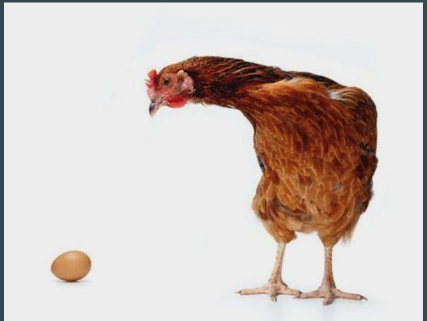
Midterm

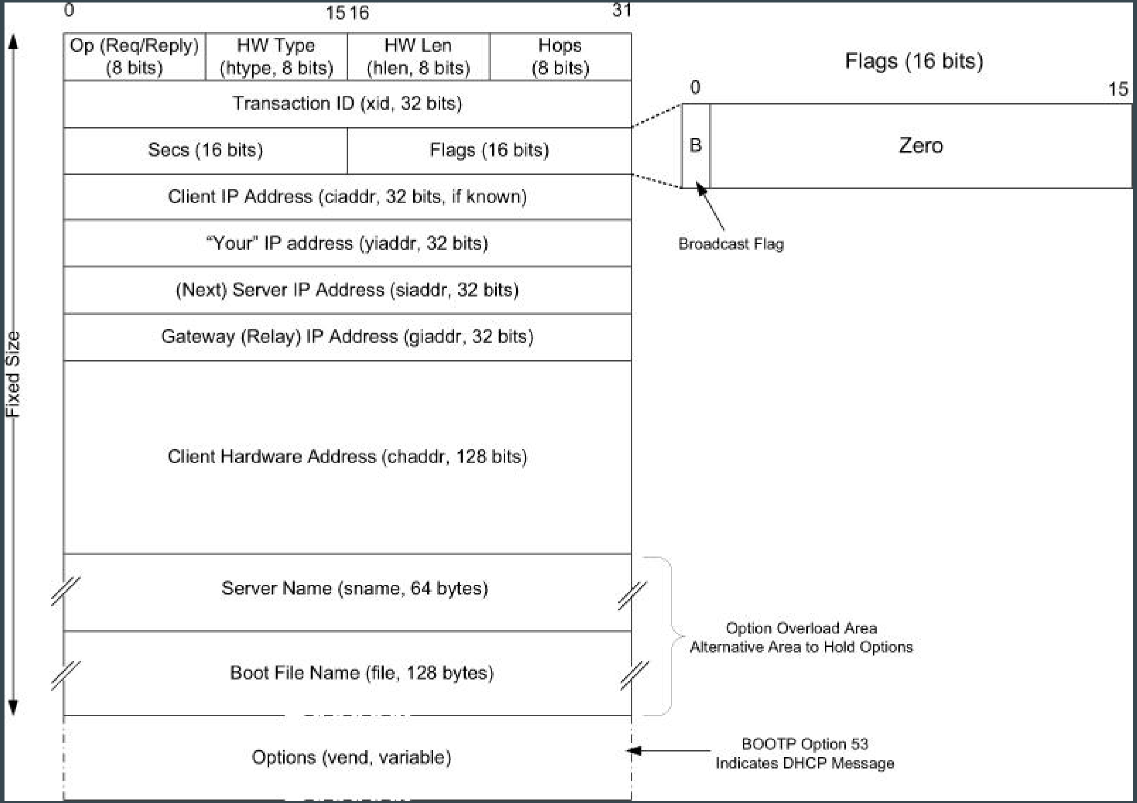
Is Fri, June 24, 8:30am a good time?

- Class reps please let me know soon.

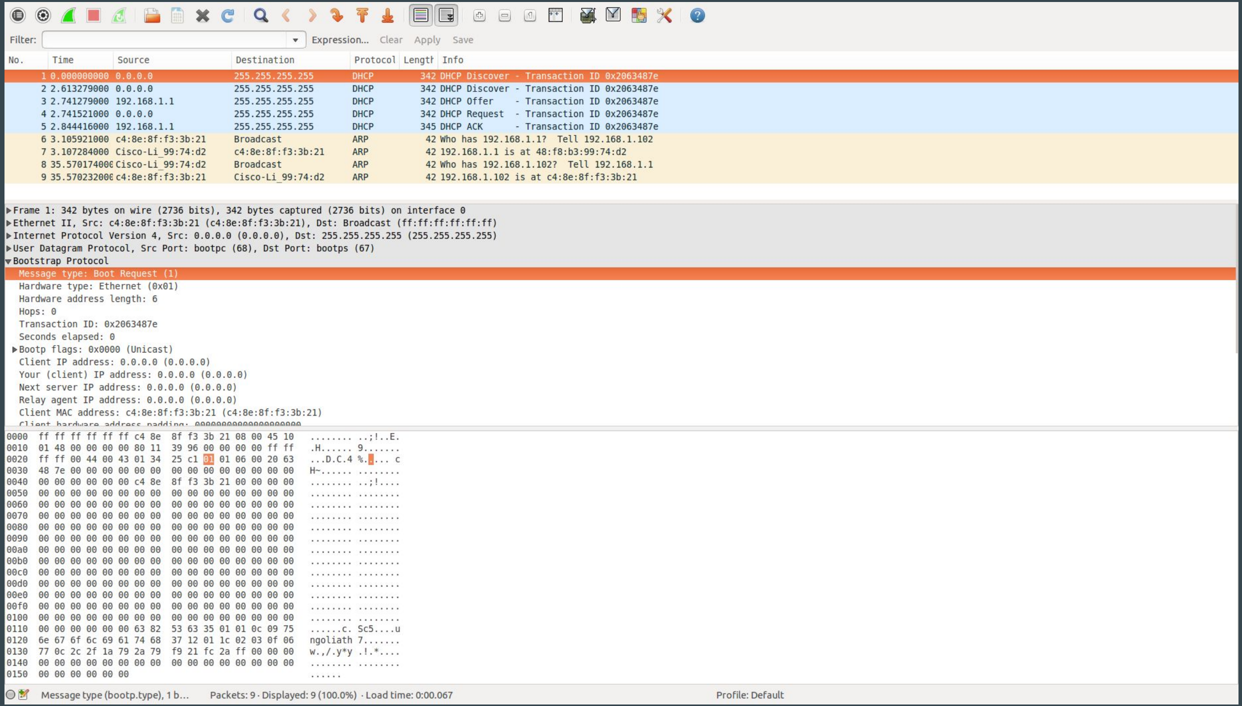
DHCP

- Dynamic Host Configuration Protocol
- Evolved from BOOTP
- “Chicken and egg” problem: how do you speak IP and acquire:
  - an IP address
  - a “default” gateway - router to the Internet
  - a nameserver
  - …




0
15 16
31
Fixed Size
Op (Req/Reply) (8 bits)
HW Type (htype, 8 bits)
HW Len (hlen, 8 bits)
Hops (8 bits)
Transaction ID (xid, 32 bits)
Secs (16 bits)
Flags (16 bits)
Client IP Address (ciaddr, 32 bits, if known)
"Your" IP address (yiaddr, 32 bits)
(Next) Server IP Address (siaddr, 32 bits)
Gateway (Relay) IP Address (giaddr, 32 bits)
Client Hardware Address (chaddr, 128 bits)
Server Name (sname, 64 bytes)
Boot File Name (file, 128 bytes)
Options (vend, variable)
Flags (16 bits)
0
15
B
Zero
Broadcast Flag
Option Overload Area
Alternative Area to Hold Options
BOOTP Option 53
Indicates DHCP Message

Wireshark capture



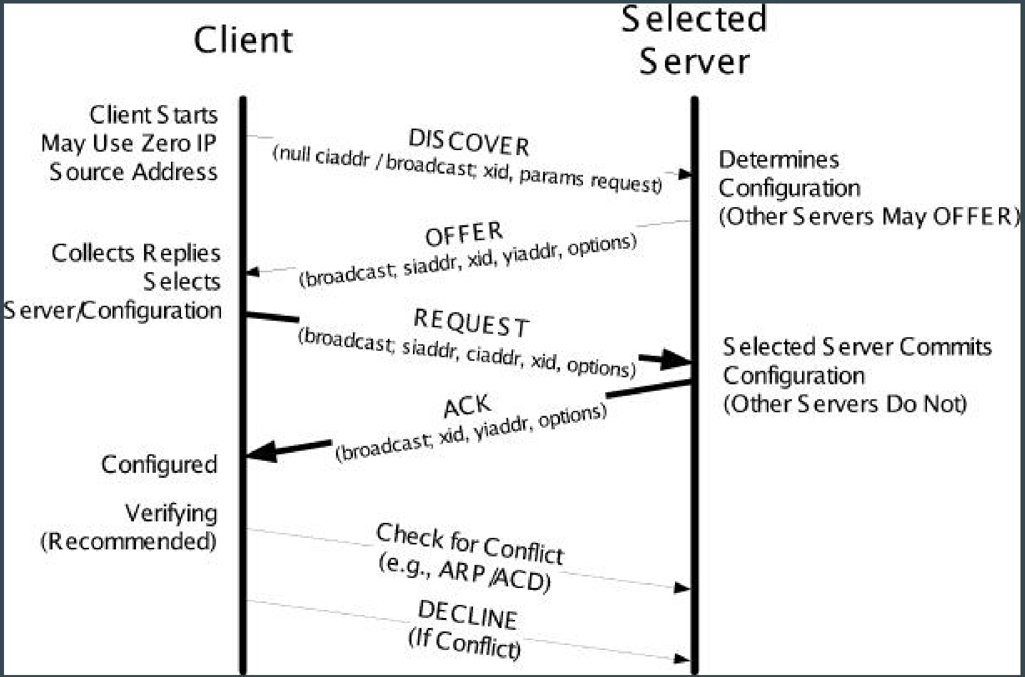
```
No.     Time         Source             Destination        Protocol Lengtł Info
      1 0.000000000  0.0.0.0            255.255.255.255    DHCP        342 DHCP Discover - Transaction ID 0x2063487e
      2 2.613279000  0.0.0.0            255.255.255.255    DHCP        342 DHCP Discover - Transaction ID 0x2063487e
      3 2.741279000  192.168.1.1        255.255.255.255    DHCP        342 DHCP Offer    - Transaction ID 0x2063487e
      4 2.741521000  0.0.0.0            255.255.255.255    DHCP        342 DHCP Request  - Transaction ID 0x2063487e
      5 2.844416000  192.168.1.1        255.255.255.255    DHCP        345 DHCP ACK      - Transaction ID 0x2063487e
      6 3.105921000  c4:8e:8f:f3:3b:21  Broadcast          ARP          42 Who has 192.168.1.1?  Tell 192.168.1.102
      7 3.107284000  Cisco-Li_99:74:d2  c4:8e:8f:f3:3b:21  ARP          42 192.168.1.1 is at 48:f8:b3:99:74:d2
      8 35.57017400€ Cisco-Li_99:74:d2  Broadcast          ARP          42 Who has 192.168.1.102?  Tell 192.168.1.1
      9 35.57023200€ c4:8e:8f:f3:3b:21  Cisco-Li_99:74:d2  ARP          42 192.168.1.102 is at c4:8e:8f:f3:3b:21
```

```
▶Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶Ethernet II, Src: c4:8e:8f:f3:3b:21 (c4:8e:8f:f3:3b:21), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▶User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▼Bootstrap Protocol
   Message type: Boot Request (1)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0x2063487e
   Seconds elapsed: 0
  ▶Bootp flags: 0x0000 (Unicast)
   Client IP address: 0.0.0.0 (0.0.0.0)
   Your (client) IP address: 0.0.0.0 (0.0.0.0)
   Next server IP address: 0.0.0.0 (0.0.0.0)
   Relay agent IP address: 0.0.0.0 (0.0.0.0)
   Client MAC address: c4:8e:8f:f3:3b:21 (c4:8e:8f:f3:3b:21)
   Client hardware address padding: 00000000000000000000
```

```
0000  ff ff ff ff ff ff c4 8e  8f f3 3b 21 08 00 45 10   ........ ..;!..E.
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   .H...... 9.......
0020  ff ff 00 44 00 43 01 34  25 c1 01 01 06 00 20 63   ...D.C.4 %..... c
0030  48 7e 00 00 00 00 00 00  00 00 00 00 00 00 00 00   H~...... ........
0040  00 00 00 00 00 00 c4 8e  8f f3 3b 21 00 00 00 00   ........ ..;!....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 0c 09 75   ......c. Sc5....u
0120  6e 67 6f 6c 69 61 74 68  37 12 01 1c 02 03 0f 06   ngoliath 7.......
0130  77 0c 2c 2f 1a 79 2a 79  f9 21 fc 2a ff 00 00 00   w.,/.y*y .!.*....
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0150  00 00 00 00 00 00                                  ......
```

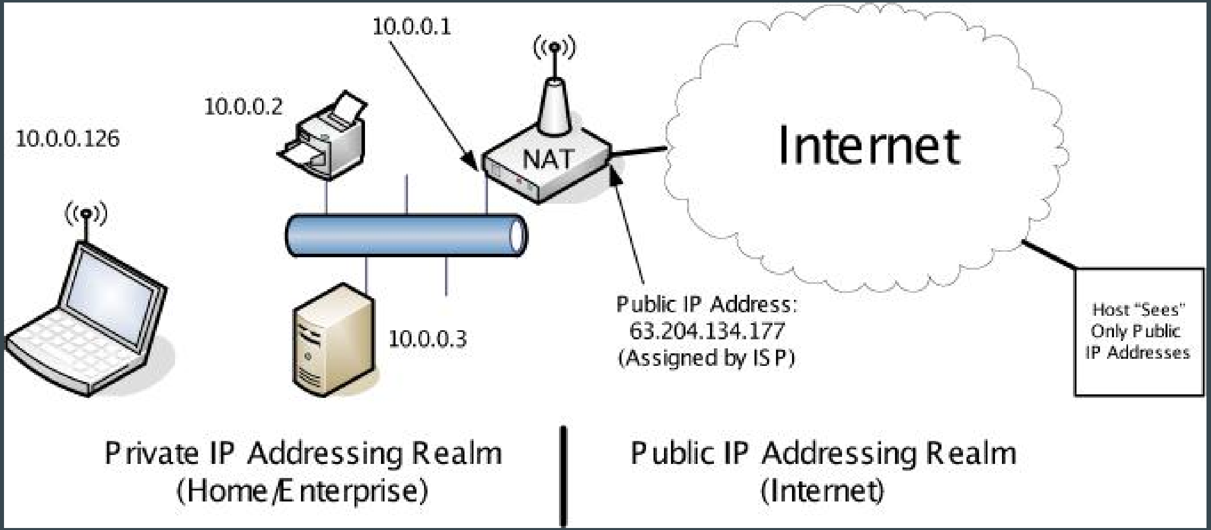
Message type (bootp.type), 1 b... Packets: 9 · Displayed: 9 (100.0%) · Load time: 0:00.067 Profile: Default

Typical exchange

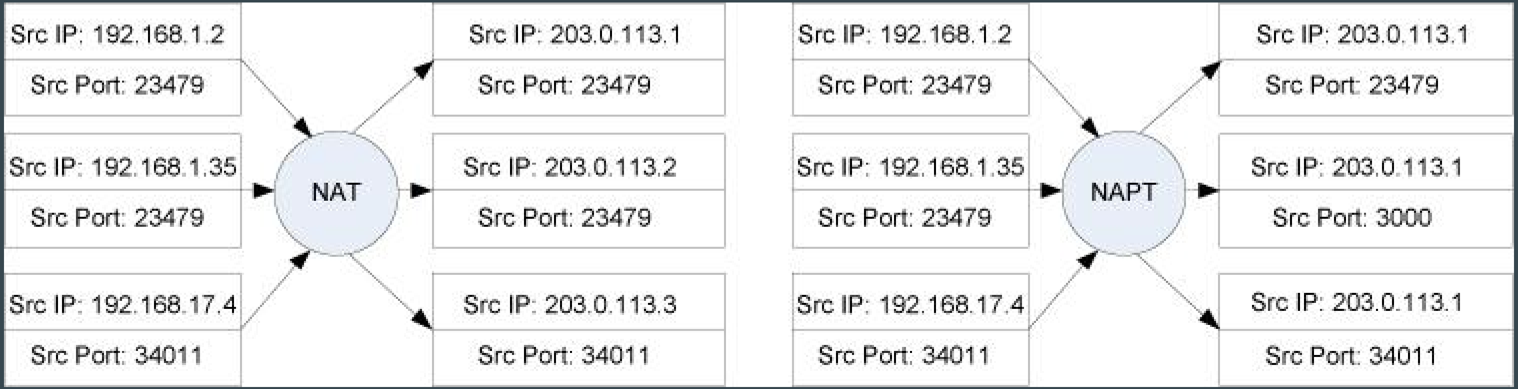


NAT

- Network Address Translation



Basic NAT & NAPT (NA Port T)



Src IP: 192.168.1.2 Src Port: 23479	NAT	Src IP: 203.0.113.1 Src Port: 23479	
Src IP: 192.168.1.35 Src Port: 23479		Src IP: 203.0.113.2 Src Port: 23479	
Src IP: 192.168.17.4 Src Port: 34011		Src IP: 203.0.113.3 Src Port: 34011	

Src IP: 192.168.1.2 Src Port: 23479	NAPT	Src IP: 203.0.113.1 Src Port: 23479	
Src IP: 192.168.1.35 Src Port: 23479		Src IP: 203.0.113.1 Src Port: 3000	
Src IP: 192.168.17.4 Src Port: 34011		Src IP: 203.0.113.1 Src Port: 34011	

Basic NAT

- Rewrite IP addresses only
- Available # publicly routable addresses ≥ # internal hosts

NAPT

- Use IDs from higher-layer than IP to mux/demux
    - UDP/TCP port #s
    - ICMP query ID
    - …
- Private IP address ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16

NAPT + TCP

- Will discuss later, once we introduce TCP
- Broadly, NAPT device has to detect:
  - Connection-setup and teardown
  - Every TCP segment that corresponds to connection

NAPT + UDP

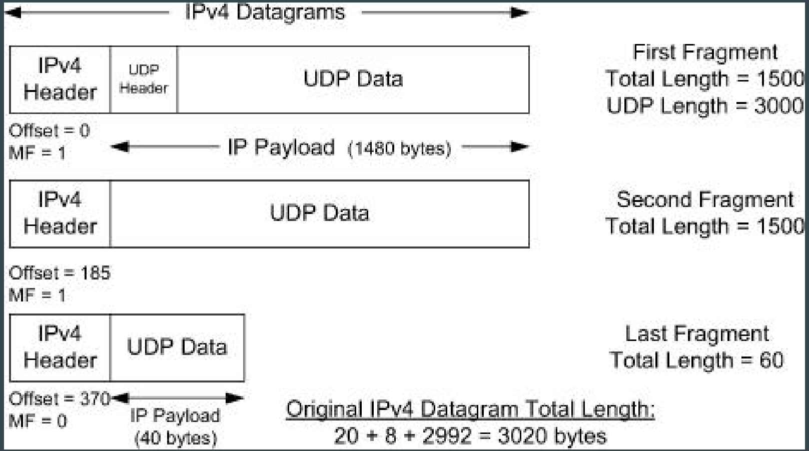
- Potential challenges
  - No notion of connection in UDP
    - Adopt notion of a “session.” Guess when it starts, timer for when it ends.
  - Session identified by two-tuple only. Not 4-tuple as in TCP
    - *Port-preservation*:
      - Retain port # chosen by internal host
      - Use that as index to table to determine internal host for packets received from outside
      - Discussed more in a couple of slides in the context of translation “behaviour.”

NAPT + UDP, mapping timer

- 1 timer per UDP session
- Expiry time: ≥ 2 min, recommended: 5 min.
- “Refresh behaviour” - when is timer reset
    - Required to be true for outgoing packets

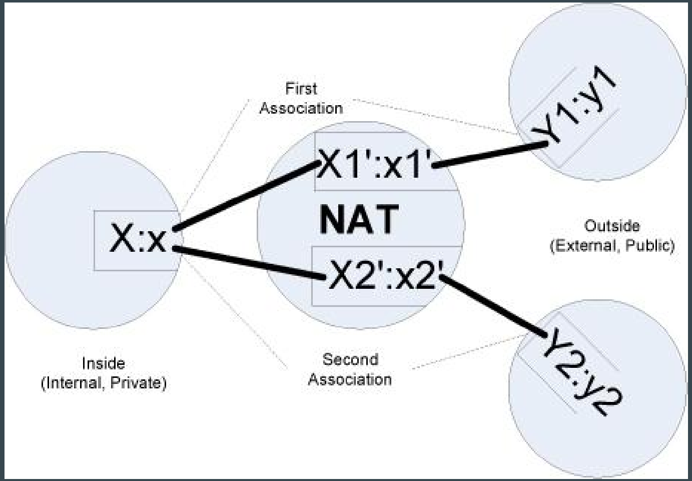
NAPT + UDP + IP Fragmentation

- Fragmentation cannot coexist with NAPT
  - UDP header not available for later fragments to be mapped

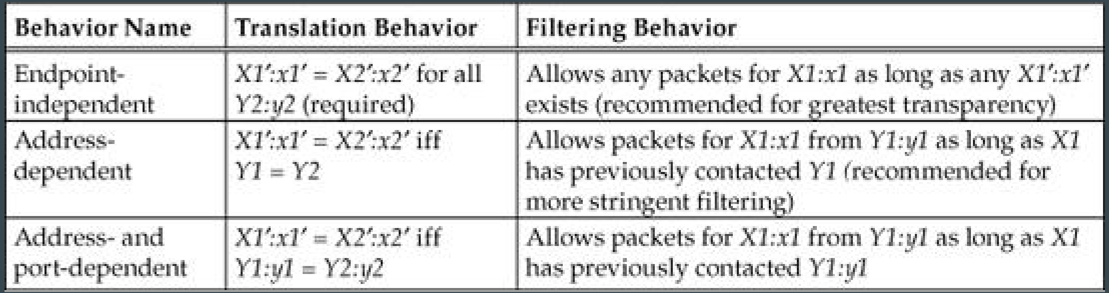


Translation “behaviour”

What source-ip, source-port should be in packet that exits to Internet?



Translation behaviour, contd.



Behavior Name	Translation Behavior	Filtering Behavior
Endpoint-independent	$X1':x1' = X2':x2'$ for all $Y2:y2$ (required)	Allows any packets for $X1:x1$ as long as any $X1':x1'$ exists (recommended for greatest transparency)
Address-dependent	$X1':x1' = X2':x2'$ iff $Y1 = Y2$	Allows packets for $X1:x1$ from $Y1:y1$ as long as $X1$ has previously contacted $Y1$ (recommended for more stringent filtering)
Address- and port-dependent	$X1':x1' = X2':x2'$ iff $Y1:y1 = Y2:y2$	Allows packets for $X1:x1$ from $Y1:y1$ as long as $X1$ has previously contacted $Y1:y1$

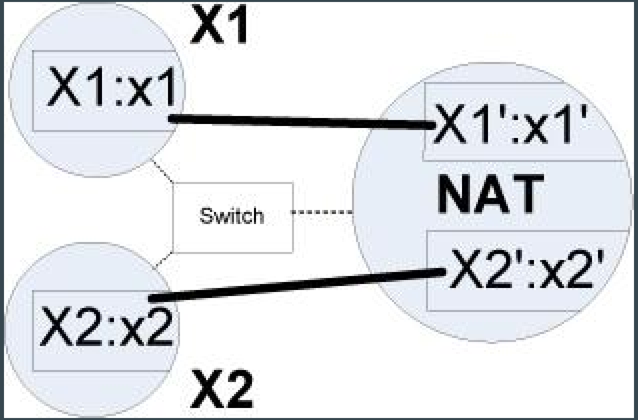
- Required behaviour for TCP/UDP: endpoint-independent.

Other issues

- Pairing
  - Internal host A establishes several connections/sessions
  - Should all be associated with the same public IP address?
  - ‘Yes’ answer (i.e., “pairing”) is recommended
- Port-preservation
- Port-parity
  - Even numbered internal port mapped to even numbered externally-visible port

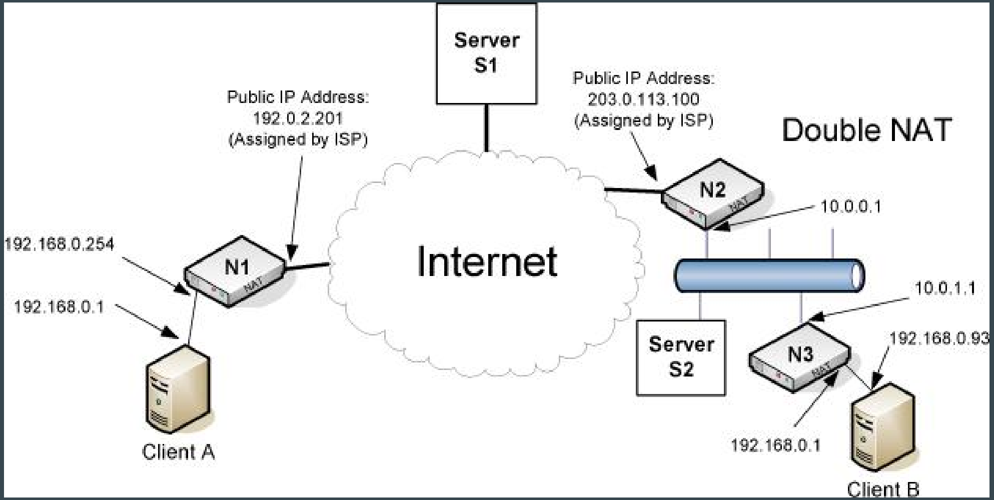
More issues - hairpinning

- When we run a server within NAT-ed network...
- In example below, should X2:x2 see as source, X1:x1 or X1’:x1’?



Hole-punching

- Two clients use server to discover and communicate directly with one another


Server S1
Public IP Address: 192.0.2.201 (Assigned by ISP)
Public IP Address: 203.0.113.100 (Assigned by ISP)
Double NAT
N2
NAT
10.0.0.1
192.168.0.254
N1
NAT
Internet
192.168.0.1
10.0.1.1
Server S2
N3
NAT
192.168.0.93
Client A
192.168.0.1
Client B