CS 372 Lecture #32

IP Network Address Translation (NAT)

- implementation
- issues

Note: Many of the lecture slides are based on presentations that accompany *Computer Networking: A Top Down Approach,* 6th edition, by Jim Kurose & Keith Ross, Addison-Wesley, 2013.

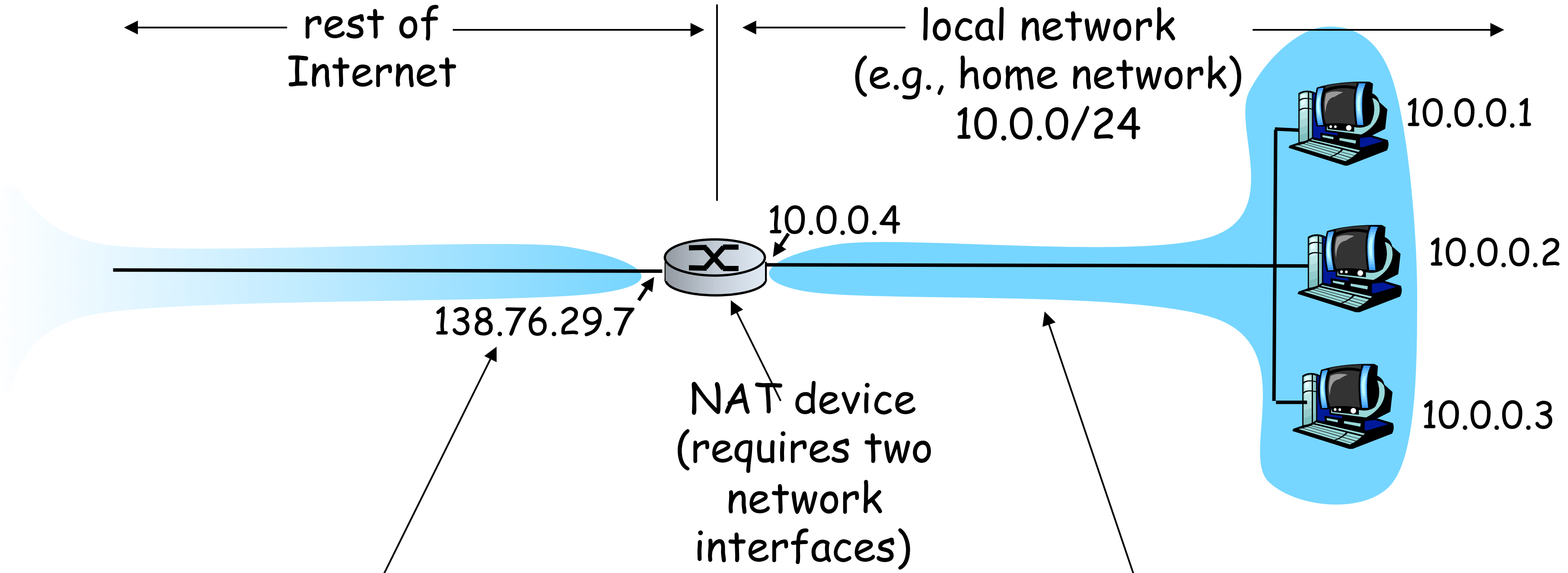
Sharing an IP address

- Motivated by
  - exhaustion of IP address space
  - conservation of resources
    - share internet access through just one IP address
  - home networks, other small LANs
    - too expensive to have unique IP address for each host
- … but users want to maintain security/privacy
  - avoid address conflicts, collisions

Network Address Translation (NAT)

- Multiple computers at one site can share a single global IP address (external IP address)
  - entire local network uses just one external IP address
    - theoretically, over 65,000 hosts
    - all internal addresses managed locally
    - individual addresses are treated like global addresses for security/privacy
    - transparent to all users
  - can change ISP / external address without affecting local addresses
  - devices inside local net can not be explicitly addressed by external hosts
    - a security plus!
- Implementation
  - in-line configuration
    - All traffic entering or leaving the network must go through the NAT device
    - Internal communications do not use the NAT device
    - 10.0.x.x addresses reserved for internal use

NAT Implementation (example)


rest of Internet
local network (e.g., home network) 10.0.0/24
10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
138.76.29.7
NAT device (requires two network interfaces)

<u>All</u> datagrams leaving local network have <u>same single source NAT IP address</u>: 138.76.29.7, <u>different source port numbers</u>

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

Implementation

- Software solutions
  - Standard PC with
    - NAT software, e.g.:
      - Linux *masquerade*
      - Windows *RRAS* (Routing and Remote Access Server)
    - extra NIC required
  - OK for slower speed networks (e.g., 10 Mbps)
    - NAT box must translate addresses in time for the usual network functions to work
      - calculating RTT, detecting congestion, etc.
- Hardware solutions
  - Special-purpose hardware for high-speed networks (e.g., gigabit Ethernet)
- Hybrid solutions
  - Routers can incorporate software for NAT
  - Used in medium-speed networks (e.g., 100 Mbps)

NAPT

- Network Address and Port Translation
  - Most popular implementation of NAT
    - Usually just called NAT
  - Keeps track of local/external IP addresses and port numbers
  - Allows
    - multiple applications on a single host in the private network to communicate with multiple destinations
    - multiple hosts in the private network to communicate with a single destination
  - The effect of NAT is to form a virtual private connection between a computer in a private network and a remote host (internet site).
    - Of course, the connection may be to a computer in a separate private network (through another NAT box)

Example NAT table

- Entry in table records protocol port number as well as IP address
- Port numbers are re-assigned to avoid conflicts
- Note: this requires the NAT box (router) to have some transport-layer functionality

Example: NAT device external address is **128.210.24.6**

Direction	Initial value	Translated	Unchanged
out	**Source** **10.0.0.125:30000**	**Source** **128.210.24.6:40001**	**Destination** **68.18.6.225:80**
out	**Source** **10.0.0.77:30000**	**Source** **128.210.24.6:40002**	**Destination** **68.18.6.225:80**
in	**Destination** **128.210.24.6:40002**	**Destination** **10.0.0.77:30000**	**Source** **68.18.6.225:80**
in	**Destination** **128.210.24.6:40001**	**Destination** **10.0.0.125:30000**	**Source** **68.18.6.225:80**

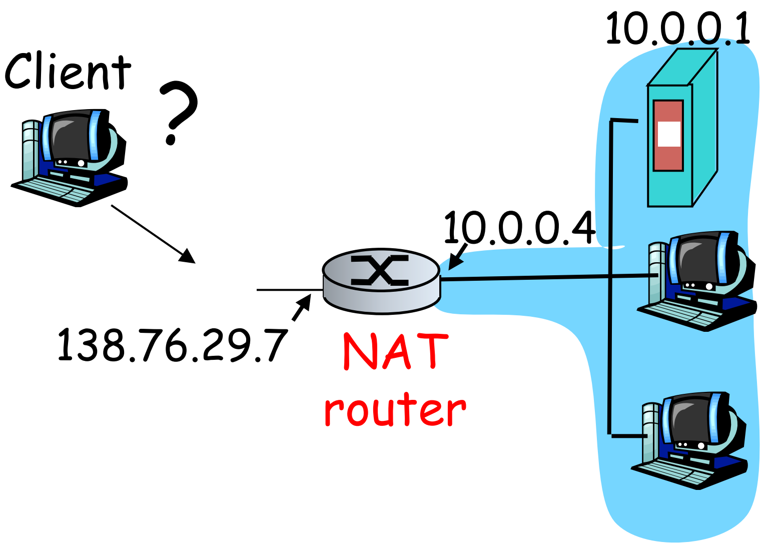
NAT table

- For an <u>out-going</u> datagram:
  - Translation table records
    - internal source address
    - original source port number
  - Source address is changed to the NAT' s external address.
  - Source port number is re-assigned
  - Translation table records
    - destination address
    - re-assigned source port number
  - Checksum is recalculated
  - Datagram is reconstructed
  - (Destination address / port number are not changed)

- For an <u>in-coming</u> datagram:
  - Destination address is changed to the internal address recorded in the translation table.
  - Destination port number is changed to the port number recorded in the translation table.
  - Checksum is recalculated
  - Datagram is reconstructed
  - (Source address / port number are not changed)

NAT traversal problem

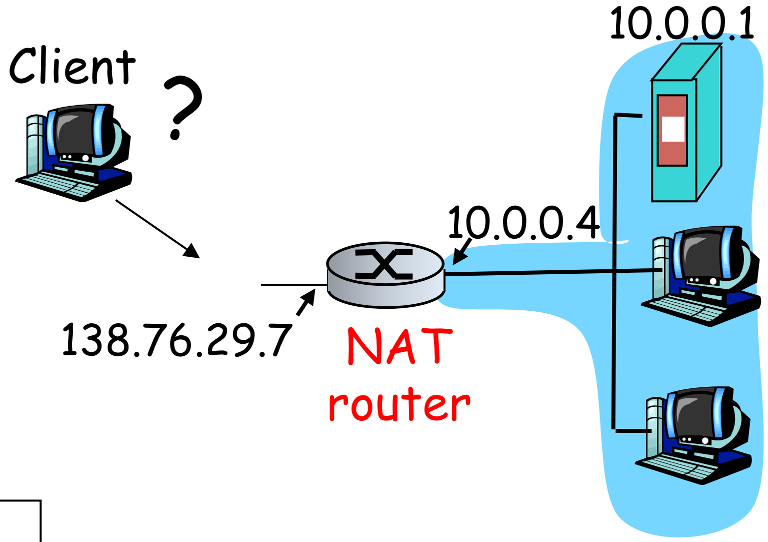
- When initial contact is attempted from outside the site, there is no translation table entry
  - E.G., a private network might be running one or more servers through a NAT system
- Example: External client wants to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can't use it as destination address)
  - only one externally visible NAT'ed address: 138.76.29.7



NAT traversal problem

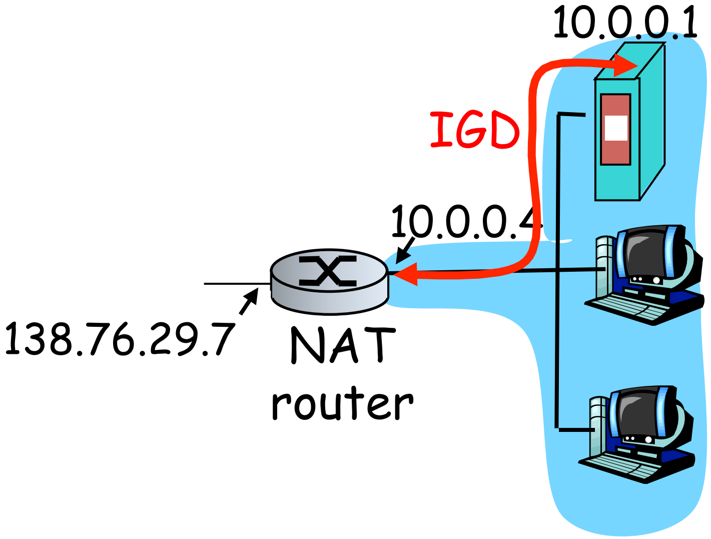
Solution 1: Statically configure NAT to forward incoming connection requests at given port to server (one server only)

- e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000

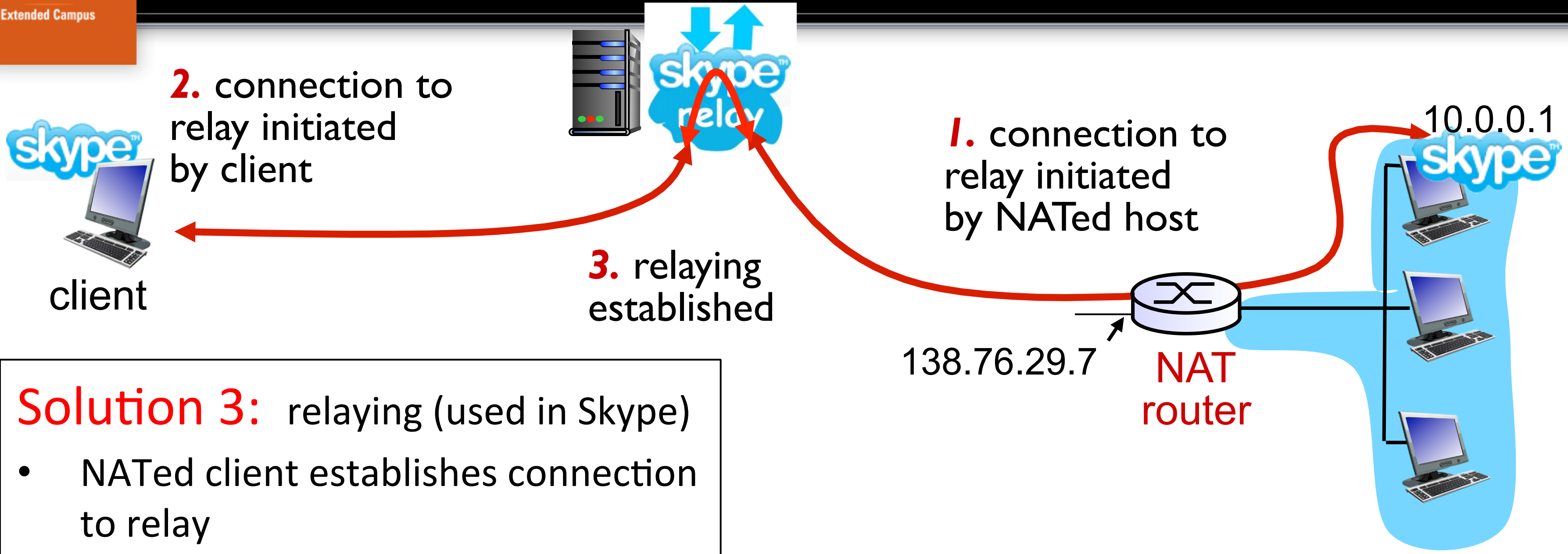


Solution 2: Universal PnP Internet Gateway Device (IGD) Protocol (one server only).

- Automates static configuration
- Allows NAT'ed host to:
  - map (private IP, private port #) to (public IP, public port #)
  - advertise (public IP, public port #)
    - So DNS can work
  - add/remove (lease) port mappings



NAT traversal problem


2. connection to relay initiated by client
client
1. connection to relay initiated by NATed host
10.0.0.1
3. relaying established
138.76.29.7
NAT router

Solution 3: relaying (used in Skype)

- NATed client establishes connection to relay
- external client connects to relay
- relay bridges packets between to connections

Solution 4: (Twice NAT)

- NAT box provides DNS service
  - Works in most cases
  - Doesn't work if remote request uses IP address instead of domain name

Network Address Translation

- 16-bit port-number field:
  - ~65,000 simultaneous connections with a single external address!
- NAT is controversial.
  - Objections include:
    - routers should only process up to the network layer
      - NAT requires access to port numbers
    - ISP overload
    - address shortage should instead be solved by IPv6

Summary Lecture #32

- NAT
  - external/internal address
  - external/internal port numbers
  - translation table
  - initial contact solutions
  - objections