

Tarea 1: Preparar la Red

Paso 1: Cablee una red de manera similar al diagrama de topología

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando este tenga las interfaces necesarias que se muestran en la topología. El resultado que se muestra en esta práctica está basado en los switches 2960. El uso de cualquier otro tipo de switch puede producir resultados distintos.

Observe en la tabla de direccionamiento que las PCs se han configurado con una dirección IP predeterminada de Gateway. Esta sería la dirección Ip del router local que no se incluye en este escenario de práctica de laboratorio. El Gateway predeterminado, el router sería necesario para las Pc en diferentes VLAN para poder comunicarse.

Paso 2: Borre toda configuración existente en los Switches

Utilice el comando show vlan para verificar que solo exista VLAN predeterminada y que todos los puertos se asignen a la VLAN 1.

Paso 3: Deshabilitar todos los puertos con el comando shutdown

Repita esos comandos para cada switch de la topología

Tarea 2: Realizar las configuraciones básicas del switch

Paso 1: Complete la configuración básica de los switches S1, S2 y S3

Configure las switches S1, S2 y S3 según las siguientes pautas y guarde todas sus configuraciones:

- Configura el nombre del host del switch segú8n lo indicado en la topología
- Deshabilite la búsqueda DNS
- Configura una contraseña en modo EXEC: class
- Configure la contraseña cisco para las conexiones de consola
- Configure la contraseña cisco para las conexiones de vty

Paso 2: Vuelva a Habilitar los puertos de usuario en S2 y S3

Configure los puertos de usuario en modo de acceso. Consulte el diagrama de topología para determinar cuáles puertos están conectados a dispositivos de usuario final.

Paso 3: Rehabilitar los puertos troncales en S1, S2 y S3

Tarea 3: Configurar las interfaces Ethernet en las PC host

Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP y las Gateway predeterminadas indicadas en la tabla de direccionamiento.

Verifique que la PC1 pueda hacer ping a PC4; que la PC2 pueda hacer ping a PC5 y que la PC3 pueda hacer ping a PC6

Tarea 4: Configurar VTP en los switches

VTP permite al administrador de redes controlar las instancias de las VLAN en la red creando dominios VTP. Dentro de cada dominio VTP se configura uno o más switches con servidores VTP. Las VLAN se crean en el servidor VTP y se informan de otros switches en el dominio. Las tareas comunes de configuración VTP son las configuraciones de modo operativo, del dominio y de la contraseña. En esta práctica de laboratorio se utilizará S1 como el servidor VTP, con S2 y S3 configurados como clientes VTP o en el modo transparente de VTP.

Paso 1: Verifica las configuraciones VTP actuales en los tres switches

Observe que los tres switches se encuentran en modo servidor. El modo servidor es el modo de VTP predeterminado para la mayoría de los switches Catalyst.

Paso 2: Configure el modo operativo, el nombre de dominio y la contraseña de VTP en los tres switches

Establezca Lab4 como nombre de dominio VTP y cisco como contraseña de VTP en los tres switches.

Configure S1 en modo servidor, S2 en modo cliente y S3 en modo transparente.

Paso 3: Configure los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en los tres switches

Simplifique esta tarea con el comando interface range en el modo de configuración global.

Paso 4: Configure la seguridad del puerto en los switches de la capa de acceso S2 y S3.

Configure los puertos fa0/6, fa0/11 y fa0/18 de tal modo que solo permitan un solo host y aprendan la dirección MAC del host de manera dinámica

Paso 5: Configure las VLAN en el servidor VTP.

Hay cuatro VLAN adicionales que se requieren, configúrelas en el servidor VTP.

Verifique que se hayan creado las VLAN en S1 con el comando show vlan brief.

Paso 6: Verifique que las VLAN creadas en S1 se hayan distribuido a S2 y S3.

Utilice el comando show vlan brief en S2 y S3 para determinar si el servidor VTP ha enviado su configuración VLAN a todos los switches.

¿Están configuradas las mismas VLAN en todos los switches? _____ No _____

Explique porque S2 y S3 tienen diferentes configuraciones de VLAN en este momento:

Por la diferencia en el modo VTP

Paso 7: Cree una nueva VLAN en switches 2 y 3.

¿Por qué no se le permite crear una nueva VLAN en S2 pero si en S3?

Porque S2 está en modo cliente y S3 en modo transparente

Borre la VLAN 88 de S3-

Paso 8: Configure las VLAN en forma manual.

Configure las cuatro VLAN identificadas en el paso 5 en el switch S3.

Aquí se aprecia una de las ventajas del VTP. La configuración manual es tediosa y puede suscitar errores y cualquier error introducido aquí puede evitar la comunicación entre VLAN. Además, pude resultar difícil diagnosticar este tipo de errores.

Paso 9: Configure la dirección de la interfaz de administración de los 3 switches.

Verifique que todos los switches estén correctamente conectados configurando haciendo ping entre ellos. Desde S1, haga ping a la interfaz de administración en S2 y S3. Desde S2, haga ping a la interfaz de administración en S3.

¿Los ping son exitosos? Sí

En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.

Paso 10: Asigne puertos de switch a las VLAN.

Consulte la tabla de asignación de puertos al principio de la práctica para asignar puertos a las VLAN. Simplifique esta tarea con el comando interface range. Las asignaciones de puerto deben ser configuradas en cada switch manualmente o dinámicamente con un servidor VMPS. Los comandos se muestran para S3 solamente, pero los switches S2 y S1 deben ser configurados de manera similar. Cuando termine, guarde la configuración.

Tarea 5: Configurar la depuración VTP en los switches.

La depuración VTP permite a un servidor VTP suprimir tráfico de broadcast IP para VLAN específicas a switches que no tienen ningún puerto a esa VLAN. De manera predeterminada, todos los multicasts y broadcasts en una VLAN se saturan en toda la VLAN. Todos los switches en la red reciben todos los broadcast, incluso en situaciones en las que unos pocos usuarios están conectados a esa VLAN. La depuración del VTP se utiliza para eliminar o depurar este tráfico

innecesario. La depuración ahorra banda de ancha LAN porque los broadcast no tienen que ser enviados a los switches que no lo necesitan.

La depuración se configura en el Switch del servidor mediante el comando vtp pruning en modo de configuración global, la configuración se envía a los switches del cliente,

Confirme la depuración VTP en cada switch con el comando show vtp status. El modo de depuración VTP debe estar activado en cada switch.

Tarea 6: Limpieza.

Borre todas las configuraciones y vuelva a cargar los switches.