JAVA, creación de servidores UDP

DatagramSocket socketUDP

Server

1. Crear UDP packet
   `DatagramPacket packet = new DatagramPacket(buffer, buffer.lenght)`
2. Esperar petición de fecha y hora
   `socketudp.receive(packet);`
   `InetAddress clientaddr = packet.getAddress();`
   `int clientport = packet.getPort();`
3. Obtener dir IP y puerto
   `packet.setAddress(servad);`
   `packet.setPort(port);`

   //Extra
   `String date = NewDate();`
   `packet.setData(date.getBytes());`
4. Enviar fecha y hora
   `socketudp.send(packet);`

Cliente → Tiene el puerto y address

1. Crear socket UDP → En cliente
   `DatagramSocket socketudp = new DatagramSocket();`
2. Enviar petición al servidor
   `DatagramPacket packet = new DatagramPacket(buffer, buffer.lenght, servad, port);`
   `Socketudp.send(packet);`
3. Recivir envio
   `Socketudp.receive(packet);`
4. Cerrar comunicación
   `socketudp.close();` → La cierra cliente

Ideas:

`Socketudp` → Estructura del sistema

`Packet` → Información manda

JAVA, sockets TCP sin threads → Solo 1 servicio a la vez

Server

1. TCP Listener in port
   `ServerSocket socket = new ServerSocket(port)`
2. Acepto una nueva conexión TCP (while(true))
   `Socket socket2 = socket.accept();`
3. Crear Streams asociados
   `String quote = newQuote();`
   `PrintWriter outfl = new PrintWriter(socket2.getOutputStream(), true);`
4. Mandar la quote
   `outfl.println(quote);`
5. Cerro conexión
   `socket2.close();`

Cliente

1. Crear socket TCP "serveraddi" y "port"
   `Socket socketudp = new Socket(serveraddr, port);`
2. Crear Stream de streams asociados a la conexión TCP
   `BufferedReader infl = new BufferedReader(new InputStreamReader(socketudp.getInputStream()));`
3. Recibir quote of day de la conexión TCP
   `while((quote = infl.readLine()) != null){`
   `Sout(quote); }`
4. Cerrar conexión
   `Socketudp.close();` → Lo cierra cliente

Ideas:

inflow server → client

outflow client → server

JAVA, sockets TCP con threads

La mayor diferencia es el uso de estas líneas en el código

```
Thread thread = new Thread(new ClientHandler(clientSocket));
thread.start();
```

{ En el server

Nueva clase, Handler

Clase Handler
- → Define inflows y outflows
- → Comprueba los envíos del cliente a través del servidor
- → Realiza acción principal
- → Cierra comunicaciones

Análisis protocolo DHCP

Obtención del alquiler → DORA

Discover
Offer — "Toma nueva IP, hay máscara"
Request
Ack

Renovación del alquiler → RA

Request
Ack → "Sabe a dónde mandarlo, IP usuario"

Revinculación del alquiler → RA

Request
Ack → "No sabe a dónde mandarlo, MÁSCARA 255.255.255.255"

Reasignación del alquiler → DORA

Discover
Offer
Request — "Usa una IP ya usada para alargar su tiempo de uso"
Ack

* Observar las trazas con el mismo ID
* Siempre la IP acabada en .2 es la del servidor

Comprensión configuración DHCP

1) Server IP → 192.168.10.2
Net mask → 255.255.255.0
Gateway → 192.168.10.1
Broadcast → 192.168.10.255
Range 192.168.10.10 - 192.168.10.254 (*)

Máscara que da para 255-2 conexiones, los PCs tomarán de la 10 a la 254 ya que el resto ya serán preasignadas

192.168.10.1 es la puerta de enlace para todos salvo que se especifique lo contrario.

```
host servidor-HTTP}
hardware ethernet
4a:46:f3:33:67:e3;
fixed address 192.168.10.3;
option routers 192.168.10.2;

host e-mail}
hardware ethernet 9e:d9:5b:66:97:67;
fixed-address 192.168.10.4;
option routers 192.168.10.2;
```

Anula la definición previa (*)

Control de congestión en TCP 4.2

1- Valor de la ventana inicial de congestión cuando ini

Primeros TCP → pinchas y a la derecha WS = 2 → Si pide nº de segmentos

" " → " y buscas window size = 5792 → Si pide en bytes

↝ Recuperación rápida = cambia el color a negro en Wireshark

(3) La que se emite = Fast Retransmission

Bytes en vuelo: Pant recup - Valo ACK dup + 1

ssthresh = bytes en vuelo /2

secuencia

nº blanco antes del Fast retransmission + 1448 - 1 (lenght)

532865 + 1448 - 1 : 534312

534312 - 503353 + 1 = 28960 ↳ /2

(5) Cuando cambia el color a blanco (Primer fast Retransmission = 1063 trama

(6) Recuperación rápida → arranque lento → evitación de congestión

Los ssthresh cambian

Statistics → Conversación = 992 kbps ≈ 1 Mbit/s

NAT estático = Red privada, accesible desde fuera

NAT dinámico: Trad. no existen hasta que el router no recibe info de dentro. TODO SE BORRA

NAPT = P de puerto

$2^4 + 2^{30}$

4 Gpalab, min bits mAR?

$2^2 +$

64 Gpalab 16 bits palab

$2^6 \times 2^{30}$ palab 2 bytes x palab

8 Gpalabras, palab 32 bits, 4 bytes

$2^3 \cdot 2^{30}$ palab $\cdot 2^2$ bytes/palab $= 2^{35} = 2^5$ Gbytes

4 Gbytes, palab de 16 bits

$2^2 \times 2^{30} \times 2^2$ byte x palab

16 Pbytes $= 2^4 \cdot 2^{20} = 2^{24}$

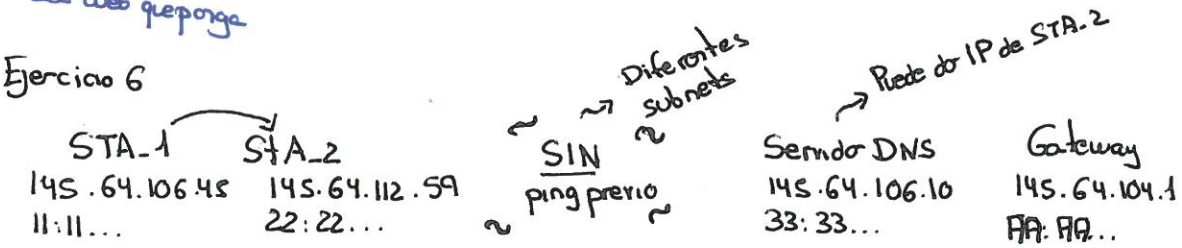
2^{24} bytes / 2^2 byte/palab $= 2^{22}$ bas

Analisis protocolo DNS

1- ¿Respuesta o petición?
   Ver info si hay response o no
2- ¿Asociado?
   Al otro que tenga → o ←
3- Envía o recibe a DNS server
   X a www.miweb.com
   Servidor DNS
4- ¿Es autoridad?
   Vas a los desplegables de abajo
   DNS → Flags → Authoritative
5- Nombre dominio
   La web que ponga

Extras
→ Las traducciones de web a IP se ven fácilmente en el info
→ Los dominios son aquellas partes de una URL que nunca cambia
   ↳ compvirtual.uclm.es
   dns2.uclm.es

Ejercicio 6



DIR MAC ORI	DIR MAC DEST	TIPO PACK
11:11	FF:FF	ARP REQUEST, MAC 145.64.106.10
33:33	11:11	ARP REPLY, MAC 145.64.106.10
11:11	33:33	PETICIÓN DNS
33:33	11:11	RESPUESTA DNS
11:11	FF:FF	ARP REQUEST, MAC 145.64.104.1
FF:FF	11:11	ARP REPLY, MAC 145.64.104.1
11:11	AA:AA	ICMP REQUEST
AA:AA	11:11	ICMP REPLY

(Al hacer una petición en el DNS, por ej. otros)

DIR IP ORI	DIR IP DEST	
—	—	Si hubiese ping previo sobra, ya que la info estaría en caché
—	—	
145.64.106.45	145.64.106.10	
145.64.106.10	145.64.106.45	
—	—	Igual que siempre. Al no estar en la misma subred, hablas por el gateway
—	—	
145.64.106.45	145.64.112.59	
145.64.112.59	145.64.106.45	

VER

"Ejemplo de configuración DHCP en Netkit (para hacer el Lab 6.1)" → Semana 11

"Ejemplo de configuración DNS (Lab 6.3)" → Semana 12

```
<VirtualHost *:80>
    ServerName intranet.bitnet.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/private
        <Directory /var/www/private>
            Option Indexes FollowSymsLinks MultiViews
                AuthName Intranet-Authentification
                AuthType Basic
                AuthUserFile /etc/apache2/userpass.pwd
                Require ValidUser
                Order deny,allow
                Deny from all
                Allow from 82.16.64.0/19
                Satisfy all
        </Directory>
</VirtualHost *:80>
```

AuthName Intranet-Authentification

```
AuthName    Intranet-Authentification
AuthType    Basic
AuthUserFile /etc/apache2/userpass.wd
Require ValidUse
```

Actividad 6.2 DNS

Trama 488

Mensaje de petición (query), relacionado con 497 (← →). Tiene el mismo Transaction ID

Servicio DNS IP → Sale directamente cerca del www...

¿Autoridad? → Ir buscarlo en la info

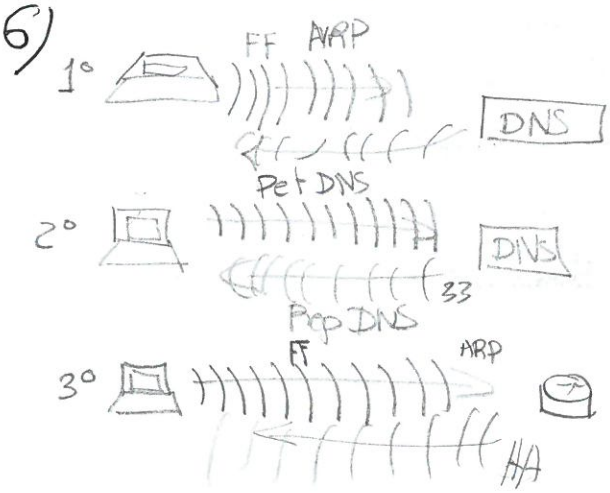
¿Dominio? → www....

Trama 374

IP del servidor DNS [...][INFO] ↵

Dominio [WWW.]

6)



Actividad 6.3 HTTP

Trama 18853

¿Petición o respuesta? GET or HTTP
petición

¿Host virtual? → host: to get el recurso /files/config...

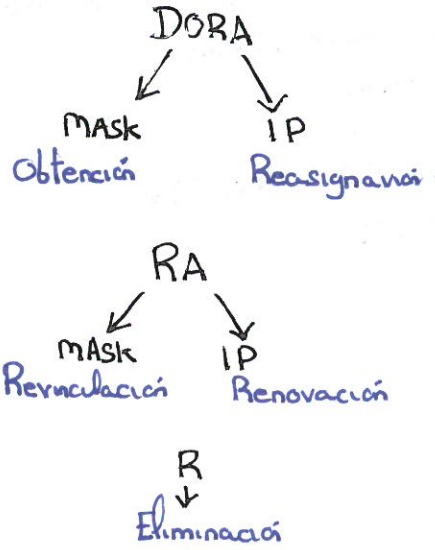
Trama 120

¿Petición o respuesta? HTTP

Actividad DHCP
6.1

"bootp" → filtra para DHCP

Trama 164



Trama 457
RA + Mask = Renovación del alquiler
La del servidor siempre 2

Trama 718
RA + IP = Renovación del alquiler

Trama 107
DORA + Mask = obtención del alquiler

Trama 50
DORA + Mask = obtención del alquiler

Trama 647
RA + IP = Renovación del alquiler

Trama 412
RA + IP → Renovación

Trama 175
RA + ~~Eliminación~~ Renovación

457
RA + MASK → Renovación

Trama 813
RA + MASK = ~~Renovación~~ Obtención

Trama 82
DORA + MASK = obtención

Trama 844
R → Eliminación

lenght == width? Lab Ejemplo 1

DHCP completo y DNS-Apache conerrores

/dhcp.esiiab.es
↳/etc
↳/default
↳\dhcp3-server
"INTERFACES="eth0" "
↳/dhcp
↳\dhcpd.conf
"option domain-name "esiiab.es";
option domain-name-server 81.125.36.0;
option subnet-mask 255.255.255.0;
option routers 81.125.36.1;
option broadcast-address 81.125.36.255;
subnet 81.125.36.0 netmask 255.255.255.0}
range 81.125.36.11 81.125.36.255;
{
host dns}
hardware ethernet 00:00:00:00:00:10;
fixed-address 81.125.36.10;
{
host http}
hardware ethernet 00:00:00:00:00:03
fixed-address 81.125.36.03;
{
host r1}
hardware ethernet 00:00:00:00:00:01
fixed-address 81.125.36.1.;
{ "
↳/network
↳\interfaces
"auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 81.125.36.2
netmask 255.255.255.0
gateway 81.125.36.1 "
↳\resolv.conf
"domain esiiab.es
search esiiab.es
nameserver 81.125.36.10"

/dns.esiiab.es
↳/etc→/bind
↳\db.36.125.81 → IP al revés
" $TTL 86400
...

@	IN	NS	dns.esiiab.es.
1	IN	PTR	r1.esiiab.es.
2	IN	PTR	dhcp.esiiab.es.
3	IN	PTR	http.esiiab.es.
10	IN	PTR	dns.esiiab.es. "

Estaba igual

↳\db.esiiab.es
"$TTL 86400
...
@ IN NS dns.esiiab.es.
r1 IN A 81.125.36.1
...
dns IN A 81.125.36.10
www IN CNAME http.esiiab.es.
intranet IN CNAME http.esiiab.es."

↳\named.conf.local
"zone "esiiab.es"}
type master;
file "/etc/bind/db.esiiab.es";{;
zone "36.125.81.in-addr.arpa"}
type master;
file "/etc/bind/db.36.125.81";

↳\db.root
↳está igual

1º Configurar interfaces

2º WWW y PCs

NAT en el router frontera R1

inside ↙ ↳ Outside

3º IP route 0.000 0.0.0.0 "ip que me dan" (internet

4º Router frontera

↳ interface inside
" ip nat inside"

↳ interface outside
" ip nat outside"

Al router frontera se le asigna la ruta por defecto

IP route 0.0.00 0.0.0.0 "ip que me dan" (internet

5º. TCP en router frontera

ip nat inside source static tcp "ip privada" puerto "ip pública" puerto

6º Access list NAT → Do acceso internet sólo donde dejan

Static → 1 sola IP (no saldrá)

Demás rangos → * deny iría 1º → red que dejan → opuesto máscara

access-list 10 permit 192.168.1.0 0.0.0.255

Wildcard → muchos

Host → 1

Dinam → varios

7º NAT (NAPT pq 1 específico a ver fuera)

ip nat inside source list 10 interface fast Ethernet 011 overload

ip nat inside source static tcp 10.0.20.100 80 160.20.36.101. 80

10.0.20.100 → IP interna WWW

80 → puerto

160.20.36.101 → IP externa WWW

En cada router, router rip

network ip con comodín

passive-interface fastEth 010... (solo los que van a PCs o internet)

2) 148.23.8.0/21 148.23.56.0/21 148.23.64.0/21 148.23.72.0/21

I) 1 con 4000
II) 3 con 1000
III) 4 con 200

I

$2^{32-21}-2 = 2^{11}-2 = 2046$

$2^m - 2 \geq 4000$

$2^m \geq 4002$; $2^{12} \geq 4002$

New mask = 32-12 = 20

bits = 20-21 = -1

Mismos 20 bits

148.23.0000 1000.0
148.23.0011 1000.0
148.23.0100 0000.0
148.23.0100 1000.0

148.23.8.0/21 → 148.23.8.1 – 148.23.55.254
148.23.56.0/21 → 148.23.56.1 – 148.23.63.254
148.23.64.0/20 → 148.23.64.1 – 148.23.74.254 ✓ 4094

II) 3 con 1000

$2^m - 2 \geq 1000$

$2^m \geq 1002$

$2^{10} \geq 1002$

New mask = 32-10 = 22

bits = 22-21 = 1

IP Bin

148.23.0000 1000.0
148.23.0000 1100.0
148.23.0011 1000.0
148.23.0011 1100.0

Dir red/masc	Rango	Host
148.23.8.0/22	148.23.8.1 – 148.23.11.254	1022 ✓
148.23.12.0/22	148.23.12.1 – 148.23.15.254	1022 ✓
148.23.56.0/22	148.23.56.1 – 148.23.59.254	1022 ✓
148.23.60.0/22	148.23.60.1 – 148.23.63.254	1022 ✗

III) 4 con 200

$2^m - 2 \geq 200$

$2^m \geq 202$

$2^8 \geq 202$

New mask = 32-8 = 24

bits = 24-22 = 2

Host $(2^8-2) = 254$

IP Bin

148.23.0011 1100.0
148.23.0011 1101.0
148.23.0011 1110.0
148.23.0011 1111.0

Dir red/masc	Rango
148.23.60.0	... 60.1 – 60.254
148.23.61.0	... ...
148.23.62.0	... ...
148.23.63.0	

1) ISN = 0 — 1000 bytes — ¿Valor campo seq del 4º seg?

1. <0:0>, SEQ = 0, sync
2. <1:1000> seq = 1
3. <1001:2000> seq = 1001
4. <2001:3000> seq = 2001
5. <3001:4000> seq = 3001

ISN = 12300 — 2000 bytes — Valor campo ACK por reconocimiento del 2º segm.

<12300:12300>, seq = 12300, sync
<12301:14300>, seq = 14301
<14301:16300>, seq = 14301

3) ISN = 100, WIN = 20 (Servidor) — ISN = 0, WIN = 60 (Cliente)

Tam. máximo seg = 20 bytes. Servidor —100b datos→ Cliente

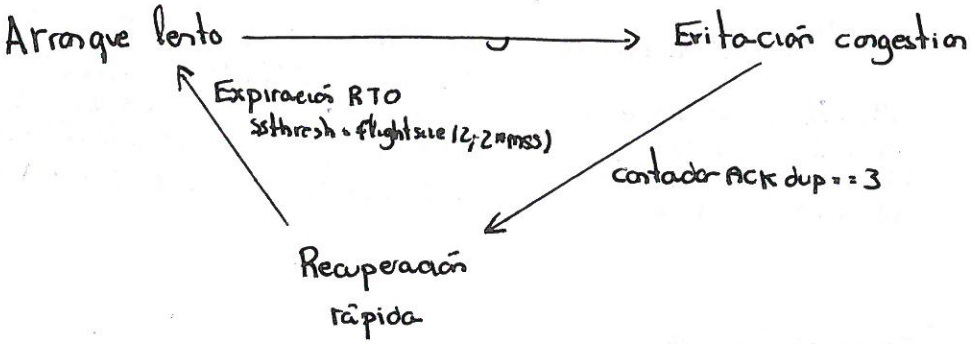
!! Segmentos necesarios = Datos/MSS = 100/20 = 5 segmentos

Sincroniza 1. <100:100>, seq = 100, sync

DATOS
2. <101:120>, seq 101,
3. <121:140>, seq 121
4. <141:160>, seq 141
5. <161:180>, seq = 161
6. <181:200>, seq = 181

De 101 a 200

FIN 7. <201:201>, seq = 201



De la 72 a la 85. Finaliza el proceso de recuperación?

Cuando se recibe un Ack mayor al punto de recuperación

Mayor nº de secuencia enviado por emisor antes de la retransmisión rápida. Después de 2 o 3 Ack repetidos?

Punto recup = Seq + lenght - 1

24617 + 1448 - 1 = 26064

Trama 44

54261 + 1448 - 1 = 55708

Trama 88

408337 + 1448 - 1 = 409784

Trama 528

1/ Solo VLSM

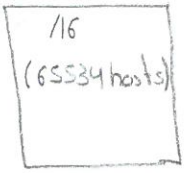
149.21.0.0/16

I) Tres clientes con 12.000 host

II/ Cuatro clientes con 1.800 host

III/ Ocho clientes con 700 host

Máscara de 16, $2^{32-16} - 2 = 65534$ hosts



I/ New mask for 12000 hosts

$2^m - 2 \geq 12000$

$2^m \geq 12002$

$2^{14} \geq 12002$

$m = 14 \rightarrow$ New mask = 32 − 14 = 18 bits

Nuevos bits: 18 − 16 = 2 bits

IP Bin	Dir. Red/máscara	Rango	Nº host
149.21. 0000 0000.0	149.21.0.0/18	149.21.0.1 – 149.21.63.254 ✓	16382
149.21. 0100 0000.0	149.21.64.0/18	149.21.64.1 – 149.21.127.254 ✓	16382
149.21. 1000 0000.0	149.21.128.0/18	149.21.128.1 – 149.21.191.254 ✓	16382
149.21. 1100 0000.0	149.21.192.0/18	149.21.192.1 – 149.21.255.254 ✗	

II) 149.21.192.0 libre, hosts de 1800

$2^m - 2 \geq 1800$

$2^m \geq 1802$

$2^{11} \geq 1802$

$m = 11$

Nueva máscara = 32 − 11 = 21 bits

Nuevos bits = 21 − 18 = 3

IP Bin	Dir red/máscara	Rango	Nº host
149.21. 1100 0000.0	149.21.192.0/21	149.21.192.1 – 149.21.199.254 ✓	2046
149.21. 1100 1000.0	149.21.200.0/21	149.21.200.1 – 149.21.207.254 ✓	2046
149.21. 1101 0000.0	149.21.208.0/21	149.21.208.1 – 149.21.215.254 ✓	2046
149.21. 1101 1000.0	149.21.216.0/21	149.21.216.1 – 149.21.223.254 ✓	...
149.21. 1110 0000.0	149.21.224.0	149.21.224.1 – 149.21.231.254	...
149.21. 1110 1000.0	149.21.232.0	149.21.232.1 – 149.21.239.254	...
149.21. 1111 0000.0	149.21.240.0	149.21.240.1 – 149.21.247.254	...
149.21. 1111 1000.0	149.21.248.0	149.21.248.1 – 149.21.255.254	

149.21.224.0 ↑ libres, host de 700

$2^m - 2 \geq 800$

$2^m \geq 802$

$2^{10} \geq 802$

Nueva_masc = 32 − 10 = 22

Nuevos bits = 22 − 21 = 1 bit

IP Bin	Dir red/masc	Rango	Nº host
149.22. 1110 0000.0	149.22.224.0/22	149.22.224.1 – 149.22.227.254	1022
149.22. 1110 0100.0	149.22.228.0/22	149.22.228.1 – 149.22.231.254	1022
149.22. 1110 1000.0	149.22.232.0/22	149.22.232.1 – 149.22.235.254	1022
149.22. 1110 1100.0	149.22.236.0	149.22.236.1 – 149.22.239.254	...
...	149.22.240.0	...	
...	149.22.244.0	...	
	149.22.248.0		
	149.22.252.0		

2) CIDR + VLSM

Puede asignar 193.31.24.0/23 , 193.31.32.0/23 , 193.31.34.0/23

I) 1 cliente con 1000 hosts 193.31.28.0/23

II) 3 clientes con 200 hosts

III) 4 clientes con 50 hosts

I) Cuántos host direccionables?

$2^{32-23} - 2 = 2^9 - 2 = 510$ hosts

Necesitamos agrupar

$2^m - 2 \geq 1000$

$2^m \geq 1002$ New mask = 32 - 10 = 22 bits

$2^{10} \geq 1002$ bits: 22 - 23 = -1 → Juntar por último bit diferente

	IP Bin	Dir. Red/másc	Rango	Hosts
	193.31.0001 1000.0	193.31.24.0/23	193.31.24.1 - 193.31.27.254	510
	193.31.0001 1100.0	193.31.28.0/23	193.31.28.1 - 193.31.31.254	510
Mismo 22 bits	193.31.0010 0000.0	193.31.32.0/22	193.31.32.1 - 193.31.35.254	1022
	193.31.0010 0010.0			

II) $2^m - 2 \geq 200$

$2^m \geq 202$ New mask = 32 - 8 = 24

$2^8 \geq 202$ bits = 24 - 23 = 1 bit

IP Bin	Dir Red/másc	Rango	Hosts
193.31.0001 1000.0	193.31.24.0/24	193.31.24.1 - 193.31.24.254	254 ✓
193.31.0001 1001.0	193.31.25.0/24	193.31.25.1 - 193.31.25.254	254 ✓
193.31.0001 1100.0	193.31.28.0/24	193.31.28.1 - 193.31.28.254	254 ✓
193.31.0001 1101.0	193.31.29.0/24	193.31.29.1 - 193.31.29.254	254 ✗

III) $2^m - 2 \geq 50$

$2^m \geq 52$ New mask = 32 - 6 = 26

$2^6 \geq 52$ bits = 26 - 24 = 2

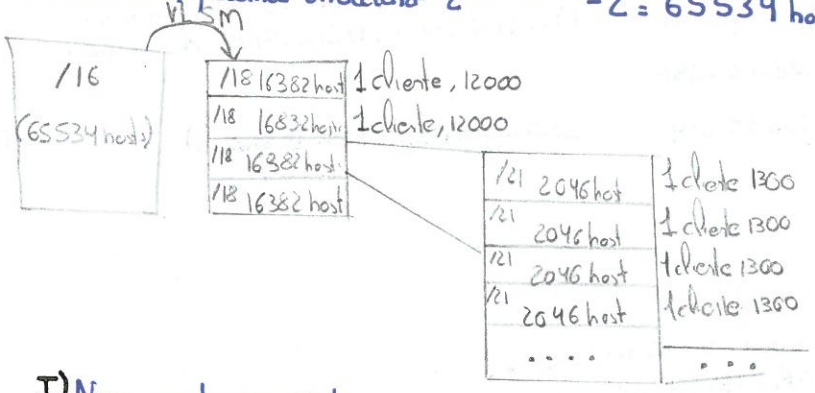
IP Bin	Dir Red/masc	Rango	Hosts
193.31.29.0000 0000	193.31.29.0/26	193.31.29.1 - 193.31.29.62 ✓	62
193.31.29.0100 0000	193.31.29.64/26	193.31.29.65 - 193.31.29.126 ✓	62
193.31.29.1000 0000	193.31.29.128/26	193.31.29.129 - 193.31.29.190 ✓	62
193.31.29.1100 0000	193.31.29.192/26	193.31.29.193 - 193.31.29.254 ✓	

2) Solo **VLSM.**

150.80.0.0/16

a) 2 clientes con 12.000 host cada uno
b) 4 clientes con 1.300 host cada uno
c) 8 clientes con 500 host cada uno

Máscara de 16, podemos direccionar $2^{32-16} = 16 - 2 = 65534$ hosts



I) New_mask, 12000 hosts

$2^m - 2 \geq 12000$ hosts

$2^m \geq 12.002$; $2^{14} \geq 12002$; $m = 14 \rightarrow$ New_mask = 32 - 14 = 18 bits

Nuevos bits máscara = n = new_mask - old_mask = 18 - 16 = 2 bits

IP en binario	Dir. Red/máscara	Rango Direccionable	Nº host	
150.80.0000 0000.0	150.80.0.0/18	150.80.0.1 - 150.80.63.254	16382	Asig ✓
150.80.0100 0000.0	150.80.64.0/18	150.80.64.1 - 150.80.127.254	16382	Asig ✓
150.80.1000 0000.0	150.80.128.0/18	150.80.128.1 - 150.80.191.254	16382	Asig ✗ ▭
150.80.1100 0000.0	150.80.192.0/18	150.80.192.1 - 150.80.255.254	16382	Asig ✗

II) 150.80.128.0 y 150.80.192.0, sin asignar (/18). Redes de 1300

$2^m - 2 \geq 1300$ hosts

$2^m \geq 1302$; $2^{11} \geq 1302$; $m = 11 \rightarrow$ New_mask = 32 - 11 = 21 bits

n = new_mask - old_mask = 21 - 18 = 3 bits

▭ 150.80.1000 0000.0	150.80.128.0/21	150.80.128.1 - 150.80.135.254	2046	Asig ✓
150.80.1000 1000.0	150.80.136.0/21	150.80.136.1 - 150.80.143.254	2046	Asig ✓
150.80.1001 0000.0	150.80.144.0/21	150.80.144.1 - 150.80.151.254	2046	Asig ✓
150.80.1001 1000.0	150.80.152.0	150.80.152.1 - 150.80.159.254	2046	Asig ✓
150.80.10100000.0	150.80.160.0	150.80.160.1 - 150.80.167.254	2046	Asig ✗ ▭

III) 150.80.160.0.... Redes de

$2^m - 2 \geq 500$ hosts

$2^m \geq 502$; $2^9 \geq 502$; $m = 9 \rightarrow$ New_mask = 32 - 9 = 23 bits

n = new_mask - old_mask = 23 - 21 = 2 → we need 2 bits

150.80.10100 00 0.0 ...

... ...

Redes II.

Tema 2.1. Direccionamiento IP

→ Clases

- Clase A 1.0.0.0 a 126.0.0.0
- Clase B 128.0.0.0 a 191.255.0.0
- Clase C 192.0.0.0 a 223.255.255.0
- Multicast 224.0.0.0 a 239.255.255.255 (reservadas)
- Clase E 240.0.0.0 a 255.255.255.254

10.0.0.0 Red privada
172.16.0.0 - 172.31.0.0 Red privada
192.168.0.0 - 192.168.255.0 Red privada
255.255.255.255 - Broadcast

1ª Evolución, las subredes

Ventajas
- Facil de encaminar
- sencillez de tablas en routers

Desventajas
- Disminución de rendimiento
- Dificultad de administración

Solución, subnetting → aparece la máscara

¿Crear subnetting?
1. Ver que las subredes a crear se pueden direccionar con el rango del host.
2. Ampliar máscara de red inicial $2^n - 2 >=$ nº subredes nuevas
3. Asignación de las nuevas dir. de subred
4. Calculo del rango del host de las nuevas subredes $2^m - 2$

1) Clase C 203.12.16.0 en 4 subredes de 30 hosts → $2^5 = 32$

Binario	Subred/máscara	Rango host
203.12.16.000x xxxx	203.12.16.0/27	
203.12.16.001x xxxx	203.12.16.32/27	203.12.16.33 - 203.12.16.62
203.12.16.010x xxxx	203.12.16.64/27	203.12.16.65 - 203.12.16.94
203.12.16.011x xxxx	203.12.16.96/27	203.12.16.97 - 203.12.16.126
203.12.16.100x xxxx	203.12.16.128/27	203.12.16.129 - 203.12.16.158
203.12.16.101x xxxx	203.12.16.160/27	...

} 4 subredes

2ª Evolución, VLSM (Variable Length Subnet Mask)

Desventaja
- Todas las subredes del mismo tamaño

Sol. ⇒ Distintas máscaras según el tamaño de subredes

Técnica VLSM ⇒ Aplicar reasignamiento subnetting, primero las grandes y luego peques

Evolución final, CIDR (Classless InterDomain Routing)

Problema actual
- Solo quedan dir. de red de clase C.

Sol. ⇒ Eliminamos las clases ⇒ Si queremos redes más grandes, agrupamos redes consecutivas, máscara menor

Si queremos redes más pequeños, usamos VLSM, máscara mayor

5/ 143.57.0.0

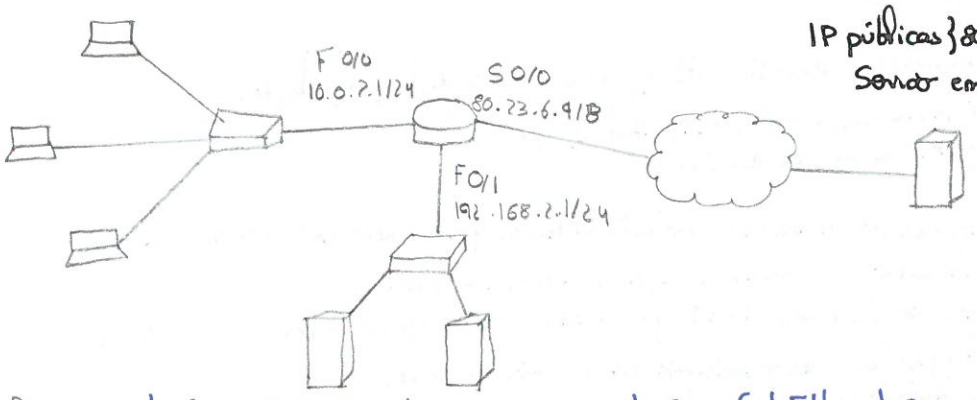
Class B

Class Mask: 255.255.0.0

Subnet mask: 256 : 64 = 4 => 255.255.252.0

32 subnets, pero oooo guuu no, asi que necesito 34 => 64

Dinámico



IP públicas {80.23.6.100, 80.23.6.110}
Servidor email TCP 25 y 110

ROUTERS
IP

interface fastEthernet 0/0
ip address 10.0.2.1 255.255.255.0
ip nat inside
no shutdown
exit

interface fastEthernet 0/1
ip address 192.168.2.1 255.255.255.0
ip nat inside
no shutdown
exit

interface serial 0/0
ip address 80.23.6.9 255.0.0.0
ip nat outside
no shutdown
exit

ip route 0.0.0.0 0.0.0.0 80.0.0.1

ACL
access-list 75 permit 10.0.2.0 0.0.0.255
exit

POOL
ip nat pool net-80 80.26.6.100 80.26.6.110 netmask 255.0.0.0
exit

NAT DINAMICO
ip nat inside source list 75 pool net-80

NAT ESTATICO
ip nat inside source static tcp 192.168.2.2 80 80.23.6.9 80

Servidor email
ip nat inside source static tcp 192.168.2.3 25 80.23.6.9 25
ip nat inside source static tcp 192.168.2.3 110 80.23.6.9 110

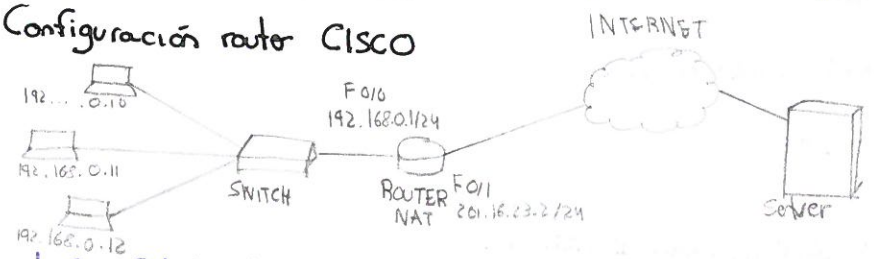
Tema 2.4. NAT y NAPT. Configuración

- NAT (Network Address Translation) Modificar IPs que viajan dentro de los paquetes IP. Para IP privadas acceder a internet. Actua en el router (frontera), que
  - → Inside network: Redes sujetas a una traducción
  - → Outside network:
- NAT Dinámico: Las traducciones no existen en la tabla NAT hasta que la inside network no comunica con el router, siendo así unidireccional. Al establecer comunicación, se vuelve bidireccional.
- NAT Estático: Las traducciones de la tabla NAT ya existen desde que se configura y solo se borrará con comandos. Para ser accesible por la outside network en cualquier momento
- NAPT: Permite a numerosas host de la inside network compartir una unica dirección de la outside

NAT y NAPT se pueden usar a la vez

Para este proceso hay que recuentas IP globales hay disponibles, cuidar el acceso de la outside en el NAT estático y valorar que no todas las aplicaciones no soportan en NAT

Configuración router CISCO



interface fastEthernet 0/0
ip address 192.168.0.1 255.255.255.0
ip nat inside
no shutdown
exit

interface fastEthernet 0/1
ip address 201.16.23.2 255.255.255.0
ip nat outside
no shutdown
exit

Estático

A
C
L → IP 192.168.0.11 para NAT estático
→ Toda la red 192.168.0.0/24 para NAT dinámico

access-list 10 deny host 192.168.0.11
access-list 10 permit 192.168.0.0 0.0.0.255
exit

Relación entre ambas

Pool: Conjunto (rango) de direcciones IP públicas sobre las que se traducirán las IPs privadas

→ Red local excepto 192.168.0.11 } 201.16.23.20, 201.16.23.25 } de la red 201.16.23.25/24

configure terminal
ip nat pool red-ejemplo 201.16.23.20 201.16.23.25 netmask 255.255.253.0

ip nat inside source list 10 pool red-ejemplo

Reglas de traducción

ip nat inside source list 89 interface fast Ethernet 0/1 overload
exit

Subnetting

VLSM = New mask = 32 - m

$2^m - 2 \geq X$

bits = old Mask - New mask = *Bits que puedo modificar

CIDR =
Si en bits ≤ 0, busco en la máscara - ese bit cuales son iguales y agrupo

Tabla de encaminamiento

- Conectados al Router. Internet solo núm máscara Ej ⇒ 180.2.32.31/8 ⇒ 180.0.0.0
  "." "." "." / " eth" ". ". ".1
- Ruta por defecto 0.0.0.0 /0 eth0 *IP Internet*

Un router guarda información sobre las máscaras para el router siguiente, pero no para dos, tres...
↓
si se juntan, masc - 1

Analisis protocolo ICMP

1. Busco paquete e identificación (...)
2. Poner ip.id ==
3. Ver el TTL del nuevo y:
   TTL - 1 si host inalcanzable, sino igual

Si la IP acaba en .1 o .2 es un router

→ Segunda parte

- Ping previo

1	2	ICMP Request		
2	1	ICMP Reply		

Fijarse en las máscaras

- Sin ping previo

1	F	ARP Request	-	-
A	1			
1	A	ARP Reply	-	-
A	1	ICMP Request		Tarea 2
		ICMP Reply	Tarea 2	

Analisis protocolo TCP