Packet Tracer: Desafío para la integración de aptitudes de CCNA

Topología

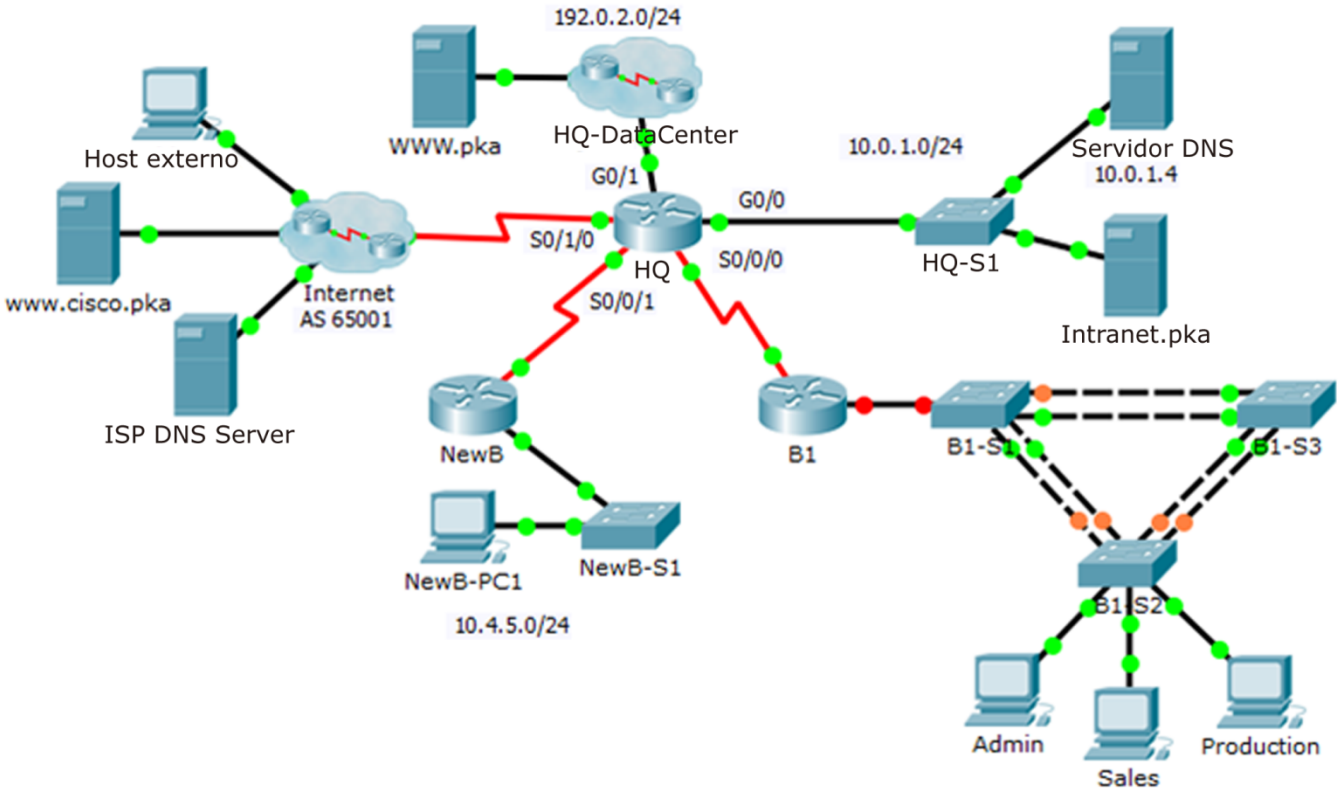

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
HQ	G0/0	10.0.1.1	255.255.255.0
	G0/1	192.0.2.1	255.255.255.0
	S0/0/0	10.255.255.1	255.255.255.252
	S0/0/1	10.255.255.253	255.255.255.252
	S0/1/0	209.165.201.1	255.255.255.252
B1	G0/0,10	10.1.10.1	255.255.255.0
	G0/0,20	10.1.20.1	255.255.255.0
	G0/0,30	10.1.30.1	255.255.255.0
	G0/0,99	10.1.99.1	255.255.255.0
	S0/0/0	10.255.255.2	255.255.255.252
B1-S2	VLAN 99	10.1.99.22	255.255.255.0

Configuraciones y asignaciones de puertos de VLAN

Número de VLAN	Dirección de red	Nombre de la VLAN	Asignaciones de puertos
10	10.1.10.0/24	Admin.	F0/6
20	10.1.20.0/24	Ventas	F0/11
30	10.1.30.0/24	Producción	F0/16
99	10.1.99.0/24	Gerencia_y_nativa	F0/1 a 4
999	N/D	BlackHole	Puertos no utilizados

Situación

En esta actividad para la integración de aptitudes de CCNA, la empresa XYZ usa una combinación de eBGP y PPP para las conexiones WAN. Otras tecnologías incluyen NAT, DHCP, routing estático y predeterminado, EIGRP para IPv4, routing entre VLAN y configuraciones de VLAN. Las configuraciones de seguridad incluyen SSH, seguridad de puertos, seguridad de switches y listas ACL.

Nota: Solo se puede acceder a **HQ**, **B1**, **B1-S2** y las PC. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiado es **class**.

Requisitos

PPP

- Configure el enlace WAN de **HQ** a Internet con encapsulamiento PPP y autenticación CHAP.
  - Cree un usuario **ISP** con la contraseña **cisco**.
- Configure el enlace WAN de **HQ** a **NewB** con encapsulamiento PPP y autenticación PAP.
  - Cree un usuario **NewB** con la contraseña **cisco**.

  Nota: Packet Tracer no califica **ppp pap sent-username**. Sin embargo, debe configurarse para que se produzca el enlace entre **HQ** y **NewB**.

eBGP

- Configure eBGP entre **HQ** e **Internet**.
  - HQ pertenece a AS 65000.
  - La dirección IP del router BGP en la nube de Internet es 209.165.201.2.
  - Anuncie la red 192.0.2.0/24 a Internet.

NAT

- Configurar NAT 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. Vincule la ACL **NAT** con el conjunto **HQ**. Configure PAT.
  - Las conexiones con **Internet** y **HQ-DataCenter** son externas a XYZ.

Routing entre redes 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.

Enrutamiento estático y predeterminado

- Configure **HQ** con una ruta estática a la LAN **NewB**. Use la interfaz de salida como argumento.
- Configure **B1** con una ruta predeterminada a **HQ**. Utilice la dirección IP del siguiente salto como argumento.

Routing EIGRP

- Configure y optimice **HQ** y **B1** con routing EIGRP.
  - Use el sistema autónomo (AS) 100.
  - Deshabilite las actualizaciones de EIGRP en las interfaces adecuadas.

Configuraciones de VLAN y enlaces troncales

Nota: El registro en la consola está desactivado en **B1-S2** para que los mensajes de discrepancia de VLAN nativa no interrumpan sus configuraciones. Si prefiere ver los mensajes de la consola, introduzca el comando de configuración global **logging console**.

- Configure los enlaces troncales y redes 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.
  - Active el modo de enlace troncal para F0/1 - F0/4.
  - Asigne las VLAN a los puertos de acceso adecuados.
  - Deshabilite todos los puertos sin utilizar y asigne la VLAN **BlackHole**.

Seguridad de puertos

- Use la siguiente política para establecer la seguridad en los puertos de acceso de **B1-S2**.
  - Permita que se aprendan dos direcciones MAC en el puerto.
  - Configure las direcciones MAC aprendidas para que se agreguen a la configuración.
  - Configure el puerto para que envíe un mensaje si se produce una violación a la seguridad. El tráfico se permite desde las dos primeras direcciones MAC aprendidas.

SSH

- Configure **HQ** para que use SSH para el acceso remoto.
  - 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.

DHCP

- En **B1**, configure un conjunto 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 distingue mayúsculas de minúsculas, es **VLAN20**.
  - Incluya el servidor DNS conectado a la LAN de **HQ** como parte de la configuración DHCP.
- Configure la PC de **Ventas** para que use DHCP.

Política de listas de acceso

- Dado que HQ está conectado a Internet, configure y aplique una ACL con el nombre **HQINBOUND** en el siguiente orden:
  - Permita las actualizaciones de BGP entrantes (puerto TCP 179) de cualquier origen a cualquier destino.
  - Permita las solicitudes HTTP de cualquier origen a la red **HQ-DataCenter**.
  - 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 que la conectividad sea total desde cada PC a **WWW.pka** y **www.cisco.pka.**
- El host externo debe poder acceder a la página web en WWW.pka.
- Todas las pruebas de la situación 0 deberían producir resultados correctos.