UDLAP

Universidad de las Américas Puebla

Seventh Semester

Autumn 2023

Practice 4

Computer Networks lab

Students:

Jesus Eduardo Ávila Maldonado - 170423

André Federico López Hernández - 167564

Jonathan Eliasib Rosas Tlaczani - 168399

Profesor:

Dr. Eduardo Javier Jiménez Lopez

Department of Computing, Electronics and Mechatronics

San Andrés Cholula, Puebla; September 2023.

Abstract

In this practice we are going to know how to work with an Extreme Switch. We will understand its configuration modes and its most important commands. Removing and adding ports from a VLAN (virtual local area network) is going to be an important part of the practice also. A telnet link will be used to configure connected switches. We will master the configuration of a wireless network for a switch configuration. In the last part of the practice the deployment of a wireless local network will be necessary to configure connected switches.

Theorical Analysis

1. **Extreme XOS (ExtremeX Operating System)**:

    - **Modular Operating System**: Extreme XOS is designed as a modular operating system, which means that it's built in a way that allows different modules or software components to be added, removed, or upgraded independently. This modularity enhances flexibility and scalability.
    - **Highly Available**: Extreme XOS is built with high availability in mind. It ensures network reliability by supporting features such as redundancy and failover mechanisms to minimize downtime.
    - **Security Capabilities**: Extreme XOS is equipped with robust security features. It integrates network access control, endpoint integrity checking, identity management, and protection for network control and management planes. This comprehensive security approach helps safeguard the network from threats and unauthorized access.
    - **Support for VLANs**: Virtual LANs (VLANs) can be implemented within Extreme XOS. VLANs enable network segmentation, improving network performance, security, and manageability.
    - **STP (Spanning Tree Protocol)**: Extreme XOS supports Spanning Tree Protocol, a vital network protocol used to prevent loops in Ethernet networks and ensure network stability.
    - **IPv4 and IPv6 Support**: Extreme XOS offers support for both IPv4 and IPv6, making it suitable for modern networks that require compatibility with both IP versions.

- **Distributed Software Architecture**: The distributed software architecture allows for efficient resource utilization and scalability in large network environments.
- **Process Control**: Extreme XOS provides control over various network processes, enabling administrators to manage and optimize network performance.
- **Multiprocessor Support**: By supporting multiprocessors, Extreme XOS can efficiently distribute and process network tasks, enhancing overall performance.

2. **Extremeware**:
    - **Comprehensive Security**: Extremeware is known for delivering comprehensive security features. It can help protect networks from various threats and vulnerabilities.
    - **Intuitive Management**: Extremeware offers intuitive network management capabilities, making it easier for network administrators to configure, monitor, and troubleshoot network devices.
    - **Hardware Control for "i" Series Equipment**: Extremeware provides control and management capabilities specifically designed for "i" series equipment. This allows for fine-tuned control and optimization of hardware resources.
    - **VLAN Implementation**: Extremeware supports VLANs, which are essential for network segmentation and traffic isolation.
    - **STP, NAT, BGPv4, and More**: Extremeware offers a wide range of networking protocols and features, including support for Spanning Tree Protocol (STP), Network Address Translation (NAT), and Border Gateway Protocol version 4 (BGPv4). These features are crucial for building and managing complex networks.

Both Extreme XOS and Extremeware are designed to cater to the needs of modern networks, providing the necessary tools and features for security, manageability, and performance optimization. Depending on the specific requirements of your network, you can choose the operating system that best suits your needs.

In short, switches play an essential role in Extreme Networks network infrastructure, providing the connectivity, management, and security necessary to support modern, highly efficient network

operations. Choosing the right switch will depend on the specific network requirements and deployment strategy of each organization.

The wireless connection to the switches is necessary for this practice. To test different configurations and changes to the switches it is necessary to have a device with wireless access and Telnet software such as a laptop, a tablet or even a cellphone.

Methodology and Experimental Results

Development:

With advice from the instructor:

We connect the assigned computer equipment to a Switch via console connection using

serial cables.

We set the default VLAN IP according to the Instructor's directions.

Configure the IP address of the Switch with the following command:

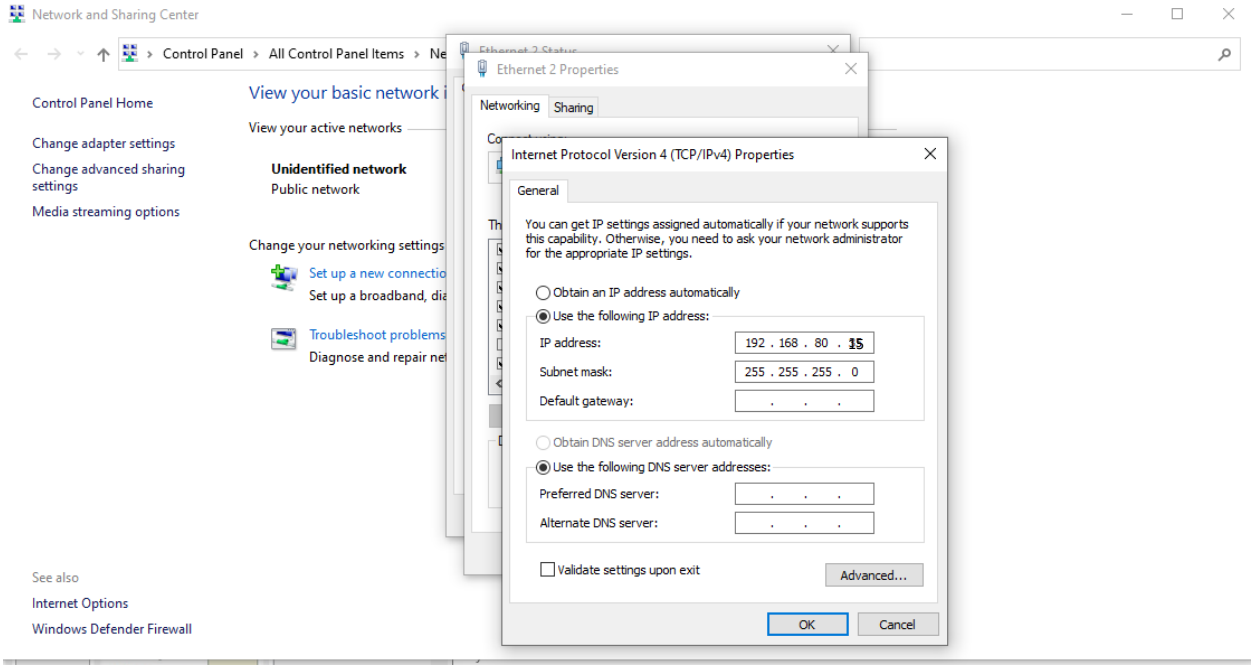


Fig. 1 configure vlan default ipaddress 192.168. 80.1x

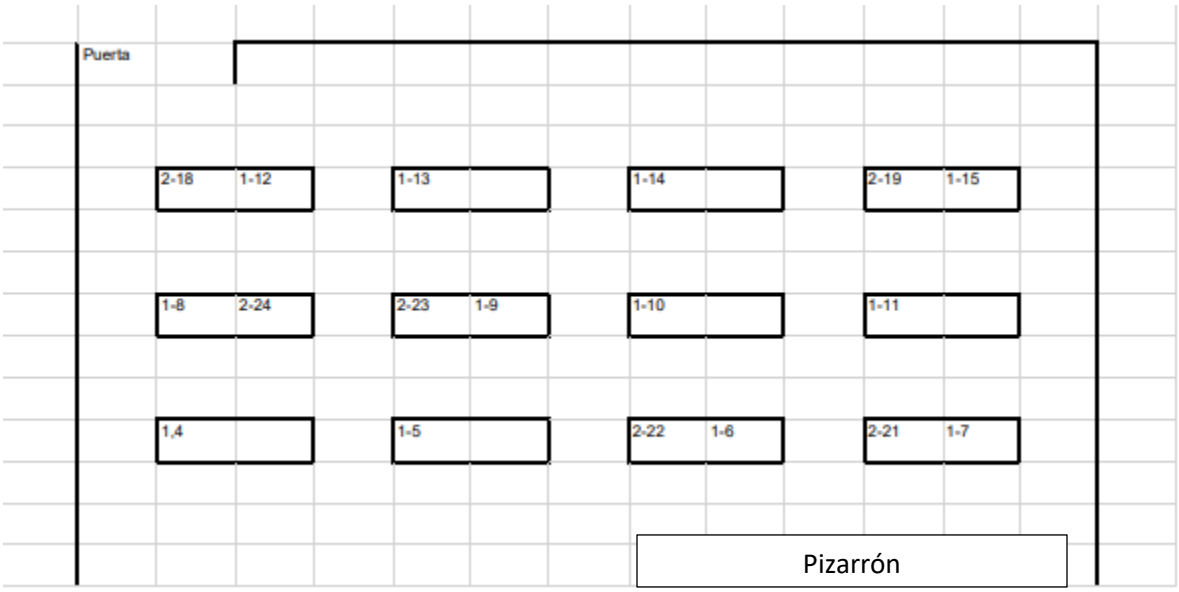
where x is the assigned switch number.

Once the IP address of the Switch is configured, it is possible to configure it using an

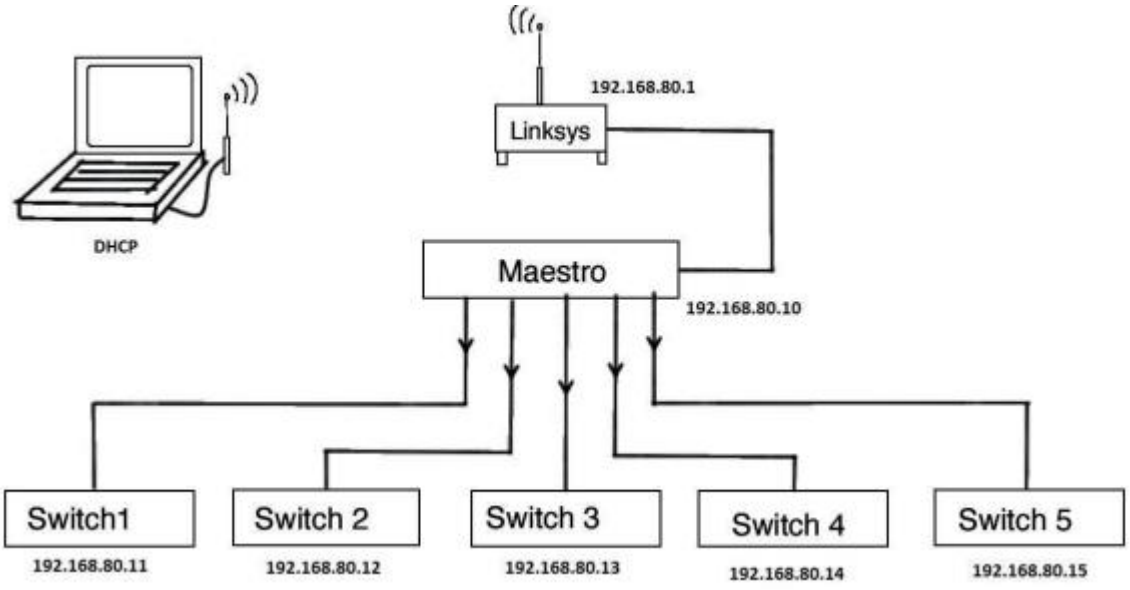
Ethernet connection and using Telnet instead of Hyperterminal.

Once the IP is assigned:

We connect an Ethernet cable between a computer and the assigned switch. Use the following patching scheme to use the existing cabling structure.



Connect the switches and router as shown in the following figure.



We configure the default network IP addresses according to the same scheme. For this it can

be done through a console connection (serial) or by ethernet cable and using telnet if the current IP of the switch is known. Remember that the command used is:

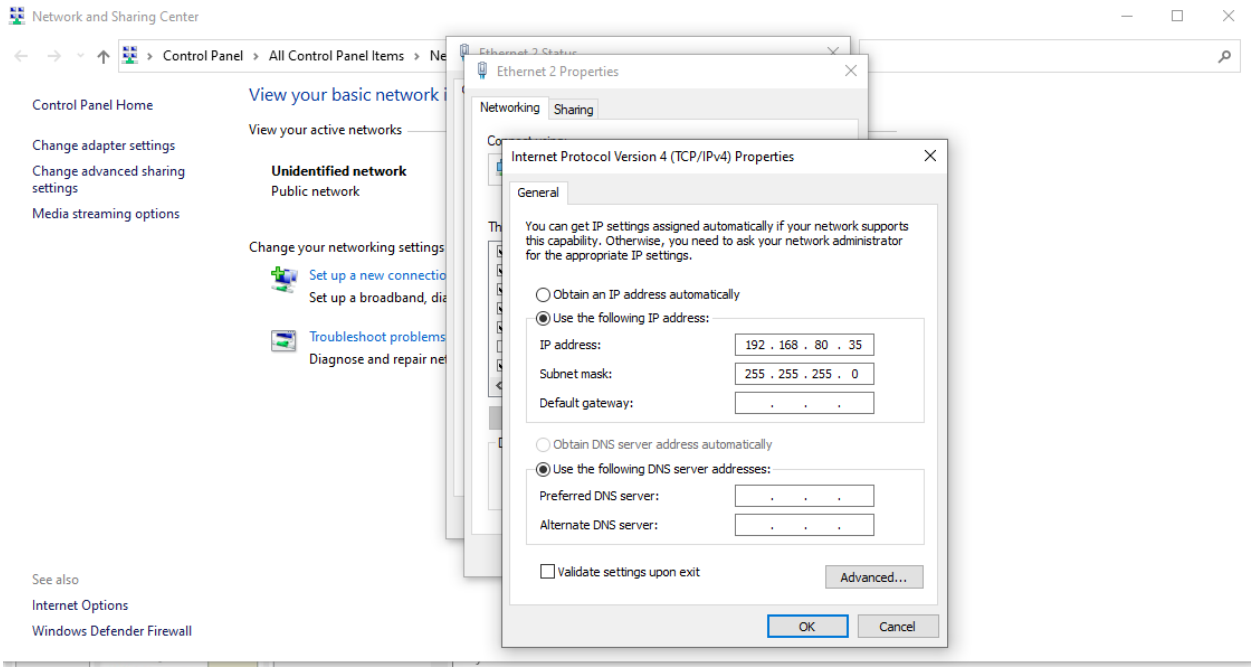


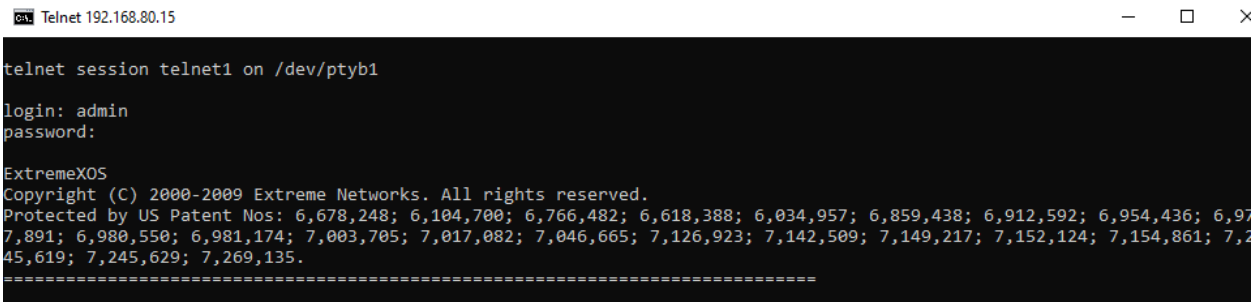
Fig. 2 configure vlan default ipaddress 192.168. 80.xx

Also configure the IP address of the wireless router. Using the router app.

The IP address of the computer equipment must be assigned automatically (DHCP), but it must be verified that it has been assigned within the subnet mask of the system, otherwise assign it manually.

Once the system is connected and configured, any of the connected switches can be accessed through a telnet session.

We run a telnet command with the IP of the Switch and access the Switch with administrator privileges.



We use the following command to assign the specific name indicated by the instructor.

Using the following command to display information about the current session.

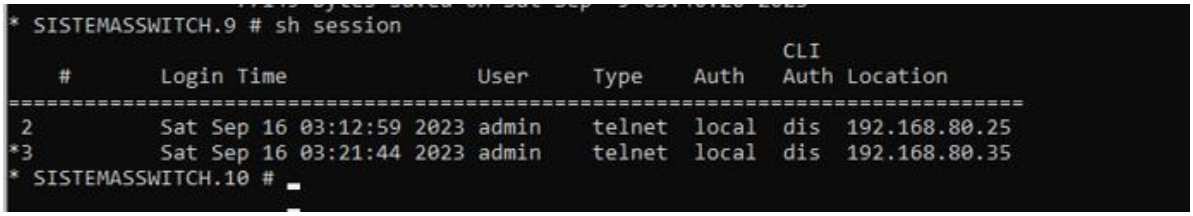


Fig. 3 show session.

As we can see in the Figure 3 there is no indication about the session has not been supported.

Then we verify existing user accounts using the following command:

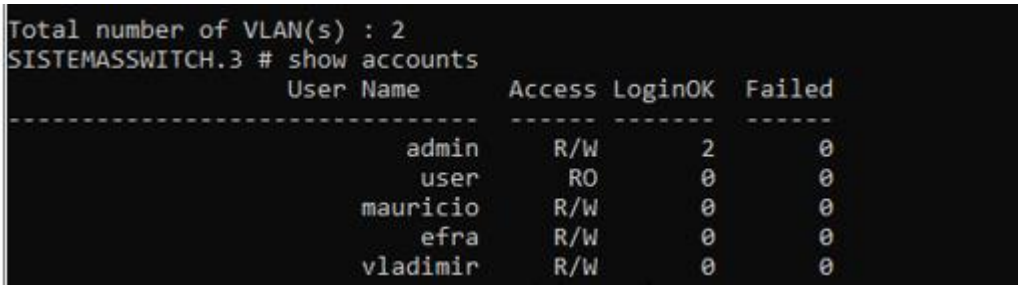


Fig. 4 show accounts

We also add a new user with administrator privileges using the following statement:

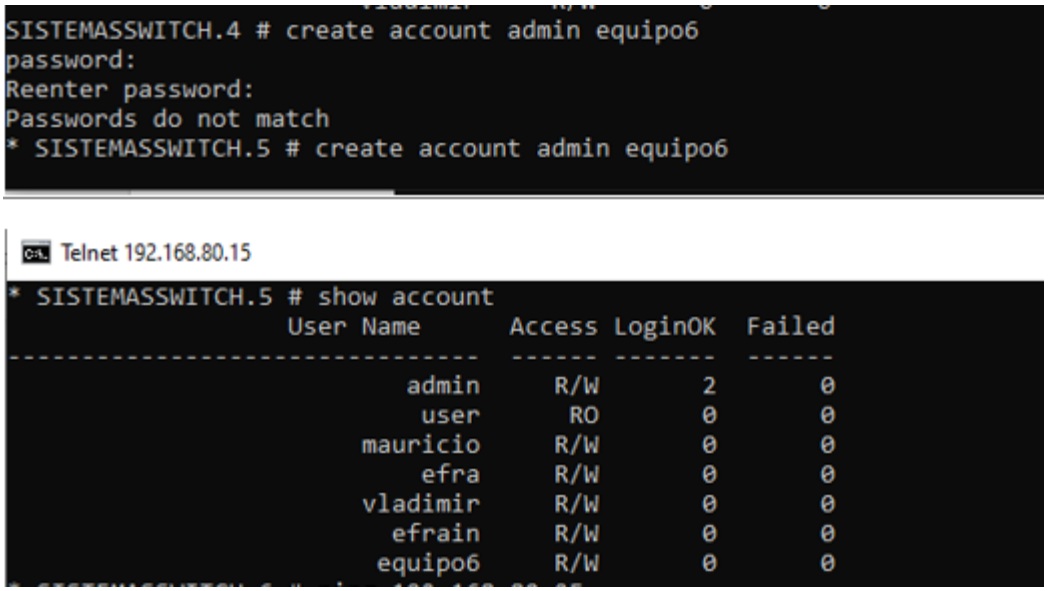


Fig. 5 create account admin < name >

Where < name > is the name of one of the team members. Do not assign ninguna

Contraseña ass is shown in Fig. 5.

By using the command again to display information about the current session, we see that the new account that we create was added to the information center.

Then we also display the default VLAN status and verify that port 2 is active, using the following command:

```
SISTEMASSWITCH.4 # show vlan default
VLAN Interface with name Default created by user
        Admin State:    Enabled         Tagging:        802.1Q Tag 1
        Virtual router: VR-Default
        Primary IP    : 192.168.80.15/24
        IPv6:           None
        STPD:           s0(Disabled,Auto-bind)
        Protocol:       Match all unfiltered protocols
        Loopback:       Disabled
        NetLogin:       Disabled
        QosProfile:     None configured
        Egress Rate Limit Designated Port: None configured
        Flood Rate Limit QosProfile:       None configured
        Ports:   26.      (Number of active ports=1)
           Untag:       1,      2,      3,      4,      5,      6,      7,
                        8,      9,     10,     11,     12,     13,     14,
                       15,     16,     17,     18,     19,     20,     21,
                       22,     23,    *24,     25,     26
        Flags:    (*) Active, (!) Disabled, (g) Load Sharing port
                  (b) Port blocked on the vlan, (m) Mac-Based port
                  (a) Egress traffic allowed for NetLogin
                  (u) Egress traffic unallowed for NetLogin
                  (t) Translate VLAN tag for Private-VLAN
                  (s) Private-VLAN System Port, (L) Loopback port
                  (e) Private-VLAN End Point Port
Press <SPACE> to continue or <Q> to quit:
```

Fig. 6 show VLAN default

We disable ports 1 through 3 on the switch using the following instruction: disable ports 1-3 and check the status of the switch ports with the following command: *show ports configuration (Fig 7)*.

```
SISTEMASSWITCH.5 # show port 1 config
Port Configuration Monitor                           Sat Sep 23 03:01:52 2023
Port     Virtual    Port  Link  Auto   Speed      Duplex   Flow  Load   Media
         router     State State Neg  Cfg Actual Cfg Actual Cntrl Master Pri Red
================================================================================
1        VR-Default  E      R    ON  AUTO       AUTO                     UTP

================================================================================
          > indicates Port Display Name truncated past 8 characters
          Link State: A-Active, R-Ready, NP-Port Not Present, L-Loopback
          Port State: D-Disabled, E-Enabled, Media: !-Unsupported Optic Module
          Media Red: * - use "show port info detail" for redundant media type
          0->Clear Counters  U->page up  D->page down ESC->exit
```

Fig. 7

So, we remove port 1 from the default VLAN, using the following command:

```
Total number of VLAN(s) : 3
* SISTEMASSWITCH.7 # config vlan default delete port 1
* SISTEMASSWITCH.8 # sh vlan default
VLAN Interface with name Default created by user
        Admin State:    Enabled         Tagging:        802.1Q Tag 1
        Virtual router: VR-Default
        Primary IP    : 192.168.80.15/24
        IPv6:           None
        STPD:           s0(Disabled,Auto-bind)
        Protocol:       Match all unfiltered protocols
        Loopback:       Disabled
        NetLogin:       Disabled
        QosProfile:     None configured
        Egress Rate Limit Designated Port: None configured
        Flood Rate Limit QosProfile:       None configured
        Ports:   25.      (Number of active ports=1)
           Untag:       2,      3,      4,      5,      6,      7,      8,
                        9,     10,     11,     12,     13,     14,     15,
                       16,     17,     18,     19,     20,     21,     22,
                       23,    *24,     25,     26
        Flags:    (*) Active, (!) Disabled, (g) Load Sharing port
                  (b) Port blocked on the vlan, (m) Mac-Based port
                  (a) Egress traffic allowed for NetLogin
                  (u) Egress traffic unallowed for NetLogin
                  (t) Translate VLAN tag for Private-VLAN
                  (s) Private-VLAN System Port, (L) Loopback port
                  (e) Private-VLAN End Point Port
Press <SPACE> to continue or <Q> to quit:
```

Fig. 8 configure vlan default delete ports 1.

And add ports 1 to the default VLAN with the following command:

```
* SISTEMASSWITCH.9 # config vlan libertad add port 1
* SISTEMASSWITCH.10 # show vlan libertad
VLAN Interface with name libertad created by user
        Admin State:    Enabled         Tagging:Untagged (Internal tag 4094)
        Virtual router: VR-Default
        Primary IP    : 192.168.70.15/24
        IPv6:           None
        STPD:           None
        Protocol:       Match all unfiltered protocols
        Loopback:       Disabled
        NetLogin:       Disabled
        QosProfile:     None configured
        Egress Rate Limit Designated Port: None configured
        Flood Rate Limit QosProfile:       None configured
        Ports:   1.       (Number of active ports=0)
           Untag:       1
        Flags:    (*) Active, (!) Disabled, (g) Load Sharing port
                  (b) Port blocked on the vlan, (m) Mac-Based port
                  (a) Egress traffic allowed for NetLogin
                  (u) Egress traffic unallowed for NetLogin
                  (t) Translate VLAN tag for Private-VLAN
                  (s) Private-VLAN System Port, (L) Loopback port
                  (e) Private-VLAN End Point Port
                  (x) VMAN Tag Translated port

* SISTEMASSWITCH.11 #
```

Fig. 9 configure vlan default add ports 1.

Finally, we verify that ports 1.2 are correctly assigned to the default VLAN by using the following command:

```
* SISTEMASSWITCH.6 # show vlan libertad
VLAN Interface with name libertad created by user
        Admin State:    Enabled         Tagging:Untagged (Internal tag 4094)
        Virtual router: VR-Default
        Primary IP    : 192.168.70.15/24
        IPv6:           None
        STPD:           None
        Protocol:       Match all unfiltered protocols
        Loopback:       Disabled
        NetLogin:       Disabled
        QosProfile:     None configured
        Egress Rate Limit Designated Port: None configured
        Flood Rate Limit QosProfile:       None configured
        Ports:   4.       (Number of active ports=3)
           Untag:      *1,     *2,      5,    *3g
        Flags:    (*) Active, (!) Disabled, (g) Load Sharing port
                  (b) Port blocked on the vlan, (m) Mac-Based port
                  (a) Egress traffic allowed for NetLogin
                  (u) Egress traffic unallowed for NetLogin
                  (t) Translate VLAN tag for Private-VLAN
                  (s) Private-VLAN System Port, (L) Loopback port
                  (e) Private-VLAN End Point Port
                  (x) VMAN Tag Translated port
```

Fig. 10

Conclusion

The lab practice effectively demonstrated the basic configuration of a switch via Telnet, covering fundamental tasks such as IP configuration, user management, SNMP setup, and VLAN/port adjustments.

It emphasized the importance of console connections for initial setup and demonstrated the transition to Ethernet-based management for easier remote access.

The lab exercise successfully familiarized individuals with essential commands and operations needed to configure and manage a network switch using Telnet.

We configured everything as were asked. We could log in into telnet as required and following that, we began entering the commands as showed in the file of the practice successfully.

We didn’t include the sh session part because we forgot it and also, we didn’t include pictures for the same reason, but we did it.

Bibliography

ExtremeXOS® Operating System - Extreme Networks - PDF Catalogs | Technical Documentation | Brochure. (s. f.). https://pdf.directindustry.com/pdf/extreme-networks/extremexos-operating-system/61501-870619.html

ExtremeWare. (s. f.). Direct Industry. Recuperado 23 de octubre de 6d. C., de https://raw.githubusercontent.com/espressif/arduino-esp32/gh-pages/package_esp32_index.json