Packet Tracer: desafío de integración de habilidades

Topología

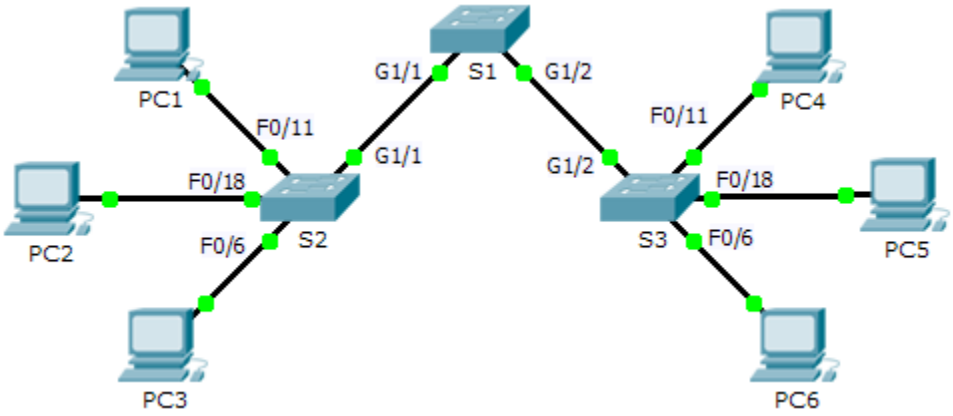

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 88	172.31.88.2	255.255.255.0	172.31.88.1
S2	VLAN 88	172.31.88.3	255.255.255.0	172.31.88.1
S3	VLAN 88	172.31.88.4	255.255.255.0	172.31.88.1
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.1
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.1
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.1
PC4	NIC	172.31.10.24	255.255.255.0	172.31.10.1
PC5	NIC	172.31.20.25	255.255.255.0	172.31.20.1
PC6	NIC	172.31.30.26	255.255.255.0	172.31.30.1

Tabla de asignación de VLAN y de puertos

Puertos	Asignaciones	Red
F0/7-12	VLAN 10: Ventas	172.31.10.0/24
F0/13-20	VLAN 20: Producción	172.31.20.0/24
F0/1-6	VLAN 30: Marketing	172.31.30.0/24
Interfaz VLAN 88	VLAN 88: Administración	172.31.88.0/24
Enlaces troncales	VLAN 99: Nativa	N/A

Situación

En esta actividad, hay dos switches completamente configurados. Usted es responsable de asignar el direccionamiento IP a una interfaz virtual de switch, configurar las VLAN, asignar las VLAN a las interfaces, configurar enlaces troncales e implementar medidas de seguridad básicas en un tercer switch.

Requisitos

El **S1** y **S2** están totalmente configurados. No puede acceder a esos switches. Usted es responsable de configurar el **S3** con los siguientes requisitos:

- Configure el direccionamiento IP y el gateway predeterminado según la **tabla de direccionamiento**.
- Cree, nombre y asigne las VLAN según la **tabla de asignación de VLAN y de puertos**.
- Asigne la VLAN 99 nativa al puerto de enlace troncal y deshabilite DTP.
- Restrinja el enlace troncal para que solo permita las VLAN 10, 20, 30, 88 y 99.
- Utilice la VLAN 99 como VLAN nativa en los puertos de enlace troncal.
- Configure la seguridad básica del switch en el S1.
  - Utilice la contraseña secreta cifrada **itsasecret.**
  - Utilice la contraseña de consola **letmein.**
  - Utilice la contraseña de VTY **c1$c0** (donde 0 es el número cero).
  - Cifre las contraseñas de texto no cifrado.
  - El mensaje MOTD debe tener el texto **Authorized Access Only!!** (¡Acceso autorizado únicamente!).
  - Deshabilitar los puertos que no se utilicen.
- Configure la seguridad de puertos en **F0/6**.
  - Solo dos dispositivos únicos tienen permitido acceder el puerto.
  - Las MAC detectadas se agregan a la configuración en ejecución.
  - Proteja la interfaz de manera que se envíe una notificación cuando se produzca una infracción, pero que el puerto no se deshabilite.
- Verifique que las computadoras en la misma VLAN ahora puedan hacer ping entre sí.