Ejercicio integral que incluye los temas de VLSM, VLANs, DHCP y NAT estático, NAT dinámico (también conocido como PAT).

Descargar archivos. Archivo en packet tracer, configuración básica

Realizaremos un caso de co-working. Leer caso. Referencias relacionadas con el tema de co-working.

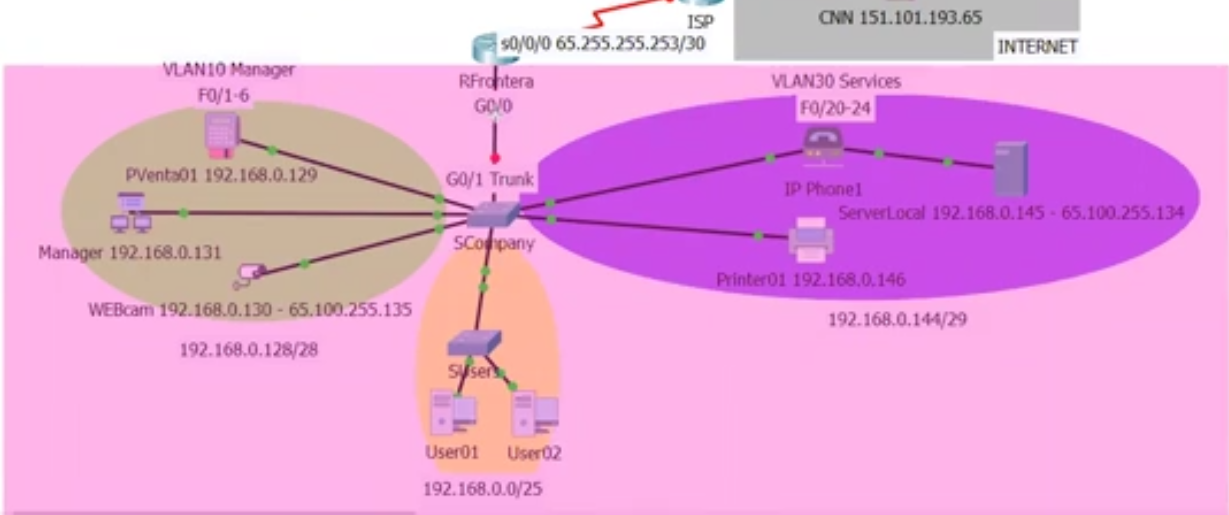
Debemos realizar el diseño con base en restricciones que han sido establecidas por el cliente.

1. Debemos utilizar **VLSM**. Ya está incluido en los tres segmentos de mis VLANs (10, 20 y 30) ya tienen su propio esquema de direccionamiento IP privado y ya construido en el propio diagrama.
2. La IP pública para conectarnos al **ISP** es **65.255.255.253/30**
3. Debemos utilizar tres **VLANS** (Manager, Users, Services) (Administrador, Usuarios y Servicios)
4. Solo el grupo de **Users** obtiene dirección IP dinámica (**DHCP**)
5. Debemos conectar la red local a los servicios de Internet, por lo que utilizaremos el siguiente bloque de IPs públicas **65.100.255.128 / 29 Son 8 direcciones IP públicas para poder salir al exterior.**
6. Por lo limitado de las IPs públicas debemos utilizar el protocolo **PAT (NAT overload)**.
7. **Servidor** y **Cámara WEB** tienen NAT estático. Las **IP públicas** para estos servicios ya han sido seleccionadas.
8. Realizar las pruebas de conectividad necesarias.

Vamos a tener una configuración básica y parciales para los equipos.

Vamos a explicar como se hace la traducción de direcciones privada a públicas.

**Todas las interfaces de nuestra red local** deben tener la acción de trabajo **inside.**

****

**La única interface con la acción outside es la del s0/0/0. Las interfases outside son todas aquellas que participan en la traducción de direccionamiento privado a público y viceversa.**

Adicionalmente para realizar la traducción en el caso de un NAT estático o un NAT de tipo público, necesitamos utilizar al menos una IP pública.

**El protocolo de nateo recibe un grupo de direcciones IPs privadas para poder ser traducidas con un conjunto de direcciones IPs limitadas públicas.**

**Hay 4 formas de instalar el servicio de NAT:**

1. **NAT puro. Una traducción de por cada dirección IP privada se traduce a una dirección pública.** Lo que consume muchas direcciones IPs públicas.
2. **NAT dinámico (PAT). Muchas direcciones IP internas privadas se traducen a pocas direcciones IP públicas.** Se utiliza la combinación de direccionamiento IP capa 3 y el puerto capa 4.
3. **NAT estático. Se requiere una dirección IP pública por una dirección IP privada.**
4. **Port forwarding,** con el uso de una única dirección IP pública, la traducción y forwardeo aunque tengamos necesidad de establecer NATeo estático.

**Instalar el servicio de DHCP.**

Tenemos tres subredes asociadas con las VLANs (10, 20 y 30).

La subred de los usuarios es a la que se le asignarán direcciones IP dinámicas.

DHCP solamente dará servicio a la subred de usuarios, que corresponde con la VLAN 20. Hay que configurar primero las excepciones que se pueden tener.

**! DHCP Exceptions**

**ip dhcp excluded-address <DirIP o Rango\_Dirs\_IP>**

Excluir la IP de la subinterface de la VLAN 20.

**ip dhcp excluded-address 192.168.0.126**

Instalar el servicio de DHCP en el router frontera como un servicio centralizado. Ahí estará también el servicio de NAT.

**! DHCP Pool**

**ip dhcp pool Users** El pool debe recibir un nombre (ip dhcp pool son palabras reservada)

**network 192.168.0.0 255.255.255.128** Va a asignar la IPs disponibles de ese bloque o de esa subred. (128 direcciones – 2 -1 gateway ) 125 ips para asignar.

**default-router 192.168.0.126**

**Si la PC de User02 solicita una IP, la subinterface g0/0.20 es la que estará respondiendo a esta petición.**

**Revisar configuración mínima de DHCP**

**Configuración de las VLANs**

**Los puertos del switch han sido divididos se la siguiente forma:**

* F0/1-6 VLAN 10 administración
* F0/7-19 VLAN 20 Usuarios
* F0/20-24 VLAN 30 Servicios

**VLANs son redes virtuales para poder segmentar el tráfico y tener distintos dominios de broadcast en una misma interface es el uso de las subinterfaces en los routers.**

El definir subinterfaces en los routers implica que la interface g0/0 recibir peticiones de la vlan 10 , vlan 20 y vlan 30. El router realiza la selección, en este caso decisiones de ruteo internos sin definir ningún protocolo de ruteo adicional (router on stick, propiedades de router on stick)

**Las subinterfaces se definen con la interface g0/0 y se le concatena la subinteface asociada con la vlan g0/0.10.** **El protocolo de encapsulamiento debe incluir el id de la vlan.**

La dirección ip de la sub-interface va a ser la última dirección ip válida de la subred o bloque. Ip nat inside ya que es una traducción interna. La única interface outside es la que conecta con el ISP, la demás interfaces y subinterfaces se configuran inside ya que es una traducción interna (traducción inside).

**! Declaración de subinterfaces.**

**! Manager**

**int g0/0.10**

**encapsulation dot1Q 10**

**ip address 192.168.0.142 255.255.255.240**

**ip nat inside**

**! Users**

**int g0/0.20**

**encapsulation dot1Q 20 (el id de la VLAN)**

**ip address 192.168.0.126 255.255.255.128**

**ip nat inside**

**! Services**

**int g0/0.30**

**encapsulation dot1Q 30**

**ip address 192.168.0.150 255.255.255.248**

**ip nat inside**

Hay que levantar todas las subinterfaces, si alguna se olvida esa interfaz no se levanta, por eso existe la posibilidad de solamente **levantar la interface física g0/0**, las subinterfaces son lógicas. Si levanto la interfaz física se levantan todas sus subinterfaces.

**int g0/0**

**no shut**

**Ahora vamos a configurar las VLANs. Tenemos tres VLANs la 10, 20 y la 30.**

**Primero hay que realizar la creación de las bases de datos de las VLANS**

**! ====================**

**! ===== SCompany ======**

**! ====================**

**ena**

**conf t**

**hostname SCompany**

**1. Creación de la base de datos de las VLANs**

**vlan 10**

**name Manager (El nombre no es obligatorio, solo descriptivo)**

**exit**

**vlan 20**

**name Users**

**exit**

**vlan 30**

**name Services**

**exit**

**!vlan 1 que es la nativa, está creada siempre por default, no la vamos a configurar.**

! Solamente la configuraríamos si queremos acceder al switch por telnet, ping o ssh

**2. DEFINIMOS PARA CADA VLANs los puertos de acceso**

! Definición de los puertos de acceso y relación a que VLAN 10

1 al 6 para managers, del 7 al 19 para users y del 20 al 24 para Servicios

**int range f0/1-6**

**switchport mode access (Puertos de acceso que pertenecen a la vlan 10)**

**switchport access vlan 10**

**int range f0/7-19**

**switchport mode access (Puertos de acceso que pertenecen a la vlan 20)**

**switchport access vlan 20**

**int range f0/20-24**

**switchport mode access**

**switchport access vlan 30**

**Definición de puertos troncales trunk G0/1**

**int g0/1**

**switchport mode trunk**

**no shut**

**En este momento el switch ha sido segmentado tanto físicamente por los puertos, como lógicamente al momento de indicar que grupo de puertos corresponden a qué VLAN.**

1. Creo la base de datos
2. Asigno los puertos de switch a la vlan correspondientes.
3. Defino el puerto troncal g0/1, ya que por ahí va a salir el tráfico de las distintas VLANs. Hay varias VLANs que van a salir por el mismo puerto.

**El switch hacia debajo de SCompany, SUsers** solamente ha sido puesto como una extensión (7 al 19 son menos puertos) y si a cada puerto le conectamos un switch con 24 puertos tendríamos. Si del 7 al 19 hay 12 puertos disponibles (12 x 24 puertos disponibles para los dispositivos de los usuarios que se pueden conectar. Estamos haciendo un cascadeo, lo que permite que más usuarios se puedan conectar. **Es switch de SUsers es otro cliente que te permite extender el dominio de broadcast.**

**El switch SUsers es una extensión de dominio. Tenemos que configurar la VLAN 20. La VLAN 20 es la que va a utilizar Users.**

**Todos los puertos de este switch (1 – 24) pertenece a la misma VLAN.**

**! El switch SUsers ha sido puesto como una extensión**

**! Si del 7 al 19 hay 12 puertos disponibles, entonces puedo poner 12 x 24 voy a**

**! tener el número total de dispositivos a conectar. El switch SUsers es un cliente**

**! mas que te permite extender el dominio para que más usuarios se puedan**

**! conectar.**

**! SUsers es una extensión de la VLAN 20 y debe incluir en su base de datos como**

**! mínimo a que VLAN pertenece o se va a comunicar, no**

**! debe tener el resto de las VLANs, pero si con la que está participando**

**ena**

**conf t**

**hostname SUsers01**

**vlan 20**

**name Users**

**exit**

**! Users**

**int range f0/1-24**

**switchport mode access**

**switchport access vlan 20**

**Configuración de rutas por default:**

**Configurar la IP del s0/0/0**

**int s0/0/0**

**desc interfaz que conecta con el ISP**

**ip address 65.255.255.253 255.255.255.252**

**ip nat outside (por ahí van a salir todas las traducciones)**

**no shut**

**No necesito configurar un protocolo de ruteo, el ruteador está configurado para trabajar como router on stick, solamente debemos saber cómo el tráfico interno va a salir al exterior.**

**! Establecer una ruta por default que se encargue de sacar el tráfico a Internet.**

* Cuando definimos nuestra interface de salida (s0/0/0) tenemos una **ruta por default directamente conectada**
* Si utilizamos la dirección IP del siguiente router, tenemos una **ruta por default recursiva**
* Si concatenamos la interface de salida de nuestro router y la ip del siguiente router, tenemos una **ruta por default completamente conectada.**

**ip route 0.0.0.0 0.0.0.0 s0/0/0**

**Configuración de NAT**

Ahora hay que instalar el servicio del NAT. De forma genérica necesita de 4 pasos.

1. Definir un **pool de direcciones globales (públicas)** que serán asignadas cuando sean necesarias. **CREACIÓN DEL POOL CON UN NOMBRE, DONDE DEFINIREMOS LAS DIRECCIONES IP PÚBLICAS QUE SE UTILIZARÁN EN LA TRADUCCIÓN. Se requiere la dirección IP inicial y la dirección IP final con su máscara de subred.**

**ip nat pool** **Nombre** dirIP-inicial dirIP-final netmask **MáscaraSubneteo**

1. Definir una **ACL estándar**: **CREACIÓN DE UNA LISTA DE CONTROL DE ACCESO ESTÁNDAR DONDE SE INDICAN TODAS LAS DIRECCIONES QUE VAN A PODER PARTICIPAR EN ESA TRADUCCIÓN.**

**access-list Número** permit dirIP-inicial **WildMask\_ACL**

1. Establecer la **traducción dinámica de direcciones** utilizando la ACL definida.

**ip nat inside source** { **list** {**Número | Nombre**} **pool** **NOMBRE [overload] | static** IP-local IP-Global }

**ip nat inside source (palabras reservadas) y luego la asociación de una lista de control de acceso si realizamos nateo dinámico o nateo estático.**

1. Especificar las **interfaces interiores y exteriores.** El último de los comandos es definir la acción que se va a realizar en cada una de las interfaces cuando tengamos el servicio de NAT instalado, que puede ser inside para todas las interfaces internas de nuestra red local o outside para la interface que se conecta con el ISP (proveedor de servicios) exterior.

**interface Tipo-Número**

**ip nat inside**

**interface Tipo-Número**

**ip nat outside**

**Hay que identificar el pool de direcciones IP públicas a utilizar.**

**Pool IP Públicas 65.100.255.128 /29**

Tenemos dos restricciones a considerar importantes, **tenemos dos dispositivos que les vamos a asignar traducción de nateo estático:**

1. **El servidor Local que le fue asignada una dirección pública 165.100.255.134 para realizar la traducción de nateo estático**
2. **La cámara web también le vamos a asignar la dirección pública 65.100.255.135 para realizar la traducción de nateo estático.**

**Cuando el direccionamiento es público en el NAT todas las direcciones se pueden utilizar.**

65.100.255.128 255.255.255.248 256 – 248 = 8

.128 + 8 = 136

.128 a .135 Puedo utilizar desde la 128 hasta la 135.

**Desde la .128 hasta la .135** Es un grupo de direcciones IP , no es una subred lo que estamos recibiendo.

**Si el pool se puede utilizar en su totalidad (.135 es la última y .134 es la penúltima del bloque), por lo que tengo desde la 128 hasta la 133 para poder realizar el direccionamiento dinámico.**

**Comenzaremos con la traducción del nateo estático, que implica dos servicios una cámara web y un servidor. Para realizar un nateo estático la palabras reservadas:**

**ip nat inside source static <DIR IP PRIVADA> <DIR IP PÚBLICA>**

**Hay que establecer la IP privada y la IP pública.**

**! NAT estático (WEBcam y ServerLocal)**

**ip nat inside source static 192.168.0.130 65.100.255.135**

**ip nat inside source static 192.168.0.145 65.100.255.134**

**ESTE NATEO ESTÁTICO TRADUCE UNA DIRECCIÓN IP PÚBLICA POR UNA IP PRIVADA.**

**Del bloque .128, ya se utilizaron las dos últimas, pero tengo desde la .128 hasta la .133 para poder realizar el nateo dinámico, que es la siguiente acción a construir. Me quedan 6 direcciones para dar servicio a todas las posibles conexiones que puedan ocurrir.** NAT no es suficiente para traducir las IPs de nuestras VLANs. Tengo pocas direcciones IP públicas y muchas direcciones IP privadas que deseamos traducir. El servicio se traduce en la construcción del servicio de PAT, el NAT se convierte en un nateo dinámico que además utiliza el protocolo para poder realizar las traducciones. Y lo único que debemos de agregar es la palabra overload al final de mi diseño de mi NAT. **No existe un comando PAT, existe el comando NAT y para construir el servicio de PAT agregamos la palabra reservada overload y lo convertimos en un servicio PAT.**

**Definición del pool, requerimos una dirección IP inicial y una dirección IP final:**

**ip nat pool MyPool 65.100.255.128 65.100.255.133 netmask 255.255.255.248**

Puedo ponerle cualquier nombre a mi Pool, la máscara es completa de todo el bloque de direcciones, aunque me falten dos.

**El siguiente comando es definir quién puede acceder al servicio de nateo.** Todos los equipos que están conectados a cualquiera de las VLANs 10,20 o 30 tienen la posibilidad de poder salir al exterior. La lista de acceso tiene que ser estándar. Puedo utilizar una lista de acceso por número o por nombre. El número puede ser desde 1 hasta 99. La acción es permitir, se define la dirección de la subred o red.

**access-list 1 permit 192.168.0.0 0.0.0.255 Tengo todo el bloque de la clase C para poder llevar a cabo la traducción. También podemos utilizar la palabra any**

**access-list 1 permit any**

**! Declarar el NAT o PAT dinámico**

**ip nat inside source list 1 pool MyPool overload**

! si le quito el overload es NAT uno a uno

! si dejo overload es PAT muchas direcciones ip privadas, van a poder

! utilizar la misma dirección ip pública para salir al exterior.

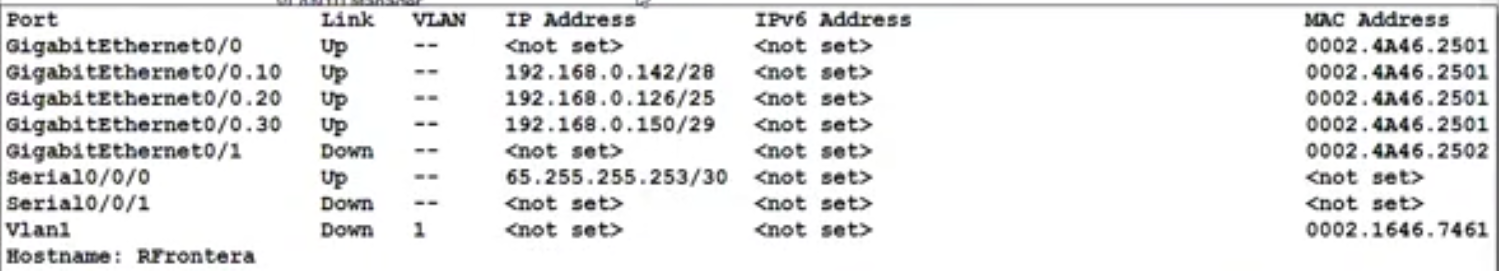
Ahora sí hay que copiar la configuración a cada equipo correspondiente.

1. Copiamos configuración de **SUsers01**
2. Después copiamos la configuración de **SCompany**
3. Copiamos configuración del router **RFrontera**

Checamos sino tenemos algún circunflejo.

Hay que esperar que las interfaces se pongan en verde.

**En el router frontera observo las subinterfaces que han sido creadas, número 10 managers, 20 users, 30 Servicios.**

****

En este momento podemos probar nuestras configuraciones.

* **Todos los equipos de la VLAN 10, ya tienen configurado su direccionamiento IP estático y su máscara de manera correcta**, como el servicio de la caja y el dispositivo al que se conecta el administrador.
* El **servidor de la VLAN 30**, ya también tiene su dirección IP.

Para probar que todo esté funcionando, tengo que realizar **pruebas de conectividad interna** primero.

* Checar conectividad de los usuario hacia la **vlan verde (10)** y
* De los usuarios hacia la **vlan morada (30)**

**Primero verifico que el servicio de DHCP** esté funcionando de forma correcta en los equipos de la VLAN (20). Activo y desactivo el servicio de DHCP. Me entrega la misma dirección, ya que no ha pasado su tiempo de arrendamiento o de gracia para liberar esa dirección. Y nos entrega exactamente la misma IP.

Vamos a realizar pruebas de conectividad interna:

* **USER 01** vamos a utilizar el direccionamiento interno o direccionamiento privado Acceso web a > **192.168.0.145 (Servidor de Services**)
* **USER 01** vamos a utilizar el direccionamiento interno o direccionamiento privado > Acceso web a **> 192.168.0.130 (Cámara web)**
* **USER 01** vamos a conectarnos al exterior con acceso web >**servidor CNN (151.101.193.65)**

1. Hemos probado **DHCP es funcional.**
2. Hemos probado el **servicio de NAT dinámico** puede salir utilizando el servicio OVERLOAD que es el servicio del PAT
3. Hemos probado la **interconexión entre las VLANs es funcional.**
4. **Lo único que nos falta probar es que desde el exterior nuestro servidor sea público**. Si yo accedo al servicio del CNN y que quiero acceder al servidor que tiene asignada una dirección pública de forma estática con la dirección **65.100.255.134** y estoy accediendo desde el Internet a este servidor.La otra de las direcciones será la **dirección pública de la cámara web (65.100.255.135)** Y desde el exterior estamos accediendo al dispositivo de la cámara web.

**Sh ip NAT translations** te permite ver las traducciones, comando que me permite ver las ips que están saliendo.

Se muestra el protocolo que se está utilizando, la dirección interna que lo está utilizando, el puerto dinámico que se generó, una dirección ip local interna (la dirección IP privada), una dirección ouside que es con quien me quiero comunicar. En este ejemplo no hay traducciones en el direccionamiento destino, el direccionamiento local coincide con el direccionamiento global o público.

**! ======== RFrontera ==========**

**ena**

**config t**

**hostname RFrontera**

**no ip domain-lookup**

**int s0/0/0**

**desc Interfaz que conecta con ISP**

**ip address 65.255.255.253 255.255.255.252**

**ip nat outside**

**no shut**

**int g0/0.10**

**description VLAN Manager**

**encapsulation dot1Q 10**

**ip address 192.168.0.142 255.255.255.240**

**ip nat inside**

**int g0/0.20**

**description VLAN Users**

**encapsulation dot1Q 20**

**ip address 192.168.0.126 255.255.255.128**

**ip nat inside**

**int g0/0.30**

**description VLAN Services**

**encapsulation dot1Q 30**

**ip address 192.168.0.150 255.255.255.248**

**ip nat inside**

**int g0/0**

**no shut**

**ip dhcp excluded-address 192.168.0.126**

**ip dhcp pool Users**

**network 192.168.0.0 255.255.255.128**

**default-router 192.168.0.126**

**ip nat inside source static 192.168.0.130 65.100.255.135**

**ip nat inside source static 192.168.0.145 65.100.255.134**

**ip nat pool MyPool 65.100.255.128 65.100.255.133 netmask 255.255.255.248**

**access-list 1 permit 192.168.0.0 0.0.0.255**

**ip nat inside source list 1 pool MyPool overload**

**ip route 0.0.0.0 0.0.0.0 s0/0/0**

**! ===== SCompany ======**

**ena**

**conf t**

**hostname SCompany**

**vlan 10**

**name Manager**

**exit**

**vlan 20**

**name Users**

**exit**

**vlan 30**

**name Services**

**exit**

**int range f0/1-6**

**switchport mode access**

**switchport access vlan 10**

**int range f0/7-19**

**switchport mode access**

**switchport access vlan 20**

**int range f0/20-24**

**switchport mode access**

**switchport access vlan 30**

**int g0/1**

**switchport mode trunk**

**no shut**

**! ====== SUsers =======**

**ena**

**conf t**

**hostname SUsers**

**vlan 20**

**name Users**

**int range f0/1-24**

**switchport mode access**

**switchport access vlan 20**