Plan de Pruebas

PAT (NAT + sobrecarga) *Entre la red de HQ y la de REMOTE*

1. Mandar paquetes de HQ a la sede remota o viceversa.

2. Utilizando el comando *sh ip nat translations* en el router, observar que se han traducido las IPs privadas en públicas y viceversa.

3. Si no hace las traducciones revisar la configuración con *sh run*. Las interfaces nat in/out y el pool de direcciones para NAT.

OSPF multiárea + autenticación *En ambos routers*

1. Consultamos la routing table *sh ip route ospf* y revisamos las entradas *O IA*.

    1.1. En caso contrario, se revisa mediante sh run que se anuncian todas las redes conectadas al router.

2. Para verificar que está autenticada utilizamos el comando *sh ip ospf int s0/0/0* y localizamos *Neighbor Count is 1, Adjacent neighbor count is 1* y *Message digest authentication enabled Youngest key id is 1 .*

    2.1. En caso contrario, se revisa mediante sh run que la contraseña es la misma y que está activada.

3. Con el comando *debug ip ospf* visualizamos el movimiento de OSPF.

PPP + autenticación CHAP *Entre la red de HQ y la de REMOTE*

1. Consultamos la información de la interfaz emitiendo el comando *sh int s0/0/0*.

2. Revisamos que aparece *Encapsulation PPP, LCP Open* y *Open: IPCP, CDPCP, crc 16, loopback not set*.

3. Con el comando debug ip ppp visualizamos el movimiento de PPP.

RSTP En los switches de HQ

1. Emitimos el comando sh spanning-tree para visualizar el tipo de STP está habilitado y el estado de las interfaces.

2. En el caso de RSTP, debe aparecer *Spanning tree enabled protocol rstp*, su dirección física y las interfaces que participan en RSTP.

VTP En los switches de HQ

1. El comando *sh vtp status* muestra la versión de VTP, el número de revisión de la configuración, el modo de operación (server, client, transparent) y el nombre del dominio VTP.

2. El nombre del dominio, la contraseña, la versión y el número de revisión tiene que ser iguales en todos los switches.

3. Con el comando *debug sw-vlan vtp events* activado se muestran los eventos de VTP. Desde el switch que sea el servior VTP se crea una nueva VLAN, y los demás switches reciben el mensaje de VTP, pero solo crearán una nueva VLAN si está en modo cliente y no transparente.

ACLs extendidas La VLAN 30 sólo puede navegar por Internet

1. Mediante el Navegador web nos dirigimos a la ip del servidor web y comprobamos que carga la página web.

2. Si nos movemos a la terminal y emitimos ping <dirección IP>, nos dará respuesta de host unreachable ya que los packetes de ping son ICMP y no HTTP.

3. Emitiendo el comando *show access-list* nos muestra el número de veces que se ha aplicado el ACL (X matches)

SNMP Router HQ y PC Admin

1. Suponiendo que el router tiene SNMP configurado y los traps activados...

2. Desde un gestor de SNMP como PowerSNMP instalado, con la herramienta de búsqueda de agentes (broadcast) observamos que aparece la ip del router en el listado de agentes encontrados.