CCNA Exploration 4 – Acceso a la WAN

Capítulo 7: Implementando Servicios de direccionamiento IP

Ricardo José Chois Antequera

INSTITUTO TECNOLÓGICO DE SOLEDAD ATLÁNTICO - ITSA

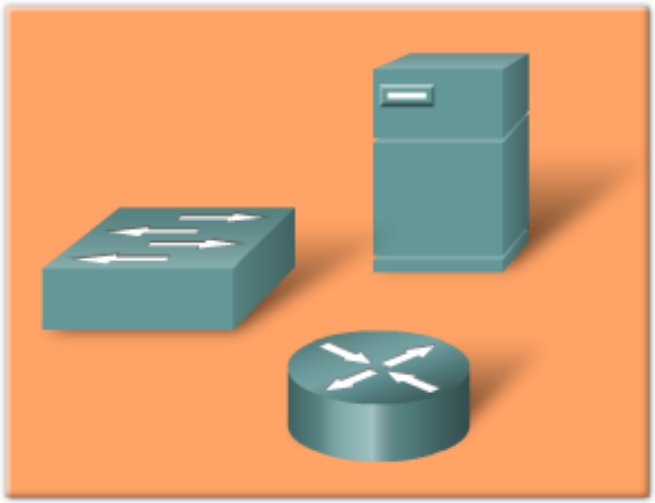
Objetivos

- Configurar DHCP en la red de una sucursal de la empresa.
- Configurar NAT en un router Cisco.
- Configurar RIPng para usar IPv6

¿Qué es DHCP?

- DHCP asigna direcciones IP y otra información de configuración de la red de manera dinámica.
- Es una herramienta muy útil y que ahorra tiempo a los administradores de red.
- Un conjunto de funciones de IOS de Cisco, llamado Easy IP, permite ofrecer un servidor de DHCP opcional con todas las funciones.

Configuración manual



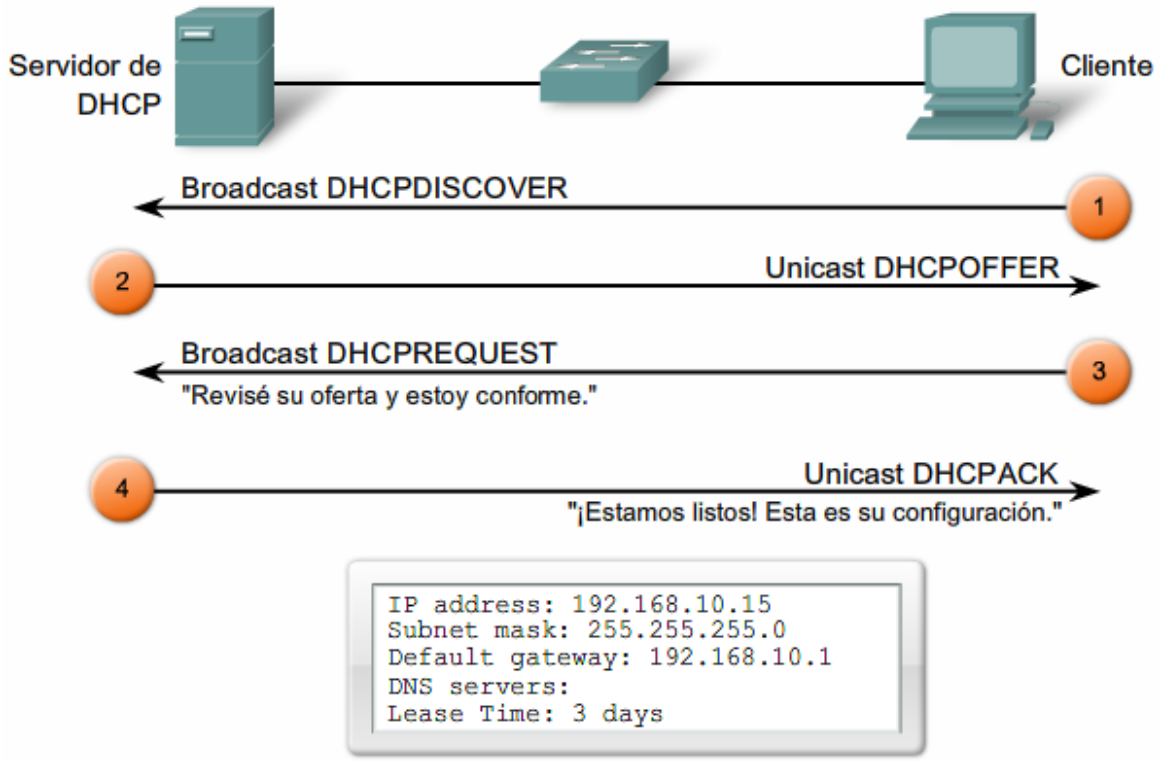
Se asignan direcciones IP estáticas a dispositivos de red que permanecen en el mismo lugar (lógica y físicamente).

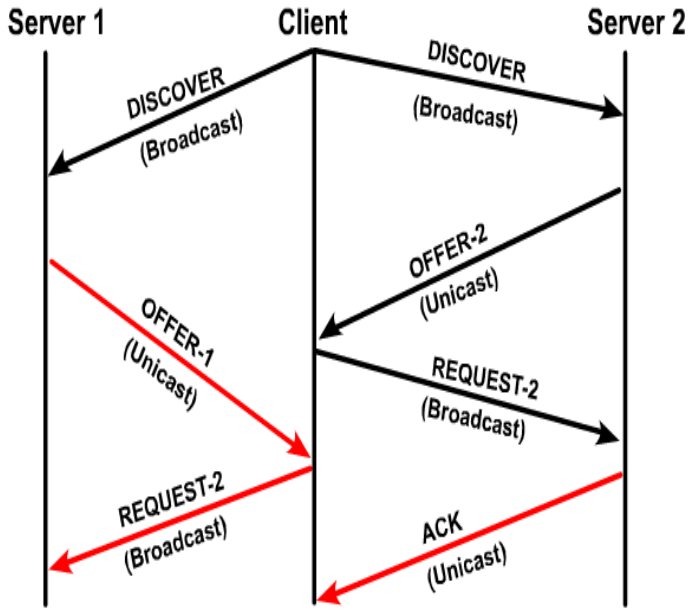
Configuración dinámica

Los dispositivos de red que se agregan, mueven o cambian (lógica y físicamente) necesitan nuevas direcciones. La configuración manual es difícil de manejar.

¿Cómo funciona DHCP?

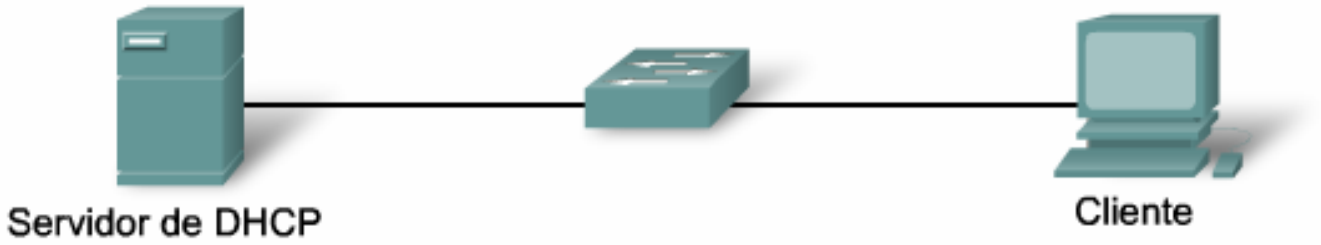
- DHCP funciona en un modo de cliente/servidor.
- Las direcciones son arrendadas y se comunican periódicamente para extender el arrendamiento.
- El proceso de intercambio se muestra en el gráfico.





BOOTP Vs DHCP

- La diferencia principal es que BOOTP se diseñó para la configuración previa manual de la información del host en una base de datos del servidor, mientras que DHCP permite la asignación dinámica de direcciones y configuraciones de red a hosts recientemente conectados.
- DHCP permite la recuperación y la reasignación de direcciones de red a través de un mecanismo de arrendamiento. BOOTP no.
- BOOT proporciona una cantidad limitada de información a un host. DHCP proporciona parámetros de configuración IP adicionales, por ejemplo WINS y nombre de dominio.



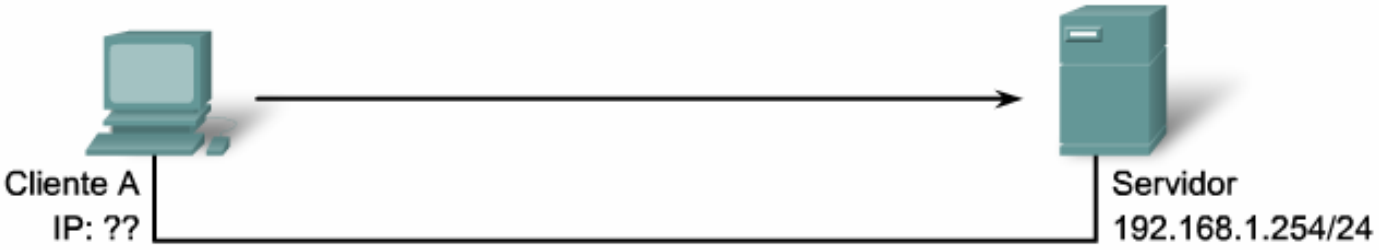
BOOTP	DHCP
Mapeos estáticos	Mapeos dinámicos
Asignación permanente	Alquiler
Sólo admite cuatro parámetros de configuración	Admite más de 20 parámetros de configuración

Formato del mensaje DHCP

- Se mantiene el formato de BOOTP, pero se agrega un campo de opciones.
  - **Código de operación (OP, Operation Code):** Tipo de mensaje. 1: mensaje de solicitud; 2: mensaje de respuesta.
  - **Tipo de hardware:** Tipo de hardware utilizado en la red. Por ejemplo, 1: Ethernet, 15:Frame Relay y 20:línea serial. Se utilizan los mismos códigos que en los mensajes de ARP.
  - **Saltos:** El cliente asigna a este parámetro un valor de 0 antes de transmitir una solicitud. Los agentes de relay lo utilizan para controlar el reenvío de los mensajes de DHCP.

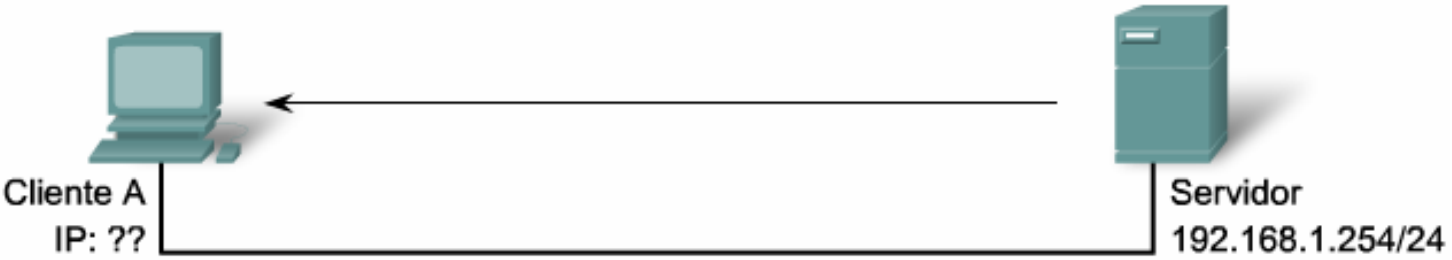
8	16	24	32
Código OP (1)	Tipo de hardware (1)	Longitud de dirección de hardware (1)	Saltos (1)
Identificador de transacción			
Segundos: 2 bytes		Señaladores: 2 bytes	
Dirección IP del cliente (CIADDR, Client IP Address): 4 bytes			
Su dirección IP (YIADDR, Your IP Address): 4 bytes			
Dirección IP de servidor (SIADDR, Server IP Address): 4 bytes			
Dirección IP del gateway (GIADDR, Gateway IP Address): 4 bytes			
Dirección de hardware del cliente (CHADDR, Client Hardware Address): 16 bytes			
Nombre del servidor (SNAME, Server name): 64 bytes			
Nombre de archivo: 128 bytes			
Opciones DHCP: variable			

Oferta y descubrimiento DHCP



Trama de Ethernet	IP	UDP	DHCPDISCOVER
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	IP SRC: ? IP DST: 255.255.255.255	UDP 67	CIADDR: ? Mask:? GIADDR: ? CHADDR: MAC A

MAC: Dirección de control de acceso al medio
CIADDR: Dirección IP del cliente
GIADDR: Dirección IP del gateway
CHADDR: Dirección de hardware del cliente



Trama de Ethernet	IP	UDP	Respuesta de DHCP
SRC MAC: MAC Serv DST MAC: MAC A	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 Mask: 255.255.255.0 GIADDR: ? CHADDR: MAC A

MAC: Dirección de control de acceso al medio
CIADDR: Dirección IP del cliente
GIADDR: Dirección IP del gateway
CHADDR: Dirección de hardware del cliente

Configuración de un Servidor DHCP

- **Paso 1.** Definición de un rango de direcciones que DHCP no debe asignar. Normalmente direcciones estáticas reservadas para la interfaz del router, la dirección IP de administración del switch, los servidores y las impresoras de red locales.

```
R1(config)#ip dhcp excluded-address low-address [high-address]
```

- **Paso 2.** Creación del pool de DHCP con el comando *ip dhcp pool*.

```
R1(config)#ip dhcp pool pool-name
```

- **Paso 3.** Configuración de los parámetros específicos del pool.

Tareas requeridas	Comando
Definir el conjunto de direcciones	`network network-number [mask | /prefix-length]`
Definir el router o gateway predeterminado	`default-router address [address2...address8]`

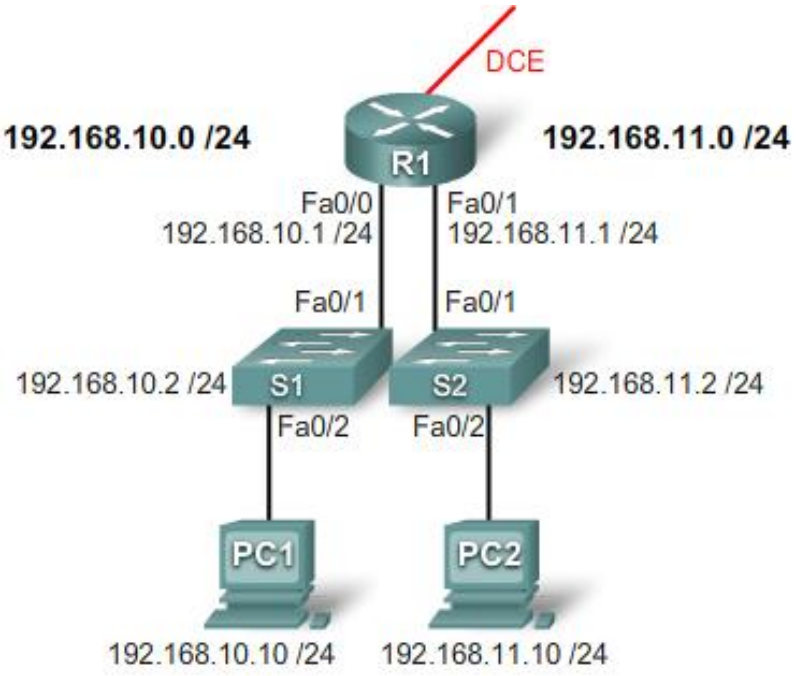
Tareas opcionales	Comando
Definir un servidor DNS.	`dns-server address [address2...address8]`
Definir el nombre de dominio	`domain-name domain`
Definir la duración del arrendamiento de DHCP	`lease { days [hours] [minutes] | infinite}`
Definir el servidor NetBIOS WINS	`netbios-name-server address [address2...address8]`

Ejemplo y verificación

- Ejemplo completo de la configuración:

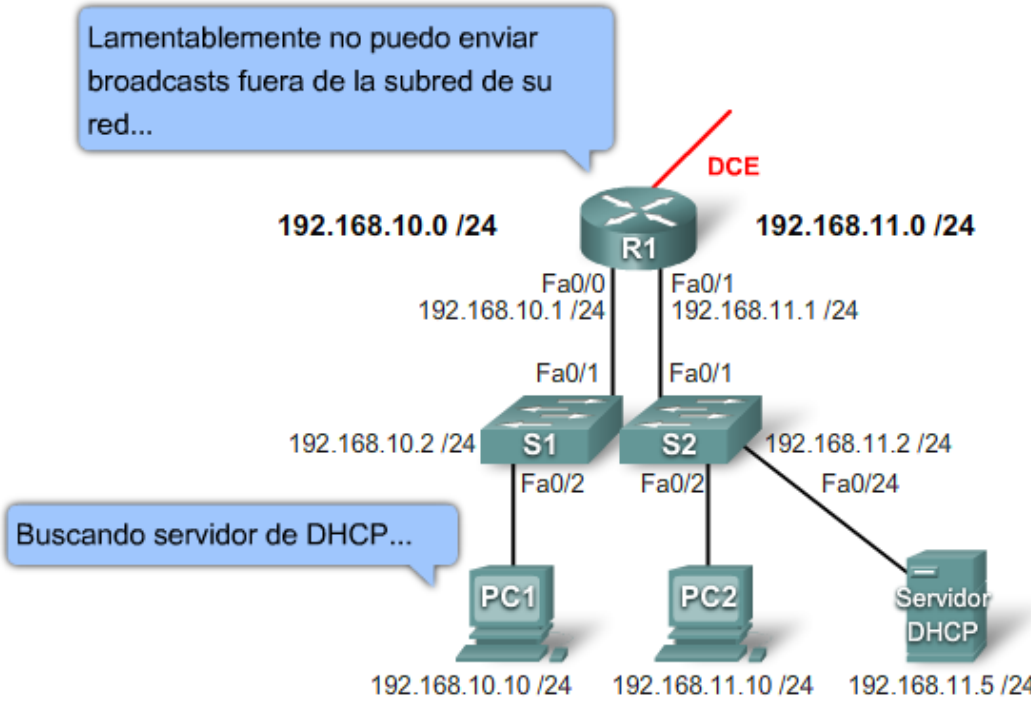
```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# domain-name span.com
R1(dhcp-config)# end
```

- Comandos de verificación:
  - *Show ip dhcp bindings*
  - *Show ip dhcp server statistics*
  - *Show ip dhcp pool*
  - *Debug ip dhcp server events*



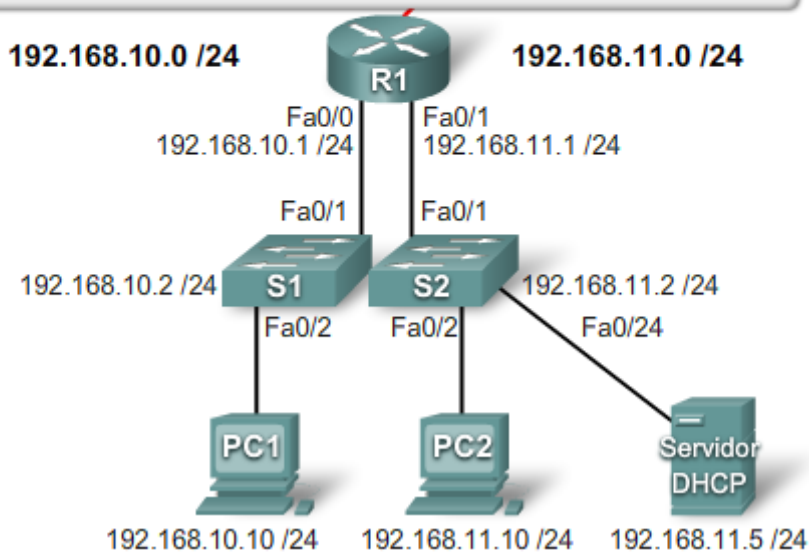
Relay DHCP

- Recuerde que los clientes DHCP usan broadcasts IP para encontrar el servidor.
- ¿Qué pasa si el servidor esta en otro segmento separado por un router?
  - Los routers no propagan los broadcast.
- Cuando sea posible, el administrador debe usar el comando en el modo de interfaz, *ip helper-address 'ip-servidor-dhcp'*

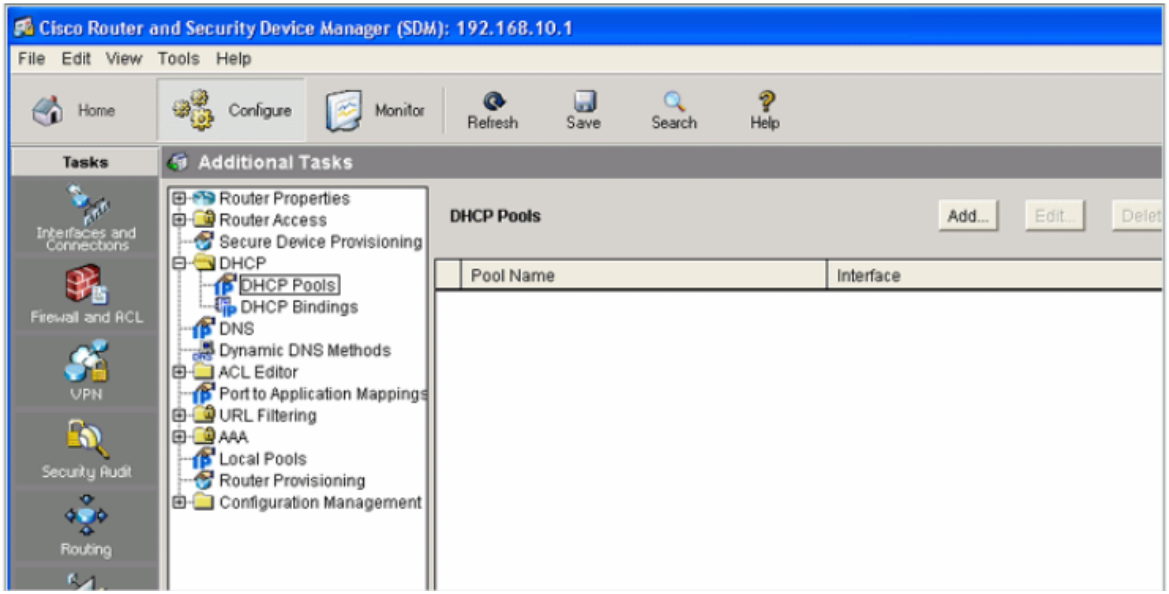


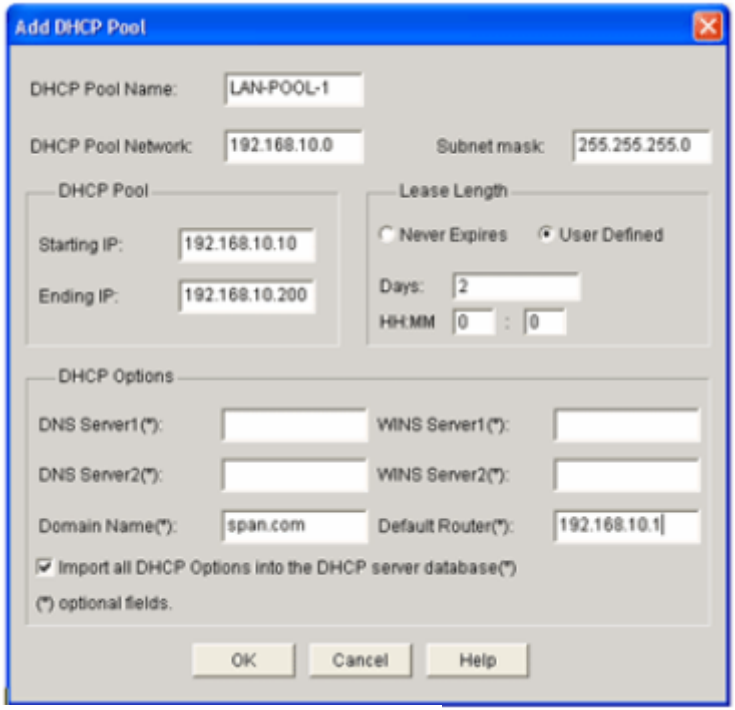
Relay DHCP

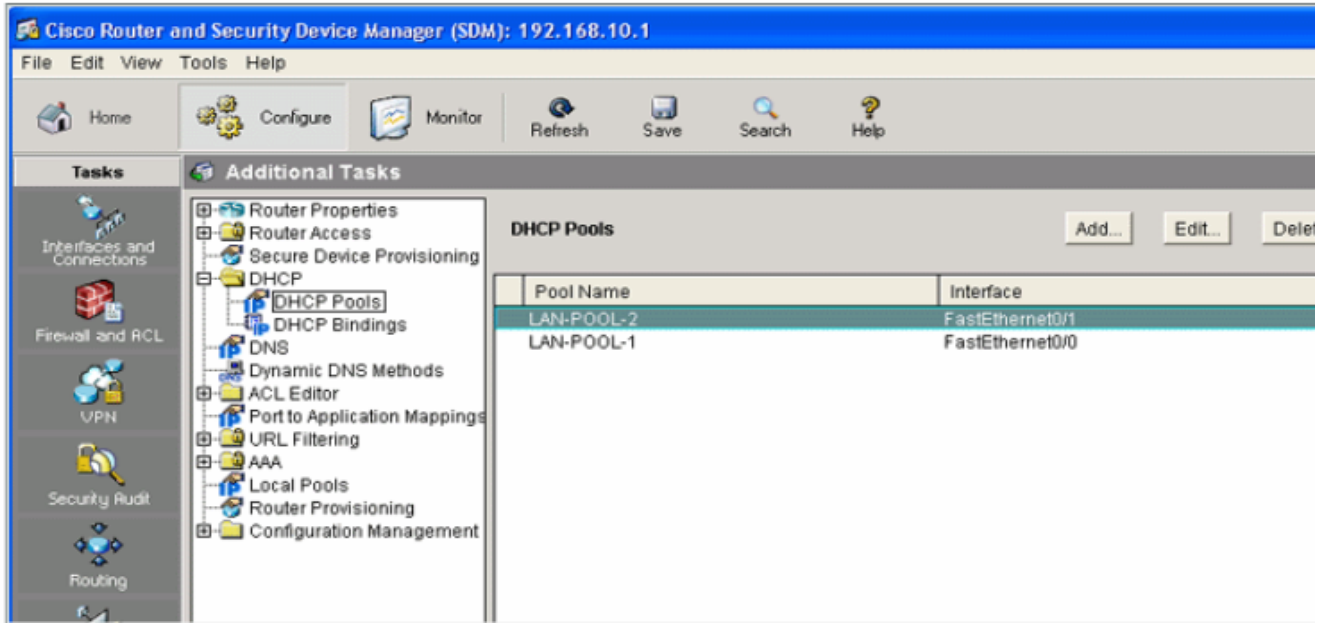
```
R1# config t
R1(config)# interface Fa0/0
R1(config-if)# ip helper-address 192.168.11.5
R1(config-if)# end
```



Configurar DHCP usando SDM







Resolución de problemas de configuración de DHCP

- Tarea 1: Solucionar los conflictos de direcciones IP
  - *show ip dhcp conflict* muestra todos los conflictos de direcciones registrados por el servidor de DHCP.
- Tarea 2: Verificar la conectividad física
  - *show interface* para confirmar que la interfaz del router que está actuando como gateway predeterminado para el cliente esté funcionando bien (…up …up).
- Tarea 3: Probar la conectividad de red mediante la configuración de un IP estática.
  - Si la estación de trabajo no puede conectarse con los recursos de la red a través de una dirección IP configurada estáticamente, la causa raíz del problema no es DHCP.
- Tarea 4: Verificar la configuración de puerto de switch (STP portfast y otros)
  - STP PortFast activada y la opción de enlace troncal y canales desactivada.
- Tarea 5: Distinguir si los clientes DHCP obtiene direcciones IP en la misma subred o VLAN que el servidor DHCP
  - Si DHCP está funcionando bien, el problema puede residir en el agente relay DHCP/BOOTP

Direccionamiento Público y Privado

- Todas las direcciones de Internet públicas deben registrarse en un registro de Internet regional (RIR, Regional Internet Registry).
- Las organizaciones pueden arrendar direcciones públicas a través de un ISP.
- No es posible enrutar direcciones privadas a través de Internet.
- Las redes necesitan un mecanismo para traducir las direcciones privadas en direcciones públicas en el extremo de la red y que funcione en ambas direcciones

Las direcciones públicas de Internet son reguladas por cinco registros americanos de números de Internet (RIR, Regional Internet Registries):

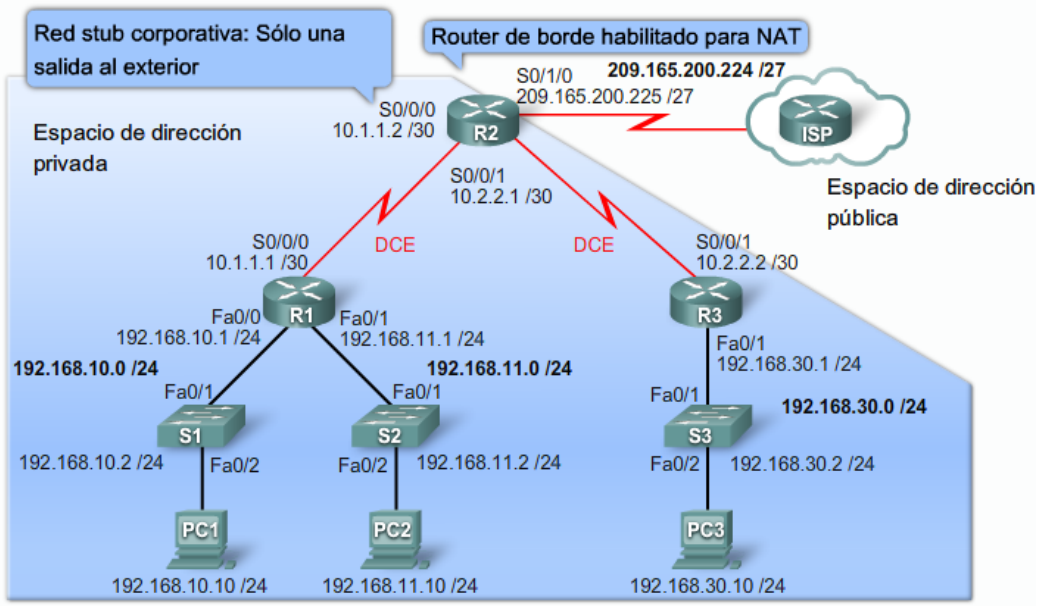
- ARIN
- RIPE
- APNIC
- LACNIC
- AfriNIC

Las direcciones privadas de Internet están definidas en RFC 1918:

Clase	Rango de direcciones internas RFC 1918	Prefijo CIDR
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

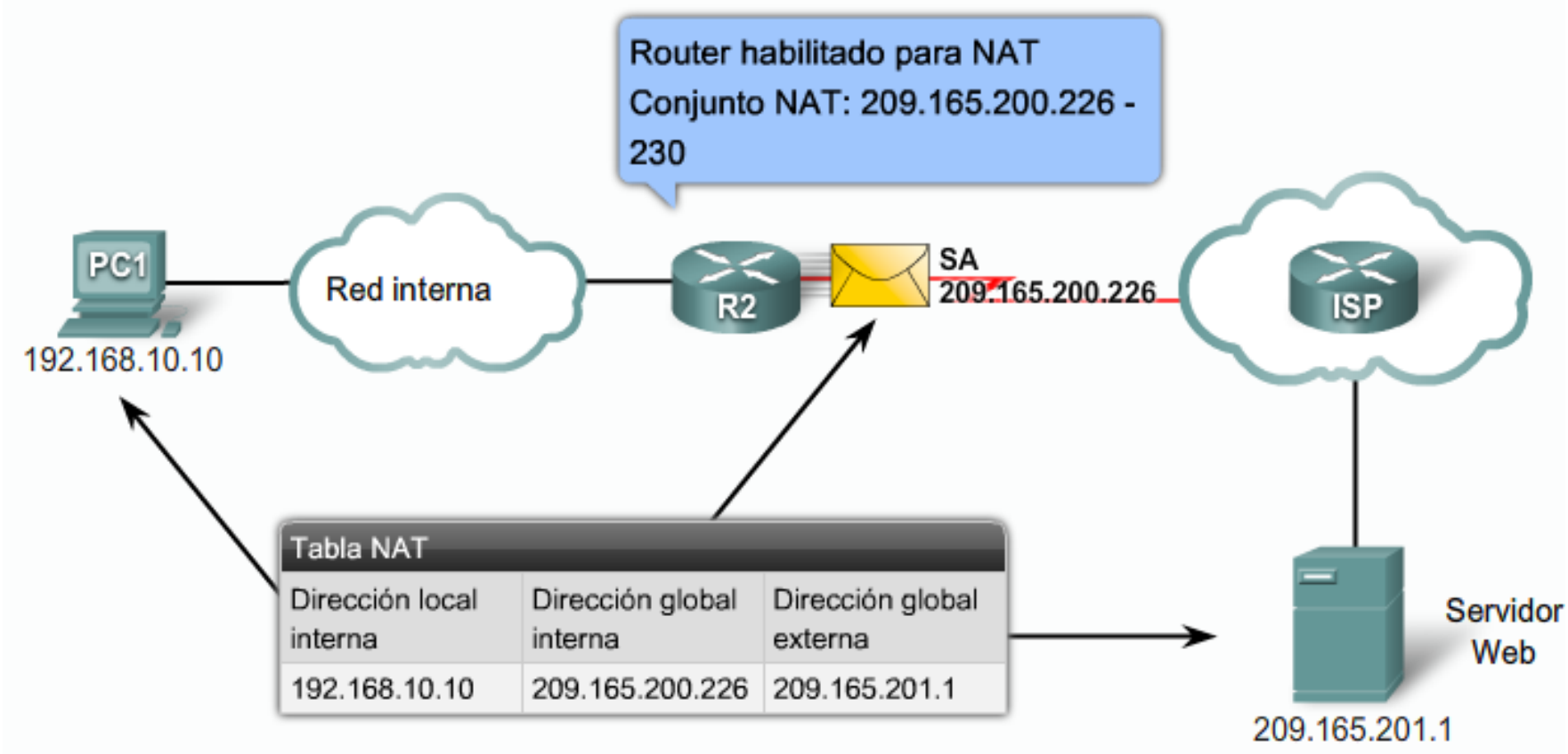
Introducción a NAT y NAT con sobrecarga (PAT)

- NAT traduce la dirección IP interna (privada) del cliente a una dirección externa (Pública).
- NAT se diseño para conservar las direcciones IP y habilitar las redes para usar direcciones IP privadas.
- NAT esta definido en la RFC 1631.
- En la práctica se usa NAT para permitir a los host de la red interna acceder a Internet.
- Las traducciones NAT pueden hacerse estática o dinámicamente.
- La mejor característica de NAT es la capacidad de usar PAT, el cual permite que muchas direcciones internas se traduzcan a una externa
- Esto es llamado algunas veces NAT de muchos a uno.



Terminología NAT

- Dirección local interna → Dirección IP privada local.
- Dirección global interna → Dirección IP pública válida asignada por el ISP.
- Dirección global externa → Dirección IP pública a la que se puede acceder.
- Dirección local externa → En la mayoría de las situaciones la misma que la global externa (No se tratan en el curso).



NAT con sobrecarga (PAT:Port Address Translation)

- Asigna varias direcciones IP privadas a una única dirección IP pública o a un grupo pequeño de direcciones IP públicas.
- La sobrecarga de NAT asegura que los clientes utilicen un número de puerto TCP diferente para cada sesión de cliente con un servidor en Internet.
- Cuando se recibe una respuesta del servidor, el número de puerto de origen, que pasa a ser el número de puerto de destino en la respuesta, determina a qué cliente se enrutan los paquetes.

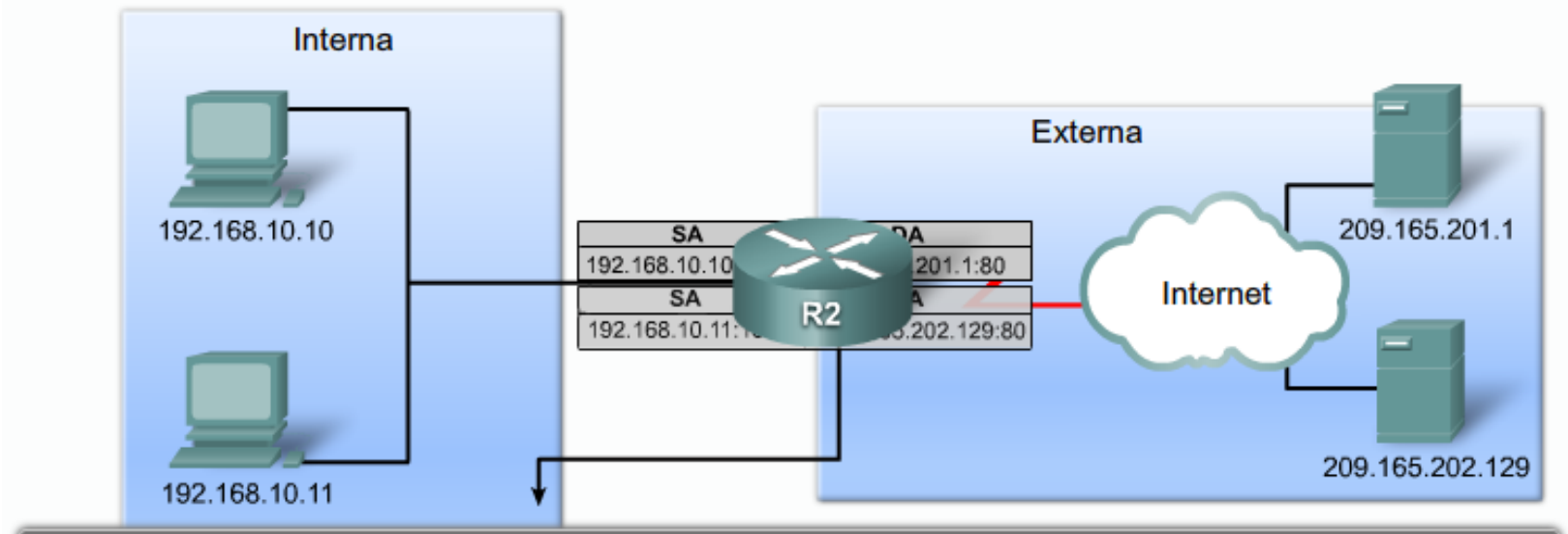


Tabla NAT con sobrecarga

Dirección IP local interna	Dirección IP global interna	Dirección IP global externa	Dirección IP local externa
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

NAT con sobrecarga (PAT:Port Address Translation)

- La sobrecarga de NAT intenta conservar el puerto de origen original.
- Si este puerto origen está en uso, la sobrecarga de NAT asigna el primer número de puerto disponible, desde el principio del grupo de puertos correspondiente 0-511, 512-1023, ó 1024-65535.
- Cuando no hay más puertos disponibles y hay más de una dirección IP externa configurada, la sobrecarga de NAT utiliza la próxima dirección IP para tratar de asignar nuevamente el puerto de origen original.

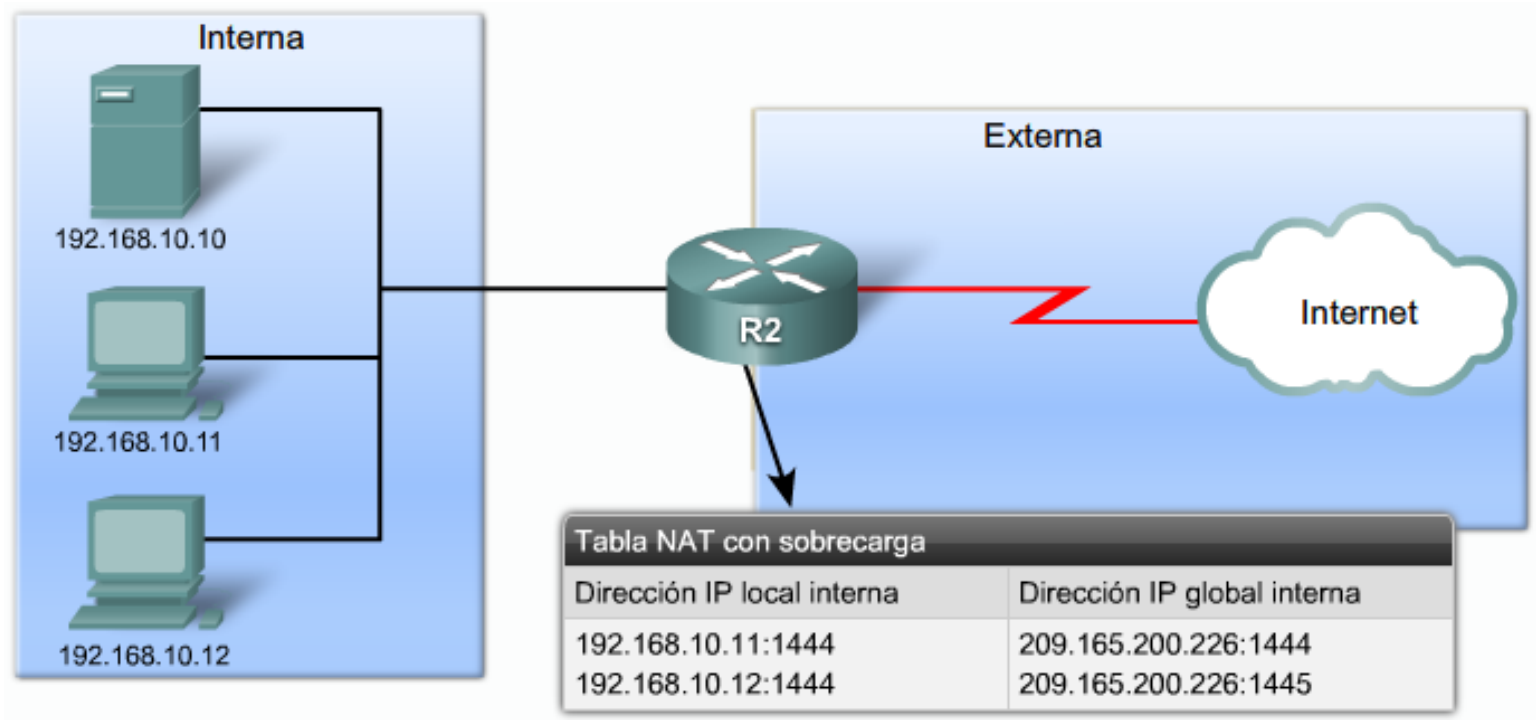


Tabla NAT con sobrecarga	
Dirección IP local interna	Dirección IP global interna
192.168.10.11:1444	209.165.200.226:1444
192.168.10.12:1444	209.165.200.226:1445

Ventajas y Desventajas de usar NAT

Ventajas de NAT

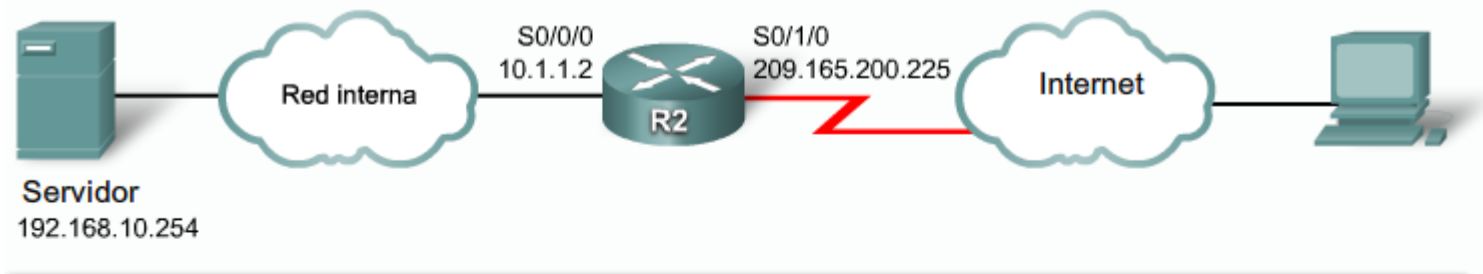
- Conserva el esquema de direccionamiento legalmente registrado
- Aumenta la flexibilidad de las conexiones con la red pública.
- Brinda regularidad para esquemas de direccionamiento de redes internas.
- Brinda seguridad de red

Desventajas de NAT

- Disminuye el rendimiento
- Disminuye la funcionalidad de extremo a extremo
- Se pierde la capacidad de rastreo IP de extremo a extremo
- El tunneling es más complicado
- Puede interrumpirse el inicio de conexiones TCP
- Las arquitecturas deben reconstruirse para adaptarse a los cambios

Configuración de NAT estático

Paso	Acción	Notas
1	Se establece la traducción estática entre una dirección local interna y una dirección global interna. `Router(config)#ip nat inside source static local-ip global-ip`	Ingrese el comando global **`no ip nat inside source`** para eliminar la traducción estática de origen.
2	Especifique la interfaz interna. `Router(config)#interface type number`	Ingrese el comando **`interface`**. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.
3	Marque la interfaz como conectada al interior. `Router(config-if)#ip nat inside`	
4	Salga del modo de configuración de interfaz. `Router(config-if)# exit`	
5	Especifique la interfaz externa. `Router(config)#interface type number`	
6	Marque la interfaz como conectada al exterior. `Router(config-if)#ip nat outside`	



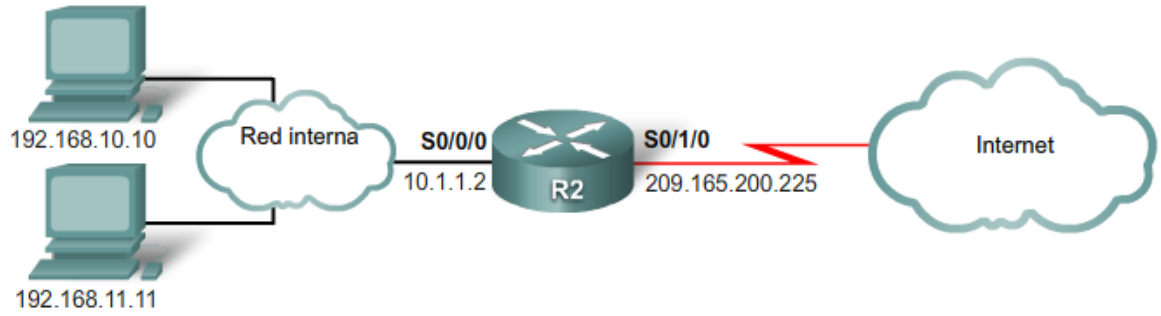

```
ip nat inside source static 192.168.10.254 209.165.200.254
!–Establishes static translation between an inside local address and an inside global address.
interface serial 0/0/0
ip nat inside
!—Identifies Serial 0/0/0 as an inside NAT interface.
interface serial 0/1/0
ip nat outside
!—Identifies Serial 0/1/0 as an outside NAT interface.
```

Con esta configuración, 192.168.10.254 siempre se traducirá a 209.165.200.254

Configuración de NAT dinámico

Paso	Acción	Notas
1	Defina un conjunto de direcciones globales para asignar según sea necesario. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask|prefix-length prefix-length}`	Ingrese el comando global `no ip nat pool name` para eliminar el conjunto de direcciones globales.
2	Defina una lista de acceso estándar que permita las direcciones que se deben traducir. `Router(config)#access-list access-list-number permit source [source-wildcard]`	Ingrese el comando global `no access-list access-list-number` para eliminar la lista de acceso.
3	Establezca la traducción dinámica de origen; para hacerlo, especifique la lista de acceso definida en el paso anterior. `Router(config)#ip nat inside source list access-list-number pool name`	Ingrese el comando global `no ip nat inside source` para eliminar la traducción dinámica de origen.
4	Especifique la interfaz interna. `Router(config)#interface type number`	Ingrese el comando `interface`. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.
5	Marque la interfaz como conectada al interior. `Router(config-if)#ip nat inside`	
6	Especifique la interfaz externa. `Router(config)#interface type number`	
7	Marque la interfaz como conectada al exterior. `Router(config-if)#ip nat outside`	
8	Salga del modo de configuración de interfaz. `Router(config-if)# exit`	

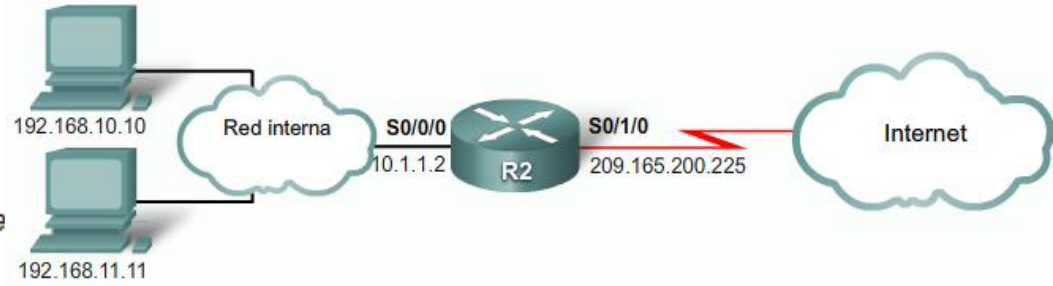
```
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
!—Defines a pool of public IP addresses under the pool name NAT-POOL1
access-list 1 permit 192.168.0.0 0.0.255.255
!—Defines which addresses are eligible to be translated
ip nat inside source list 1 pool NAT-POOL1
!—Binds the NAT pool with ACL 1
interface serial 0/0/0
  ip nat inside
!—Identifies interface Serial 0/0/0 as an inside NAT interface
interface serial 0/1/0
  ip nat outside
!—Identifies interface Serial 0/1/0 as the outside NAT interface
```



Configuración de NAT con sobrecarga (Una IP pública)

Paso	Acción	Notas
1	Defina una lista de acceso estándar que permita las direcciones que se deben traducir. `Router(config)#access-list` *acl-number* `permit` *source [source-wildcard]*	Ingrese el comando global `no access-list` *access-list-number* para eliminar la lista de acceso.
2	Establezca la traducción dinámica de origen; para hacerlo, especifique la lista de acceso definida en el paso anterior. `Router(config)#ip nat inside source list` *acl-number* `interface` *interface* `overload`	Ingrese el comando global `no ip nat inside source` para eliminar la traducción dinámica de origen. La palabra clave de sobrecarga habilita PAT.
3	Especifique la interfaz interna. `Router(config)#interface` *type number* `Router(config-if)#ip nat inside`	Ingrese el comando `interface`. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.
4	Especifique la interfaz externa. `Router(config-if)#interface` *type number* `Router(config-if)#ip nat outside`	

```
access-list 1 permit 192.168.0.0 0.0.255.255
!—Defines which addresses are eligible to be translated
ip nat inside source list 1 interface serial 0/1/0 overload
!—Identifies the outside interface Serial 0/1/0 as the inside global address to be overloaded
interface serial 0/0/0
  ip nat inside
!—Identifies interface Serial 0/0/0 as an inside NAT interface
interface serial 0/1/0
  ip nat outside
!—Identifies interface Serial 0/1/0 as the outside NAT interface
```



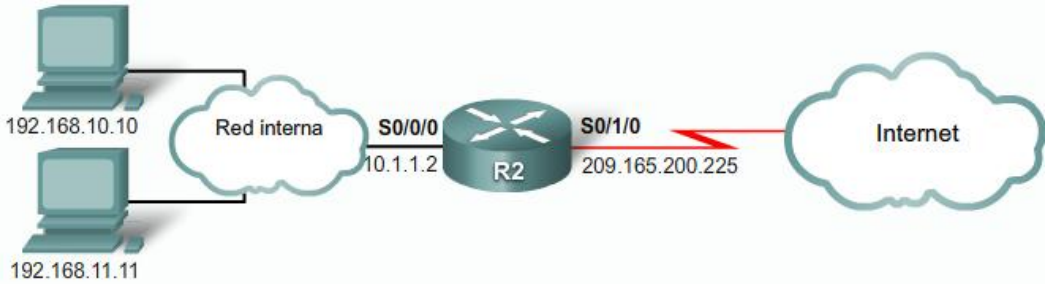
Configuración de NAT con sobrecarga (Pool IPs públicas)

Paso	Acción	Notas
1	Defina una lista de acceso estándar que permita las direcciones que se deben traducir. `Router(config)#access-list acl-number permit source [source-wildcard]`	Ingrese el comando global `no access-list access-list-number` para eliminar la lista de acceso.
2	Especifique la dirección global, como un conjunto, que se usará para la sobrecarga. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}.`	
3	Establezca la traducción de sobrecarga. `Router {config}#ip nat inside source list acl-number pool name overload.`	

4	Especifique la interfaz interna.
	`Router(config)#interface type number`
	`Router(config-if)#ip nat inside`
		Ingrese el comando **interface**. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.

5	Especifique la interfaz externa.
	`Router(config-if)#interface type number`
	`Router(config-if)#ip nat outside`	

```
access-list 1 permit 192.168.0.0 0.0.255.255
! – Defines which addresses are eligible to be translated
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
! – Defines a pool of addresses named NAT-POOL2 to be used in NAT translation
ip nat inside source list 1 pool NAT-POOL2 overload
! – Binds the NAT pool with ACL 1
interface serial 0/0/0
ip nat inside
! – Indentifies interface Serial 0/0/0 as an inside NAT interface
interface serial 0/1/0
ip nat outside
! – Indentifies interface Serial 0/1/0 as an outside NAT interface
```



Comandos clear NAT/PAT

```
Router#clear ip nat translation
```

- Clears all dynamic address translation entries

```
Router#clear ip nat translation inside global-ip local-ip [outside
local-ip global-ip]
```

- Clears a simple dynamic translation entry

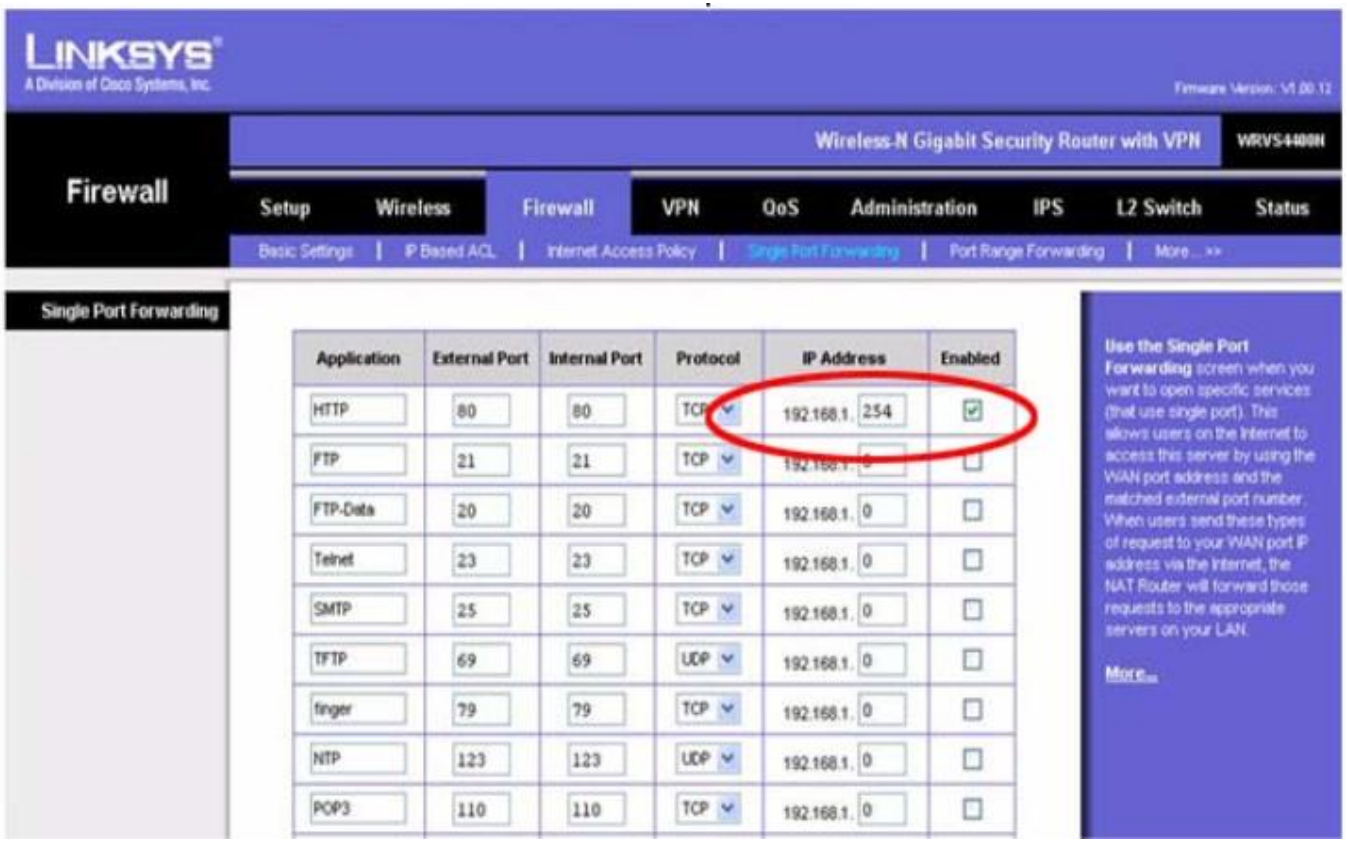
```
Router#clear ip nat translation protocol inside global-ip global-port
local-ip local-port [outside local-ip local-port global-ip
global-port]
```

- Clears an extended dynamic translation entry

Command	Description
clear ip nat translation *	Clears all dynamic address translation entries from the NAT translation table
clear ip nat translation inside *global-ip local-ip* **[outside** *local-ip global-ip*]	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation
clear ip nat translation protocol inside *global-ip global-port local-ip local-port* **[outside** *local-ip local-port global-ip global-port*]	Clears a simple dynamic translation entry

Redireccionamiento de puerto

- Permite a un usuario externo alcanzar un puerto de una dirección IP privada (perteneciente a una LAN) desde el exterior a través de un router habilitado para NAT.
- El problema es que NAT no permite las solicitudes iniciadas desde el exterior.
- El reenvío de puertos le permite identificar puertos específicos que se pueden reenviar a hosts internos.



Verificación de NAT/PAT

```
R2#show ip nat translations
Pro Inside global          Inside local          Outside local         Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642   209.165.200.254:80    209.165.200.254:80
tcp 209.165.200.225:62452  192.168.11.10:62452   209.165.200.254:80    209.165.200.254:80

R2#show ip nat translations verbose
Pro Inside global          Inside local          Outside local         Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642   209.165.200.254:80    209.165.200.254:80
    create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 4, lc_entries: 0
tcp 209.165.200.225:62452  192.168.11.10:62452   209.165.200.254:80    209.165.200.254:80
    create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 5, lc_entries: 0
R2#
```

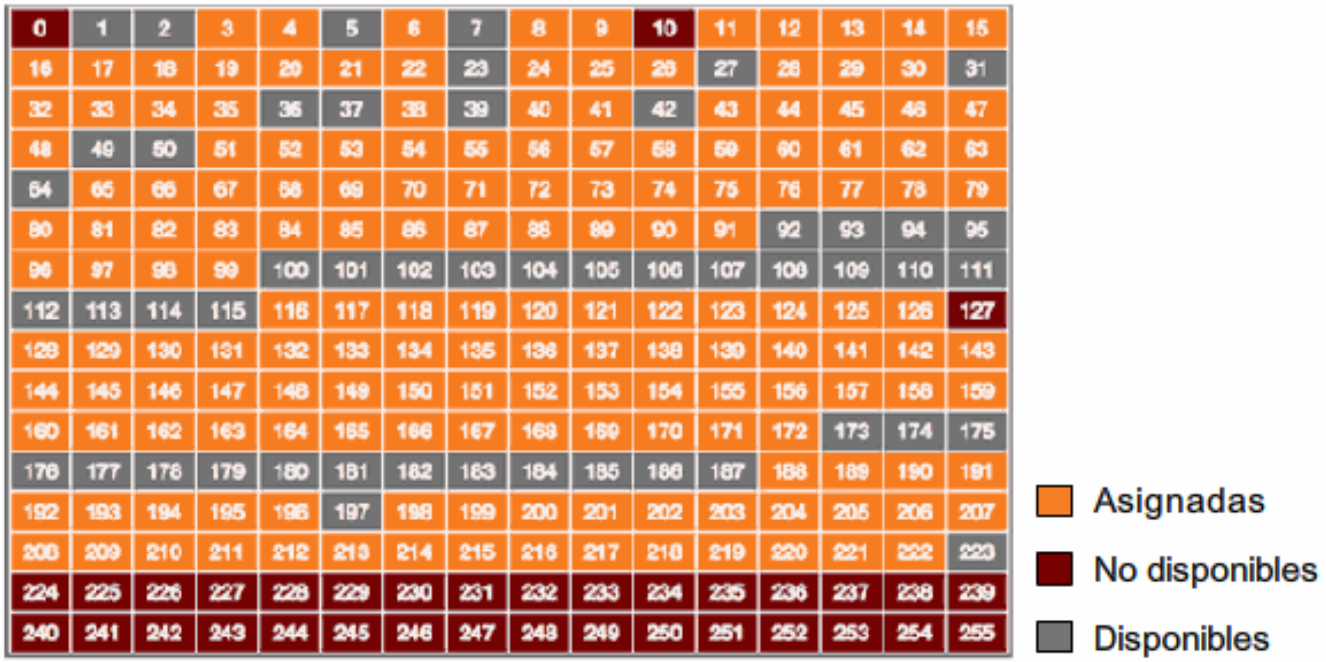
```
R2# debug ip nat
IP NAT debugging is on
R2#
*Oct  6 19:55:31.579: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14434]
*Oct  6 19:55:31.595: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6334]
*Oct  6 19:55:31.611: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14435]
*Oct  6 19:55:31.619: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14436]
*Oct  6 19:55:31.627: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14437]
*Oct  6 19:55:31.631: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6335]
*Oct  6 19:55:31.643: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6336]
*Oct  6 19:55:31.647: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14438]
*Oct  6 19:55:31.651: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6337]
*Oct  6 19:55:31.655: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14439]
*Oct  6 19:55:31.659: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6338]

<Output omitted>
```

```
R2#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0, Serial0/0/1
Hits: 173  Misses: 9
CEF Translated packets: 182, CEF Punted packets: 0
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0 refcount 3
Queued Packets: 0
R2#
```

Motivos para usar IPv6

- El espacio de direcciones de IPv4 proporciona aproximadamente 4.294’967.296 direcciones únicas.
- De éstas, sólo es posible asignar 3700 millones.
- En enero de 2007, aproximadamente 2400 millones de las direcciones IPv4 disponibles ya están asignadas
- El conjunto de direcciones se reduce por: Crecimiento de la población, Usuarios Móviles, Transporte, Productos electrónicos para los consumidores.

Bloques asignados: 2007



Representación de las direcciones IPv6

- Las direcciones IPv6 de 128 bits son más largas y necesitan una representación diferente a causa de su tamaño.
- Las direcciones IPv6 utilizan dos puntos (:) para separar entradas en una serie hexadecimal de 16 bits.

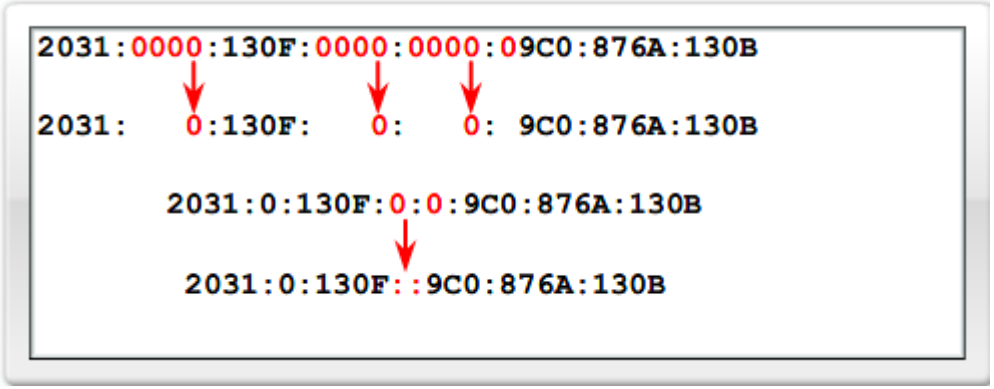
Formatos IPv6

Formato:

- **x:x:x:x:x:x:x:x**, en el que x es un campo hexadecimal de 16 bits
  - Distingue entre mayúsculas y minúsculas para A, B, C, D, E y F hexadecimal
- Los ceros iniciales son opcionales en un campo
- Los campos de ceros sucesivos pueden representarse como **::** sólo una vez por dirección

Ejemplos:

- **2031:0000:130F:0000:0000:09C0:876A:130B**
  - Puede representarse como **2031:0:130f::9c0:876a:130b**
  - No puede representarse como **2031::130f::9c0:876a:130b**
- **FF01:0:0:0:0:0:0:1** **FF01::1**
- **0:0:0:0:0:0:0:1** **::1**
- **0:0:0:0:0:0:0:0** **::**



Tipos de direcciones IPv6

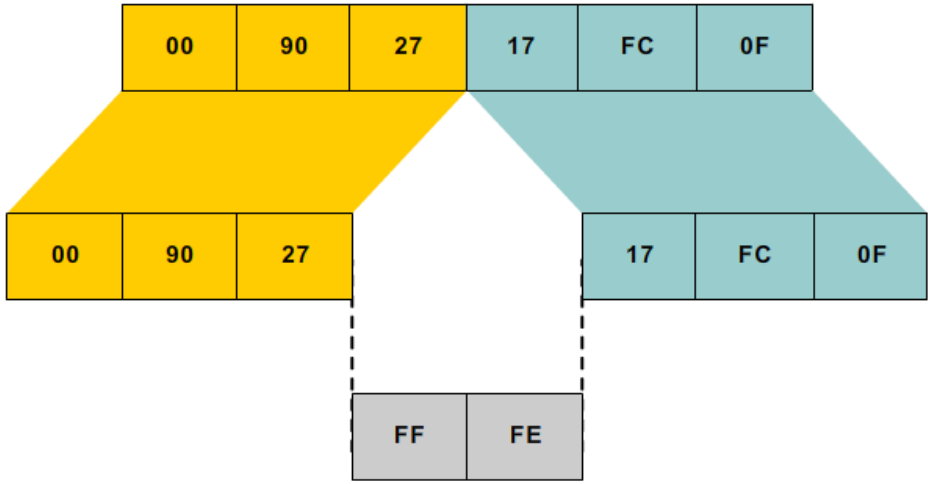
- Dirección de loobpack → ::1
- Dirección no especificada → ::

Tipo de dirección	Propósito	Prefijo	Prefijos vistos
Global Unicast	Paquetes unicast enviados a través de Internet. “Públicas”	2000::/3	2 ó 3
Unique local	Paquetes unicast dentro de una organización. “Privadas”. Reemplazan a las Site Local.	FD00::/8	FD
Link Local	Paquetes enviados un la subred local. nuevas dentro del concepto de direccionamiento con IP en la capa de red.	FE80::/10	FE8, FE9, FEA, FEB
Site Local	Como las privadas de IPv4. Su uso es problemático y esta siendo deprecado.	FEC0::/10	FEC, FED, FEE, FEF
Multicast (link local scope)	Multicast que permanecen en la red local. Usadas por los protocolos de enrutamiento	FE002::/16	FF02

Asignación de direcciones IPv6

- Asignación manual:
  - RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::72/64
- Asignación de ID de interfaz EUI-64:
  - RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::/64 eui-64
- Autoconfiguración sin estado →Entrega direcciones IP y Gateway
- DHCPv6 (con estado) → Parecido a DHCPv4.

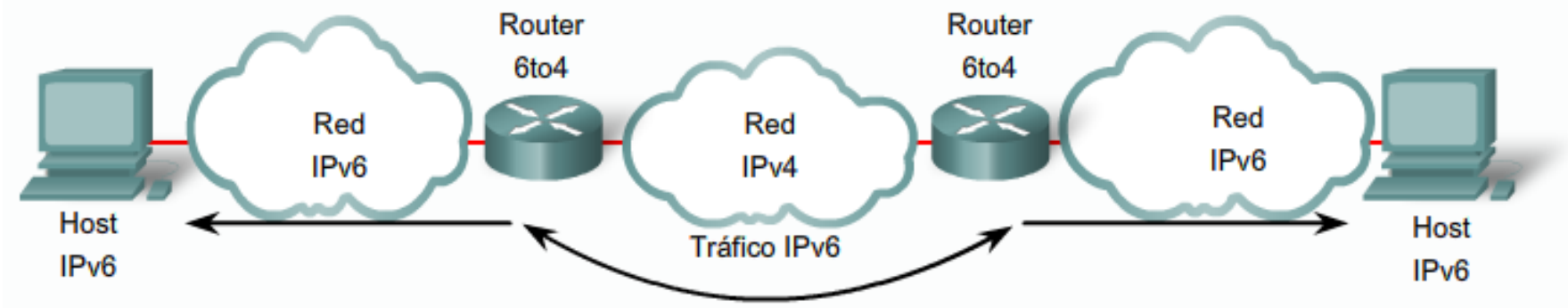
Asignación estática	Asignación dinámica
• Asignación manual de ID de interfaz • Asignación de ID de interfaz EUI-64	• Autoconfiguración sin estado • DHCPv6 (con estado)



Formato EUI-64

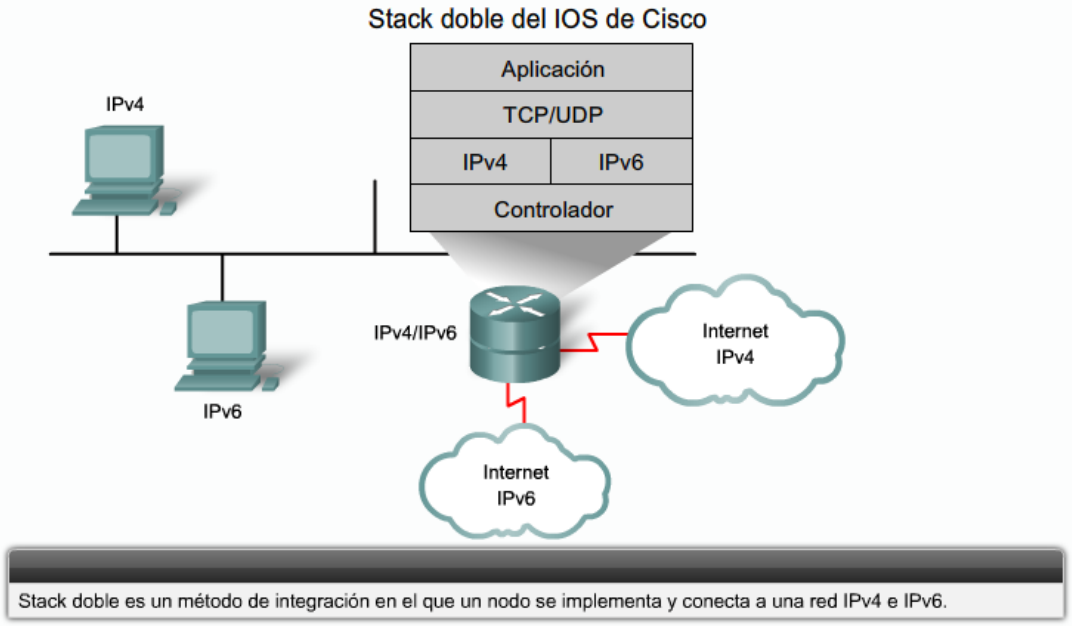
Estrategias de migración a IPv6

- Stack Doble → Un nodo tiene implementación y conectividad para redes IPv4 e IPv6. Opción recomendada .
- Tunneling → La segunda más importante. Existen varios:
  - Manual IPv6 sobre IPv4 →Un paquete de IPv6 se encapsula dentro del protocolo IPv4. Requiere routers de stack doble.
  - Dinámico 6to4 → Establece automáticamente la conexión de islas de IPv6 a través de la red IPv4, normalmente Internet.
  - ISATP → Utiliza la red IPv4 subyacente como capa de enlace para IPv6.
  - Teredo → Automático de host a host en lugar de tunneling de gateway.
- NAT-PT → Cisco IOS Release 12.3(2)T y posteriores.
  - Permite la comunicación directa entre hosts que utilizan versiones diferentes del protocolo IP. Es la opción menos favorable y debe utilizarse como último recurso.

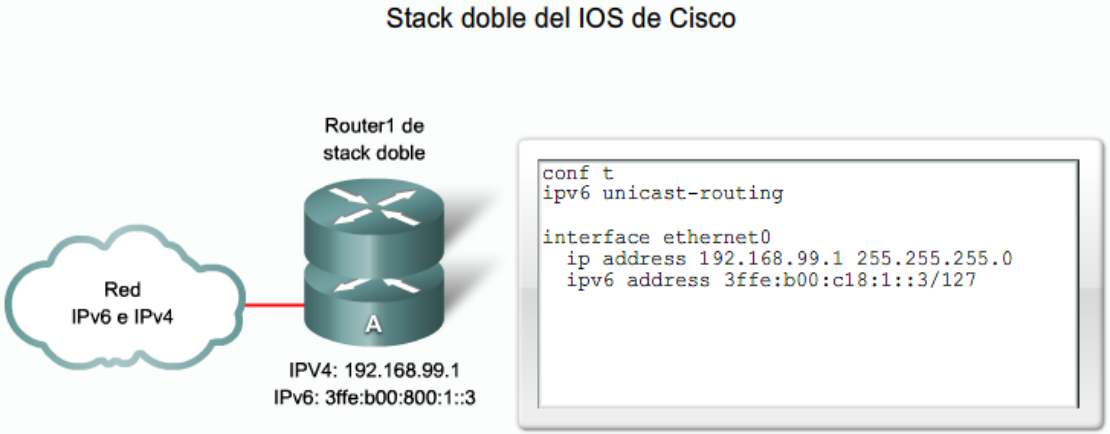


Stack doble en el IOS de Cisco

- Cada nodo tiene dos stacks de protocolos con la configuración en la misma interfaz o en varias interfaces.
- Un nodo de stack doble elige qué stack utilizar en función de la dirección de destino del paquete.
- Prefiere IPv6 si esta disponible



Stack doble es un método de integración en el que un nodo se implementa y conecta a una red IPv4 e IPv6.

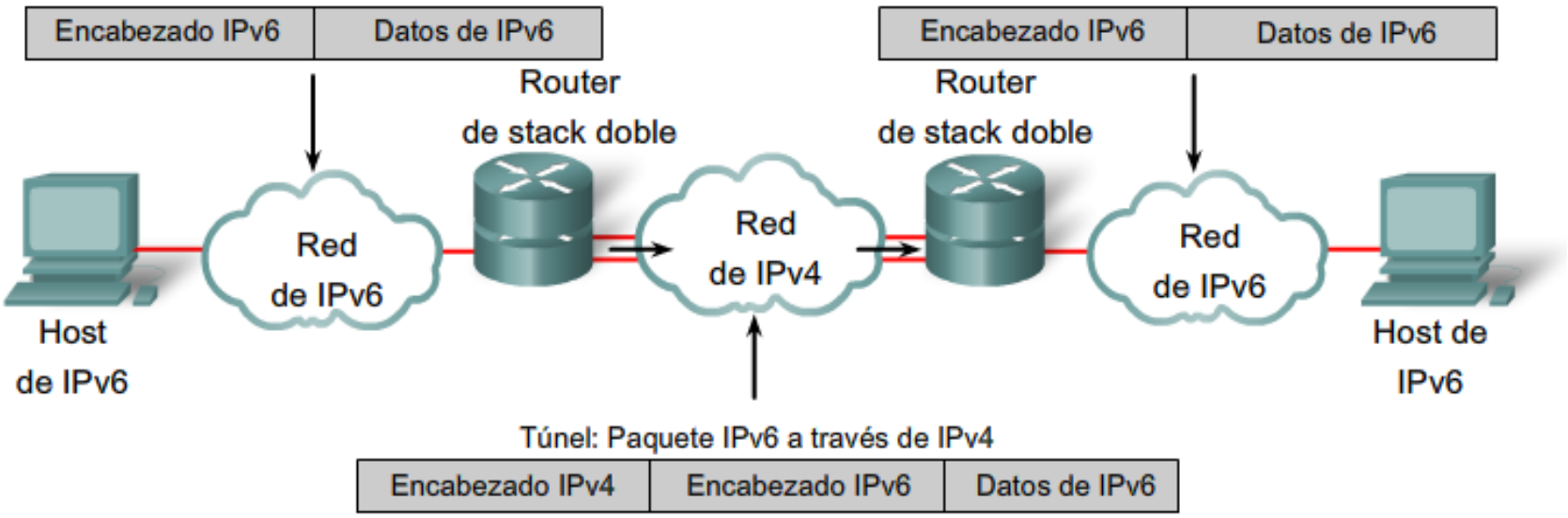


Cuando en una interfaz se configuran tanto IPv4 como IPv6, la interfaz se considera de stack doble.

- Cisco IOS Release 12.2(2)T y posteriores (con el conjunto de funciones apropiado) ya admiten IPv6.
- Tan pronto como configure IPv4 básico e IPv6 en la interfaz, la interfaz es de stack doble y reenvía el tráfico IPv4 e IPv6 en esa interfaz.

Tunneling IPv6

- Método en el cual un paquete IPv6 se encapsula dentro de otro protocolo, por ejemplo, IPv4.
- Requiere routers de stack doble.
- Problemas:
  - MTU se reduce 20 octetos si encabezado IPv4 no tiene campo opcional.
  - Los problemas de estas redes son difíciles de resolver
- Técnica intermedia, no solución definitiva. El objetivo final debe ser IPv6 nativa.



Protocolo de enrutamiento RIPng

- Las rutas de IPv6 usan los mismos protocolos y las mismas técnicas que IPv4.
- Definido por la RFC 2080
- Es compatible con Cisco IOS Release 12.2(2)T y posteriores.
- Envía actualizaciones por el puerto UDP 521.
- En implementaciones de stack doble, se necesitan RIP y RIPng.

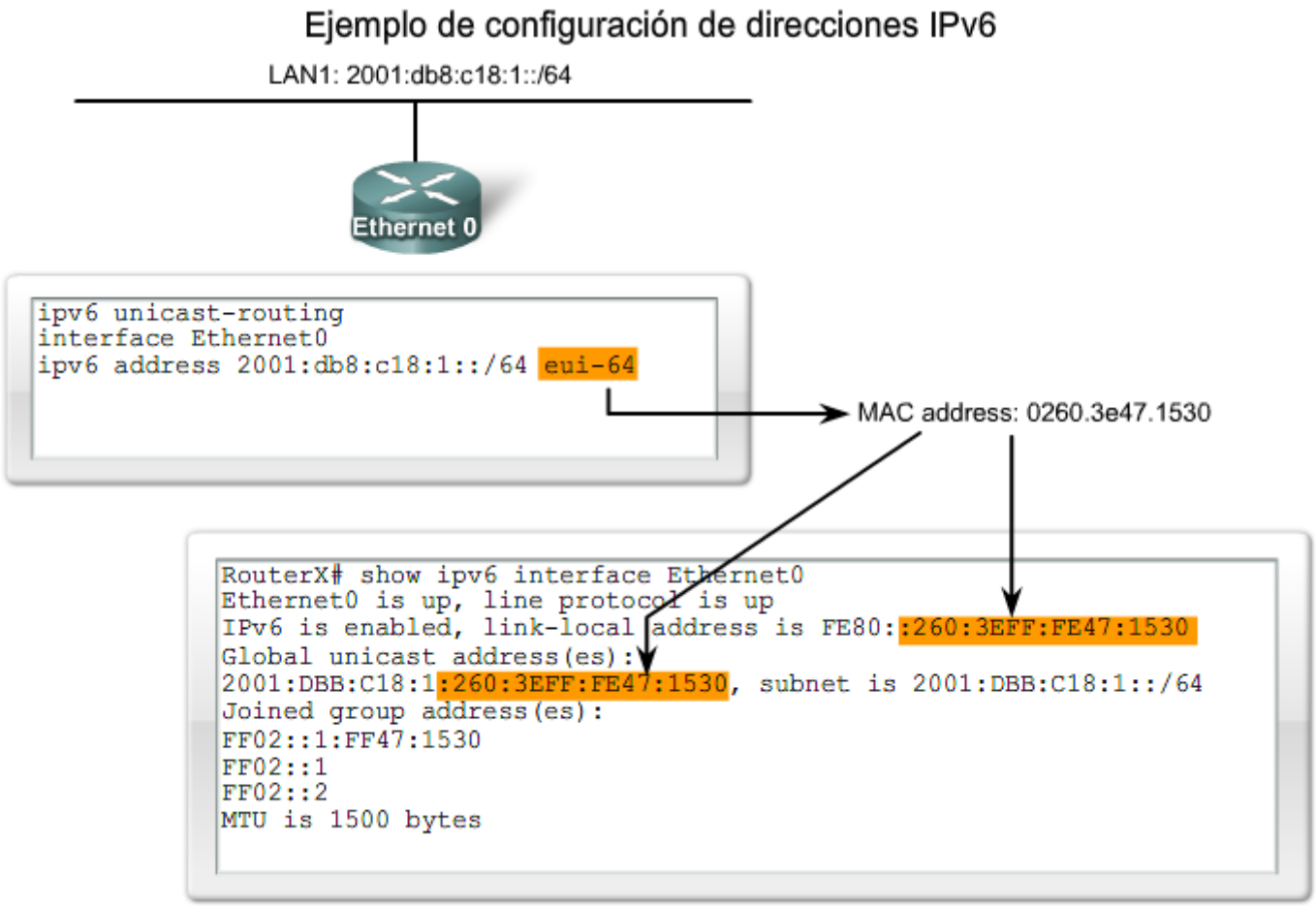
Características similares a IPv4:

- Vector distancia, radio de 15 saltos, horizonte dividido y envenenamiento en reversa
- Basado en RIPv2

Características actualizadas para IPv6:

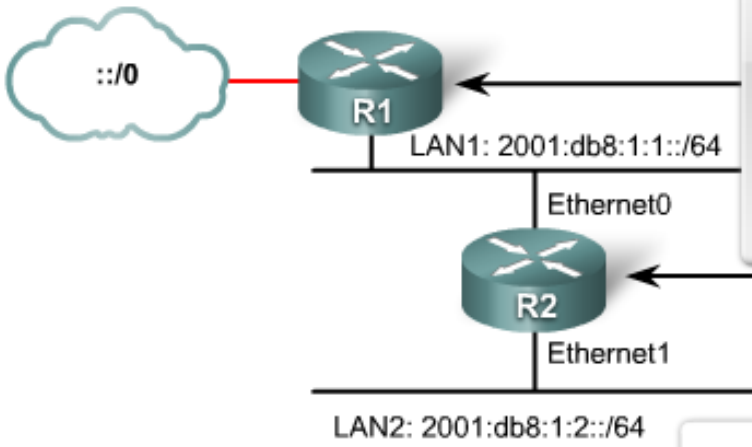
- Prefijo IPv6, dirección IPv6 de siguiente salto
- Utiliza el grupo multicast FF02::9, el grupo multicast all-rip-routers, como la dirección de destino para las actualizaciones RIP
- Usa IPv6 para transporte
- RIPng designado

Configuración de IPv6 en routers Cisco



Comando	Propósito
RouterX(config)# **ipv6 unicast-routing**	Habilita el reenvío de tráfico IPv6
RouterX(config-if)# **ipv6 address ipv6prefix/prefix-length eui-64**	Configura las direcciones IPv6 de la interfaz

Configuración de RIPng




```
ipv6 unicast-routing
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:1:1::/64 eui-64
 ipv6 rip RT0 enable
```

```
ipv6 unicast-routing
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:1:1::/64 eui-64
 ipv6 rip RT0 enable

interface Ethernet1
 ipv6 address 2001:db8:1:2::/64 eui-64
 ipv6 rip RT0 enable
```

Comando	Propósito
`RouterX(config)#ipv6 router rip name`	Crea e ingresa al modo de configuración de router RIP.
`RouterX(config-if)#ipv6 rip name enable`	Configura RIP en una interfaz.

Verificación de problemas IPv6

- Diferentes comandos de verificación:

Comando	Propósito
`show ipv6 interface`	Muestra el estado de las interfaces configuradas para IPv6.
`show ipv6 interface brief`	Muestra el estado resumido de las interfaces configuradas para IPv6.
`show ipv6 neighbors`	Muestra la información en caché de la detección de vecinos IPv6.
`show ipv6 protocols`	Muestra los parámetros y el estado actual de los procesos del protocolo de enrutamiento activo IPv6.
`show ipv6 rip`	Muestra información acerca de la actual
`show ipv6 route`	Muestra la tabla de enrutamiento IPv6 actual.
`show ipv6 route summary`	Muestra la forma resumida de la tabla de enrutamiento IPv6 actual.
`show ipv6 routers`	Muestra información de publicación del router IPv6 que se recibe de otros routers.
`show ipv6 static`	Muestra sólo las rutas IPv6 estáticas instaladas en la tabla de enrutamiento.
`show ipv6 static 2001:db8:5555:0/16`	Muestra información sólo de la ruta estática en cuanto a la dirección específica que se suministró.
`show ipv6 static interface serial 0/0`	Muestra información sólo de la ruta estática con la interfaz especificada como la interfaz de salida.
`show ipv6 static detail`	Muestra una entrada más detallada para las rutas IPv6 estáticas.
`show ipv6 traffic`	Muestra estadísticas sobre el tráfico IPv6.

Resolución de problemas IPv6

- Diferentes comandos de resolución:

Comando	Propósito
`clear ipv6 rip`	Borra rutas de la tabla de enrutamiento RIP IPv6 y, si están instaladas, las rutas de la tabla de enrutamiento IPv6.
`clear ipv6 route *`	Borra todas las rutas de la tabla de enrutamiento IPv6. NOTA: La eliminación de todas las rutas de la tabla de enrutamiento generará un alto índice de uso de la CPU mientras se reconstruye la tabla de enrutamiento.
`clear ipv6 route 2001:db8:c18:3::/64`	Elimina esa ruta específica de la tabla de enrutamiento IPv6.
`clear ipv6 traffic`	Restablece los contadores de tráfico IPv6.
`debug ipv6 packet`	Muestra mensajes de debug para paquetes IPv6.
`debug ipv6 rip`	Muestra mensajes de debug para transacciones de enrutamiento RIP IPv6.
`debug ipv6 routing`	Muestra mensajes de debug para actualizaciones de la tabla de enrutamiento IPv6 y actualizaciones de la caché de ruta.

Resumen

- Dynamic Host Control Protocol (DHCP)

  Significa asignar direcciones IP y otra información automáticamente.

- DHCP operation

  –3 métodos diferentes de asignación

  - Manual
  - Automático
  - Dinámico

  – Pasos para configurar DHCP

  - Definir un rango de direcciones
  - Crear un pool DHCP
  - Configurar los parámetros específicos del pool (Rango, Gateway, DNS, etc)

Resumen

- Relay DHCP

  Concepto de usar un router para escuchar mensajes DHCP de los clientes DHCP y enviar esos mensajes al servidor en una subred diferente.

- Troubleshooting DHCP

  –La mayoría de problemas surgen por errores en la configuración

  –Comandos que ayudan a la resolución de problemas

  - *Show ip dhcp*
  - *Show run*
  - *debug*

Resumen

- Direcciones IP privadas
  - –Clase A = 10.x.x.x
  - –Clase B = 172.16.x.x – 172.31.x.x
  - –Clase C = 192.168.x.x
- Network Address Translation (NAT)
  - –Traducción de direcciones IP privadas a direcciones IP Públicas
  - –Tipos de NAT
    - Stático
    - Dinámico
  - –Algunos comandos para la resolución de problemas
    - *Show ip nat translations*
    - *Show ip nat statistics*
    - *Debug ip nat*

Resumen

- IPv6
  - –Una dirección de 128 bits que usa dos puntos (:) para separar las entradas
  - – Normalmente escrita en 8 grupos de 4 dígitos hexadecimales
- Cisco IOS Dual Stack
  - – Una manera de permitirle a un nodo tener conectividad a una red IPv4 e IPv6 simultáneamente.
- Tunneling IPv6
  - – Un paquete IPV6 es encapsulado dentro de otro protocolo, normalmente IPv6.

Resumen

- Configurar RIPng con IPv6

  1ro Habilitar globalmente IPv6

  2nd Habilitar IPv6 en las interfaces en las cuales se requiere IPv6

  3rd Habilite RIPng usando:

  ipv6 rotuer rip *name*

  ipv6 router *name* enable