STATE OF MEXICO CAMPUS

TC3003B

Implementation of wide area networks and distributed services

Technical Memory

MUAC (Museo Universitario de Arte Contemporáneo)

Members

José Luis Madrigal Sánchez	A01745419
César Emiliano Palomé Luna	A01746493
Germán Guzmán López	A01752165
Isabel Vieyra Enríquez	A01745860
Christian Parrish Gutiérrez Arrieta	A01751584

2/05/2024

Version 2.3

Introduction

Objectives of the document

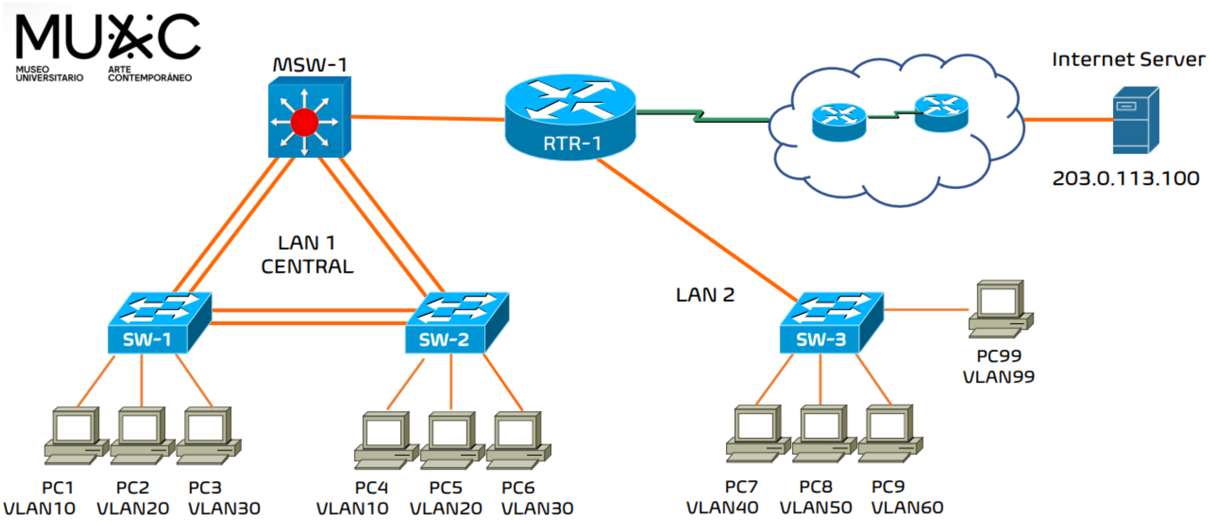
The purpose of this document is to generate value propositions in order to optimize the proposed network infrastructure. These improvements focus on several crucial aspects to ensure efficient and reliable operation of the network. Among the specific objectives are:

- **Possible improvements in Communication Speed:** Areas of the network will be sought where the data transfer speed can be optimized. This includes evaluating bandwidth capacity, the speed of network devices, and implementing technologies that improve transmission speed.
- **Prevention of the Creation of Loops:** Measures will be proposed to avoid the formation of loops in the network topology.
- **Validation of Preset Configurations:** A validation of all preset configurations on network devices will be carried out. This involves checking the consistency of the configuration, the security of the set parameters. Rigorous testing is performed to detect potential configuration conflicts.

Scope of documentation

This document focuses on analyzing and evaluating the current components of the provided network to identify areas for improvement and optimization. Information about the addition of new equipment will only be included if it is determined to be necessary to improve network performance or capacity. The project covers the review of network configurations to ensure their efficiency and optimal functionality, so adjustments and modifications will be made as necessary to improve data flow and connectivity within the network. It is important to note that improvements related to advanced cybersecurity will not be included, since the focus will be limited exclusively to aspects of network performance and efficiency, although this does not imply that some best practices or access rules will be included. The ultimate goal is to provide detailed recommendations and an action plan to improve the existing network infrastructure, ensuring optimal operation and greater efficiency in data exchange.

Brief description of network infrastructure



The network is designed with a hierarchical approach. At the top of the hierarchy, there is a router (RTR-1) connected to two distribution layer switches (MSW-1 and SW-3). These switches form two separate LANs: LAN 1 (CENTRAL) and LAN 2.

On LAN 1, MSW-1 is connected to two access layer switches (SW-1 and SW-2). Each of these switches is connected to multiple devices that are in turn divided into different VLANs (VLAN10, VLAN20 and VLAN30).

In LAN 2, RTR-1 is connected to another access layer switch (SW-3), which in turn is connected to several devices belonging to separate VLANs (VLAN40, VLAN50, VLAN60 and VLAN99).

Finally, the router (RTR-1) is connected to an Internet server with the IP address 203.0.113.100.

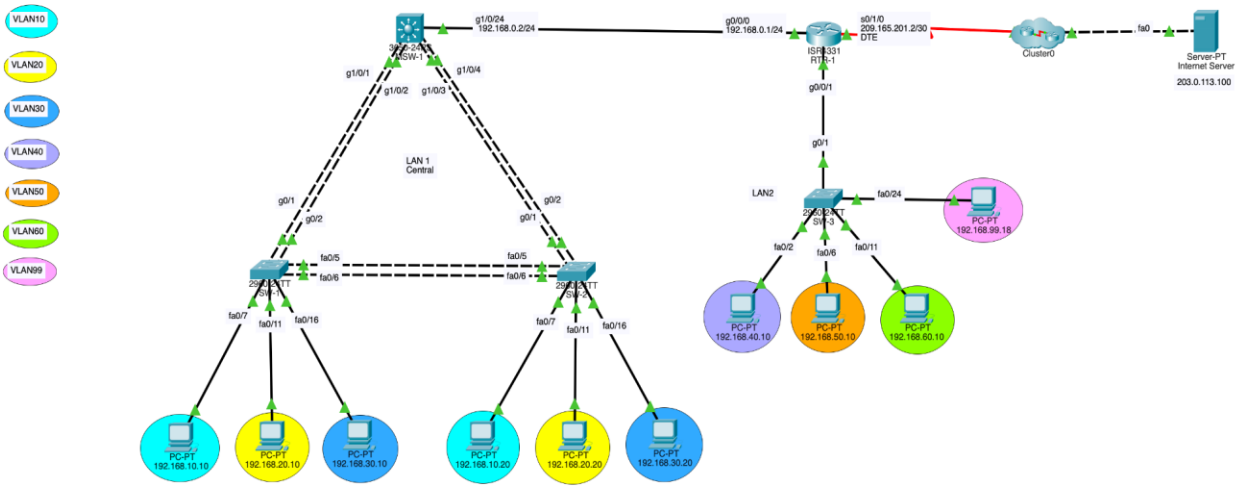
General description of network infrastructure

Network architecture: physical and logical topology

Physical: At the top of the hierarchy we have a router model ISR-4321 (RTR-1), which acts as the connectivity center. From RTR-1, the main branches of the network extend, connected to two switches via Ethernet cables. One of these switches is multilayer, model L3-3650 (MSW-1), while the other is L2-2960_24TT (SW-3). MSW-1 and SW-3 form the bases of LAN 1 (CENTRAL) and LAN 2. Within LAN 1, MSW-1 connects to two L2-2960_24TT access switches (SW-1 and SW-2). And in LAN 2, the RTR-1 is directly connected to a switch L2-2960_24TT (SW-3), which serves as the access point for the devices on that network.

Logic: Regarding the logical architecture, all data traffic is directed from the devices to the central router (RTR1), through the switches as necessary. RTR-1 determines the best route to send data, either within the same LAN or to external destinations. When data leaves the local network, RTR-1 sends it to the Internet server through the connection to its WAN port, and upon receiving a response, the information follows the same path back to the connected devices.

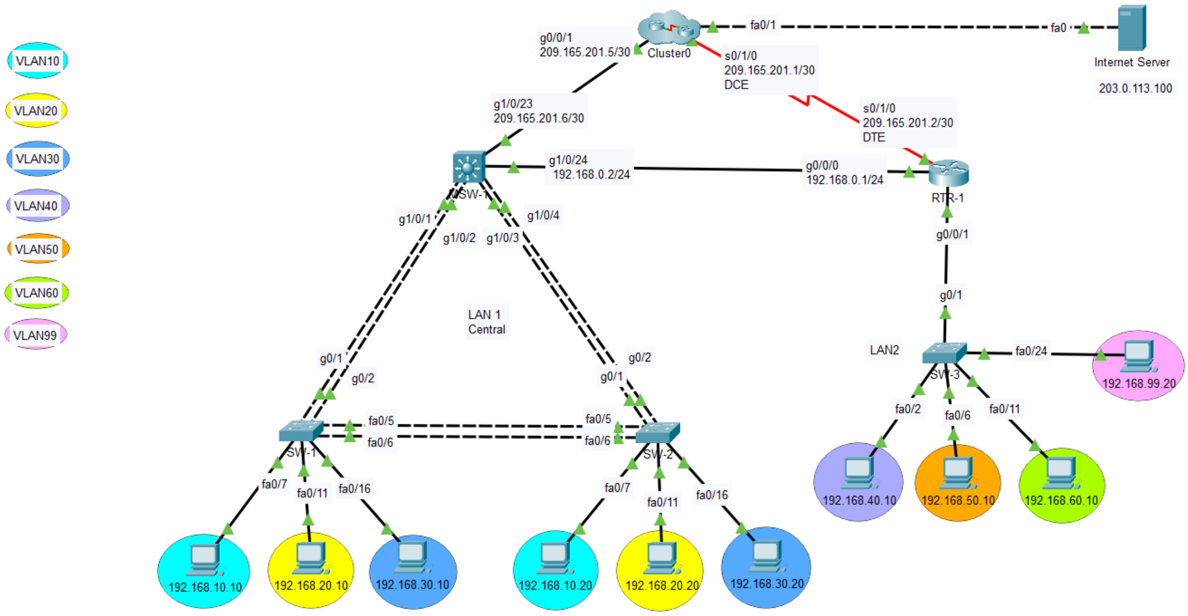
Network diagrams: documented visual illustrations of infrastructure



Prototype of network in Packet Tracer

Recommendations and improvements

Simulation of new infrastructure



Justification of suggested improvements

It is important to mention that the given configurations lacked some things to achieve connectivity between the equipment. Basically, the vlans had to be established on the multilayer switch and ospf had to be completed on the RTR-1 and MSW, because it did not have all its networks directly connected in the protocol. This way any computer can ping any other and also the server.

1. Create a connection on the multilayer switch to the Internet
In case there is a failure in the border router that provides Internet access, it is a good implementation to establish a connection between the multilayer switch and the Internet exit to implement redundancy. It is important to mention that this also implies that the routing protocol is updated, so that the equipment in the different VLANs can pass through that link. It is important to mention that in addition to redundancy, the multilayer switch allows the use of a gigabit Ethernet cable to offer greater speed.

2. Implementation of Access Lists for VLAN 99
An access list can be implemented on the router to manage VLAN 99 traffic and give priority to being the only address that allows connection via SSH instead of Telnet. This is considered a good option since VLAN 99 is intended for management so it could be a security and best practice inclusion. Despite the presence of CIsco DNA Center, it is good to have a VLAN intended for management as a backup.

3. Establishing Multilayer as root in STP
We consider that one way to maintain the good level of network performance is by redefining the root of the spanning-tree, because this was originally switch 1, but when analyzing the network, when the connection of the multilayer switch to the Internet is included, This

becomes more relevant, since traffic is mainly routed through that link, so making that computer root is a good way to ensure that it is recognized as an important point within the network.

On the other hand, some possible future implementations are proposed that can be of great help for the MUAC, both in the performance, security and user experience sections. It is worth mentioning that these solutions may require more considerable investments, so prioritizing current needs and requirements is essential.

4. Inclusion of APs within the network
The inclusion of Access Points in a public environment such as a museum is crucial to improving the visitor experience by providing reliable, high-speed connectivity. This allows visitors to easily access online resources, such as applications or simulations that the museum may offer. In addition, by offering a stable Wi-Fi connection, there can be an improvement in the services that the museum wishes to offer to improve the user experience.

5. Implementation of PAT by interface to the Internet
It is essential to ensure security and efficient control of traffic on a network. Additionally, assigning unique ports to each outgoing connection makes it easier to identify and track traffic, improving network manageability and monitoring. But it is important to mention that although the multilayer switch has routing capabilities, it is more advisable to designate a new edge router in that section, which can be used for NAT translations. It is worth mentioning that the RTR-1 router, which is a normal router, already has PAT working correctly.

6. HSRP
Having a protocol that allows you to define the main router that will lead to the Internet is a good practice to have greater availability and redundancy in routing, which is why it can be beneficial to use this protocol to generate greater availability and load balancing. In addition, this protocol allows for a more efficient response to failures, because it provides the ability to establish an automatic backup of the routers, since the status of the active router is constantly monitored.

Implementation of improvements in simulation

First, the spanning-tree of the multilayer switch was changed, putting priority 0 to make it root, but this blocked port channel 3, so in the presentation Frank stressed to us that the solution was simple, he simply also put priority 0 to the switch 1 and thus the entire network remains accessible.
Later, the gigabit Ethernet cable from the multilayer switch was added to the Internet, with the IP addresses of the next segment that used the serial, and this involved including these new networks in the ospf of both the multilayer and Internet router 1, so now Packets from any vlan pass over that link to reach the server.
Finally, the ssh connection was made from vlan 99 to RTR-1 and MSW-1, by defining a default gateway in SW-3 and access list in both the router and multilayer. So you can now

make a connection from PC 192.168.99.20 with the command ssh -l admin 192.168.99.17 or to 192.168.0.2.
It is important to mention that PAT was configured per interface in the normal router, so the addresses that come out through the serial are translated when they reach the Internet.

Additional documentation

Technical support contacts

Cisco:
Telephone: 001 888 443 2447

Telmex
Telephone: 800 123 9434 , 800 123 1114

Totalplay:
Telephone: 800 510 0510

Megacable:
Telephone: 33 9690 0000

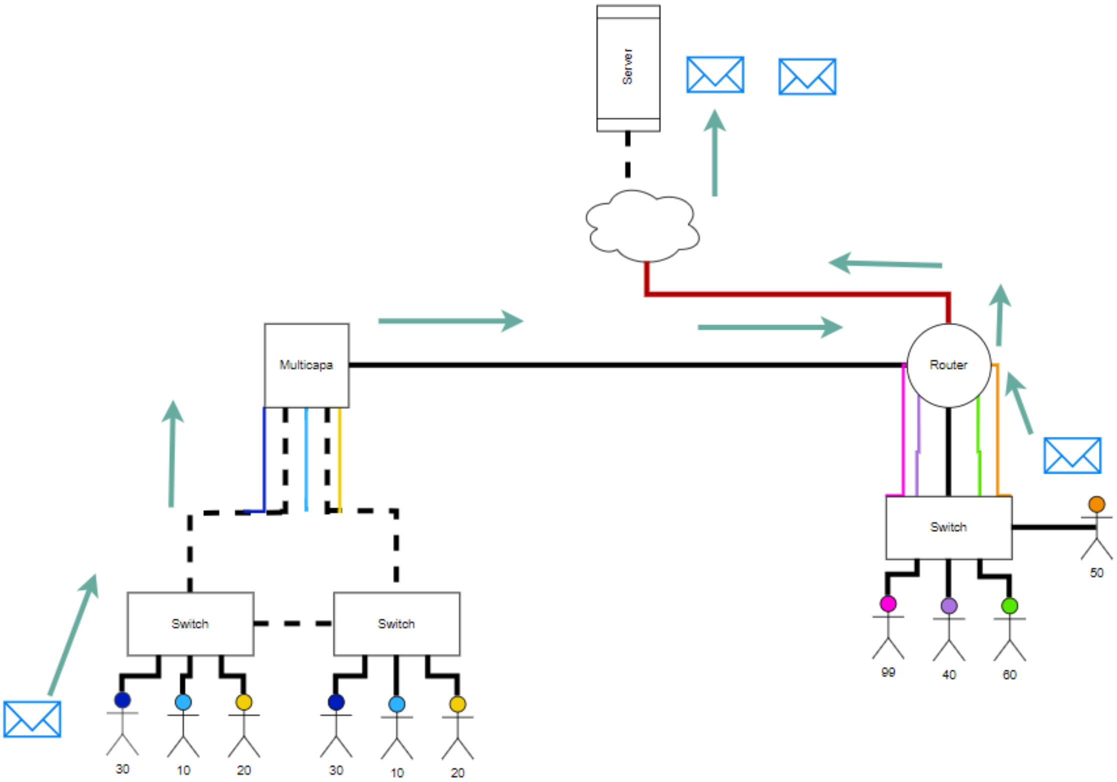
Izzi:
Telephone: 800 120 5000

Providers and service contrats

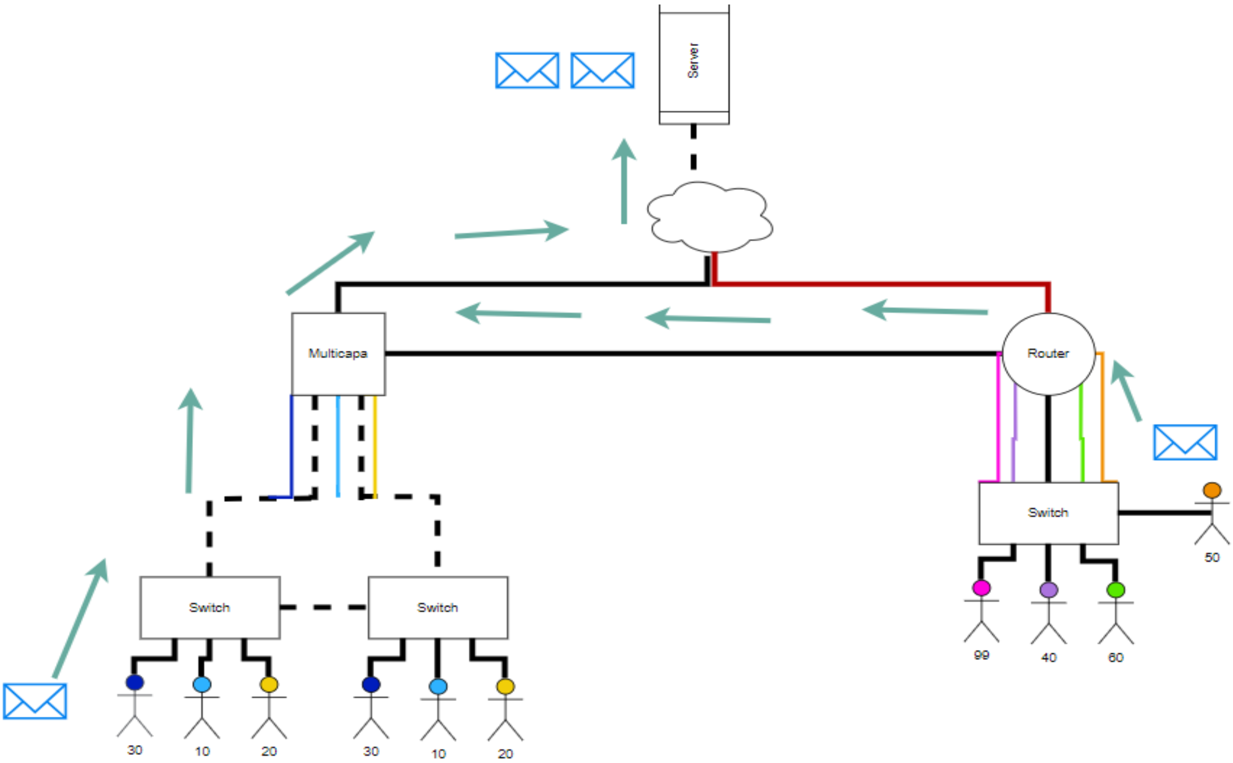
Provider	TELMEX	TotalPlay	Megacable	Izzi
Type of service	Fiber optic	Internet cable	Internet cable	Hybrid connection of fiber and cable
Characteristics	High speed, low latency	Symmetrical download and upload speed	Wide coverage, flexible speed options	All-in-one service packets
Packet	Unlimited internet, 2 telephone lines, 1000 Megas	1000 Megas, 2 telephone lines	750 Megas, unlimited telephony	100 Megas, 2 telephone lines with unlimited calls
Price MXN	$1,400	$1,305	$850	$1,200

This table provides a general idea of the Internet service packages offered by different providers in the area. Each provider offers a variety of options for businesses or companies with different connection speeds and prices. We believe that these packages can be adapted to the needs of the MUAC, providing options to maintain a fast connection for online activities and visitor interaction.

Data flow and processes diagram



The flowchart presents a graphical view of how the network is distributed and how packets travel (represented by the blue cards), showing their flow and passage through the different components (shown with the blue arrows) until reach the server located on the internet. Likewise, through the colored lines we can see the distribution of the Vlans through the interfaces of the Switches and Routers. In this way we can see more clearly the flow of data exchange and distributions in the system.



After the improvements were made, routing began to be done first by the multilayer switch, because its Gigabitethernet interface has a higher speed than the router's serial interface and that it is the root of the spanning-tree. Therefore, as long as the multilayer link is available, all packets from both LANs will pass through it, which generates greater network performance and therefore the services offered by the server are more efficient. This is also directly related to generating redundancy towards the internet, which is beneficial to ensure that the connection to the server is not easily lost.

References

Comprender las funciones y la funcionalidad del HoT Standby Router Protocol. (2023, 14 septiembre). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

Configuración de los parámetros de interfaz de puerto a VLAN en un switch a través de la CLI. (2024, 1 enero). Cisco. https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5653-configure-port-to-vlan-interface-settings-on-a-switch-throug.html

Configuración del SSH en routers y switches. (2024, 16 febrero). Cisco. https://www.cisco.com/c/es_mx/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

Configurar ACL de IP de uso general. (2023, 27 noviembre). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html

Configurar NAT para habilitar la comunicación entre redes superpuestas. (2022, 12 marzo). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html

Configuring OSPF. (2016, 29 julio). Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html

Configuring the Access Point for the First Time. (2019, 2 marzo). https://community.cisco.com/t5/networking-knowledge-base/configuring-the-access-point-for-the-first-time/ta-p/3154316

Ejemplo de configuración de IP MultiLayer Switching. (2022, 13 marzo). Cisco. https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-6000-series-switches/12022-39.html

PAT. (2022, 27 septiembre). https://community.cisco.com/t5/security-knowledge-base/pat/ta-p/3114711

Work smarter with Webex Meetings. (2023, 5 enero). [Vídeo]. Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/how-to-setup-network-switch.html