

Configuración de VLAN y asignaciones de puertos

Número de VLAN	Dirección de red	Nombre de la VLAN	Asignaciones de puertos
10	10.1.10.0/24	Admin	Fa0/6
20	10.1.20.0/24	Ventas	Fa0/11
30	10.1.30.0/24	Producción	Fa0/16
99	10.1.99.0/24	Mgmt&Native	Fa0/1-4
999	No aplicable	BlackHole	Puertos no utilizados

Situación

En esta actividad integral de habilidades de CCNA, la empresa XYZ usa una combinación de Frame Relay y PPP para las conexiones WAN. Otras tecnologías incluyen NAT, DHCP, el routing estático y predeterminado, EIGRP para IPv4, el routing entre VLAN y la configuración de VLAN. Las configuraciones de seguridad incluyen SSH, seguridad de puertos, seguridad de switches y ACL.

Requisitos

Nota: la contraseña de EXEC del usuario es **cisco** y la contraseña de EXEC privilegiado es **class**.

SSH

- Configure **HQ** para usar acceso remoto mediante SSH.
 - Establezca el módulo en **2048**. El nombre de dominio es **CCNASkills.com**.
 - El nombre de usuario es **admin** y la contraseña es **adminonly**.
 - Solo se debería permitir SSH en las líneas VTY.
 - Modifique los valores predeterminados de SSH: versión 2; tiempo de espera de 60 segundos; dos reintentos.

Frame Relay

- Configure Frame Relay entre **HQ** y **B1**.
 - Consulte la tabla de direccionamiento para obtener la dirección IP, la máscara de subred y el DLCI.
 - HQ** usa una subinterfaz punto a punto y un DLCI 41 para conectarse a **B1**.
 - El tipo de LMI se debe configurar manualmente como **q933a** para **HQ** y **B1**.

PPP

- Configure el enlace WAN de **HQ** a Internet mediante la encapsulación PPP y la autenticación CHAP.
 - Cree un usuario **ISP** con la contraseña **cisco**.
- Configure el enlace WAN de **HQ** a **NewB** (NuevoB) mediante la encapsulación PPP y la autenticación PAP.
 - HQ** es el lado DCE del enlace. Elija la frecuencia de reloj.
 - Cree un usuario **NewB** con la contraseña **cisco**.

NAT

- Configure la NAT estática y dinámica en HQ.
 - Permita que todas las direcciones del espacio de direcciones 10.0.0.0/8 se traduzcan mediante una lista de acceso estándar con nombre **NAT**.
 - La compañía XYZ posee el espacio de direcciones 209.165.200.240/29. El conjunto, **HQ**, usa las direcciones .241 a .245 con una máscara /29.
 - El sitio web **WWW.pka** en 10.0.1.2 está registrado en el sistema DNS público en la dirección IP 209.165.200.246 y se debe poder acceder a él desde el **host externo**.

DHCP

- En **B1**, configure un pool de DHCP para la VLAN 20 de Ventas con los siguientes requisitos:
 - Excluya las primeras 10 direcciones IP en el rango.
 - El nombre del pool, que distinga mayúsculas de minúsculas, es **VLAN20**.
 - Incluya el servidor DNS conectado a la LAN de **HQ** como parte de la configuración DHCP.
- Configure la computadora **Ventas** para usar DHCP.

Enrutamiento estático y predeterminado

- Configure **HQ** con una ruta predeterminada a **Internet** y una ruta estática a la LAN de **NewB**. Use la interfaz de salida como argumento.

Routing EIGRP

- Configure y optimice **HQ** y **B1** con el routing EIGRP.
 - Use el sistema autónomo 100 y deshabilite la sumarización automática.
 - **HQ** debe anunciar el router estático y predeterminado a **B1**.
 - Deshabilite las actualizaciones de EIGRP en las interfaces adecuadas.
 - Resume manualmente las rutas EIGRP de modo que el router **B1** solo anuncie el espacio de direcciones 10.1.0.0/16 a **HQ**.

Routing entre VLAN

- Configure **B1** para el routing entre VLAN.
 - Mediante la tabla de direccionamiento para los routers de sucursal, configure y active la interfaz LAN para el routing entre VLAN. La VLAN 99 es la VLAN nativa.

Configuraciones de VLAN y enlaces troncales

- Configure los enlaces troncales y las VLAN en **B1-S2**.
 - Cree y nombre las VLAN que se indican en la tabla de **Configuración de VLAN y asignaciones de puertos** solo en **B1-S2**.
 - Configure la interfaz y el gateway predeterminado de la VLAN 99.
 - Asigne las VLAN a los puertos de acceso adecuados.
 - Establezca el modo de enlace troncal en activado para Fa0/1 a Fa0/4.
 - Deshabilite todos los puertos sin utilizar y asigne la VLAN **BlackHole**.

Seguridad del puerto

- Use la siguiente política para establecer la seguridad de puertos en los puertos de acceso de **B1-S2**:
 - Permita que se descubra una de las direcciones MAC en el puerto.

- Configure la primera dirección MAC descubierta para que se ajuste a la configuración.
- Configure el puerto para que se desconecte si se produce una violación de seguridad.

Política de lista de acceso

- Debido a que HQ se conecta a Internet, configure una ACL con nombre denominada **HQINBOUND**, en el siguiente orden:
 - Permita las solicitudes HTTP entrantes en el servidor de **WWW.pka**.
 - Permita solo las sesiones TCP establecidas desde Internet.
 - Permita solo las respuestas de ping entrantes desde Internet.
 - Bloquee explícitamente todos los demás accesos entrantes desde Internet.

Conectividad

- Verifique la plena conectividad de cada computadora a **WWW.pka** y a **www.cisco.pka**.