last project. [6]

Nowadays there isn't specific standard that helps the development of management policies for that reason is realized taking as guide the functional areas of management model based on the ISO standard:

Management Policies of the local area network data

Objective Of Management policy.

- ✓ Authorities engagement.
- Configuration Management
 - ✓ Income network device management software.
 - ✓ Configuring network devices.
- Management failures .
 - ✓ failure handling.
 - ✓ Management thresholds.
- Management Accounting.
 - ✓ Parámetros de monitoreo.
- Monitoring parameters.
 - ✓ Collection of statistical data network performance.
 - ✓ Reports.
- Security Management.
 - ✓ Access Management Software.
 - ✓ Access to managed network devices

K. Implementation Management Tools Local Network Data Ibarra –GAD.

Implementation inside the Configuration Management.

This management area comprises the analysis of the current state of the data network of Ibarra –GAD to meet the physical and logical state in which it's located.

Requirements to choose the management software.

Inside of this management area is required prior comparative analysis of the functionalities and best features of management software, has been selected Pandora FMS, Zabbix, Cacti and Nagios. Management software was chosen based on the IEEE Std. 830-1998, by reference to the fulfillment of FCAPS management model and the needs of the entity.

It was chosen Nagios because it meets aspects; to present centralized management interface, support remote monitoring of multiple operating systems, setting thresholds that generate alerts when they reach their maximum performance and send e-mail notifications or SMS network administrator provides various options for generating reports, statistics, based on the information collected and also supports installation in a virtualized environment essential feature for the development of implementation [7]

Design used to implement the management model functional network

Once determinate the management software to use and the requeriment hardware needs to your function proceeded to perform design management system as shown in Figure 6. Where it is explained that the management server Nagios is installed on an HP BL 460 G6 physical server using a virtualized environment, it was inducted into the operating system Debian 6.0.1 because servers are currently in a virtualization environment and using this version of free software.

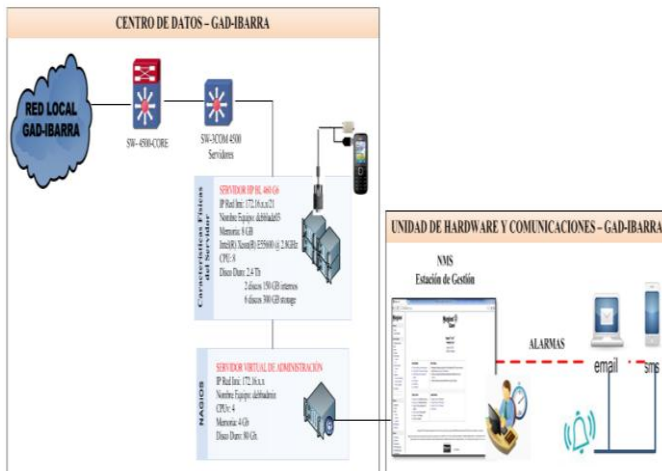


Figure 6. Design Management System implemented
Source: Based on ICT inventory Ibarra- GAD

Configuration Manager.

Inside this supplement configuration management sequence of installation steps need Nagios management software for operation and in Figure 7 it's illustrate the same:

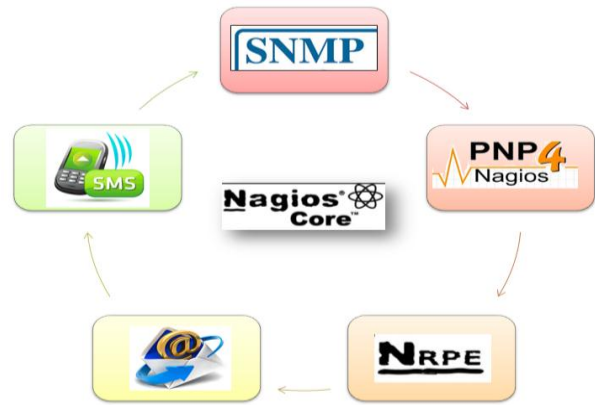


Figure 7. Representation of the order of installation
Source: Based on Nagios management software

- Installation and configuration management software Nagios.
- SNMP Setting to communicate with the agents.
- Setting pnp4nagios to generate graphs of critical links.
- NRPE Setting Nagios complement to communicate with physical and virtual servers running inside free software.
- Server setting of mail so, serves as transport for sending mail to the administrator about critical states of managed devices.
- Application setting to send of para el envío de short text messages (SMS).

Implementation inside the Fault Management.

Inside this fault management presented two scenarios to consider

- avoid failure before it happens in charge proactive management and management of preventive tests.
- If the failure has occurred is responsible reactive management.

Proactive management.

This management determines a failure before it happens, that is determining thresholds in the Nagios software for the administrator to view faults and according to the colors has to take remedial action.

Threshold definition

The thresholds set forth below in Table 1 are based on the characteristics of the managed device, for that reason a margin or percentage reference.

Tabla 1. Thresholds for Monitoring

Managed devices	metrics	thresholds warning (WARNING)	thresholds critical (CRITICAL)
	CPU charge	70 %	80 %

Switches			
Memory (RAM y Flash)	30 %	20 %	
spent of bandwidth interfaces	40 %	50 %	
Servers			
CPU charge	60 %	75 %	
Memory(RAM y Swap)	30 %	20 %	
Cd	25 %	15 %	
Margen de funcionamiento recomendable			< 60%

Source: Based on monitoring thresholds

It's established Warning threshold to administrator can give a quick fix before the managed device reaches a critical state and thus optimize their resources. [8]

Management of preventive tests.

This management is responsible for avoiding failure before it happens through tests that are explained below:

. Testing physical connectivity.

Tests realized to verify that the transmission means are in operation, namely; network cards, network cables, cables power supplies, ups, voltage regulators.

. Logical connectivity tests.

Reactive management

This type of management is executed when the fault has occurred and the process to detect, isolate, diagnose, correct and document as shown in sequence Figure 8:

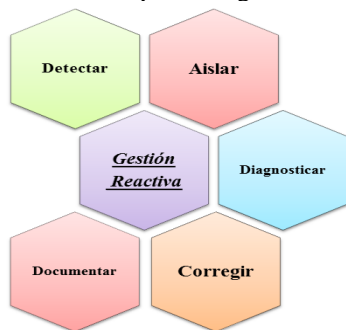


Figure 8. Reactive Process Management
Source: Based on Reactive Management

Detect.

Nagios allow detect in the first signal issued the decision by displaying changing colors on the map of the web interface according to (parents) ie device that is affected, a switch of the access layer that is connected to the switch core or server that is connected to a switch of the distribution layer. Figure 9 is

observed as Nagios allows the administrator to easily detect a fault.

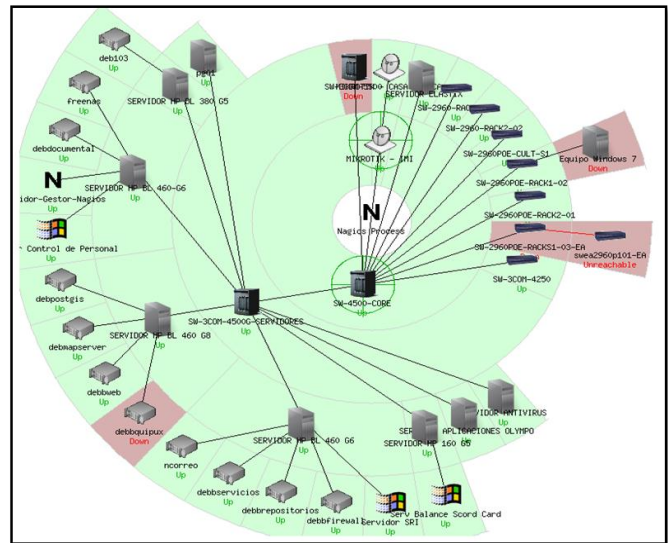


Figure 9. Detect on the map of the web interface
Source: Extracted manager Nagios

Sending notifications route email and SMS

Moreover the network administrator can detect a fault when Nagios making the notification of the existence of a fault and where it has been generated through a text message or an e-mail in the following instances.

In the figures 10 y 11 it's indicate a notification send from Nagios to the mail electronic count Gmail which reports that there is a problem, the number 17 service which is configured interface GigabitEthernet 1/20 fiber optic link that connects the Old Building of Switch_CORE with IP address 172.xxx presents a critical state because the interface is down (down).

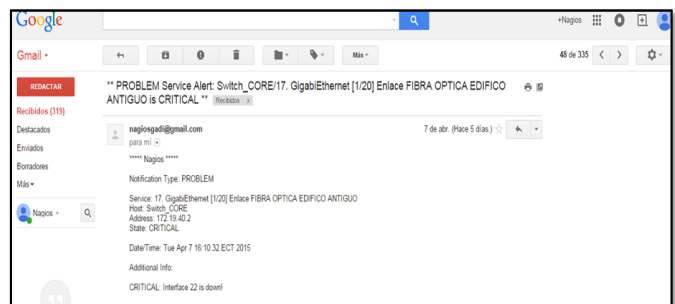


Figure 10. Sending email from Nagios
Source: Extracted from Gmail mail account created specifically for the entity

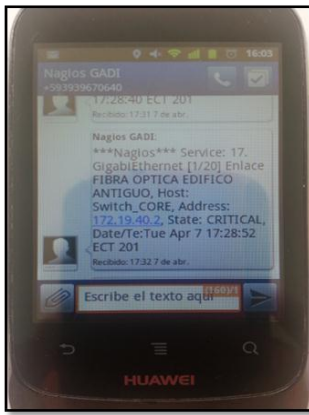


Figure 11. Sending text message from Nagios
Source: Extracted from mobile phone network administrator


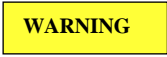


Isolate

Nagios can isolate a fault by the hierarchy of network devices called parents (parents) where you can easily isolate that managed network device is affected and not for lack of such equipment is affected throughout the network, also allows isolating a failure by a alerts hierarchy according to operating conditions generated by each device as shown below:

Hierarchy alerts

Table 2 indicates how to isolate one depending on the color generated by the managed devices according to hierarchy alerts by five types of state failure, and of trying that other teams are not affected because of the same problem to find the best solution.

Table 1. Hierarchy of alerts generated by Nagios

Estado	Representaciones	Descripción
Recovery/Recuperado		When a host is in UP or service is OK in the latest status check.
Warning/Advertencia		When it has detected problems in the last check on a host or service, before becoming critical.
Down/Abajo		When the last status check failure has occurred, a host is in Down / Down or unreachable / unreachable. When a service is in state Critical / Critical because they present problems that go beyond the normal operating thresholds.
Unreachable/Inalcanzable		
Critical/Crítico		
Unknow/Desconocido		When a service is not well defined this state has known.

Pending/Pendiente

PENDING

When a new setting is recognized.

Source: Data obtained from Nagios management software

Diagnostic

Once it's has detected and isolated the source of the fault either equipment or services were affected. It proceeds to establish a diagnosis by Nagios possible causes that have caused a fault:

- The managed device logical connectivity lost, there isn't response times in both directions of communication.
- The managed device physical connectivity lost, broken network cables, network cards damaged.
- Managed devices don't respond to SNMP requests
- Just by to click on the device has been detected and isolated Nagios diagnosed a critical failure when there is a high consumption levels normal thresholds.
- Failures that are related to network traffic and the lack of availability of services

Correct.

Following the process of reactive management in this part must be taken sufficient actions to repair the damage. Among the most common and most used mechanisms include the following:

- Replacement of damaged resources, there are network equipment for changing modules instead of changing it completely. In the local network infrastructure data GAD-Ibarra most susceptible to failure and more critical in the networked computers are the Cisco Catalyst 2960 series which are part of the access layer.
- If you have a redundant resource, the service is changed to this item. At this point, the network design of the entity's existence has an active redundant connection to the server chassis, thus ensuring the normal functioning of the services used by the different teams of the distribution layer and the layer core.
- Network devices are stabilized recover connectivity and if they are restarted.

Document.

The documentation will be registered in a database for its respective management and monitoring. In addition it should be emphasized that this management area is the responsibility only of the entity.

Implementation inside Management Accounting.

Inside the management accounting it is considered the following parameters chosen according to the needs of the local data network Ibarra - GAD:

- Monitoring parameters.
- Status parameters.
- Check parameters.

Implementation inside Performance Management.

This area of management is to keep constantly monitored the status of managed devices and safeguard its performance to determine whether this behavior in a time interval or real time.

Performance of the Layer core

Nagios allows the administrator web interface displayed on the name of the managed device, which is monitoring service, state check time, duration and service information in real time. Then the parameters indicating the web interface in the Figure 12

Host	Service	Status	Last Check	Duration	Attempt	Status Information
SW-4303-CORE	01. PING	OK	04-01-2015 14:51:34	154.48-42m 56s	1/3	PING OK - Packet loss = 0%, RTT = 1.26 ms
	02. Memoria RAM	OK	04-01-2015 14:54:04	154.48-43m 26s	1/3	OK: Processor: valid, Used: 1271472608 Free: 86709408 (41%)
	03. Sensor de Temperatura Chassis	OK	04-01-2015 14:53:49	04.2h-34m 54s	1/3	SIMP OK: "Chassis Temperature Sensor"
	04. Carga de CPU	OK	04-01-2015 14:54:05	154.48-43m 36s	1/3	OK: CPU(000): 17% 20% 21%
	05. Ventilador	CRITICAL	04-01-2015 14:53:51	154.48-43m 18s	3/3	CRITICAL: Power Supply 1 Fan: normal Chassis Fan Tray 1: normal Power Supply 2 Fan: notPresent!
	06. Fuente de Alimentacion	CRITICAL	04-01-2015 14:54:05	154.48-43m 56s	3/3	PS: Ch1 - 2 PS are running, Power Supply 2 -> notPresent have an error

Figure 12. Service yield figure of Switch Core
Fuente: catch own taken Nagios management software

Processing core switch does not exceed 25% peak utilization during the ten months of monitoring so it follows that the sizing of the network computers meets the actual needs.

In Figure 13 present the yield by Nagios web interface of each of the Gigabit Ethernet and VLAN interfaces configured the core switch and are connected to different distribution and access switches entity performance shown.

07. GigabitEthernet [11] Hacia SW-2960-RACK1-01	OK	03-22-2015 11:35:56	4d 23h 44m 43s	1/3	OK - Average IN: 184.29Kbps 0.15% Average OUT: 222.33Kbps 0.22%
08. GigabitEthernet [12] Hacia SW-2960-RACK1-02	OK	03-22-2015 11:36:06	2d 0h 43m 45s	1/3	OK - Average IN: 42.99Kbps 0.04% Average OUT: 165.08Kbps 0.16%
09. GigabitEthernet [13] Hacia SW-300M-550D-RACK1-01	OK	03-22-2015 11:36:31	2d 2h 46m 44s	1/3	OK - Average IN: 12.34Kbps 0.01% Average OUT: 44.00Kbps 0.04%
10. GigabitEthernet [17]	OK	03-22-2015 11:36:46	2d 2h 46m 42s	1/3	OK - Average IN: 1.24Kbps 0.00% Average OUT: 18.52Kbps 0.02%
11. GigabitEthernet [16] Hacia LINK-1-CHECKPOINT	OK	03-22-2015 11:36:21	2d 2h 46m 43s	1/3	OK - Average IN: 4.31Mbps 4.31% Average OUT: 157.59Kbps 0.16%
12. GigabitEthernet [110] Hacia LINK-2-CHECKPOINT	CRITICAL	03-22-2015 11:36:16	5d 1h 27m 29s	3/3	CRITICAL: Interface 12 is down!
13. GigabitEthernet [111] Hacia SW-300M-SERVIDORES	OK	03-22-2015 11:36:15	2d 0h 15m 43s	1/3	OK for 13 - Average IN: 77.49Kbps 0.01% Average OUT: 455.74Kbps 0.05%
14. GigabitEthernet [112] Hacia SW-2960POE-RACK1-05	OK	03-22-2015 11:35:51	2d 2h 46m 6s	1/3	OK - Average IN: 406.27Kbps 0.41% Average OUT: 2.53Kbps 2.53%
15. GigabitEthernet [115] Hacia CUARTEL	CRITICAL	03-22-2015 11:36:11	4d 23h 36m 14s	3/3	CRITICAL: Interface 20 is down!
16. GigabitEthernet [118] Enlace FIBRA OPTICA CULTURA	OK	03-22-2015 11:36:31	2d 2h 46m 6s	1/3	OK - Average IN: 11.64Kbps 0.01% Average OUT: 36.42Kbps 0.04%
17. GigabitEthernet [120] Enlace FIBRA OPTICA EDIFICIO ANTIGUO	CRITICAL	03-22-2015 11:35:58	4d 23h 36m 13s	3/3	CRITICAL: Interface 22 is down!
18. GigabitEthernet [247] Hacia SW-2960POE-RACK1-06	OK	03-22-2015 11:35:58	2d 2h 46m 6s	1/3	OK - Average IN: 11.19Kbps 0.01% Average OUT: 27.49Kbps 0.03%
19. GigabitEthernet [248] Hacia Servidor VoIP	OK	03-22-2015 11:36:45	2d 2h 46m 11s	1/3	OK - Average IN: 16.59Kbps 0.02% Average OUT: 26.79Kbps 0.03%
20. VLAN 1	OK	03-22-2015 11:36:29	2d 2h 46m 41s	1/3	OK - Average IN: 134.13Kbps 0.13% Average OUT: 4.55Kbps 4.55%
21. VLAN 2	OK	03-22-2015 11:36:11	2d 2h 46m 6s	1/3	OK - Average IN: 1.70Kbps 0.00% Average OUT: 967.73bps 0.00%
22. VLAN 3 VoIP	CRITICAL	03-22-2015 11:35:51	1d 18h 29m 13s	3/3	CRITICAL: Traffic IN for 80 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel for interface 80
23. VLAN 7	OK	03-22-2015 11:36:11	4d 23h 36m 53s	1/3	OK - Average IN: 166.25Kbps 0.17% Average OUT: 224.33Kbps 0.22%

Figura 13. Redimiento de servicios del Switch Core
Fuente: Captura propia extraída de software de gestión Nagios

Implementación dentro de la Gestión de Seguridad.

Dentro de esta área de gestión es necesario que solo el administrador de la red pueda realizar cambios de configuración al software de gestión por lo que se describe los siguientes parámetros:

Acceso y autorización al software de gestión.

The nagiosadmin user is the administrator user management software which has all the privileges necessary to perform any modification (aggregation, change, deletion, configuration) equipment and services. In addition Nagios sends email notifications and text messages to mobile phone to a single contact informing failures that occur on critical devices.

III. PROCEDURE MANUALS

Inside of it's section is present establishing structured procedures manuals for each functional area network management based on ISO standard.

A. Introduction.

TIC apartment of Ibarra-GAD has the obligation to keep operating the computing tasks that are performed within their various departments, to provide a quality service to the public, therefore teams must maintain high levels of performance and availability.

Therefore the structure of these manuals is done with their respective guidelines to help network managers to diagnose and fix problems on the local data network in the shortest time possible by the five management areas which are interrelated to obtain a higher return on their managed funds. The entry process and equipment configuration, troubleshooting, bug fixes, viewing reports and reports sent notifications, so on. [9]

- *Procedures Manual to setting Management.*
- Objective.- Indicate to network administrators the setup of new devices to manage.
- Link.- This manual applies to software revenue management devices, which meet the requirements of network and technical specifications nomenclature also presents the procedure to switches and servers.

Procedures Manual for Fault Management.

- Objective.- Find the best solution to a problem that is present in the local network data before it is perceived by users.
- Range.- Apply establishment of thresholding to resources to be managed, managing to have greater availability of local network operation data you. Restore service as soon as possible and to identify and analyze the cause of the incident in order to prevent their recurrence.

Procedures Manual for Management Accounting.

- Objective.- Indicate the parameters to be used for monitoring and configuration of network devices to be managed in the local data network.
- Range.- It is present the procedure to add network devices and services management software Nagios them that must comply with the characteristics set so they can be monitored and relevant information on the use of each resource.

Procedures Manual for Performance Management.

- Objective.- Collect and analyze information about the performance of resources managed devices.
- Range.- This management relates conjunction with fault management, therefore here the behavior is determined in various ways, either on a particular time interval or in real time. This will make the respective decisions according to the results that generate the behavior of the managed devices.

Procedures Manual for Safety Management.

- Objetivo.- Provide security management system which requires the ability to authenticate users and applications management, in order to ensure the confidentiality and integrity of exchanges of management operations and prevent unauthorized access.
- Range.- Information Ibarra- GAD has a very important value because it links the financial system and the

service to users of citizenship for that reason it is essential to maintain protected resources that enable connectivity and communication with external entities.

IV. CONCLUSIONS

The implementation of a management model based on the ISO standard, it is essential and necessary in a local network of government data as GAD-Ibarra, due to the high availability of network equipment that manages to provide greater connectivity both units internal and external, and the duty of the institution to provide quality service to the citizen.

By means of the functional model of network management it was able to establish the interaction of the five management areas such as; configuration, fault, accounting, performance and security, with the needs that the entity where was determined the implementation criteria.

With the realization of the analysis of the current state of the network entity was identified critical areas through a hierarchical model determined by layers; core, distribution and access is also possible to determine critical network devices that support SNMP enablement through inventories, topological map, technical features, consumption measurement data sent and received by the monitoring software to check Ntop services for network coursing through physical servers and active virtuals.

By describing management policies of the five functional areas of management model it's determined guidelines to help improve the performance and availability of devices that are part of the network entity.

Through the guidance given by the IEEE 830 standard it was determined as the best option to Nagios management software tool that provides solutions regarding the optimal management of network resources, allowing administrators to view real-time information on an interface web centralized and easily adaptable..

Incidents in the network devices can be harmful to the organization so Nagios allows the administrator to identify a failure by the hierarchy of easy alerts to recognize also devices greater criticality they have an identification extra failures, such as sending notification of an email or a text message to mobile phone, 24 hours a day, 7 days a week, for any

eventuality programmed and can respond immediately to solve the problem by reducing the impact of unavailability network.

The behavior of Nagios inside the local data network entity does not affect the performance of sending and receiving information, as it was possible to demonstrate through data obtained from the monitoring software Ntop where it was verified that Nagios doesn't generate storms broadcast traffic through Wireshark software and verified that the UDP traffic generated by the SNMP protocol does not exceed the normal percentage consumed before and after implementation of the management model.

Through the implementation of management software Nagios is able to develop, procedures manuals based on the functional areas of management model, which serve as guide for network administrators can use these processes in future and thus managed devices form the network entity is constantly updated and monitored to ensure the availability of operating their resources.

Carlos A. Vásquez A.



He was born in Quito - Ecuador 19th September, 1981. Electronics and Telecommunications Engineer, Escuela Politécnica Nacional School at 2008. Nowadays is profesor Engineering in Electronics and Communication Networks career at North Technical University , Ibarra-Ecuador, and almost over Master of Communication Networks Pontificia Catolica del Ecuador University, Quito-Ecuador.

Viviana E. Ayala Y.



She was born in Carchi - Ecuador 17th August de 1989. Realized her primary studies at "María Angélica Idrobo". In 2006 years she got her Bachelor's title in mathematics physical sciences at "Nacional Ibarra" high school. Nowadays, almost over Engineering in Electronics and Communication Networks career at North Technical University Ibarra city.

REFERENCIAS

- [1] Alarcón Ávila, R. (2007). Gestión y Administración de Redes como Eje Temático de Investigación . Bogotá: Universida Libre.
- [2] ISO / IEC . (1989, 11 15). ISO / IEC 7498-4:1989. Retrieved from ISO / IEC 7498-4:1989: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?cnumber=14258
- [3] Ding, J. (2010). Advances in Network Management. United States of America: Auerbach Publications Taylor & Francis Group.
- [4] Orozco, P. (2010). Gestión de Red del boli al SNMP. CASTELLDEFELS: UPCnet.
- [5] GAD-Ibarra. (2013). Inventario de depencias. Ibarra: Gobierno Autónomo Descentralizado de San Miguel de Ibarra.
- [6] Cevallos Michilena, M. A. (2013). Metodología de seguridad informática con base en la norma iso 27002 y en herramientas de prevención de intrusos para la red administrativa del Gobierno Autónomo Descentralizado de San Miguel de Ibarra. Ibarra: Universidad Técnica del Norte.
- [7] Nagios Enterprises. (2014, Marzo 05). Nagios Core Documentación. Retrieved from <http://www.nagios.org/>
- [8] Microsoft. (2005, Octubre 25). Microsoft TechNet. Retrieved from [http://technet.microsoft.com/es-es/library/bb124583\(v=exchg.65\).aspx](http://technet.microsoft.com/es-es/library/bb124583(v=exchg.65).aspx)
- [9] Rea Lozada, R. A. (2012). "NORMAS DE CONTROL INTERNO EMITIDAS POR LA CONTRALORÍA GENERAL DEL ESTADO, APLICADAS A LA DIRECCIÓN DE TECNOLOGÍAS. Ibarra: Universidad Técnica del Norte.