Connecting

G54ACC

Lecture 12

richard.mortier@nottingham.ac.uk

Contents

- Internet Quality of Service
- Network Address Translation
- End-to-End

Contents

- Internet Quality of Service
  - Type of Service, ToS
  - Differentiated Services, DiffServ
  - Integrated Services, IntServ
  - Problems
- Network Address Translation
- End-to-End

Quality of Service

- What do you do when capacity < demand?
  - If capacity > demand, no need for QoS
- Wish to keep queuing minimal
  - As queuing directly impacts latency, jitter, loss
  - At least, in a stable network (cf. dynamic routing)
  - How?
- Retrofitted to the Internet
  - Not especially widely used
  - Inelastic *vs*. Elastic traffic: higher layer responses

IP Type of Service, ToS

- Single IP header byte
- Precedence
  - For “special” traffic
- Service class
  - How to treat traffic
- But what do they *mean*?!
  - To the network?
  - To an application?

```
Bits 0-2:  Precedence.
Bit    3:  0 = Normal Delay,       1 = Low Delay.
Bits   4:  0 = Normal Throughput,  1 = High Throughput.
Bits   5:  0 = Normal Reliability, 1 = High Reliability.
Bit  6-7:  Reserved for Future Use.

0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
|                 |     |     |     |     |     |
|   PRECEDENCE    |  D  |  T  |  R  |  0  |  0  |
|                 |     |     |     |     |     |
+-----+-----+-----+-----+-----+-----+-----+-----+

Precedence

111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 – Flash
010 – Immediate
001 – Priority
000 - Routine
```

Differentiated Services, DiffServ

- Operates on *traffic aggregates*
  - Label packets with desired service class via ToS
  - Routers apply queuing as operator sees fit
- Four service classes, or *per-hop behaviours*
  - Default: best effort
  - Expedited Forwarding: low delay, loss, jitter
  - Assured Forwarding: low loss provided within rate
  - Class Selector: use ToS precedence bits

Integrated Services, IntServ

- Very similar to ATM in many respects
  - Operates on explicitly signalled *flows*
  - Flow setup specifies some QoS
  - Routers perform <u>C</u>onnection <u>A</u>dmission <u>C</u>ontrol
- Many similar problems
  - Per-flow state
  - What QoS should be requested?
  - Service level agreements, accounting, billing

Problems

- IntServ
  - Complexity
  - Mapping requirements to parameters, cf. ATM
  - Per-flow state
- DiffServ
  - End-to-end semantics
  - Mapping to service level agreement
  - Mapping to application demands

Contents

- Internet Quality of Service
- Network Address Translation
  - Address Shortages
  - Implementation
  - Full Cone/Restricted Cone/Symmetric
  - NAT Traversal
- End-to-End

Address Shortages

- IPv4 supports 32 bit addresses
  - 95% allocated already (300,000 netblocks)
  - June 2011 (global), Feb 2012 (regional) zero-day
  - ...yet #connected devices is exploding
- IPv6 supports 128 bit addresses
  - So not a problem?
  - ...except for the routing protocols
  - ...and all the associated services needing to move

Network Address Translation

- Private Addressing, RFC1918
  - 172.16/12, 192.168/16, 10/8
  - Should never be externally routed
  - Not a security mechanism!
- Traditional NAT, RFC3022; see also RFC2663
  - Use private addresses internally
  - Map into a (small) set of routable addresses
  - Use source ports to distinguish connections

Implementation

- Requires IP, TCP/UDP header rewriting
  - Addresses, ports, checksums at least
- Behaviours
  - Network Address Translation
  - Network Address and Port Translation
- Types
  - Full Cone
  - Address/Port Restricted Cone
  - Symmetric

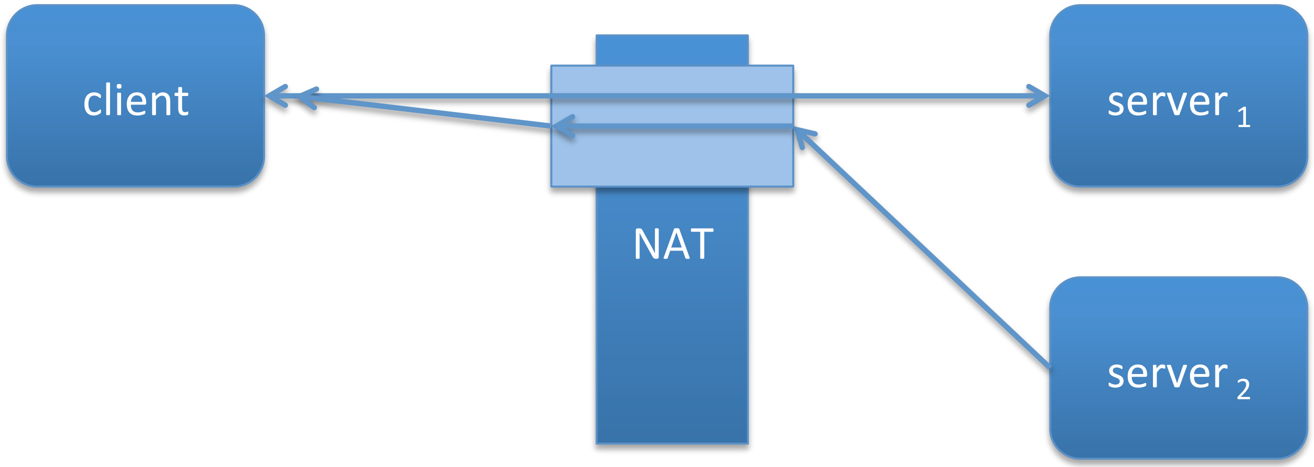
Full Cone NAT

(ia:ip → ea:ep) → da:dp

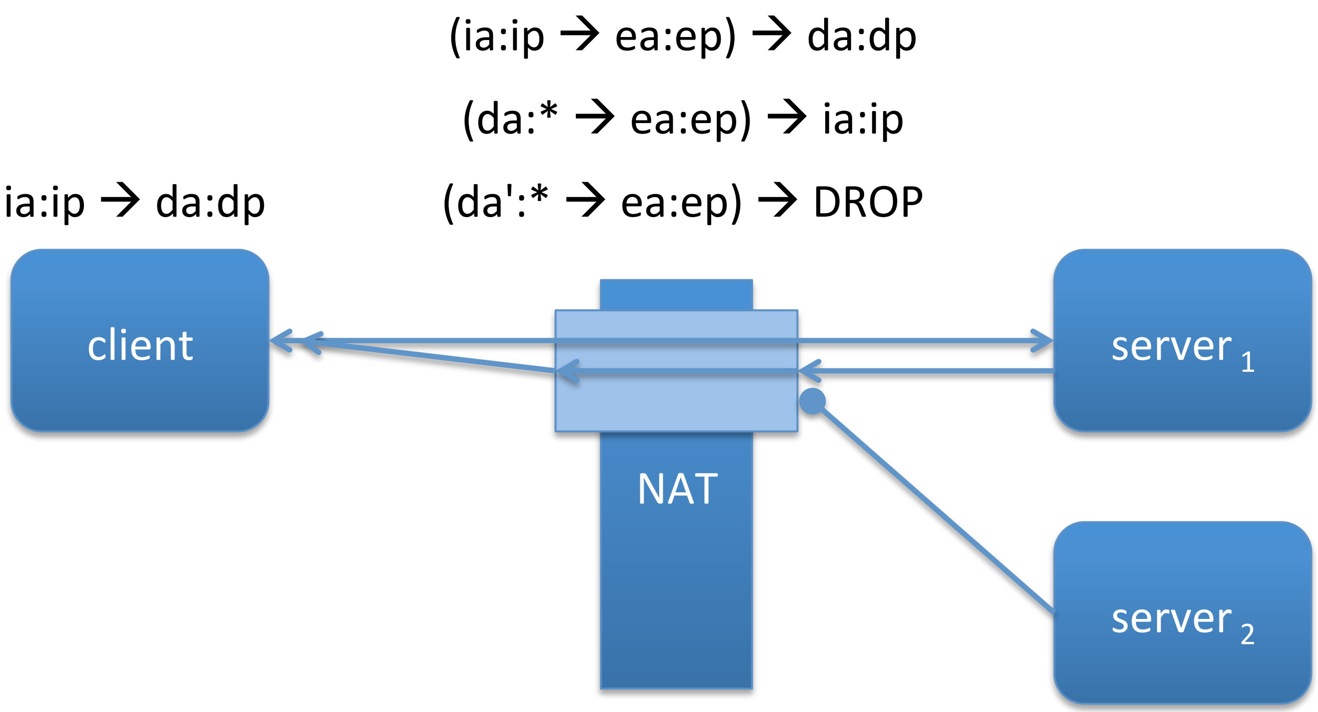
(da:* → ea:ep) → ia:ip

ia:ip → da:dp

(da':* → ea:ep) → ia:ip



(Address) Restricted Cone NAT



Port Restricted Cone NAT

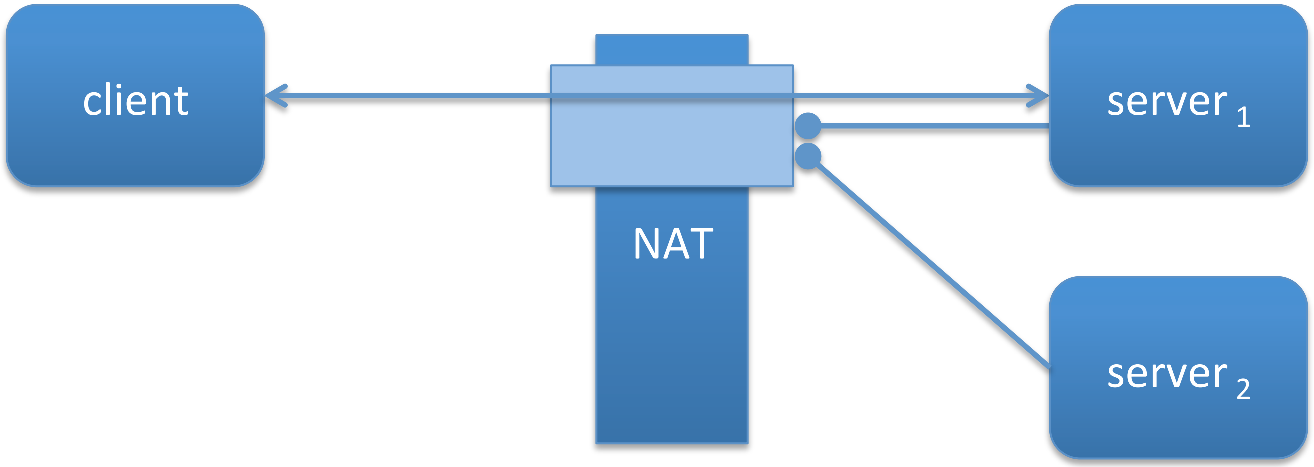
(ia:ip → ea:ep) → da:dp

(da:dp → ea:ep) → ia:ip

(da:dp’ → ea:ep) → DROP

ia:ip → da:dp

(da’:* → ea:ep) → DROP



Symmetric NAT

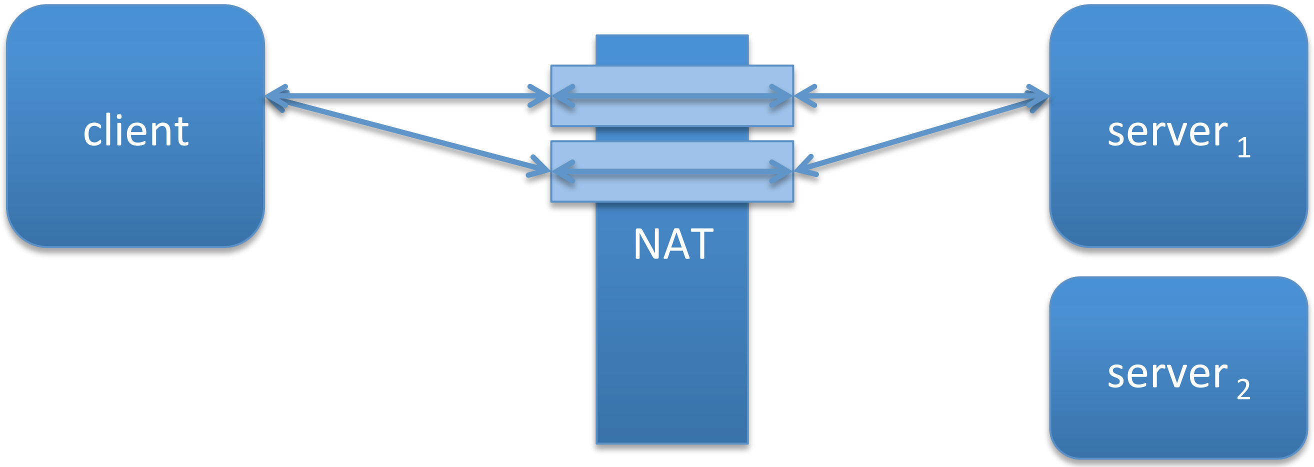
(ia:ip → ea:ep) → da:dp

(da:dp → ea:ep) → ia:ip

(ia:ip → ea':ep') → da:dp

(da:dp → ea':ep') → ia:ip

ia:ip → da:dp



ICE, STUN

- Session Traversal Utilities for NAT, RFC5389
  - Client attempts to characterise NAT behaviour using a third-party server "on the outside"
- Interactive Connectivity Establishment, RFC5245
  - Commonly used with SIP, SDP (for voice-on-IP)
    - In general, "offer/answer" protocols
  - Uses STUN (or TURN or ...) to determine and select from set of "candidate transport addresses"
  - Selected addresses are then propagated and used

Contents

- Internet Quality of Service
- Network Address Translation
- End-to-End
  - Middleboxes
  - Layer Violation
  - Impact on Extension

End-to-end Argument

- Salzer *et al*. "End-to-End Arguments in System Design". ACM Transactions on Computer Systems, 2(4), pages 277-288, 1984.
  - Earlier version in 1981
- Functions whose implementation requires application involvement should not be provided at lower layers
  - Unless partial implementation helps performance

Middleboxes

- A NAT is an example of a (transparent) middlebox
- There are others
  - Firewalls
  - Proxies
  - Caches
- They often provide very useful services
- But can be a complete pain
  - Buggy, unreliable
  - Incomplete protocol support (ICMP, &c.)

Layer Violation

- Information leaking from one layer to another
  – Generally considered poor form
  – Sometimes useful for features or performance
- NAT often causes this to explode
  – E.g., addresses (ab)used as host identifiers
    - They're not, they're addresses for routing to interfaces
    - But cf. pseudo-header
  – Also IP fragmentation, some options, some ICMP
  – And both ends may be NATted

“Is it still possible to extend TCP?”

Keio et al, ACM Internet Measurement Conference (IMC) 2011

- At least 25% of paths interfered with TCP
  - Beyond basic firewalling
- Option negotiation is required during handshake
  - But can be removed from SYN/ACK, so client doesn’t know
- Proxies are common, particularly on port 80
  - Proxies will remove options
- Segments may be both split and coalesced
  - Can’t assume sequence numbers are unmodified
  - Can’t assume message boundaries are preserved

Contents

- Internet Quality of Service
  - Type of Service, ToS
  - Differentiated Services, DiffServ
  - Integrated Services, IntServ
  - Problems
- Network Address Translation
  - Address Shortages
  - Implementation
  - Full Cone/Restricted Cone/Symmetric
  - NAT Traversal
- Middleboxes
  - End-to-end Argument
  - Layer Violation
  - Impact on Extension

Summary

- Quality of Service
- Features introduced to manage the changing environment
  – E.g., address shortages
- Dealing with NAT
  – The law of *unintended consequences*
- The end-to-end argument is an *argument*!

Quiz

1. Compare the QoS capability provided by IntServ to that of ATM – how are they similar, how are they different?
2. What is the difference between *elastic* and *inelastic* traffic?
3. How is DiffServ an evolution of the original IP ToS byte?
4. What are some of the problems of deploying DiffServ in a commercial Internet?
5. You are using a computer with the IPv4 address 192.168.0.2. You connect to a website at 128.232.0.10 through your home router which has the internal address 192.168.0.1. Draw a picture showing these three entities, and describe which incoming traffic is permitted and denied if your home router implements each of the four types of NAT given on slide 12.