Arquitectura i Seguretat en Xarxes Informàtiques

Tema 6 – Aplicaciones y seguridad

Temario

- ~~1) Introducción~~
- ~~2) El medio físico~~
- ~~3) Redes de área local (LAN)~~
- ~~4) Redes IP~~
- ~~5) Protocolos UDP y TCP~~
- **6) Aplicaciones y seguridad**

Tema 6 – Aplicaciones y seguridad

- Introducción
- Aplicaciones de red
- Seguridad en redes
  - NAT
  - Firewall y ACLs
- Conceptos básico de criptografía
  - Seguridad en los protocolos

Tema 6 – Aplicaciones y seguridad

- **Introducción**
- Aplicaciones de red
- Seguridad en redes
  - NAT
  - Firewall y ACLs
- Conceptos básico de criptografía
  - Seguridad en los protocolos

Tema 6 – Aplicaciones y seguridad

- Objetivo de la capa aplicación
  - Mecanismos y protocolos que proporcionan determinados servicios a la red o al usuario
  - Proporcionar formatos estándares a los datos

Tema 6 – Aplicaciones y seguridad

- Introducción
- **Aplicaciones de red**
- Seguridad en redes
  - NAT
  - Firewall y ACLs
- Conceptos básico de criptografía
- Seguridad en los protocolos

Tema 6 – Aplicaciones de red

- Son aplicaciones propias de la red
- Sirvan para facilitar su funcionamiento, su aspecto de cara al usuario, su mantenimiento, etc.
- Por ejemplo
  - RIP es una aplicación de red ya que facilita la construcción de las tablas de encaminamiento y su mantenimiento en los routers
  - DHCP es una aplicación de red que permita la autoconfiguración de un host
  - DNS es un sistema que facilita los usuarios ya que pueden tratar los hosts con nombres en lugar de con números (@IP)
- RIP lo hemos visto, DHCP y DNS se tratan en AWUG2

Tema 6 – Aplicaciones y seguridad

- Introducción
- Aplicaciones de red
- **Seguridad en redes**
  - NAT
  - Firewall y ACLs
- Conceptos básicos de criptografía
  - Seguridad en los protocolos

Tema 6 – Seguridad en redes

- Objetivos de la seguridad
  - Confidencialidad: solo origen y destino deben poder entender el mensaje
  - Autentificación: origen y destino deben poder confirmar la identidad del otro
  - Integridad del mensaje: origen y destino quieren poder asegurar que el mensaje se recibe sin alterar y que nadie más lo haya podido recibir
  - Acceso y disponibilidad: los servicios deben ser accesibles y disponibles a los usuarios

Tema 6 – Seguridad en redes

- Tipos de ataques
  - De reconocimiento de vulnerabilidad y acceso
    - Tipo de servidores, sistema operativo, @IP, etc.
  - Denegación del servicio
    - Inhabilitar o corromper un servicio o una red
  - Introducir gusanos, virus o troyanos
    - Acceder, modificar y atacar otros servicios desde dentro una red

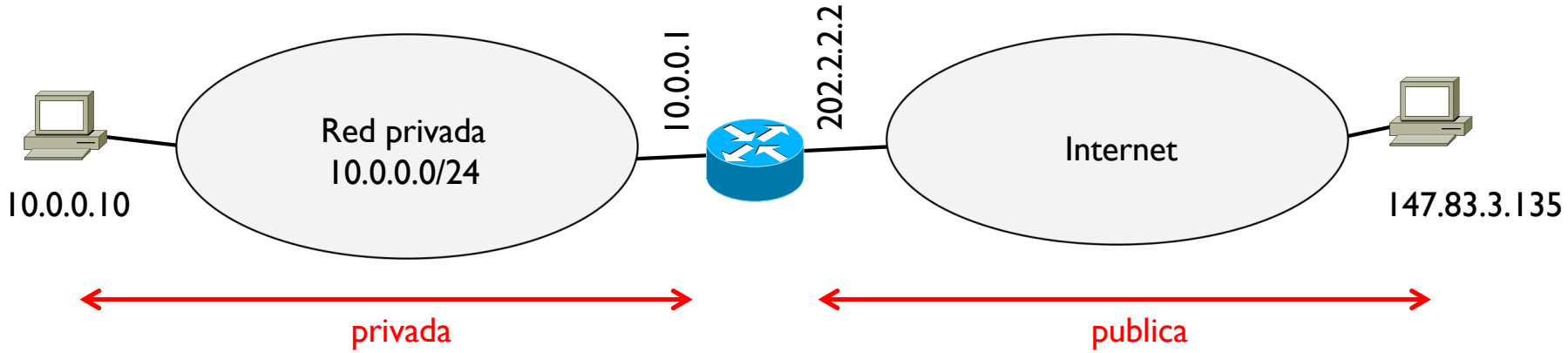
Tema 6 – Aplicaciones y seguridad

- Introducción
- Aplicaciones de red
- Seguridad en redes
  - **NAT**
  - Firewall y ACLs
- Conceptos básicos de criptografía
  - Seguridad en los protocolos

Tema 6 – NAT

- Network Address Translation
- RFC 1631, 2663, 3022
- Es un mecanismo (no es un protocolo)
- Objetivo
  - Permitir el uso de direcciones privadas (no visibles desde Internet) pero poder igualmente acceder a Internet
- Como
  - Traduciendo direcciones privadas en direcciones públicas
- Ventajas
  - Seguridad
  - Permite ahorrar @IP en Internet
  - Administración de la red (no depende de Internet ni del ISP)

Tema 6 – NAT



- Considerar un host en una red privada
- Si no hubiera NAT, este host no podría acceder ni recibir nada de Internet ya que su @IP es privada
- Se necesita configurar el router para que implemente NAT
  - Un router con NAT mantiene una tabla NAT donde se asocian @IP publicas con @IP privadas

Tema 6 – NAT

- NAT estático
  - Se asigna una @IP publica a una @IP privada
  - Principalmente para servidores
- NAT dinámico
  - Se configura un rango de @IP publicas y se asignan a las @IP privadas según se necesite
  - Principalmente para clientes
- PAT o NAT por puertos o NAT overload
  - Se usa una única @IP publica (generalmente la @IP del router hacía Internet) y se configura un rango de puertos
  - Todas las @IP privadas que van a Internet se traducen con la misma @IP publica
  - Principalmente para redes pequeñas

Tema 6 – NAT estático

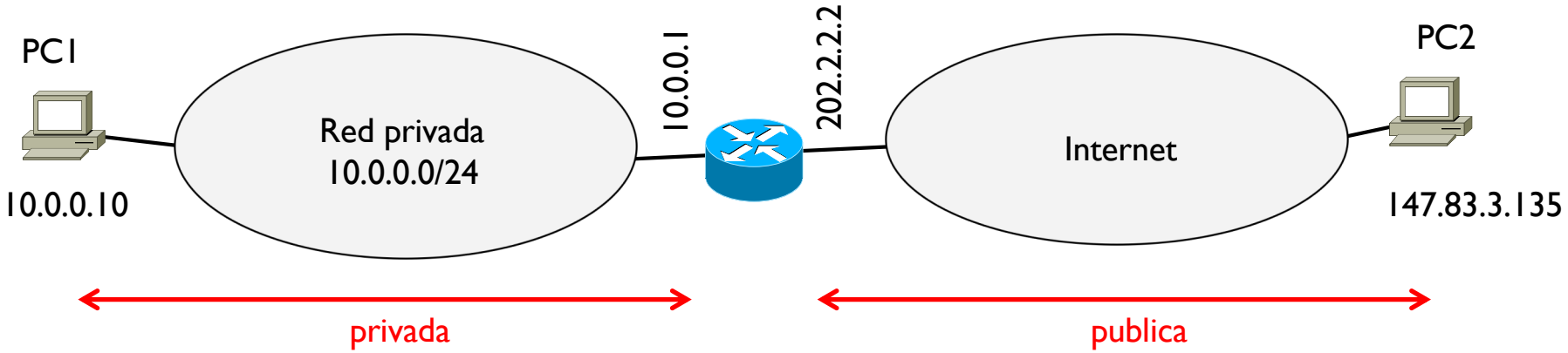


Tabla NAT

Direcciones internas	Direcciones externas

El router mantiene una tabla NAT con una columna con @IP internas (privadas) y otra columna con @IP externas (públicas)

Tema 6 – NAT estático

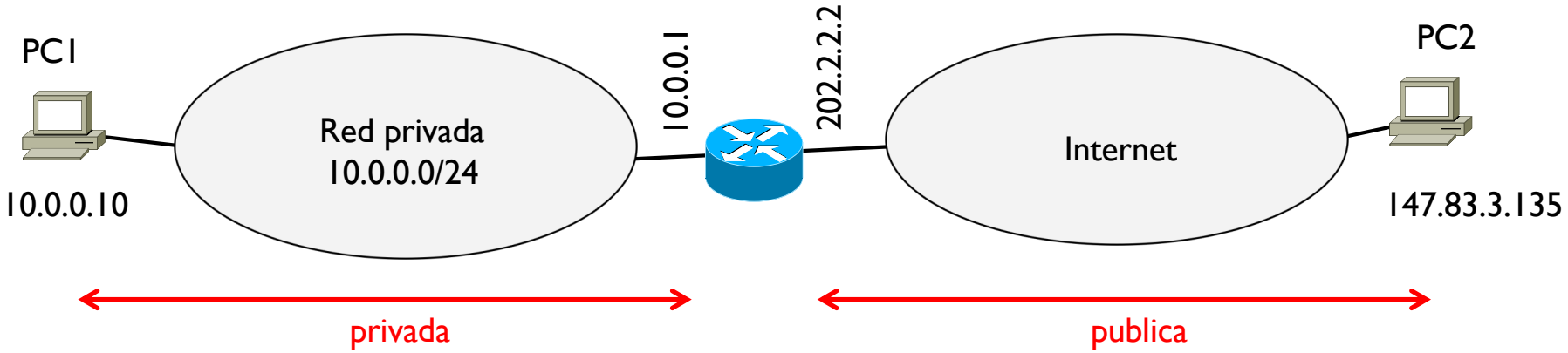


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10

En el caso de NAT estático, en el router se configura la traducción de la @IP privada 10.0.0.10 a la @IP pública 181.5.57.10

Tema 6 – NAT estático

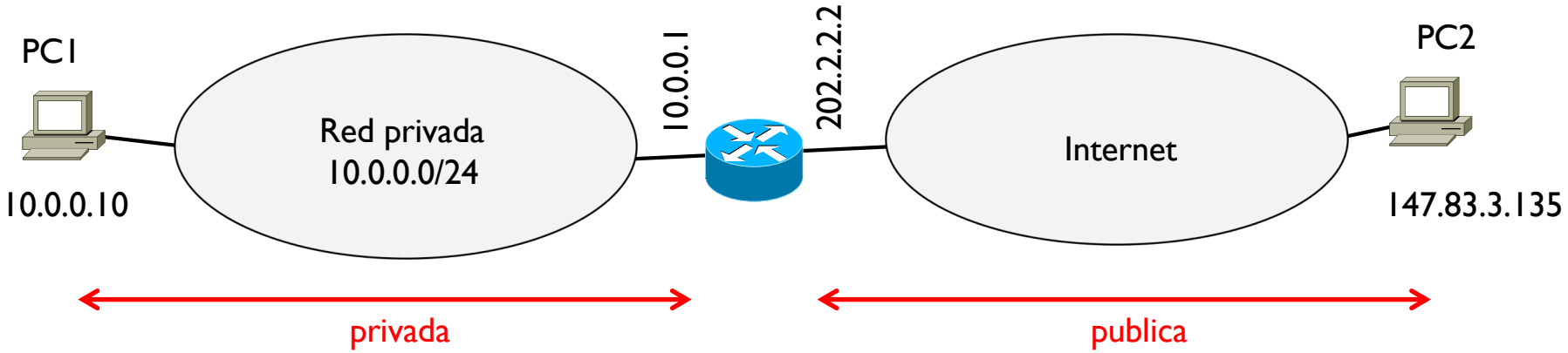
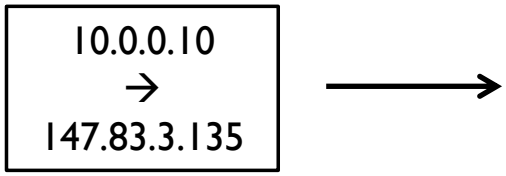


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



El host interno PC1 quiere transmitir a PC2 de Internet
El datagrama tendrá estas @IP origen y destino

Tema 6 – NAT estático

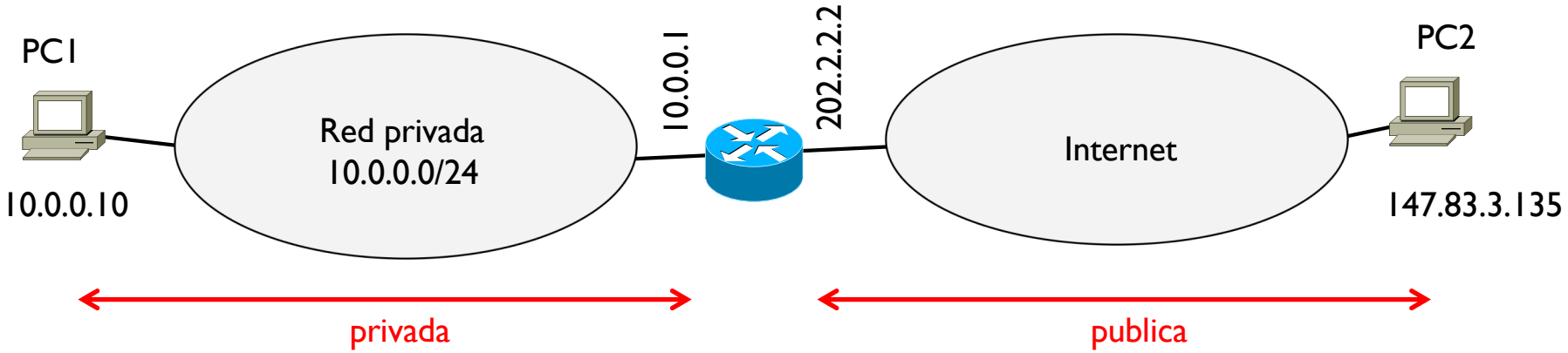
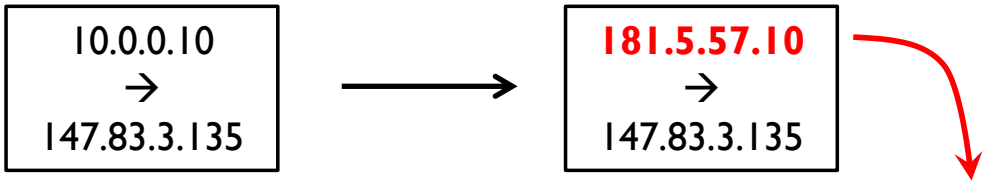


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



El router no puede transmitir este datagrama en Internet con esta @IP origen
El router substituye la @IP origen por la @IP que tiene asociada en la tabla NAT

Tema 6 – NAT estático

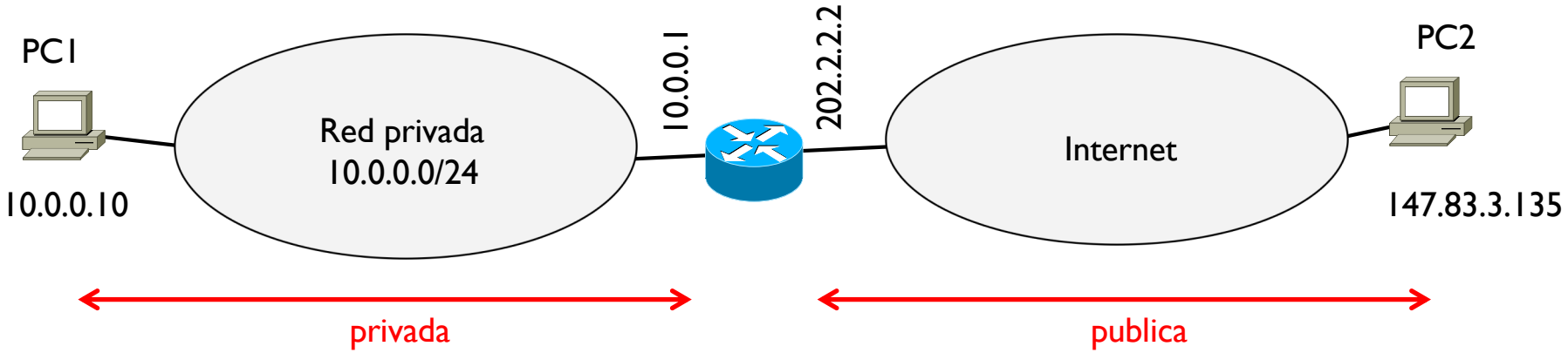
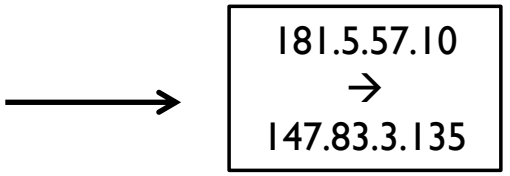


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



El destino PC2 recibe este datagrama con esta @IP origen
PC2 no puede saber cual es la @IP real de PC1

Tema 6 – NAT estático

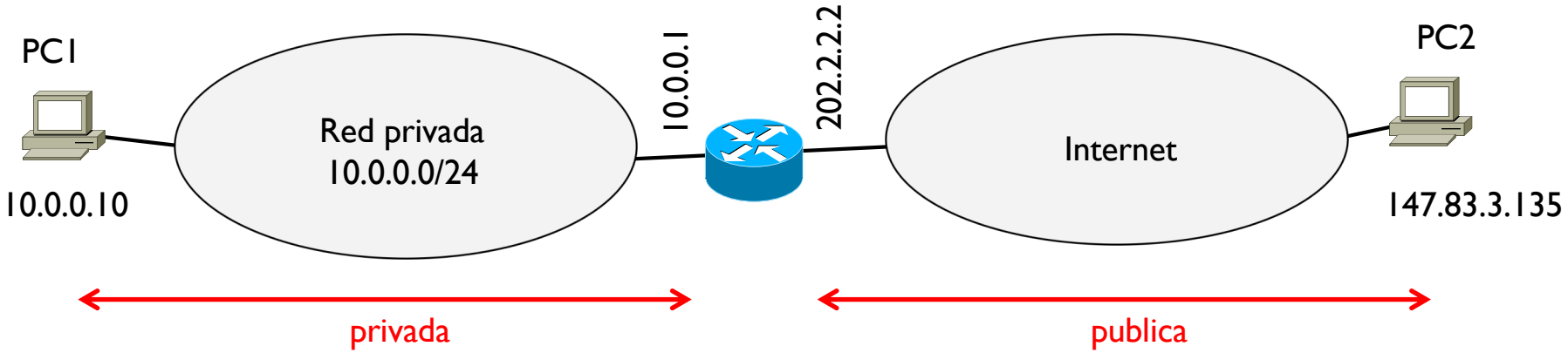


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10

147.83.3.135
→
181.5.57.10

Si PC2 quiere contestar al PC1, PC2 transmitirá un datagrama con estas @IP origen y destino
Para PC2, la @IP de PC1 es 181.5.57.10

Tema 6 – NAT estático

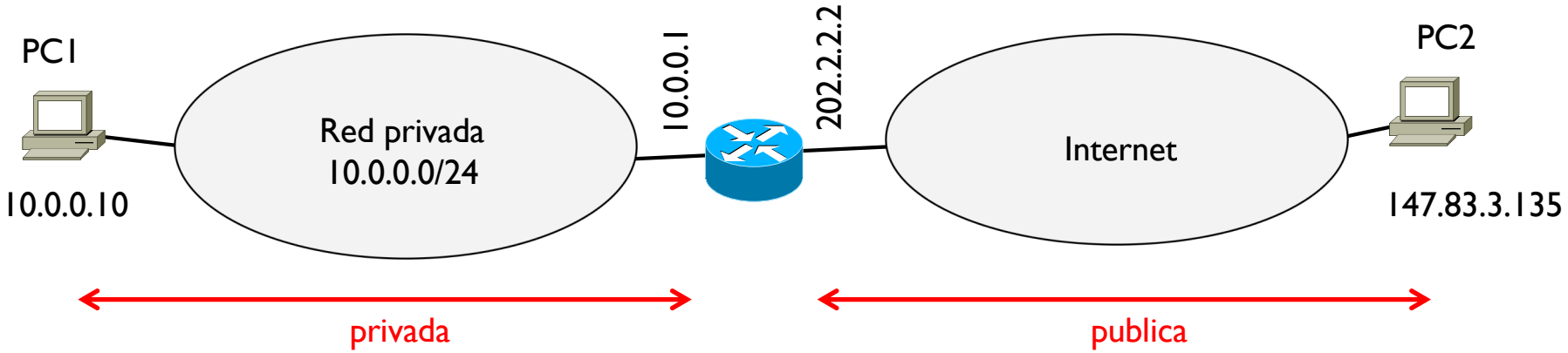
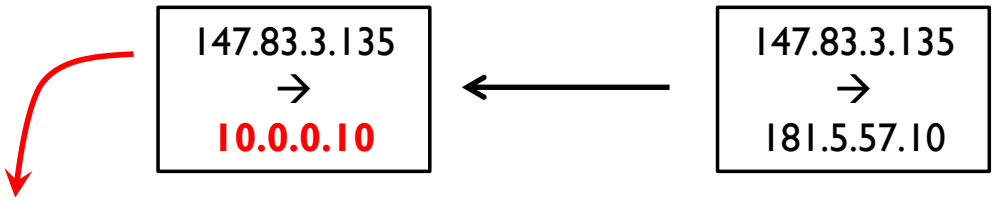


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



Cuando el datagrama llega al router, este hará la substitución inversa: cambia la @IP publica 181.5.57.10 en la @IP privada interna de PC1
En este caso la que cambia es la @IP destino

Tema 6 – NAT estático

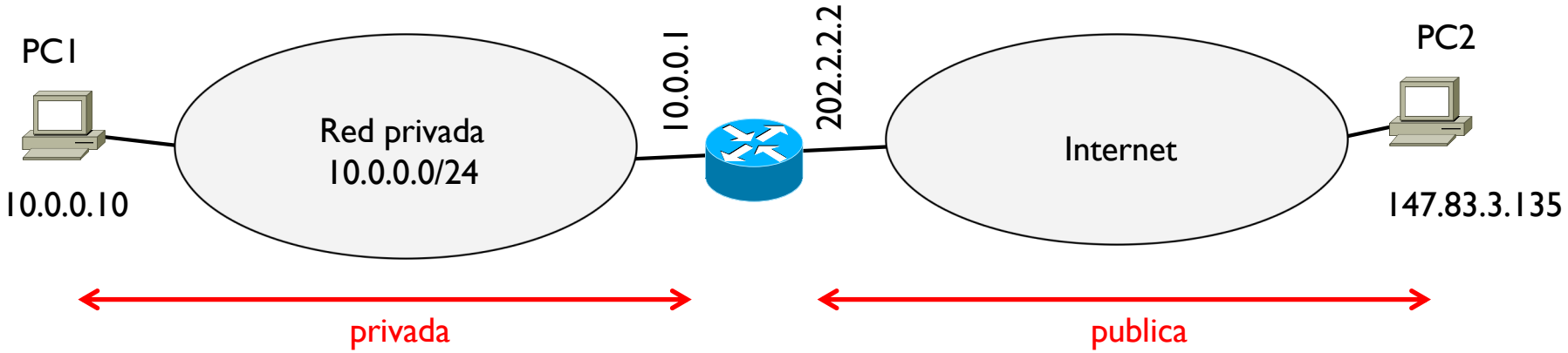
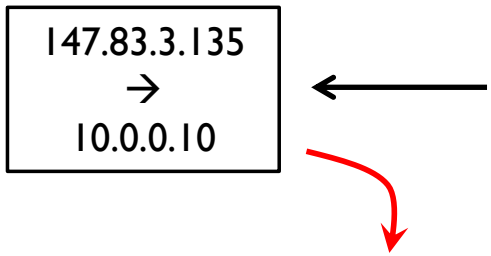


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



PC1 recibe correctamente el datagrama con su @IP destino

Tema 6 – NAT estático

- Si hubiera más hosts de la red privada que necesitan un NAT estático, entonces habría que configurar una entrada en la tabla NAT para cada @IP privada

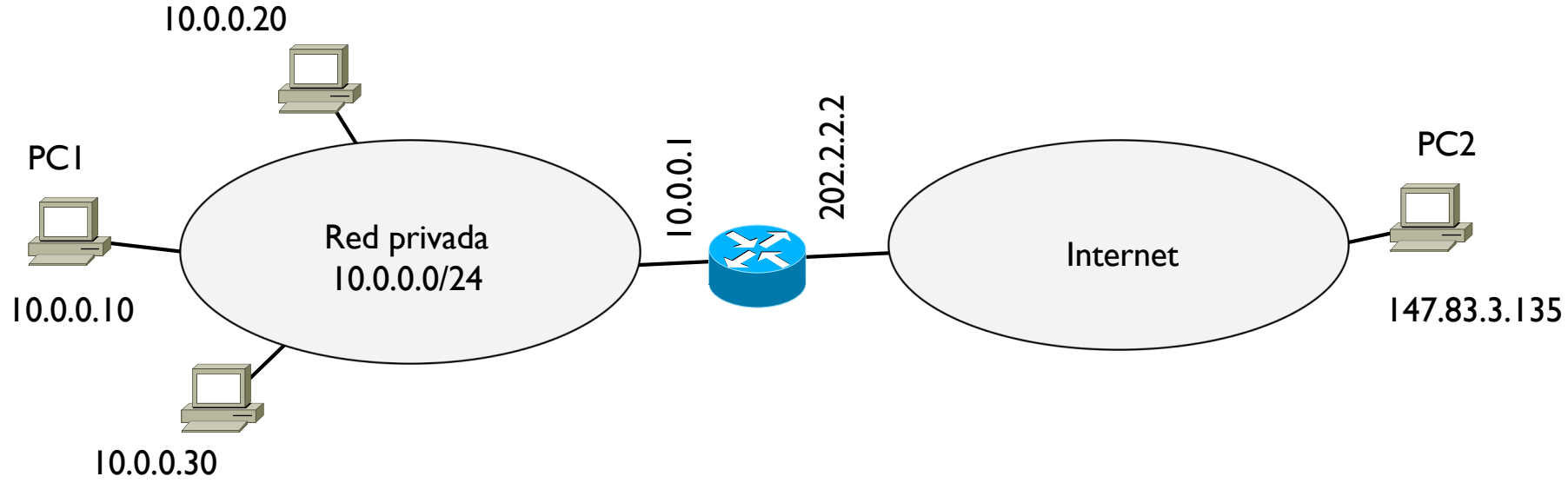


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10
10.0.0.20	181.5.57.11
10.0.0.30	181.5.57.12

Tema 6 – NAT estático

- Si hubiera más hosts de la red privada que necesitan un NAT estático, entonces habría que configurar una entrada en la tabla NAT para cada @IP privada

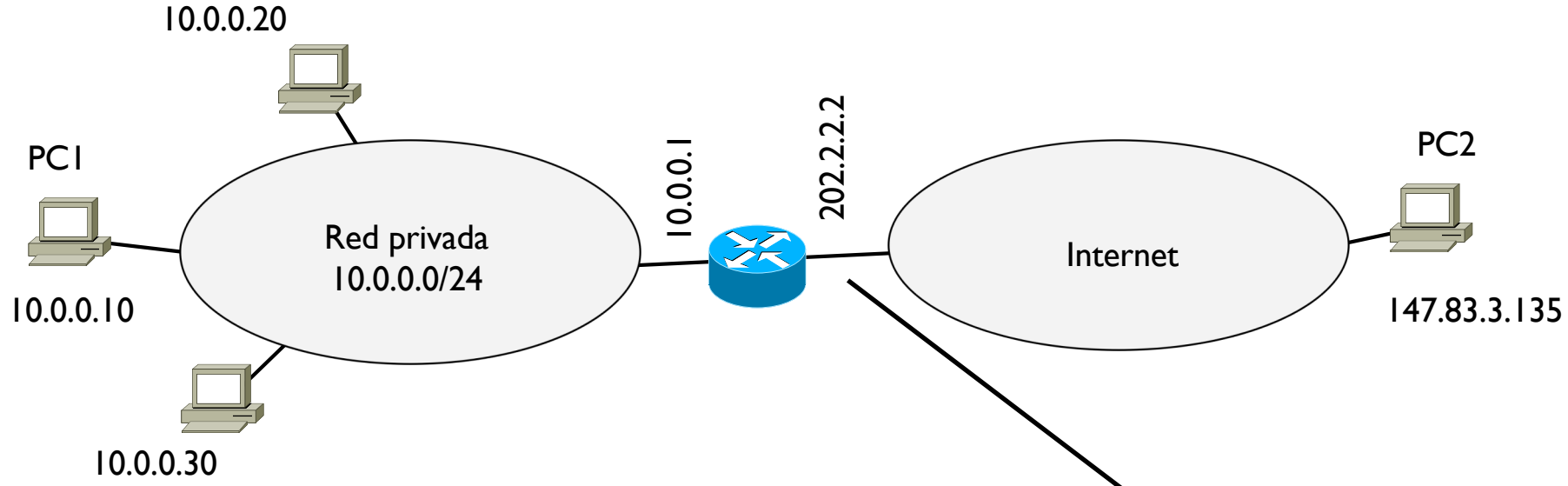


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10
10.0.0.20	181.5.57.11
10.0.0.30	181.5.57.12

Fijarse que en este ejemplo, se necesitan 4 @IP públicas
Es decir hay que reservar y pagar 4 @IP publicas

Tema 6 – NAT dinámico

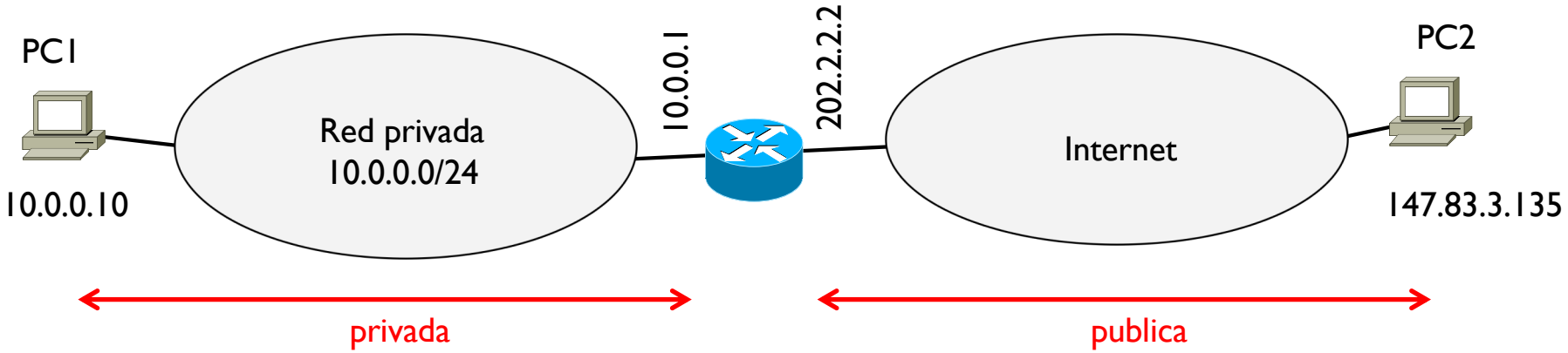


Tabla NAT

Direcciones internas	Direcciones externas	Duración

Rango: 180.0.0.1-180.0.0.10

También en este caso el router mantiene una tabla NAT. Ahora pero esta tabla está inicialmente vacía y tiene una columna más que se llama duración.
Y en el router se necesita configurar un rango de @IP publicas (previamente reservadas en Internet) disponibles para el NAT dinámico

Tema 6 – NAT dinámico

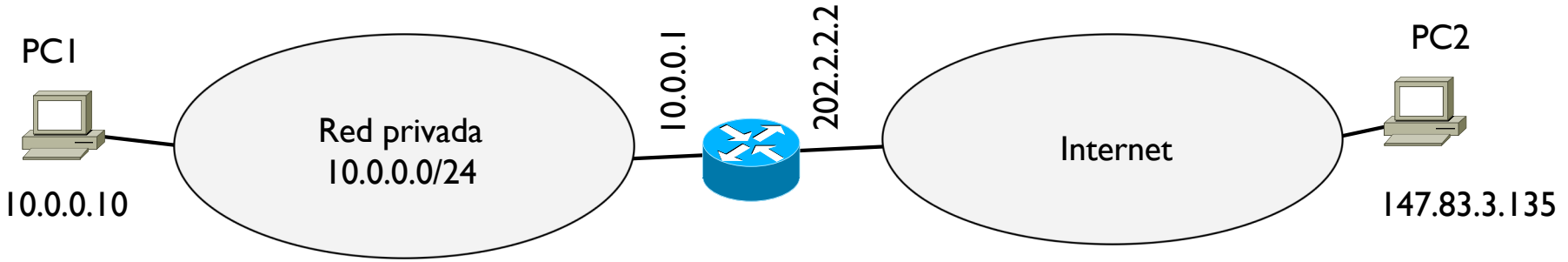


Tabla NAT

Rango: 180.0.0.1-180.0.0.10

Direcciones internas	Direcciones externas	Duración

La tabla NAT está inicialmente vacía

10.0.0.10
→
147.83.3.135

Como en el caso anterior, el host interno PC1 quiere transmitir a PC2 de Internet
El datagrama tendrá estas @IP origen y destino

Tema 6 – NAT dinámico

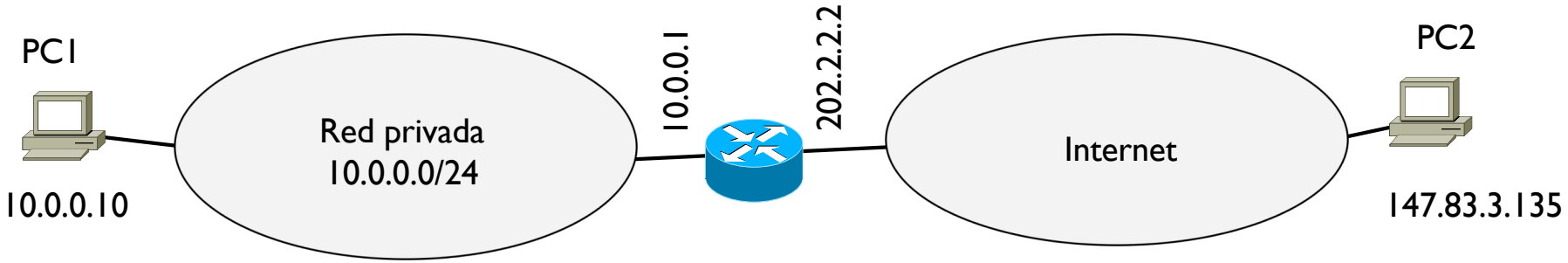
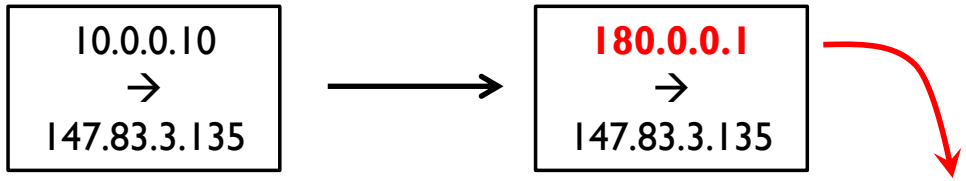


Tabla NAT

Direcciones internas	Direcciones externas	Duración
10.0.0.10	180.0.0.1	30 min

Rango: 180.0.0.1-180.0.0.10



Como en el caso anterior, este datagrama no se puede transmitir por Internet
El router substituye la @IP privada por la primera disponible del rango
Y además pone esta substitución en la tabla NAT asignándole una duración

Tema 6 – NAT dinámico

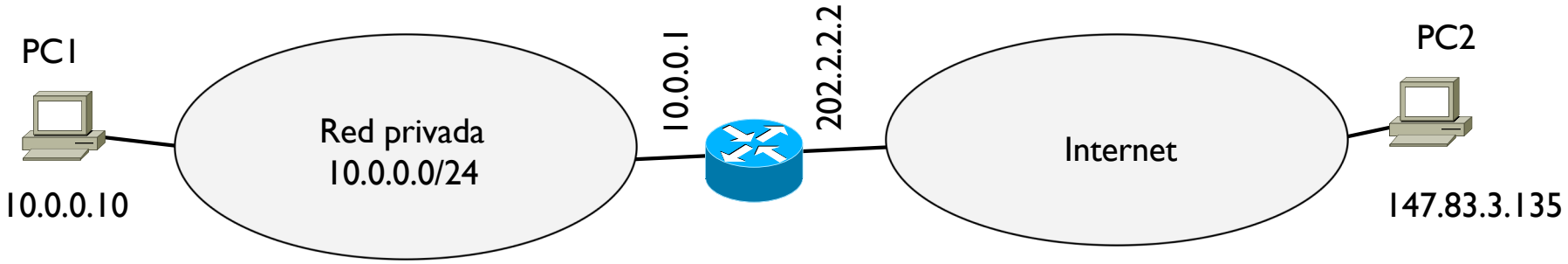
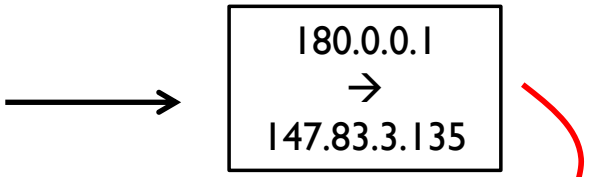


Tabla NAT

Direcciones internas	Direcciones externas	Duración
10.0.0.10	180.0.0.1	30 min

Rango: 180.0.0.1-180.0.0.10



El destino PC2 recibe este datagrama con esta @IP origen
PC2 no puede saber cual es la @IP real de PC1

Tema 6 – NAT dinámico

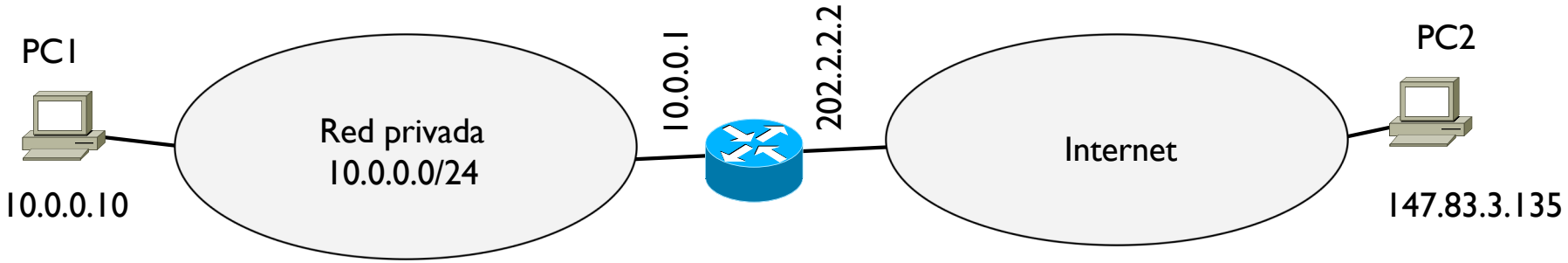
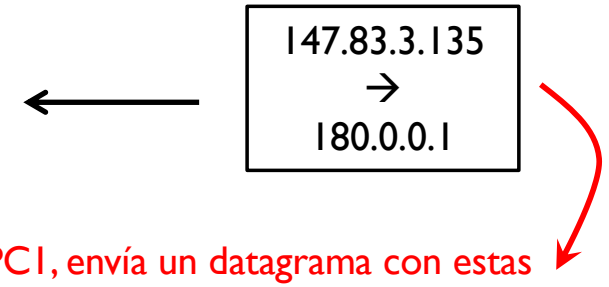


Tabla NAT

Direcciones internas	Direcciones externas	Duración
10.0.0.10	180.0.0.1	30 min

Rango: 180.0.0.1-180.0.0.10



Si PC2 quiere contestar a PC1, envía un datagrama con estas @IP origen y destino

Tema 6 – NAT dinámico

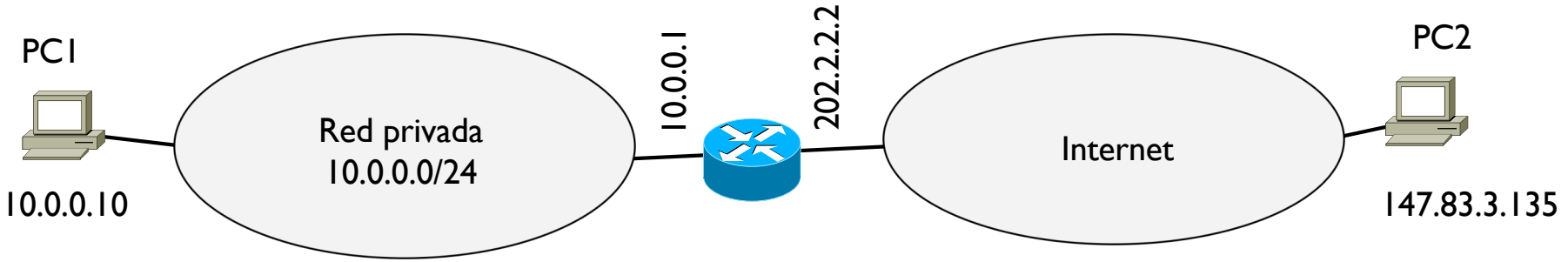
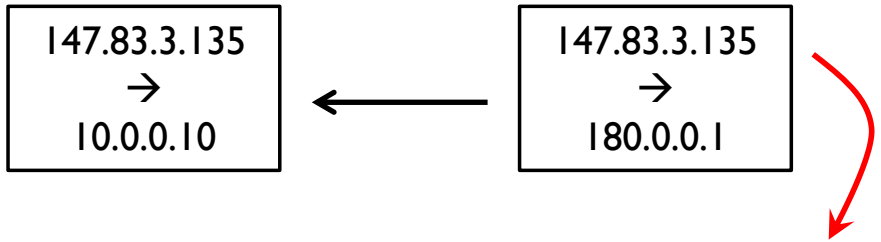


Tabla NAT

Direcciones internas	Direcciones externas	Duración
10.0.0.10	180.0.0.1	30 min

Rango: 180.0.0.1-180.0.0.10



Al recibir el datagrama, el router consulta la tabla NAT y hace la traducción inversa

Tema 6 – NAT dinámico

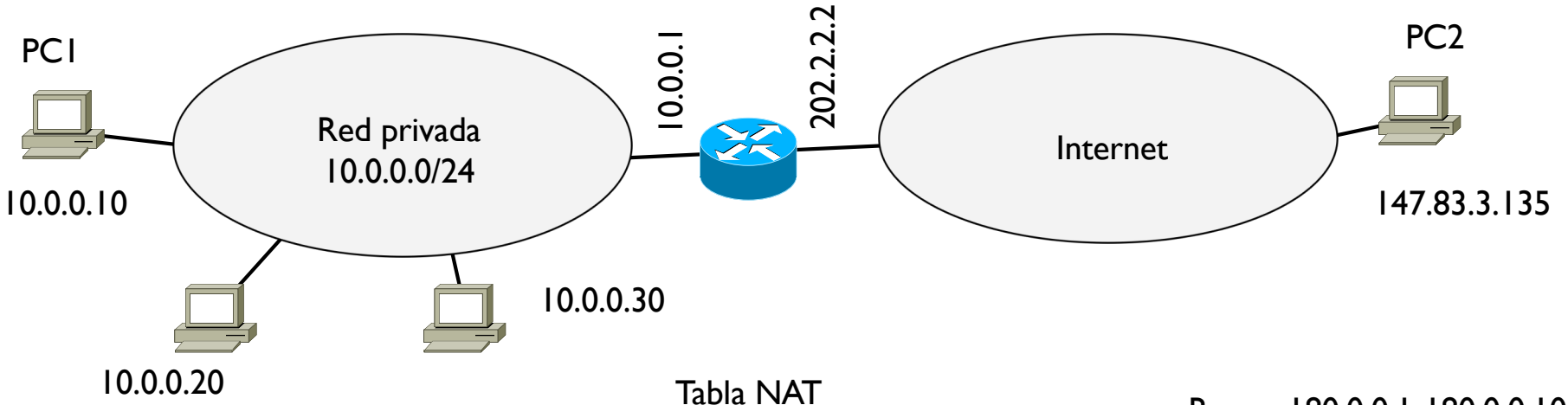


Tabla NAT

Rango: 180.0.0.1-180.0.0.10

Direcciones internas	Direcciones externas	Duración
10.0.0.10	180.0.0.1	30 min

Si hay otros PC de la red privada interna, estos no tienen entradas en la tabla NAT hasta que no envíen el primer datagrama hacia Internet
Si transmiten a Internet, el router asigna la primera @IP disponible del rango

Tema 6 – NAT dinámico

- En este caso se podría reservar un número inferior de @IP públicas del número de host de la red privada

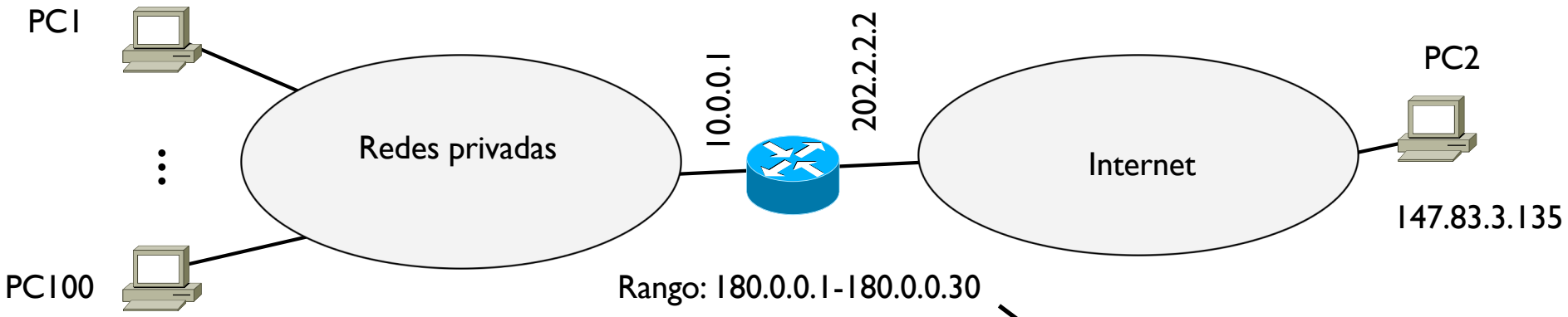


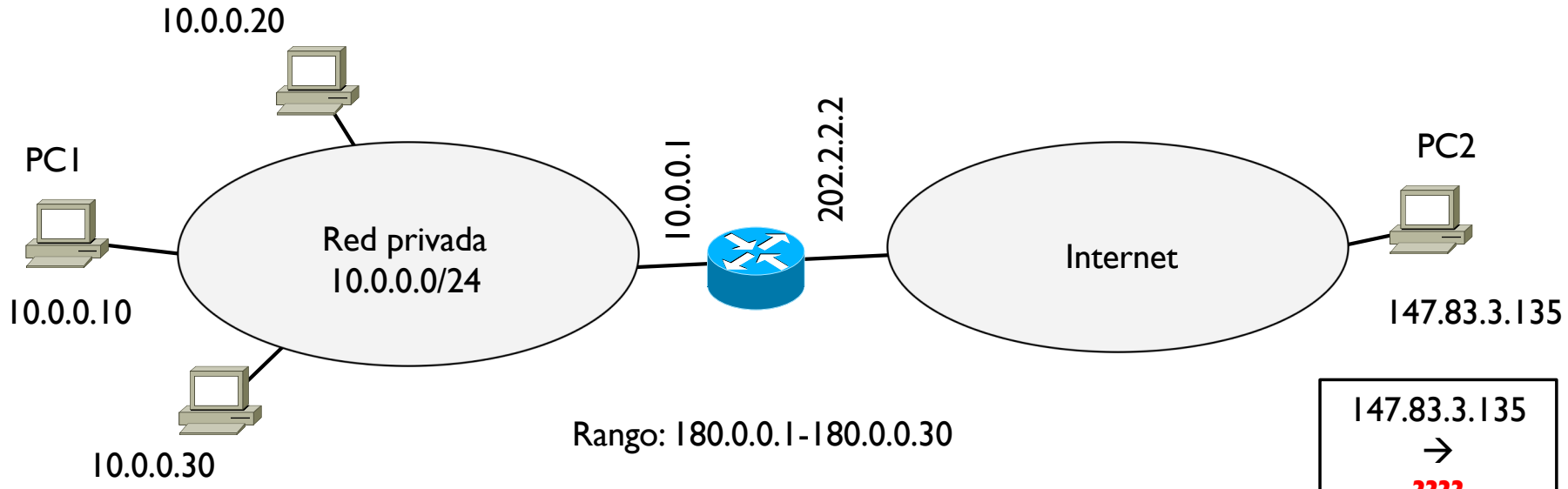
Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.38	180.0.0.1
10.0.0.41	180.0.0.2
10.0.0.124	180.0.0.3

Sabiendo que al mismo tiempo un número limitado de hosts de la red interna se comunican con Internet, se pueden reservar menos @IP que hosts e ir compartiéndolas según las necesidades

Tema 6 –NAT estático vs. dinámico

- En el caso de NAT dinámico, un host de Internet no puede empezar una comunicación con un host interno, ya que el externo no sabe cual es su @IP pública



Rango: 180.0.0.1-180.0.0.30

Tabla NAT

Direcciones internas	Direcciones externas

147.83.3.135
→
????

La @IP pública de PC1 podría ser cualquiera del rango
Además esta podría cambiar en el tiempo según como se han ido asignando

Tema 6 –NAT estático vs. dinámico

- En el caso de NAT estático, un host de Internet puede empezar una comunicación con un host interno ya que este tiene asignada una @IP pública fija

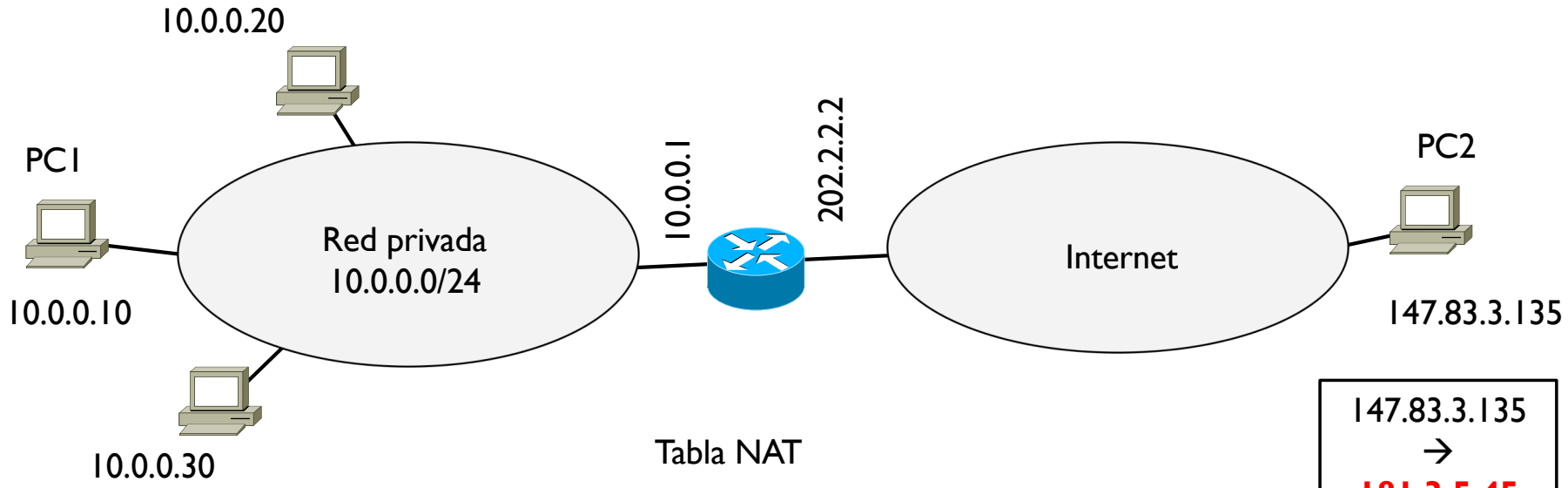


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.3.5.45

147.83.3.135 → **181.3.5.45**

La @IP pública de PC1 es siempre la misma
Además está @IP se puede registrar en DNS con asociado un nombre

Tema 6 – NAT estático vs. dinámico

- Por esta razón, el NAT estático se usa generalmente para servidores que están en la red interna y deben ser alcanzables desde Internet con una @IP fija y conocida
- El NAT dinámico se usa generalmente para clientes, donde son estos que empiezan una comunicación con otro host (típicamente un servidor)
  - Por lo tanto el cliente es el primero en pasar por el router que crea la traducción correspondiente
  - El servidor contesta a la @IP que el router ha asignado al cliente traduciendo por lo tanto también la comunicación en sentido contrario

Tema 6 – PAT

- Port Address Translation

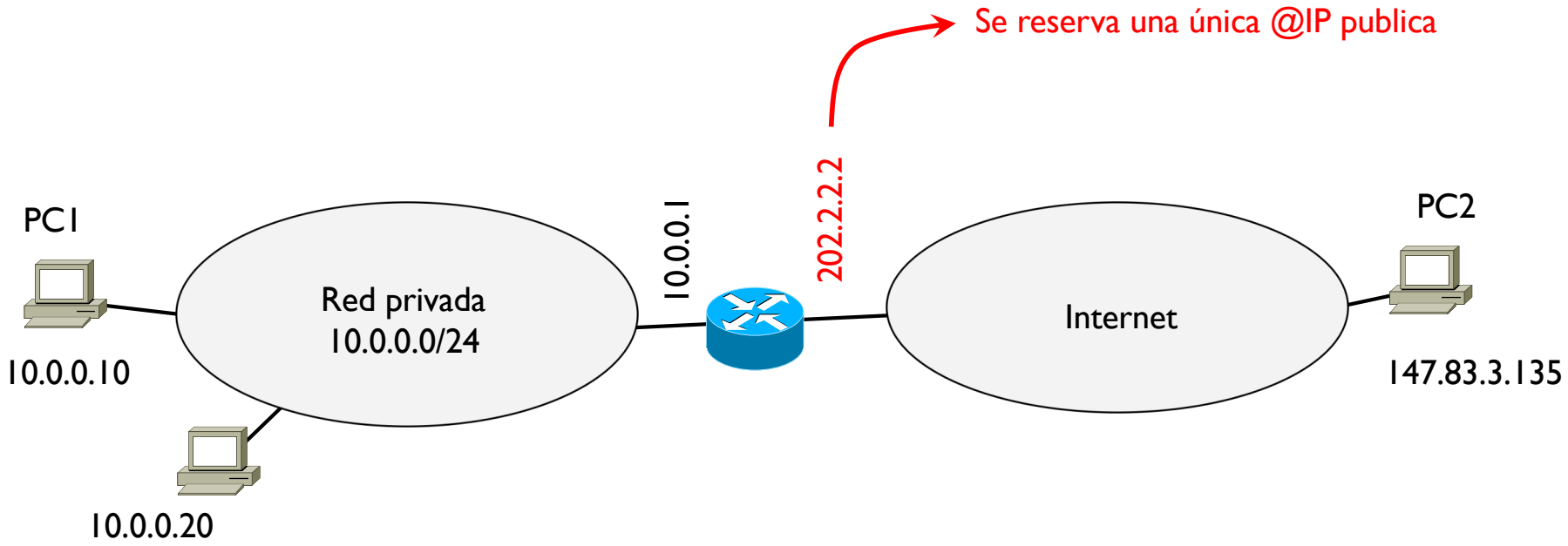


Tabla NAT

Interna	Externa
Direcciones	Direcciones

Tema 6 – PAT

- Port Address Translation

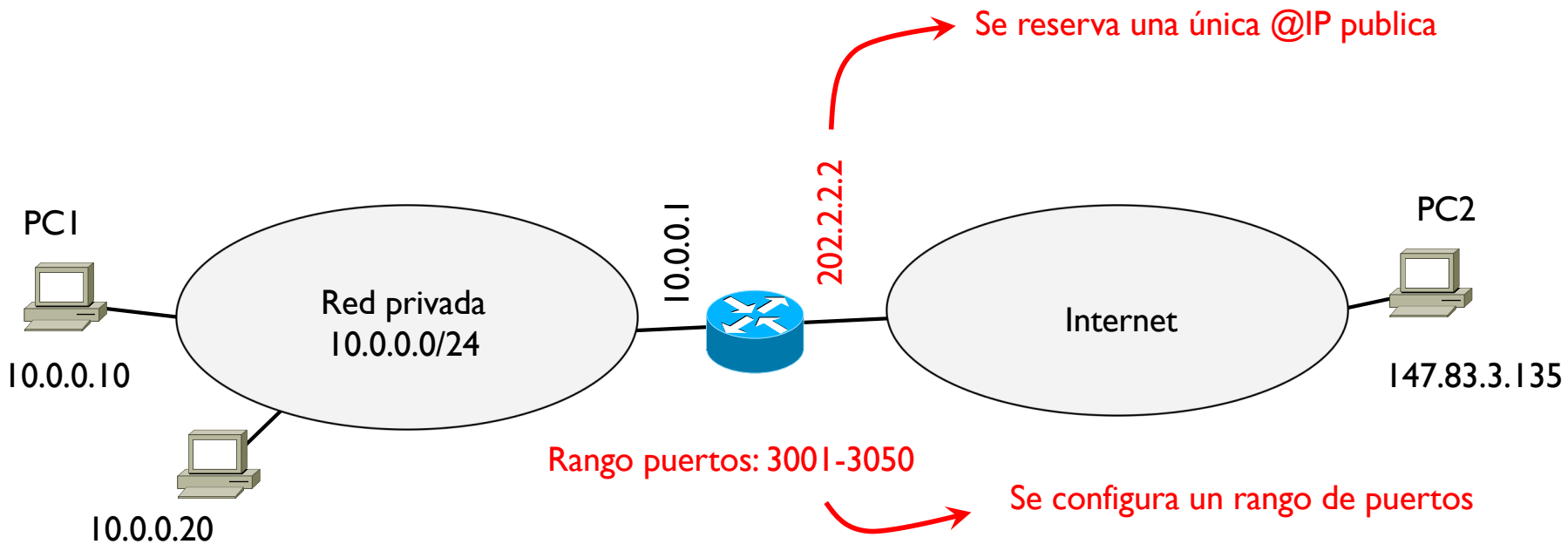
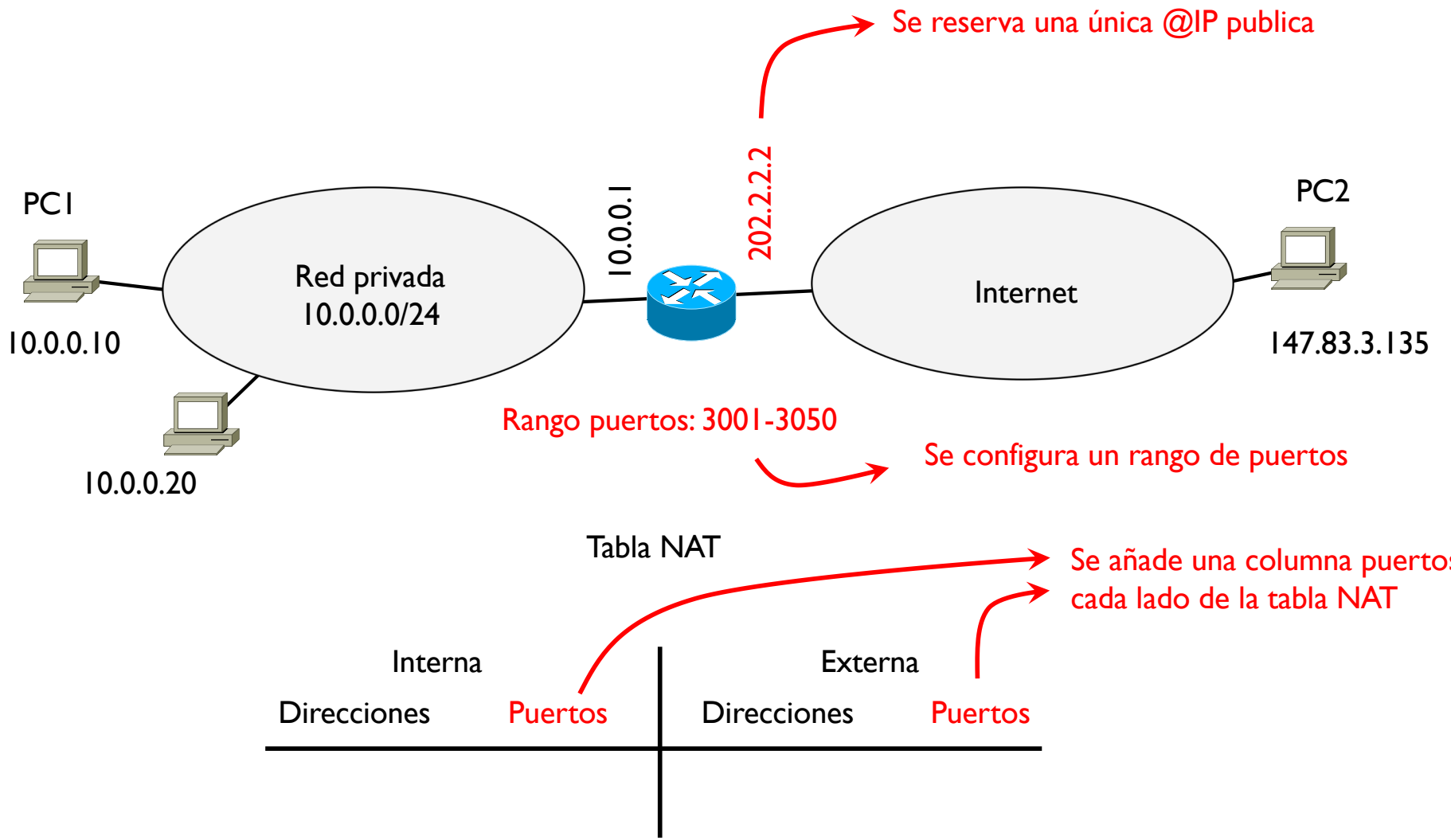


Tabla NAT

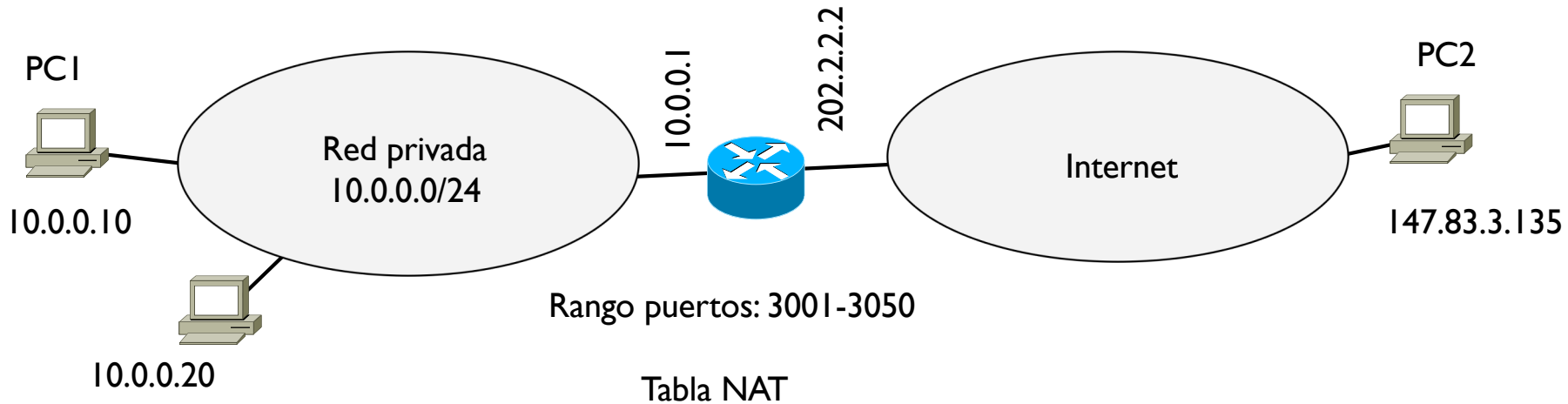
Interna	Externa
Direcciones	Direcciones

Tema 6 – PAT

- Port Address Translation



Tema 6 – PAT



Rango puertos: 3001-3050

Tabla NAT

Interna		Externa	
Direcciones	Puertos	Direcciones	Puertos

La tabla NAT está inicialmente vacía

TCP	IP
1046 → 80	10.0.0.10 → 147.83.3.135

El host interno PC1 quiere transmitir a PC2 de Internet
En este caso interesan las @IP y también los puertos

Tema 6 – PAT

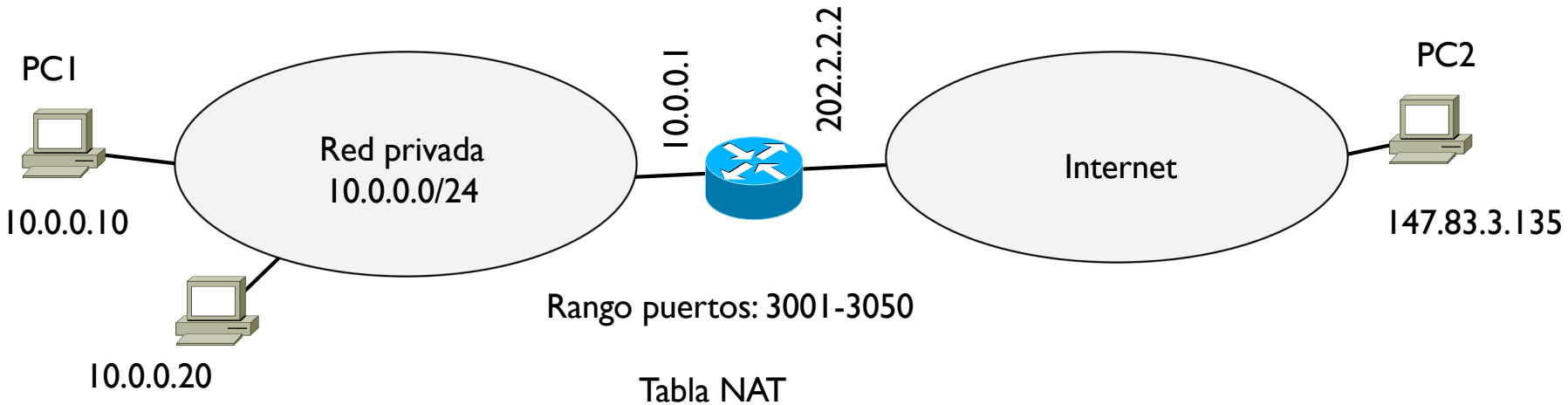


Tabla NAT

Interna		Externa	
Direcciones	Puertos	Direcciones	Puertos
10.0.0.10	1046	202.2.2.2	3001

1046 → 80	10.0.0.10 → 147.83.3.135	**3001** → 80	**202.2.2.2** → 147.83.3.135

El router cambia la @IP privada origen por su propia @IP publica y cambia el puerto origen por el primer puerto disponible del rango

Tema 6 – PAT

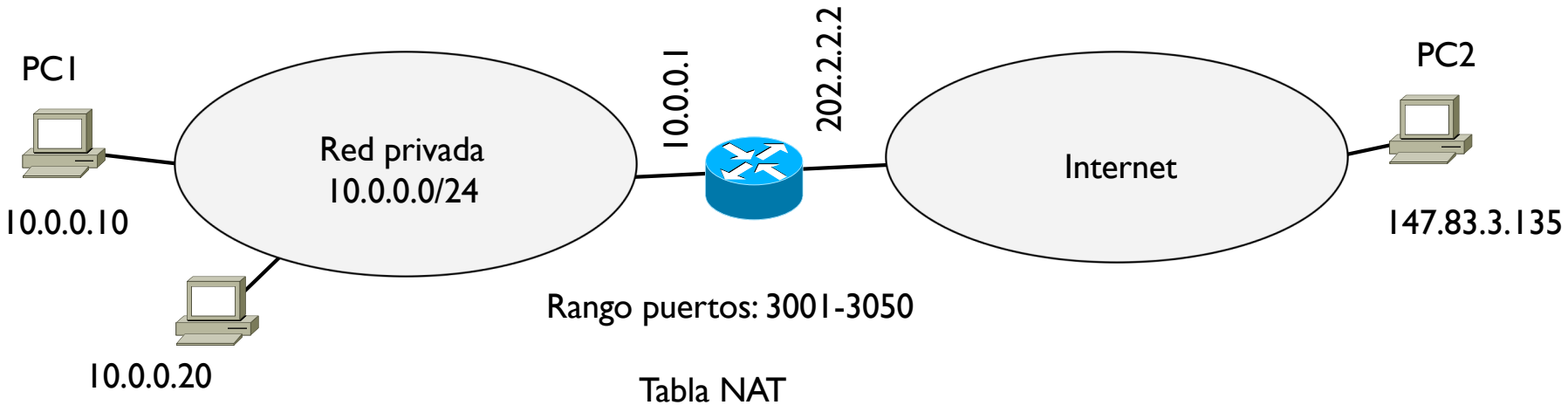
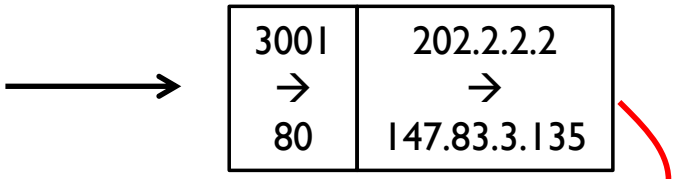


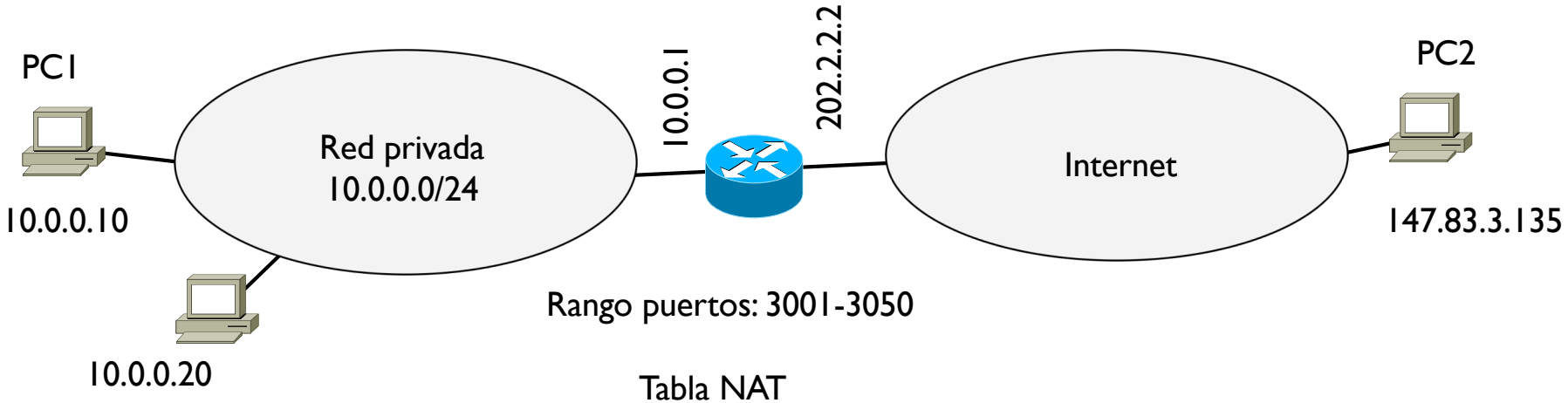
Tabla NAT

Interna		Externa	
Direcciones	Puertos	Direcciones	Puertos
10.0.0.10	1046	202.2.2.2	3001



PC2 recibe el datarama con la @IP del router y el puerto origen del rango

Tema 6 – PAT



Rango puertos: 3001-3050

Tabla NAT

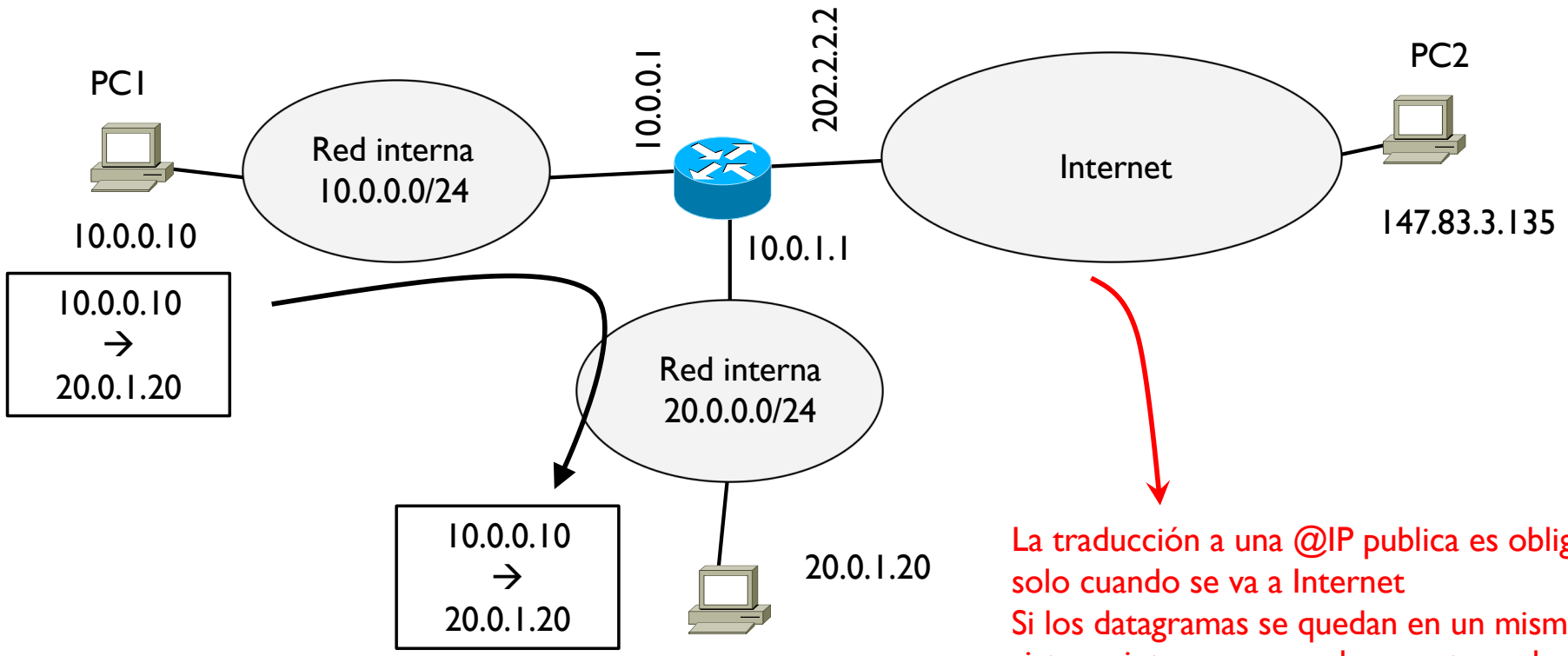
Interna		Externa	
Direcciones	Puertos	Direcciones	Puertos
10.0.0.10	1046	202.2.2.2	3001
10.0.0.20	3678	202.2.2.2	3002

3678 → 53	10.0.0.20 → 147.83.3.135	**3002** → 53	**202.2.2.2** → 147.83.3.135

Si otro PC transmite hacia Internet, el router vuelve a usar su @IP como origen y el siguiente puerto disponible del rango

Tema 6 – NAT detalles

- Una comunicación interna no necesita traducciones

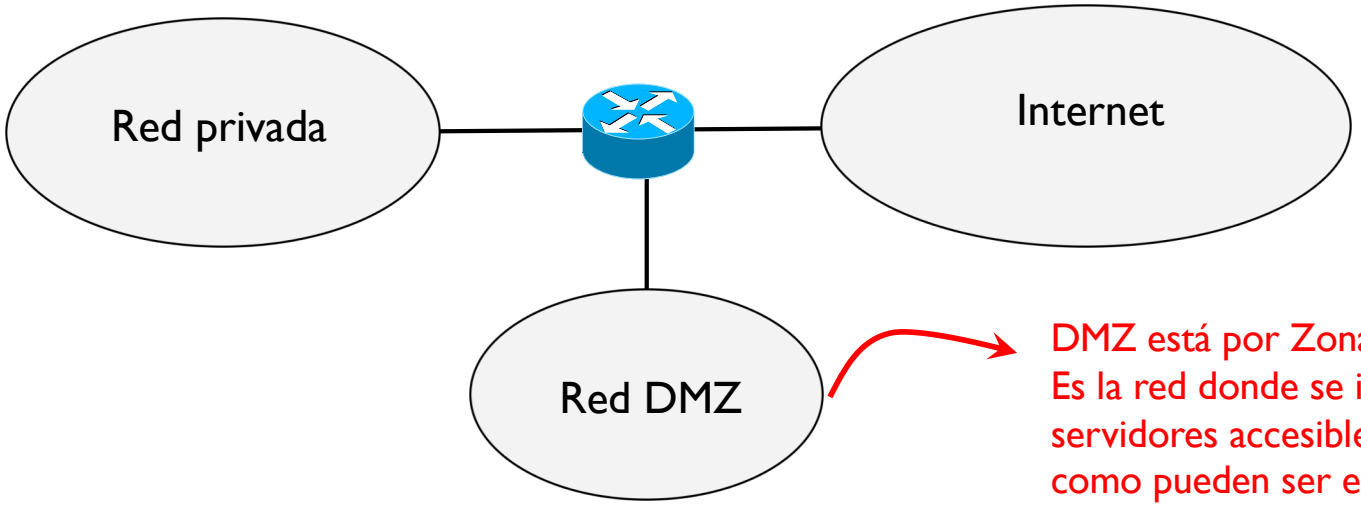


Tema 6 – Aplicaciones y seguridad

- Introducción
- Aplicaciones de red
- Seguridad en redes
  - NAT
  - **Firewall y ACLs**
- Conceptos básicos de criptografía
  - Seguridad en los protocolos

Tema 6 – Firewall y ACLs

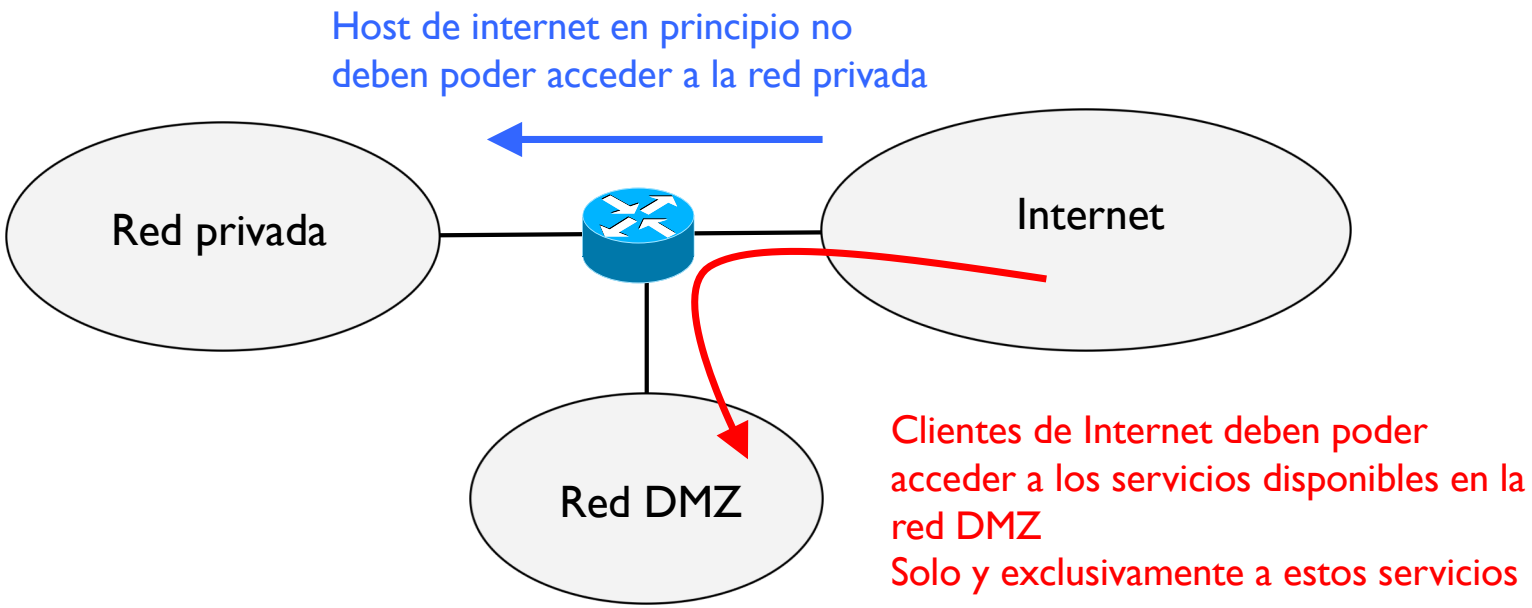
- Un firewall (o cortafuego) es un equipo de red que permite controlar la entrada y salida de la información y, si necesario, filtrar aquella no permitida
- Generalmente la configuración de una red interna tiene esta estructura



DMZ está por Zona DeMilitarizada
Es la red donde se instalan los servidores accesibles desde Internet como pueden ser el servidor web, de correo, de DNS, etc.

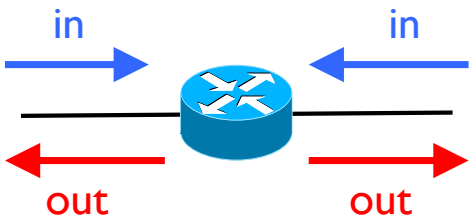
Tema 6 – Firewall y ACLs

- De manera que el acceso a las dos redes internas, la privada y la DMZ desde Internet debe estar controlada para evitar fallos de seguridad
- En concreto, el router necesita implementar funciones de Firewall para inspeccionar todos los datagramas y descartar los que no están permitidos



Tema 6 – Firewall y ACLs

- El control en el router se hace con Listas de Acceso (ACLs)
- Las ACLs se aplica a las interfaces del router y pueden ser de entrada o de salida

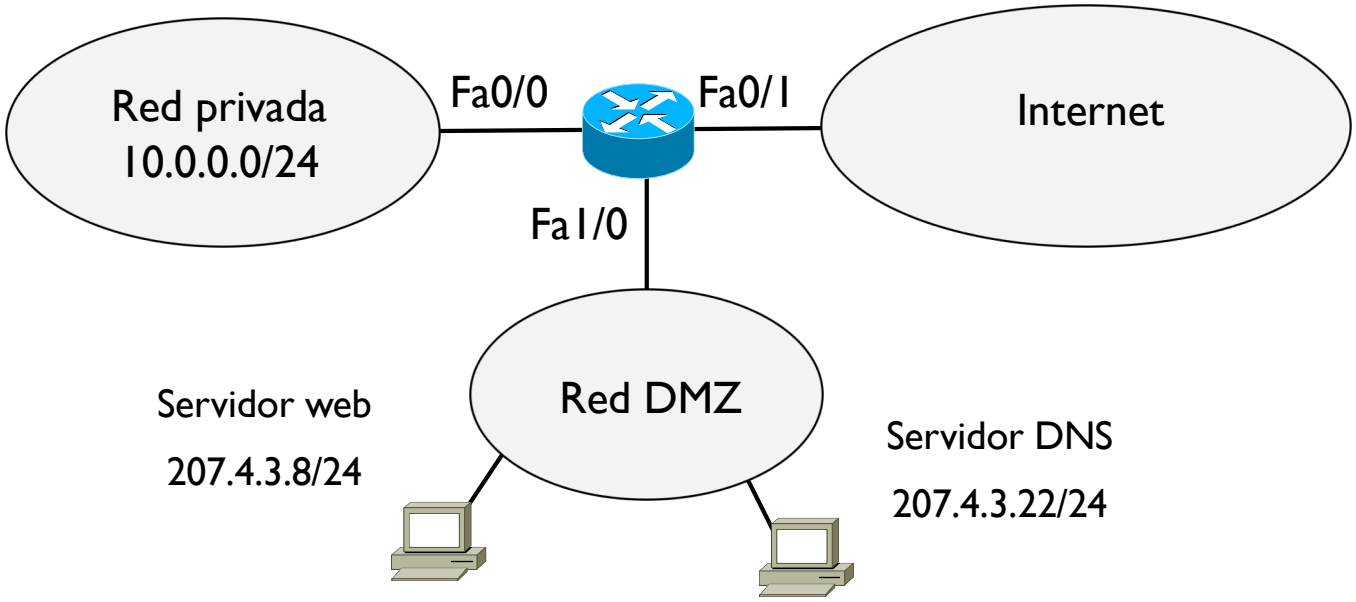


- Una ACL es una lista secuencial de condiciones de permiso o prohibición según
  - @IP origen y destino
  - Puertos origen y destino
  - Protocolo (IP, TCP, UDP, ICMP, etc.)
  - Estado (cualquiera o respuesta)

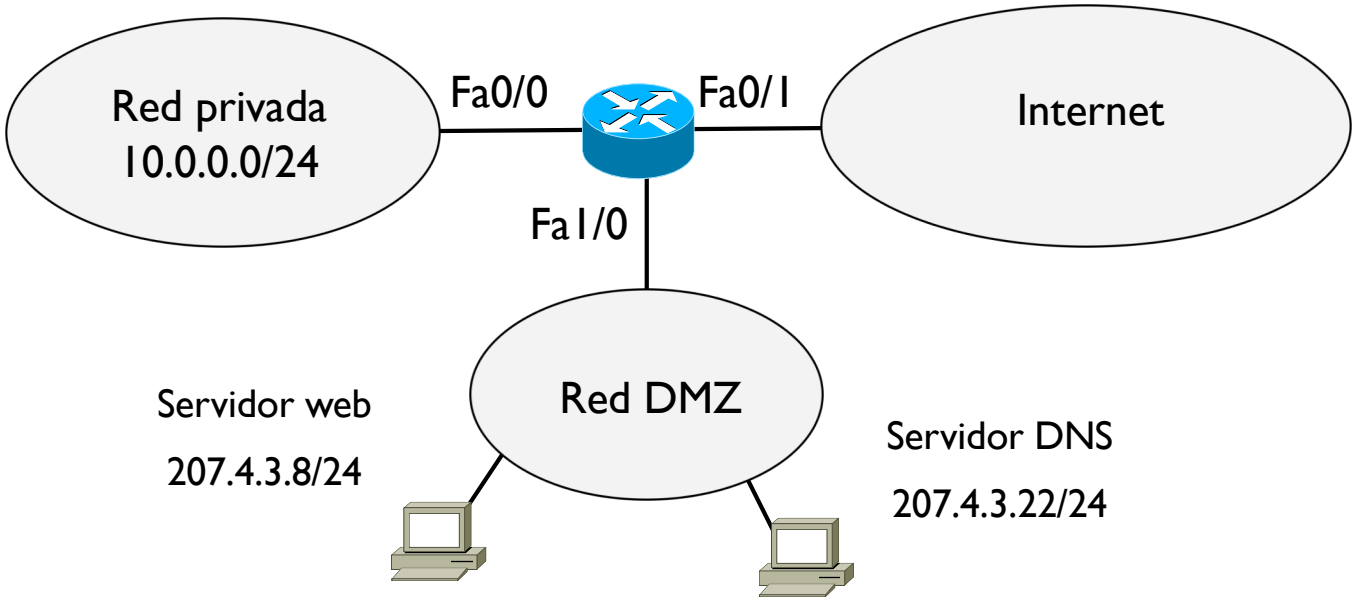
Tema 6 – Firewall y ACLs

- Para evitar complicar una ACL mezclando permisos con prohibiciones, generalmente se usa uno de estos dos enfoques
- En el primero, se crea una lista de condiciones permitidas y se concluyen con una última línea que deniega todo lo que queda
  - Permitir condición_1
  - Permitir condición_2
  - ...
  - Permitir condición_n
  - Prohibir todo
- El segundo enfoque es el contrario del primero: la lista tiene una sería de condiciones prohibidas y se concluyen con una que permite todo
  - Prohibir condición_1
  - Prohibir condición_2
  - ...
  - Prohibir condición_n
  - Permiti todo

Tema 6 – Firewall y ACLs ejemplo

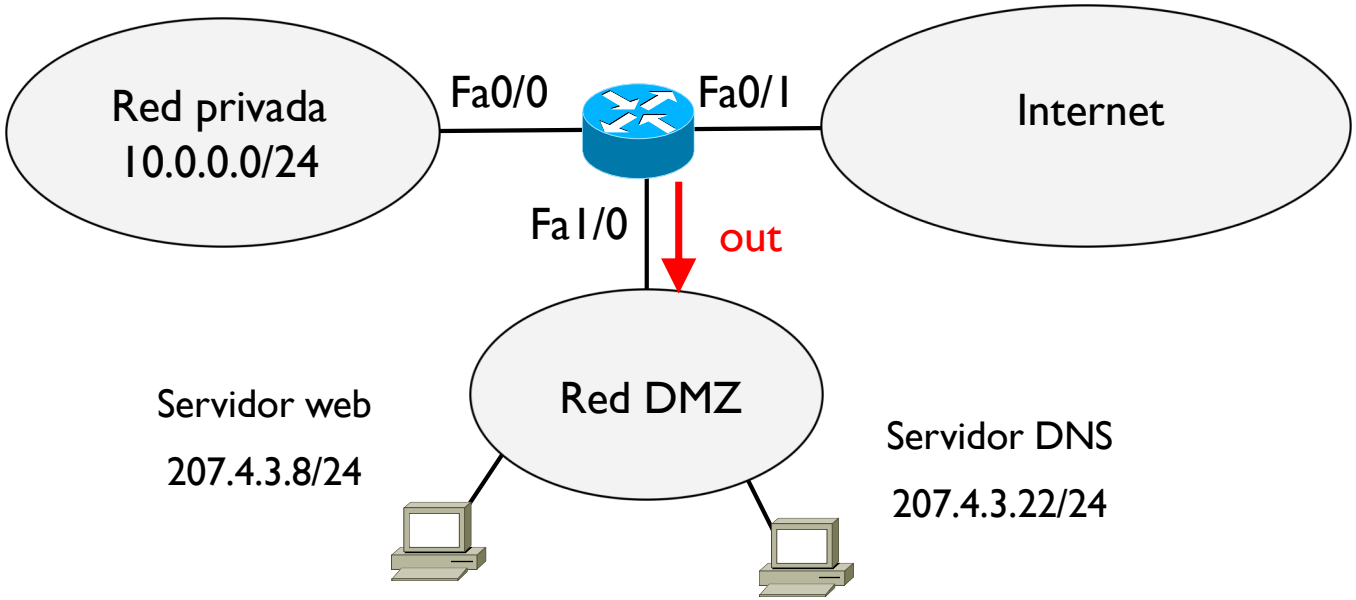


Tema 6 – Firewall y ACLs ejemplo



- Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ
- Hay que definir donde aplicar esta ACL
  - Se recomiendo aplicarla siempre lo más próximo posible a la zona que se quiere proteger
  - En este caso conviene aplicarla a la interfaz Fa1/0 de salida respecto al router (es decir hacia la red DMZ)

Tema 6 – Firewall y ACLs ejemplo

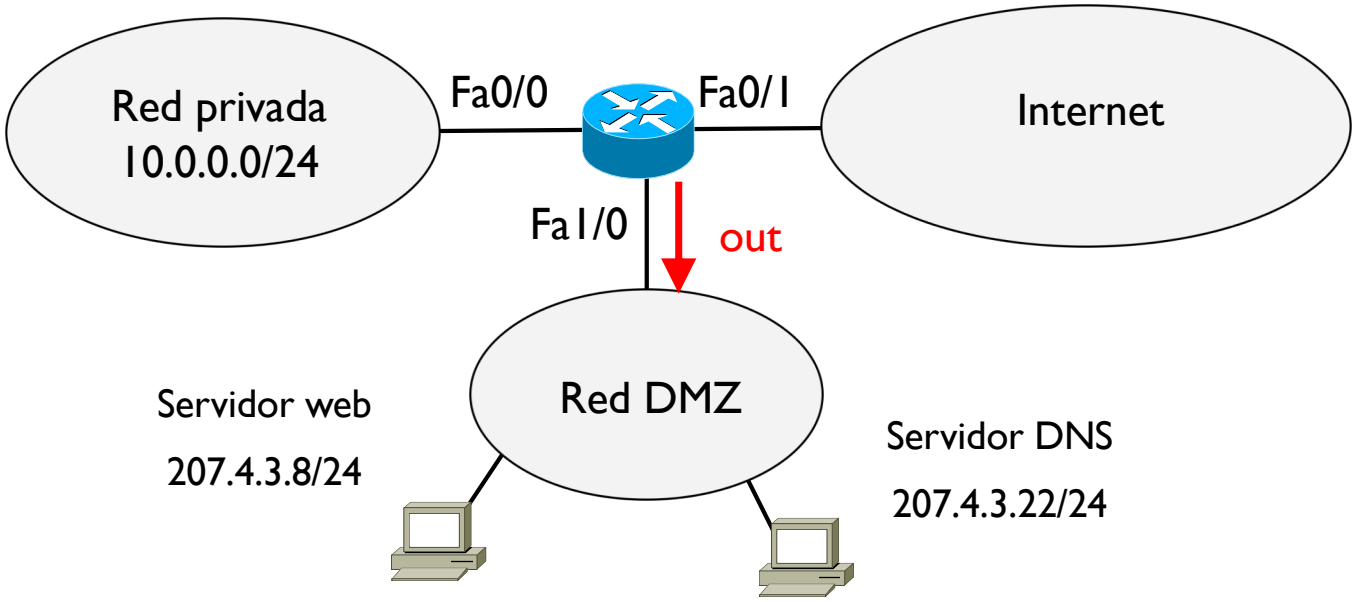


- Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

acción

Tema 6 – Firewall y ACLs ejemplo

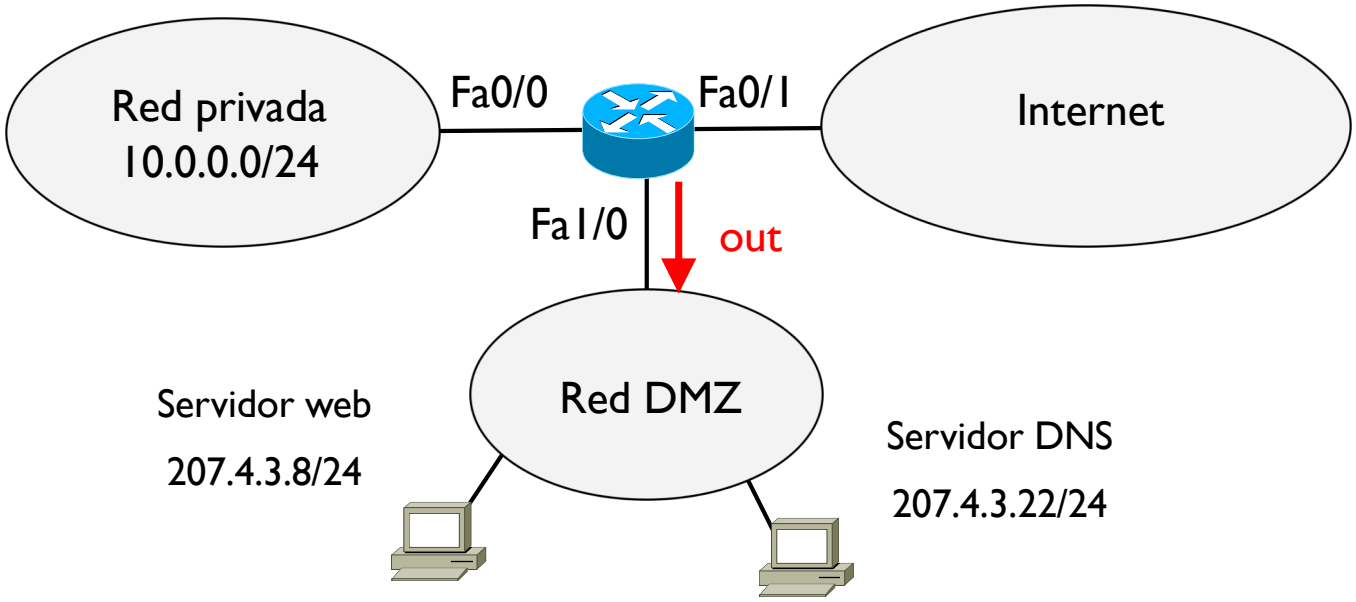


- Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

Protocolo de transporte
usado por el servidor web

Tema 6 – Firewall y ACLs ejemplo

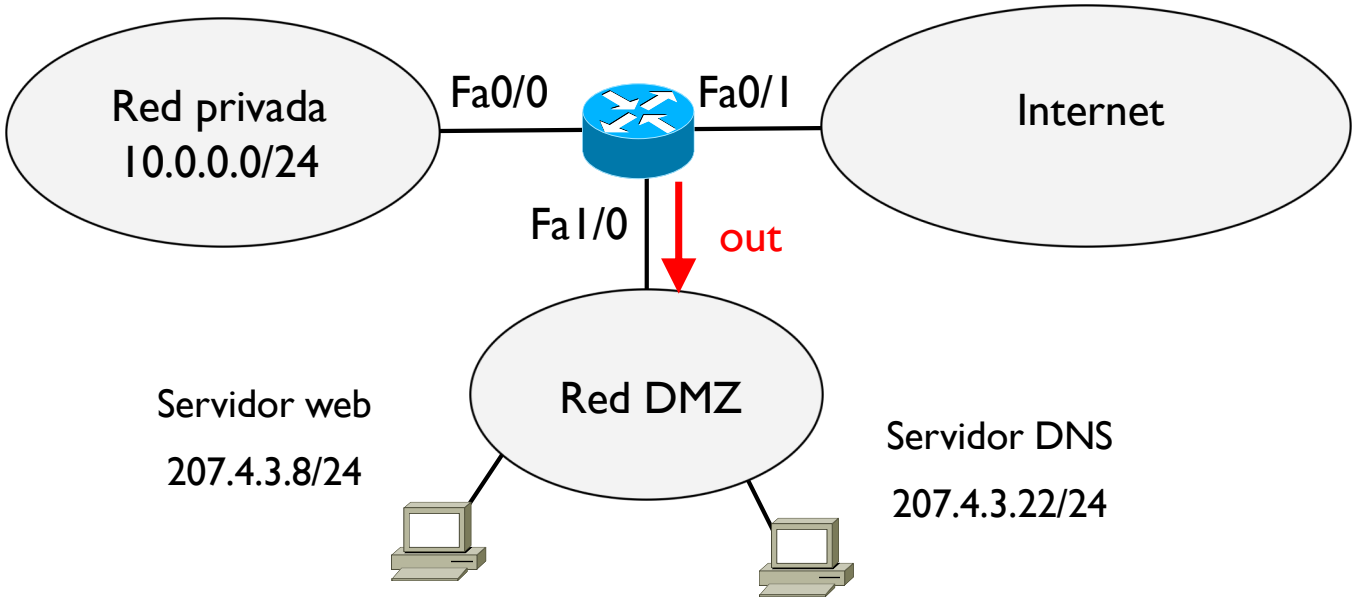


- Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

La @IP origen puede ser cualquiera

Tema 6 – Firewall y ACLs ejemplo

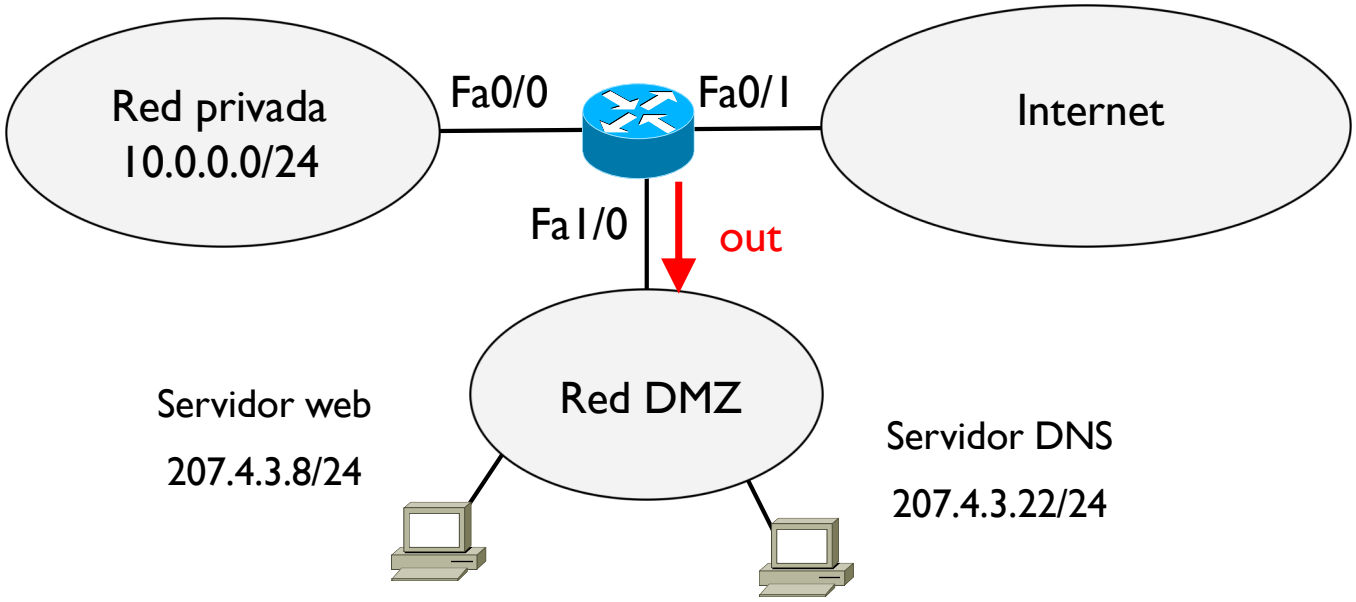


- Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

Se quiere acceder acceder al servicio web por lo tanto el puerto origen es un puerto efimero mayor igual que 1024

Tema 6 – Firewall y ACLs ejemplo

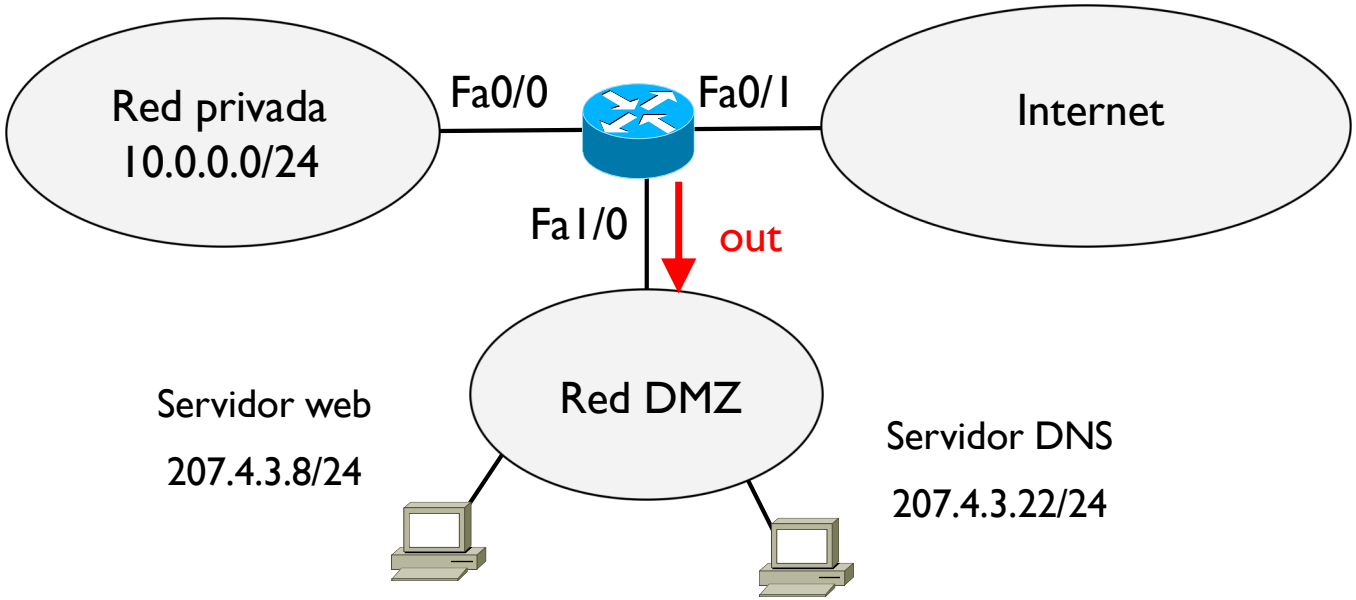


- Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

La @IP destino debe ser la del servidor web

Tema 6 – Firewall y ACLs ejemplo

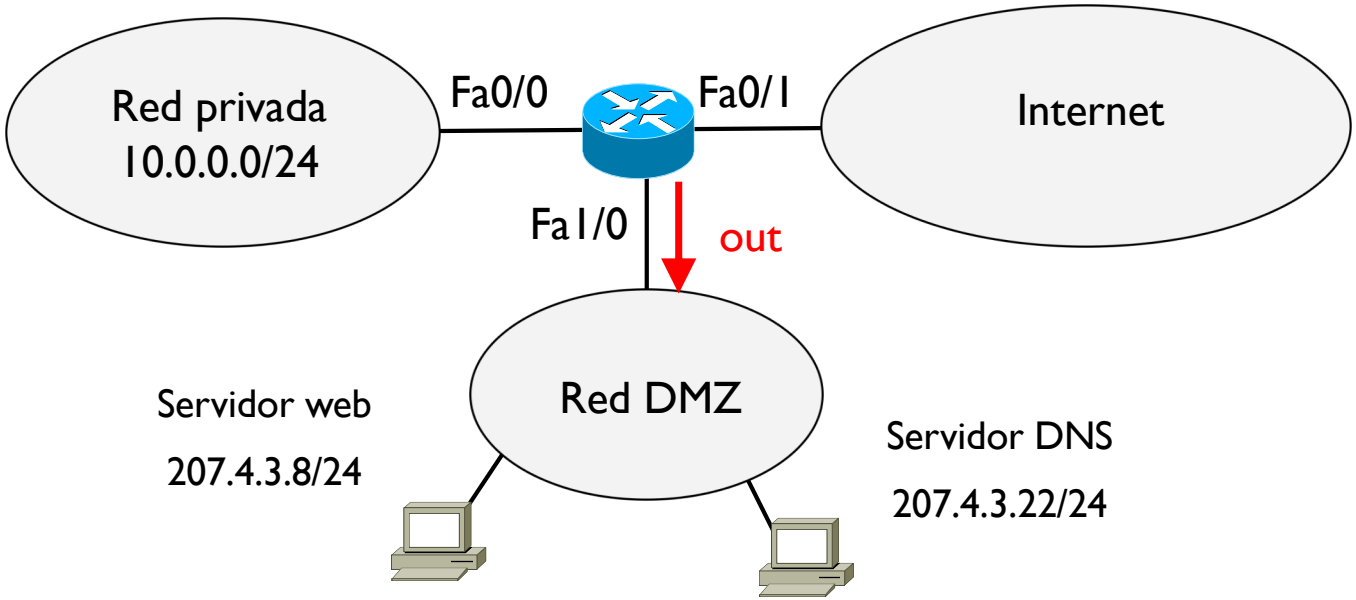


- Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

Se accede a este servidor exclusivamente para su servicio 80, es decir páginas web HTTP

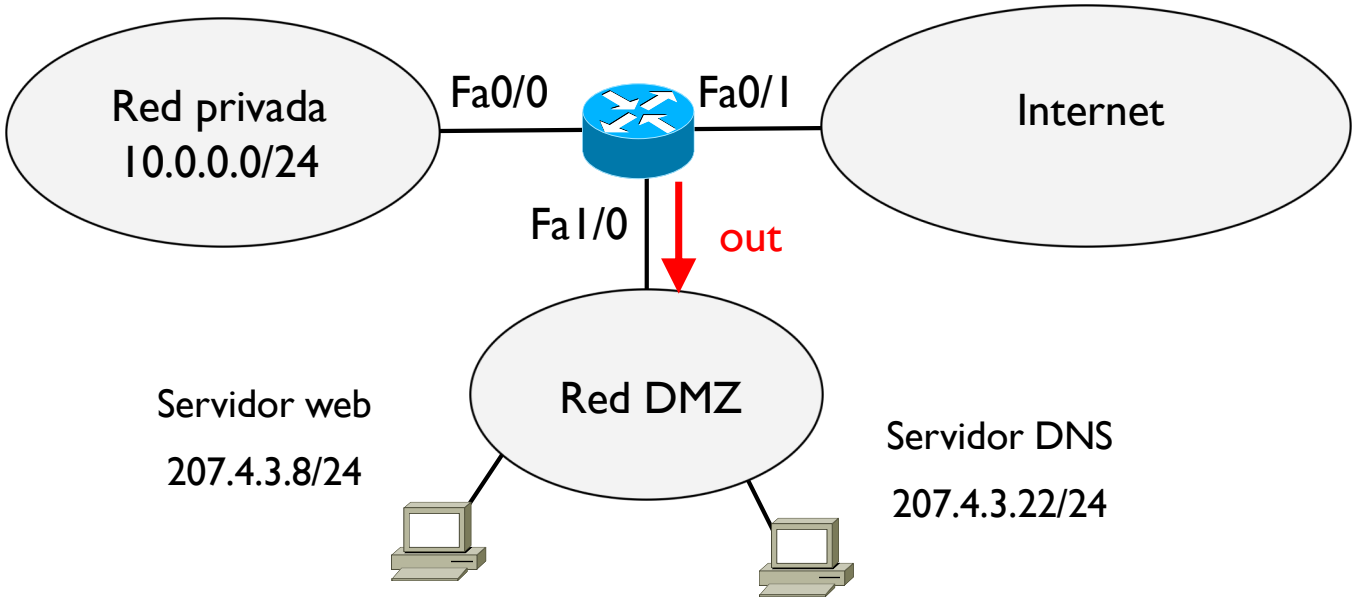
Tema 6 – Firewall y ACLs ejemplo




```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
permitir UDP 0.0.0.0/0 ≥1024 207.4.3.22/24 53
```

Lo mismo con el servicio DNS que usa UDP

Tema 6 – Firewall y ACLs ejemplo




```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
permitir UDP 0.0.0.0/0 ≥1024 207.4.3.22/24 53
prohibir IP 0.0.0.0/0 0.0.0.0/0
```

Se denega todo. Como es una lista secuencial, si una de las dos primeras condiciones se verifica, se permite y se sale de la lista.
Esta última prohibición se haría solo si no se cumpliesen las dos primeras condiciones, es decir es como si fuera una regla por defecto que se hace en última instancia

Tema 6 – Aplicaciones y seguridad

- Introducción
- Aplicaciones de red
- Seguridad en redes
  - NAT
  - Firewall y ACLs
- **Conceptos básicos de criptografía**
  - Seguridad en los protocolos

Tema 6 – Conceptos básicos de criptografía

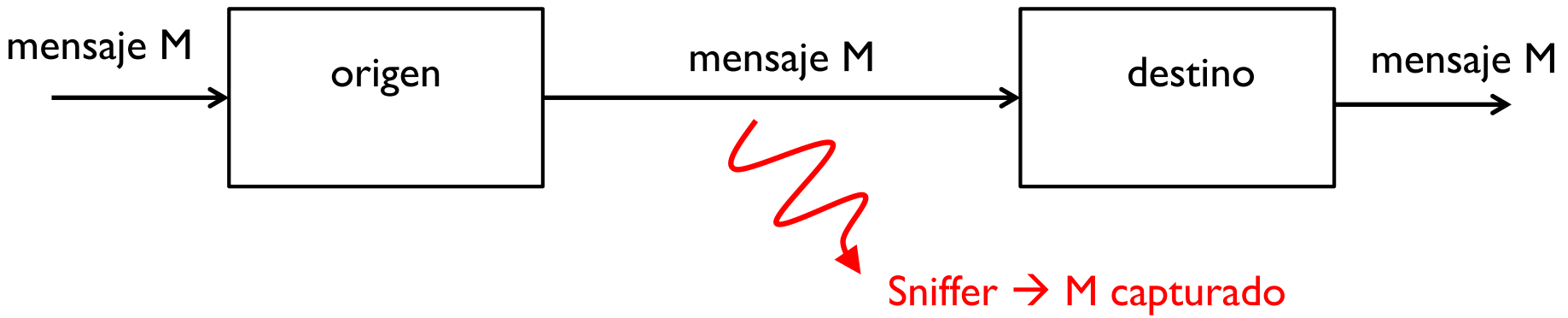
- Confidencialidad: solo origen y destino deben poder entender el mensaje
- Autentificación: origen y destino deben poder confirmar la identidad del otro
- Integridad del mensaje: origen y destino quieren poder asegurar que el mensaje se recibe sin alterar y que nadie más lo haya podido recibir
- Acceso y disponibilidad: los servicios deben ser accesibles y disponibles a los usuarios

Tema 6 – Conceptos básicos de criptografía

- ¿Que es lo que puede hacer un "bad boy"?
  - Eavesdrop: interceptar mensajes
  - Insertar mensajes en una conexión
  - Impersonation: hacerse pasar por otro alterando campos de los datos (por ejemplo @IP origen) para acceder a determinados servicios
  - Hijacking: meterse en una conexión activa quitando uno de los dos extremos y hacerse pasar por este
  - Denial of Service: inhabilitar un servicio mediante el envío de gran cantidad de solicitudes desde uno o mas ordenadores (generalmente zombis) hasta saturar los dispositivos de red

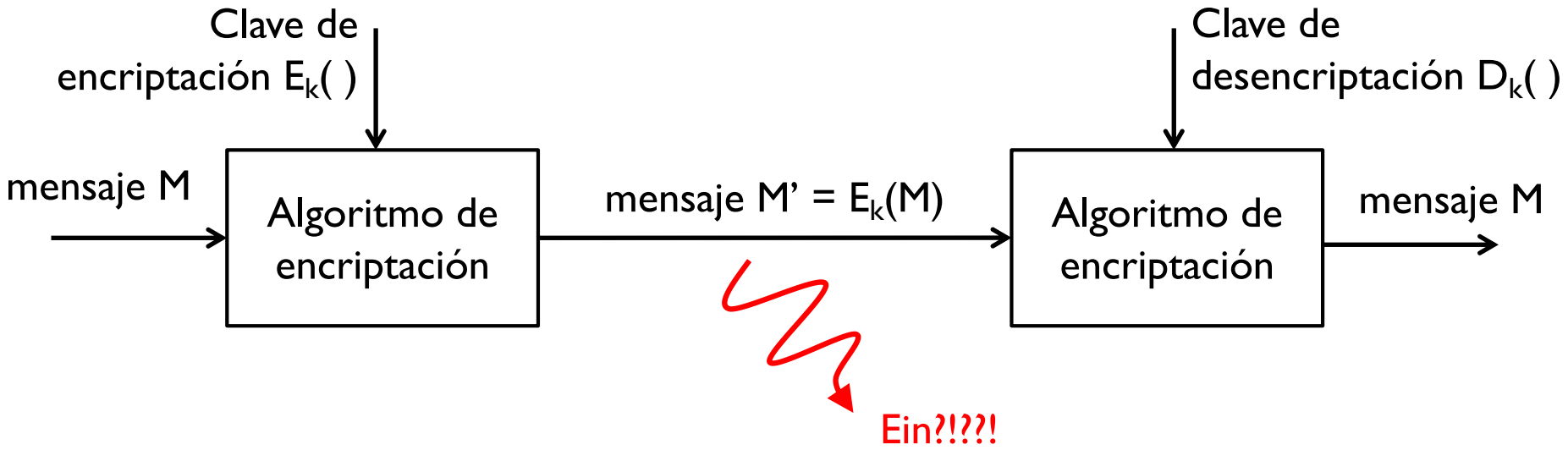
Tema 6 – Conceptos básicos de criptografía

- Criptografía
  - Del griego *krypto* (oculta) y *grapho* (escritura)
  - Literalmente escritura oculta
  - Se ocupa de las técnicas de cifrado o codificado destinadas a alterar la representación lingüística de un mensaje con el fin de hacerlo ininteligible a receptores no autorizados



Tema 6 – Conceptos básicos de criptografía

- Criptografía
  - Del griego *krypto* (oculta) y *grapho* (escritura)
  - Literalmente escritura oculta
  - Se ocupa de las técnicas de cifrado o codificado destinadas a alterar la representación lingüística de un mensaje con el fin de hacerlo ininteligible a receptores no autorizados



Tema 6. Criptosistemas históricos

- Los cifrados más clásicos son el de transposición y el de substitución
- Cifrado por **transposición**: reordenar las letras en un mensaje
- Ejemplo:
  - Transposición con un periodo fijo k = 3
  - M = CRYPTOGRAPHY se convierte en $E_k(M)$ = YCROPTAGRYPH
  - $D_k(E_k(M))$ = CRYPTOGRAPHY

Tema 6. Criptosistemas históricos

- Los cifrados más clásicos son el de transposición y el de substitución
- Cifrado por **substitución**: substituir letras o grupos de letras con otras letras o grupos de letras en un mensaje
- Ejemplo:
  - Substitución de una letra con otra k = 3 posiciones más adelante en el alfabeto
  - M = CRYPTOGRAPHY se convierte en $E_k(M)$ = GUBSXRJUDSKB
  - $D_k(E_k(M))$ = CRYPTOGRAPHY

Tema 6. Criptosistemas

- Generalmente
  - El algoritmo de encriptación y desencriptación es conocido
  - Lo que es secreto es la clave
  - En los ejemplos anteriores, k es el factor desconocido en el cifrado

Tema 6. Shannon best practices

- Idea de "confusión y difusión"
- Confusión
  - Hacer que la relación entre clave e mensaje cifrado sea la más compleja posible
  - Es decir, hacer realmente difícil encontrar la clave aunque se tuviera a disposición un gran número de mensajes no cifrados y mensajes cifrados con una misma clave
- Difusión
  - Hacer de manera que el bloque cifrado dependa del bloque no cifrado de una manera muy compleja
  - Es decir, si se cambiara aunque solo un bit del bloque no cifrado, el bloque cifrado debería cambiar completamente
- Shannon definió este concepto como una condición necesaria para un cifrado seguro y práctico

Tema 6. Tipos

- Criptografía privada
  - También conocida como criptografía simétrica
  - Origen y destino usan la misma clave secreta
- Criptografía publica
  - También conocida como criptografía asimétrica
  - Se usan dos claves, una pública y una privada

Tema 6 – Criptografía privada

- También conocida como criptografía simétrica
- Origen y destino usan la misma clave secreta
- Única técnica de cifrado públicamente conocida hasta junio de 1976
- Actualmente se usan métodos basados en cifrado en bloques y cifrado por flujo
- Se necesita el intercambio de la clave entre los dos extremos a través de un sistema seguro
  - Hoy en día existen métodos de intercambio de claves de forma segura sobre un medio no seguro (por ejemplo el Diffie-Hellman)

Tema 6 – Criptografía privada

- Cifrado en bloques
  - Se define un grupo de bits, llamado bloque, que tiene una transformación invariante
  - Por ejemplo el bloque de bits 1100 se transforma siempre en el 0111
- Estándares más conocidos
  - One Time Pad (OTP)
  - Data Encryption Standard (DES)
  - 3DES
  - Advanced Encryption Standard (AES)

Tema 6 – OTP

- Cada bloque de bits del mensaje es encriptado usando una clave secreta aleatoria de la misma longitud que el bloque

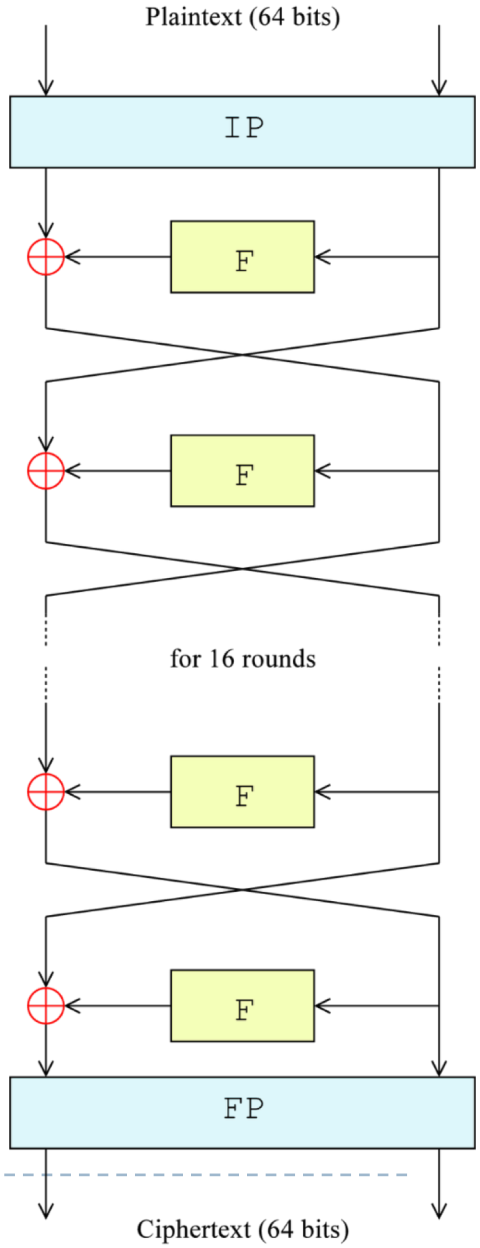
```
SENDING
-------
message: 0 0 1 0 1 1 0 1 0 1 1 1 ...
pad:     1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR      --------------------------
cipher:  1 0 1 1 0 0 0 1 1 1 0 0 ...

RECEIVING
---------
cipher:  1 0 1 1 0 0 0 1 1 1 0 0 ...
pad:     1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR      --------------------------
message: 0 0 1 0 1 1 0 1 0 1 1 1 ...
```

- Si la clave es realmente aleatoria, del mismo tamaño que un bloque del mensaje y se usa una única vez, el mensaje cifrado es imposible de desencriptar sin conocer la clave
- Usado durante la guerra fría para la comunicación entre EEUU y URSS (famoso teléfono rojo en las pelis)

Tema 6 – DES

- Elaborado por IBM y estandarizado en el 1976
- Usa bloques de 64 bites que se transforman en bloques cifrados de 64 bits
- Se usa una clave de 56 bits
- El algoritmo es conocido (en la figura)
  - Consiste de una permutación inicial (IP) y una permutación final (FP) que son una el inverso del otra
  - Y de 16 rondas F iguales
  - Antes de empezar las rondas, el bloque se divide en dos mitades de 32 bits que se procesan alternativamente en las rondas F
  - En cada ronda F, una mitad de 32 bits se mezcla con parte de la clave y el resultado se combina con la otra mitad de 32 bits



Tema 6 – DES

- Basado en la idea de "confusión y difusión"
- Confusión
  - Hacer que la relación entre clave e mensaje cifrado sea la más compleja posible
  - Es decir, hacer realmente difícil encontrar la clave aunque se tuviera a disposición un gran número de mensajes no cifrados y mensajes cifrados con una misma clave
- Difusión
  - Hacer de manera que el bloque cifrado dependa del bloque no cifrado de una manera muy compleja
  - Es decir, si se cambiara aunque solo un bit del bloque no cifrado, el bloque cifrado debería cambiar completamente
- Shannon definió este concepto como una condición necesaria para un cifrado seguro y práctico

Tema 6 – DES

- Fue la técnica de encriptación aceptada por la NSA de EEUU
- Su esquema base así como sus mejoras fueron usadas hasta el 26 de mayo de 2002 cuando fue reemplazado por el AES

- El ataque más practico para romper el cifrado DES es la fuerza bruta, es decir usar una por una todas las combinaciones posibles de claves que son 2^{56}
- De hecho, se especula que la NSA impuso una clave de solo 56 bits porque en aquellos tiempos sola la NSA tenía la capacidad computacional necesaria para romper el cifrado DES
- Hoy en día se puede descifrar un DES en pocos minutos (en 1998 se demostró que era rompible en 2 días)

Tema 6 – 3DES

- Después de descubrir que el DES es "fácilmente" rompible, se pasó a usar el 3DES
- El 3DES aplica el DES tres veces con tres claves distintas, haciendo así incrementar la clave hasta los 168 bits (3 x 56 bits)
- De momento no hay vulnerabilidad conocida pero es extremadamente lento
- AES puede llegar a ser 6 veces más rápido que el 3DES

Tema 6 – AES

- Reemplazo del DES como estándar de la NSA de EEUU desde 2002
- También conocido como cifrado Rijndael por sus dos autores Joan Daemen y Vincent Rijman que lo estandarizaron el 26 de noviembre de 2001
- Basado en una red de substitución y permutación
- Relativamente fácil de implementar y usa poca memoria
- Hoy en día se usa a gran escala (por ejemplo en WPA2 en 802.11)
- Se usan bloques de 128 bits y tamaños de claves de 128, 192 o 256 bits

Tema 6 – AES

- El algoritmo es conocido
  - Se organizan los 128 bits en una matriz de 4x4 bytes (16 bytes x 8 = 128 bits)
  - Se hace un primera operación de combinación de cada byte con la clave modificada según una determinada operación
  - Se hacen luego 10 (clave de 128 bits), 12 (192 bits) o 14 (256 bits) rondas, cada una con estos pasos
    1. En cada ronda se hace una substitución de cada byte por otro según una tabla conocida
    2. Las últimas tres líneas de bytes de la matriz se desplazan un cierto número de posiciones
    3. Se combinan los 4 bytes de cada columna usando una transformación lineal conocida
    4. Se combina cada bytes de la matriz con la clave modificada según la ronda
  - Se hace una última etapa donde se aplican una última vez los pasos 1, 2 y 4

Tema 6 – Criptografía privada

- Cifrado por flujo
  - Para algunas aplicaciones, el cifrado en bloques es inapropiada porque los flujos de datos se producen en tiempo real en pequeños fragmentos (por ejemplo telefonía).
  - Técnicas de cifrado que realizan el cifrado incrementalmente, convirtiendo el mensaje en claro en mensaje cifrado bit a bit.
- Estándares más conocidos
  - RC4 (usado en WEP de 802.11)
  - A5/1 (usado en GSM)

Tema 6. Problemas

- Distribución de la clave
  - Los usuarios deben intercambiarse la clave antes de empezar la comunicación
- Gestión de la clave
  - Si hay n usuarios, cada pareja debe intercambiarse una clave, con lo que se van a necesitar n(n-1)/2 claves
- Firma digital
  - No es posible tener una firma propia digital ya que cada clave es compartida entre, por lo menos, dos usuarios

Tema 6 – Criptografía publica

- También conocida como criptografía asimétrica
- Cada extremo posee dos claves, una publica y una privada
  - Las claves publicas deben estar disponibles para todos
  - Las dos claves se generan a través de un algoritmo de generación de claves
- Si un origen quiere transmitir un mensaje encriptado a un destino
  - el origen debe usar la clave publica del destino para cifrar el mensaje
  - nadie podrá descifrar el mensaje salvo el destino con su clave privada
- De esta forma no se necesita el intercambio de claves para encriptar y desencriptar los mensajes

Tema 6 – Criptografía publica

- Funcionamiento en el origen
  - El origen A quiere transmitir un mensaje M al destino B
  - A encuentra la clave pública PK_b de B en un directorio publico
  - A computa M' = E_{PKb}(M) donde E es un algoritmo de encriptación publico
  - A envía el mensaje M' a B
- Funcionamiento en el destino
  - El destino B recupera su clave privada SK_b
  - B computa D_{SKb}(M') = M donde D es un algoritmo de desencriptación publico
  - B lee el mensaje M

Tema 6. Firma Digital

- Para firmar de forma digital un documento
  - Si U quiere firmar un mensaje M, simplemente aplica el algoritmo E con su clave privada de forma que el mensaje firmado es $S = E_{SKu}(M)$
  - Para verificar que el que ha firmado es realmente U, cualquier usuario puede aplicar el algoritmo de decifrar usando la clave publica de U sobre el mensaje cifrado y comparar el resultado con el mensaje no cifrado, es decir verificar que $D_{PKu}(S) = M$

VISTO BUENO DEL INFORME ANUAL DE EVALUACIÓN

I. INFORME DEL DIRECTOR/A

Valoración de la consecución de los objetivos por parte del beneficiario/a durante la anualidad a la que se refiere este informe:

(●) Favorable: se aconseja la continuidad de la ayuda

( ) NO favorable: NO se aconseja la continuidad de la ayuda

Motivación del informe NO favorable:

Grado aproximado de consecución de los objetivos marcados para la anualidad objeto de este informe:

	Excelente	Notable	Aceptable	Insuficiente
Metodología	●	○	○	○
Tareas y resultados	●	○	○	○
Programa formativo	●	○	○	○

Motivación de la calificación:

La valoración del desarrollo de la tesis doctoral hasta este punto es muy positiva. Cabe destacar las numerosas colaboraciones lideradas por el beneficiario con instituciones tanto nacionales (p.e., Telefónica I+D, Fundación i2CAT, ATOS Origin) como internacionales (p.e., Predictive Network Solutions, Brno University of Technology), las cuáles han permitido la preparación de un número substancial de artículos de investigación para su publicación en revistas de prestigio y para su presentación en conferencias. Un ejemplo de estos es el artículo aceptado en la revista indexada en los JCR European Transactions on Telecommunications, o las ponencias en IEEE GLOBECOM o en el Workshop NetCloud 2016.

Firma electrónica del director/a:

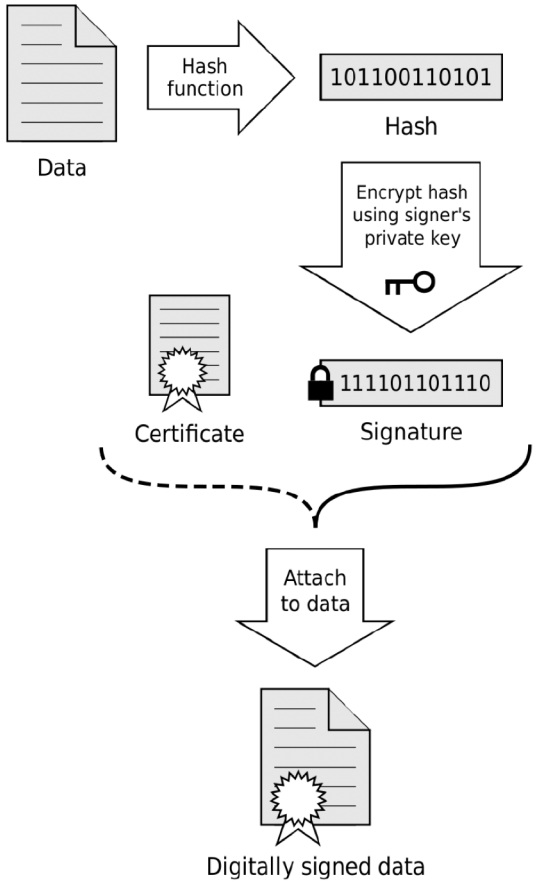
Una vez firmado, debe enviar este documento a la COMISIÓN ACADÉMICA para que cumplimente y firme electrónicamente la página 8.
Es importante que al firmar NO bloquee el documento.

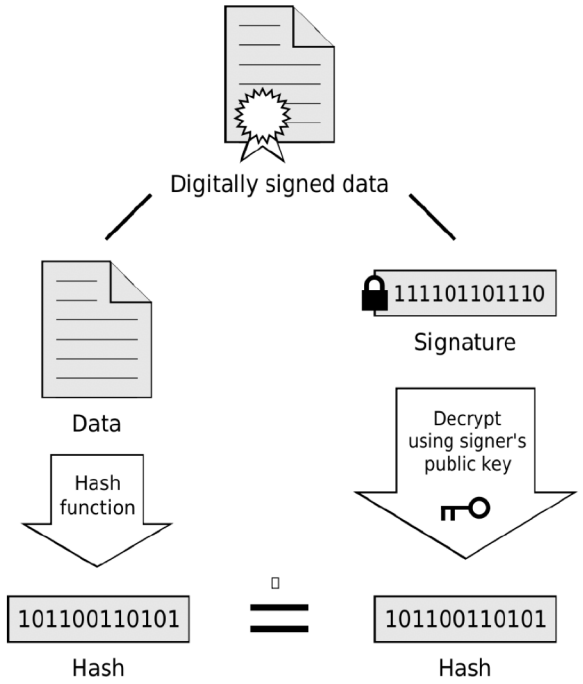
CAREGLIO DAVIDE - X3055490D

Digitally signed by CAREGLIO DAVIDE - X3055490D
Date: 2017.11.07 15:00:14 +01'00'

Tema 6. Firma Digital

- Ya que cifrar todo el documento puede resultar computacionalmente costoso, lo que se hace es
  - Calcular una función de Hash (de un tamaño fijo) sobre el documento
  - Firmar el resultado de esta función
  - Para autentificar la firma, se hace la operación inversa





Tema 6 – Criptografía híbrida

- Se emplean ambos cifrados
  - Se usa un cifrado asimétrico para enviar la clave del cifrado simétrico al destino usando la clave pública del destino
  - Se usa el cifrado simétrico para encriptar el mensaje
- Ejemplos
  - PGP y GnuPG usan un sistema de cifrado híbrido
  - La clave de la comunicación (clave simétrica) es cifrada con la clave pública del destino y el mensaje es cifrado con la clave simétrica. Se junta todo en un mismo paquete y se envía
  - El destino usa su clave privada para descifrar la clave simétrica y luego descifra el mensaje con esta
  - De esta forma la clave puede cambiar por cada comunicación

Tema 6 – Aplicaciones y seguridad

- Introducción
- Aplicaciones de red
- Seguridad en redes
  - NAT
  - Firewall y ACLs
- Conceptos básico de criptografía
  - **Seguridad en los protocolos**

Tema 6 – Seguridad en los protocolos

- Autentificación e integridad: mediante firma digital
- Privacidad y seguridad de los datos: mediante cifrado
- Protocolos mas conocidos
  - PGP (Pretty Good Privacy)
  - S/MIME (Secure / Multipurpose Internet Mail Extensions)
  - SSL (Secure Sockets Layer)
  - TSL (Transport Layer Security)
  - PCT (Private Communications Technology)
  - S-HTTP (Secure HTTP)
  - IPSEC (IP Secure)

Tema 6 – Seguridad en los protocolos

- PGP (Pretty Good Privacy)
  - Usado en los correos electrónico
  - Cifrado híbrido
- SSL (Secure Sockets Layer)
  - Una capa de seguridad entre la capa de transporte y la capa de aplicación de red
  - Usado en los navegadores, correo electronico, chats, voice over IP, etc.
  - Cifrado híbrido
  - En la versión 3.0 (1996) descubierta vulnerabilidad (2014)
  - Muchas malas implementaciones (IE6, Konquerer, etc.) lo hicieron vulnerable

Tema 6 – Seguridad en los protocolos

- TLS (Transport Layer Security)
  - Substituye SSL pero es incompatible con SSL
  - Muchas aplicaciones negocian el protocolo de seguridad, sabiendo que si no se consiguen TTL, pasan a SSL y pueden ser atacados
  - Actualmente versión 1.2 (1.3 muy pronto)
- IPSec (IP security)
  - Protocolo seguro para el nivel 3
  - Añade autentificación entre los dos puntos y encriptación de la información mediante cifrado público
  - Modo transporte (entre dos extremos de una comunicación)
    - Solo encripta el contenido del datagrama pero no la cabecera IP
  - Modo túnel (entre dos routers, por lo tanto entre una o más redes y otra u otras redes)
    - Se encripta todo el datagrama y se pone una segunda cabecera IP no cifrada

Arquitectura i Seguretat en Xarxes Informàtiques

Tema 6 – Aplicaciones y seguridad