



# NAT Y PAT

Traducción de direcciones IP y Puertos



# Índice

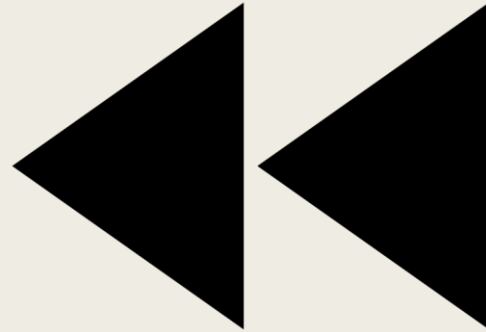
- Modelo Classful/Classless - Direcciones IP Privadas / Públicas
- Introducción al NAT y su terminología
- NAT estático
- Terminología CISCO para NAT: Inside Local, Inside Global, Outside Local / Global
- Práctica de NAT estático con PacketTracer
- PAT Estático - Port Forwarding
- Práctica de PAT estático con PacketTracer
- PAT dinámico
- Práctica de PAT dinámico con PacketTracer

# MODELO CLASSFUL/CLASSLESS

- DIRECCIONES IP PRIVADAS /  
PÚBLICAS

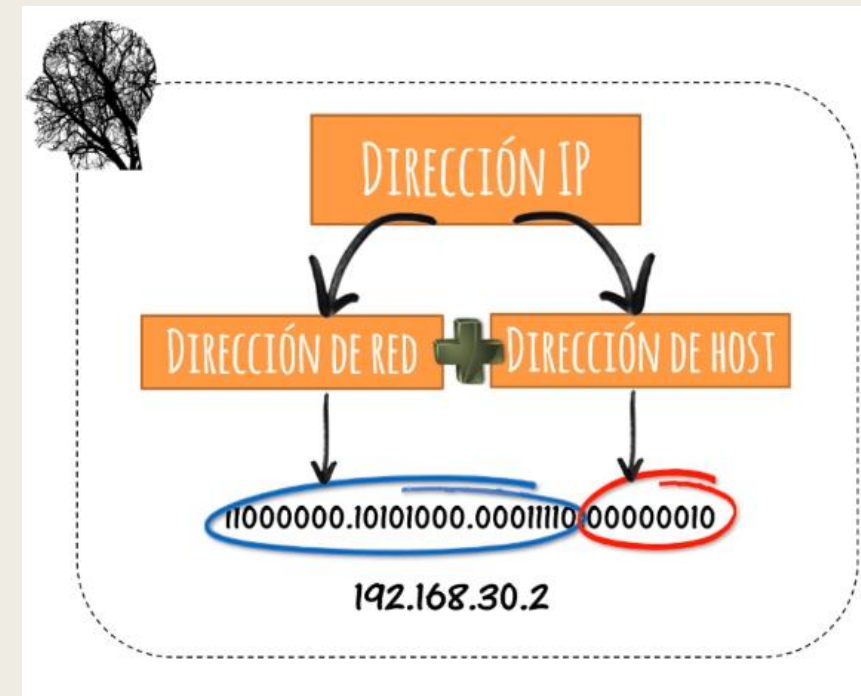
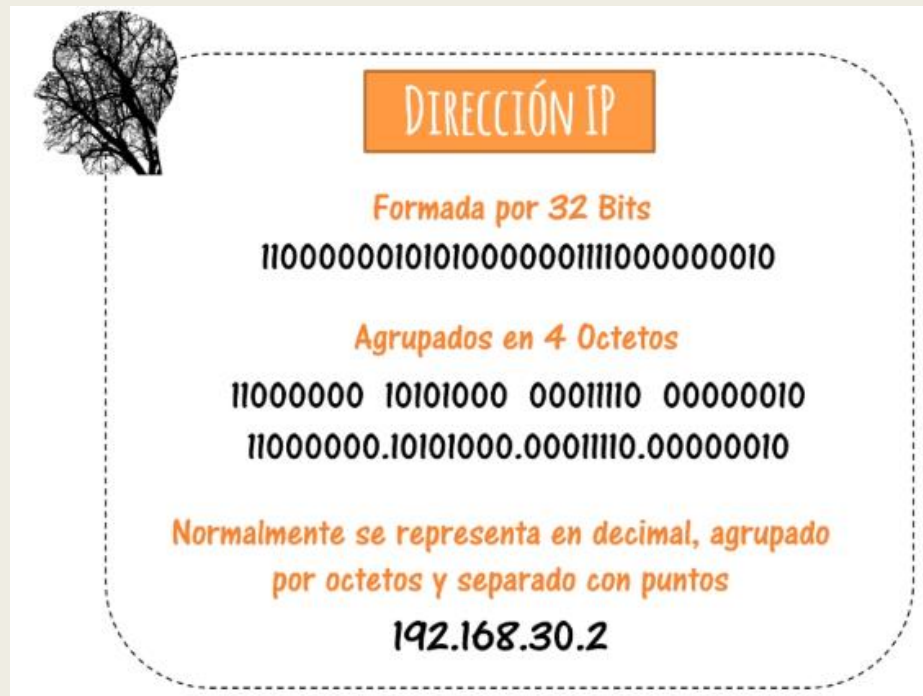
# Recordatorio para poder trabajar

- Vamos a dedicar esta sección a repasar algunos conceptos de direccionamiento IP y así poder comprender mejor los conceptos de NAT y PAT.



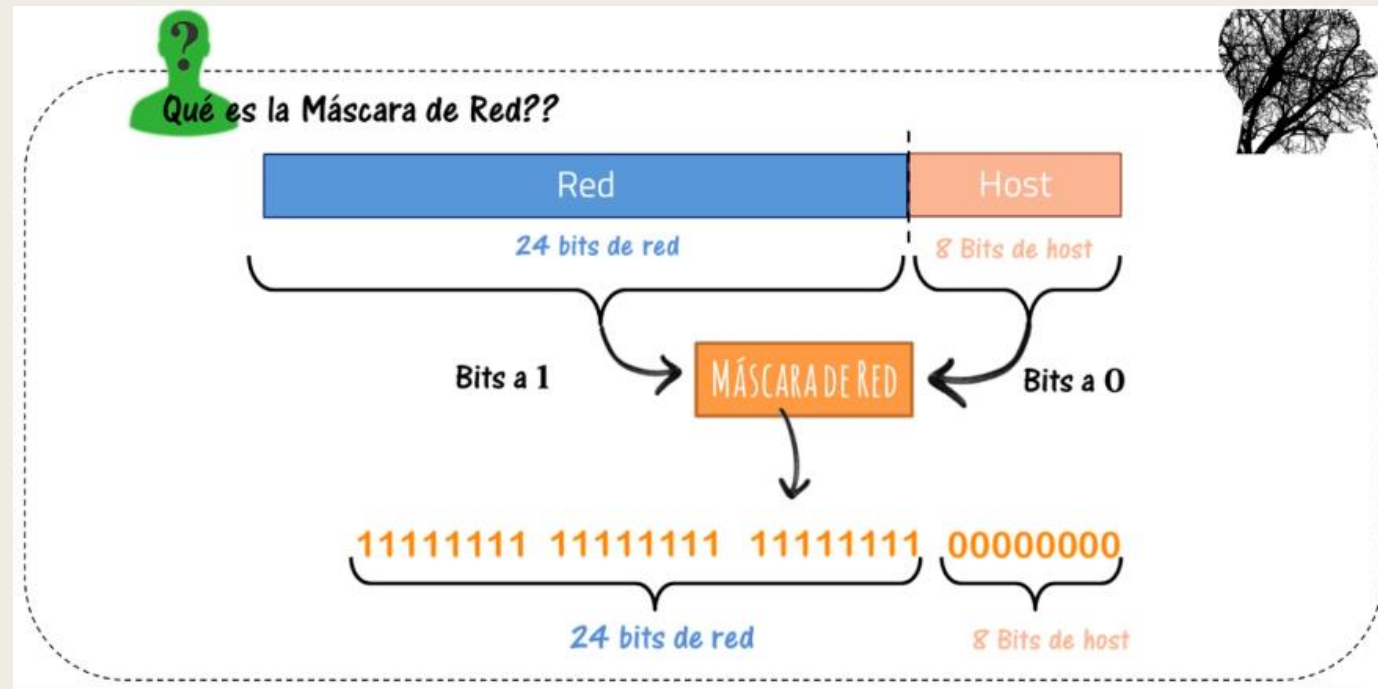
# Dirección IP

- Ya conocemos que las direcciones IPv4 se forman por 32 bits repartidos en 4 octetos. Y se expresan en formato decimal.
- Cada dirección IPv4 tiene una porción de red y una porción de host.



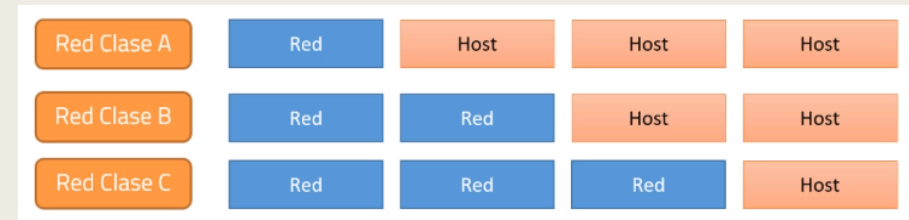
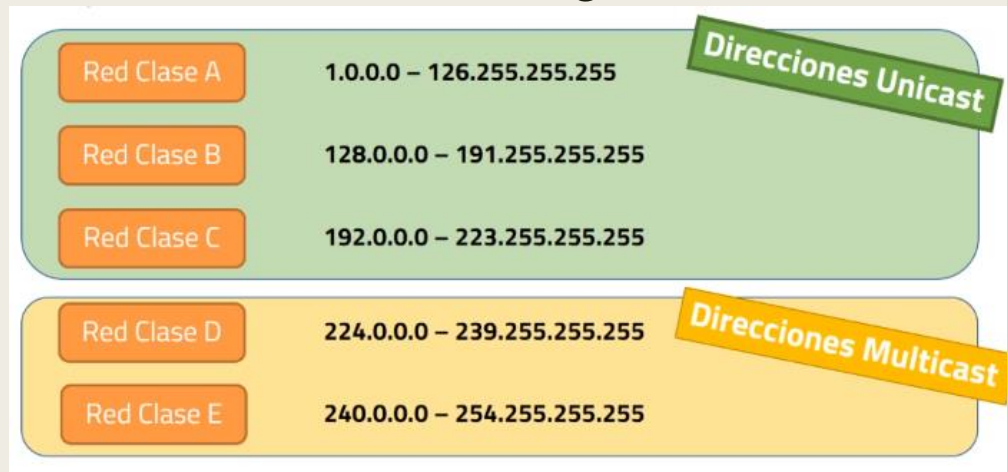
# Máscara de red

- Para determinar qué porción es de red y qué porción es de host, se utiliza la máscara de red.
- La máscara de red tiene el formato de una IP pero está formada por una serie de bits a 1 y otra de 0 (que no se entremezclan)
- Si hacemos comparación binaria de máscara de red con IPv4...
  - *Porción a 1 → porción de red*
  - *Porción a 0 → porción de host*



# Classful vs Classless 1 / 2

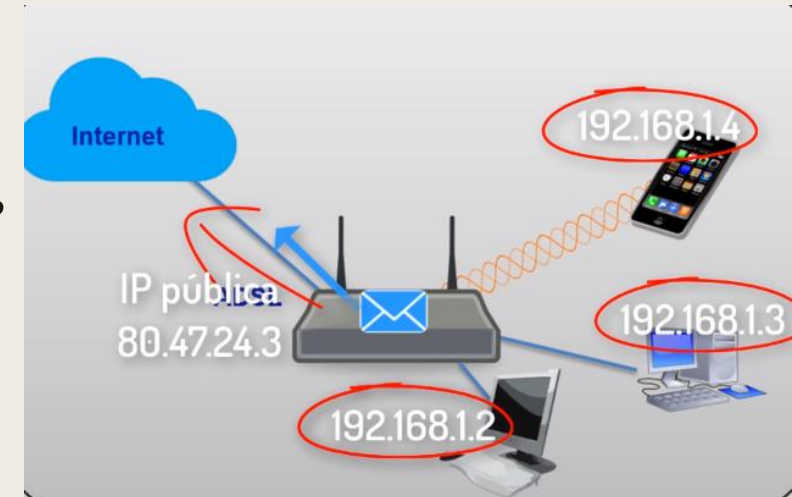
- Antiguamente las redes IP se dividían en clases → Modelo Classful
  - *La máscara era siempre /8 /16 /24 y podía no venir explícita ya que se sobreentendía según la IPv4.*



- Este modelo era muy ineficiente dado que asignaba octetos enteros, y acabó en un agotamiento de las direcciones IP disponibles.
- Hubo que buscar una solución → **Modelo Classless**
- El modelo classless permite asignar redes con máscaras no limitadas a /8 /16 /24

# Classful vs Classless 2/2

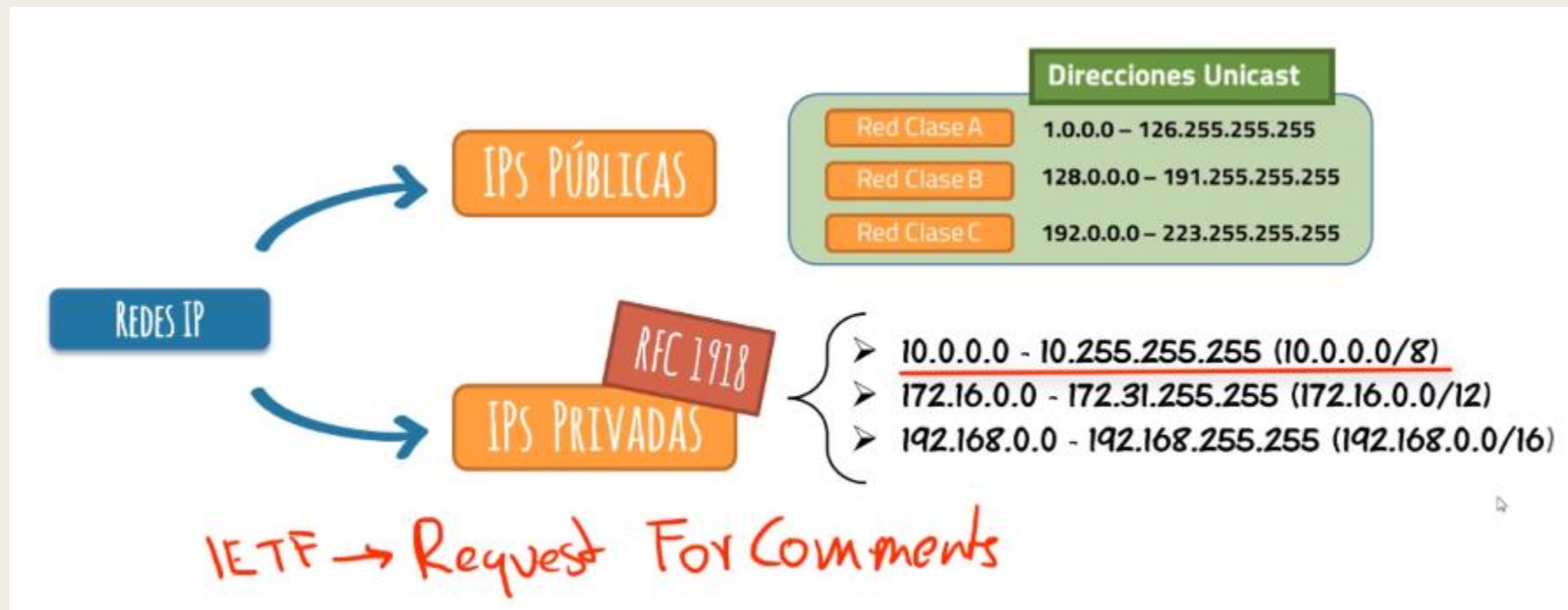
- Con el modelo Classless aparecieron las **direcciones IP públicas y privadas**.
  - *Con classful todas las direcciones eran públicas.*
- Con IPs privadas, cada empresa puede tener tantas direcciones como necesite en su organización, solo que estas direcciones no tienen acceso directo a internet.
  - *Al no salir a internet, estas direcciones pueden repetirse en muchas redes. Por eso todos en casa tenemos por ejemplo la red 192.168.1.0*
- Con el uso de una única IP pública, todos los equipos de la red con IPs privadas pueden salir al exterior.
  - *Para hacer esto, las direcciones se traducen de IP privada a IP pública.*
- El proceso de traducción de IPs privadas a públicas recibe el nombre de **NAT (Network Address Translation)**





# Rangos de IPs públicas y privadas

- Recordemos que el modelo classful está obsoleto y no se usa, pero los términos sí se siguen utilizando en muchas ocasiones.
- Recordemos también que las IP privadas NO son enrutables en internet.



# INTRODUCCIÓN AL NAT Y SU TERMINOLOGÍA



# Introducción

- En esta sección vamos a ver cómo funciona NAT.
- Como ya mencionamos en la sección anterior:
- NAT son las siglas de Network Address Translation
- Tradicionalmente se ha utilizado para traducir direcciones IP privadas a públicas
  - *y viceversa.*

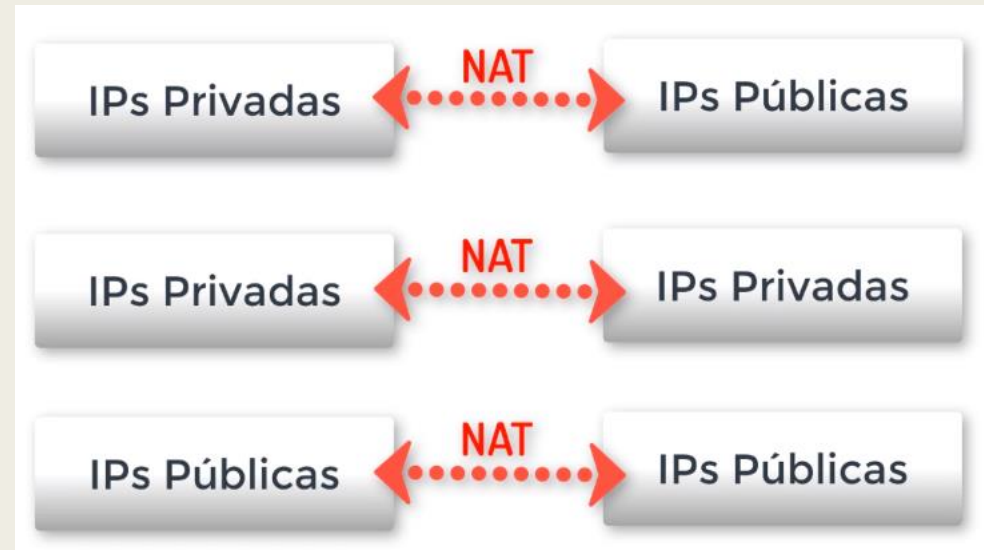


- Recordemos que el motivo de esto era debido a que las IPs públicas son limitadas, pero las IPs privadas, al ser reutilizables en cada red, son infinitas.

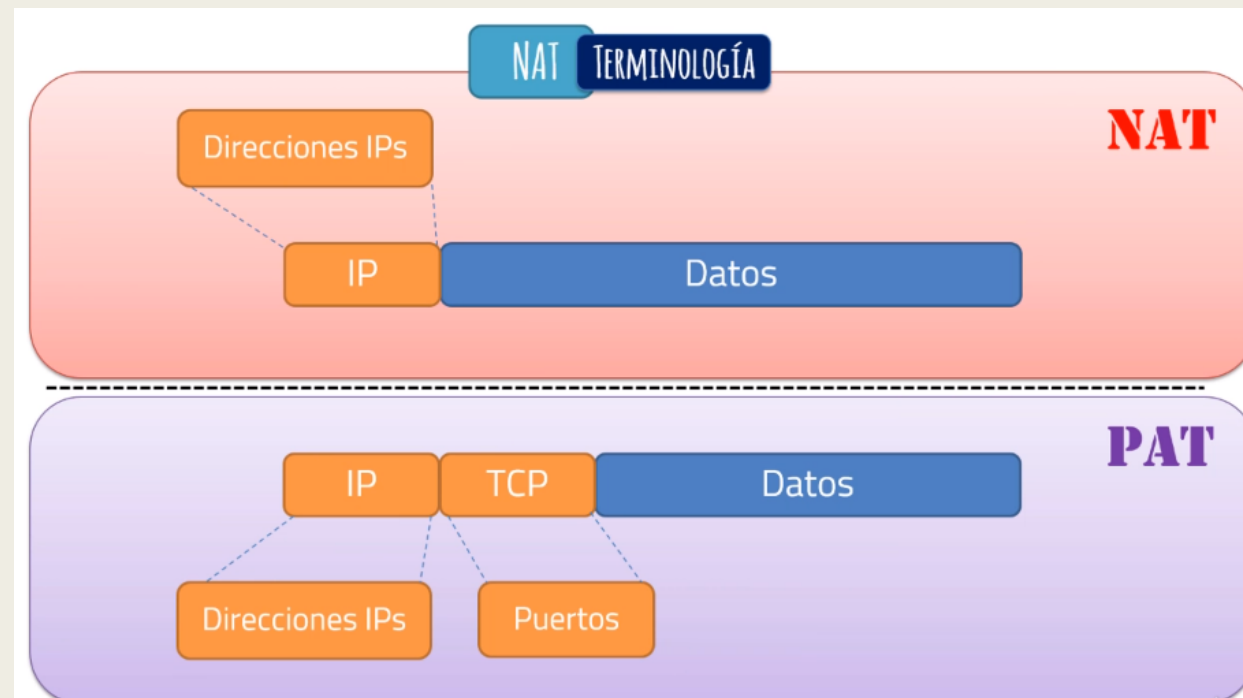
# NAT no se limita a



- Aunque NAT ha sido tradicionalmente usado para traducir IPs privadas a públicas y viceversa, no hay ninguna norma que lo limite solo a esto.
- NAT solo traduce unas IPs por otras, no importa si son públicas o privadas.
- De modo que lo siguiente es posible con NAT:



# Terminología



- Es posible que aparte de NAT, hayamos escuchado también PAT.

- Las siglas de PAT son Port Address Translation.

- A diferencia de NAT, que solo traduce direcciones IP

- PAT traduce direcciones IP + Puertos

- Ejemplo:

- Privada → 192.168.1.1 ↔ 10.10.1.34 ← Pública

- Privada → 192.168.1.1 : 1000 ↔ 10.10.1.34 : 1900 ← Pública

Los puertos en NAT no se involucran, pero siguen existiendo

Como NAT modifica IPs, solo actúa sobre la Capa 3.

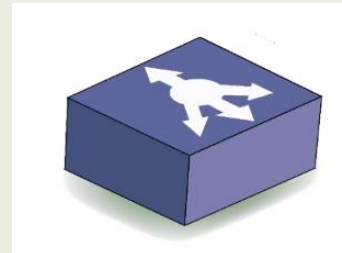
Pero PAT al modificar IPs y puertos, actúa sobre la Capa 3 y 4

# ¿Quién realiza el NAT / PAT?

- Durante el curso veremos cómo hacerlo con ROUTERS.



- Pero no es exclusivo de los routers, dado que los Firewalls, los balanceadores de carga y otros equipos de red pueden hacer NAT y PAT.



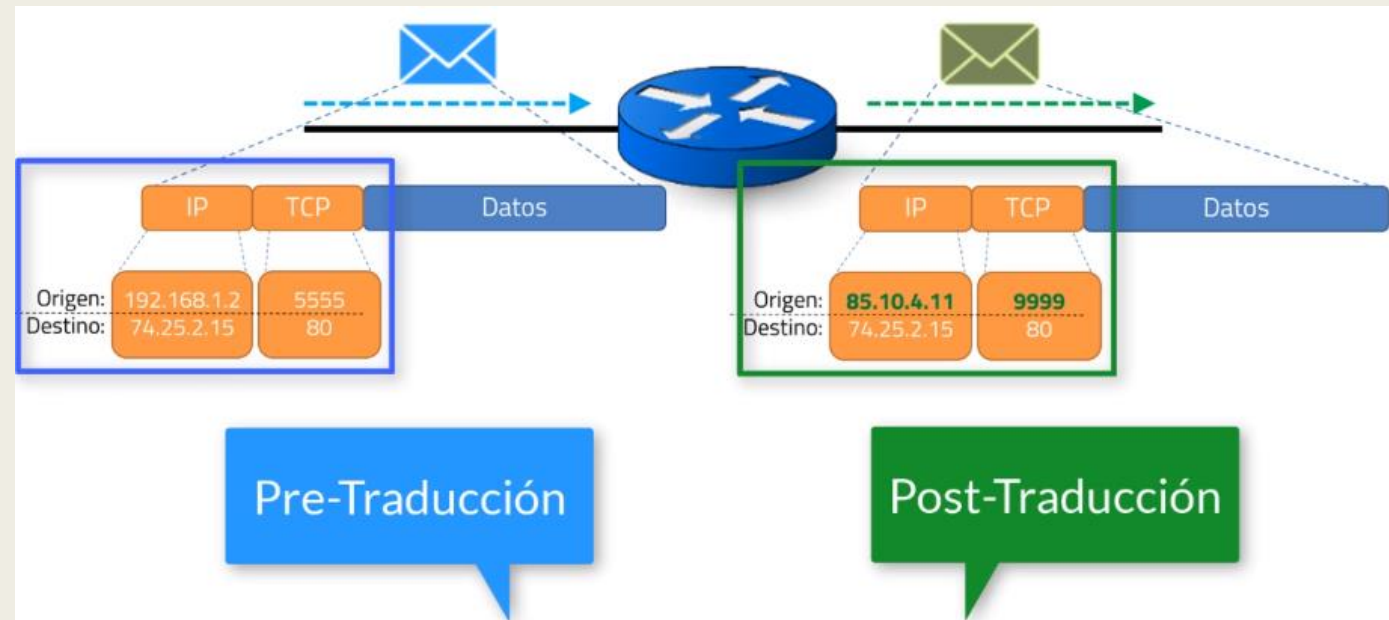
# Tipos de NAT y PAT: Estático y Dinámico

- Si los valores que toman las traducciones los ha definido de forma fija previamente el administrador, hablamos de NAT y PAT estático.
- Si los valores de las traducciones los ha seleccionado el equipo de red de forma aleatoria o que no podemos predecir, hablamos de NAT y PAT dinámico.



# Breve inciso para facilitar las explicaciones

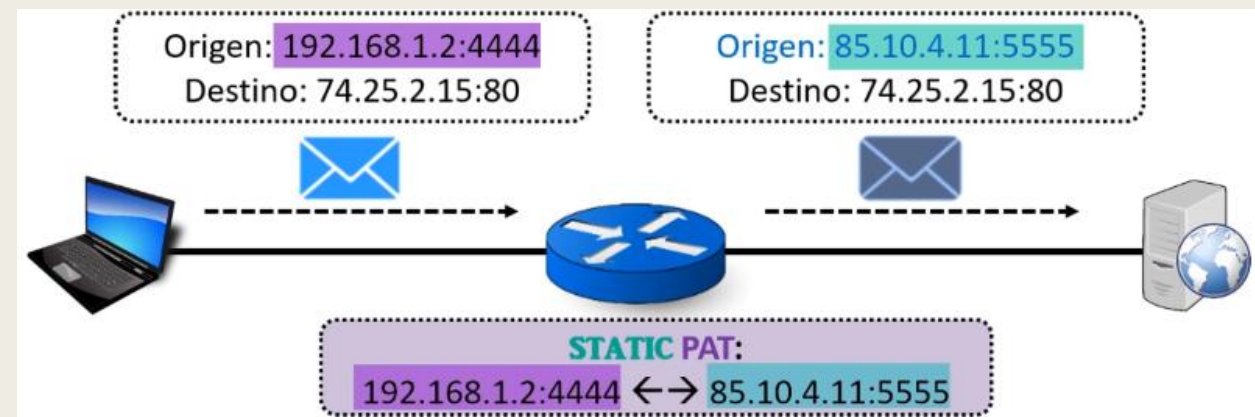
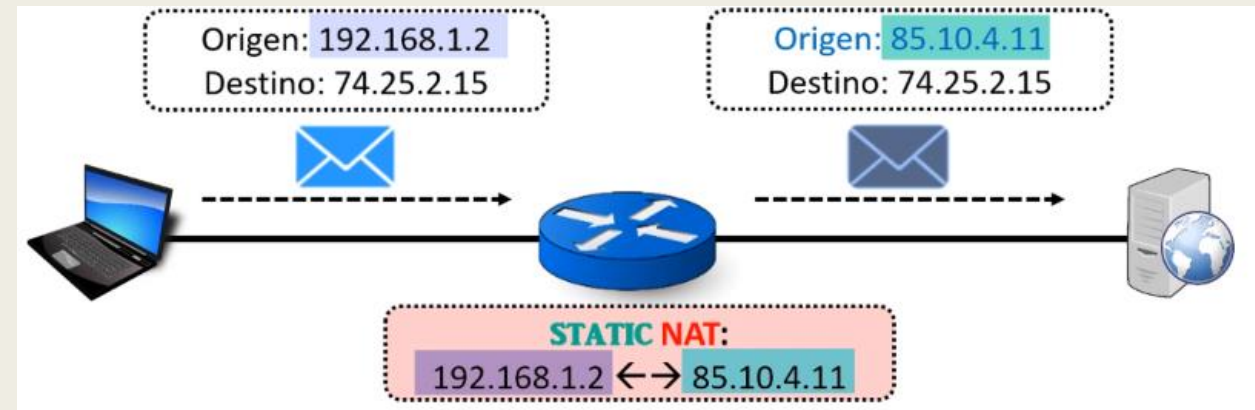
- Cuando hablemos de valores Post-Traducción, a partir de ahora nos referiremos a los valores después de haberse hecho la conversión de valores.
- Cuando hablemos de valores Pre-Traducción, a partir de ahora nos referiremos a los valores antes de haberse hecho la conversión de valores.





# Ejemplo de traducción ESTÁTICA

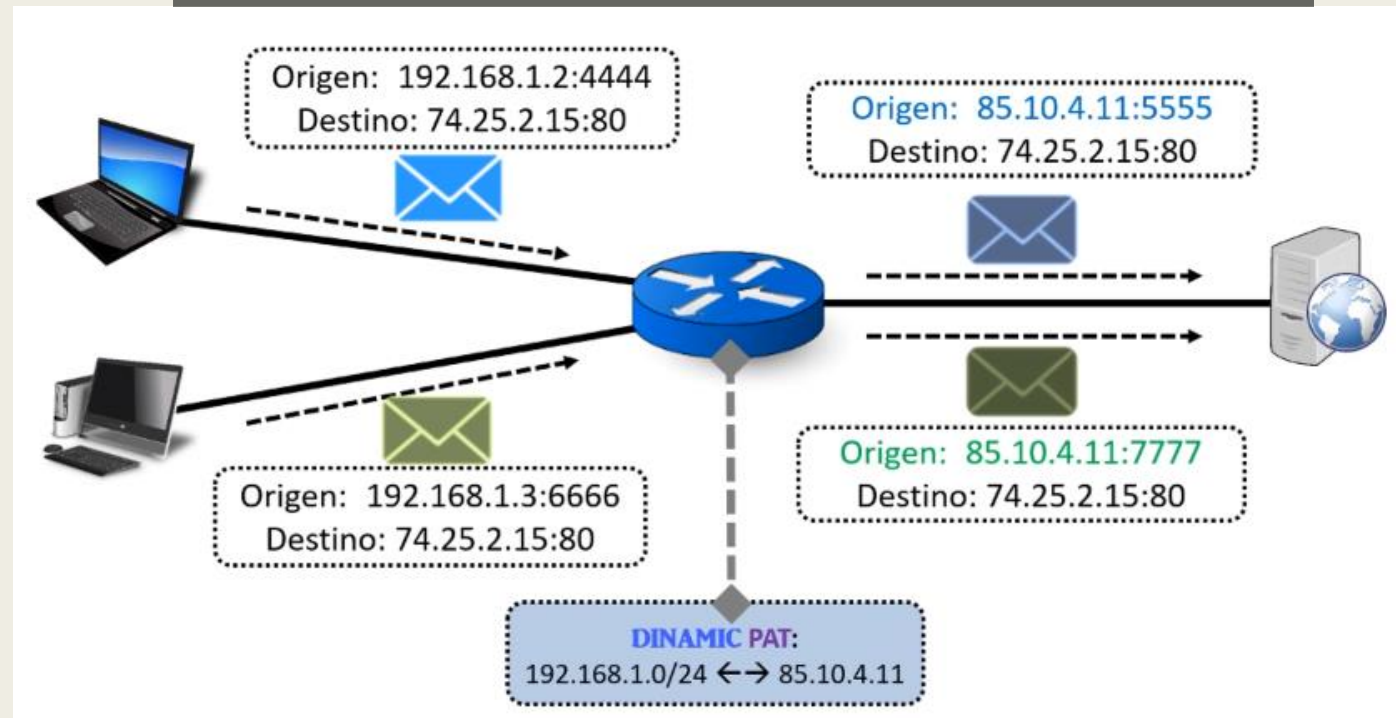
- A este tipo de traducciones se les llama One-to-One.
  - *Porque una dirección siempre se asocia a otra de forma fija.*
  - *Como ya hemos visto, puede ser una dirección a otra, o una dirección + puerto a otra dirección + puerto.*
- Podemos asociar la traducción estática con la palabra **fija**.
  - *Porque siempre va a traducir los mismos valores pre-traducción a los mismos valores post-traducción.*



# Traducciones de tipo DINÁMICO

- Con las traducciones de tipo dinámico, que se dan en PAT principalmente.
- En este caso, es el equipo de red el que asigna los valores de IP y puerto de forma aleatoria en función de unos rangos dados.
- El administrador lo que define es un rango de direcciones IP posibles y un rango de puertos posibles.
- Es decir, hasta el momento que se haga la traducción, no se sabe qué valores post-traducción tendrá un equipo.

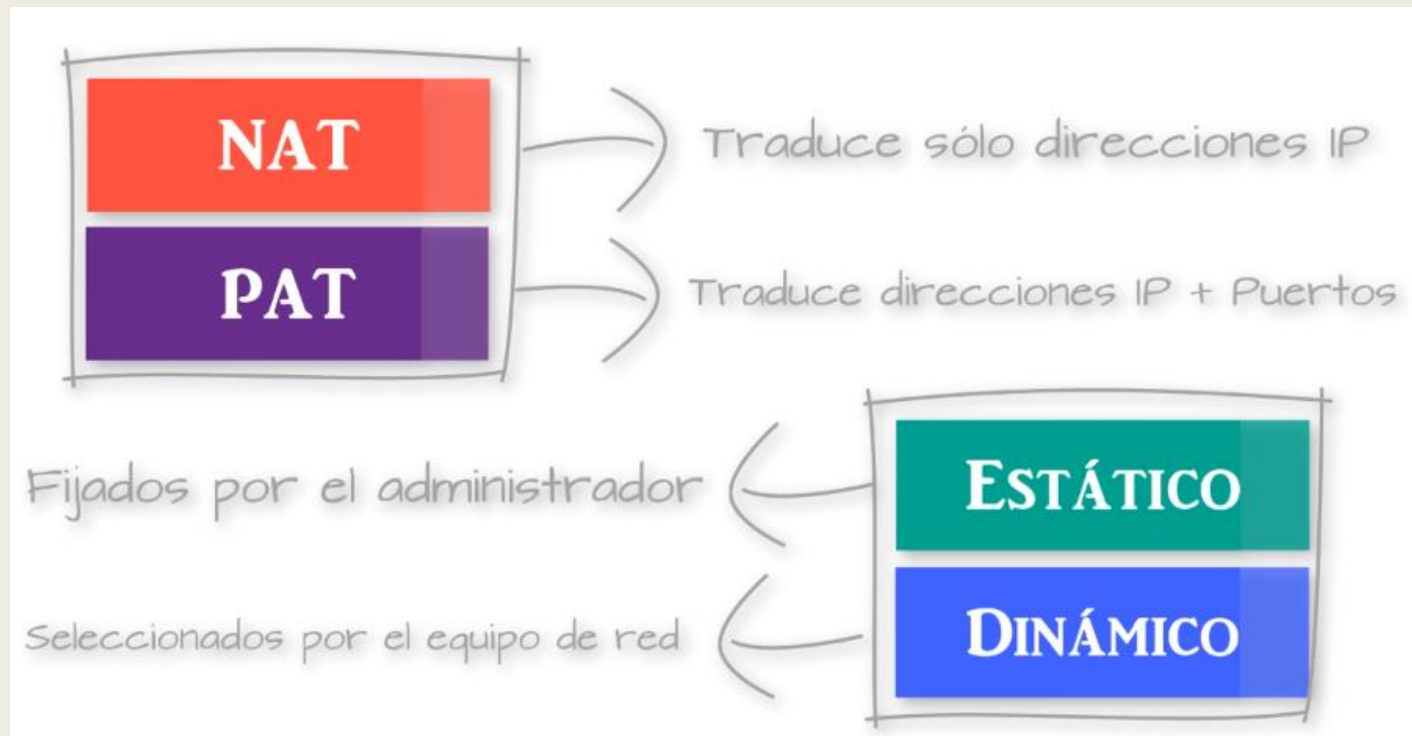
## Traducción One-to-Many



En este ejemplo, dos equipos salen con la misma IP, pero el PAT asigna puertos distintos entre un rango

# NAT y PAT combinado con Estático y Dinámico

- En las siguientes secciones veremos en detalle las distintas combinaciones de los conceptos que hemos visto:



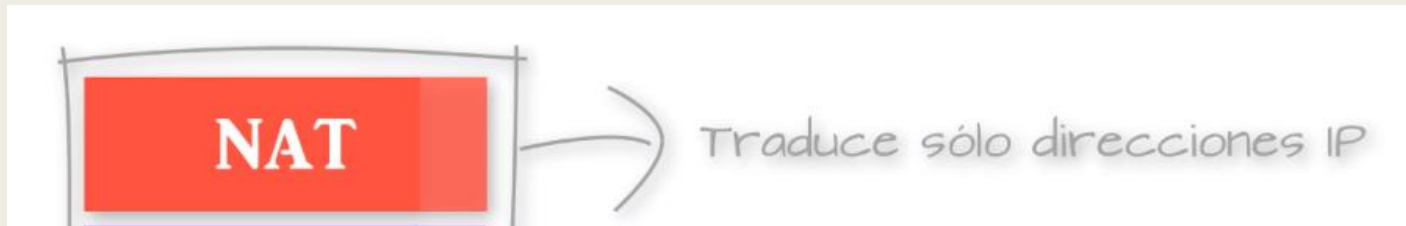
NAT	ESTÁTICO
PAT	ESTÁTICO
PAT	DINÁMICO
NAT	DINÁMICO

NAT ESTÁTICO




# Introducción

- Vamos a empezar con el NAT ESTÁTICO
- Es el más sencillo de todos los casos expuestos



NAT	ESTÁTICO
PAT	ESTÁTICO
PAT	DINÁMICO
NAT	DINÁMICO

# Tabla de traducciones



PRE-TRADUCCIÓN				POST-TRADUCCIÓN			
IP Origen	Puerto Origen	IP Destino	Puerto Destino	IP Origen	Puerto Origen	IP Destino	Puerto Destino
10.1.1.20	4512	84.125.3.9	80	42.4.4.10	4512	84.125.3.9	80
10.1.1.23	23012	200.74.15.68	443	42.4.4.11	23012	200.74.15.68	443
10.20.20.58	9651	4.4.4.2	53	42.4.4.20	14554	4.2.2.2	53
...	...	...	...	...	...	...	...

- La traducción de las direcciones IP y los puertos se configuran en la TABLA DE TRADUCCIONES.
- En el caso de NAT estático, todas las traducciones IP estarán en esta tabla.
  - *El puerto no variará.*
- De momento mostraremos la tabla de traducciones de forma simplificada para facilitar la comprensión:

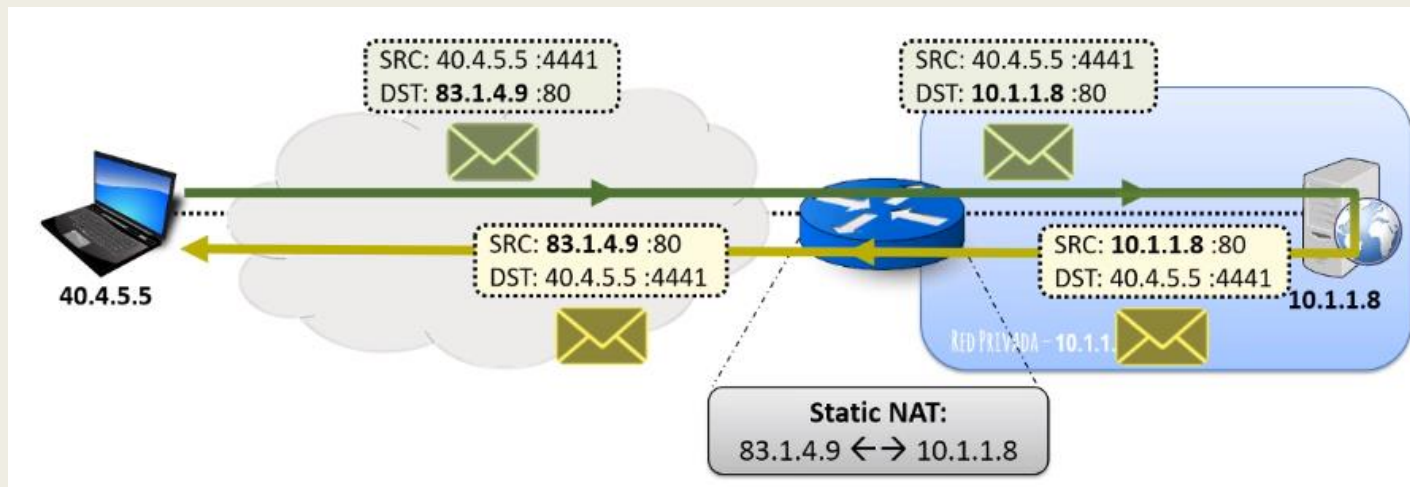




# Ejemplo común NAT estático

- Un ejemplo típico de NAT estático es el acceso a un servidor web.
- A continuación se muestra el proceso de envío de una solicitud de un equipo a un servidor web mediante NAT estático:

One-to-One



SRC = Source = Origen

DST = Destination = Destino

Comunicación Bidireccional:  
Tanto el origen como el destino pueden iniciar la conversación.

- Cuando el PC envía la información, lo hace a la IP pública de la red IP del servidor, que se traducirá a la privada al llegar al router destino.
- Por otro lado, cuando el servidor responde, su IP de origen es la que será traducida dado que debe salir a internet con la pública.

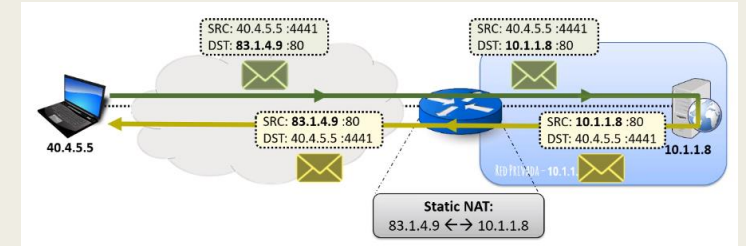
# ¿Se usa hoy en día NAT Estático?

- NAT Estático apenas se usa.
- ¿Por qué?
- Porque no se ahorran direcciones IP.
- Cada equipo que quiera salir a internet necesitaría una IP pública para asignársela de manera estática.
- Teniendo en cuenta que cada vez hay menos direcciones IP, no es una solución óptima.
- **PERO** es posible encontrarlo en alguna red o en algún momento nos interese configurarlo en alguna red.
  - *Y veremos cómo configurarlo en un router CISCO.*



**TERMINOLOGÍA CISCO PARA NAT:  
INSIDE LOCAL, INSIDE GLOBAL,  
OUTSIDE LOCAL / GLOBAL**

# Introducción



- En esta sección vamos a cubrir la terminología que utiliza CISCO para denominar a las diferentes direcciones que encontraremos en el proceso de traducción.

- Hasta ahora, hemos hablado de:

- *Dirección IP origen* SRC: 40.4.5.5 :4441
- *Dirección IP destino* DST: 83.1.4.9 :80

- También de valores:

- *Pre-traducción*
- *Post-traducción*



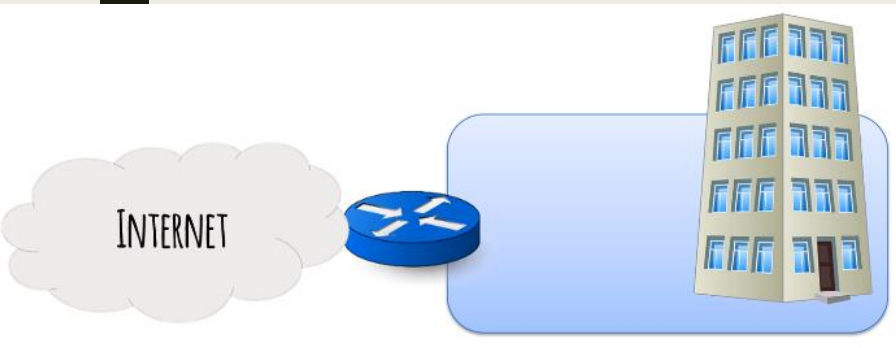
- Pero el proceso de traducción tiene una ida y una vuelta de información, donde son diferentes tanto las IPs de destino como de origen, y si decimos lo siguiente:

**Traducir la IP origen 83.1.4.9 por la 10.1.1.8**

- No es suficientemente preciso.
- Cisco ha establecido una terminología para esto y que no haya ambigüedades.

# CISCO usa 4 conceptos principales

- ★ Inside Local
- ★ Inside Global
- ★ Outside Local
- ★ Outside Global



- Para todos estos conceptos vamos a hablar desde la perspectiva del router.
  - *Vamos a apoyarnos en la imagen de la izquierda.*
- INSIDE / OUTSIDE: Ubicación física del equipo al que pertenece esa dirección.
  - *Inside sería la red interna*
  - *Outside sería internet*
- LOCAL / GLOBAL: Perspectiva desde la que vemos esa dirección.
  - *Hablamos de local al direccionamiento visible desde la perspectiva de la red interna.*
  - *Hablamos de global al direccionamiento visible desde la perspectiva de la red externa.*

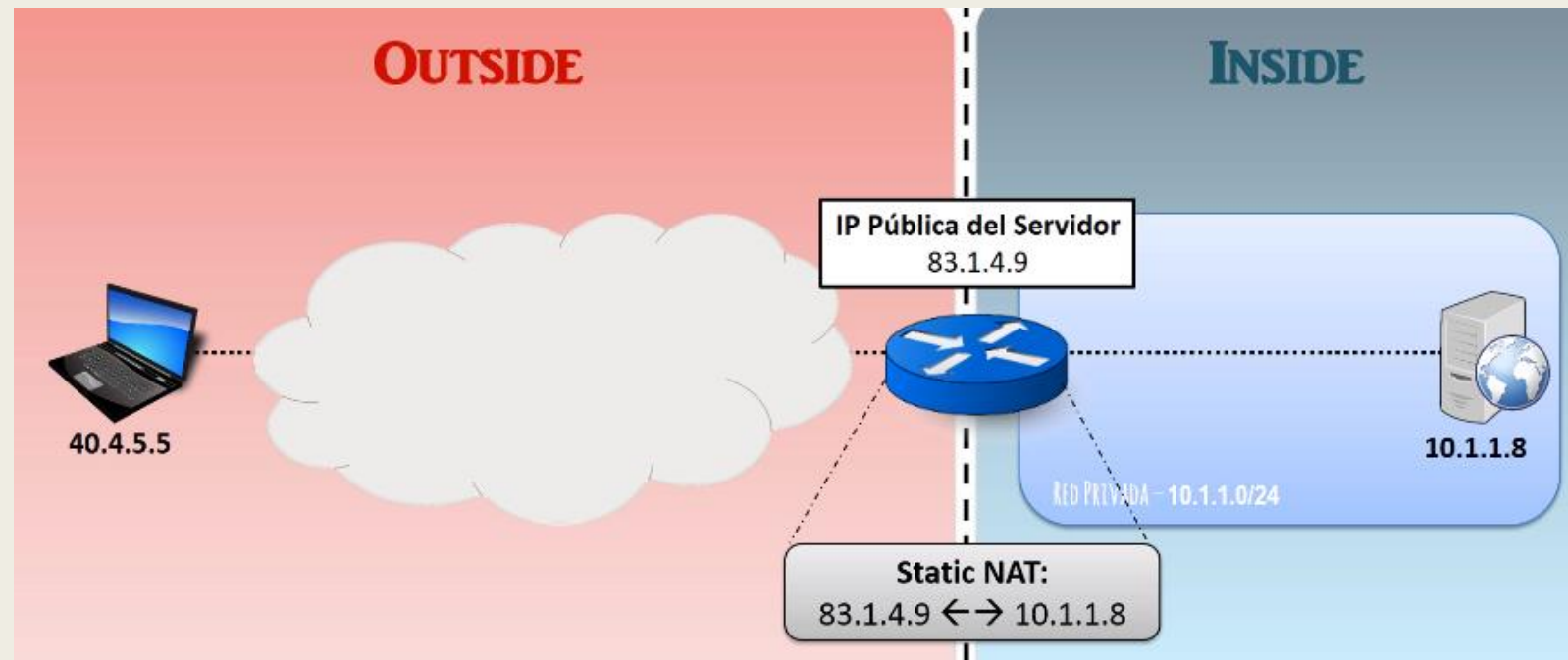
# Ejemplo de uso de la terminología

Recordatorio: TODA ESTA TERMINOLOGÍA ES DESDE LA PERSPECTIVA DE LA RED INTERNA DEL ROUTER

- Inside local: 10.1.1.8
- Inside global: 83.1.4.9
- Outside local: 40.4.5.5
- Outside global: 40.4.5.5

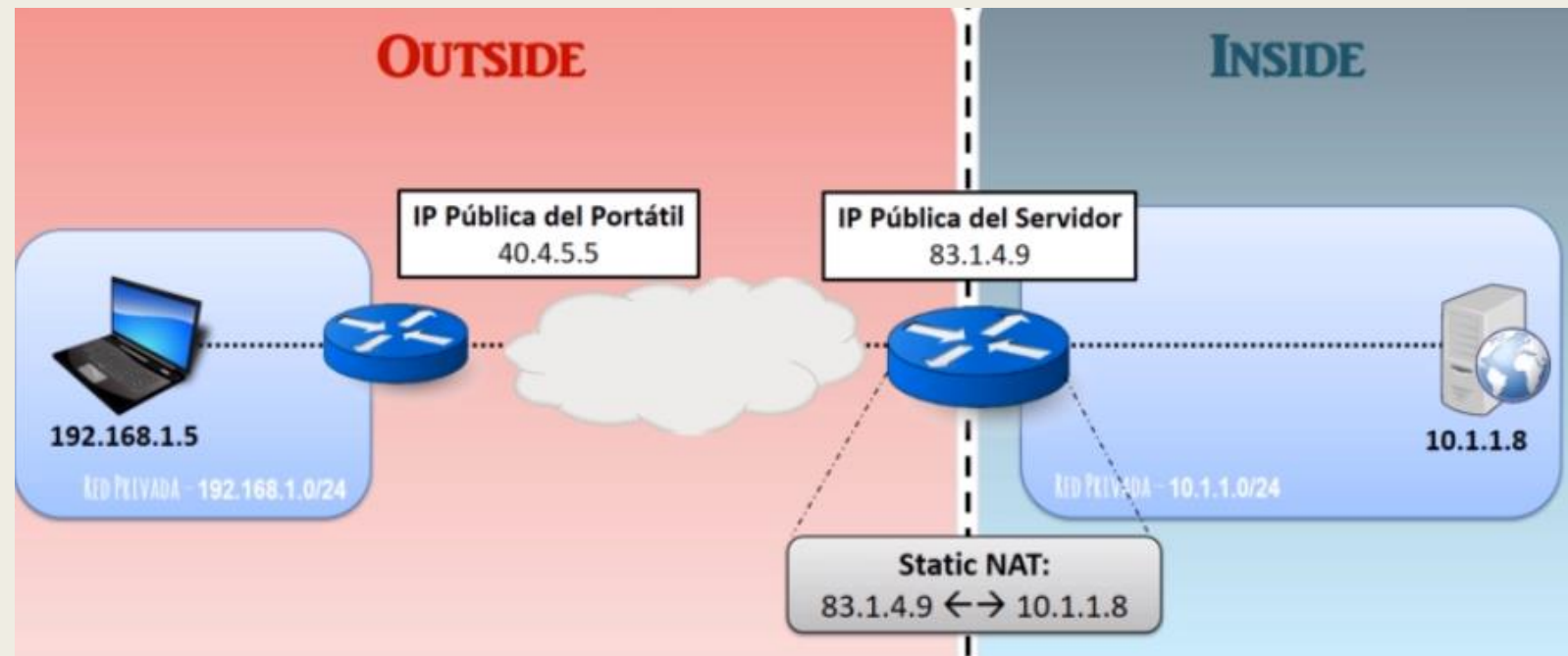
Desde la red interna del router, la IP a la que vamos a llegar y conocemos es 40.4.5.5

Solo en casos más complejos como doble NAT podría ser diferente la outside local y outside global



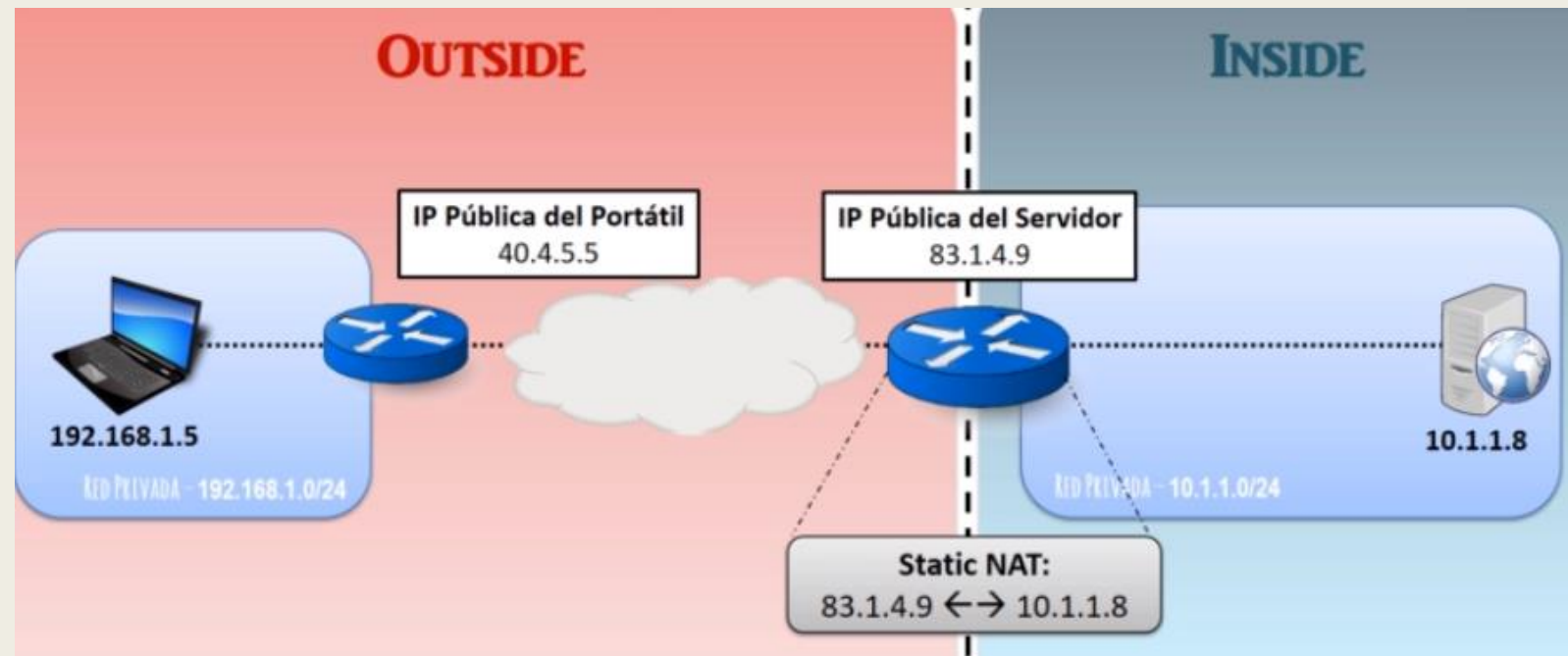
# Otro ejemplo - Pregunta

- Inside local: ????
- Inside global: ????
- Outside local: ????
- Outside global: ????



# Otro ejemplo - Solución

- Inside local: 10.1.1.8
- Inside global: 83.1.4.9
- Outside local: 40.4.5.5
- Outside global: 40.4.5.5
- Se toman exactamente los mismos valores que en el otro ejemplo, porque es la perspectiva de la red interna del router y él no puede conocer la IP local del equipo destino.





# ¿Cómo habría sido la descripción de las IPs sin la terminología CISCO?

La dirección 10.1.1.8 es el valor pretraducción de la dirección origen en el tráfico de salida hacia la red externa, originado por el equipo de la red privada. Y dicha dirección tomará un valor post traducción de 83.1.4.9, que en la respuesta que se recibirá de la red externa, pasará a ser la dirección destino.

- Para cualquier técnico es más sencillo conocer las IPs local y global de inside y outside. Eso junto a saber qué parte es la inside y cuál la outside le permitirá conocer en detalle la red.
- En la siguiente sección veremos cómo se configura un NAT estático.

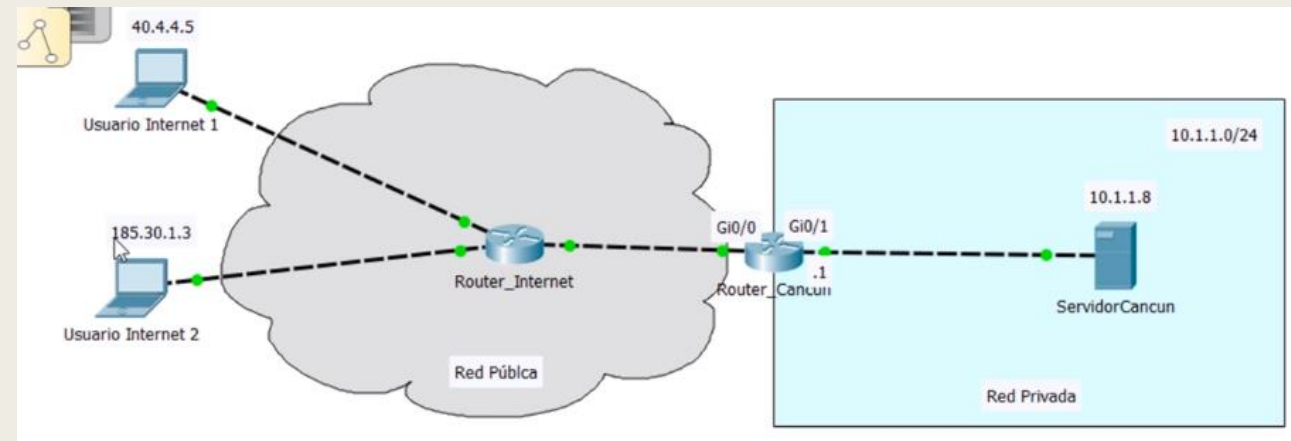
# PRÁCTICA DE NAT ESTÁTICO CON PACKETTRACER



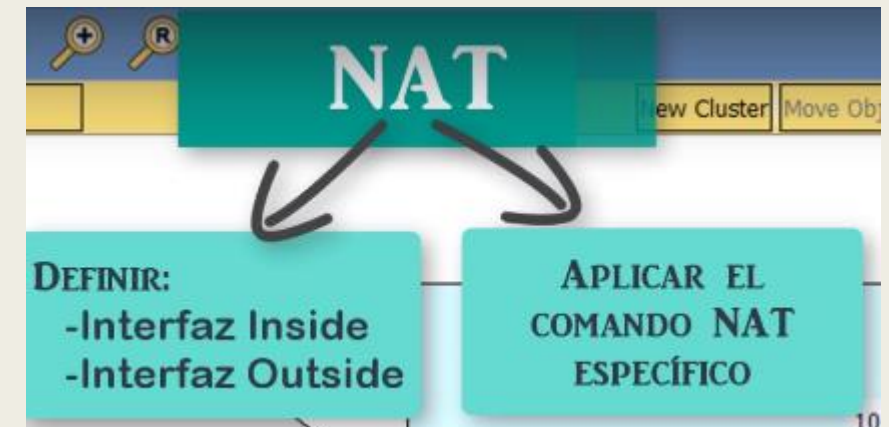


# Introducción

- En esta sección vamos a hacer una práctica de configuración de NAT estático.
- El material base se encuentra para descargar en el aula virtual.
- Router\_internet, usuario internet 1 y usuario internet 2 ya están configurados.



Objetivo: Configurar NAT estático en el Router\_Cancun para hacer visible a Internet al ServidorCancun con la IP pública 83.1.4.9



# Definir interfaz inside y outside



- Para definir en la configuración del router qué interfaz es inside y cuál es outside...
- Para interfaz outside:
  1. *Acceder a la configuración global.*
  2. *Acceder a la interfaz que va a ser outside.*
  3. *Introducir el comando **ip nat outside***
- Para interfaz inside:
  1. *Acceder a la configuración global.*
  2. *Acceder a la interfaz que va a ser outside.*
  3. *Introducir el comando **ip nat outside***
- Si hacemos un show running-config vemos que está aplicado →

```
Router_Cancun(config)#int gigabitEthernet 0/0
Router_Cancun(config-if)#ip nat out
Router_Cancun(config-if)#ip nat outside
Router_Cancun(config-if)#
```

```
Router_Cancun(config)#interface gigabitEthernet 0/1
Router_Cancun(config-if)#ip nat in
Router_Cancun(config-if)#ip nat inside
```

```
interface GigabitEthernet0/0
ip address 2.2.2.2 255.255.255.0
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
```

# Aplicar el comando NAT específico

- Para indicarle al router cómo debe traducir una IP inside en outside, lo haremos así:
  1. Accederemos al modo de configuración global (no entramos a ninguna interfaz).
  2. Usamos el comando: `ip nat inside source static ip_inside_local ip_inside_global`

```
ip nat inside source static 10.1.1.8 83.1.4.9
```

# Consultar la tabla de traducciones

- Para consultar la tabla de traducciones del router, lo haremos desde el modo privilegiado.
- Usaremos el siguiente comando:

```
show ip nat translations
```

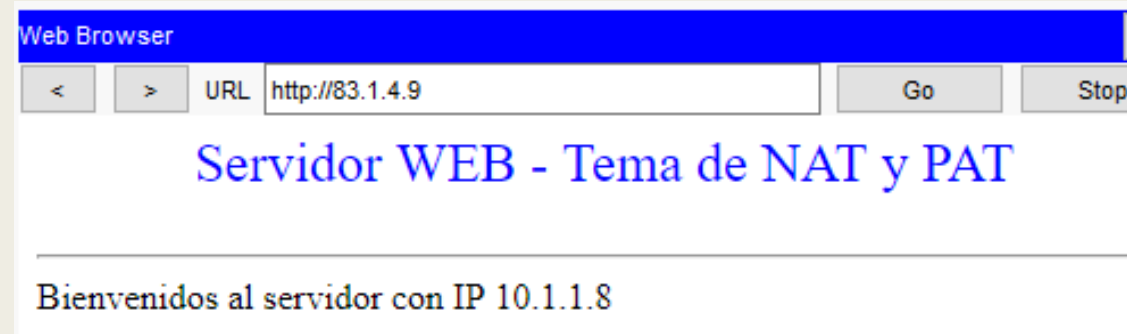
- Y nos mostrará lo siguiente:

```
Router_Cancun#sh ip nat translations
Pro  Inside global      Inside local  Outside local  Outside global
---  83.1.4.9            10.1.1.8     ---           ---
```

- Esto significa que lo que venga de internet con destino la 83.1.4.9, se traducirá a 10.1.1.8 al llegar al router.
  - *Y del mismo modo, lo que vaya a salir del router con 10.1.1.8, se traducirá en el router a 83.1.4.9*

# Probar la conectividad

- En lugar de hacer un ping, como hemos hecho hasta ahora, probaremos una petición web.
- En esta práctica está configurado en el servidor Cancún un servicio web.
- Accedemos al portátil “usuario internet 1” y en desktop, en lugar de aplicaciones, elegimos la opción WEB BROWSER.
- Nos aparecerá un navegador, donde tenemos que poner la IP adecuada:



# Analizando paquetes en la IDA

- Si volvemos a probar la conectividad pero activando el simulador...
- Cuando el paquete llega al router, vemos lo siguiente en las cabeceras:

Layer4	Layer4
Layer 3: IP Header Src. IP: 40.4.4.5, Dest. IP: 83.1.4.9	Layer 3: IP Header Src. IP: 40.4.4.5, Dest. IP: 10.1.1.8
Layer 2: Ethernet II Header 0060.5C37.05B7 >> 0006.2A74.CE05	Layer 2: Ethernet II Header 000D.BD93.1948 >> 000C.CFDA.B746
Layer 1: Port GigabitEthernet0/0	Layer 1: Port(s): GigabitEthernet0/1

- Hace la conversión de direcciones.
- Si consultamos la tabla de traducciones veremos lo siguiente:

Router_Cancun# Router_Cancun#sh ip nat translations				Entradas Dinámicas
Pro	Inside global	Inside local	Outside local	
tcp	83.1.4.9:80	10.1.1.8:80	40.4.4.5:1025	40.4.4.5:1025
tcp	83.1.4.9:80	10.1.1.8:80	40.4.4.5:1026	40.4.4.5:1026
tcp	83.1.4.9:80	10.1.1.8:80	40.4.4.5:1027	40.4.4.5:1027

- Automáticamente el router ha añadido una serie de entradas dinámicas (24h).
- Se han añadido 3, dos de la primera consulta, 1 de la segunda (aún no ha terminado el proceso de consulta de la web).

# Analizando paquetes en la VUELTA

- Cuando el servidor manda la respuesta al ordenador, y paquete pasa por el router, vemos lo siguiente en las capas:

Layer 3: IP Header Src. IP: 10.1.1.8, Dest. IP: 40.4.4.5	Layer 3: IP Header Src. IP: 83.1.4.9, Dest. IP: 40.4.4.5
Layer 2: Ethernet II Header 000C.CFDA.B746 >> 000D.BD93.1948	Layer 2: Ethernet II Header 0006.2A74.CE05 >> 0060.5C37.05B7
Layer 1: Port GigabitEthernet0/1	Layer 1: Port(s): GigabitEthernet0/0

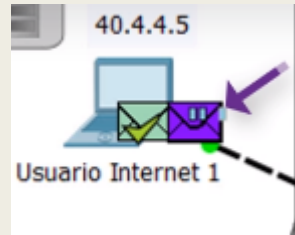
- Vuelve a hacerse la traducción de IPs.
- Si consultamos la tabla de traducciones, en este punto vemos que tiene los mismos valores que antes:

```
Router_Cancun#show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
tcp 83.1.4.9:80         10.1.1.8:80       40.4.4.5:1025     40.4.4.5:1025
tcp 83.1.4.9:80         10.1.1.8:80       40.4.4.5:1026     40.4.4.5:1026
tcp 83.1.4.9:80         10.1.1.8:80       40.4.4.5:1027     40.4.4.5:1027
--- 83.1.4.9           10.1.1.8          ---               ---
```

- Lo que podemos apreciar en la tabla de traducciones es que se lanzan varias peticiones TCP, y en ellas, lo que varía es el puerto, así es como se pueden distinguir.



# Extra: El segundo envío de paquete



- Después de enviarse el primer paquete, vemos que se lanza un segundo paquete.
- Este segundo paquete se corresponde con la petición HTTP, es aquí donde nos enviarán el contenido de la página web.
- ¿Y el primero qué tenía entonces?
- El primero se correspondía con el Establecimiento de la conexión TCP.
  - *El 3-way-handshake que estudiamos en fundamentos de la capa 4.*
    - El paquete que envía el usuario internet 1 es el SYN
    - La respuesta del servidor es el SYN+ACK
    - Y el siguiente paquete ya contiene la petición HTTP y el ACK
  - *Si le damos a “siguiente” vamos comprobando cómo se van enviando numerosos paquetes hasta completar la carga de la web.*

```
Router_Cancun#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global	
tcp	83.1.4.9:80	10.1.1.8:80	40.4.4.5:1025	40.4.4.5:1025	Acceso HTTP-1
tcp	83.1.4.9:80	10.1.1.8:80	40.4.4.5:1026	40.4.4.5:1026	
tcp	83.1.4.9:80	10.1.1.8:80	40.4.4.5:1027	40.4.4.5:1027	Acceso HTTP-2
tcp	83.1.4.9:80	10.1.1.8:80	40.4.4.5:1028	40.4.4.5:1028	



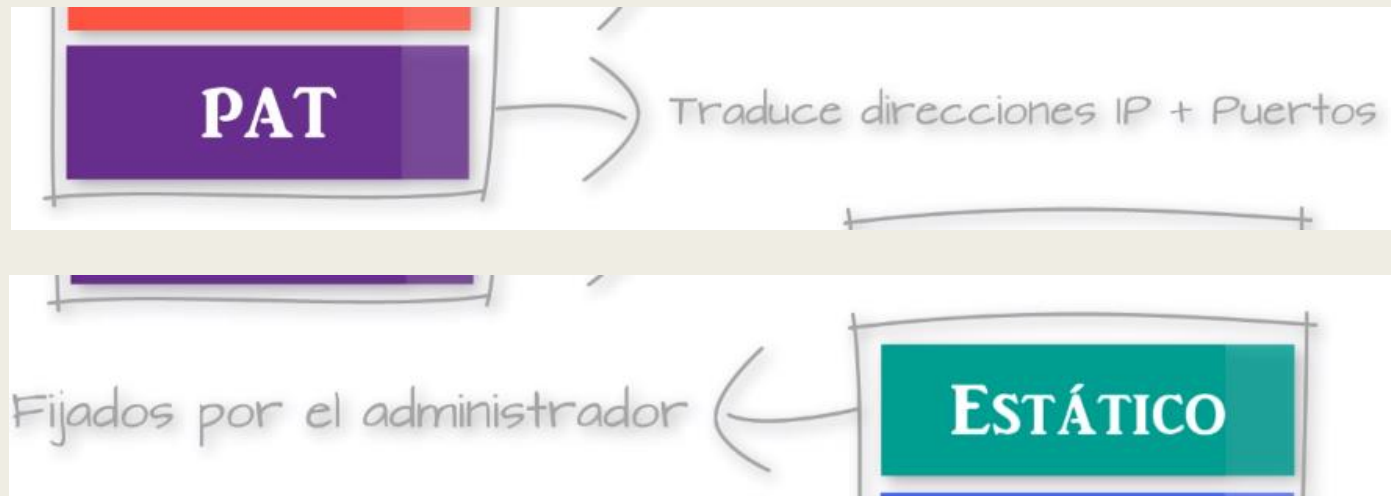
# PAT ESTÁTICO - PORT FORWARDING



# Introducción

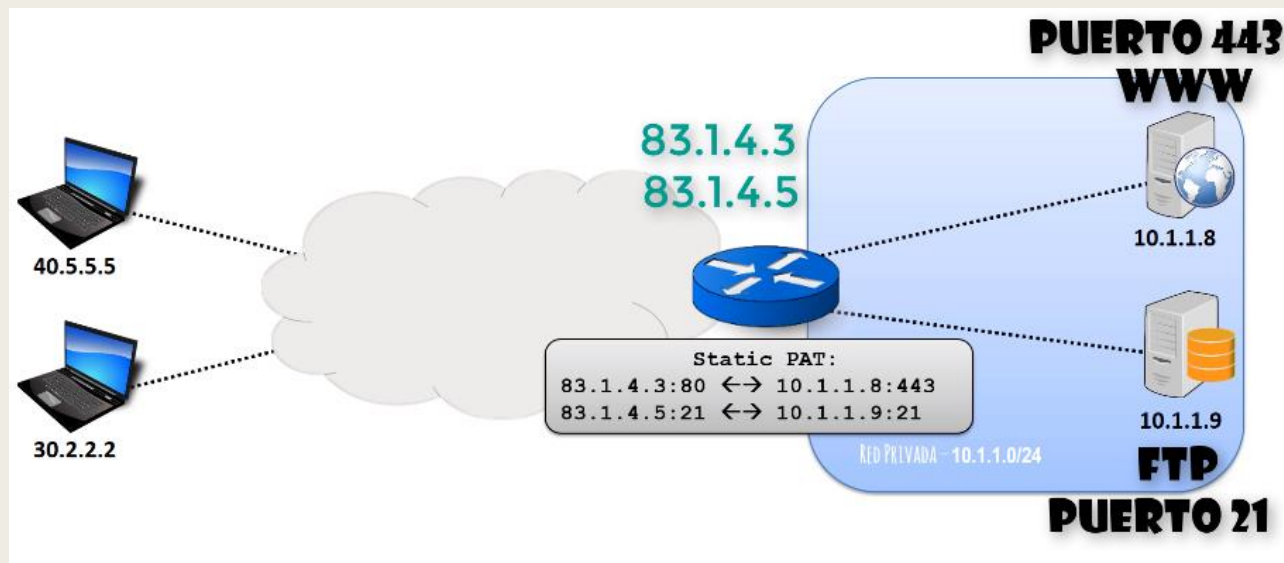
NAT	ESTÁTICO
PAT	ESTÁTICO
PAT	DINÁMICO
NAT	DINÁMICO

- Hemos visto el NAT Estático y ahora vamos a pasar a ver el PAT Estático



# Escenario 1

- En esta ocasión contamos con un router que tiene disponibles 2 IPs públicas.
- También contamos con 2 servidores:
  - *Servidor web que escucha por 443*
  - *Servidor FTP que escucha por 21*

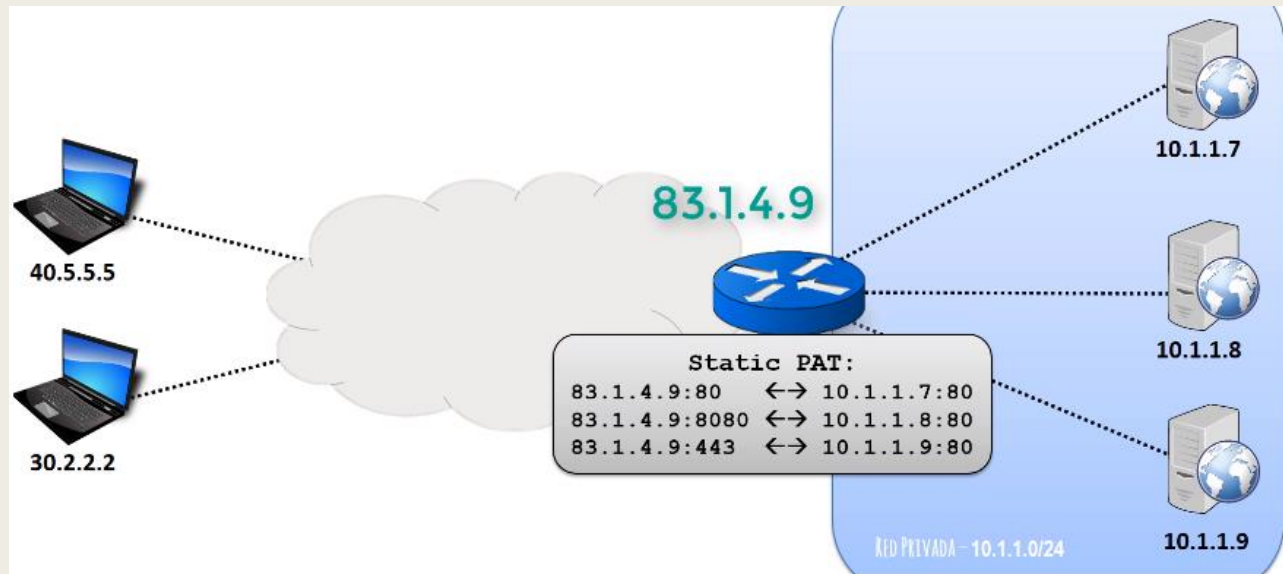


- En este escenario se traduce:
  - *83.1.4.3 :80 por 10.1.1.8 :443*
  - *83.1.4.5 :21 por 10.1.1.9 :21*
- ¿Qué significa esto?
  - *Si un paquete apunta a un puerto diferente a los dos indicados, se descartará.*

Con NAT no se tendría en cuenta el puerto

# Escenario 2

- En esta ocasión contamos con un router que tiene disponible 1 IP pública.
- También contamos con 3 servidores.
- ¿Cómo haremos para un paquete llegue al destino adecuado? Con los puertos.



- En este escenario se traduce:
  - 83.1.4.9 :80 por 10.1.1.7 :80
  - 83.1.4.9 :8080 por 10.1.1.8 :80
  - 83.1.4.9 :443 por 10.1.1.9 :80
- ¿Qué significa esto?
  - El router se encargará de enviar el paquete a un destino u otro en función del puerto indicado.
  - Todo a través de la misma IP.

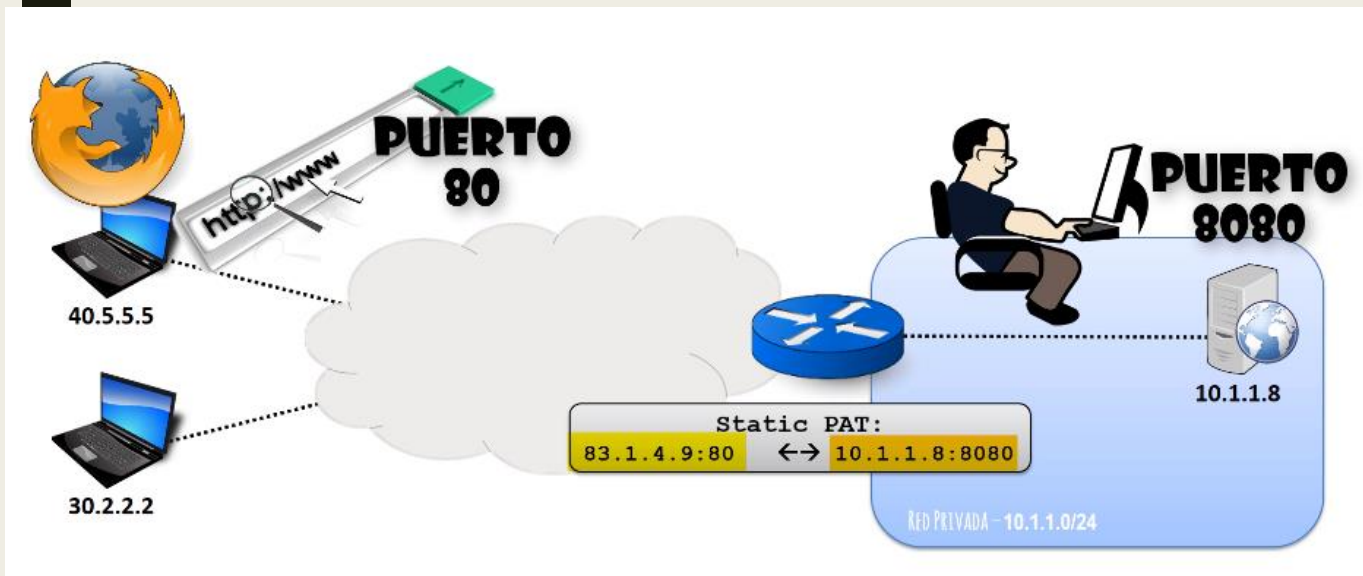
**AHORRO DE  
DIRECCIONES!**

**PAT static**

**One-to-Many**

# Escenario 3

- Puede darse el caso típico que queramos acceder a una página web.
- Al escribir la dirección en el navegador, no indicamos el puerto, y por defecto es el 80. Pero puede darse el caso que el servidor escuche por otro, como 8080.
- Para estos casos, el uso de PAT estático nos puede solucionar el problema



- En este caso, donde usamos el PAT para hacer una redirección de puertos, hablamos de:
  - *Port Forwarding (reenvío de puertos).*

Más seguridad →

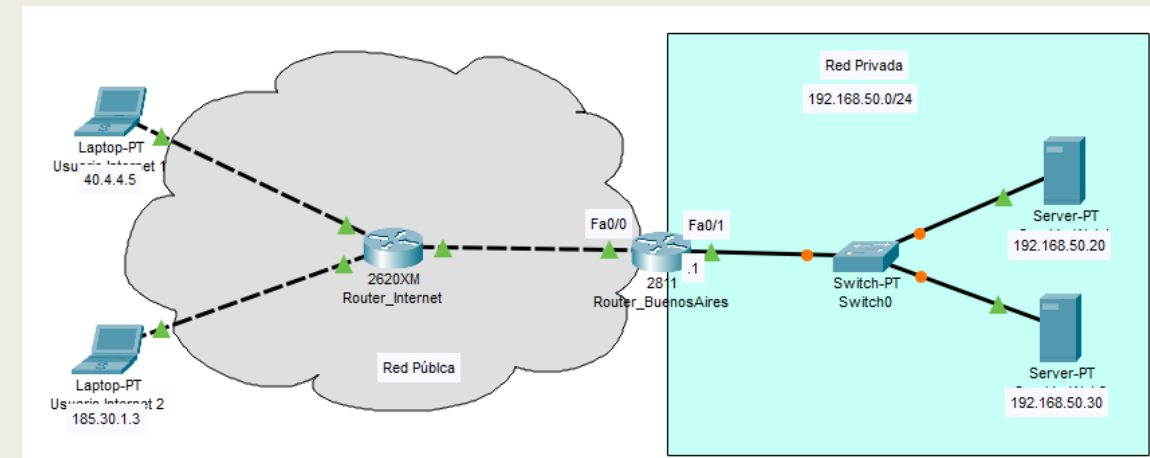
# Últimos detalles PAT estático

- Es preciso destacar que al usar PAT estático se cierran todos los puertos no configurados.
  - *Es decir, si solo se permite acceder a una IP con puerto 100, se rechazará cualquier conexión por un puerto distinto.*
  - *Esto implica una mayor seguridad de nuestra red al no permitir accesos distintos a los indicados en los puertos.*
- Otro aspecto a destacar es debido a que en la capa 4 tenemos dos protocolos: TCP y UDP.
  - *Por lo tanto, cuando definimos el PAT estático, también definiremos si la traducción es solo para TCP, solo para UDP, o para las dos.*

# PRÁCTICA DE PAT ESTÁTICO CON PACKETTRACER



# Introducción



- En el aula virtual está colgado el material base para realizar la práctica.
- En la misma práctica aparecen las instrucciones para realizarla.

-- Objetivo1 -- Configurar PAT estático en el Router\_BuenosAires para publicar el servicio web del ServidorWeb1 por la IP pública 125.2.2.2 por el puerto 80

-- Objetivo2 -- Configurar PAT estático en el Router\_BuenosAires para publicar el servicio web del ServidorWeb2 por la IP pública 125.2.2.2 por el puerto 8080 y por el puerto 443

Tanto el ServidorWeb 1 como el 2, están escuchando por el puerto 80

Una vez configurado el NAT, probar:

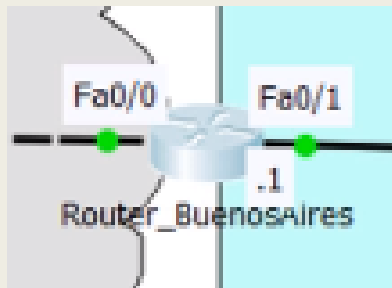
Conectividad desde Usuario de Internet1, conexión con el navegador a la IP 125.2.2.2

Conectividad desde Usuario de Internet1, conexión con el navegador a la IP 125.2.2.2 por el puerto 8080 y después por el 443



# Paso 1 - Definir interfaces inside y outside

- Antes de empezar a definir IPs y traducciones, debemos indicar qué interfaz del router es la inside y qué interfaz es la outside.



```
Router_BuenosAires#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_BuenosAires(config)#int
Router_BuenosAires(config)#interface fa
Router_BuenosAires(config)#interface fastEthernet 0/0
Router_BuenosAires(config-if)#ip nat
Router_BuenosAires(config-if)#ip nat out
Router_BuenosAires(config-if)#ip nat outside
Router_BuenosAires(config-if)#exi
Router_BuenosAires(config)#
Router_BuenosAires(config)#interface fastEthernet 0/1
Router_BuenosAires(config-if)#ip nat
Router_BuenosAires(config-if)#ip nat in
Router_BuenosAires(config-if)#ip nat inside
Router_BuenosAires(config-if)#exi
Router_BuenosAires(config)#e
```

-- Objetivo1 -- Configurar PAT estático en el Router\_BuenosAires para publicar el servicio web del ServidorWeb1 por la IP pública 125.2.2.2 por el puerto 80

- Ahora que vamos a configurar el PAT estático, tendremos una ligera variación del comando que escribimos con NAT
  - ¡PORQUE TENEMOS QUE INDICAR EL PUERTO!
  - HTTP es un puerto que corre sobre TCP, elegimos TCP

```
Router_BuenosAires(config)#ip nat inside source static ?  
  A.B.C.D  Inside local IP address  
→ tcp    Transmission Control Protocol  
  udp    User Datagram Protocol
```

- El resto del comando es igual, pero indicando ahora también los puertos con espacios
  - *ip nat inside source static tcp ip\_inside\_local puerto\_inside\_local ip\_inside\_global puerto\_inside\_global*

```
Router_BuenosAires(config)#ip nat inside source static tcp 192.168.50.20 80 125.2.2.2 80
```

# Comprobamos la tabla de traducciones

- Antes de seguir comprobamos en la tabla de traducciones que efectivamente ya tenemos añadida la dirección de traducción:
- `show ip nat translations`

```
Router_BuenosAires#  
Router_BuenosAires#sh ip nat tra  
Router_BuenosAires#sh ip nat translations  
Pro  Inside global      Inside local      Outside local      Outside global  
tcp  125.2.2.2:80          192.168.50.20:80  ---              ---  
Router_BuenosAires#
```

- Podemos apreciar que el protocolo es TCP

# Comprobamos el funcionamiento con el navegador

- Para comprobar la conectividad no es necesario en esta ocasión indicar el puerto.
  - *El puerto por defecto es el 80 en el navegador web.*



– Objetivo2 – Configurar PAT estático en el Router\_BuenosAires para publicar el servicio web del ServidorWeb2 por la IP pública 125.2.2.2 por el puerto 8080 y por el puerto 443

- En este caso, como nos piden configurar el servidor web 2 por dos puertos, tendremos que añadir 2 entradas.

```
Router_BuenosAires(config)#ip nat inside source static tcp 192.168.50.30 80 125.2.2.2 8080
```

```
Router_BuenosAires(config)#ip nat inside source static tcp 192.168.50.30 80 125.2.2.2 443
```

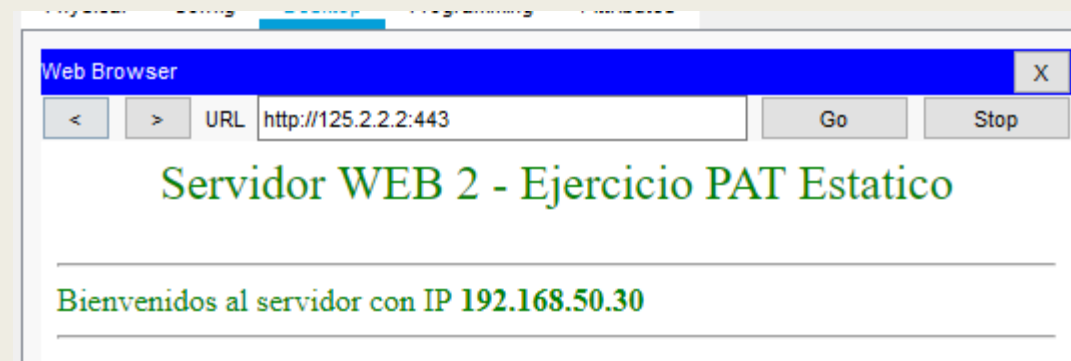
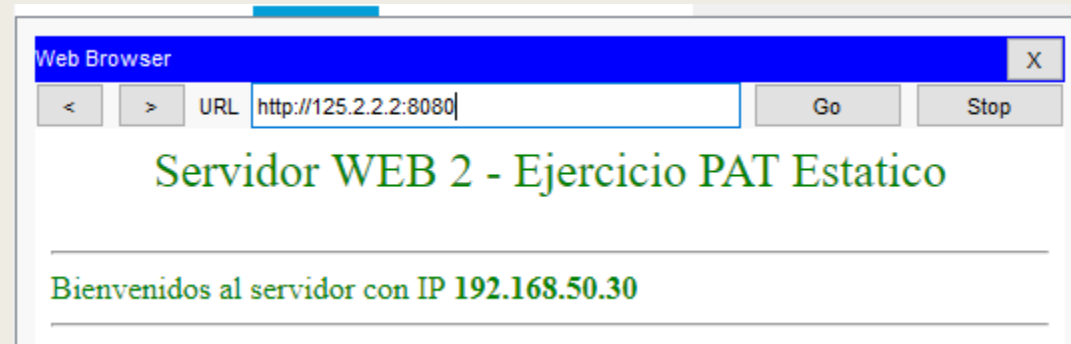
- Tras hacerlo, comprobamos la tabla de traducciones para ver que efectivamente se han añadido:

```
Router_BuenosAires#sh ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	125.2.2.2:443	192.168.50.30:80	---	---
tcp	125.2.2.2:8080	192.168.50.30:80	---	---
tcp	125.2.2.2:8080	192.168.50.30:80	185.30.1.3:1027	185.30.1.3:1027
tcp	125.2.2.2:8080	192.168.50.30:80	185.30.1.3:1028	185.30.1.3:1028
tcp	125.2.2.2:80	192.168.50.20:80	---	---
tcp	125.2.2.2:80	192.168.50.20:80	40.4.4.5:1025	40.4.4.5:1025
tcp	125.2.2.2:80	192.168.50.20:80	40.4.4.5:1026	40.4.4.5:1026

# Comprobamos el funcionamiento en el navegador

- Para estos casos sí es necesario indicar el puerto.
- Vemos que funciona.



PAT DINÁMICO

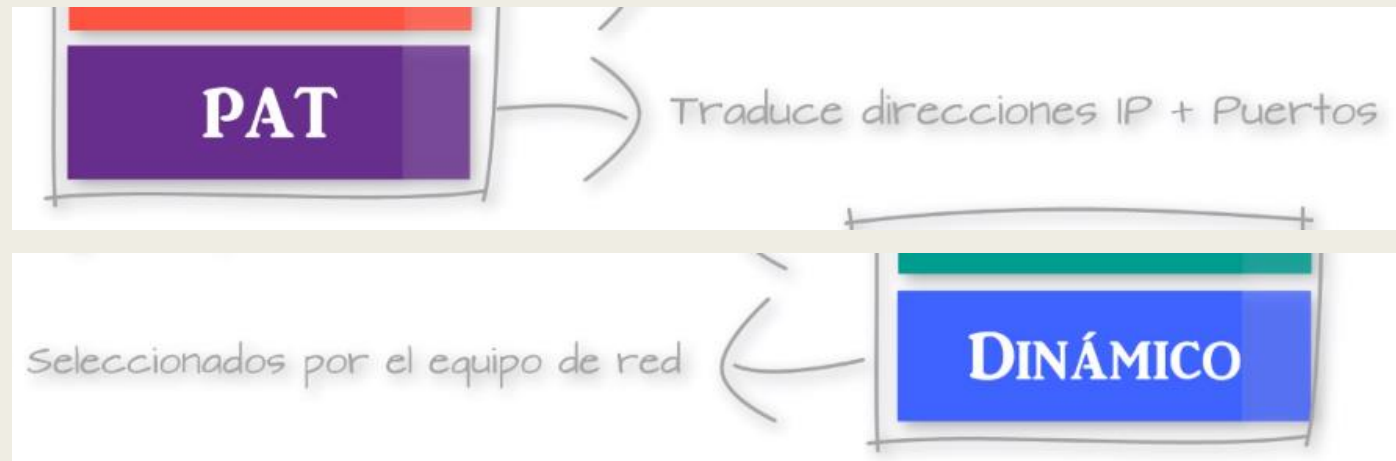




# Introducción

NAT	ESTÁTICO
PAT	ESTÁTICO
PAT	DINÁMICO
NAT	DINÁMICO

- Ya hemos visto NAT estático y PAT estático, en esta sección veremos PAT dinámico.

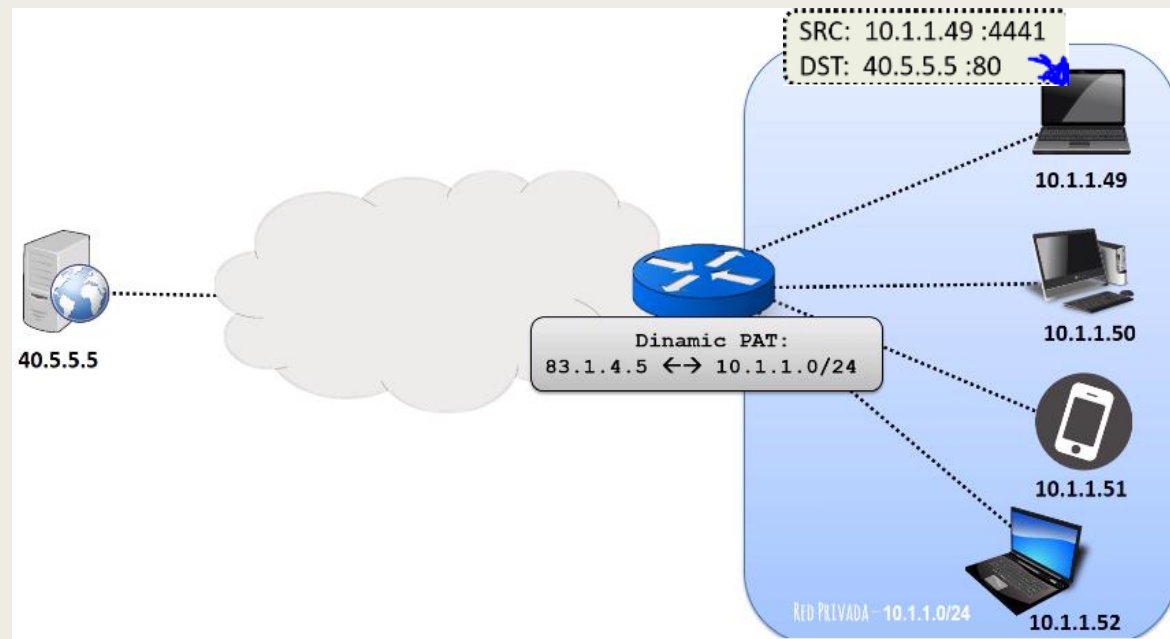


- Este es el tipo de traducción más utilizado.
  - *Es el que tenemos en casa, el que hay en hoteles, restaurantes, aeropuertos...*



# Escenario 1 / 2

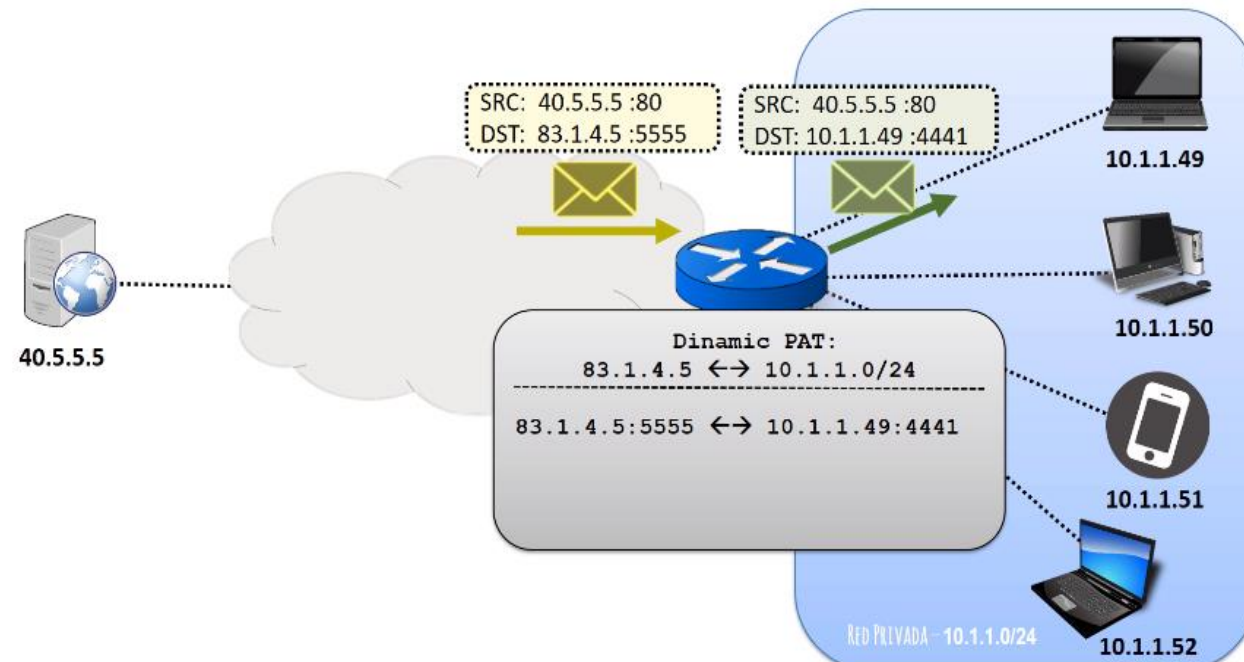
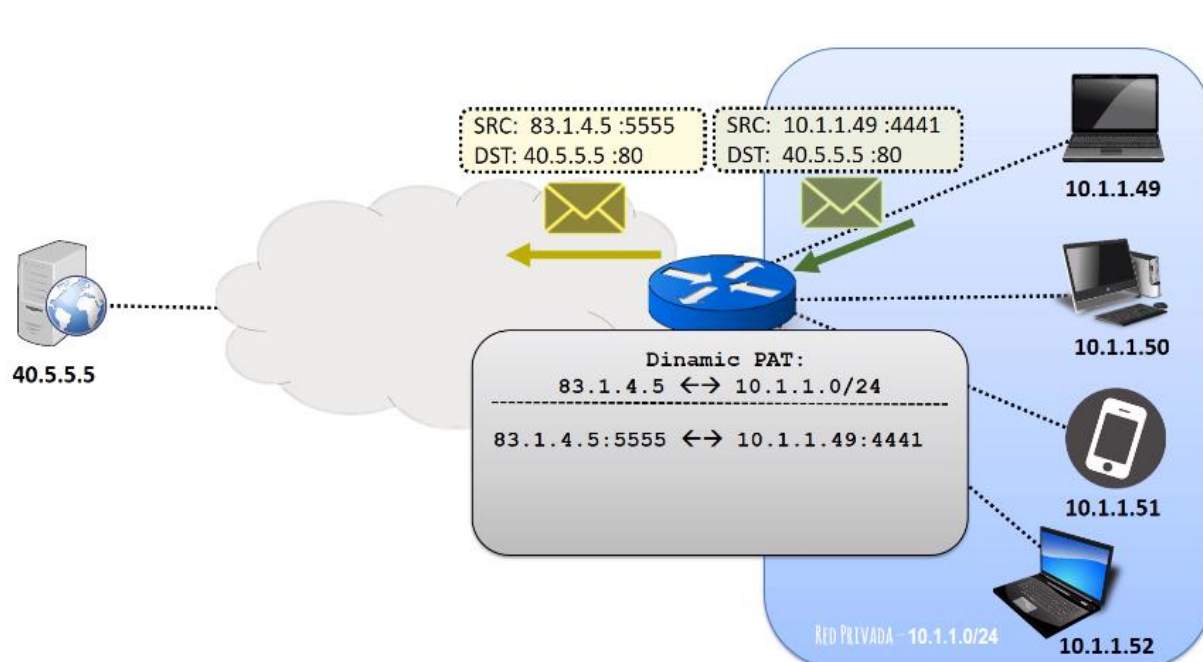
- Partimos del siguiente escenario, donde diferentes equipos pueden salir a internet a través de la misma IP pública.
- Supongamos que el portátil de arriba quiere acceder al servidor web 40.5.5.5



- El paquete que viene del portátil llegará al router.
  - Como origen tiene asignado un puerto aleatorio, y como destino el por defecto, el 80.
- El router comprobará si la dirección hace match en su tabla de traducciones.
  - Lo hará porque tiene como rango la dirección de red 10.1.1.0 / 24

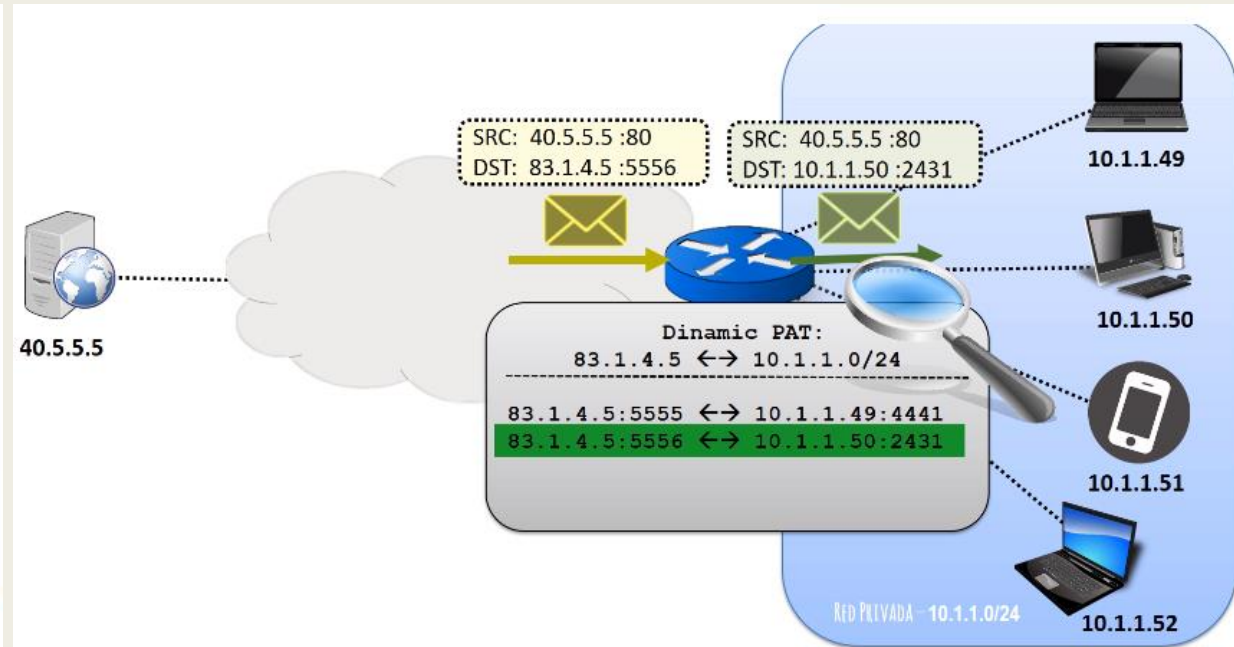
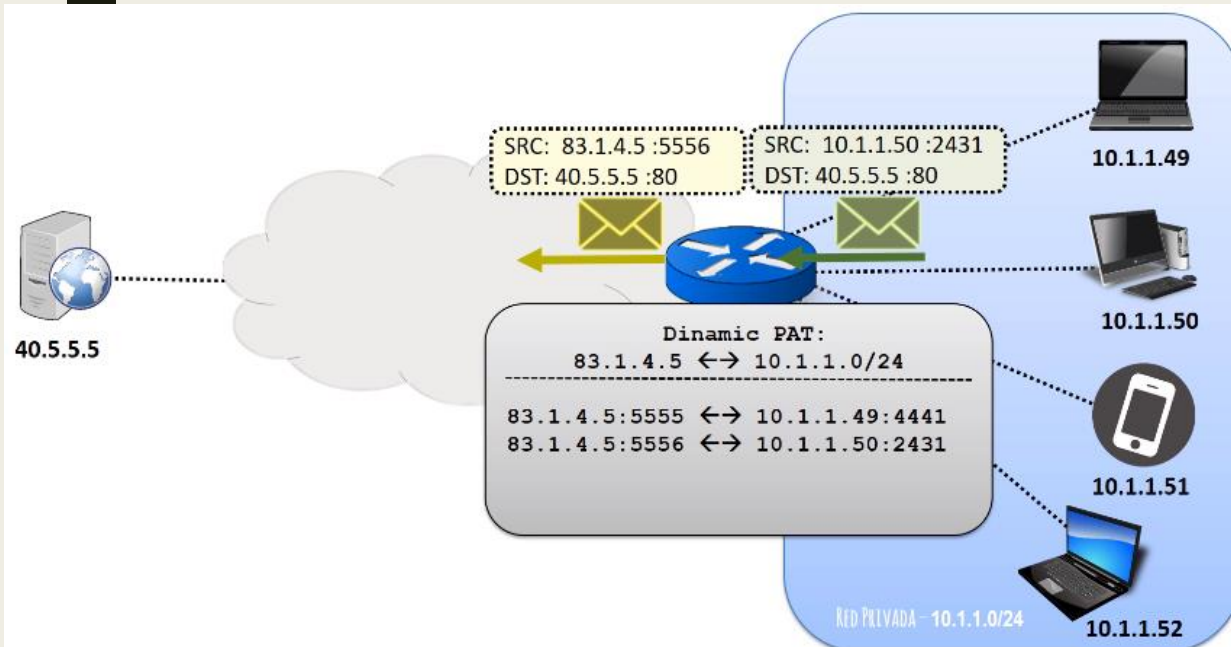
# Escenario 2/2

- El router realizará una traducción similar a la que se ve en la imagen:
  - Traducirá la IP por la pública (suponemos que solo hay una para simplificar).
  - Traducirá el puerto por otro (uno aleatorio que no se repita).
  - Se guardará la dirección y puerto traducido en una tabla para luego poder retraducirla.
- En la respuesta del servidor, el router hará match en la ruta de traducción dinámica generada.



# Mismo escenario, otra casuística

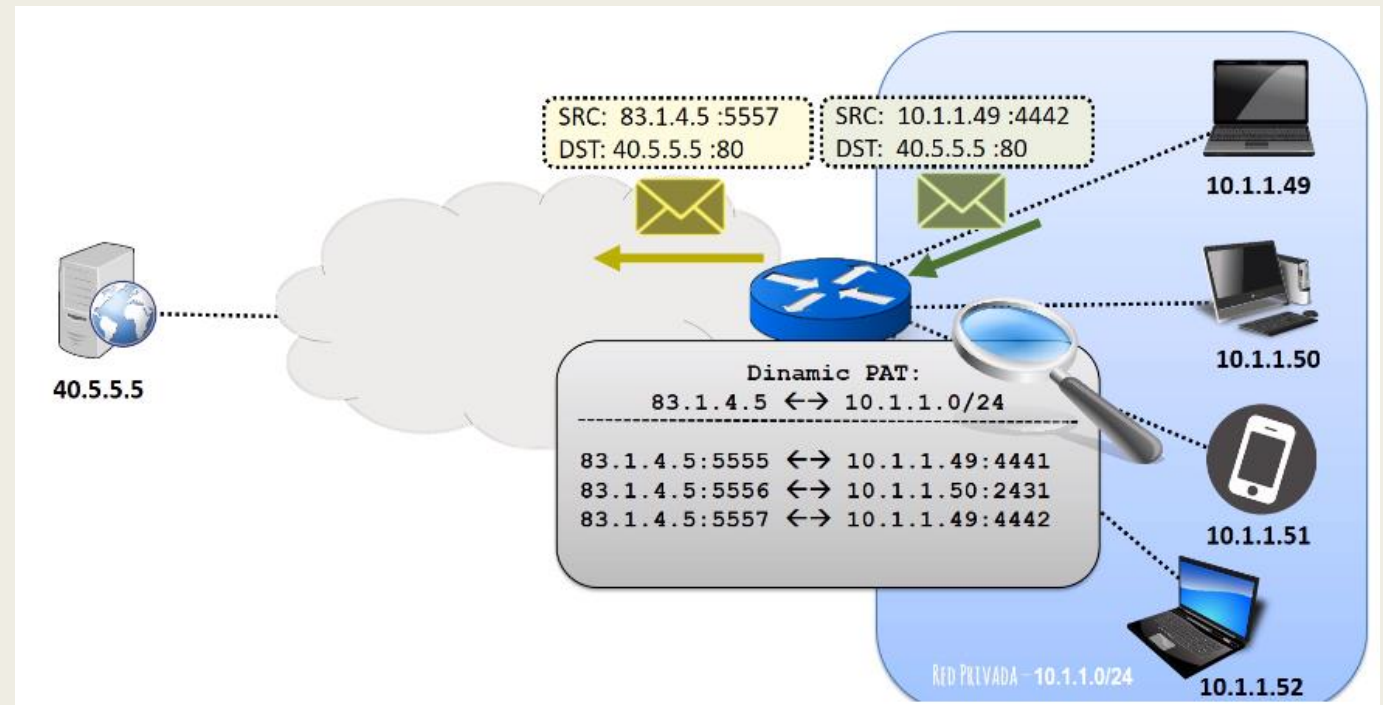
- Supongamos que después de lanzarse la petición del portátil 1, se lanza también otra petición del ordenador que está justo debajo.
- Sucederá lo mismo que en el caso anterior, el router traducirá la IP privada por la pública, y asignará un valor aleatorio que no esté ya en la tabla al puerto y lo guardará en la tabla de traducciones.
- Cuando el servidor responda al equipo, el router sabrá a qué equipo corresponde gracias al puerto, y podrá devolver este paquete al equipo adecuado.



# Sobre la tabla de traducciones

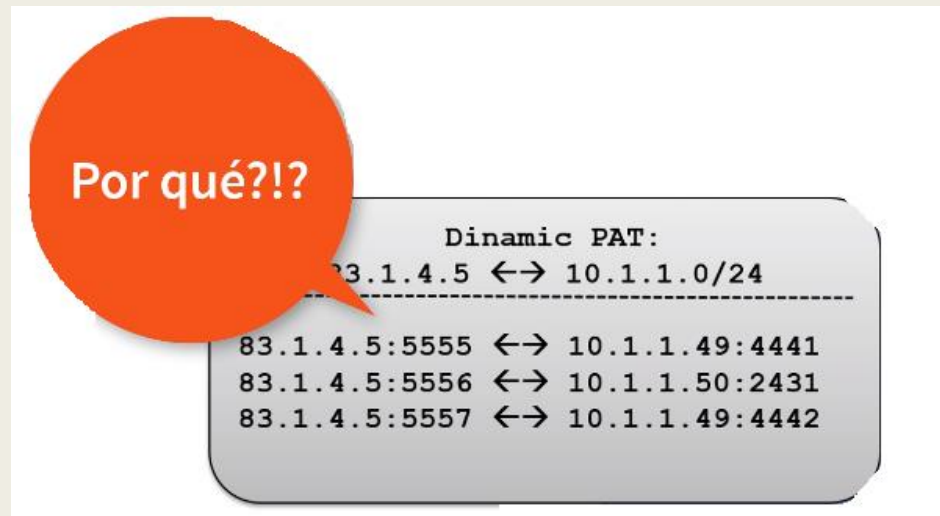
- La tabla de traducciones del router NO genera una entrada por cada equipo.
  - *GENERA 1 ENTRADA POR CADA CONEXIÓN.*
- Por lo tanto, cada equipo generará varias entradas dinámicas en la tabla de traducciones.

- Si el primer equipo lanza una petición nueva al servidor web, el router le asignará un nuevo registro en la tabla de traducciones.



# Pregunta

- ¿Por qué si los equipos generan un puerto aleatorio para realizar la conexión el router vuelve a generar otro puerto aleatorio?
  - *¿No podría aprovechar el que ya se ha generado?*



SRC: 10.1.1.49 :4441  
DST: 40.5.5.5 :80

SRC: 10.1.1.50 :2431  
DST: 40.5.5.5 :80





# Respuesta



- ¿Por qué si los equipos generan un puerto aleatorio para realizar la conexión el router vuelve a generar otro puerto aleatorio?
  - *Porque el rango de puertos que se generan aleatoriamente en los equipos finales va desde 0 a 65535, y ellos NO comprueban si está repetido o no.*
- Podría darse el caso de que dos equipos generaran aleatoriamente el mismo puerto.
  - *Esto puede suceder dado que normalmente se generan muchas peticiones al exterior.*
- De esta forma evitamos el problema que pudiera ocasionarnos.

```
Dinamic PAT:
83.1.4.5 ↔ 10.1.1.0/24
-----
83.1.4.5: 4441 ↔ 10.1.1.49:4441
83.1.4.5: 2431 ↔ 10.1.1.50:2431
83.1.4.5: 4442 ↔ 10.1.1.49:4442
83.1.4.5: 4441 ↔ 10.1.1.51:4441
```

# PAT Dinámico es unidireccional

- Con PAT dinámico los equipos del exterior no pueden acceder a equipos de una red.
  - *¿Por qué? Nunca harán match en la tabla de direcciones al no tener ningún registro del router de IP + Puerto aleatorio*

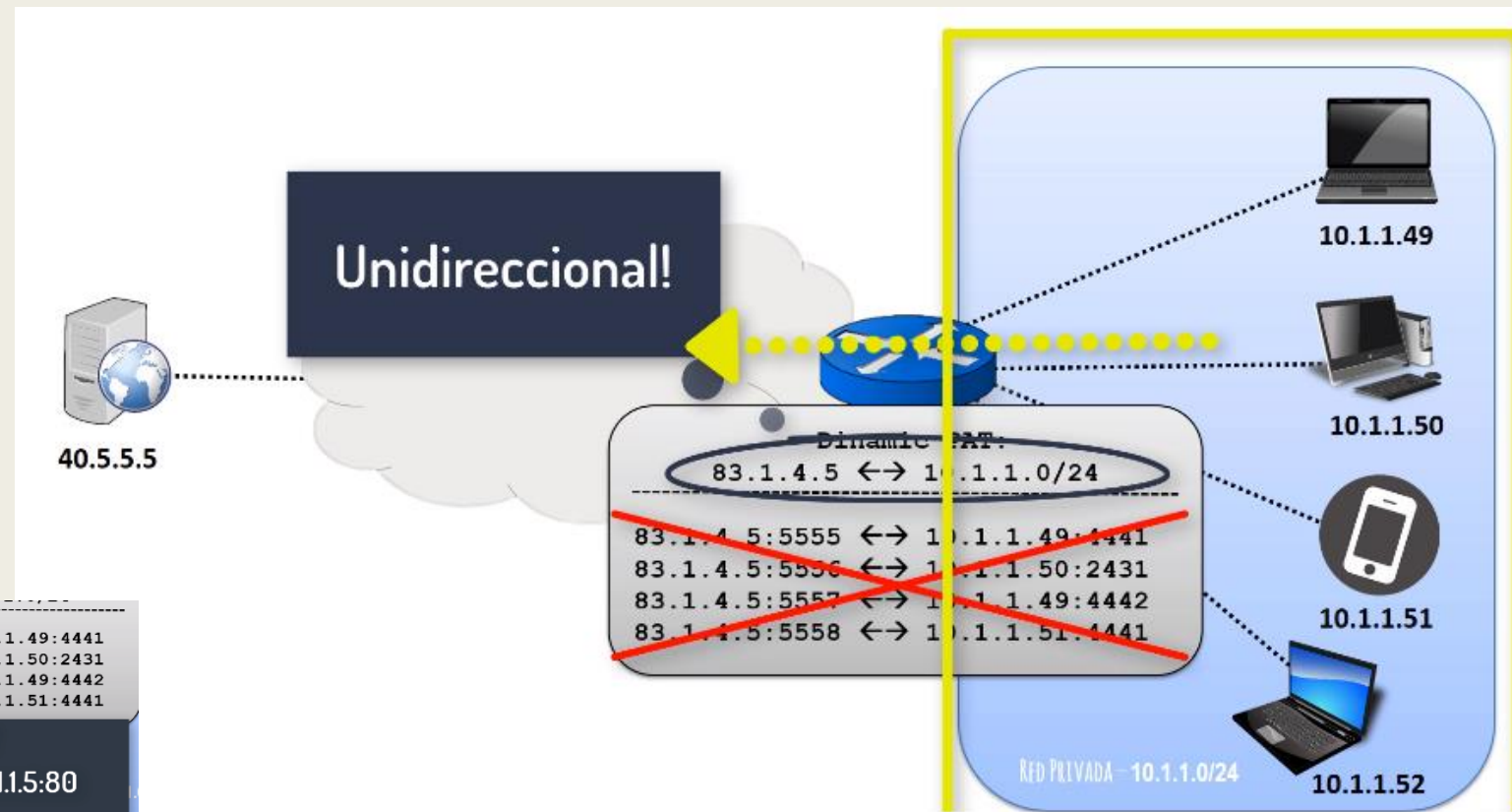
- Si quisiéramos que alguno de nuestro equipos de la red, por ejemplo, un servidor, pudiera ser llamado desde el exterior...

- Tendríamos que configurar además del PAT dinámico, un PAT estático.

83.1.4.5:5555	↔	10.1.1.49:4441
83.1.4.5:5556	↔	10.1.1.50:2431
83.1.4.5:5557	↔	10.1.1.49:4442
83.1.4.5:5558	↔	10.1.1.51:4441

**+** Static PAT

83.1.4.5:80	↔	10.1.1.50:80
-------------	---	--------------



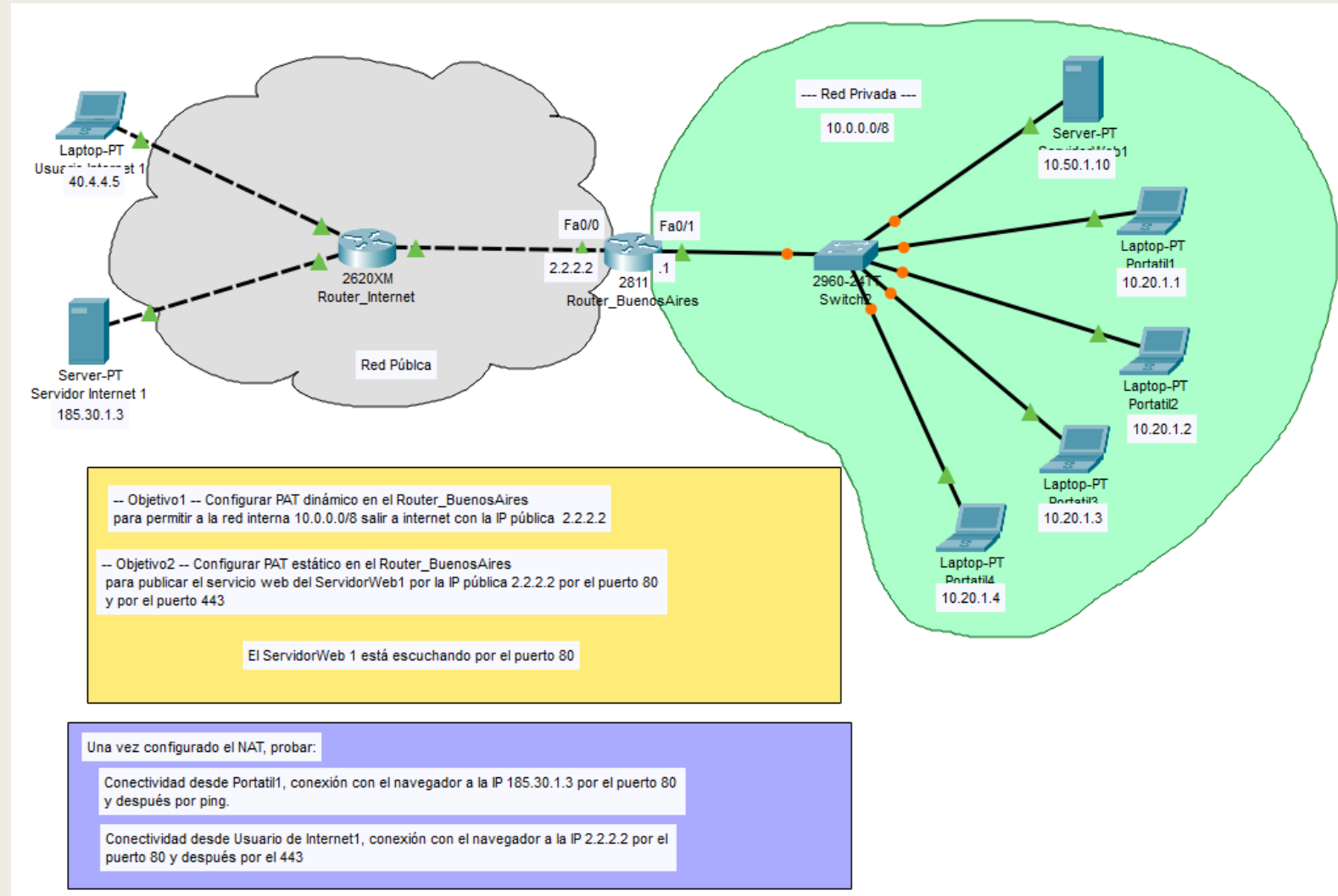
# PRÁCTICA DE PAT DINÁMICO CON PACKETTRACER





# El laboratorio

- El material base para esta práctica está colgado en el aula virtual.
- En esta práctica vamos a configurar un pat dinámico para una red, y un pat estático para un servidor de la red.
  - *Tanto el PAT dinámico como el estático se configurarán con la misma IP pública.*



## 1/2

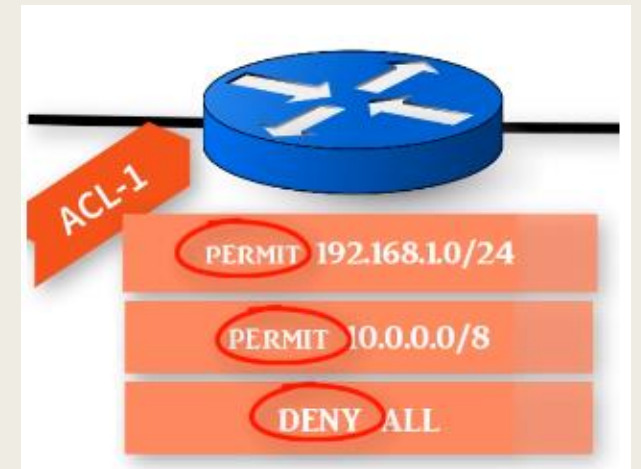
— Objetivo1 — Configurar PAT dinámico en el Router\_BuenosAires para permitir a la red interna 10.0.0.0/8 salir a internet con la IP pública 2.2.2.2

- 1. Definir la interfaz inside y outside

```
Router_BuenosAires(config)#interface fastEthernet 0/0
Router_BuenosAires(config-if)#ip nat outside
Router_BuenosAires(config-if)#exit
Router_BuenosAires(config)#
Router_BuenosAires(config)#
Router_BuenosAires(config)#interface fastEthernet 0/1
Router_BuenosAires(config-if)#
Router_BuenosAires(config-if)#ip nat inside
```

# Breve inciso: ACCESS-LIST (ACL)

- Para configurar el PAT dinámico debemos conocer qué es una Access-List (ACL).
- Las Access-List se utilizan para hacer match de cierto tráfico.
  - *Podemos utilizarlas en NAT / PAT*
- Por ejemplo, si las utilizamos como una regla de PAT:
  - *Todo lo que haga match en esa ACL → Hará match en el PAT*
    - Y por lo tanto se traducirá.
- Las ACL se utilizan muy comúnmente en temas de seguridad.
  - *Por ejemplo, aplicando una ACL en una interfaz, se define qué datos pueden pasar y qué datos no pueden pasar por una interfaz.*
- Para indicar qué puede pasar y qué no, usamos **permit** y **deny**
- Para crear una ACL escribiremos el comando: `Router BuenosAires(config)#ip access-list standard RED INTERNA`
- Al crearla, accederemos a ella para poder configurarla:



```
Router BuenosAires(config-std-nacl)#?  
<1-2147483647> Sequence Number  
default      Set a command to its defaults  
deny         Specify packets to reject  
exit         Exit from access-list configuration mode  
no           Negate a command or set its defaults  
permit       Specify packets to forward  
remark       Access list entry comment
```

2/2

— Objetivo1 — Configurar PAT dinámico en el Router\_BuenosAires para permitir a la red interna 10.0.0.0/8 salir a internet con la IP pública 2.2.2.2

- 2. Configuramos una ACL donde permitamos todas las conexiones:

```
Router_BuenosAires(config)#ip access-list standard RED INTERNA
```

```
Router_BuenosAires(config-std-nacl)#permit any
```

- Lo hacemos así porque vamos a indicar ahora que el router acepte todas las peticiones *INSIDE* que le lleguen.

- 3. Configuramos el PAT dinámico:

```
Router_BuenosAires(config)#ip nat inside source list RED INTERNA interface fastEthernet 0/0 overload
```

- Con list RED\_INTERNA estamos indicando nuestra ACL
- interface habría aceptado también pool si tuviéramos más de una dirección IP
- overload lo utilizamos para indicarle al router que con una sola IP pública podemos traducir muchas IP privadas sobrecargando los puertos (lo que hace el PAT normalmente).
  - Si no ponemos overload, nos puede dar problemas, porque tenemos un many-to-one

# Ver la configuración aplicada

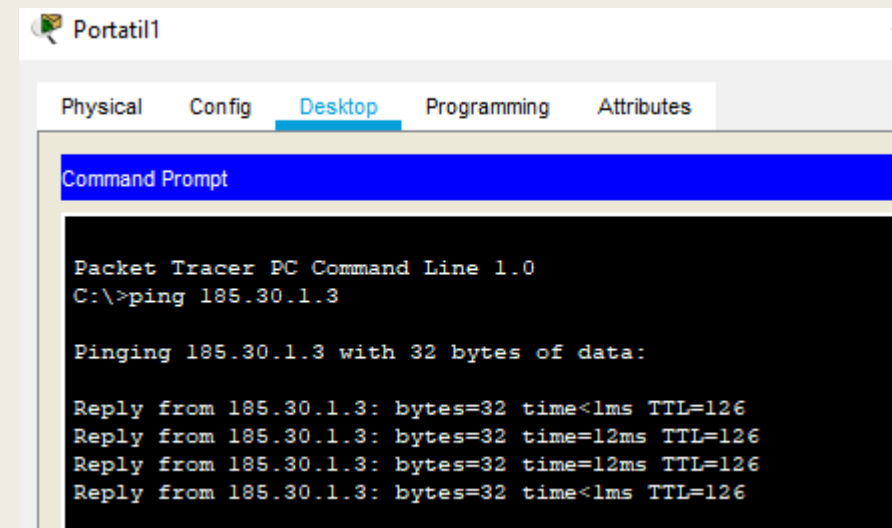
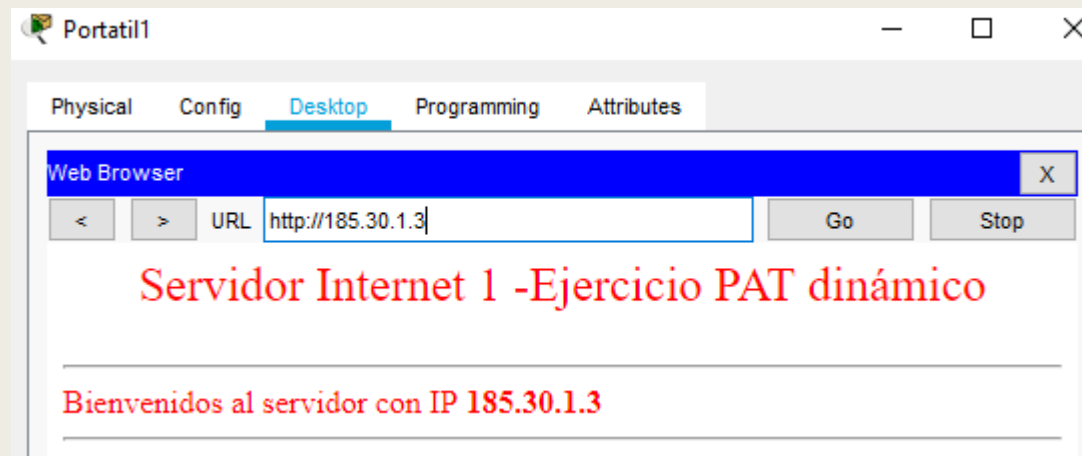
- Si hacemos un running-config podemos ver que se está aplicando el PAT dinámico.

```
ip nat inside source list RED_INTERNA interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 2.2.2.1
!
ip flow-export version 9
!
!
ip access-list standard RED_INTERNA
permit any
```

- *Para el router, lo que significa la regla que hemos puesto es:*
  - Todo lo que me entre por la inside, con la source (dirección origen) que haga match en esta ACL (es decir, cualquier cosa que llegue porque hemos puesto permit any) lo voy a traducir cambiando la dirección por la de la interfaz Fa0/0 y voy a hacer overload (sobrecarga de puertos, es decir, vamos a sobrecargar 2.2.2.2 jugando con diferentes puertos) → **O lo que es lo mismo, vamos a hacer PAT dinámico.**
- Si consultamos la tabla de traducciones, no vamos a ver nada. Porque el PAT dinámico no mostrará nada hasta que no generemos tráfico.

```
Router_BuenosAires#show ip nat translations
Router_BuenosAires#
```

Conectividad desde Portatil1, conexión con el navegador a la IP 185.30.1.3 por el puerto 80 y después por ping.



- Si hacemos ahora un show ip nat translations, vemos que la tabla ya tiene contenido:

```
Router_BuenosAires#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 2.2.2.2:1          10.20.1.1:1       185.30.1.3:1       185.30.1.3:1
icmp 2.2.2.2:2          10.20.1.1:2       185.30.1.3:2       185.30.1.3:2
icmp 2.2.2.2:3          10.20.1.1:3       185.30.1.3:3       185.30.1.3:3
icmp 2.2.2.2:4          10.20.1.1:4       185.30.1.3:4       185.30.1.3:4
tcp  2.2.2.2:1025       10.20.1.1:1025    185.30.1.3:80      185.30.1.3:80
```

— Objetivo2 — Configurar PAT estático en el Router\_BuenosAires para publicar el servicio web del ServidorWeb1 por la IP pública 2.2.2.2 por el puerto 80 y por el puerto 443

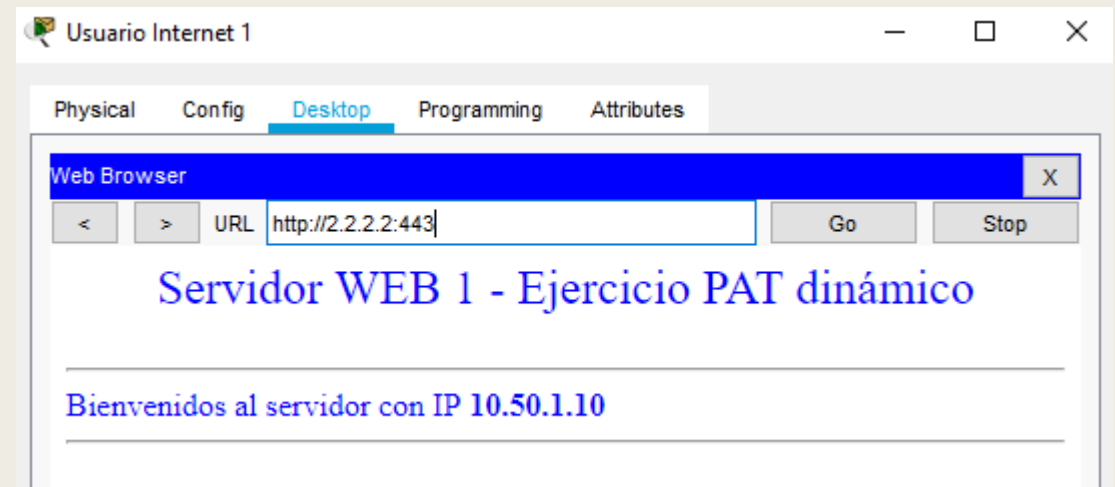
- Ya sabemos cómo configurar el PAT estático.
- Como nos lo piden para dos puertos, tendremos que usar el comando dos veces.

```
Router_BuenosAires(config)#ip nat inside source static tcp 10.50.1.10 80 2.2.2.2 80  
Router_BuenosAires(config)#ip nat inside source static tcp 10.50.1.10 80 2.2.2.2 443
```

- Los comandos dirían: Todo lo que llegue a 2.2.2.2 por los puertos 80 y 443, se redirigirá hacia 10.50.1.10 con puerto 80

Conectividad desde Usuario de Internet1, conexión con el navegador a la IP 2.2.2.2 por el puerto 80 y después por el 443

- Probamos la conectividad por ambos puertos:



```
Router_BuenosAires#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
tcp  2.2.2.2:1025         10.20.1.1:1025    185.30.1.3:80      185.30.1.3:80
tcp  2.2.2.2:443          10.50.1.10:80     ---                ---
tcp  2.2.2.2:443          10.50.1.10:80     40.4.4.5:1026      40.4.4.5:1026
tcp  2.2.2.2:80           10.50.1.10:80     ---                ---
tcp  2.2.2.2:80           10.50.1.10:80     40.4.4.5:1025      40.4.4.5:1025
```



# Fin de la unidad

- Hemos visto:
  - *NAT estático*
  - *PAT estático*
  - *PAT dinámico*
- Y os preguntaréis, ¿y el NAT dinámico?
  - *En un principio no vamos a explicarlo.*
    - ¿Por qué?
      - *Porque se utiliza muy poco (nada).*
    - Lo que más se utiliza es PAT estático y dinámico.
    - El NAT estático se utiliza en ocasiones, pero no tanto porque tiene el problema de que tenemos que asignar 1 IP - 1 servidor y esto resulta muy costoso dado el problema del agotamiento de direcciones IPv4.
- Lo que hemos visto cubre el 99% de los casos.

¿Preguntas?



# NAT Y PAT

Traducción de direcciones IP y Puertos

