Diseño y desarrollo de un marco de pruebas y detección de NATs

Autor: Francisco José Blázquez Sánchez

Tutor: Francisco Valera Pintor

Ingeniería en Informática. Octubre de 2009

Índice

1. Introducción y objetivos. Introducción

- Escasez direcciones IPv4. Solución IPv6.
- NAT (The Ip Network Address Translator [RFC 1631] Mayo 1994)
  - Permite compartir una única dirección publica entre usuarios de una red privada.
  - Rompe el principio ‘end-to-end’
  - Problemas en aplicaciones extremo a extremo (P2P, juegos multiusuario, voz).
- Motivación
  - **No estandarizado.**
  - **Diferentes implementaciones.**
  - **Comportamiento no determinístico.**
  - **Problemas en las aplicaciones para detectar el tipo de NAT que tienen detrás**

1. Introducción y objetivos. Objetivos

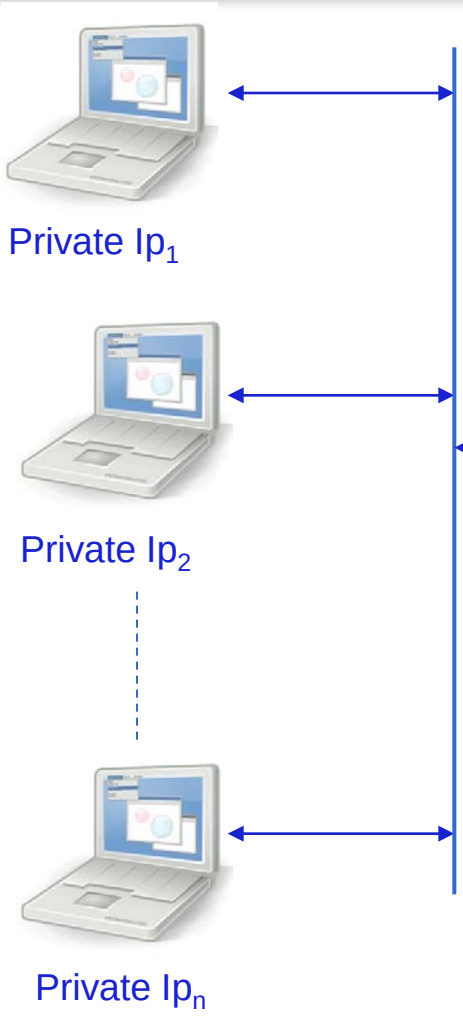
1º Definir un marco que permita caracterizar diferentes tipos de NATs y sobre el que podamos probar diferentes aplicaciones basadas en UDP

- Multithreading: Paralelismo
- Sockets RAW: Envío selectivo (IP y puerto origen)
- PCap: Recepción selectiva (Protocolo, IP y puerto origen y destino)
- Cliente STUN
- Simulador NAT
- Servidor STUN

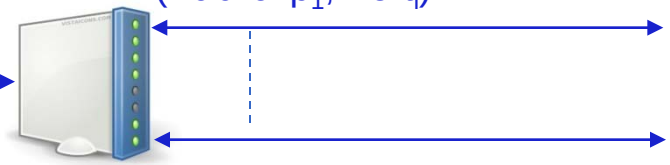
2º Validar el marco desarrollado mediante los requisitos propuestos en IETF Behave

- Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [RFC 4787] January 2007.

2. NATs. Expansión de conexiones



Problema: <u>muchos tipos de NATs</u>



Nº de clientes > Nº IPs públicas	n > m
Puertos disponibles para cada IP pública	0 < i < 65535
Nº de comunicaciones máximo	m * 65535

2. NATs. Clasificación IETF

Network Address Translation, Behavioral Requirements for Unicast UDP [RFC 4787] Enero 2007

Mapeo:

1. Mapeo independiente del extremo.
2. Mapeo dependiente de la dirección.
3. Mapeo dependiente del puerto.

Asignación IP:

4. Asignación de IP pareada.
5. Asignación de IP arbitraria.

Asignación del puerto:

6. Conservativa.
7. No conservativa.
8. Sobrecargada.
9. Conservando la paridad.
10. Asignación del puerto contiguo.

Filtro de paquetes de entrada:

11. Filtro independiente del extremo.
12. Filtro dependiente de la dirección.
13. Filtro dependiente del puerto.

Timeout (grandes diferencias):

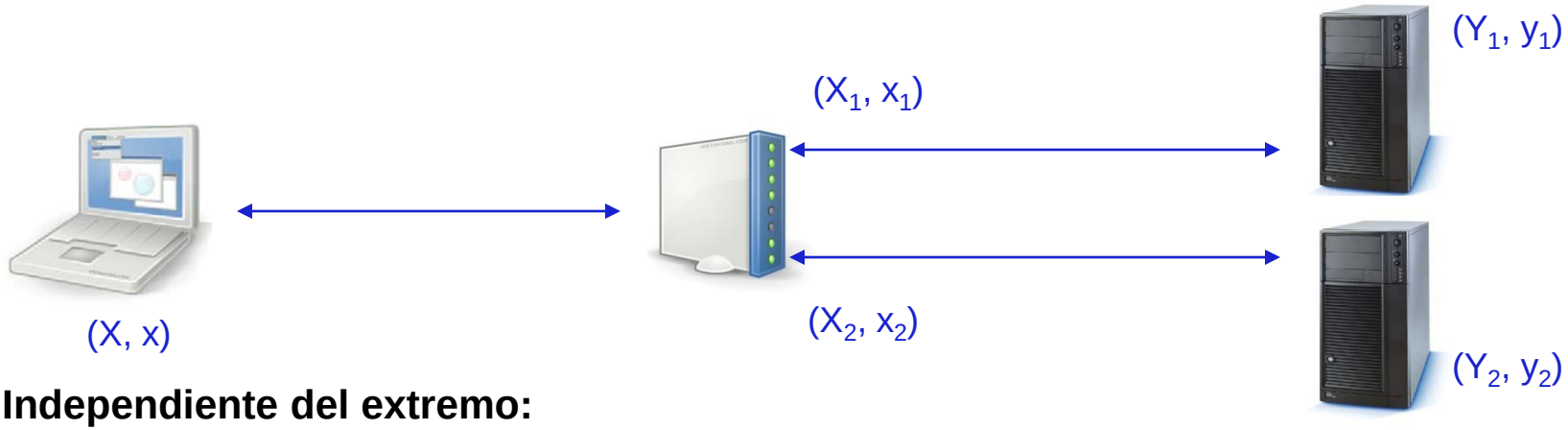
14. Refresco de salida.
15. Refresco de entrada.
16. Refresco de entrada y salida.

Otras:

17. Soporte de paquetes en horquilla.
18. ALGs empotrados.
19. Soporte ICMP.
20. Fragmentación de paquetes.

2. NATs. Ejemplo: mapeo

Network Address Translation, Behavioral Requirements for Unicast UDP [RFC 4787] Enero 2007



- **Independiente del extremo:**

  $(X_1, x_1) = (X_2, x_2)$ para todo (Y_i, y_i)

- **Dependiente de la dirección:**

  $(X_1, x_1) = (X_2, x_2)$ si y solo si $Y_1 = Y_2$

- **Dependiente de la dirección y del puerto:**

  $(X_1, x_1) = (X_2, x_2)$ si y solo si $(Y_1, y_1) = (Y_2, y_2)$

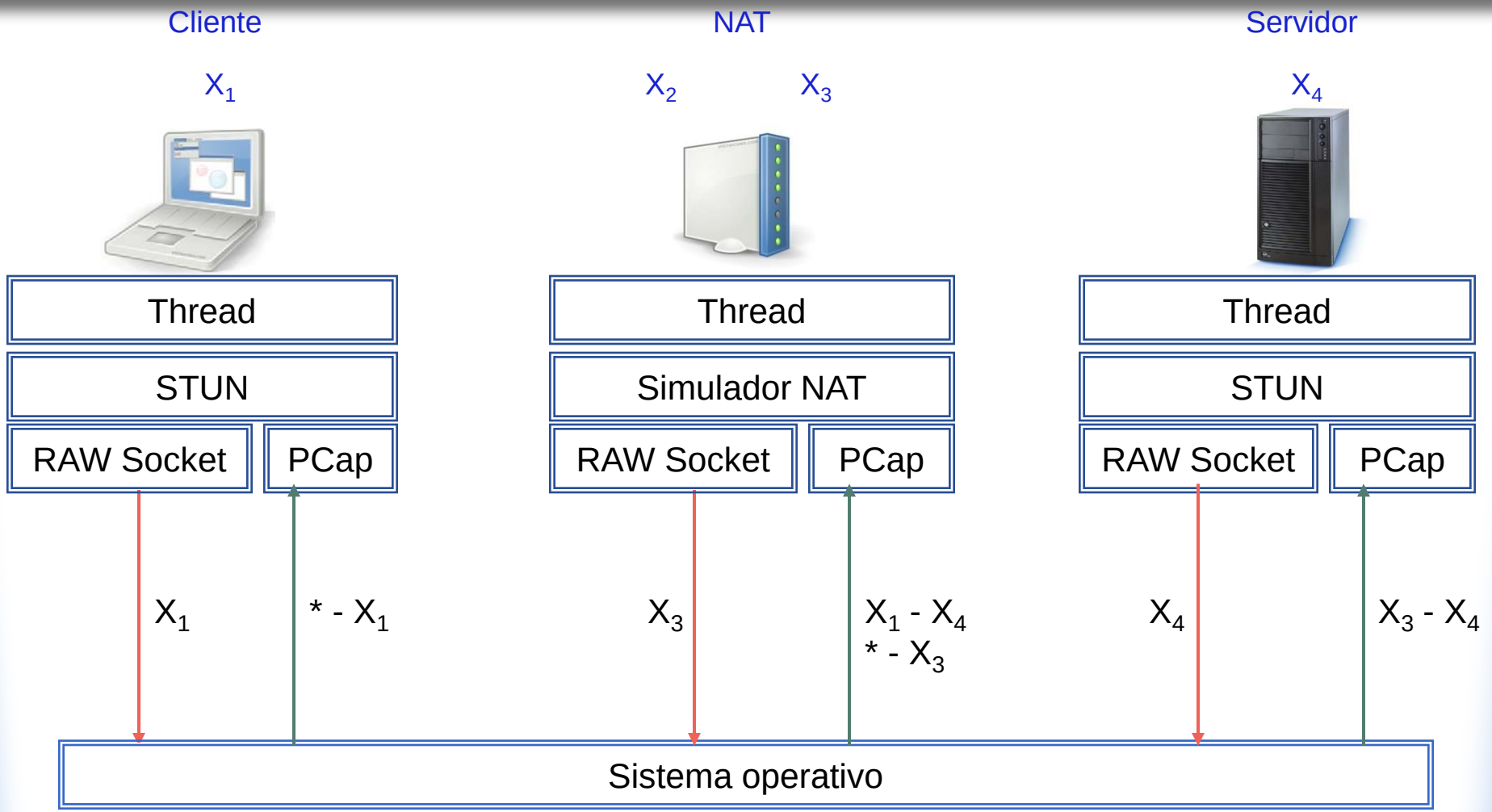
IETF: *debe ser Independiente del extremo*

SOLUCIÓN IMPLEMENTADA

análisis, diseño y validación

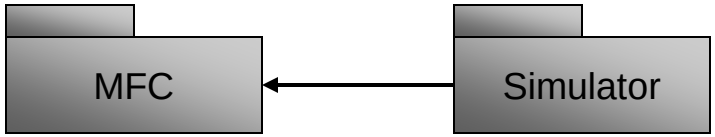
3. Análisis. NAT

3. Análisis. Componentes



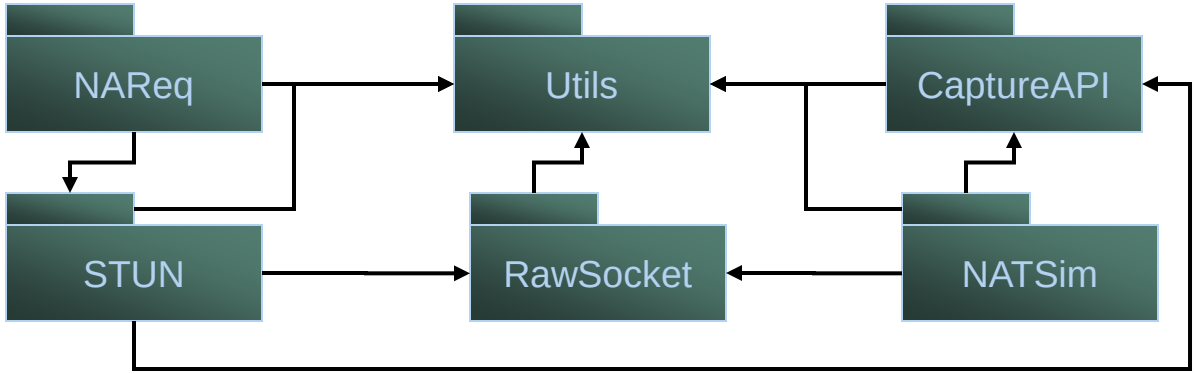
4.Diseño. Librerías

- Microsoft Foundation Class Library



- Librerías C++ desarrolladas

Portable



- PTHREAD Opensource. POSIX 1003.1c 1995 Standard para Win32
- PCAP Interface de alto nivel para la captura de paquetes

5. Validación. Requisitos IETF (I)

Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [RFC 4787].

CARACTERISTICA	FUNCIONAMIENTO	NECESIDAD
MAPEO	Independiente del extremo	Obligatorio
PARQUE IPs EXTERNAS	Asignación pareada	Recomendable
SOBRECARGA DE PUERTOS	No	Obligatorio
	Conservar rangos	Recomendable
PARIDAD DE PUERTOS	Sí	Recomendable
EXPIRACION MAPEO UDP	Mínimo 2 minutos	Obligatorio
	Puertos bien conocidos, menor de 2 minutos	Posible
	Tiempo configurable	Posible
	Al menos 5 minutos	Recomendable
	Refresco de salida	Obligatorio
	Refresco de entrada	Posible
FILTRO	Independiente del extremo	Recomendable
	Dependiente de dirección	Recomendable
	Configurable	Posible

5. Validación. Requisitos IETF (II)

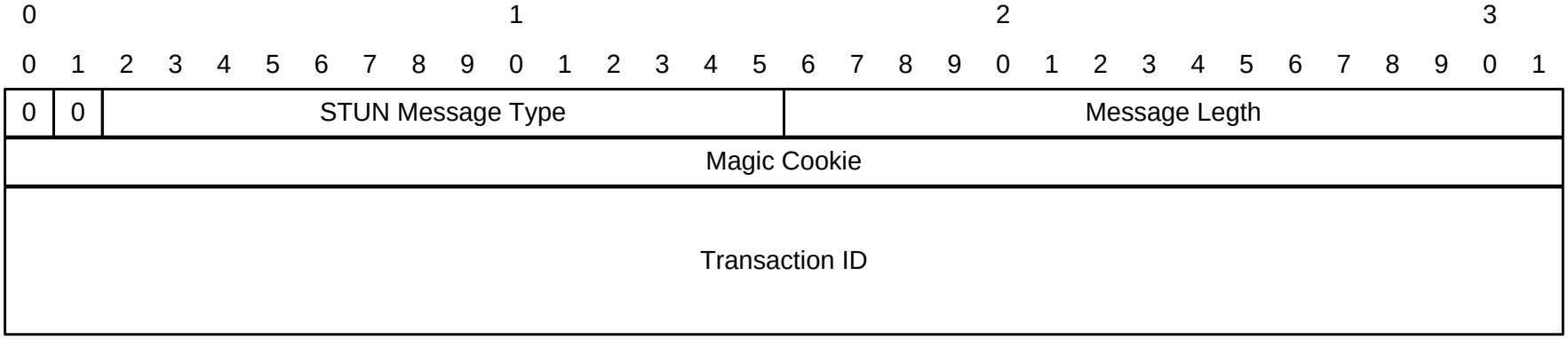
Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [RFC 4787].

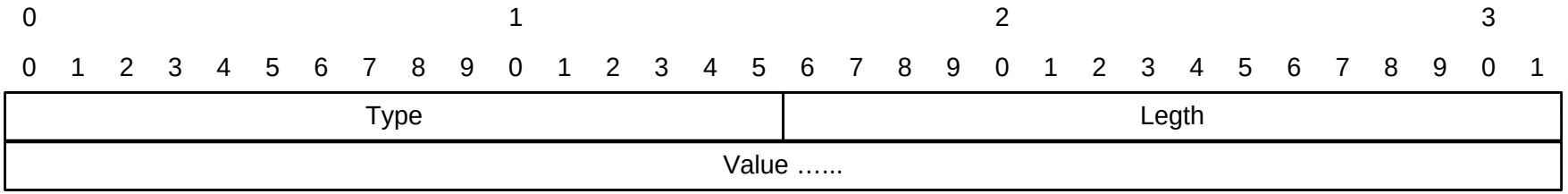
CARACTERISTICA	FUNCIONAMIENTO	NECESIDAD
HORQUILLA	Presentar paquetes en horquilla con dirección externa	Obligatorio
ALGs	Desactivados	Obligatorio
	Administrados	Recomendable
COMPORTAMIENTO (MAPEO Y FILTRO)	Determinístico	Obligatorio
RECEPCIÓN ICMP	No termina mapeo	Obligatorio
	No filtra basándose en IP origen	Obligatorio
	Soporte de mensaje de destino inalcanzable	Obligatorio
FRAGMENTACION	Soporte de envío en orden	Obligatorio
	Recepción en orden y fuera de orden	Obligatorio

5. Validación. STUN (I)

Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) [RFC 3489] March 2003

- **Session Traversal Utilities for NAT (STUN)**: protocolo tipo cliente/servidor que proporciona funciones para que entidades situadas detrás de un NAT conozcan la dirección asignada y sean capaces de mantener esta dirección abierta el tiempo que la necesiten.





5. Validación. STUN (II)

MENSAJES

BINDING REQUEST:	0x0001
BINDING RESPONSE:	0x0101

ATRIBUTOS

PETICIÓN:

RESPONSE ADDRESS	0X0002
CHANGE REQUEST	0x0003
Change IP	0x0004
Change Port	0x0002
Change both	0x0006

RESPUESTA:

MAPPED ADDRESS	0x0001
SOURCE ADDRESS	0x0004
CHANGED ADDRESS	0x0005
XOR MAPPED ADDRESS	0x8020

BINDING-REQUEST

CHANGE_REQUEST Change IP: 0 Change Port: 0

00 01 00 08
8F FC 04 00 8F FC 04 00 D9 54 00 00 D9 54 00 00
00 03 00 04 00 00 00 00

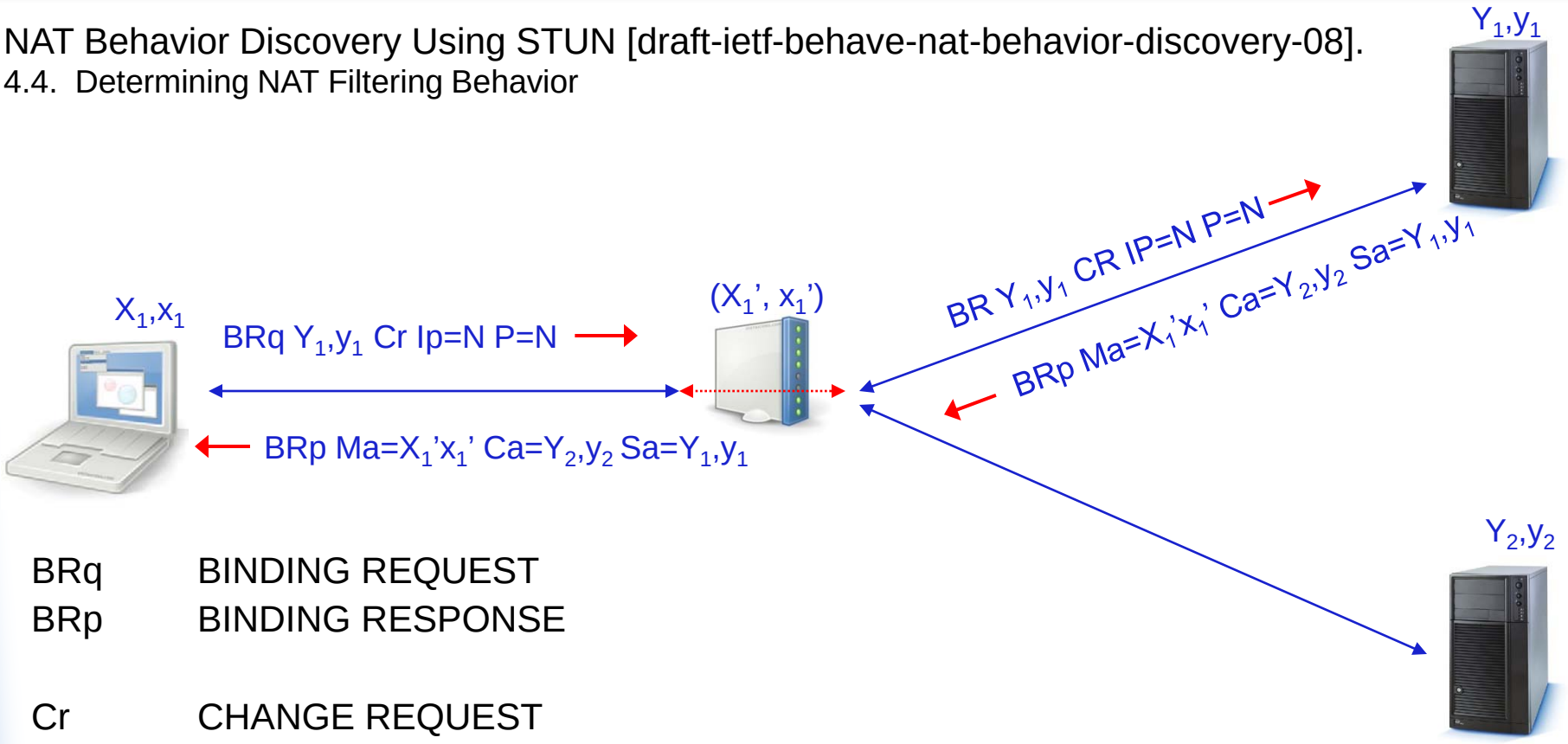
BINDING-RESPONSE

MAPPED_ADDRESS	217.125.242.41.10000
SOURCE_ADDRESS	169.0.209.22.3478
CHANGED_ADDRESS	169.0.208.27.3479
XOR_MAPPED_ADDRESS	86.129.246.41.56223

01 01 00 30
8F FC 04 00 8F FC 04 00 D9 54 00 00 D9 54 00 00
00 01 00 08 00 01 27 10 D9 7D F2 29
00 04 00 08 00 01 0D 96 A9 00 D1 16
00 05 00 08 00 01 0D 97 A9 00 D0 1B
80 20 00 08 00 01 DB 9F 56 81 F6 29

5. Validación. Mapeo (I)

NAT Behavior Discovery Using STUN [draft-ietf-behave-nat-behavior-discovery-08].
4.4. Determining NAT Filtering Behavior



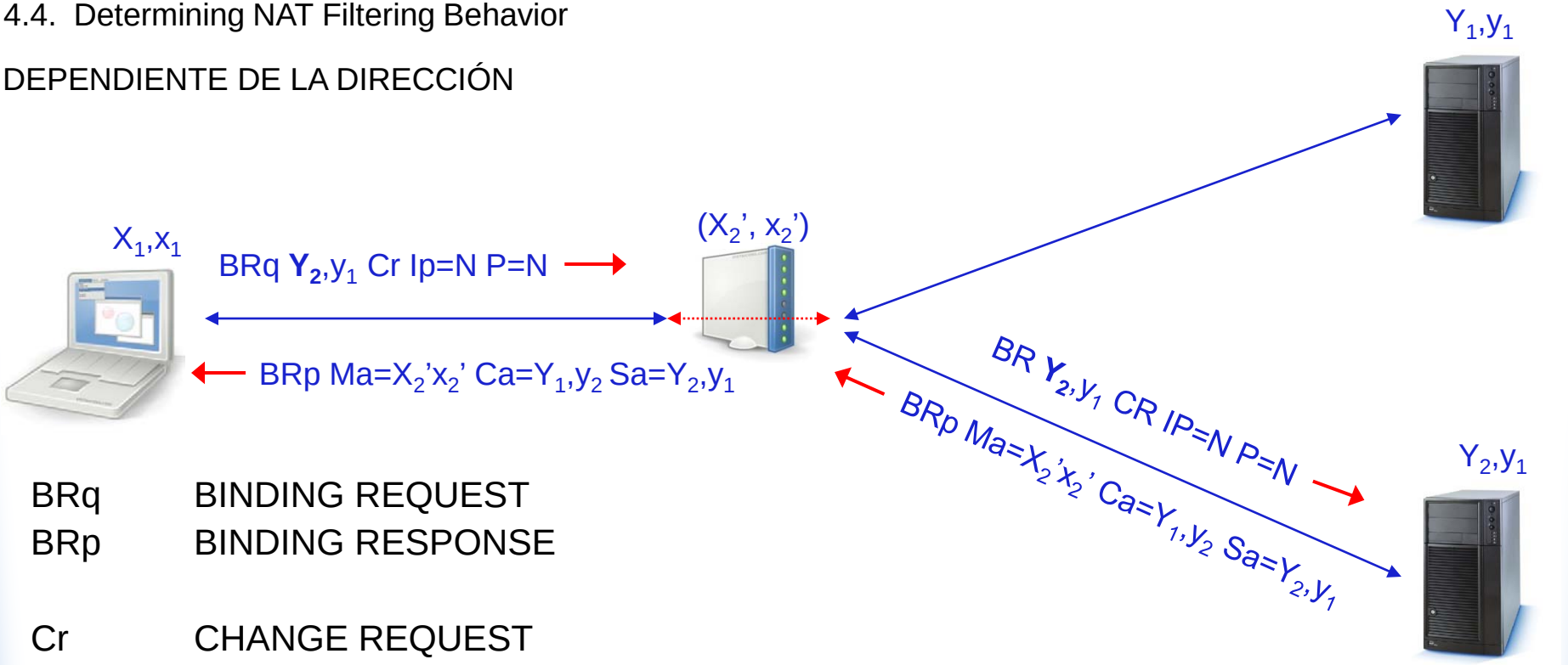
BRq	BINDING REQUEST
BRp	BINDING RESPONSE
Cr	CHANGE REQUEST
Ma	MAPPED ADDRESS
Ca	CHANGED ADDRESS
Sa	SOURCE ADDRESS

5. Validación. Mapeo(II)

NAT Behavior Discovery Using STUN [draft-ietf-behave-nat-behavior-discovery-08].

4.4. Determining NAT Filtering Behavior

DEPENDIENTE DE LA DIRECCIÓN



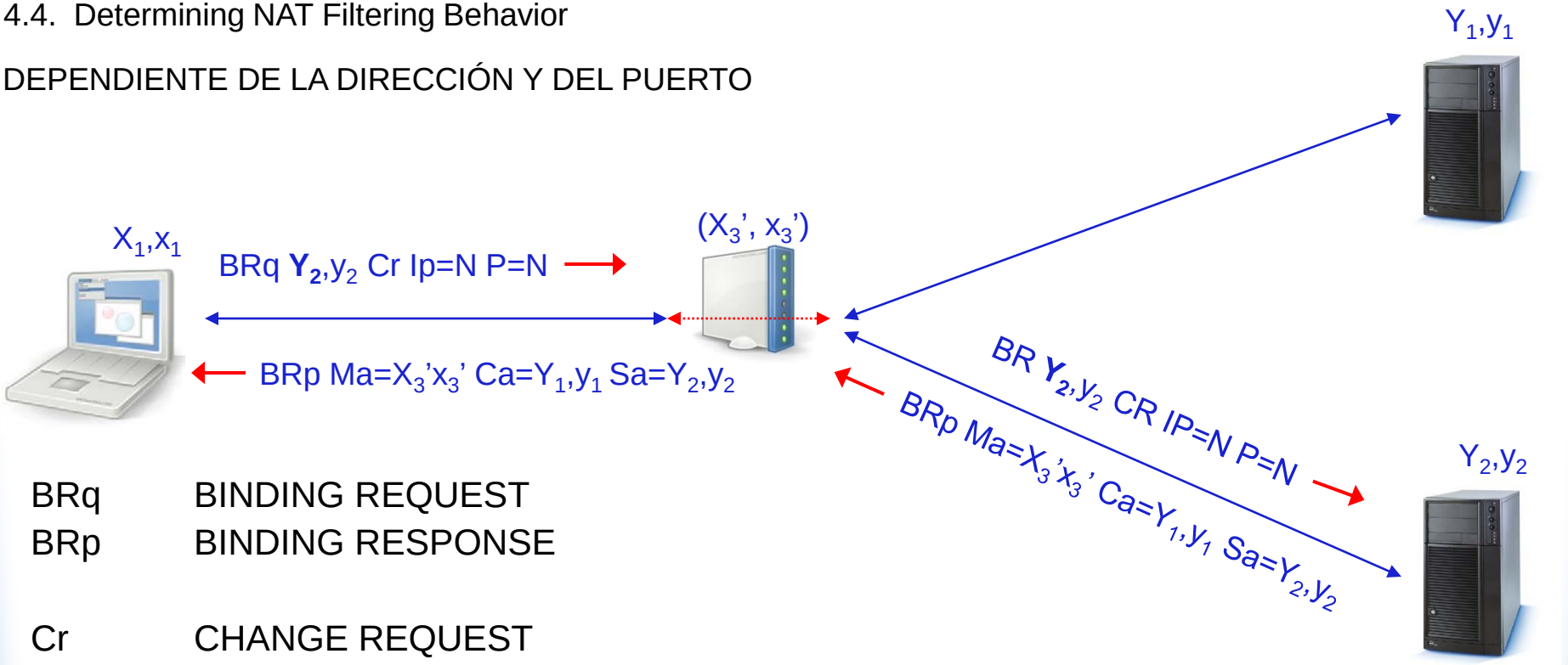
BRq	BINDING REQUEST
BRp	BINDING RESPONSE
Cr	CHANGE REQUEST
Ma	MAPPED ADDRESS
Ca	CHANGED ADDRESS
Sa	SOURCE ADDRESS

5. Validación. Mapeo (III)

NAT Behavior Discovery Using STUN [draft-ietf-behave-nat-behavior-discovery-08].

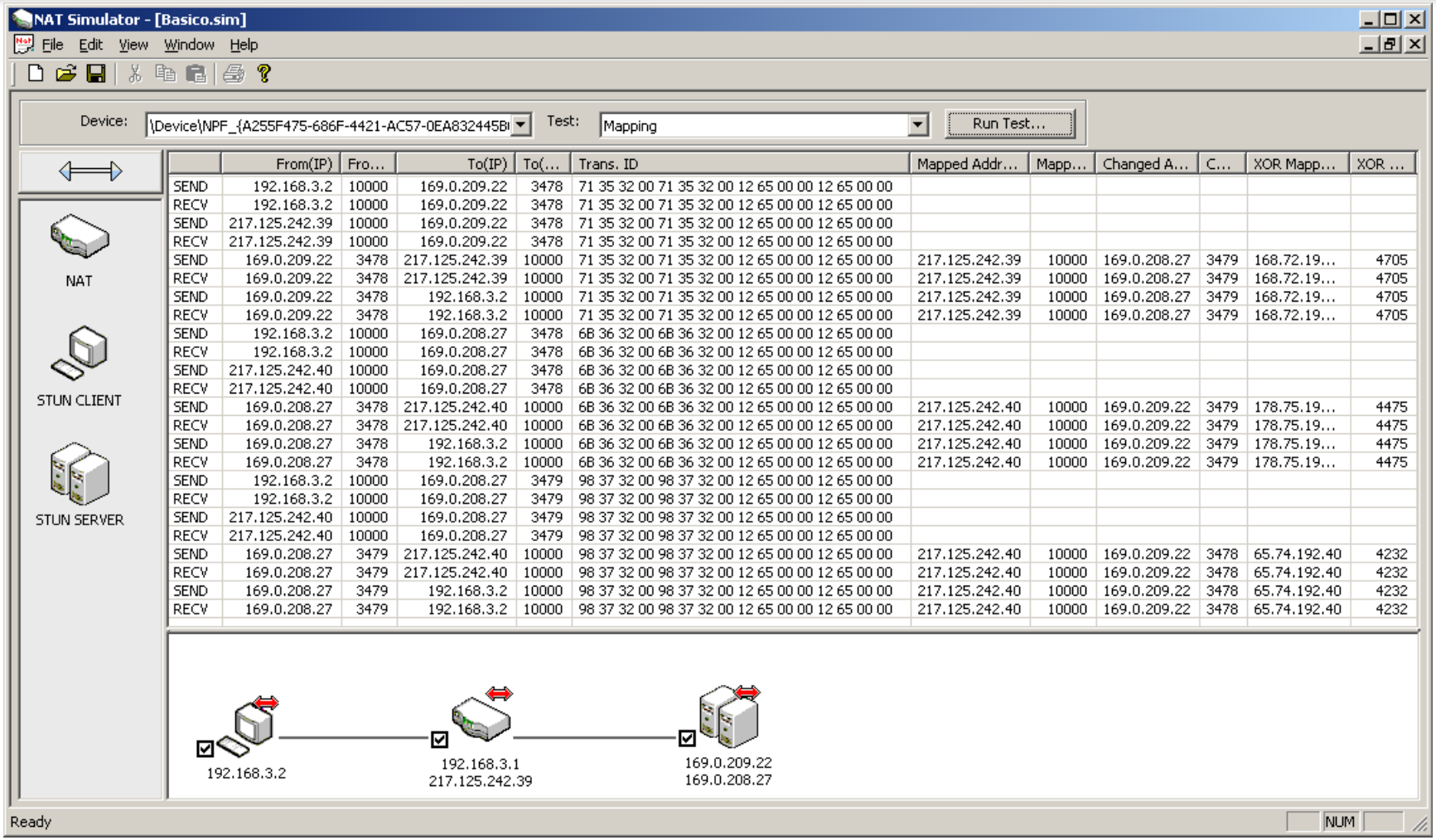
4.4. Determining NAT Filtering Behavior

DEPENDIENTE DE LA DIRECCIÓN Y DEL PUERTO



BRq	BINDING REQUEST
BRp	BINDING RESPONSE
Cr	CHANGE REQUEST
Ma	MAPPED ADDRESS
Ca	CHANGED ADDRESS
Sa	SOURCE ADDRESS

6 DEMO



	From(IP)	Fro...	To(IP)	To(...	Trans. ID	Mapped Addr...	Mapp...	Changed A...	C...	XOR Mapp...	XOR ...
SEND	192.168.3.2	10000	169.0.209.22	3478	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00						
RECV	192.168.3.2	10000	169.0.209.22	3478	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00						
SEND	217.125.242.39	10000	169.0.209.22	3478	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00						
RECV	217.125.242.39	10000	169.0.209.22	3478	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00						
SEND	169.0.209.22	3478	217.125.242.39	10000	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00	217.125.242.39	10000	169.0.208.27	3479	168.72.19...	4705
RECV	169.0.209.22	3478	217.125.242.39	10000	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00	217.125.242.39	10000	169.0.208.27	3479	168.72.19...	4705
SEND	169.0.209.22	3478	192.168.3.2	10000	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00	217.125.242.39	10000	169.0.208.27	3479	168.72.19...	4705
RECV	169.0.209.22	3478	192.168.3.2	10000	71 35 32 00 71 35 32 00 12 65 00 00 12 65 00 00	217.125.242.39	10000	169.0.208.27	3479	168.72.19...	4705
SEND	192.168.3.2	10000	169.0.208.27	3478	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00						
RECV	192.168.3.2	10000	169.0.208.27	3478	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00						
SEND	217.125.242.40	10000	169.0.208.27	3478	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00						
RECV	217.125.242.40	10000	169.0.208.27	3478	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00						
SEND	169.0.208.27	3478	217.125.242.40	10000	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3479	178.75.19...	4475
RECV	169.0.208.27	3478	217.125.242.40	10000	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3479	178.75.19...	4475
SEND	169.0.208.27	3478	192.168.3.2	10000	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3479	178.75.19...	4475
RECV	169.0.208.27	3478	192.168.3.2	10000	6B 36 32 00 6B 36 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3479	178.75.19...	4475
SEND	192.168.3.2	10000	169.0.208.27	3479	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00						
RECV	192.168.3.2	10000	169.0.208.27	3479	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00						
SEND	217.125.242.40	10000	169.0.208.27	3479	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00						
RECV	217.125.242.40	10000	169.0.208.27	3479	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00						
SEND	169.0.208.27	3479	217.125.242.40	10000	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3478	65.74.192.40	4232
RECV	169.0.208.27	3479	217.125.242.40	10000	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3478	65.74.192.40	4232
SEND	169.0.208.27	3479	192.168.3.2	10000	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3478	65.74.192.40	4232
RECV	169.0.208.27	3479	192.168.3.2	10000	98 37 32 00 98 37 32 00 12 65 00 00 12 65 00 00	217.125.242.40	10000	169.0.209.22	3478	65.74.192.40	4232

Conclusiones

- Cliente y servidor STUN siguiendo la RFC 3489.
- NAT UDP válido para otros test de aplicaciones que operan a través de NAT.
- Tests de traspaso de NAT basados en RFC 4787 y testeados contra servidores STUN públicos.
- Arquitectura polivalente aplicable a otros escenarios de conexión sobre IP.
- Código portable a otras arquitecturas.

Trabajos futuros

- Implementación en el NAT de la capa TCP.
- Generación de test para requisitos no implementados.
- Mejoras en la forma de asignar filtros a los componentes basadas en tablas de rutas.
- Adaptación a IPv6 en previsión de detectar dispositivos similares a NAT.
- Pasarelas IPv6<->IPv4.
- Migración a 64 bits.
- Implementación de la interfaz gráfica con librerías portables (p.e. Qt).
- Otras simulaciones .

GRACIAS

Diseño y desarrollo de un marco de pruebas y detección de NATs

Autor: Francisco José Blázquez Sánchez

Tutor: Francisco Valera Pintor

Ingeniería en Informática. Octubre de 2009

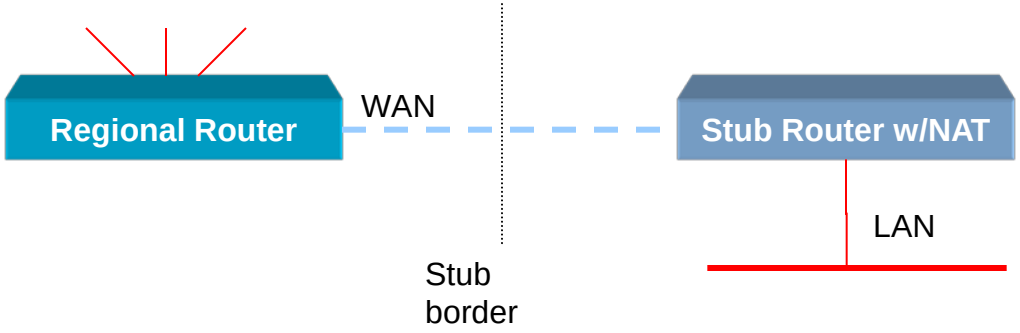
DOCUMENTACIÓN DE APOYO

2. NATs. Definición

IP Network Address Translator (NAT) Terminology and Considerations
[RFC 2663] August 1999

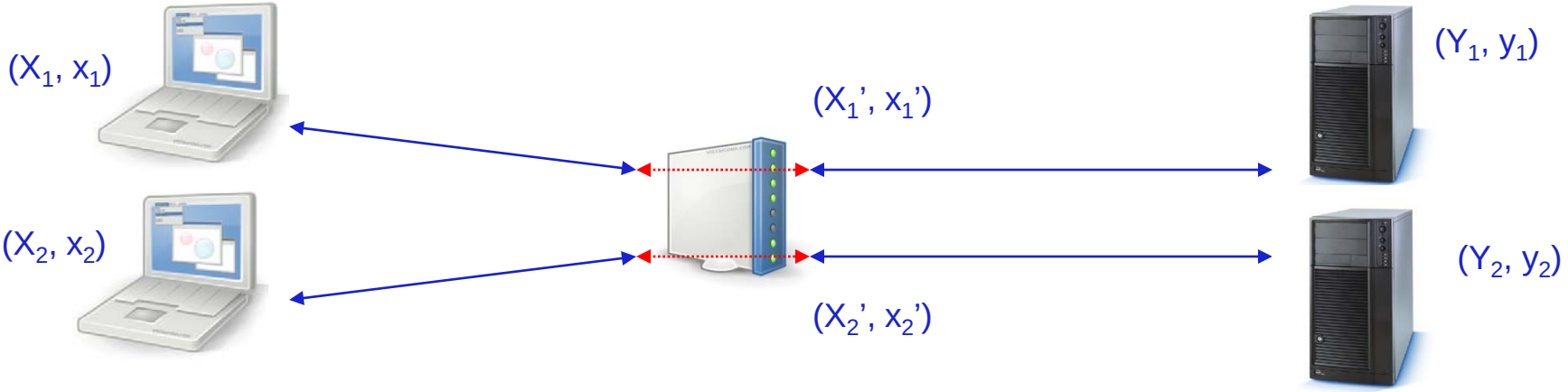
La traducción de dirección de red (Network Address Translation), es un método por el cual las direcciones IP son mapeadas desde un espacio de direcciones a otro, proporcionando enrutamiento transparente en los extremos finales. Hay muchas variantes para la traducción de direcciones que se prestan a diferentes usos. Sin embargo, todos los dispositivos NAT deberían compartir las características siguientes:

a) Traducción de direcciones transparente.
b) Enrutamiento transparente por medio de traducción de direcciones.
Enrutamiento como reenvío de paquetes y no intercambio de información de enrutamiento.
c) Traducción de paquetes de error ICMP.



2. NATs. Asignación IP y puerto

Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [RFC 4787].



- Asignación de IP pareada
- Asignación de IP arbitraria

IETF: Debe ser pareada

- Asignación de puerto conservativa

$x_1 = x_1'$ y $x_2 = x_2'$

- Asignación de puerto no conservativa

$x_1 <> x_1'$ y $x_2 <> x_2'$

IETF : Recomendable conservar rangos

- Asignación de puerto con sobrecarga

$x_1 = x_1' = x_2 = x_2'$

IETF: No debe ser sobrecargada

- Asignación de puerto conservando paridad

IETF: Recomendable

- Asignación de puerto contiguo (RTCP=RTP+1)

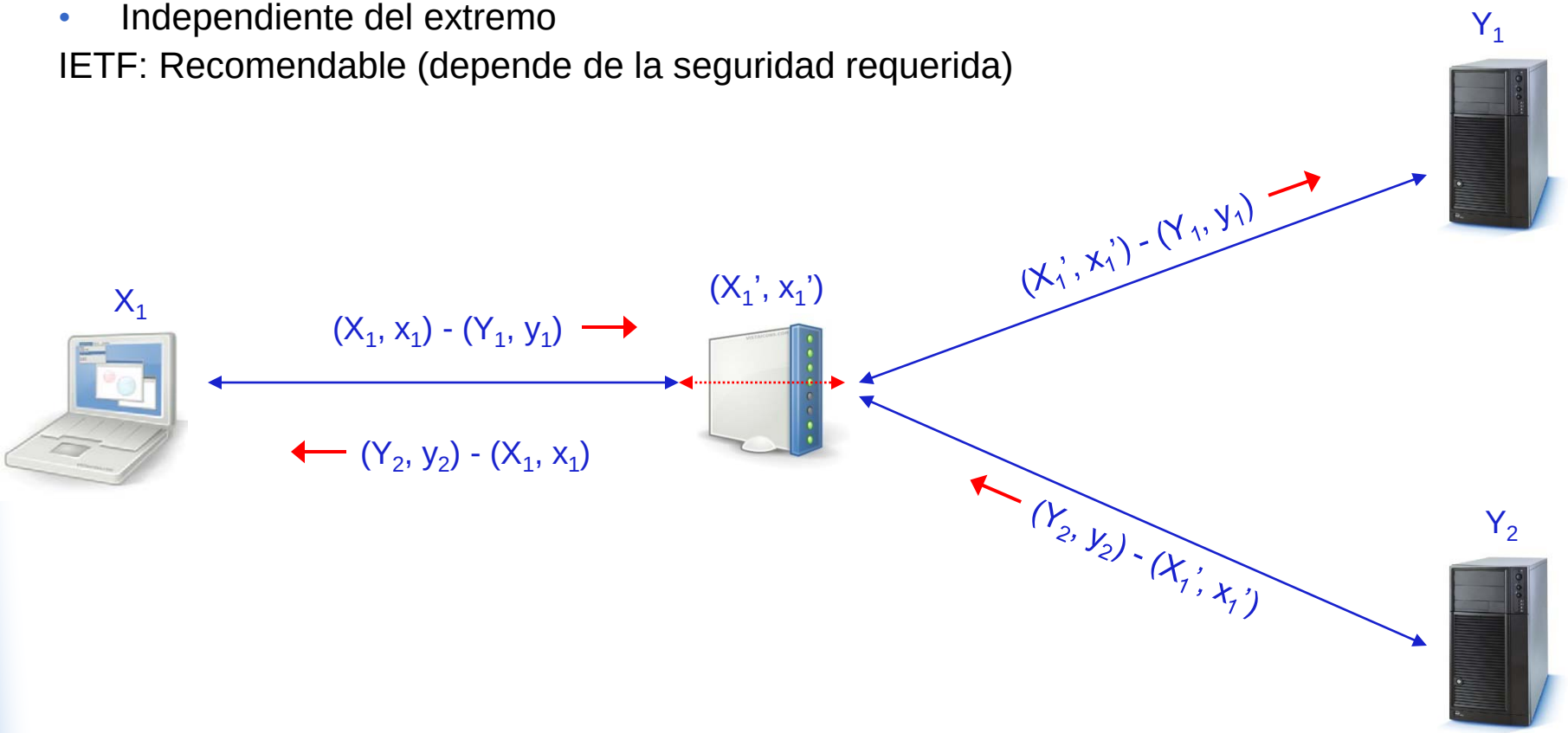
IETF: Aplicaciones negocian puertos

2. NATs. Filtrado de paquetes (I)

Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [RFC 4787].

- Independiente del extremo

IETF: Recomendable (depende de la seguridad requerida)

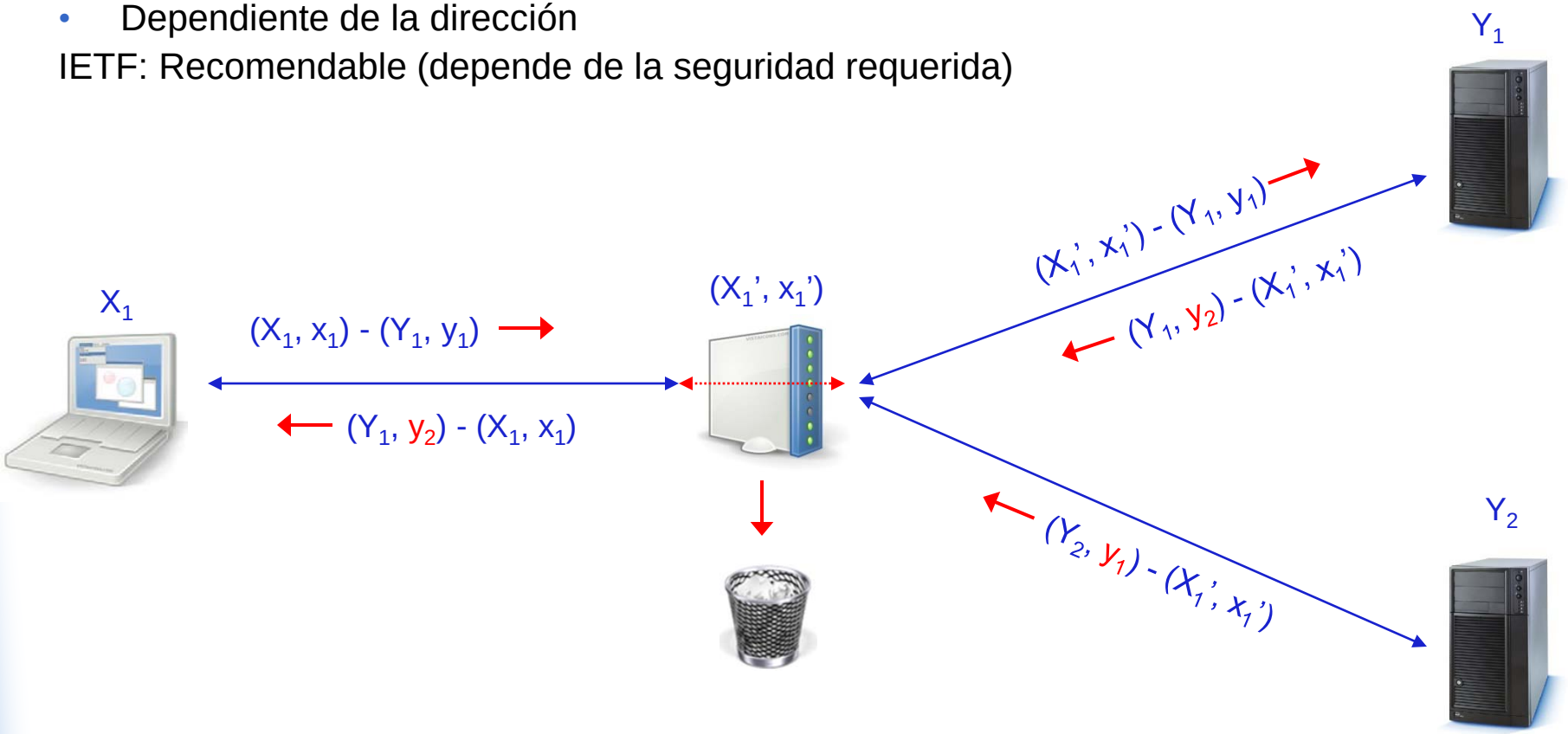


2. NATs. Filtrado de paquetes (II)

Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [RFC 4787].

- Dependiente de la dirección

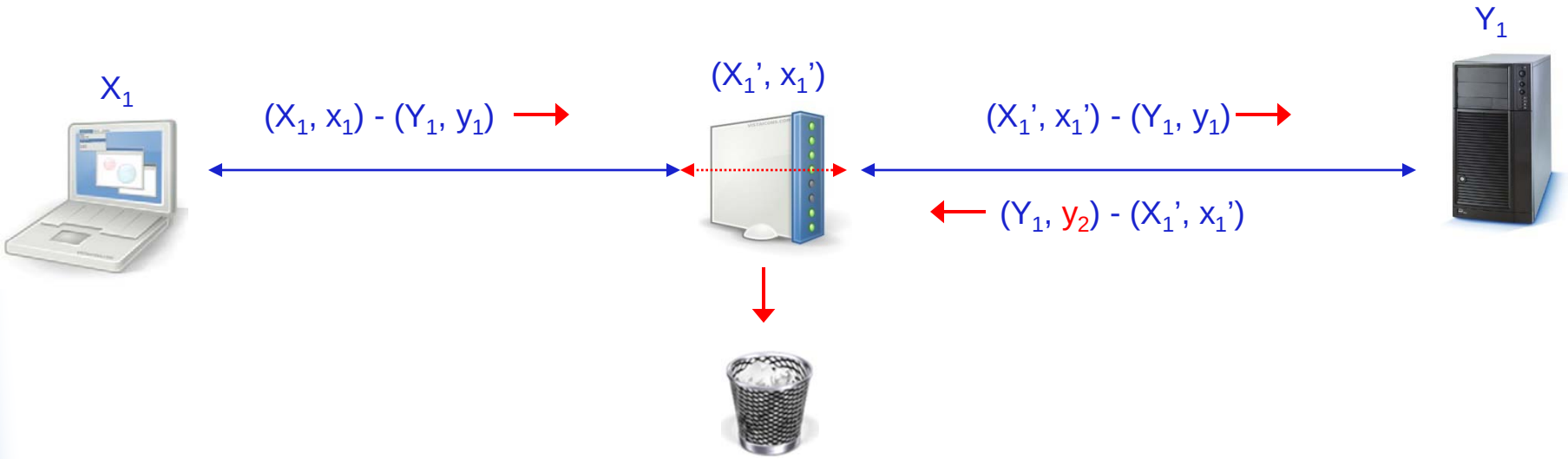
IETF: Recomendable (depende de la seguridad requerida)



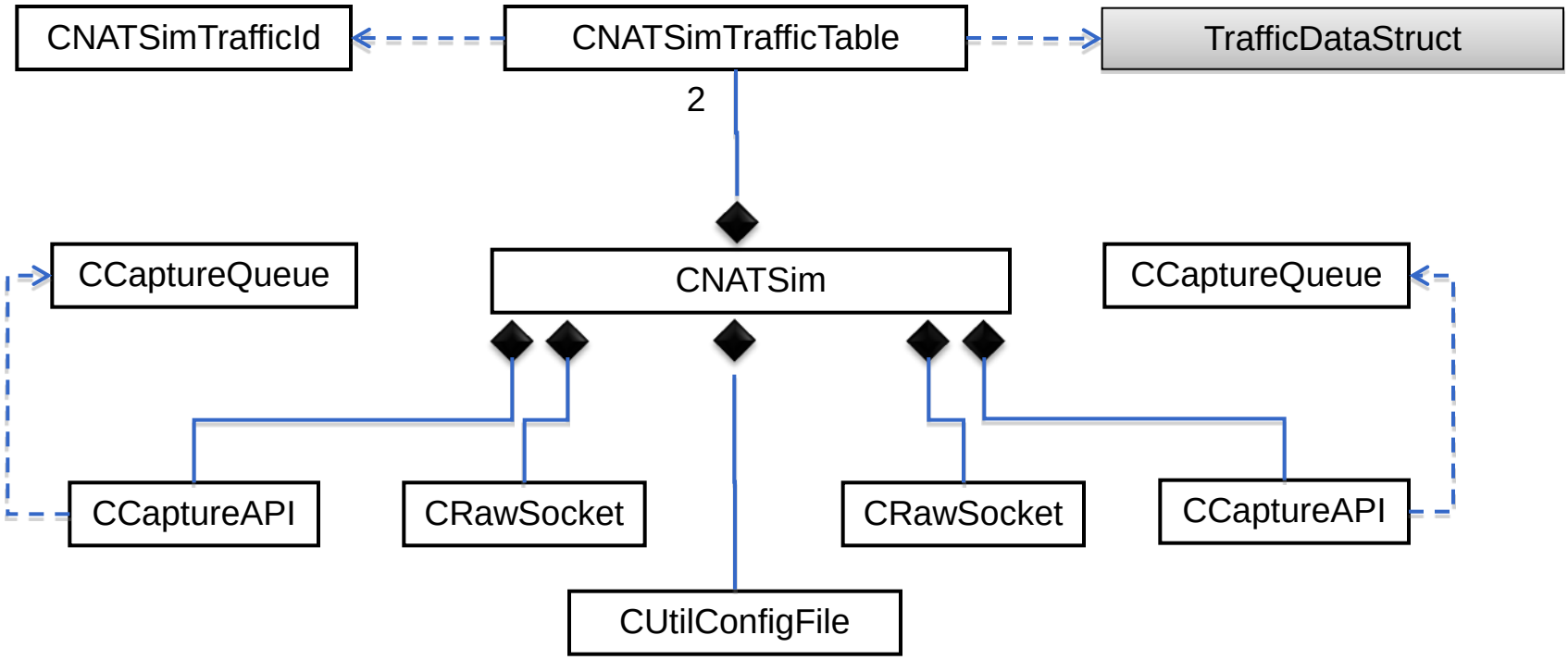
2. NATs. Filtrado de paquetes (III)

Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [RFC 4787].

- Dependiente de la dirección y del puerto

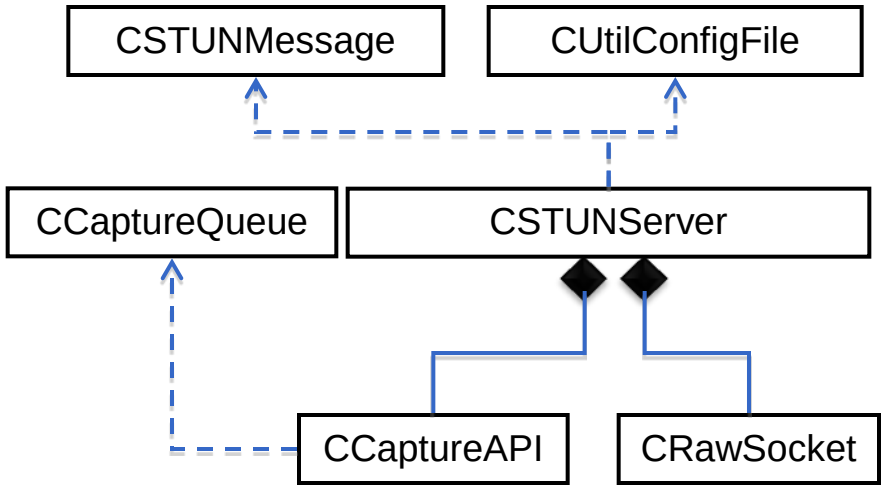


4. Diseño. NAT

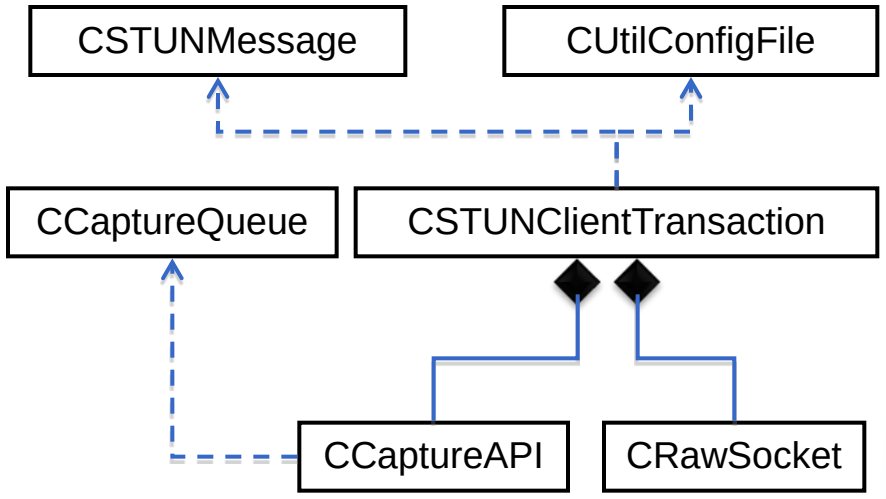


Simulador de NATs

4. Diseño. STUN

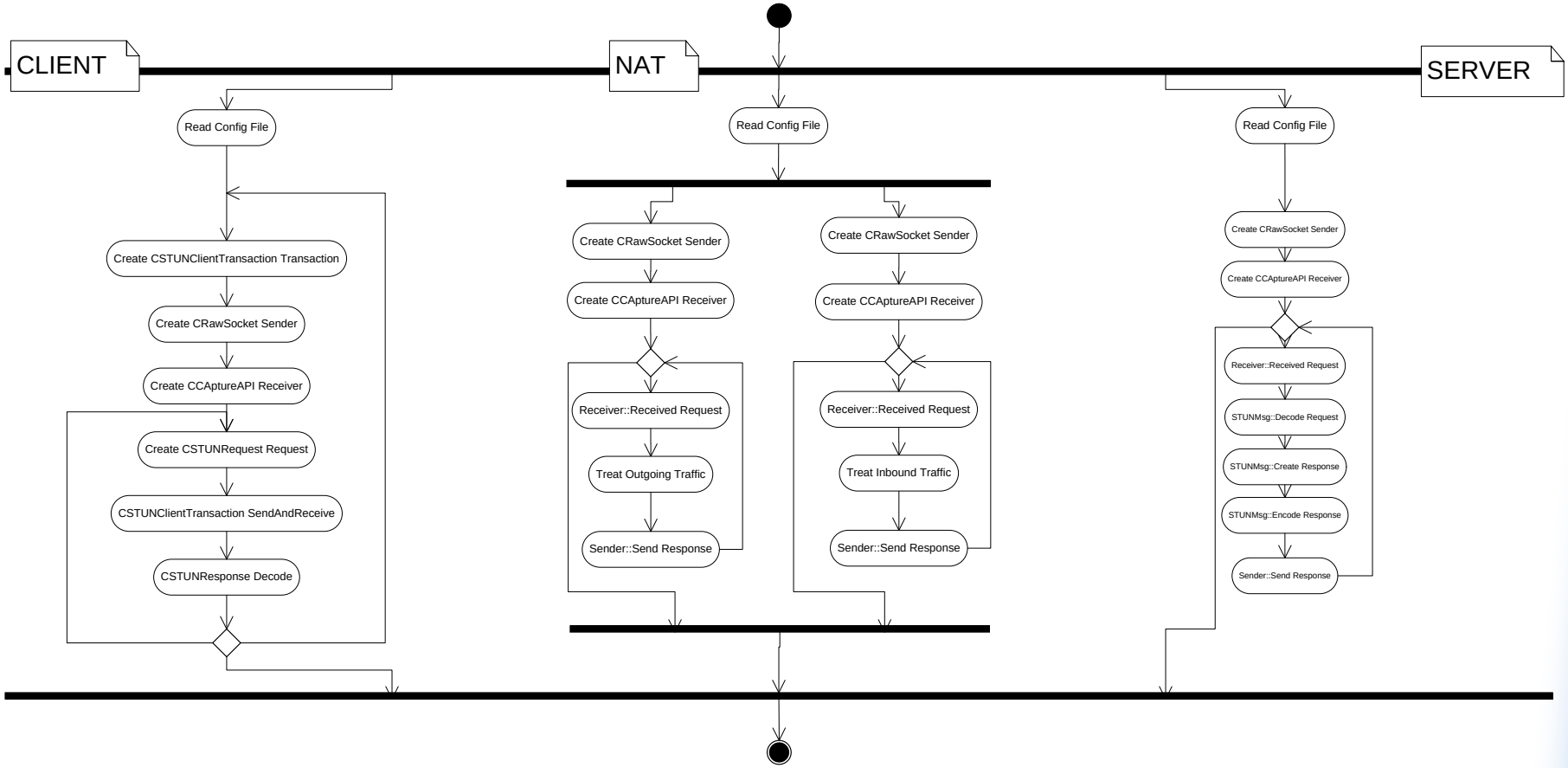


Servidor



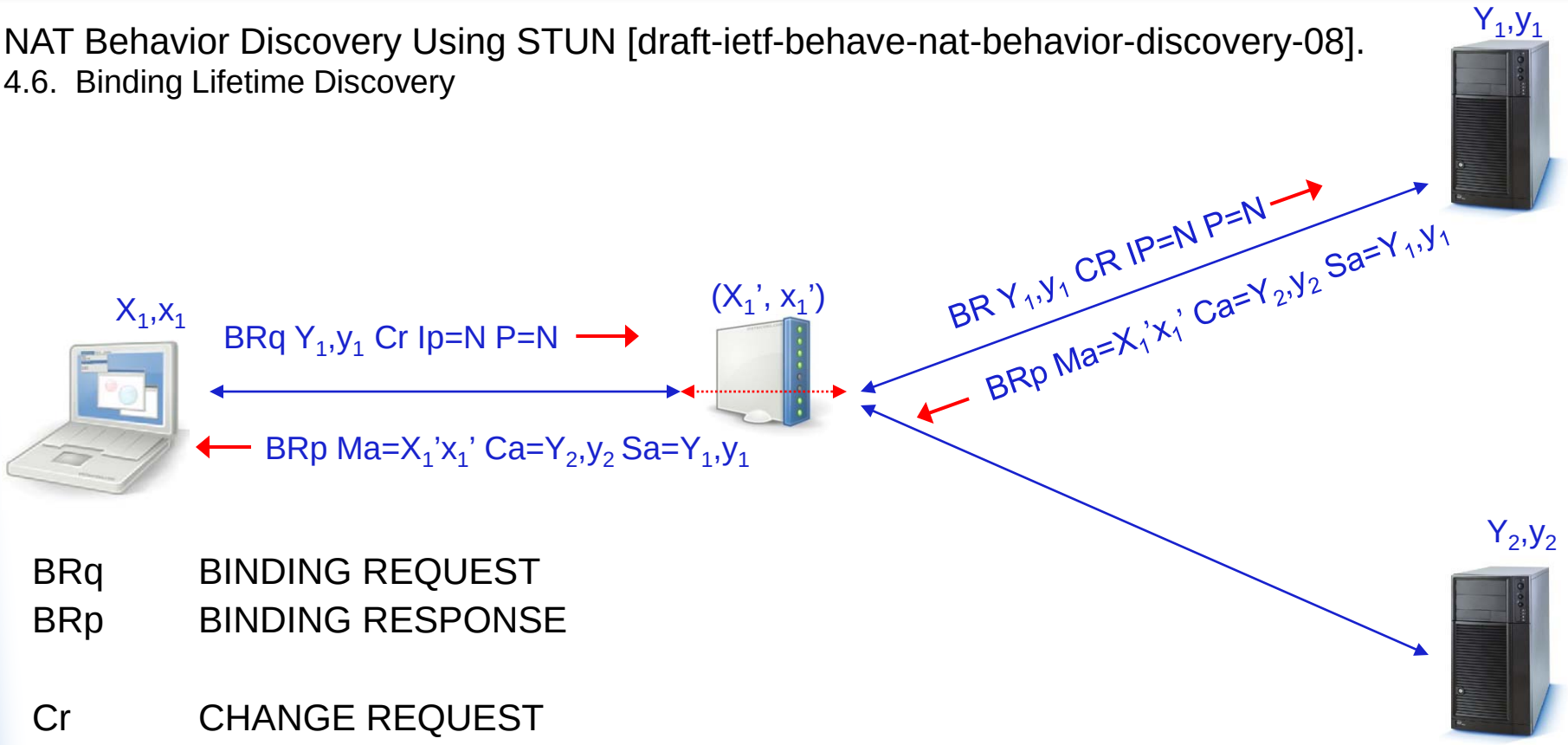
Cliente

4. Diseño. Diagrama completo



5. Validación. Timeout

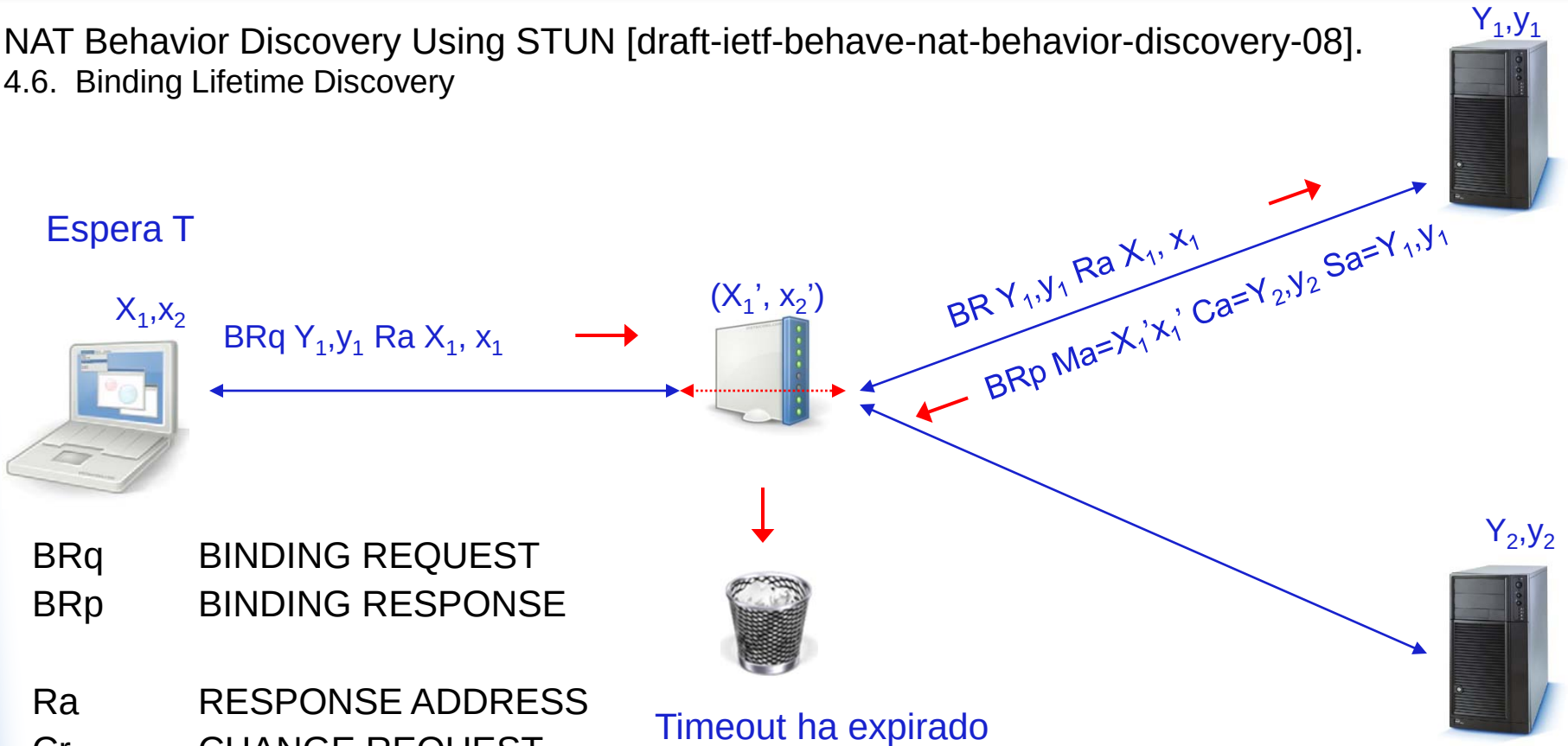
NAT Behavior Discovery Using STUN [draft-ietf-behave-nat-behavior-discovery-08].
4.6. Binding Lifetime Discovery



BRq	BINDING REQUEST
BRp	BINDING RESPONSE
Cr	CHANGE REQUEST
Ma	MAPPED ADDRESS
Ca	CHANGED ADDRESS
Sa	SOURCE ADDRESS

5. Validación. Timeout (II)

NAT Behavior Discovery Using STUN [draft-ietf-behave-nat-behavior-discovery-08].
4.6. Binding Lifetime Discovery



BRq	BINDING REQUEST
BRp	BINDING RESPONSE
Ra	RESPONSE ADDRESS
Cr	CHANGE REQUEST
Ma	MAPPED ADDRESS
Ca	CHANGED ADDRESS
Sa	SOURCE ADDRESS