Date: 1st May 2023 Alumno

Word count: 2,999 Alvaro Gallardo

Prácica 4. "Proyecto Privado"

Contents

1 Análisis de problema

El parque de diversiones tiene una red de computadoras y dispositivos de comunicación que deben ser gestionados de forma independiente y segura. El parque de diversiones cuenta con los siguientes dispositivos en su red:

- Un servidor de correo electrónico y un servidor web que deben estar accesibles al público.
- Un sistema de puntos de venta para la venta de entradas, alimentos y souvenirs.
- Cámaras de seguridad distribuidas en todo el parque.

- Dispositivos para los empleados.

Para asegurar la eficiencia y seguridad de la red, es necesario dividirla en cuatro VLANs. Estas son:

- VLAN de invitados: Esta VLAN se utiliza para ofrecer acceso a Internet a los visitantes del parque. En esta red, el servidor web y el servidor de correo electrónico estarán disponibles para el público. Además, se debe configurar la red para restringir el acceso a otros recursos de la red, como el sistema de puntos de venta, las cámaras de seguridad y los dispositivos móviles de los empleados.
- VLAN de venta: Esta VLAN se utiliza para el sistema de puntos de venta. Aquí se puede manejar y controlar las transacciones de ventas del parque. Se puede limitar el acceso a esta red sólo a los empleados que trabajan en los puntos de venta, ya que el acceso a esta red es crítico para el funcionamiento del parque.
- VLAN de seguridad: Esta VLAN se utiliza para las cámaras de seguridad del parque. En esta red, las cámaras están conectadas a un sistema de grabación y monitoreo que sólo está disponible para el personal de seguridad y para aquellos que necesitan acceso a las grabaciones para investigar incidentes.
- VLAN de administración: Esta VLAN se utiliza para los dispositivos móviles de los empleados, como radios de comunicación y teléfonos móviles. En esta red, los empleados pueden comunicarse entre sí y acceder a los recursos de la red que necesitan para realizar su trabajo.

Con la creación de estas cuatro VLANs, se puede lograr una red más segura y eficiente para el parque de diversiones. Además, la segmentación de la red facilitará la gestión y el mantenimiento de la misma.

2 Comandos de seguridad básicos

```
1    enable
2    configure terminal
3    enable password ******
4    exit
```

3 Diseño de subredes

El alumno será capaz de identificar los diferentes protocolos de capa 3, analizando los comandos necesarios para activarlos y modificarlos, siendo capaz de configurar los principales protocolos de esta capa.

4 Manejo de vlans

Host	VLAN	NOMBRE
60	20	Contabilidad
20	30	Sistemas
8	40	Ventas
5	10	Gerencias

Table 1: Tabla de Vlans

VTP (VLAN Trunking Protocol) es un protocolo de administración de VLAN que se utiliza en redes Cisco para simplificar la configuración y el mantenimiento de VLAN. VTP permite a los switches de la red compartir información sobre las VLAN, incluyendo su nombre, ID y parámetros de configuración.

En Cisco Packet Tracer, puedes configurar VTP en los switches de la red utilizando la interfaz de línea de comandos (CLI) del switch. Aquí hay algunos comandos básicos de VTP en Cisco Packet Tracer:

```

switch(config)# vlan 10
switch(config-vlan)# name gerencia
switch(config-vlan)# exit
```

vtp

```
switch(config)# vtp mode server
switch(config)# vtp domian central
switch(config)# vtp password ***
```

4.1 Manejo de troncales

1. Identificar los protocolos de capa 3.
2. Identificar los comandos básicos para la configuración de redes internas.
3. Configurar la interconexión de redes

5 Materiales

- Packet tracer
- 3 Router ISR 4331
- 3 PC

6 Procedimiento y Configuración

6.1 Topología

Para está práctica, se creará la topología expuesta en la imagen .

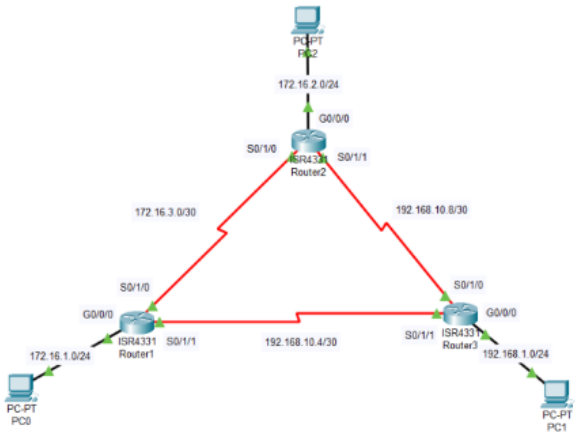

Figure 1: Topología L3

6.2 Conexión de dispositivos

- Router-Router = conexión serial
- Router-PC = conexión straight through

6.3 Configuración

6.3.1 Crea un proceso de EIGRP entre el R1 y el R3

Para poder realizarlo se emplean los siguiente: Entrar al CLI del router 1

```
1
2  conf t
3  router eigrp 22                    //22 es el nombre
4  do sh ip int br                   //ver interfaces
5  network 192.168.10.4
6  network 172.16.1.0.0.0.0.3    //30 en tabla es 0.0.0.3
7  eigrp router-id 1.1.1.1       // por se router 1
8  passive-interface default     // se despasivan
9  no passive-interface g0//0/0
10 no passive-interface s0//1/1
```

Ahora se debe trabajar con el router 3, para ello se recomienda emplear los siguientes comandos:

```
en
show ip int br
router eigrp 22
network 192.168.10.4
```

Router 1

```
do sh ip eigrp nei      //mostrar vecino
do sh ip prot           //ver informacion
```

Con lo anterior se crea una adyacencia

Router 3

```
network 192.168.1.0    //Usar red Gigabit 0
```

Router 1

```
do sh ip route         // Comprobar ciendo por cual
                              // serial esta trabajando
                       // la red 192.168.1.0
```

Posteriormente se debe ingresar al PC 0 y PC1 y hacer ping. Nota: Quizás tarda en responder.

```
ping 192.168.1.2
```

6.3.2 Crea un proceso de OSPF entre el R1 y R2

Se debe ir al router 1 e ingresar los siguientes comandos en la terminal:

```
router ospf 5
router-id 11.11.11.11 //11 para que sea diferente de 1
do sh ip int br
network 172.16.3.0    // Es izquierda en diagrama
network 172.16.3.0 0.0.0.3 area 0
network 172.16.1.0 0.0.0.255 area 0 // 255 por tabla
do sh ip prot         // verificar que corran OSPF y
                       // EIGRP
passive-interface default
no passive-interfacfe serial 0/1/0
```

```
no passive-interface gigabitEthernet 0/0/0
```

Router 2

```
en
sh ip int br
router ospf 5 //mismo n que el router 1
network 172.16.3.0  0.0.0.3 area 0
network 172.16.2.0 0.0.0.255 area 0 //poner vecino
do sh ip route
passive-interface default
no passive-interface serial 0/1/0   //la que se ocupa
mo passive-interface gigabitEthernet 0/0/0
```

6.3.3 Crea un gateway router para poder comunicar a todos los dispositivos

Entrar a Router 3 debido a que tiene el OSPF Y EIGRP

```

en
conf t
ip route 0.0.0.0  0.0.0.0 192.168.10.5 // Conexion
do sh ip route  // Gateway of
exit
ip route 0.0.0.0 0.0.0.0 172.16.3.1  //RUTA Estatica
do sh ip route
```

Nota: Se debe ir a la PC2 y poner poner de forma manual IP 172.16.2.2 y en la Subnet 255.55.0.0

Hacer Ping en la PC2

```
ping  172.16.1.2
```

6.3.4 Genera las redes estáticas necesarias para comunicar a todos los dispositivos si algún enlace serial falla

En el router 1 se debe emplear lo siguiente:

```

 enable
 configure terminal
 interface Ethernet 0/0
```

```
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 interface Serial 0/0/0
 ip address 10.0.0.1 255.255.255.0
 clock rate 64000
 no shutdown
interface Serial 0/0/1
ip address 10.0.1.1 255.255.255.0
clock rate 64000
no shutdown
```

En el router 2 se debe emplear lo siguiente:

```
enable
configure terminal
 interface Serial 0/0/0
 ip address 10.0.0.2 255.255.255.0
 clock rate 64000
 no shutdown
interface Serial 0/0/1
ip address 10.0.2.1 255.255.255.0
 clock rate 64000
 no shutdown
```

En el router 3 se debe emplear:

```
enable
configure terminal
interface Serial 0/0/0
ip address 10.0.1.2 255.255.255.0
 clock rate 64000
 no shutdown
 interface Serial 0/0/1
 ip address 10.0.2.2 255.255.255.0
 clock rate 64000
 no shutdown
```

Configurar las rutas estáticas.

Router 1

```
 enable
```

```
configure terminal
 ip route 10.0.0.0 255.255.255.0 10.0.0.2
 ip route 10.0.1.0 255.255.255.0 10.0.1.2
```

Router 2

```
 enable
configure terminal
 ip route 10.0.1.0 255.255.255.0 10.0.2.2
 ip route 10.0.1.0 255.255.255.0 10.0.1.2
```

Router 3

```
 enable
configure terminal
 ip route 10.0.0.0 255.255.255.0 10.0.1.1
 ip route 192.168.1.0 255.255.255.0 10.0.2.1
```

Simular una falla en un enlace serial.

En la pestaña "Físico" en el menú de la izquierda, hacer clic en el enlace serial que se desea desconectar. En la sección de "Estado de enlace", hacer clic en "Desconectar".

NOTA:

Si ya tienes OSPF configurado en la red, entonces no es necesario configurar rutas estáticas adicionales, ya que OSPF se encarga de calcular y distribuir las rutas automáticamente. OSPF es un protocolo de enrutamiento dinámico que permite que los routers intercambien información de enrutamiento y calculen las mejores rutas en función de la topología de la red.

Por lo tanto, en lugar de configurar rutas estáticas, puedes verificar la configuración de OSPF en cada router para asegurarte de que se esté ejecutando correctamente y que los routers estén intercambiando información de enrutamiento. Aquí te proporciono algunos comandos útiles para verificar la configuración de OSPF en cada router:

Para verificar la configuración de OSPF en un router:

```
 enable
show running-config | section router ospf
```

Para verificar las rutas aprendidas a través de OSPF en un router:

```
 enable
show ip route ospf
```

7 Conclusión

A manera de conclusión se puede decir que los requerimientos solicitados para el proyecto fueron alcanzados. Por otro lado gracias al mismo proyecto se pudo alcanzar un mejor entendimiento de los temas estudiados a lo largo del curso y se pudo entender la importancia de la interconexión de redes en el mundo actual.

8 Referencias

Cisco CCNA Routing and Switching 200-125 Official Cert Guide Library.

Cisco Networking All-in-One For Dummies.