Seguridad en Sistemas II

Vlans, Ruteos y ACLs

Profesor: Arturo Ocampo Silva

Alumnos:

Gonzalo Ruvalcaba Solís

María Fernanda Hermosillo Orenday

José Julián Carreón Plasencia

Zaid Diaz Salazar

Fecha de entrega: 29 de octubre de 2024

Índice

Introducción

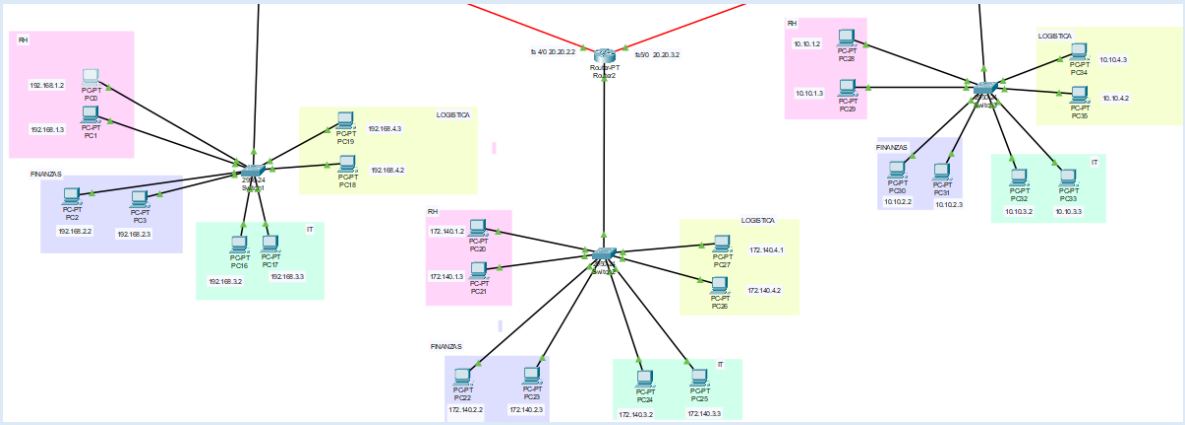
En este presente proyecto, se desarrollará la administración de una red empresarial que conecta tres empresas automotrices trabajando en colaboración. Cada empresa cuenta con su propia estructura de red y un conjunto de cuatro departamentos: Recursos Humanos, Finanzas, Operaciones y Ventas. La comunicación entre departamentos está limitada por reglas de seguridad, lo que permite únicamente la interacción entre los mismos departamentos de cada empresa, mientras que se restringe la comunicación con otros departamentos dentro de la misma organización. Para asegurar esta conectividad controlada, se implementarán VLANs en cada empresa y se configurarán reglas de ruteo y listas de control de acceso (ACL) en los routers, garantizando la seguridad y eficiencia de la red. Este proyecto se basa en la configuración de subredes específicas para cada empresa, asignando direcciones IP en los rangos 192.168.x.x, 172.140.x.x y 10.10.x.x respectivamente, lo que permitirá la adecuada segmentación de la red y un control detallado del tráfico entre las diferentes áreas y empresas involucradas.

Objetivo

Diseñar y configurar una red que permita la comunicación segura y controlada entre tres empresas automotrices. Cada empresa tiene cuatro departamentos, y cada departamento debe comunicarse únicamente con su equivalente en las otras dos empresas. Describe también los objetivos específicos, como la configuración de VLANs, enrutamiento con ACL y encapsulamiento.

Desarrollo

1. **Computadoras correctamente configuradas**



Cada computadora tiene su ip correspondiente, su mascara de red y su Gateway.

Para la empresa 1, se tiene la dirección ip de 192.168.x.x

Para el departamento de RH

- Para la computadora 1 de la empresa 1 tiene la ip 192.168.1.2
- Para la computadora 2 de la empresa 1 tiene la ip 192.168.1.3

  Y así para los demás departamentos de la empresa 1.

Para la empresa 2, se tiene la dirección ip de 172.140.x.x

Para el departamento de RH

- Para la computadora 1 de la empresa 2 tiene la ip 172.140.2.2
- Para la computadora 2 de la empresa 1 tiene la ip 172.140.2.3

  Y así para los demás departamentos de la empresa 2.

Para la empresa 1, se tiene la dirección ip de 10.10.x.x

Para el departamento de RH

- Para la computadora 1 de la empresa 1 tiene la ip 10.10.3.2
- Para la computadora 2 de la empresa 1 tiene la ip 10.10.3.3

Y así para los demás departamentos de la empresa 3.

De igual manera el Gateway le fue asignada a cada computadora según el departamento y la empresa:

Para la empresa 1 y dpto de Rh:

- Para la computadora 1 se le asigno 192.168.1.1
- Para la computadora 2 se le asigno 192.168.2.1

Para la empresa 2 y dpto de Rh:

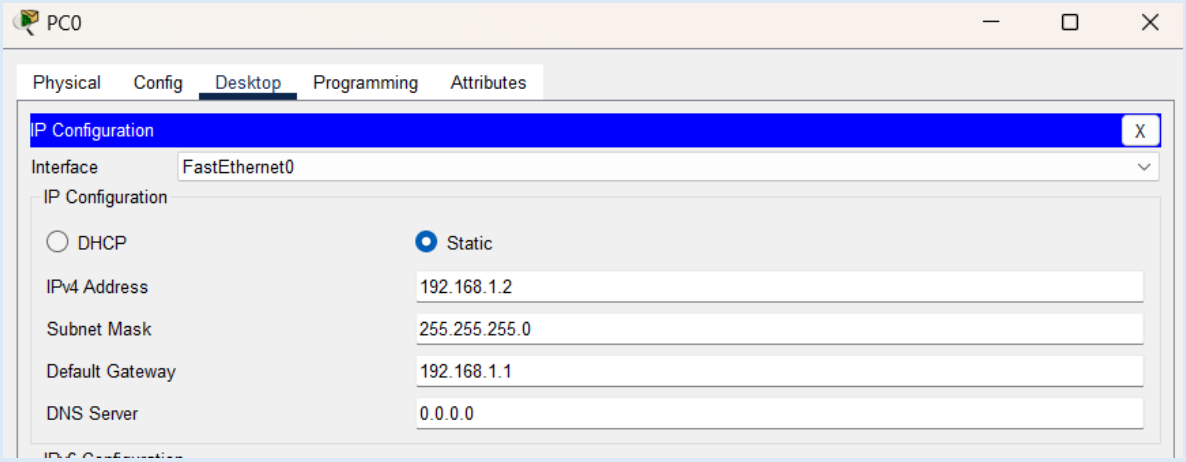
- Para la computadora 1 se le asigno 172.140.1.1
- Para la computadora 2 se le asigno 172.140.2.1

Para la empresa 3 y dpto de Rh:

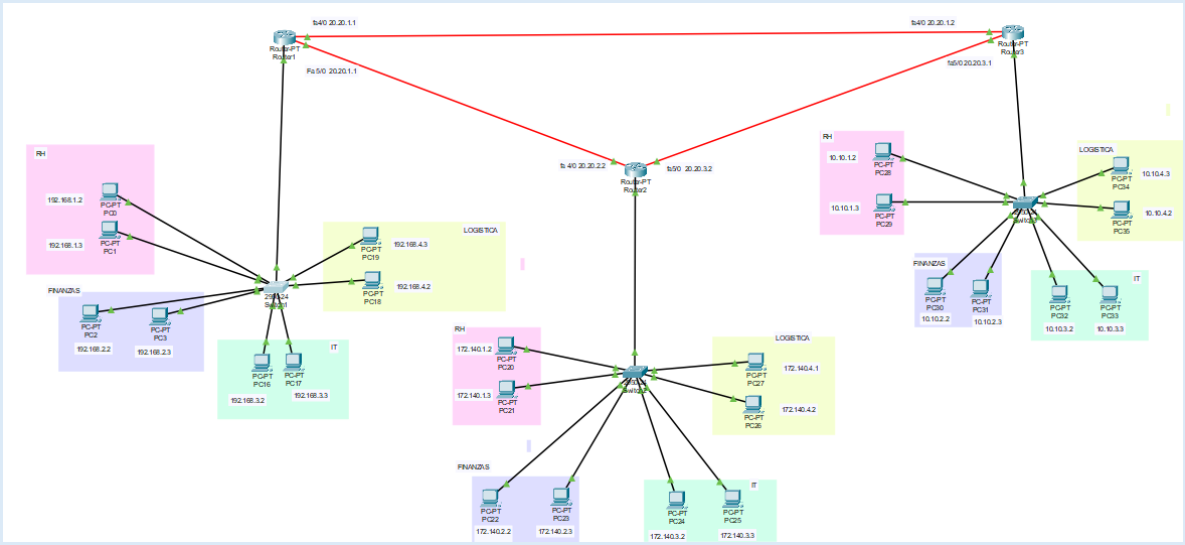
- Para la computadora 1 se le asigno 10.10.1.1
- Para la computadora 2 se le asigno 10.10.2.1

Se siguió el mismo procedimiento para asignar el Gateway a las demás computadoras de los distintos departamentos, el gateway en la configuración de red de cada computadora es la dirección IP del dispositivo que actúa como puerta de enlace para enviar y recibir datos hacia y desde redes externas a la suya.

Por ejemplo, esta es la configuración de una computadora para el departamento de Rh de la empresa 1:



2. Estructura básica de switch con sus respectivas vlan



Se tienen tres switches, cada switch para una empresa automotriz, en cada switch tenemos conectadas 8 computadoras, estas 8 computadoras las dividimos para que cada dos pertenecieran a un departamento, es decir dos computadoras pertenecen al departamento de RH, dos computadoras pertenecen a Finanzas, 2 computadoras pertenecen a IT y dos computadoras pertenecen a Logística. En total se tienen cuatro departamentos, cada departamento tiene su propia vlan, para RH se tiene la vlan 10, para Finanzas se tiene la vlan 20, para IT se tiene la vlan 30 y para Logística se tiene la vlan 40.

Cada vlan está aislada de las demás para garantizar la seguridad interna.

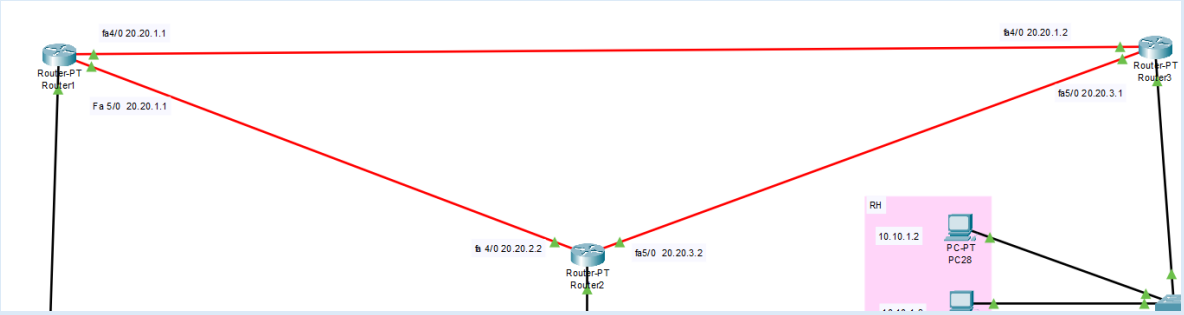
Ejemplo del switch 1 del departamento 1:

```
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   RH                               active    Fa0/2, Fa0/3
20   Finanzas                         active    Fa0/4, Fa0/5
30   IT                               active    Fa0/6, Fa0/7
40   Logistica                        active    Fa0/8, Fa0/9
```

```
Device Name: Switch1
Device Model: 2950-24
Hostname: Switch

Port              Link   VLAN   IP Address         MAC Address
FastEthernet0/1   Up     --     --                 0090.0C69.2C01
FastEthernet0/2   Up     10     --                 0090.0C69.2C02
FastEthernet0/3   Up     10     --                 0090.0C69.2C03
FastEthernet0/4   Up     20     --                 0090.0C69.2C04
FastEthernet0/5   Up     20     --                 0090.0C69.2C05
FastEthernet0/6   Up     30     --                 0090.0C69.2C06
FastEthernet0/7   Up     30     --                 0090.0C69.2C07
FastEthernet0/8   Up     40     --                 0090.0C69.2C08
FastEthernet0/9   Up     40     --                 0090.0C69.2C09
```

3. Routers con su respectivo encapsulamiento

Como se observó anteriormente cada switch tiene sus propias vlan para cada uno de los 4 departamentos, después se siguió con hacer el encapsulamiento de las vlan en cada uno de los router.



La configuración de VLANs y el encapsulamiento en routers permite dividir una red física en varias redes lógicas, lo que aumenta la seguridad y el rendimiento. Cada departamento, como en este caso, tiene su propia VLAN (Virtual LAN), lo que significa que los dispositivos de cada VLAN pueden comunicarse entre sí directamente, pero no con dispositivos de otras VLAN sin la intervención de un router. Esto tiene varias ventajas:

1. **Segmentación de la Red**: Al asignar a cada departamento su propia VLAN (por ejemplo, VLAN 10 para un departamento, VLAN 20 para otro), estamos creando subredes separadas dentro del mismo switch. Esto mejora la seguridad, ya que cada VLAN actúa como una red independiente, limitando el acceso y tráfico entre departamentos.
2. **Optimización del Tráfico**: Las VLANs reducen la cantidad de tráfico de red innecesario. Por ejemplo, los mensajes de difusión (broadcasts) que envía un dispositivo en una VLAN solo alcanzarán a otros dispositivos en la misma VLAN, evitando que la red se congestione.
3. **Seguridad**: Al separar los departamentos en VLANs, limitamos el acceso de usuarios de una VLAN a otra. Esto significa que los empleados de un departamento solo pueden acceder a los recursos de su propia VLAN, a menos que haya una configuración específica que lo permita.
4. **Encapsulamiento y Comunicación entre VLANs (Router-on-a-Stick)**: Para que los dispositivos en diferentes VLANs puedan comunicarse, se utiliza un router con la técnica *router-on-a-stick*. Aquí, el router debe estar configurado para manejar varias VLANs mediante encapsulamiento 802.1Q, que permite al router reconocer el tráfico de cada VLAN y reenviar los paquetes al destino correcto.

Para cada switch debe hacerse lo mismo, asignar a cada puerto la vlan correspondiente.

Para esto se hace uso de los comandos:

```
Switch1(config)# interface FastEthernet0/2
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit
Switch1(config)# interface FastEthernet0/3
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit
```

Aquí estamos configurando el puerto `0/2` y 0/3 para que pertenezca a la **VLAN 10**. Si conectamos una computadora a este puerto, estará en la red de ese departamento y solo podrá comunicarse con otros dispositivos en la VLAN 10, a menos que el router esté configurado para permitir la comunicación entre VLANs.

Entonces debemos seguir el mismo camino para los demás puertos al 0/4 y 0/5 le correspondería la Vlan 20, al 0/6 y 0/7 la Vlan 30 y por último a los puertos 0/ y 0/9 la Vlan 40.

4. Routers Con sus respectivas ACL

Una ACL (Access Control List) o Lista de Control de Acceso es un conjunto de reglas en dispositivos de red, como routers o switches, que define qué tipo de tráfico puede pasar a través de una red. Las ACLs ayudan a gestionar y filtrar el tráfico de red,

permitiendo o denegando el acceso a determinados datos según criterios específicos.

Se implementaron Listas de Control de Acceso (ACL) en los routers de la red para permitir la comunicación únicamente entre computadoras de departamentos específicos, garantizando que solo los dispositivos pertenecientes a un mismo departamento puedan establecer conexiones entre sí a través de routers distintos. Esto se logró mediante la configuración de reglas de acceso que limitan el tráfico según las direcciones IP de origen y destino correspondientes a cada departamento.

Router 1:

Después de realizar nuestras reglas podemos revisarlas en el router, revisamos que se hayan aplicado con el siguiente comando:

show access-lists

```
Extended IP access list 100
    10 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
    20 permit ip 192.168.1.0 0.0.0.255 172.140.1.0 0.0.0.255
    30 permit ip 192.168.1.0 0.0.0.255 10.10.1.0 0.0.0.255
    40 permit ip 172.140.1.0 0.0.0.255 192.168.1.0 0.0.0.255
    50 permit ip 172.140.1.0 0.0.0.255 10.10.1.0 0.0.0.255
    60 permit ip 10.10.1.0 0.0.0.255 192.168.1.0 0.0.0.255
    70 permit ip 10.10.1.0 0.0.0.255 172.140.1.0 0.0.0.255
    80 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
    90 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
    100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
    110 deny ip any any
Extended IP access list 101
    10 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255
    20 permit ip 192.168.2.0 0.0.0.255 172.140.2.0 0.0.0.255
    30 permit ip 192.168.2.0 0.0.0.255 10.10.2.0 0.0.0.255
    40 permit ip 172.140.2.0 0.0.0.255 192.168.2.0 0.0.0.255
    50 permit ip 172.140.2.0 0.0.0.255 10.10.2.0 0.0.0.255
    60 permit ip 10.10.2.0 0.0.0.255 192.168.2.0 0.0.0.255
    70 permit ip 10.10.2.0 0.0.0.255 172.140.2.0 0.0.0.255
    80 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
    90 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Tomando como ejemplo las siguientes líneas explicamos que es lo que hacemos:
Línea 20: Permite tráfico de 192.168.2.0/24 a 172.140.2.0/24.

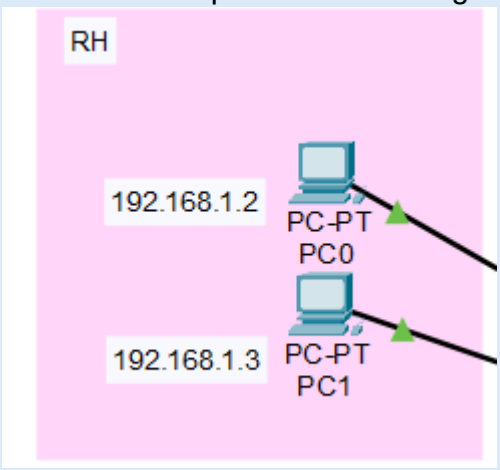
Línea 30: Permite tráfico de 192.168.2.0/24 a 10.10.2.0/24.

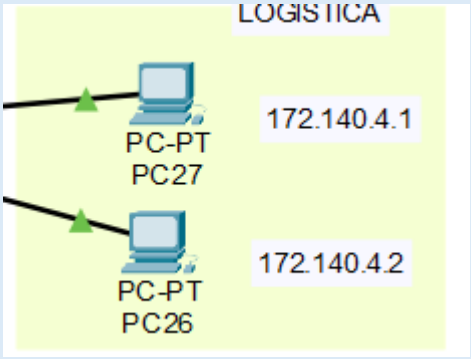
Línea 40: Permite tráfico de 172.140.2.0/24 a 192.168.2.0/24.

Permitimos que las computadoras que son del mismo departamento se puedan conectar entre sí, pero si son de departamentos diferentes se negara la conexión, esto aplicara para todos los departamentos, además las reglas las tiene cada router.

Ejemplo:
Si queremos conectar cualquiera de las siguientes computadoras del

departamento de RH con el departamento de logística del router 2:





Si realizamos ping desde la PC0 la cual es del router1 en el departamento de RH hacia la PC27 podremos observar en la siguiente imagen que esto no será posible

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.140.4.1

Pinging 172.140.4.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 172.140.4.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Conclusión

En este proyecto se logró diseñar y configurar exitosamente una red que conecta tres empresas automotrices con estrictas medidas de seguridad y segmentación de red. Utilizando VLANs, ruteo entre VLANs y listas de control de acceso (ACL), se implementó una infraestructura robusta que permite la comunicación controlada entre los departamentos equivalentes de cada empresa y limita el acceso entre departamentos distintos dentro de una misma organización. Esto asegura que cada departamento funcione como una red independiente, lo que optimiza el tráfico, mejora la seguridad y facilita la gestión de la red.

La asignación de rangos IP específicos y el uso de técnicas como "router-on-a-stick" permitieron crear un entorno segmentado y eficiente, donde el tráfico de cada departamento está confinado, reduciendo el riesgo de accesos no autorizados. Las ACLs configuradas en los routers refuerzan esta seguridad, permitiendo únicamente la comunicación entre los mismos departamentos de diferentes empresas. En conjunto, estos componentes aseguran un flujo de datos seguro y adecuado para la colaboración entre las empresas, cumpliendo con los objetivos de segmentación y control establecidos desde el inicio del proyecto.

Bibliografía

▷ *Configurar SWITCH CISCO ✔ Packet Tracer*. (s. f.). Solvetic. https://www.solvetic.com/tutoriales/article/3711-configuracion-basica-switch-cisco/

Configurar ACL de IP de uso general. (2024, 1 agosto). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html

Configuración de los parámetros de la dirección IP en un switch mediante la CLI. (2024, 1 enero). Cisco. https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-350-series-managed-switches/smb5557-configure-the-internet-protocol-ip-address-settings-on-a-swi.html