UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

CENTRO DE CIENCIAS BÁSICAS
DEPARTAMENTO SISTEMAS ELECTRÓNICOS
SEGURIDAD EN SISTEMAS II

Vlans, Ruteo y ACLs

INGENIERÍA EN SISTEMAS COMPUTACIONALES

KEVIN DE JESUS GARCES DIAZ ID: 291461
ALAN UZIEL LOPEZ GARCIA ID: 297944
LUIS ANGEL ALVIZO LOPEZ ID: 291339
DANIEL PRECIADO DELGADILLO ID: 294165

9° SEMESTRE GRUPO A

PROFESOR: ARTURO OCAMPO SILVA

29/10/2024

ÍNDICE

INTRODUCCIÓN 3

OBJETIVO 4

DESARROLLO 5

Computadoras correctamente configuradas 6

Estructura básica de switch con sus respectivas vlan 8

VLAN 10 - "Sistemas" 8

VLAN 20 - "RH" (Recursos Humanos) 9

VLAN 30 - "Compras" 9

VLAN 40 - "Contabilidad" 9

Routers con su respectivo encapsulamiento 11

Routers con sus respectivas ACL 15

CONCLUSIONES 20

BIBLIOGRAFÍA 21

INTRODUCCIÓN

En este proyecto nos hemos embarcado en el reto de diseñar y gestionar una red de comunicaciones para tres empresas automotrices que trabajan en conjunto. Cada una tiene sus propias necesidades y particularidades, lo que hace que la tarea sea más que simplemente conectar computadoras y cables; es un desafío de coordinación y seguridad.

La idea central es que cada empresa cuente con su propia estructura de red, pero manteniendo la capacidad de comunicarse con las otras cuando sea necesario. Sin embargo, no todos los departamentos pueden interactuar libremente. Los equipos de Recursos Humanos de las tres empresas, por ejemplo, deben estar en contacto, pero la privacidad entre otras áreas debe mantenerse. Es decir, si bien las empresas colaboran, cada departamento necesita trabajar aislado para evitar posibles conflictos de información.

Para lograrlo, hemos configurado una serie de VLANs, routers y listas de control de acceso (ACLs) que garantizan que solo el tráfico necesario fluya entre los distintos segmentos de la red. Esto permite que las empresas trabajen codo a codo, compartiendo lo que deben, pero manteniendo la privacidad y seguridad en cada espacio donde es crítico. A lo largo del proyecto, cada paso se ha enfocado en cumplir con estos requisitos de manera clara y efectiva, asegurando que la red funcione de forma ágil y segura.

OBJETIVO

El objetivo de esta práctica es configurar y administrar una red conformada por tres empresas automotrices que trabajan en conjunto, utilizando la herramienta Cisco Packet Tracer. Cada empresa tiene su propia estructura de red con cuatro VLANs (Sistemas, Recursos Humanos, Contabilidad y Compras), y se requiere permitir la comunicación entre las VLANs equivalentes de las diferentes empresas, mientras se asegura el aislamiento de los departamentos internos de cada empresa. Además, se deben implementar reglas de enrutamiento y listas de control de acceso (ACLs) para controlar el flujo de información entre las redes.

La práctica busca garantizar que solo los dispositivos que pertenecen a la misma VLAN en diferentes empresas puedan comunicarse entre sí, manteniendo aisladas las demás VLANs y asegurando que no haya comunicación no autorizada. Para lograr este objetivo, se configuraron subinterfaces en routers, se implementaron rutas estáticas, y se aplicaron Access Lists para cumplir con los requerimientos de seguridad y segmentación de la red.

DESARROLLO

Para cada empresa, se segmentó la red de la siguiente manera:

Para la Empresa 1:

- **VLAN 10 (Sistemas)**: 192.168.10.0/24
- **VLAN 20 (Recursos Humanos)**: 192.168.20.0/24
- **VLAN 30 (Contabilidad)**: 192.168.30.0/24
- **VLAN 40 (Compras)**: 192.168.40.0/24

Para la Empresa 2:

- **VLAN 10 (Sistemas)**: 172.140.10.0/24
- **VLAN 20 (Recursos Humanos)**: 172.140.20.0/24
- **VLAN 30 (Contabilidad)**: 172.140.30.0/24
- **VLAN 40 (Compras)**: 172.140.40.0/24

Para la Empresa 3:

- **VLAN 10 (Sistemas)**: 10.10.10.0/24
- **VLAN 20 (Recursos Humanos)**: 10.10.20.0/24
- **VLAN 30 (Contabilidad)**: 10.10.30.0/24
- **VLAN 40 (Compras)**: 10.10.40.0/24

En la figura 1 presentada se muestra el resultado final de la práctica, en la cual se puede observar la estructura de red implementada para cada empresa. Cada empresa tiene su propio router conectado a un switch de capa 2, el cual segmenta la red en las diferentes VLANs establecidas. Los routers están interconectados mediante enlaces troncales que permiten la comunicación entre las VLANs equivalentes de las tres empresas. Los enlaces rojos en la imagen indican las conexiones físicas entre los routers, mientras que los enlaces negros muestran la conexión de los dispositivos finales a los switches de cada empresa.

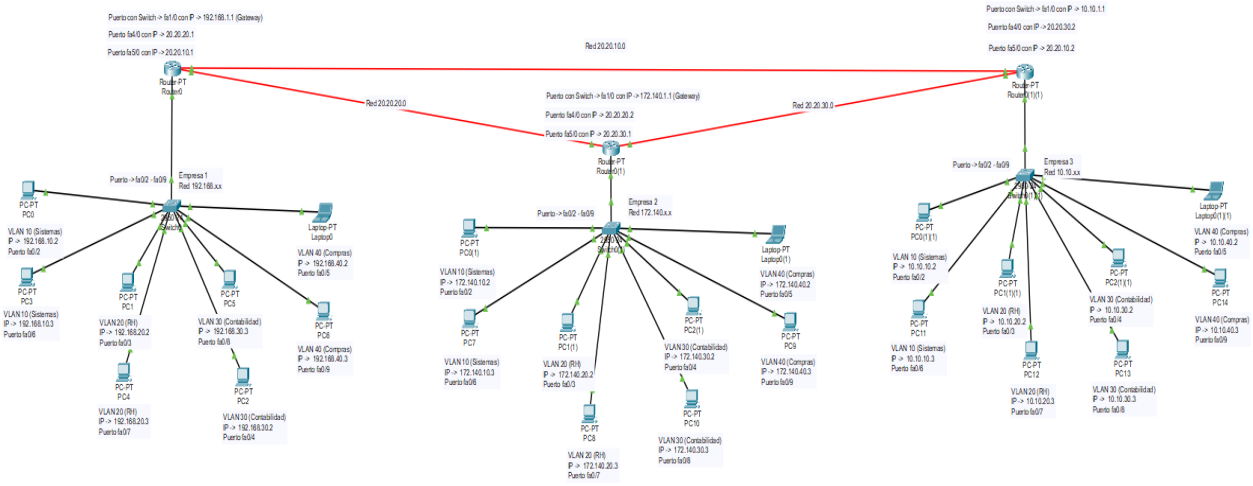


Figura 1 Red de las tres empresas

Computadoras correctamente configuradas

En este apartado se verificó que todas las computadoras estuvieran correctamente configuradas con las siguientes características:

1. **Direcciones IP asignadas**: Se configuraron las direcciones IP adecuadas para cada VLAN, asegurando que cada computadora tenga una IP única dentro de su subred y que pertenezca al rango correspondiente a su VLAN (Sistemas, Recursos Humanos, Contabilidad o Compras). Esta configuración fue fundamental para garantizar que cada dispositivo pudiera comunicarse con los recursos de su misma VLAN sin conflictos y evitando problemas de duplicación de IPs, lo cual es crítico para el funcionamiento estable de la red, a continuación, se podrá ver en las siguientes tres figuras las direcciones IP de cada computadora en su respectiva empresa.

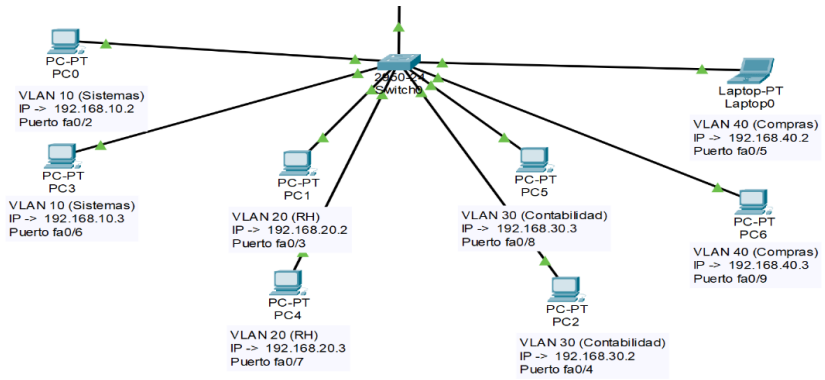


Figura 2 Computadoras configuradas en la Empresa 1

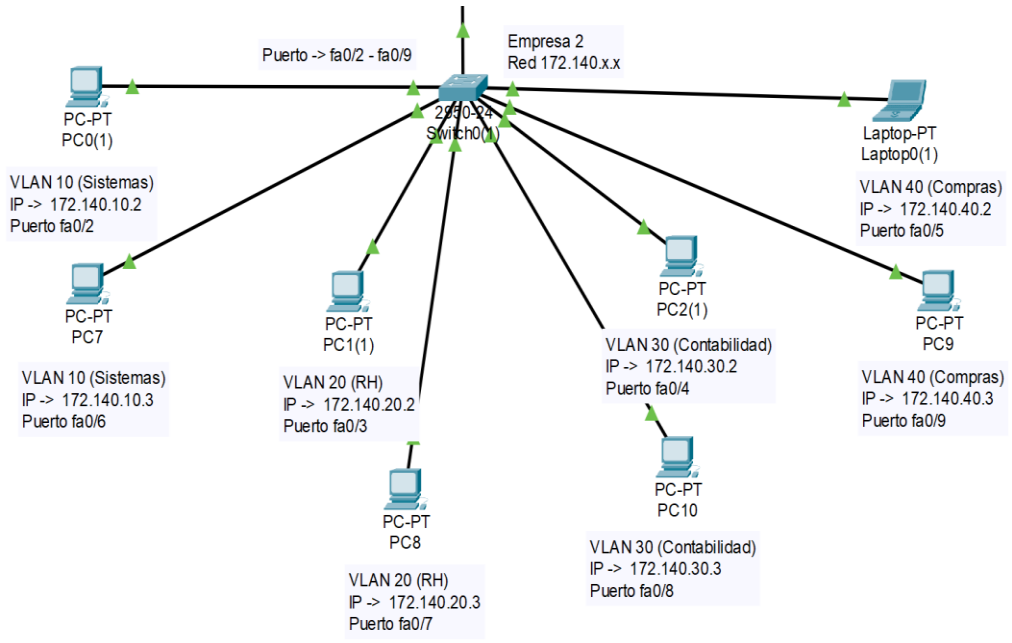


Figura 3 Computadoras configuradas en la Empresa 2

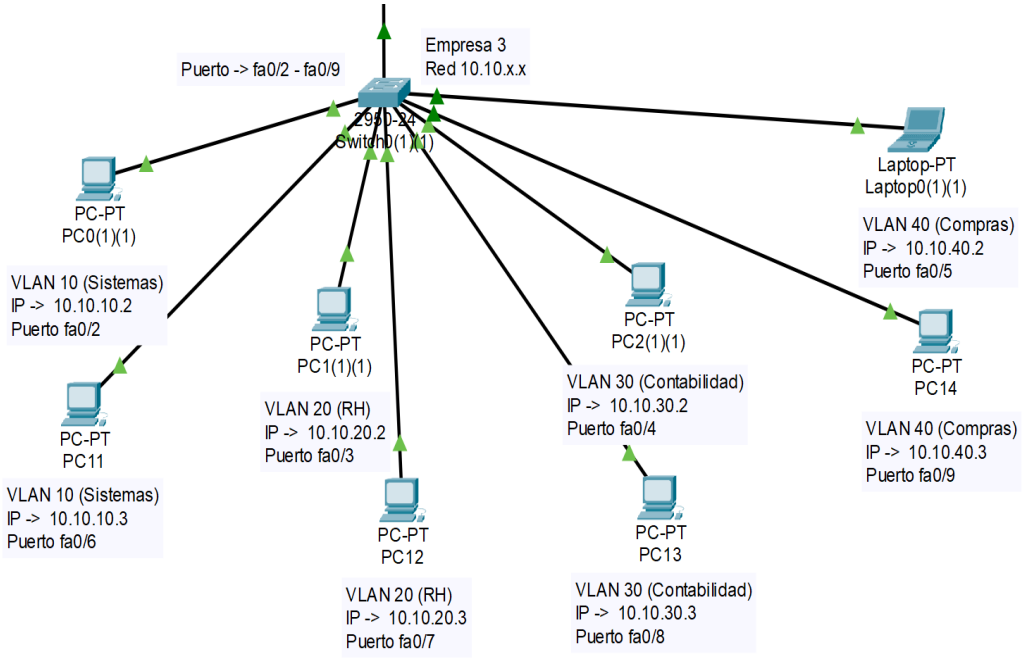


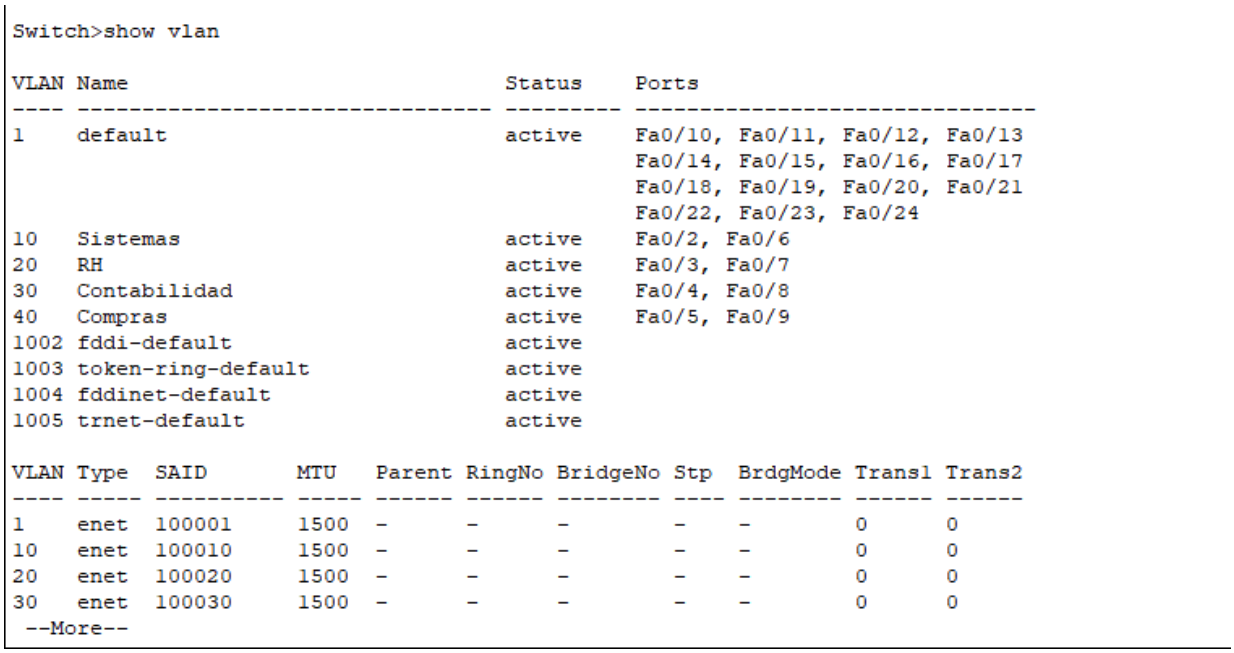
Figura 4 Computadoras configuradas en la Empresa 3

2. **Puerta de enlace predeterminada**: Se configuró la puerta de enlace predeterminada para cada computadora, asegurando que la dirección IP del gateway corresponda a la subinterfaz del router que maneja la VLAN específica. Por ejemplo, para las computadoras en la **VLAN 10 (Sistemas)** de la **Empresa 1**, se utilizó la subinterfaz **fa1/0.10** con la dirección **192.168.10.1**

como puerta de enlace. De manera similar, se configuraron las puertas de enlace para las demás VLANs en cada empresa, garantizando que cada dispositivo pudiera comunicarse adecuadamente fuera de su subred local, facilitando la conectividad hacia otras VLANs equivalentes en las diferentes empresas. La correcta configuración de las puertas de enlace asegura que el tráfico pueda ser redirigido apropiadamente y evita problemas de comunicación inter-VLAN.

Estructura básica de switch con sus respectivas vlan

Se puede observar la estructura básica de las VLAN configuradas dentro del Switch en la **figura 5**, el cual, esto mismo se aplicó para las tres empresas**.**



```
Switch>show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
10   Sistemas                          active    Fa0/2, Fa0/6
20   RH                                active    Fa0/3, Fa0/7
30   Contabilidad                      active    Fa0/4, Fa0/8
40   Compras                           active    Fa0/5, Fa0/9
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
 --More--
```

Figura 5 Estructura básica del switch y sus VLAN

VLAN 10 - "Sistemas"

- **Estado**: Active
- **Puertos asignados**: Fa0/2 y Fa0/6
- **Descripción**:
    - Esta VLAN está configurada para el departamento de Sistemas. Los puertos **Fa0/2** y **Fa0/6** están dedicados a dispositivos o usuarios que pertenecen a este departamento, asegurando que todo el tráfico en estos puertos se mantenga dentro de la VLAN de Sistemas.

    - **VLAN ID (SAID)**: **100010**
    - **MTU**: 1500 (tamaño de paquete estándar)

VLAN 20 - "RH" (Recursos Humanos)

- **Estado**: Active
- **Puertos asignados**: Fa0/3 y Fa0/7
- **Descripción**:
    - Esta VLAN está configurada para el departamento de Recursos Humanos (RH). Los puertos **Fa0/3** y **Fa0/7** están dedicados exclusivamente a este departamento, aislando su tráfico de otras áreas de la red.
    - **VLAN ID (SAID)**: **100020**
    - **MTU**: 1500

VLAN 30 - "Compras"

- **Estado**: Active
- **Puertos asignados**: Fa0/4 y Fa0/8
- **Descripción**:
    - Esta VLAN está configurada para el departamento de Compras. Los puertos **Fa0/4** y **Fa0/8** pertenecen a esta VLAN, asegurando que todos los dispositivos conectados en estos puertos estén en la red del departamento de Compras.
    - **VLAN ID (SAID)**: **100030**
    - **MTU**: 1500

VLAN 40 - "Contabilidad"

- **Estado**: Active
- **Puertos asignados**: Fa0/5 y Fa0/9
- **Descripción**:
    - Esta VLAN está destinada al departamento de Contabilidad. Los puertos **Fa0/5** y **Fa0/9** se utilizan exclusivamente para este departamento, asegurando un tráfico segmentado y aislado del resto de la red.
    - **VLAN ID (SAID)**: **100040**

- **MTU**: 1500

Dentro de la estructura básica del switch, también podemos observar lo que se muestra en la **Figura 6**. En esta figura se presenta la configuración de las interfaces FastEthernet0/1 a FastEthernet0/9, donde cada una está configurada para pertenecer a una VLAN específica o como puerto troncal, esto se realizó en cada Switch de cada respectiva empresa.

```
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 40
 switchport mode access
!
```

Figura 6 Configuración de VLANs y Puertos en el Switch

- **Modo Trunk** (Interfaz FastEthernet0/1):
  El puerto Fa0/1 está configurado como troncal, permitiendo que varias VLANs (10, 20, 30, 40) compartan el puerto.

- **Modo Access** (Interfaz FastEthernet0/2 - Fa0/9):
  Todos los demás puertos (Fa0/2 hasta Fa0/9) están configurados en modo de acceso, lo que significa que cada puerto pertenece a una sola VLAN específica (VLAN 10, 20, 30, o 40). Esto aísla el tráfico de cada VLAN y permite la segmentación de la red por departamentos u otras funciones.

Routers con su respectivo encapsulamiento

En la figura 7 se muestra la configuración de un Router (Router0) que utiliza subinterfaces en la interfaz FastEthernet1/0 para manejar el tráfico de diferentes VLANs mediante el protocolo 802.1Q. Cada subinterfaz tiene un encapsulamiento y una dirección IP específica para enrutar el tráfico de una VLAN.

Cada subinterfaz tiene asignado un grupo de acceso (access-group) para controlar el tráfico saliente, ayudando a administrar la seguridad y el enrutamiento entre VLANs. Esta configuración permite que el router funcione como un enrutador de inter-VLAN, facilitando la comunicación entre dispositivos en diferentes VLANs mediante la misma interfaz física, esta configuración le corresponde al Router de la **empresa número uno**.

```
interface FastEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip access-group 1 out
!
interface FastEthernet1/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip access-group 2 out
!
interface FastEthernet1/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group 3 out
!
interface FastEthernet1/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 ip access-group 4 out
!
```

Figura 7 Configuración de Subinterfaces en el Router0 con Encapsulamiento para VLANs

Detalles de configuración:

- **FastEthernet1/0:** Interfaz principal con la IP 192.168.1.1 y configuración automática de duplex y speed.
- **FastEthernet1/0.10:** Subinterfaz para la VLAN 10 con encapsulamiento dot1Q 10 y dirección IP 192.168.10.1.
- **FastEthernet1/0.20:** Subinterfaz para la VLAN 20 con encapsulamiento dot1Q 20 y dirección IP 192.168.20.1.
- **FastEthernet1/0.30:** Subinterfaz para la VLAN 30 con encapsulamiento dot1Q 30 y dirección IP 192.168.30.1.
- **FastEthernet1/0.40:** Subinterfaz para la VLAN 40 con encapsulamiento dot1Q 40 y dirección IP 192.168.40.1.

En la figura 8 se presenta la configuración de subinterfaces en la interfaz **FastEthernet1/0** del **Router0(1)**. Estas subinterfaces permiten al router gestionar el tráfico de distintas VLANs mediante encapsulamiento **802.1Q**, facilitando el enrutamiento entre las VLANs, esta configuración le corresponde al Router de la **empresa número dos**.

```
interface FastEthernet1/0
 ip address 172.140.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0.10
 encapsulation dot1Q 10
 ip address 172.140.10.1 255.255.255.0
 ip access-group 1 out
!
interface FastEthernet1/0.20
 encapsulation dot1Q 20
 ip address 172.140.20.1 255.255.255.0
 ip access-group 2 out
!
interface FastEthernet1/0.30
 encapsulation dot1Q 30
 ip address 172.140.30.1 255.255.255.0
 ip access-group 3 out
!
interface FastEthernet1/0.40
 encapsulation dot1Q 40
 ip address 172.140.40.1 255.255.255.0
 ip access-group 4 out
!
```

Figura 8 Configuración de Subinterfaces en el Router0(1)

con Encapsulamiento para VLANs

Detalles de configuración:

- **FastEthernet1/0**:
  - **IP**: 172.140.1.1
  - **Máscara**: 255.255.255.0
  - Configuración de **duplex** y **speed** automáticas.
- **Subinterfaz FastEthernet1/0.10**:
  - **Encapsulación**: dot1Q 10 (VLAN 10)
  - **IP**: 172.140.10.1
  - **Máscara**: 255.255.255.0
  - **Grupo de acceso**: access-group 1 out
- **Subinterfaz FastEthernet1/0.20**:
  - **Encapsulación**: dot1Q 20 (VLAN 20)
  - **IP**: 172.140.20.1
  - **Máscara**: 255.255.255.0
  - **Grupo de acceso**: access-group 2 out
- **Subinterfaz FastEthernet1/0.30**:
  - **Encapsulación**: dot1Q 30 (VLAN 30)
  - **IP**: 172.140.30.1
  - **Máscara**: 255.255.255.0
  - **Grupo de acceso**: access-group 3 out
- **Subinterfaz FastEthernet1/0.40**:
  - **Encapsulación**: dot1Q 40 (VLAN 40)
  - **IP**: 172.140.40.1
  - **Máscara**: 255.255.255.0
  - **Grupo de acceso**: access-group 4 out

En la **Figura 9**, se muestra la configuración de **subinterfaces** en la interfaz **FastEthernet1/0** de **Router0(1)(1)**. Esta configuración permite al router enrutar tráfico para diferentes VLANs en la red 10.10.X.X utilizando encapsulamiento **802.1Q,** esta configuración le corresponde al Router de la **empresa número tres**.

```
interface FastEthernet1/0
 ip address 10.10.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
 ip access-group 100 out
!
interface FastEthernet1/0.20
 encapsulation dot1Q 20
 ip address 10.10.20.1 255.255.255.0
 ip access-group 2 out
!
interface FastEthernet1/0.30
 encapsulation dot1Q 30
 ip address 10.10.30.1 255.255.255.0
 ip access-group 3 out
!
interface FastEthernet1/0.40
 encapsulation dot1Q 40
 ip address 10.10.40.1 255.255.255.0
 ip access-group 4 out
!
```

Figura 9 Configuración de Subinterfaces en el Router0(1)(1)

con Encapsulamiento para VLANs

Cada subinterfaz de FastEthernet1/0 se ha configurado con un encapsulamiento 802.1Q que permite al router identificar el tráfico de cada VLAN (10, 20, 30, 40) y asignarle una dirección IP específica en la red 10.10.X.X. Los grupos de acceso aplicados a cada subinterfaz controlan el tráfico saliente, proporcionando un nivel de seguridad y filtrado en el enrutamiento entre VLANs. Esto permite que el router actúe como un enrutador de inter-VLAN, permitiendo comunicación entre dispositivos de diferentes VLANs dentro de la red definida.

Routers con sus respectivas ACL

En esta sección se detallan las configuraciones de los routers para cada una de las tres empresas, haciendo especial énfasis en las Access Lists (ACLs) utilizadas para controlar el flujo de tráfico entre las VLANs equivalentes y asegurar el aislamiento de las VLANs no autorizadas. Las ACLs juegan un papel crucial en garantizar la seguridad y segmentación de la red, permitiendo la comunicación únicamente entre dispositivos que pertenecen a la misma VLAN en las diferentes empresas, mientras se bloquea el acceso entre VLANs diferentes.

Para cada empresa, se configuraron las ACLs necesarias para permitir la comunicación entre las VLANs equivalentes y denegar cualquier otro tráfico. A continuación, se presentan las capturas de pantalla de las ACLs aplicadas en cada router y una breve explicación de su propósito y funcionamiento.

Empresa 1:

- En el router de la Empresa 1 se crearon ACLs estándar que permiten el tráfico de la VLAN 10 (Sistemas) hacia las VLAN 10 de las otras dos empresas (Empresa 2 y Empresa 3). De igual forma, se realizaron configuraciones similares para las demás VLANs. La figura 10 muestra las reglas implementadas, las cuales incluyen las instrucciones permit para los rangos de direcciones IP equivalentes. Esta configuración asegura que únicamente los dispositivos de la misma VLAN puedan comunicarse, garantizando el aislamiento necesario entre los departamentos.

  Las ACLs fueron asignadas a las respectivas subinterfaces, como fa1/0.10 para VLAN 10 y así sucesivamente para las otras subinterfaces y su respectiva VLAN asegurando que cada regla se aplique solo al tráfico correspondiente a su VLAN, esto se puede apreciar en la figura 11.

```
Standard IP access list 1
    10 permit 172.140.10.0 0.0.0.255
    20 permit 10.10.10.0 0.0.0.255
Standard IP access list 2
    10 permit 172.140.20.0 0.0.0.255
    20 permit 10.10.20.0 0.0.0.255
Standard IP access list 3
    10 permit 172.140.30.0 0.0.0.255
    20 permit 10.10.30.0 0.0.0.255
Standard IP access list 4
    10 permit 172.140.40.0 0.0.0.255
    20 permit 10.10.40.0 0.0.0.255
```

Figura 10 Access list creadas para la empresa uno

```
interface FastEthernet1/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip access-group 1 out
!
interface FastEthernet1/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip access-group 2 out
!
interface FastEthernet1/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group 3 out
!
interface FastEthernet1/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 ip access-group 4 out
```

Figura 11 Asignación de Access list en la subinterface correspondiente

Empresa 2:

- El router de la Empresa 2 tiene configuradas ACLs similares a las de la Empresa 1. Se definieron reglas específicas para permitir el tráfico entre las VLANs equivalentes (por ejemplo, la VLAN 20 de Empresa 2 puede

comunicarse con las VLAN 20 de Empresa 1 y Empresa 3), mientras que el acceso a las VLANs no equivalentes se deniega. La figura 12 muestra cómo se estructuraron las reglas permit, junto con los números de secuencia que ayudan a mantener un orden claro y preciso en la aplicación de las políticas de filtrado. Estas ACLs también fueron asignadas a las subinterfaces correspondientes, como **fa1/0.20** para **VLAN 20**, para asegurar un control efectivo del tráfico (figura 13).

```
Standard IP access list 1
    10 permit 192.168.10.0 0.0.0.255
    20 permit 10.10.10.0 0.0.0.255
Standard IP access list 2
    10 permit 192.168.20.0 0.0.0.255
    20 permit 10.10.20.0 0.0.0.255
Standard IP access list 3
    10 permit 192.168.30.0 0.0.0.255
    20 permit 10.10.30.0 0.0.0.255
Standard IP access list 4
    10 permit 192.168.40.0 0.0.0.255
    20 permit 10.10.40.0 0.0.0.255
```

Figura 12 Access list creadas para la empresa dos

```
interface FastEthernet1/0.10
 encapsulation dot1Q 10
 ip address 172.140.10.1 255.255.255.0
 ip access-group 1 out
!
interface FastEthernet1/0.20
 encapsulation dot1Q 20
 ip address 172.140.20.1 255.255.255.0
 ip access-group 2 out
!
interface FastEthernet1/0.30
 encapsulation dot1Q 30
 ip address 172.140.30.1 255.255.255.0
 ip access-group 3 out
!
interface FastEthernet1/0.40
 encapsulation dot1Q 40
 ip address 172.140.40.1 255.255.255.0
 ip access-group 4 out
```

Figura 13 Asignación de Access list en la subinterface correspondiente

Empresa 3:

- En el router de la Empresa 3 también se implementaron ACLs extendidas para cumplir con los mismos objetivos. Las ACLs permiten el tráfico entre las VLANs equivalentes y bloquean el tráfico entre VLANs no autorizadas. Las reglas fueron aplicadas de tal forma que cualquier paquete de una VLAN que no sea equivalente sea inmediatamente bloqueado, proporcionando un nivel adicional de seguridad. En la captura de pantalla se puede observar la estructura de estas ACLs y cómo se configuraron para asegurar que cada VLAN esté correctamente segmentada, manteniendo la integridad de los datos y el acceso controlado. Estas ACLs fueron asignadas a las subinterfaces respectivas, como **fa1/0.30** para **VLAN 30**, garantizando que cada VLAN esté protegida de manera adecuada, esto se puede observar en la figura 14 y 15.

```
Standard IP access list 1
    10 permit 192.168.10.0 0.0.0.255
    20 permit 172.140.10.0 0.0.0.255
    30 permit 10.10.10.0 0.0.0.255
Standard IP access list 2
    10 permit 192.168.20.0 0.0.0.255
    20 permit 172.140.20.0 0.0.0.255
Standard IP access list 3
    10 permit 192.168.30.0 0.0.0.255
    20 permit 172.140.30.0 0.0.0.255
Standard IP access list 4
    10 permit 192.168.40.0 0.0.0.255
    20 permit 172.140.40.0 0.0.0.255
```

Figura 14 Access list creadas para la empresa tres

```
interface FastEthernet1/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
 ip access-group 100 out
!
interface FastEthernet1/0.20
 encapsulation dot1Q 20
 ip address 10.10.20.1 255.255.255.0
 ip access-group 2 out
!
interface FastEthernet1/0.30
 encapsulation dot1Q 30
 ip address 10.10.30.1 255.255.255.0
 ip access-group 3 out
!
interface FastEthernet1/0.40
 encapsulation dot1Q 40
 ip address 10.10.40.1 255.255.255.0
 ip access-group 4 out
```

Figura 15 Asignación de Access list en la subinterface correspondiente

CONCLUSIONES

Luis Angel Alvizo López.- En este proyecto aprendí la importancia de organizar bien una red y asegurar la comunicación entre diferentes áreas de manera controlada. Al configurar las VLANs y las ACLs, entendí cómo segmentar la red para que solo ciertos departamentos puedan comunicarse, manteniendo la privacidad de cada uno.

También me quedó claro cómo funcionan las subinterfaces y el encapsulamiento, que permiten manejar el tráfico de varias VLANs en un solo router. Esto fue clave para mantener el orden y control en la red. Al final, me di cuenta de que configurar una red no es solo conectar equipos, sino pensar en cómo proteger y organizar la información de manera eficiente.

Kevin de Jesús Garcés Díaz.- En conclusión, al realizar este trabajo, logramos trabajar en equipo para configurar los routers, donde definimos las direcciones IP, los saltos que podían ocurrir entre redes, y creamos las VLANs necesarias. También configuramos el modo trunk para permitir la comunicación entre ellas, además de crear subinterfaces y encapsularlas correctamente para segmentar el tráfico de manera eficiente. Cada paso fue crucial para garantizar que la red estuviera bien estructurada y pudiera funcionar sin problemas.

A lo largo del proceso, enfrentamos algunos errores que resolvimos colaborando y revisando cada detalle, como los saltos entre las nuevas subinterfaces. Finalmente, creamos reglas de acceso (ACLs) para asegurar el control del tráfico en cada segmento de la red. El trabajo en equipo fue clave para superar los desafíos y asegurarnos de que todo estuviera correctamente configurado.

Alan Uziel López García.- Esta práctica me permitió comprender a cómo segmentar y asegurar una red empresarial mediante el uso de VLANs, subinterfaces, rutas estáticas y ACLs. La configuración de las ACLs para controlar la comunicación entre las VLANs equivalentes y asegurar el aislamiento adecuado para crear un entorno seguro y eficiente. Además, trabajar con las subinterfaces y ver cómo cada segmento de la red interactúa me ayudó a tener una visión más clara sobre la importancia de la segmentación y la administración adecuada del tráfico.

Daniel Preciado Delgadillo.- Durante el desarrollo de esta práctica se comprendió la importancia de una correcta configuración de VLANs y ACLs dentro de una red, esto con el objetivo de lograr una aislamiento y protección.

BIBLIOGRAFÍA

Cisco Networking Academy. (n.d.). *Cisco Networking Academy Courses*. Cisco Systems. Recuperado de https://www.netacad.com/courses/networking

Walton, A. (2020, June 10). Configuración de VLAN [Comandos] CCNA desde Cero. CCNA Desde Cero. https://ccnadesdecero.es/configuracion-vlan/