NAT

Como poder instalar un servicio de traducción de direcciones privadas en una organización para poder conectarnos con la red pública (Internet). El direccionamiento público está limitado a unas cuantas direcciones IP v4 para poder conectarnos.

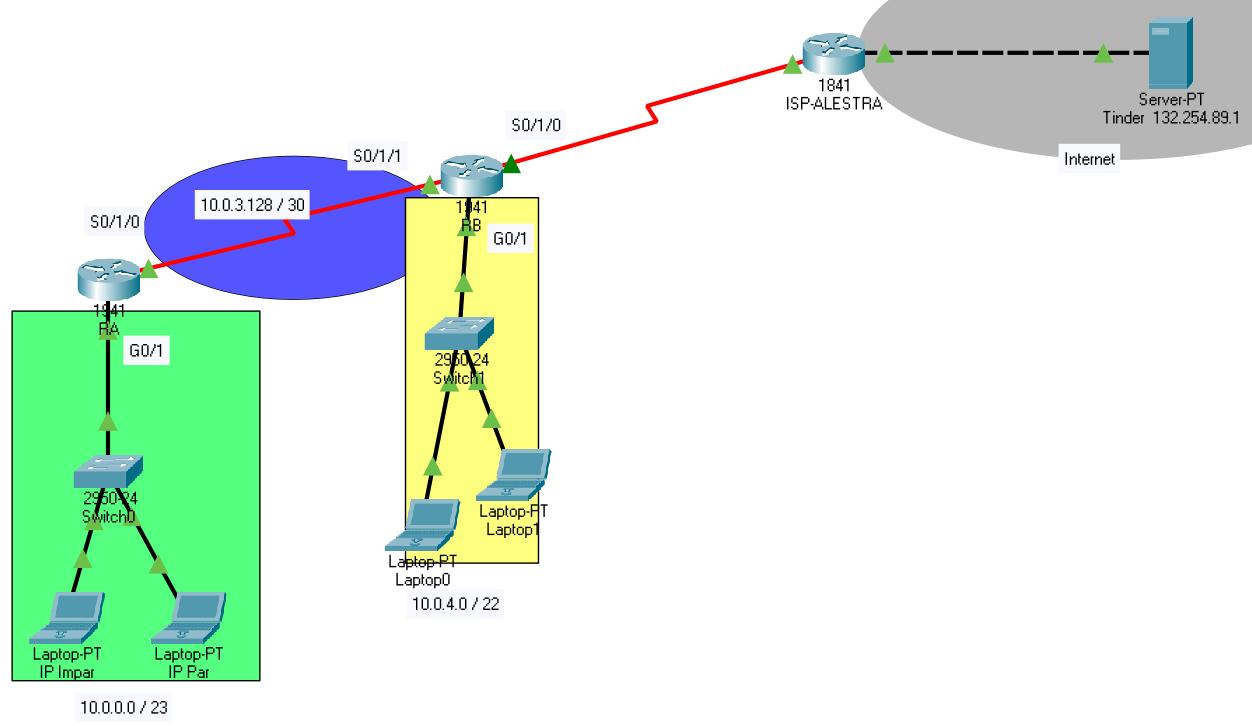
Mejores prácticas para realizar configuraciones exitosas

1. **Diseñar** un esquema de **subredes** que de servicio a los requerimientos de conectividad de la red (de la organización)
2. **Asignar**, siguiendo algún estándar, **direcciones IP a las interfaces de los equipos** de interconexión. (primera o última dirección IP válida de la subred o bloque)
3. **Configurar**, de acuerdo a la asignación de **direcciones IP y máscaras**, **las interfaces de los equipos** de interconexión
4. **Configurar equipos terminales** con sus respectivas IPs. Verificar conectividad con puerta de enlace predeterminada.
5. **Configurar protocolo de ruteo dinámico**, **rutas estáticas** y **rutas por default(que me permiten sacar el tráfico de todo lo que no es de mi dominio local hacia la red de cobertura amplia** (en caso de que se utilicen)
6. **Configurar** el servicio de **DHCP (Nos permite asignar direccionamiento dinámico cuando los equipos así lo solicitan, utilizando el protocolo DHCP). Hemos configurado DHCP de forma distribuida y centralizada. El ejercicio de hoy se trabajará DHCP de forma centralizada, solamente tendríamos un servidor DHCP.**
7. **Configurar el servicio de NAT.**
8. Diseñar e instalar esquemas básicos de seguridad (**ACLs**) Instalar listas de control de acceso estándar o extendidas.

En el ejercicio que vamos a realizar se tiene el diseño de una red ya establecida, con un Subneteo con máscaras de longitud variable (VLSM), vamos a trabajar con una red privada 10, simulando la red del tec. Se instalarán los servicio de NAT, DHCP y se instalará un servidor con direccionamiento estático para accederlo desde el exterior.

En el ejercicio se tienen dos subredes, la subred de color amarillo (10.0.4.0/22) y la subred de color verde (10.0.0.0) y la subred azul que interconecta (10.0.3.128/30) que interconecta las dos interfaces seriales de nuestra red. local. Nuestra red local solamente abarca estas subredes. El ISP ya está configurado y está restringido.

Vamos a analizar la configuración de los routers RA y RB. En el router A y B se tiene la configuración básica: configuración de interfaces, protocolo de ruteo y el router B además un ruteo estático hacia el exterior.



Instalaremos el servicio de **DHCP centralizado**. Un servicio centralizado es aquel que se pone en un solo router.

¿Dónde instalaremos el servicio? Tenemos dos routers donde se puede instalar el servicio de DHCP, tenemos el router frontera y el router A. La mejor de las opciones es el router B.

¿Cómo seleccionar la IP de la interfaz que ayudará a resolver el DHCP?

Los pasos más básicos para instalar la configuración del servicio de DHCP se resumen en tres:

Los tres elementos mínimos se puede instalar el servicio de DHCP, ya que los equipos terminales requieren de una dirección IP, su máscara y su puerta de enlace predeterminada:

1. Excluir las direcciones estáticas del pool de DHCP.

**ip dhcp excluded-address** Dir\_IP\_Inicial Dir\_IP\_Final

1. Definir un **pool de direcciones dinámicas** que serán asignadas cuando sean solicitadas.

**ip dhcp pool** **NombrePool (1. Definir el nombre del pool)**

**network** dirIP\_inicial Máscara de subred (**2. Definir cuál el bloque de direcciones que se van a distribuir a través de esa petición de DHCP**)

1. Agregar la configuración del default Gateway:

**default-router** dirIP (**3. Establecer la puerta de enlace predeterminada (default Gateway))**

**La primera de las acciones no es un requisito que exista, es opcional, pero hay que excluir las direcciones de los equipos que requieren de una dirección estática como servidores, impresoras, etc.**

Se revisa la configuración del router B: No hay passwords.

Sh run

Están configuradas las interfaces.

G0/1 10.0.7.254

La serial que va hacia Internet es un /27 tengo 65.108.66/27 la subred me da 32 direcciones – 2 = 30 direcciones de las cuales ya están utilizadas dos para las seriales. Me quedan 28 direcciones disponibles, ya que al mismo tiempo que me conectan con el exterior me están asignando un pool de direcciones. Y son las direcciones públicas que con NAT estaremos programando

Protocolo de ruteo rip v2

Redistribuye la ruta estática por default que está utilizando la interface directamente conectada.

Ip route 0.0.0.0 0.0.0.0 serial0/1/0

En el router B cuales serían las interfaces pasivas?

G0/1

S0/1/0

router rip

version 2

passive-interface g0/1

passive-interface s0/1/0

En el router A cuales serían las interfaces pasivas?

G0/1

router rip

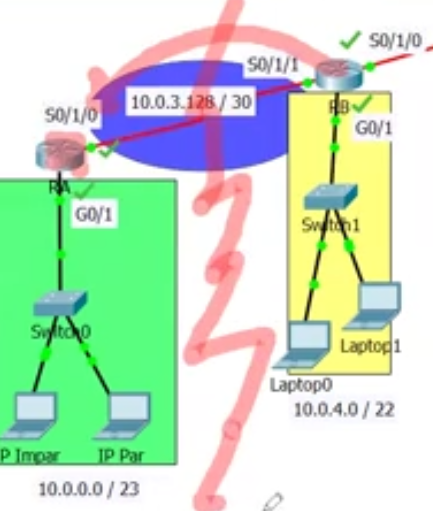
version 2

passive-interface g0/1

Solamente, ya que si hacemos pasiva la interface no podríamos inyectar nuestras tablas de ruteo.

Si ponemos pasiva la interface s0/1/0 del router RA, no va a inyectar información de su tabla de ruteo ya que estaría bloqueada la interface.

El router RB está bloqueado para inyectar sus tablas de ruteo por la interfaz g0/1, pero si está facultado para inyectar sus tablas hacia el RA. El RA es capaz de escuchar pero no de inyectar, por lo tanto la red queda completamente fracturada.



**El comando no auto-summary evita que RIP haga un resumen automático de la red 10.0.0.0/8, si no lo hacemos así, los routers no van a ser capaces de conocer las subredes de esa red principal. De esta forma los forzamos a que publiquen las subredes tal como son.**

Se revisa configuración del router A.

Cuando en los equipos terminales está configurado tomar direccionamiento dinámico, y el servicio DHCP no funciona, de manera automática va a tomar un direccionamiento dentro de la red 169.254.x.x, Si mis equipos toman este direccionamiento, podemos concluir que no ha atrapado direccionamiento dinámico.

En el router B, vamos a instalar el servicio dhcp para las subredes verde y amarilla.

En el router B, la interface g0/1 va a atender las peticiones de la subred amarilla y en el router A la interface g0/1 va a atender las peticiones de la subred verde. Vamos a configurar dos pools con nombres significativos para la subred verde y la subred amarilla.

**!CONFIG ROUTER B**

!VAMOS A EXCLUIR LA IP DE LA INTERFACE G0/1

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

! DIRECCIONES EXCLUIDAS DE LAS INTERFACES PUERTAS DE ENLACE PREDERTMINADAS

**ip dhcp excluded-address 10.0.7.254** corresponde con la puerta de enlace predeterminada

**! DHCP para la subred RB\_G0/1**

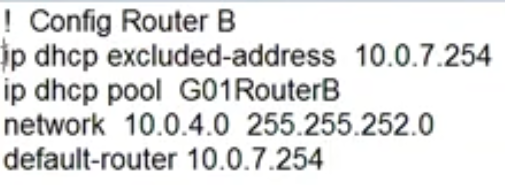
**ip dhcp pool RB\_G0/1 nombre significativo g0/1 del router B. Este es el pool para la interface g0/1 del router B.**

**network 10.0.4.0 255.255.252.0 se asigna bloque de direcciones de la subred amarilla.**

**! Tenemos 1024 direcciones disponibles – 2 en esa subred y una ya**

**! está ocupada por la interface g0/1 o la puerta de enlace predeterminada.**

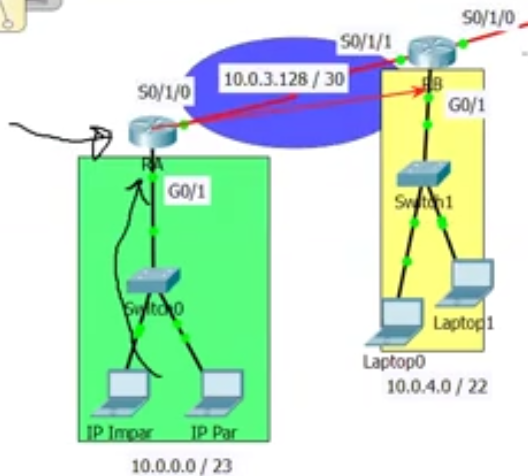
**default-router 10.0.7.254 Permite establecer la puerta de enlace predeterminada, que es la g0/1 que estamos excluyendo.**

****

**Se coloca configuración en el router b para probarla**

**Checamos si la laptop0 y la laptop1 toman direccionamiento dinámico. Activando DHCP en las laptops. Cada dispositivo tiene su IP, su máscara y su puerta de enlace predeterminada.**

**Ahora se instala el segundo de los pools para la subred verde. El sentido del tráfico va hacia la interface g0/1 del router A. En el router A se tiene que instalar un servicio que es una primitiva o comando que me permite darle una dirección IP del dispositivo que tiene publicado el servicio de DHCP para mi subred verde. Hay tres posibilidades para indicarle al router A, quién me va a apoyar con mi dirección IP, máscara y puerta de enlace predeterminada de mis equipos de mi subred verde. Una opción sería utilizar la dirección IP de la interface s0/1/1, otra la g0/1 o la s0/1/0 del router B. Se va a instalar la interface más directa y después se hará un cambio. Solamente necesito una dirección IP del router a donde está instalado el servicio DHCP, no necesariamente la interfaz más cercana.**

****

**Se configura el pool y luego la IP que me auxiliará para llevar a cabo la conexión**

**!DHCP PARA SUBRED VERDE**

!VAMOS A EXCLUIR LA IP DE LA INTERFACE G0/1

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

! DIRECCIONES EXCLUIDAS DE LAS INTERFACES PUERTAS DE ENLACE PREDERTMINADAS

**ip dhcp excluded-address 10.0.1.254** corresponde con la puerta de enlace predeterminada

**! DHCP para la subred RA\_G0/1**

**ip dhcp pool RA\_G0/1 nombre significativo g0/1 del router B. Este es el pool para la interface g0/1 del router A.**

**network 10.0.0.0 255.255.254.0 se asigna bloque de direcciones de la subred verde.**

**! Tenemos 512 – 2 direcciones IP disponibles en esa subred y una ya**

**! está ocupada por la interface g0/1 o la puerta de enlace predeterminada.**

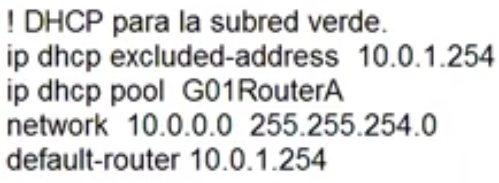
**10.0.0.1 hasta 10.0.1.254**

**10.0.0000 000 0. 00000000**

**0. 00000001**

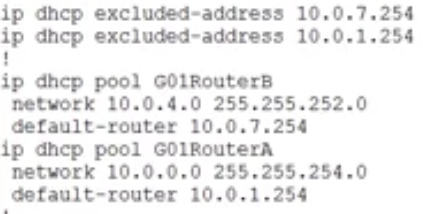
**1. 11111110**

**1. 11111111**

****

**Configuramos pool en router B.**

**Con sh run checar que los dos pools estén funcionando. Primero se instalan las ips excluidas de la subred amarilla y luego la verde. En el orden en que fueron creados el pool de la subred amarilla del router b directamente conectada y el pool de la subred verde que no está directamente conectada. El router ya tiene configurados los dos pools.**

****

**Se revisa si las laptops están tomando direccionamiento IP en la subred verde. Se confirma que el protocolo no está encontrando el servidor dhcp y asigna direcciones 169.254.x.x**

**Que es lo que nos falta para completar el protocolo de instalación del DHCP. Instalar en el router A solamente para la interfaz g0/1 el comando ip helper, con el IP helper se resuelve el problema de que el router no tiene el servicio DHCP pero alguien más si lo tiene y lo voy a poder contactar por alguna de sus tres interfaces.**

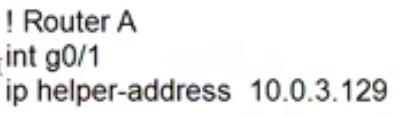
**PARA QUE EL DHCP CENTRALIZADO FUNCIONE HAY QUE CONFIGURAR EN EL ROUTER A QUIEN ES LA IP DE LA INTERFACE DEL ROUTER QUE ME VA A ESTAR APOYANDO CON EL SERVICIO DE DHCP, YA QUE EL ROUTER A NO LO TIENE INSTALADO. La dirección IP puede estar dos routers adelante, 25 routers adelante, lo importante es que tenga la dirección IP DEL router que va a escuchar nuestras peticiones de IPs y respondernos.**

**¡ ROUTER A**

**Int g0/1**

**Ip helper-address 10.0.3.129 debe tomar alguna dirección del router b. Podemos asignarle la dirección más cercana.**

**CON ESTE COMANDO ES SUFICIENTE PARA QUE EL ROUTER A CONTACTE AL ROUTER B PARA QUE LE ENTREGUE DIRECCIONES IPS, MÁSCARA Y PUERTA DE ENLACE PREDETERMINADA A TODOS LOS EQUIPOS DE LA SUBRED VERDE.**

****

**Copiamos comando en router A. NO TENGO EL POOL EN EL ROUTER A PERO PUEDO SOLICITARLE A ALGUIEN CON UNA DIRECCIÓN EN ALGUN LUGAR DONDE ESTÉ INSTALADO EL DHCP QUE ME DE RESPUESTA A ESA PETICIÓN.**

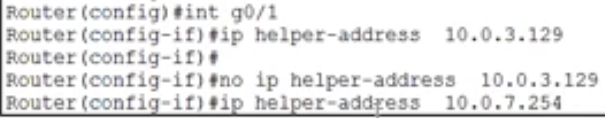
**A partir de este momento el routerA sabe de dónde va a sacar el pool de DHCP porque tiene una dirección a quién contactar. Así estuviera, un router, dos routers, 25 routers adelante la dirección, habrá alguien que me estará respondiendo. Y como le hace el servidor DHCP para asignar los pools, si cuento con múltiples interfaces, por la puerta de enlace predeteterminada, sabe a qué subred responder.**

**Checamos los equipos de la subred verde y ya tienen IP.**

**Prueba de conectividad entre subred verde y amarilla.**

**Ping de pc verde a pc amarilla (10.0.4.1) y debe funcionar.**

**Quitar la ip de la interfaz serial y agregamos la ip de la interfaz g0/1 del router b.**

****

**Probamos que ya no hay ips dinámicas y damos enter para probar la otra ip. El router B tiene tres interfaces por las cuales nos puede atender para resolver el DHCP. El poner una interface pasiva solamente va a aplicar para el protocolo de ruteo y le dice que no inyecte tablas de ruteo a través de esa interface. Poner pasiva la interface no significa que el DHCP no responda.**

**Ya se configuró servicio de DHCP, ahora vamos a configurar NAT.**

**¿Cómo conectar direccione IP privadas con direcciones IP públicas?**

**La dirección 10.x.x.x es una dirección clase A privada. Qué es lo que tengo que hacer para conectar los direccionamientos privados como los de la casa (192.168.x.x) o como el tec (10.0.0.0) como los voy a conectar con direccionamientos públicos. Necesitamos instalar el servicio de NAT.**

**El NAT traduce de direccionamiento privado a direccionamiento público y viceversa.**

**Las direcciones IP v4 públicas están limitadas. De hecho hay una teoría de que ya debieron haberse acabado desde hace como 8 años, pero se siguen utilizando, ya que su uso sigue vigente, por lo mismo el servicio de NAT sigue vigente. El servicio de NAT se puede configurar con 4 pasos.**

**1. Definir un pool de direcciones globales (públicas) que serán asignadas cuando sean necesarias.**

**Las direcciones ip públicas son aquellas que no son privadas.**

**NO PODEMOS TOMAR DIRECCIONES IP PUBLICAS AL AZAR, HAY ORGANISMOS EN CADA REGIÓN MÉXICO, CENTROAMERICA, ETC. Y ESE ORGANISMO ES EL QUE SE ENCARGA DE ASIGNARNOS UN BLOQUE DE DIRECCIONES IP PÚBLICAS. LAS DIRECCIONES IP PUBLICAS ESTÁN MUY LIMITADAS.**

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

**Definir nombre del pool, dirección inicial y dirección final y todas las direcciones de ese pool deben ser utilizables y válidas. Viene una máscara de subred que debe agrupar ese grupo de direcciones**

**2. Definir una ACL estándar: DEFINO QUIEN TIENE PERMISO PARA LLEVAR A CABO ESA TRADUCCIÓN. Puede ser en el tec, todos los que tengan direccionamiento dinámico pueden salir al exterior, utilizando la lista de control de acceso.**

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

**La lista de control de acceso la podemos programar por número o por nombre. Para más simple, es mejor programarla por número (1 – 99). Podemos tener dos acciones permitir o negar, como queremos traducir la acción es permitir. Necesitamos la IP inicial del bloque y su máscara complemento.**

**Primero construimos el pool, segundo construimos la lista de control de acceso para indicar quién tiene permiso.**

**3. Establecer la traducción dinámica de direcciones utilizando la ACL definida. Tenemos que decidir que es lo que vamos a instalar. En la práctica del día de hoy se hará la traducción de direccionamiento público a privado y viceversa.**

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

**Todo lo que está en negritas es una palabra reservada.**

**Tenemos dos opciones:**

1. **Utilizamos una lista de control de acceso donde vamos a asociar el pool con quienes tienen permiso.(Todo lo que está en amarillo es una lista de control de acceso) Si utilizamos la palabra al final de overload para poder llevar a cabo una traducción no solamente uno a uno de direcciones sino el esquema de direccionamiento de tipo IP público es muy pequeño en comparación con el direccionamiento privado que es grande (subred amarilla 1024 direcciones), es un conjunto muy pequeño vs un conjunto muy grande, se utiliza overload para que la traducción utilice el puerto desde la cual la estación me está contactando. (puerto generado de manera dinámica y aleatoria arriba de 1024.) Muchos direccionamientos IP privados utilizan pocos direccionamientos IP públicos**
2. **Reservado para dispositivos fijos como un servidor, una cámara, un dispositivo de IoT. El cual necesita una dirección IP única por la cual contactar. Reservada para direccionamientos con traducciones de uno a uno. Una dirección IP privada interna se traduce a una dirección IP pública global.**
3. **Especificar las interfaces interiores y exteriores (Especificar si haremos nateo interno o externo)**

**interface Tipo-Número**

**ip nat inside**

**TODAS LAS INTERFACES QUE TENGAMOS CONFIGURADAS EN NUESTRA RED DE COBERTURA LOCAL TENDRÁN QUE SER INSIDE.**

**interface Tipo-Número**

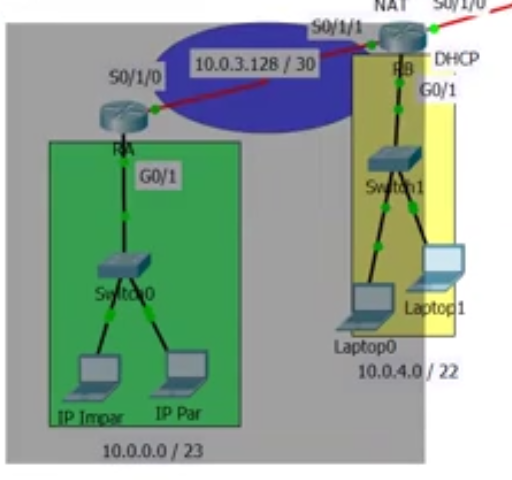
**ip nat outside (CADA INTERFACE QUE TENGAMOS CONFIGURADA CON UN PROVEEDOR DE SERVICIOS TIENE QUE SER CONFIGURADA ip nat outside, porque por ahí va salir una traducción de direccionamiento privado a público)**

**SIN ESTOS ÚLTIMOS COMANDOS LA LISTA DE CONTROL DE ACCESO, EL POOL Y LA CREACIÓN DEL NAT NO TIENEN EFECTO**

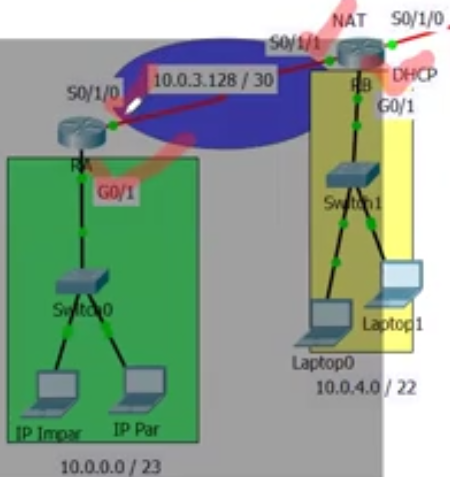
**Configuraremos el servicio de NAT para una lista de control de acceso cuando queremos que todos los usuarios de nuestra red de cobertura local puedan salir al exterior.**

**EL ROUTER B tendrá configurado el servicio de NAT, ya se configuró DHCP.**

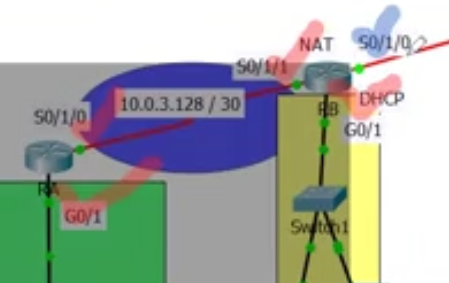
**Tengo que programar o configurar un servicio que me dé a todas las direcciones IP que fueron entregadas de forma dinámica y que me permitan llevar a cabo la traducción para poder sacar la información hacia el exterior.**

****

**Ojo todas las interfaces internas tendrán que ser interfaces configuradas como ip nat inside.**

****

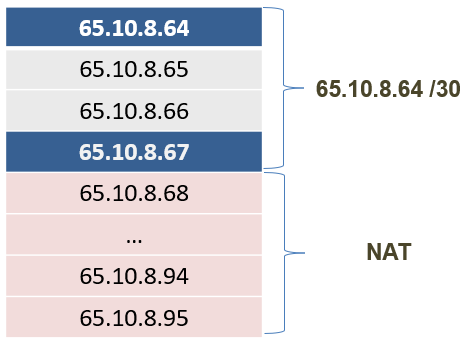
**La única interface que está jugando el papel de llevar de un dominio interno hacia un dominio externo el direccionamiento privado es el que será configurada como ip nat outside, sería la serial 0/1/0**

****

**Por cada ISP que tenga conectado necesito un servicio de NAT.**

**La interface que conecta mi router frontera con el proveedor de servicios debe ser configurada outside.**

**65.10.8.64 / 27**

****

**Este bloque se ha subneteado para la conexión entre los dos seriales. Las interfaces a ser utilizadas son la .65 (isp) y la .66 (routerB), y la .64 y la .67 no se pueden utilizar. El resto de las direcciones IP son IPs válidas que pueden ser utilizadas para NAT.**

**Ahora sí ya vamos a configurar este pool de NAT.**

**SERVICIO NAT**

**Ip nat pool son palabras reservadas, el nombre que gustemos, la ip inicial y la ip final y la máscara de subred de ese bloque de direcciones públicas.**

**PASO1 DEFINIR POOL**

**ip nat pool MyPool 65.10.8.68 65.10.8.95 netmask 255.255.255.224**

**PASO2 QUIEN VA A PARTICIPAR EN LA TRADUCCIÓN**

**Hay que definir una lista de control de acceso estándar**

**access-list 10 permit any (10.0.0.0 y todas las posibles combinaciones 255.255.255.255)**

**PASO3. ENCONTRAR LA RELACIÓN DE ESA LISTA QUIEN VA A ACCEDER A QUE POOL**

**ip nat inside source**

**dos posibles fuentes una lista de control o una dirección IP de traducción estática. Estamos en el primer caso.**

**Ip nat inside source list 10 pool MyPool**

**Hasta el momento tenemos una traducción uno a uno, por cada dirección ip privada demandará una dirección IP PÚBLICA y solamente tendría máximo 28 ips disponibles públicas y en la subred amarilla me demanda 1024-2 IPs y en la subred verde 512-2. El espacio es insuficiente. Tengo más dispositivos que quieren conectarse al exterior contra las direcciones IPs públicas que puedo tener. La solución para hacer una reutilización de direcciones IPs. La palabra overload permite lo que se conoce como PAT la traducción de direccionamiento utilizando de manera adicional el puerto.**

**Si la relación es uno a uno se conoce como NAT (Direccionamiento privado a público)**

**Si la relación es muchas direcciones IP privadas contra una dirección IP pública se le conoce como PAT.**

**PAT (Esta es la programación de PAT)**

**ip nat inside source list 10 pool MyPool overload**

**En las prácticas que se realizarán en los próximos días, en una práctica se instalará el servicio de NAT, y en la otra práctica se instalará el servicio de PAT.**

**PAT puede soportar múltiples direcciones aun teniendo una única dirección IP pública para salir al exterior.**

**Int s0/1/0 (en cada interfaz te tenga conexión al exterior)**

**Ip nat outside**

**Las demás interfaces serán internas.**

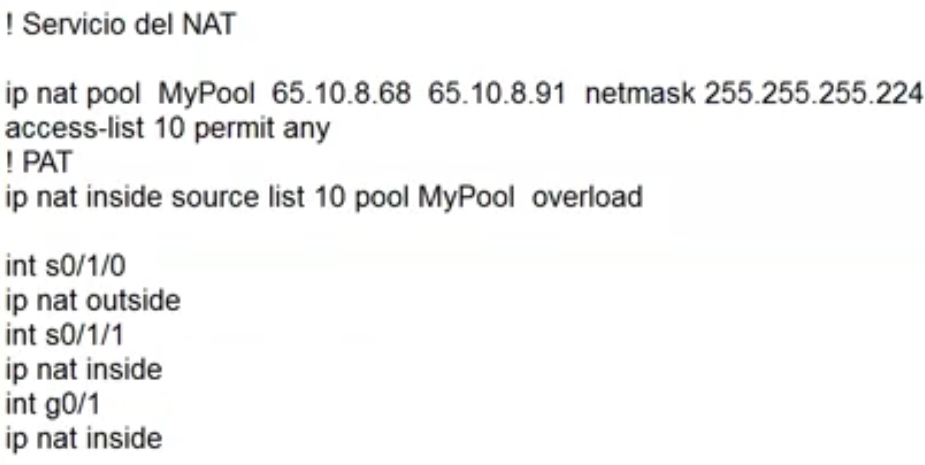
**Int s0/1/1**

**Ip nat inside**

**Int g0/1**

**Ip nat inside**

**Son las acciones que hay que poner en práctica**

****

**Físicamente en el router a, tenemos que configurar las interfaces serial y ethernet son de aplicación inside, si no las configuro los equipos no voy a poder conectarse al exterior. En el simulador es posible se puedan conectar al exterior, en los equipos físicos no.**

**En el router A**

**Int s0/1/0**

**Ip nat inside (tiene que tener la acción)**

**Int g0/1**

**Ip nat inside (tiene que tener la acción)**

**Instalamos el servicio en el router A.**

**Sh run**

**Ip helper**

**Ip nat inside (para que el nateo se pueda ejecutar)**

**Se copia configuración en router b.**

**Hay que checar si traducción sale.**

**Hacer pruebas de conectividad.**

**Laptop subred verde acceso web a servidor externo 132.254.89.1**

**Laptop1 de amarilla acceso web a servidor externo 132.254.89.1**

**NAT implica dirección ip privada a dirección ip pública.**

**EN una red doméstica la dirección que te llega es una IP dinámica, no tienes control de que dirección tienes. Cuantos pueden salir a web todos.**

**Netstat en comand prompt (cmd)**

**Control c**

****

**Si me conecto con un servicio**

**Tengo la ip de mi computadora, te conectas con el exterior a la dirección 193.123.146.149, si habláramos de la capa 3 del modelo OSI, tenemos direccionamiento IP origen e IP destino, si hablamos de la capa 4 del modelo OSI, necesitamos puerto origen y puerto destino. El puerto origen de mi host es un número aleatorio arriba de 1024. La asignación de esos puertos es dinámica. Puedo tener 65535 puertos distingos en mi compu (2 a la 16) Una única dirección ip de salida soporta 65 535 conexiones.**

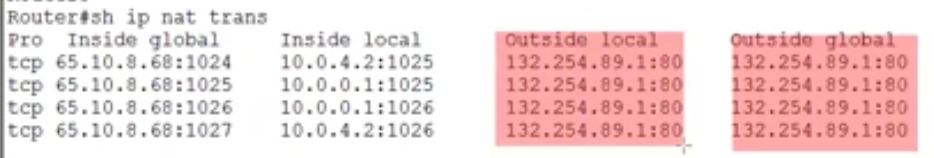
**El puerto del cliente es dinámico. El cliente genera el puerto de conexión de forma dinámica. El servidor establece de forma preestablecida su puerto.**

****

**Hay que realizar laboratorios de NAT y PAT.**

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

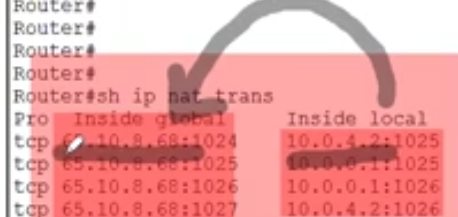
**Se muestra el protocolo que se está utilizando, la dirección interna que lo está utilizando, el puerto dinámico que se generó, una dirección ip local interna (la dirección IP privada), una dirección ouside que es con quien me quiero comunicar. En este ejemplo no hay traducciones en el direccionamiento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

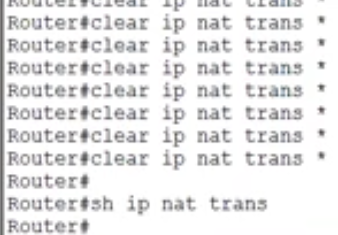
****

**En mi red local, el direccionamiento local corresponde con direcciones 10.x.x.x y el direccionamiento externo toma las direcciones 65.10.8.68 y estos son los puertos que tomó prestados para salir.**

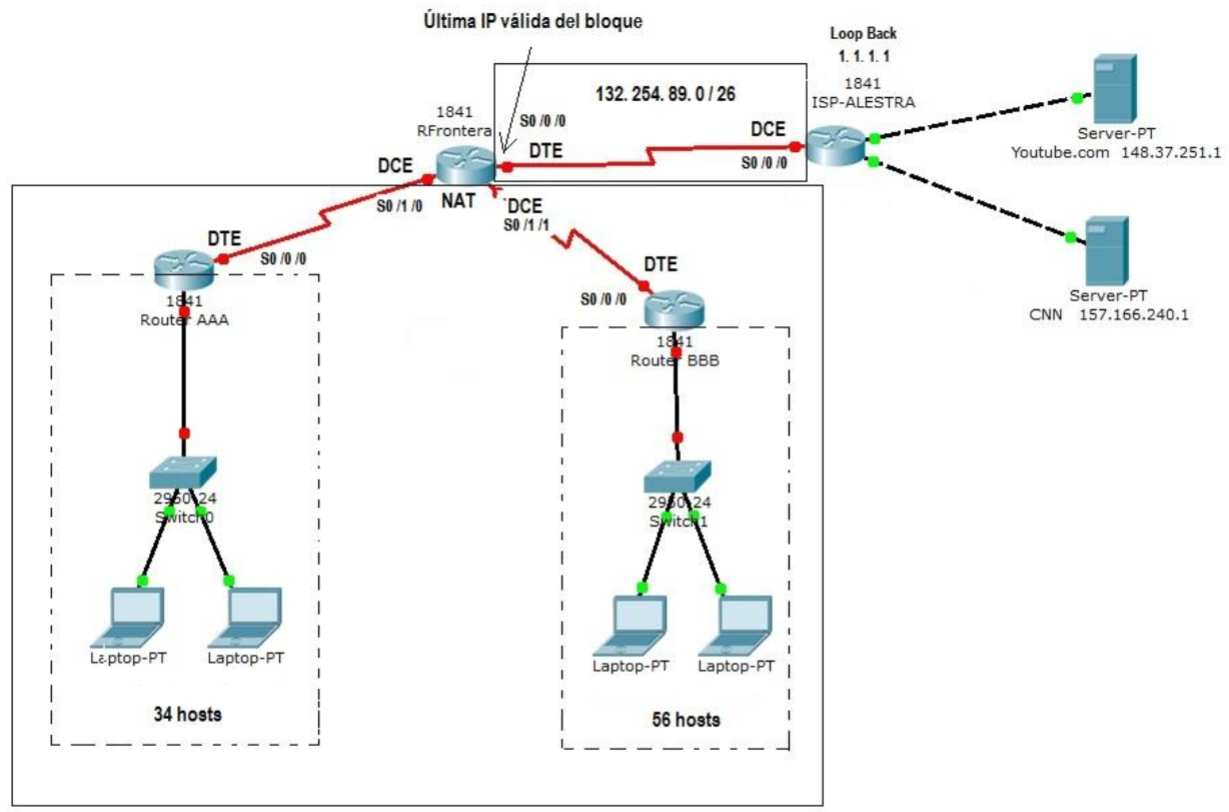
**Las primeras dos columnas es lo que se produce internamente (el NAT se encuentra en las primeras dos columnas pasa de direccionamiento privado a direccionamiento público), las últimas columnas son lo que estamos contactando.**

**Como lo hace toma direcciones privadas y las convierte a públicas dentro del pool permitido (.68, .69, etc). Por cada IP pública tiene 2 a la 16 combinaciones distintas, para hacer un mapeo de una dirección hacia muchas direcciones internas, por eso es PAT.**

****

****

**Limpiar clear ip nat trans varias veces y se borra la tabla de traducciones. La tabla se vuelve a llenar cuando contactamos externamente al servidor. Tiene un tiempo de vida esta tabla, y se limpia automáticamente cuando ya no haya interacción entre una estación local y una remota.**

****