JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

Proposal for the redesign of the corporate data network of the Decentralized Autonomous Government of the province of Bolivar (Ecuador)

Alejandro Silva-Lara*
Universidad Politécnica Salesiana, Carrera de Ingeniería en Sistemas, CP:170131, Quito (Ecuador)
*Corresponding author: asilva@ups.edu.ec

Marco Naranjo-Cruzatty
Universidad Politécnica Salesiana, Carrera de Ingeniería en Sistemas, CP:170131, Quito (Ecuador)

Jorge López-Logacho
Universidad Politécnica Salesiana, Carrera de Ingeniería en Sistemas, CP:170131, Quito (Ecuador)

Abstract

This work describes the analysis of the current situation of the DAGPB (Decentralized Autonomous Government of the province of Bolivar) data network and presents a proposal for its redesign, for which the PPDIOO and Top-Down network methodology was used. The proposed data network was designed under a 3-layer hierarchical structure model, consisting of core switch, distribution and access, as well as a DMZ was defined. Then the OPNET simulation of the current and proposed topology was carried out, obtaining statistical results on the traffic generated by the different services provided, and the use that each of the users will make within the organization, as well as OPNET allowed to carry out comparatives between both topologies.

Keywords*:* Proposal, redesign, data network, DAGPB

1. INTRODUCTION

With the introduction of computers and the use of applications to automate information, the need to implement information security systems became evident. According to **Katz, (2013)**, the most important factors that must be covered within the administration of the network are in order of priority, functionality, security and speed.

Network security is directly related to the business continuity of an organization; therefore, a security breach can cause data loss, or affect the privacy of people and compromise the integrity of information (**Watkins and Wallace 2008**).

Hierarchical Design Model

For the design of a LAN, some important aspects that must satisfy the needs of an organization are taken into account, achieving a reliable infrastructure and responsiveness. A hierarchical data network divides the network into layers or levels, which is why it has many benefits in design, being understandable for its configuration, easy growth and maintenance. Layered design serves to define specific assigned functions, which simplifies the design of the network, its implementation and subsequent administration. Speaking of dividing the network into layers does not necessarily refer to a physical separation, but logically **(Galarza-Macancela, 2018)**

Benefits of a tiered or layered network

Among the benefits are: Easy scalability in the network, Easy administration and maintenance, Reliability, Better cost/benefit ratio, Redundancy for permanent availability, Performance and Security (**Guijarro-Rodríguez et al., 2018).**

PPDIOO Network Design Methodology

This methodology was designed by CISCO in which a series of phases are defined that the network must go through before being implemented **(Calvo-García, 2017)** as shown in Figure 1.

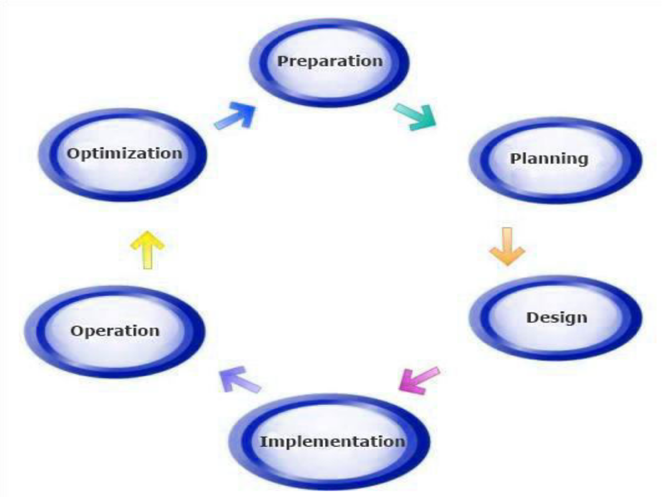

Figure 1. Steps of the PPDIOO Methodology

Top-Down network design

Top-Down network design is a methodology used to design networks starting from the top layer to the bottom layer, having as reference the OSI model consisting of 7 layers, its main objective being to divide a project into different layers, which makes it easier handle and modify (**Disbergen et al., 2018**). Table 1 shows a comparative table between Top-Down and Bottom-Up.

Table 1. Advantages and disadvantages of Top-Down.

Methodology	Advantages	Disadvantages
Top-Down	Analyze the business and focus on the essential needs before taking into account the technical details.	Longer analysis time to obtain results
Bottom-Up	Part of the design to find a solution faster.	The method reaches solutions, but it does not cover all the needs of the organization.

Source: Pasanen-Mortensen et al. (2017).

2. METHODOLOGY

2.1. Situational analysis

A situational analysis of the DAGPB (Decentralized Autonomous Government of the province Bolivar) computer system was carried out. Its infrastructure is distributed in 3 fully identified areas that are: Main or parent building (administration and coordination "three floors"), Mechanics/Roads Workshop and Multiple Workshop.

Regarding the distribution of RED, the DAGPB has a LAN network in the matrix, it is given through a data network connected with UTP category 5e cable, there is 1 main rack that stores the main equipment; with servers outside of Rank due to lack of physical space. It has a total of 21 distributed connectivity equipment (18 Switch and 3 Routers).

In the Logical Diagram of the current network, the DAGPB does not have a core or distribution switch, having a switch that connects the servers directly with the users, as well as other switches that act as repeaters. In addition, the DAGPB does not perform a correct control of the users because it does not have a dynamic IP address distribution. Also, none of the current switches are manageable (no remote access in case of network error tracking).

The DAGPB does not have any SDF's in its infrastructure, so the connection is made directly from the main MDF to the switches of each department.

The DAGPB network infrastructure does not have a computer room, the main network devices are distributed in the same office. So, security is poor (even anyone outside the organization has contact with the equipment room). Similarly, the DAGPB in the cabling lacks labeling in the main rack. even electrical wiring connections are next to data cables.

In addition to the equipment installed in the rack, there are several connectivity equipment distributed throughout the infrastructure of the DAGPB building. There is a total of 110 terminal equipment.

The DAGPB has 5 servers. Also, it has some institutional applications, such as SDM Document Management, Zimbra for mail use and Olympo for the financial system. There is a large consumption of traffic by different IP addresses, which cause that in certain periods during the day there are lost connections, but because there is no control over the users, the use of the link to which these addresses are connected. The most used protocol is HTTP because the vast majority of users need to access the organization's WEB page. The DAGPB does not have the use of DNS and DHCP services.

3. PROPOSAL FOR A REDESIGN OF THE DATA NETWORK.

The proposal for the design of the DAGPB data network, where the methodology was Top-Down, for which, a voice and data solution based on the requirements requested by the organization was contemplated, as shown in Figure 2.

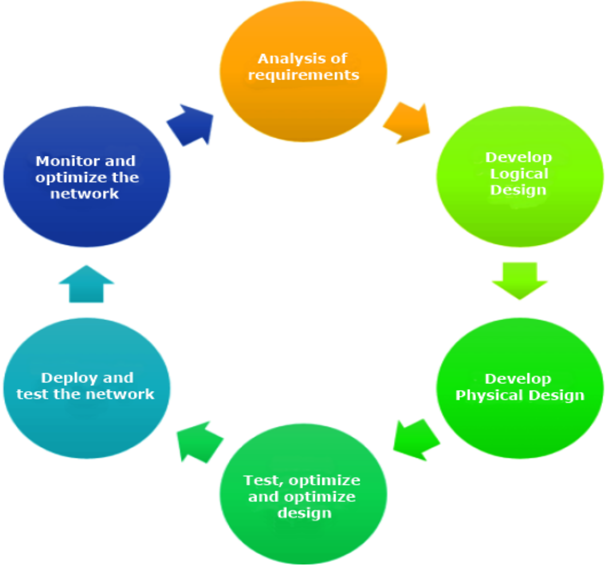
Analysis of requirements
Develop Logical Design
Develop Physical Design
Test, optimize and optimize design
Deploy and test the network
Monitor and optimize the network

Figure 2. Proposal for a redesign of the data network

3.1. Requirements for redesign.

The requirements demanded by the DAGPB Technology Department were considered, for which the needs of users have been taken into account (The requirements mostly coincide with the deficiencies of the computer system previously listed in the DAGPB Situational Analysis section).

3.1.1. Analysis of user requirements.

It can be argued that it is necessary to define a network that allows optimizing all existing resources, which must be evaluated and adapted to the new data network, which requires:

- Identify the physical area for the equipment room and telecommunications room.
- Correct identification of the wiring through labels following the Standards.
- Correct location and installation of network equipment and components in the rack, such as trays, organizers, path panel, among others.
- Comply with the Standards that refer to structured cabling ANSI/EIA-TIA.
- Improve physical security regarding access to the equipment room.
- Define the equipment to be reused and new equipment such as routers, switches, etc.
- Define the characteristics of the new servers or repower the current ones.
- Define the study, analysis, design and adequate dimensioning of the network to support IP Voice and data.

3.1.2. Applications to use.

The DAGPB requires certain applications such as institutional mail and other services for its daily tasks, which must be in optimal operating conditions. For this activity and others, Table 2 details the services that the DAGPB corporate data network will have, improving the service to users, as well as improving the response capacity of the technological development department to current problems such as the lack of security and redundancy that currently exists.

Table 2. Planning of network services

Services	Comments
Security	Physical firewall to protect the internal information of the organization, limiting access. Antivirus to avoid contagion with incoming traffic.
Quality of service	The QoS Policies to highlight are aimed at average network performance, transmission errors, bandwidth, transmission delay, availability, among others.
Network administration	Implementation of services such as Cacti and Radius, to improve network administration, monitoring and performance.
High availability	Provide redundancy improving network availability, avoiding different information losses.

3.2. Active network design

Ip address

VLANs have been created for each department using VLSM. VLSM, this helps prevent IP addresses from being depleted, and takes advantage of IP addresses, taking into account network scalability.

3.2.2. Logical design of the DAGPB data network

The data network will base your equipment distribution on a hierarchical model, which will make the network much easier to manage, flexible, and scalable. The access switches have been placed according to the organization's need for connectivity.

3.2.3. Physical design of the DAGPB data network

Many technical aspects have been taken into account in the physical design of the network, such as the implementation of hierarchical networks in three layers.

- A CISCO ASA 5512-IPS-K9 will be installed, adding physical security that will allow users to control the services provided by the organization **(Ciscon Lab, 2012; Cisco s.f,).**
- The Cisco C4500X-32SPF + brand Core switch will provide stability and speed to the network, with the creation of VLANs allowing control over users.
- Cisco Catalyst 3850 Switch will be used in the distribution layer, leaving a series of interfaces available at the time that the increase in the network is necessary, this switch will provide redundancy to the data network in the organization.
- Cisco Catalyst 2960-L will be used as an access switch that will connect users and finally, a Cisco Aironet 1560 Access Point will be added to provide service to citizens within the DAGPB facilities.

Connectivity within the organization will be carried out using UTP cat 6A cable, the link with the extensions will be made through Fiber Optics.

3.3. Equipment sizing for the active network

The minimum necessary characteristics of the connectivity equipment for the optimal operation of the proposed network are detailed.

Router ISP

The ISP router will be in charge of establishing the connection between the inside of the LAN and the Internet provider, and also provides security against possible computer attacks.

Characteristics.

High service availability and performance level; Mitigation of security risks (3DES data privacy, IPsec); 802.11n LAN and WLAN ports; Routing protocols: Rip v1 and v2, EIGRP, OSPF, DHCP, DNS, Spanning Tree Protocol, Network Access translation NAT, Border Gateway Protocol BGP, IPV4 and IPV6 multicast.

Firewall

The use of a Firewall is proposed, which combines firewall and VPN security, and allows controlling access to network resources to protect data.

Characteristics.

IPsec, VPN; Cisco Cloud users Web Security; Virtual interfaces (VLANs); High availability services; 3DES/AES VPN throughput: 100 Mbps; Memory: 512 MB; Simultaneous sessions: 10000/25000.

Switch Core

Equipment suitable for performing Layer 2 and Layer 3 functions is required, which is proposed to be implemented in the core layer of the DAGPB data network. Providing high speed and it has 10 Gigabit and 1 Gigabit Ethernet ports.

Characteristics.

Network management interface: 10/100/1000 10G Ethernet; Application monitoring through Netflow; Bandwidth forwarding; VLAN; Dual Core CPU 1.5 GHz, RAM 4 GB, Flash Memory 2 GB

Switch Distribution

A stackable multigigabit network switch is required for the Distribution layer.

Characteristics.

24 POE ports; 10/100/1000 Mbps/10 Gbps network management interface; PoE+power available; Bandwidth Forwarding (Gbps); Manageable and support VLAN; Multicore CPU, RAM 4 GB; Flash memory 2 GB; Support: VLAN, Voice VLAN, 802.3ad, RIPv1, v2 EIGRP, OSPF, OSPFv3, EIGRPv6 protocols.

Switch access layer

The switch must be 24 10/100/1000 Mbps Ethernet ports.

Characteristics.
24 PoE ports; 10/100/1000 Mbps Ethernet network management interface; CPU 800MHz; 256 MB Flash memory; Manageable and support VLANs

WLAN network router.

The Router must comply with flexibility and robustness in outdoor wireless networks. Its implementation in the SSID network is proposed.
Characteristics.
Radio 802.11ac standard; 1.3 Gbps data rates (theoretical); Multi-user MIMO (MU-MIMO); Radius support; Security and encryption policy.

Servers

They will be implemented with the use of free software such as the Ubuntu operating system, Linux Centos and proprietary software such as Windows Server, depending on the need to use.

On the mail and web server, it is recommended to maintain the use of Zimbra as email for the DAGPB Institution. These two servers, both Mail and Web, will be configured in the DMZ demilitarized zone, where traffic from outside to the servers is allowed. The same that will be installed on the HP PROLiant DL380G7 server under the Centos operating system.

Application server, The Quipux Document Management System will continue to be used and Olympo is the HP PROLiant DL380G9 equipment.

Monitoring server, in a group of 4 to more servers the installation of a monitoring server is recommended, which will allow to know the state of hardware use, it will also serve to know if a server is failing.

IP telephony server.
The use of the elastix server will be maintained for voice communication requirements, the same that is installed in the HP PROLiant DL380G9 equipment.

WLAN authentication radius server.
In the redesign of the DAGPB data network, it is proposed to implement a WLAN network, for the use of 200 users of Wi-Fi connection to the SSID: "Prefecture connects you".

DHCP, DNS and authentication server.
For the implementation of DNS, DHCP and directory services in the DAGPB data network, resource control, establishing policies at the company level, Active Directory installed under the Windows Server operating system will be used.

3.4. Traffic sizing for the new data network.

With the redesign of the DAGPB corporate data network, bandwidth must be provided that meets the needs of all the services provided to its users. The sizing will guarantee the performance of the network.

Bandwidth for Mail Server (we use 75 Kbyte).

Bandwidth for Web Server (average size to access 965 Kbyte having 10 income for one hour). *Bandwidth for file transfer* (average of downloaded files of 1MB).

Bandwidth for IP Telephony (average transfer rate of 87.2 Kbps that are required for Ethernet environments using the G.711 codec.)

Bandwidth for Video Conference (packet size of 768Kbps).

Total Bandwidth (The bandwidth requirements within the organization were analyzed and taking into account every detail the following bandwidth could be obtained with which the organization will obtain a performance according to its needs).

3.5. Passive network design.

3.5.1. Structured cabling design

In order to size the category of twisted pair Ethernet cable to be used in the new redesign of the DAGPB data network, it has been decided to take into account the three important factors such as: transfer speed, bandwidth and reduction in interference.

3.5.2. Horizontal wiring proposal.

Each work area will have the necessary connections, face plates and their respective RJ-45 Jack. Category 6a twisted pairs will use the T568B standard at both ends as they are different layer equipment.

In addition, in order to support the services required by the DAGPB, category 6a UTP cable is recommended for connections from the work area to the different access switches. The same one that has a transmission speed of 10 Gbps, bandwidth reaches 500 Mhz.

3.6. DAGPB MDF/SDF diagram redesign.

The interconnection between the MDF and the SDFs has been designed with fiber optics, while between the SDFs and their respective switches the wiring to be used will be UTP category 6e.

3.6.1. Cable labeling.

Labels will be placed on each end of the UTP cable, both on the patch panels and on the face-plates, for which, the standard of the TIA/EIA 606-A standard that regulate signaling and labeling will be taken into account.

3.6.2. Equipment room.

In the equipment room, a series of parameters must be taken into account, such as: physical elements, air conditioning, energization, security, lighting, equipment that will be installed according to what is established in the EIA/TIA 569 standard.

3.6.3. Equipment distribution.

It must have a height of 2.6 m, the location of the Racks must be 50 centimeters with respect to the wall, guaranteeing free movement spaces of at least 40% and 50% the size of the racks. The rows of the equipment must be located parallel to the ventilation systems providing free circulation and without problems of air interruption inside the room.

3.6.4. Network security design.

Firewall

The DAGPB data network firewall will be the team that must protect the exchange of information between the internal network and the WAN network, for which it will implement permit and prohibition policies.

4. Conclusions

The redesign will allow the number of users to increase without having to make modifications. When redesigning the data network, many factors have been taken into account, such as the new services, and calculations have been made of the bandwidth to be used, thus guaranteeing that each user can make use of them without having any inconvenience. your connectivity.

5. Acknowledgements

The Authors thank the DAGPB for allowing us to carry out this work.

References

Calvo-García AL. (2017). *Gestión de redes telemáticas.* Madrid: IC Editorial.

Cisco Lab, W. (2012). *Cgtic.* http://www.cgtic.unacar.mx/normatividad/norma568.pdf

Cisco. (s.f.). *Cisco.* http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-519930.html.

Disbergen NR, Valente G, Formisano E, Zatorre RJ. (2018). Assessing Top-Down and Bottom-Up Contributions to Auditory Stream Segregation and Integration With Polyphonic Music. *Frontiers in neuroscience*, *12*, 121. https://doi.org/10.3389/fnins.2018.00121

Galarza-Macancela M. (2018). Design and implementation of a secure data network for the Pontificia Universidad Católica del Ecuador, Santo Domingo. Dom. Cien. 2(2): 123-137. http://dx.doi.org/10.23857/dom.cien.pocaip

Guijarro-Rodríguez A, Yepez-Holgin JM, Peralta-Guaraca J, Ortiz M. (2018). Depth defense applied to a business environment. Revista Espacios; 39(42): 19.

Katz, MD. (2013). Redes y Seguridad. México: Alfaomega.

Pasanen-Mortensen M, Elmhagen B, Lind H, Bergstrom R, Wallgren M, van der Velde P, Cousins S. (2017). The changing contribution of top-down and bottom-up limitation of mesopredators during 220 years of land use and climate change. Journal of Animal Ecology; 86,566–576. doi: 10.1111/1365-2656.12633.

Watkins M and Wallace K. (2008). CCNA Security Official Exam Certification Guide. EEUU: Cisco Press.