Se realizará un **ejercicio integral**, que integra los temas de **VLSM**, **DHCP**, **NAT** y **PAT**.

Lee de Power Point oportunidad de negocio.

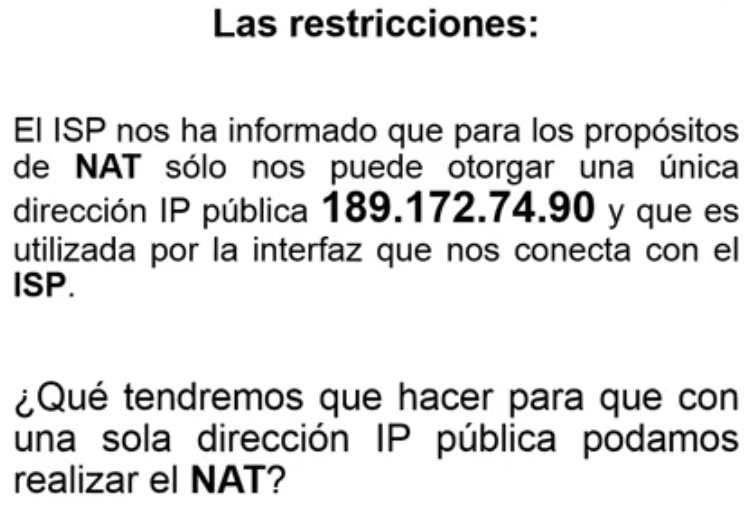
Revisar tabla de VLANs.

* Las subinterfaces de las VLANs van a utilizar la **última IP válida** de la subred, para la puerta de enlace predeterminada.
* En la tabla viene el **ID** de la VLAN y los puertos que le corresponden a cada vlan.

Solamente vamos a utilizar una IP pública, podremos instalar servidores, cámaras, impresoras, etc…, la respuesta es si, accesibles desde el exterior.

Vamos a configurar PAT

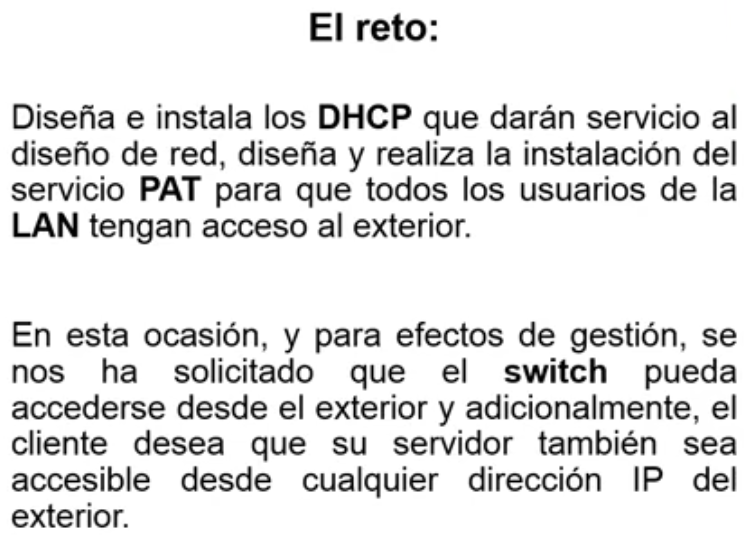
El término genérico es NAT, nosotros lo que vamos a implementar es una versión del NAT que se llama PAT. NAT es el nombre completo real para el protocolo de traducción de direcciones.



Revisar video. En el video se habla del protocolo NAT y de sus distintas versiones. Vamos a realizar un breve resumen de estas versiones.

* **NAT estático.** Se recomienda realizar traducciones de forma estática cuando tenemos servidores que queremos que puedan ser contactados desde el exterior.
* **NAT dinámico.** El nateo dinámico depende de varios elementos, entre ellos un pool de direcciones.

1. **NAT dinámico puro:** Cuando requerimos la traducción del mismo número de IPs públicas y de IP privadas, en una relación uno a uno se le conoce como NAT.
2. **PAT:** Cuando requerimos la traducción de muchas direcciones IPs internas privadas a unas cuantas direcciones IP públicas la versión de esta implementación del NAT se le conoce como PAT, que lo que traducen son protocolos. Al final de la configuración se debe colocar la palabra reservada overload.
3. **Port forwarding:** Se utiliza cuando tenemos una única dirección IP pública para traducir muchas IP privadas, incluyendo direcciones estáticas como los servidores, impresoras, etc.



**Por lo tanto el switch y el servidor requerirán NAT estático.**

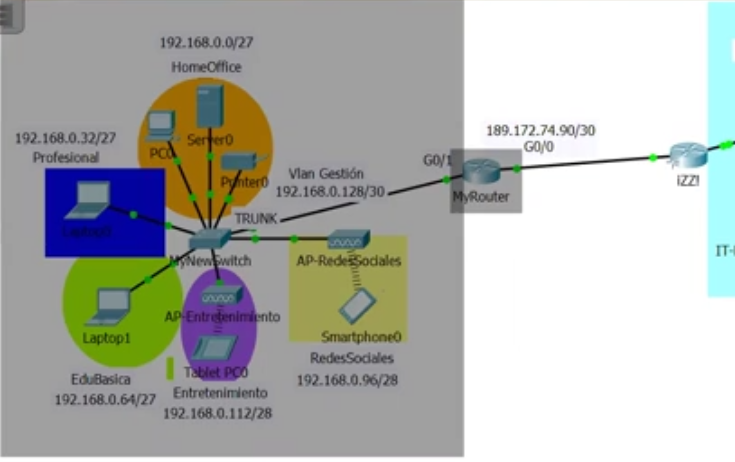
**Red local y el router a configurar.**

VLAN 10 de HomeOffice, VLAN 20 de Profesional, VLAN 30 de Educación básica, VLAN 40 Redes sociales y VLAN 50 de entretenimiento.

La última dirección ip disponible del bloque o subred le corresponderá a la subinterface asociada con esa VLAN.

Descargar archivos y se comenzará con configuración de estos elementos. El dominio local de la red es todo lo que se encuentra en gris. Esa es nuestra red de cobertura local.

**My router** hay que revisar la configuración establecida y configurada. En el switch **MyNewSwitch** hay que revisar configuraciones. **ISP ya está configurado.**



**Revisar switch**

El switch ya se encuentra configurado. (checar las vlans configuradas)

MyNewSwitch#**sh vlan**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/22, Fa0/23, Fa0/24, Gig0/2

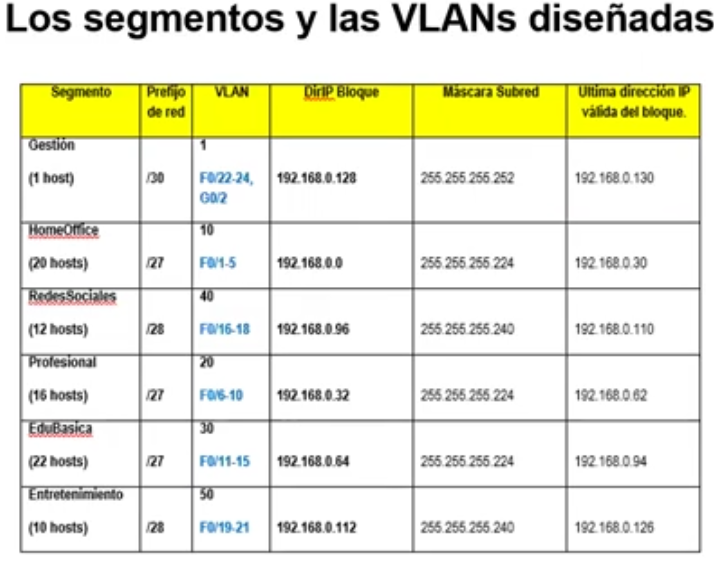
10 HomeOffice active Fa0/1, Fa0/2, Fa0/3, Fa0/4,Fa0/5

20 Profesional active Fa0/6, Fa0/7, Fa0/8, Fa0/9,Fa0/10

30 EduBasica active Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15

40 RedesSociales active Fa0/16, Fa0/17, Fa0/18

50 Entretenimiento active Fa0/19, Fa0/20, Fa0/21



Las primeras 1000 VLANs son las que nos pueden dar servicio.

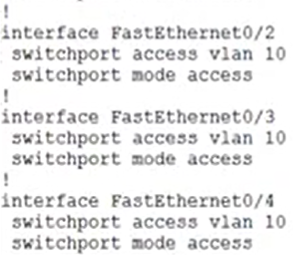
La VLAN 1 no tiene nombre (configurada como default), es la VLAN nativa y tiene asignados los puertos 22 – 24 y el g0/2. Si nos conectamos a estos puertos estaremos entrando a la VLAN 1.

Los puertos corresponden con la información proporcionada en un inicio.

**Checamos la configuración del switch**

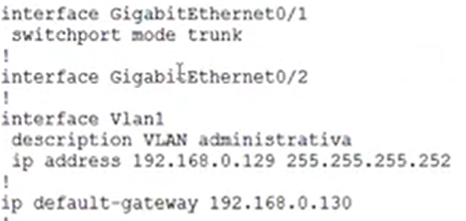
**Sh run**

Podemos ver los puertos que han sido asociados a cada VLAN.

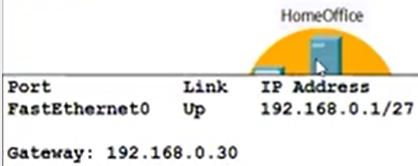


Podemos ver el puerto que ha sido establecido como **troncal g0/1**. El **puerto troncal**, nos va a permitir llevar todo el tráfico de distintas VLANs al router que tiene programadas las subinterfaces.

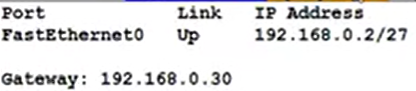
**La VLAN 1** tiene un direccionamiento IP, que es una interface lógica, no física, es una interface virtual al igual que las interfaces loopbacks y requieren de un direccionamiento IP para que puedan ser accesibles. **Todo dispositivo que tenga acceso a la red, requiere de tres elementos**: dirección IP, máscara y puerta de enlace predeterminada. Y esos elementos ya están incluidos en la configuración de la VLAN 1. El switch está preparado y va a poder ser accedido desde el exterior.



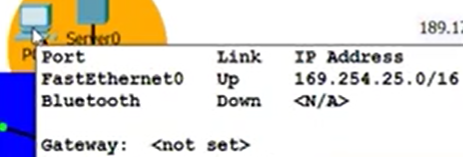
Vamos a ver la configuración del **servidor de HomeOffice** y ya tiene una dirección IP asignada, su máscara /27 y una puerta de enlace predeterminada. Este equipo ya es funcional. El Gateway tiene la última IP válida de esa subred.



La **impresora** también tiene una dirección IP



Pero los equipos como la **PC0** que requiere de un servicio de DHCP que no está instalado. En este momento toma una dirección IP automática que le asigna automáticamente Windows o el protocolo 169.254.x.x, lo mismo ocurre con la **Laptop,** la **Tablet** y el **Smathphone**.



Hemos determinado que el **switch está configurado**, que los equipos tienen activo el protocolo DHCP para atrapar una dirección de forma automática.

EL **servidor** y **la impresora** tienen una **dirección IP estática**.

La impresora y el servidor de HomeOffice ya tienen ips asignadas, las demás son ips dinámicas que se obtendrían con DHCP

**Router**

**Sh run**

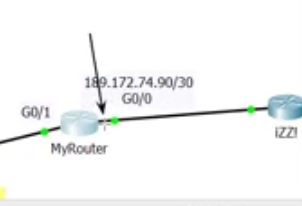
Tiene configuración básica, passwords, hostname

La interfaz **g0/0** está configurada con la IP que nos asignó el proveedor y ya está configurada.

interface **GigabitEthernet0/0**

**ip address 189.172.74.90 255.255.255.252**

Es la dirección ip que nos asignó el proveedor de servicios IZZI



La **interfaz g0/1** va a recibir distintos tipos de tráfico, va a necesitar utilizar subinterfaces.

* Todo el tráfico que sale de la **vlan naranja** va a ser entregado al router.
* Todo lo que sale de la **vlan amarilla** sigue el mismo camino al router, utilizando una única interface.
* Todo lo que sale de la **vlan verde** llega a su subinterface del router.
* Todo el tráfico que sale de la **vlan azul** llega a la subinterface correspondiente en el router.

Si las VLANs corresponden con la VLAN 10, 20, 30, 40 o 50, **se sugiere identificar a las subinterfaces con el mismo ID** que le corresponde a la VLAN.

interface **GigabitEthernet0/1.1**

description VLAN administrativa

encapsulation dot1Q 1 native **//Encapsulamiento universal dot1Q**, el ID de la **vlan 1 la nativa. No había configurado el comando native, en la vlan nativa se requiere configurarlo.**

ip address 192.168.0.130 255.255.255.252 **// ultima IP correspondiente de su subred**

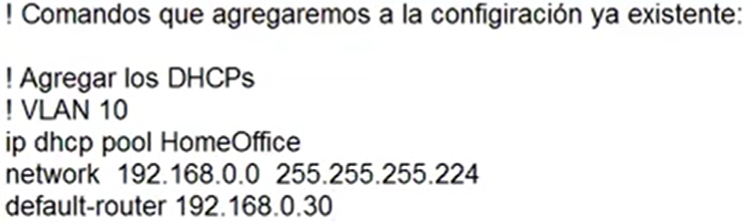
La VLAN 1 ES LA VLAN administrativa, es la nativa.

También tenemos configuradas las subinterfaces de la vlan 10, 20, 30, 40 y 50.

Ya tenemos conexión hacia el exterior, ya que tenemos configurada una ruta estática por default directamente conectada a la interface g0/0.



En el reto, se nos pide instalar el serviciode **DHCP**

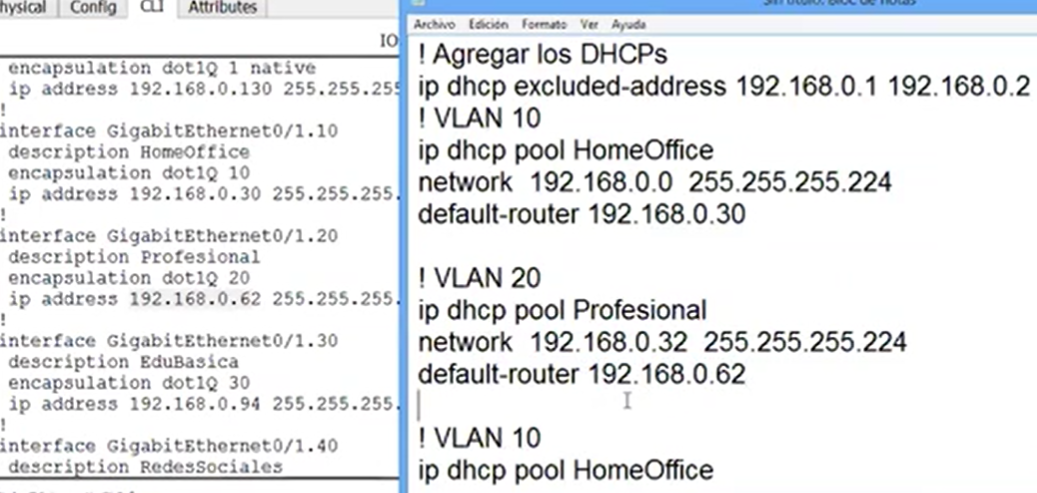
****

La primera IP disponible va a ser la .1, .2, etc. hasta llegar a la .30. El problema es que el **server** tiene la dirección **.1**, la **impresora** tiene la dirección **.2**, ya también está utilizada, por lo que vamos a excluir estás dos direcciones más la **IP del Gateway**. Vamos a pedir que excluya esas direcciones para que no puedan ser asignadas dinámicamente.

**ip dhcp excluded-address 192.168.0.1 192.168.0.2 // IMPRESORA Y SERVIDOR**

**ip dhcp excluded-address 192.168.0.30 // DEFAULT GATEWAY**

Copiamos y pegamos la VLAN y la modificamos para las VLANs 20, 30, 40 y 50 y copio la puerta de enlace predeterminada de las subinterfaces del router.

****

**Están intercambiadas las VLAN 40 Y 50, vlan 40 Redes sociales y vlan 50 Entretenimiento.**

****

**Falta excluir todos los default-routers de todas las VLANs**

En este momento, ya los equipo terminales de la VLAN, podrían obtener direccionamiento IP dinámico.

**Nos falta llevar a cabo la conexión de todos los dispositivos hacia el exterior instalando el protocolo de NAT**. En este caso como tenemos una única dirección de tipo IP tenemos que utilizar un protocolo de tipo **PAT**, donde muchas IPs privadas se pueden traducir con pocas IPs públicas.

Para **configurar PAT** tenemos que hacer lo siguiente:

1. Construir la **lista de control de acceso estándar 1** permit que permita todo el tráfico de la red privada 192.168.0.0 sea traducido a IP público.



Construir la **lista de control de acceso estándar 1** permit que permita todo el tráfico de la red

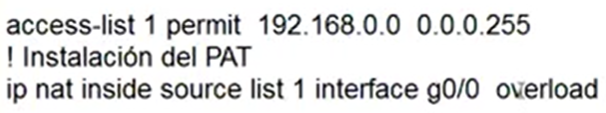
1. **Crear la traducción dinámica de direcciones** con la ACL definida, utilizando la **dirección del puerto** como la única dirección IP pública.

**ip nat inside source list 1 interface g0/0**

La fuente es una lista de control de acceso 1, permitiendo que todo el tráfico se pueda traducir de la red 192.168.0.0, si utilizáramos la información de un pool, el siguiente elemento sería el nombre del pool, pero como solamente vamos a utilizar la dirección IP de la interface g0/0, se utiliza la palabra interface y la interface de la cual queremos recuperar la ip pública (189.172.74.90) y que se conecta directamente con el proveedor de servicio. Tomará la ip 189.172.74.90 para la traducción de IPs privadas.

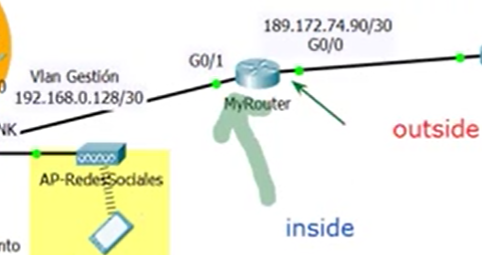
Para concluir, para que muchas IPs privadas internas puedan salir utilizando una dirección IP pública, necesitamos poner la palabra **overload** y con eso instalamos el servicio del PAT.

Tenemos el access list y la instalación del PAT con una única dirección.

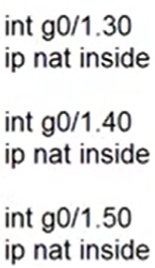
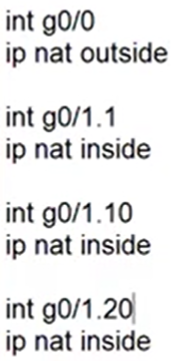


El siguiente paso es **configurar las interfaces que son outside y las interfaces que son inside**. En MyRouter se va a instalar el servicio de nateo.

* La interface **g0/0** es una interface de salida, que se conecta con el proveedor de servicios y será activada o configurada como **outside**.
* **Todas las interfaces y subinterfaces g0/1 serán configuradas como inside**, ya que participarán internamente en el nateo. La interface g0/1 recibe el tráfico de múltiples VLANs, por lo que todas las subinterfaces hay que configurarse inside, porque son el equivalente a todas la interfaces con dominio interno local.

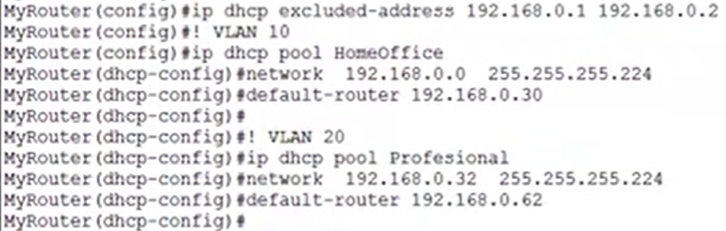


**Int g0/0 es la única interface outside**, ya que es la interface que tiene conexión con el proveedor de servicios y que realizará la traducciones de direccionamiento privado a público. Y que transporta el tráfico de salida

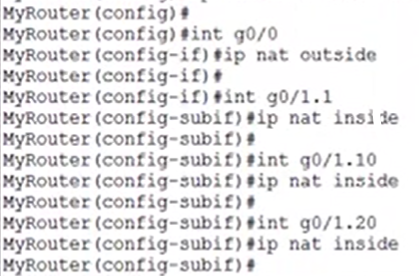
****

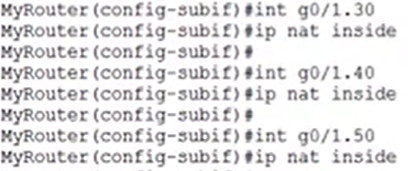
Con esto permitimos que todas las estaciones locales puedan salir al exterior.

Ahora hay que copiar esta configuración, para probar que podemos salir desde cualquier dispositivo al exterior.

****

****

****

****

**Pruebas del servicio DHCP**

* Revisamos si la **PC0** ya tiene IP dinámica. Hay que permitir que atrape una dirección IP a través del servicio de DHCP. Me entrega la dirección 192.168.0.3, ya que hemos excluido la .1 y la .2 para el servidor y la impresora.
* Revisamos si la **Laptop0** ya tiene IP dinámica (192.168.0.33)
* Revisamos si la **Laptop1** ya tiene IP dinámica (192.168.0.65)
* Revisamos si la **Tablet** ya tiene IP dinámica (192.168.0.113)
* Revisamos si el **Smartphone** ya tiene IP dinámica (192.168.0.97)

**Pruebas de conectividad externa**

* Revisamos si la **PC0** tiene acceso web al **servidor de IZZI (132.254.89.100**). Con esto comprobamos que el servicio de **PAT** está funcionando correctamente, con una sola dirección públicaestamos saliendo al exterior.
* Revisamos si del **SmarthPhone** tiene acceso web al **servidor de IZZI (132.254.89.100**). Con esto comprobamos que el servicio de **PAT** está funcionando correctamente, con una sola dirección públicaestamos saliendo al exterior.

**Pruebas de conectividad interna**

* Revisamos si el **SmartPhone** tiene acceso al **servidor de HomeOffice**.(192.168.0.1) Es la dirección IP privada del servidor. Ya acceso al servidor de manera interna.

**¿El servidor puede acceder al exterior?**

* Revisamos si el **Servidor de HomeOffice** tiene acceso web al **servidor de IZZI (132.254.89.100**).
* Con esto podemos concluir que todos los equipos de la red de cobertura local tienen la posibilidad de ser traducidos para salir al exterior, pero viene la siguiente pregunta, **¿cómo le hago para que desde el exterior pueda acceder al** **switch (192.168.0.129)**.

**Vamos a instalar el Port Forwarding en el router MyRouter.**

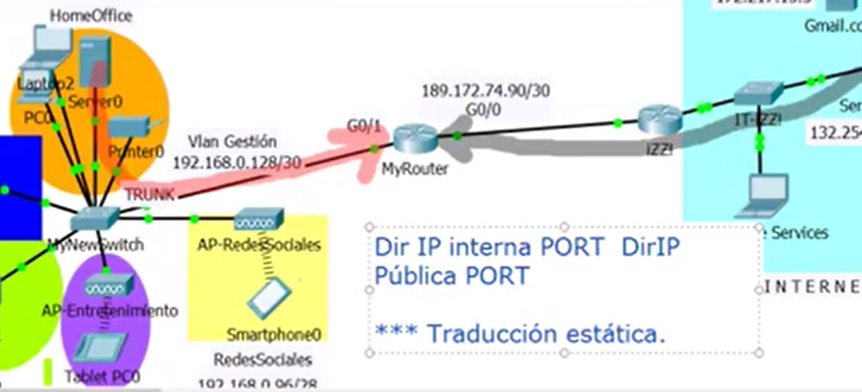
Para poder realizar port forwarding tenemos dos tipos de protocolos: **protocolo interno local y protocolo externo.**

* Todo lo que el **Servidor de HomeOffice** quiera publicar, **MyRouter** tiene que hacer una traducción.
* Todo lo que desde el exterior quiera acceder al **servidor de homeOffice**, tiene que llegar al router, con la dirección pública se tiene que hacer una traducción para poder entrar hasta los dominios del **servidor de HomeOffice**.
* Para el funcionamiento del protocolo **NAT con port – forwarding**, necesitamos

1. Una **dirección IP interna**, un **protocolo** (del protocolo TCP o del protocolo UDP) y un **puerto**
2. **Para poder comunicarnos desde el exterior necesito forzosamente una** dirección IP **pública** y un **puerto**.

Los puertos pueden ser iguales o distintos. Se llama port forwarding, ya que lo que llega por un puerto de petición, lo podemos enviar a otro puerto diferente o al mismo puerto. Quiero acceder por el puerto 80, pero desde el exterior lo conozco por el puerto 50012

1. Se debe tener una **traducción estática**, con esto conseguimos el port forwarding.



**Detalles en cuanto a la instalación de Port forwarding**

Para poder instalar **port forwarding** necesito realizar **una traducción estática, necesito dirección IP privada y dirección IP pública.** Pero le vamos a agregar el **protocolo** y el **puerto** por el que vamos a estar escuchando y con qué puerto vamos a estar traduciendo.

**! PORT FORWARDING REQUISITO REALIZAR NAT ESTÁTICO**

**! --------------------------------------------------**

**!ip nat inside source static 192.168.0.1 189.172.74.90**

! ESTO CONSUME TODOS LOS SERVICIOS DE LA TRADUCCIÓN DEL NATEO ESTÁTICO Y LOS DEMÁS USUARIOS NO PODRÁN HACER LA TRADUCCIÓN.

Para resolver este problema existe el **port forwarding,** que es un requisito construirlo a partir de

Un **nateo estático**.

Pero tenemos que establecer cuál es el **protocolo que queremos escuchar y forwardear y este es el protocolo TCP.**

**El servidor web utiliza un puerto, a continuación debo establecer cuál es el puerto interno a través del cual voy a escuchar todas las peticiones (el puerto es el 80).**

**Se llama port forwarding porque yo puedo definir desde el exterior que puerto quiero que me contacten al servidor del 80, en el router al momento de hacer el nateo se va a identificar el puerto por el que llega y el puerto por el que debe entrar al servidor.**

ip nat inside source static **tcp** 192.168.0.1 **80** 189.172.74.90 **50000**

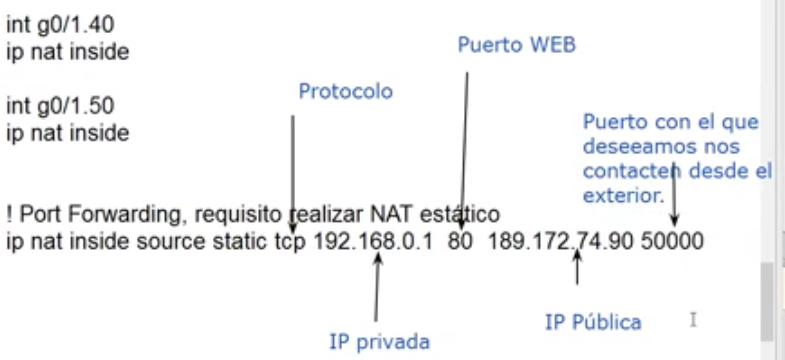
**! tengo hasta 65000 para el puerto, el 50000 es un puerto válido.**

**Notas importante:**

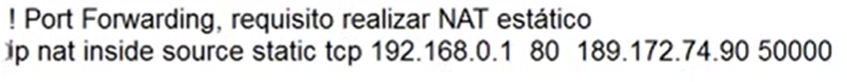
**El port forwarding necesita forzosamente de los siguientes elementos:**

1. **Los comandos: ip nat inside source static**
2. **Tengo que poner el tipo de protocolo que se va a traducir**
3. **La dirección interna privada (IP privada)**
4. **Identificar el puerto: WEB (estamos publicando desde el protocolo web) puerto por el que me voy a conectar**
5. **La dirección ip pública**
6. **El puerto por el cual nos van a contactar desde el exterior.**

Quien nos va a contactar, todos los que se encuentran en el exterior. El puerto por el que nos van a contactar puede ser cualquiera de los permitidos 2 a 16 (65536). Disponibles desde el 0 hasta el 65536.

****

**Pegar esta traducción en el router, la traducción del servidor:**

****

A partir de este momento el servidor de HomeOffice va a ser contactable a través de la dirección IP pública que hemos utilizado y el puerto por el que queremos que nos contacten.

Desde la computadora del **IT Remoto** vamos a contactar por acceso web a la dirección **189.172.74.90:50000** y el puerto que públicamente anuncié y configuré para que me contacten.

SI responde la traducción de port forwarding es correcta. Puedo encontrar la forma de cómo me contacten desde el exterior a este servidor público.

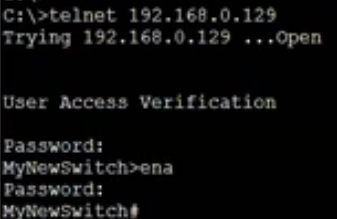
Si no pongo el puerto y como web trabaja con el puerto 80 me van a contactar, solamente accedemos con la ip **189.172.74.90** esto va a fallar (Server Reset Connection), no hay la posibilidad de que esta traducción exista y por consiguiente no me pueden atender.

**Si intentamos acceder por el puerto 80 de web 189.172.74.90:80 el resultado es el mismo.**

Yo publique que el servidor HomeOffice estará disponible a través de puerto **50000**

Como hago para entrar al **switch myswitch** desde el exterior, si de manera interna lo probamos con un telnet al switch myswitch debe funcionar. Por ejemplo, del **Smarthphone** hago un **telnet** hacia la vlan 1 del switch myswitch

**telnet 192.68.0.129**

****

**Sh run podemos ver la configuración del switch.**

**Como le hacemos para acceder al servicio telnet del switch desde el exterior.**

**¡Port forwarding del switch, copiamos la misma configuración del server, hay que cambiar la ip del switch, el puerto por el que me voy a conectar es telnet voy a utilizar 23 y el puerto desde el exterior también lo vamos a poner como 23**

ip nat inside source static **tcp** 192.168.0.1 **80** 189.172.74.90 **50000**

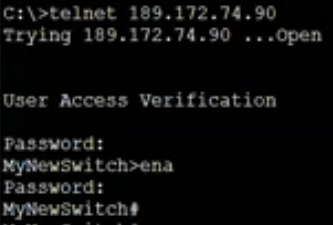
ip nat inside source static **tcp** 192.168.0.129 **23** 189.172.74.90 **23**

**Con esta configuración, desde el exterior, nuestro proveedor de servicios que conoce esta configuración va a poder entrar a nuestro switch, por el puerto 23**

**Podemos incrementar el nivel de seguridad si adicionamos el servicio de ssh. Copiamos y pegamos.**

Probamos que podamos acceder desde el equipo externo **IT-Remote Services** podemos entrar al switch a través del protocolo telnet

**telnet 189.172.74.90**

****

Ya estando en el switch podría modificar la configuración del switch.

Con esto terminamos la configuración del protocolo del PAT, incluyendo Port forwarding.

NAT incluye 4 posibilidades.

Tener una traducción estática.

Tener la creación de un pool dinámico

Poder traducir con puertos conocido como PAT

**Port forwarding cuando solamente tenemos una IP pública para la traducción de direccionamiento estático y dinámico.**

**Comandos que agregaremos a la configuración ya existente en el ROUTER:**

**!Agregar los DHCPs**

**----------------------**

**!VLAN 10**

**!------------**

**! HomeOffice 192.168.0.0/27**

**! DIRECCIONES EXCLUIDAS**

**ip dhcp excluded-address 192.168.0.30**

**ip dhcp excluded-address 192.168.0.1 192.168.0.2**

**! Excluimos servidor e impresora**

**! DHCP para HomeOffice g0/1.10**

**ip dhcp pool HomeOffice**

**network 192.168.0.0 255.255.255.224**

**default-router 192.168.0.30**

**exit**

**!VLAN 20**

**!------------**

**! Profesional 192.168.0.32/27**

**! DIRECCIONES EXCLUIDAS**

**ip dhcp excluded-address 192.168.0.62**

**! DHCP para Profesional g0/1.20**

**ip dhcp pool Profesional**

**network 192.168.0.32 255.255.255.224**

**default-router 192.168.0.62**

**exit**

**!VLAN 30**

**!------------**

**! EduBasica 192.168.0.64/27**

**! DIRECCIONES EXCLUIDAS**

**ip dhcp excluded-address 192.168.0.94**

**! DHCP para EduBasica g0/1.30**

**ip dhcp pool EduBasica**

**network 192.168.0.64 255.255.255.224**

**default-router 192.168.0.94**

**exit**

**!VLAN 40**

**!------------**

**! Redes sociales 192.168.0.96/28**

**! 96 + 16 = 112 -2 = 110**

**! DIRECCIONES EXCLUIDAS**

**ip dhcp excluded-address 192.168.0.110**

**! DHCP para RedesSociales g0/1.40**

**ip dhcp pool RedesSociales**

**network 192.168.0.96 255.255.255.240**

**default-router 192.168.0.110**

**exit**

**!VLAN 50**

**!------------**

**! Entretenimiento 192.168.0.112/28**

**! 112 + 16 = 128 -2 = 126**

**! DIRECCIONES EXCLUIDAS**

**ip dhcp excluded-address 192.168.0.94**

**! DHCP para Entretenimiento g0/1.50**

**ip dhcp pool Entretenimiento**

**network 192.168.0.112 255.255.255.240**

**default-router 192.168.0.126**

**exit**

**----------------------------------------------**

**! INSTALACIÓN DE NAT. HAY UNA SOLA DIRECCIÓN IP PÚBLICA 189.172.74.90**

**access-list 1 permit 192.168.0.0 0.0.0.255**

**! ip nat pool MyPool 189.172.74.90 255.255.255.252**

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

! esto si usaramos un pool

! pero como queremos utilizar la ip de la interface que me une con el ISP.

! y de la cual quiero recuperar la información

**! INSTALACIÓN DEL PAT CON UNA SOLA DIRECCIÓN**

**!--------------------------------------------**

**ip nat inside source list 1 interface g0/0 overload**

**! overload para que muchas direcciones internas puedan usar**

**! una sola dirección pública.**

**! CONFIGURAR INTERFASES Y SUBINTERFASES INSIDE Y OUTSIDE.**

**! ------------------------------------------**

**int G0/0**

**ip nat outside**

**! INTERFASE DE SALIDA**

**! INTERFASES DE ENTRADA**

**int G0/1.1**

**ip nat inside**

**int G0/1.10**

**ip nat inside**

**int G0/1.20**

**ip nat inside**

**int G0/1.30**

**ip nat inside**

**int G0/1.40**

**ip nat inside**

**int G0/1.50**

**ip nat inside**

**int G0/1**

**no shut**

**! PORT FORWARDING REQUISITO REALIZAR NAT ESTÁTICO**

**! --------------------------------------------------**

**!ip nat inside source static 192.168.0.1 189.172.74.90**

! ESTO CONSUME TODOS LOS SERVICIOS DEL NATEO ESTÁTICO

! TRADUCCIÓN PARA EL SERVIDOR

**ip nat inside source static tcp 192.168.0.1 80 189.172.74.90 50000**

! A partir de este momento si ya el servidor podía acceder a los servicios del exterior,

! a partir de este momento nuestro servidor es contactable desde el exterior a través

! de la dirección ip pública 189.172.74.90 y el puerto con el que queremos que nos

! contacten (50000)

**! TRADUCCIÓN PARA EL SWITCH**

**ip nat inside source static tcp 192.168.0.129 23 189.172.74.90 23**

! A partir de este momento nuestro switch es contactable desde el exterior a través

! de la dirección ip pública 189.172.74.90 y el puerto con el que queremos que nos

! contacten (23)

**! tengo hasta 65536 para el puerto. Elevar 2 a la 16 = 65536 desde 0 - 65536**

**! tengo que poner el tipo de protocolo que se va a traducir, la dirección**

**! interna privada, el puerto WEB y la dirección ip pública y el puerto**

**! por el cual nos van a contactar desde el exterior.**

**! Debo definir el puerto por el que voy a estar escuchando todas la peticiones**

**! El puerto es el 80**

**! Se llama port forwarding porque yo puedo definir desde el exterior**

**! que puerto quiero que me contacten a mi servidor del 80**

**! Y en el router al momento de hacer el nateo se va a identificar**

**! el puerto por el que llegué y el puerto por el que debo entrar al servidor**

**! Como hacemos para acceder al switch desde el exterior**

**! NAT CON PORT FORWARDING**

**! 1. Dirección IP interna PORT Dirección IP pública PORT**

**! Se llama port forwarding porque lo que lo que llega por un puerto de petición**

**! lo podemos enviar a otro puerto diferente o al mismo puerto**

**! 2. Traducción estática (dirección privada - dirección pública)**

**! Con eso conseguimos el port-forwarding**