



Network Layer

Part 6

Mark Allman
mallman@case.edu

EECS 325/425
Fall 2018

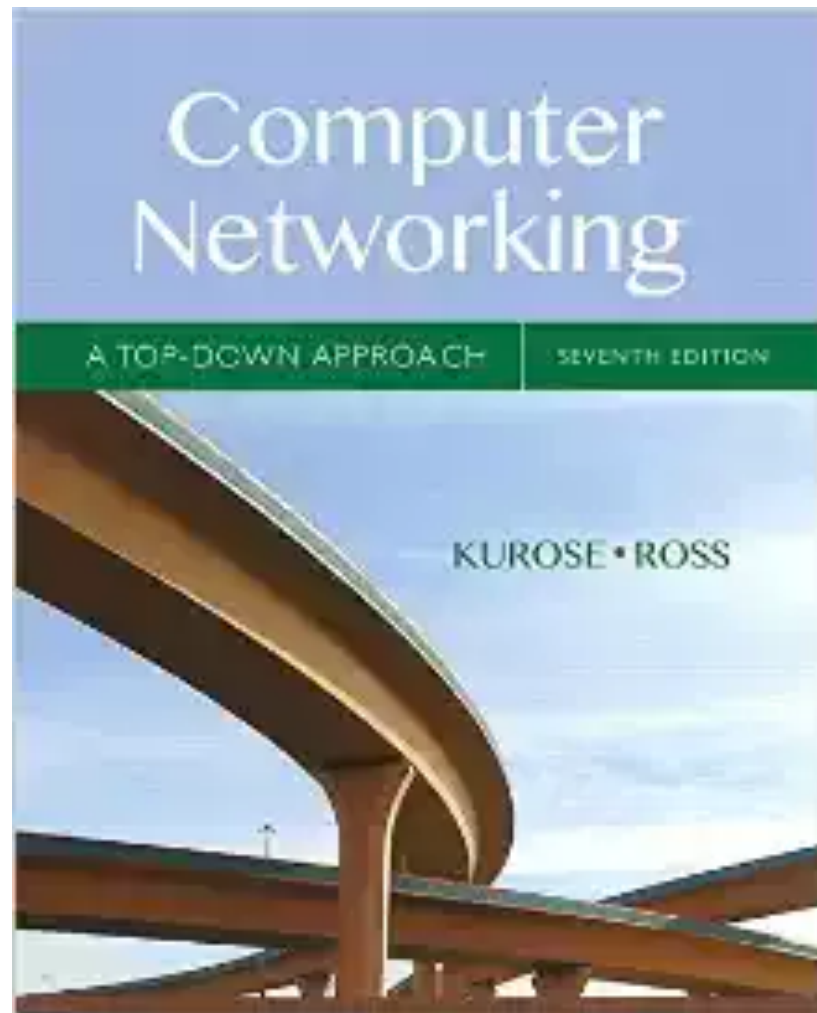
*“And so I wake in the morning and I step outside
And I take a deep breath and I get real high
And I scream from the top of my lungs... WHAT’S GOING ON?”*

These slides are more-or-less directly from the slide set developed by Jim Kurose and Keith Ross for their book “Computer Networking: A Top Down Approach, 5th edition”.

The slides have been lightly adapted for Mark Allman’s EECS 325/425 Computer Networks class at Case Western Reserve University.

All material copyright 1996-2010
J.F Kurose and K.W. Ross, All Rights Reserved

Reading Along ...



- Network layer is chapters 4 & 5
- Address shortage

Address Shortage

Address Shortage

- ❖ The supply of IPv4 addresses thinned to the point of extinction
- ❖ What to do?

Address Shortage

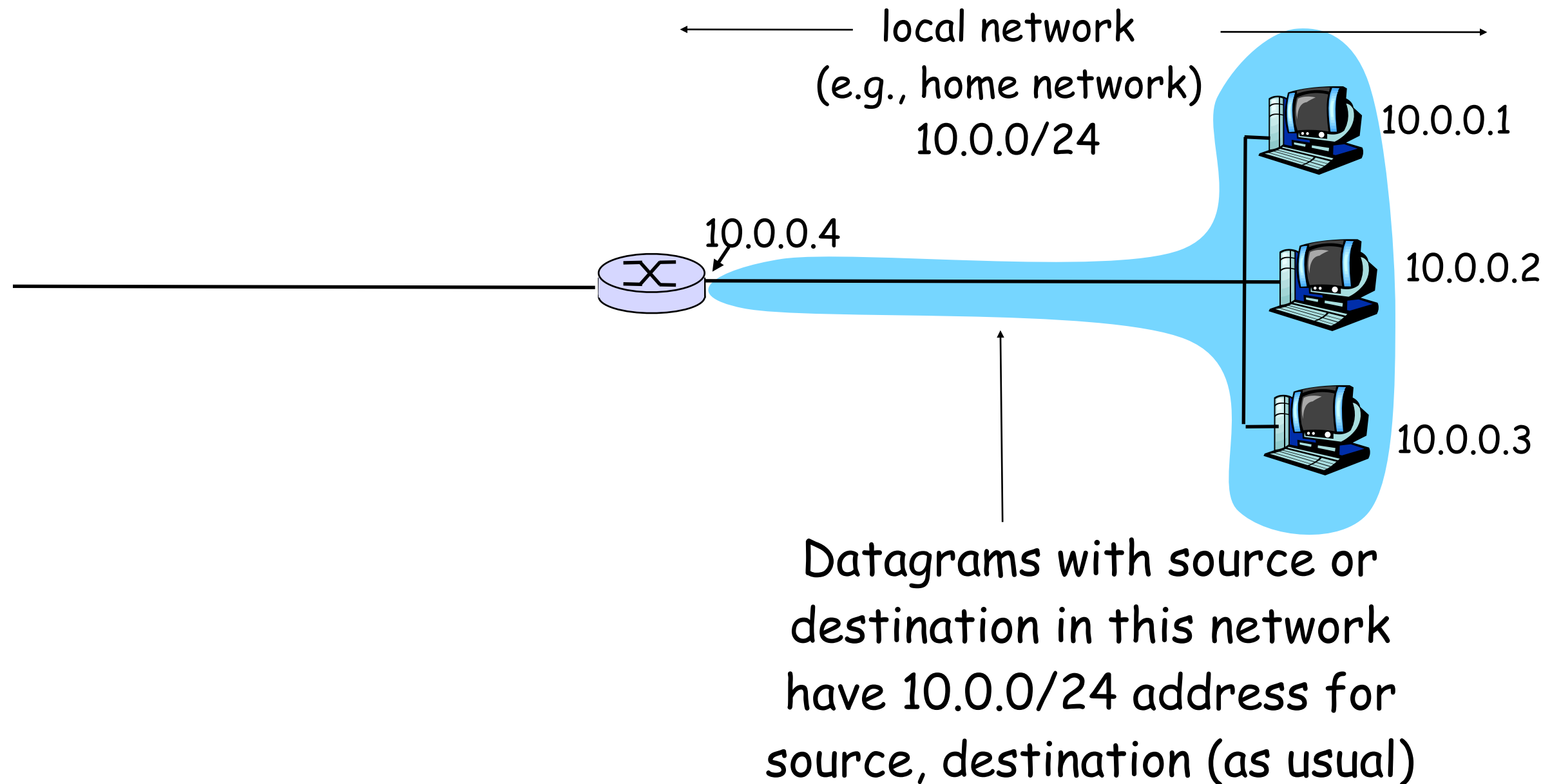
- ❖ The supply of IPv4 addresses thinned to the point of extinction
- ❖ What to do?
 - CIDR to provide more fine-grained address allocations
 - quick fix
 - IPv6 to provide more addresses
 - long term fix

Address Shortage

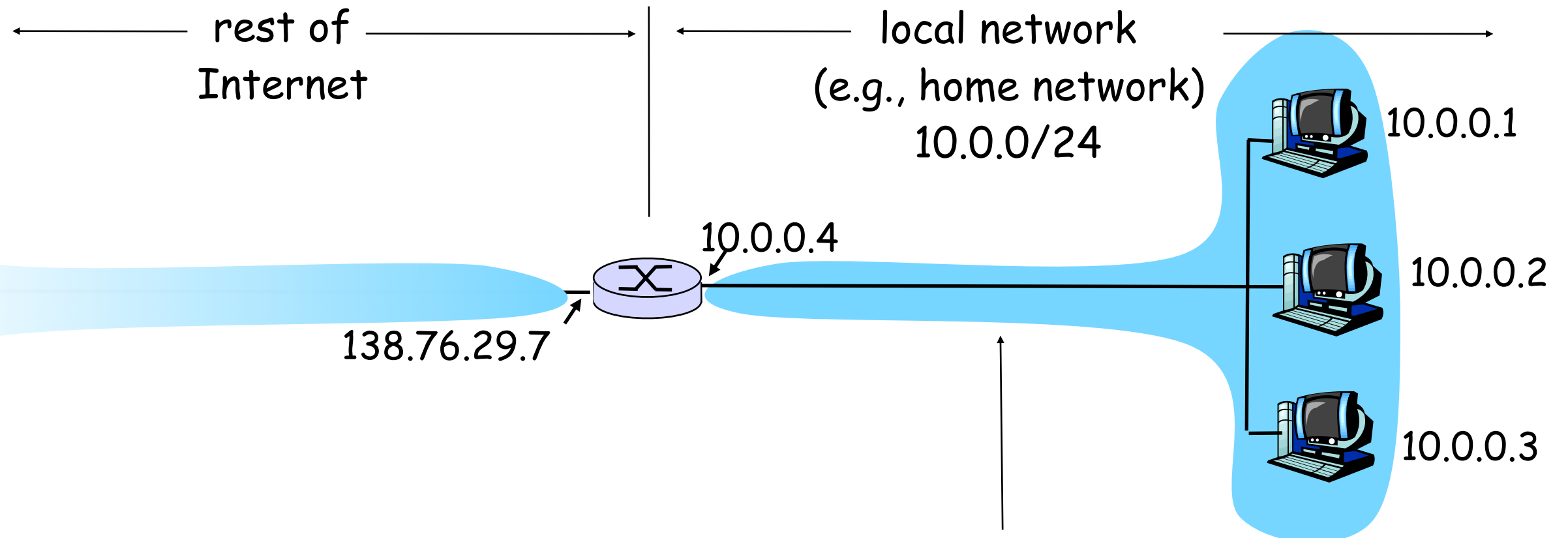
- ❖ The supply of IPv4 addresses thinned to the point of extinction
- ❖ What to do?
 - CIDR to provide more fine-grained address allocations
 - quick fix
 - IPv6 to provide more addresses
 - long term fix
 - NAT to better leverage constrained IPv4 address space

NAT: Network Address Translation

NAT: Network Address Translation

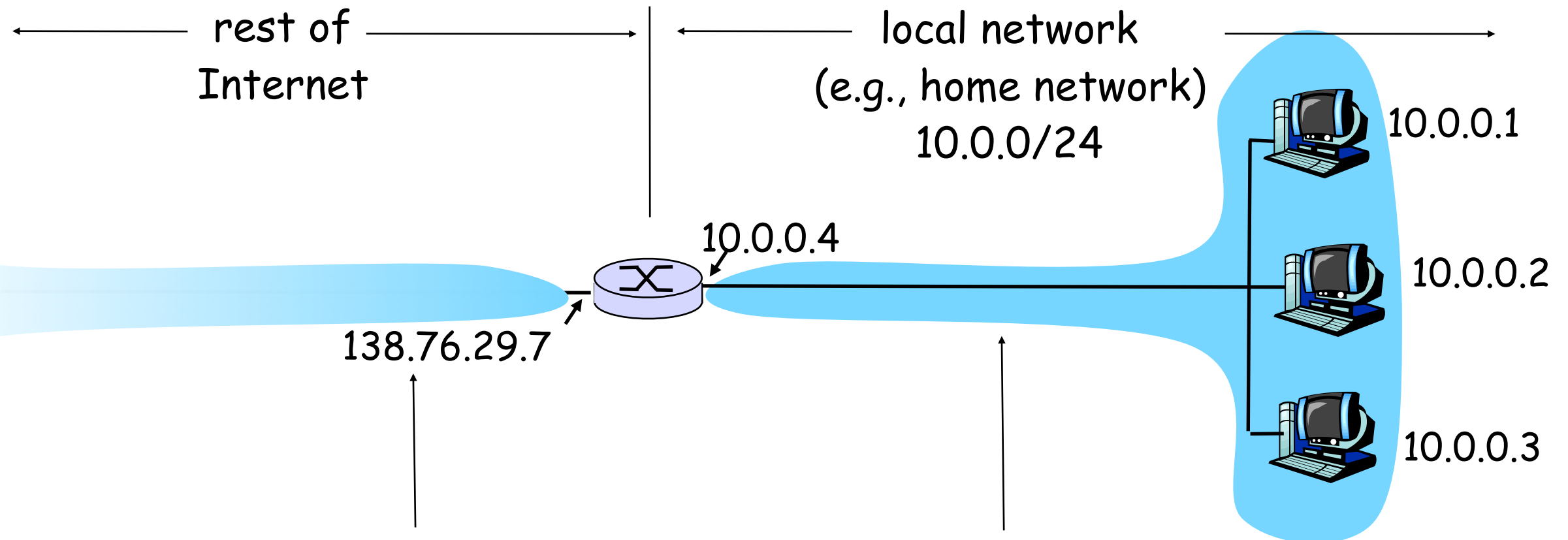


NAT: Network Address Translation



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

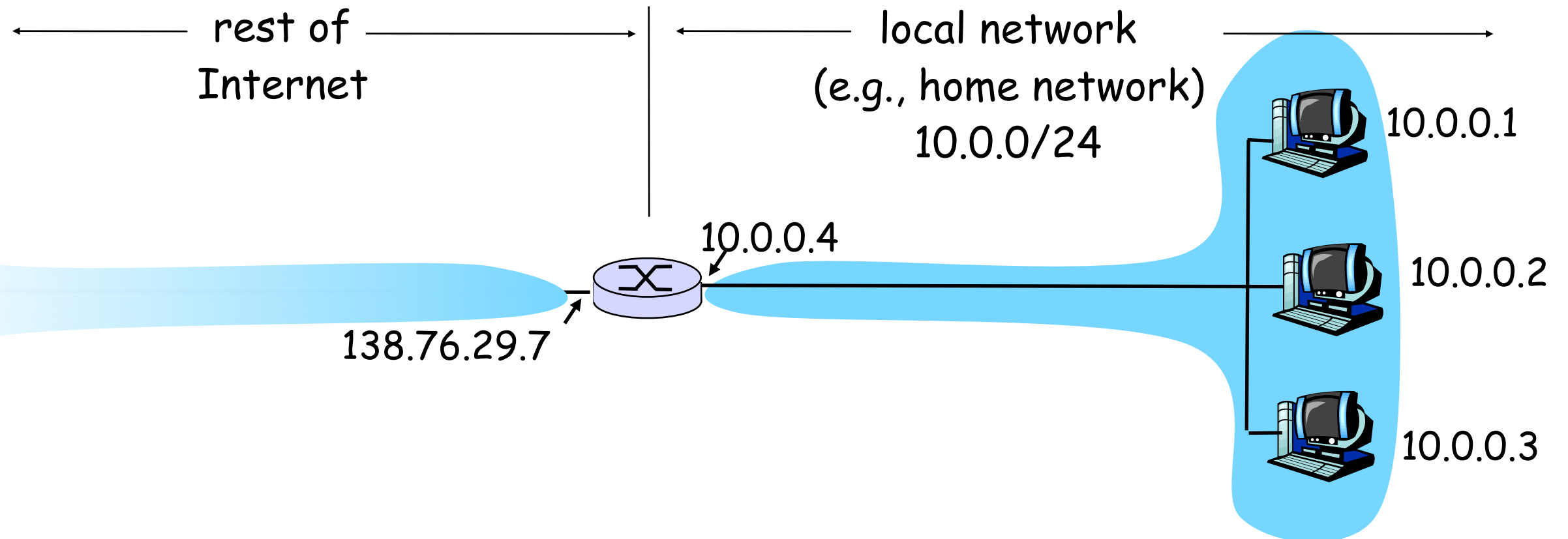
NAT: Network Address Translation



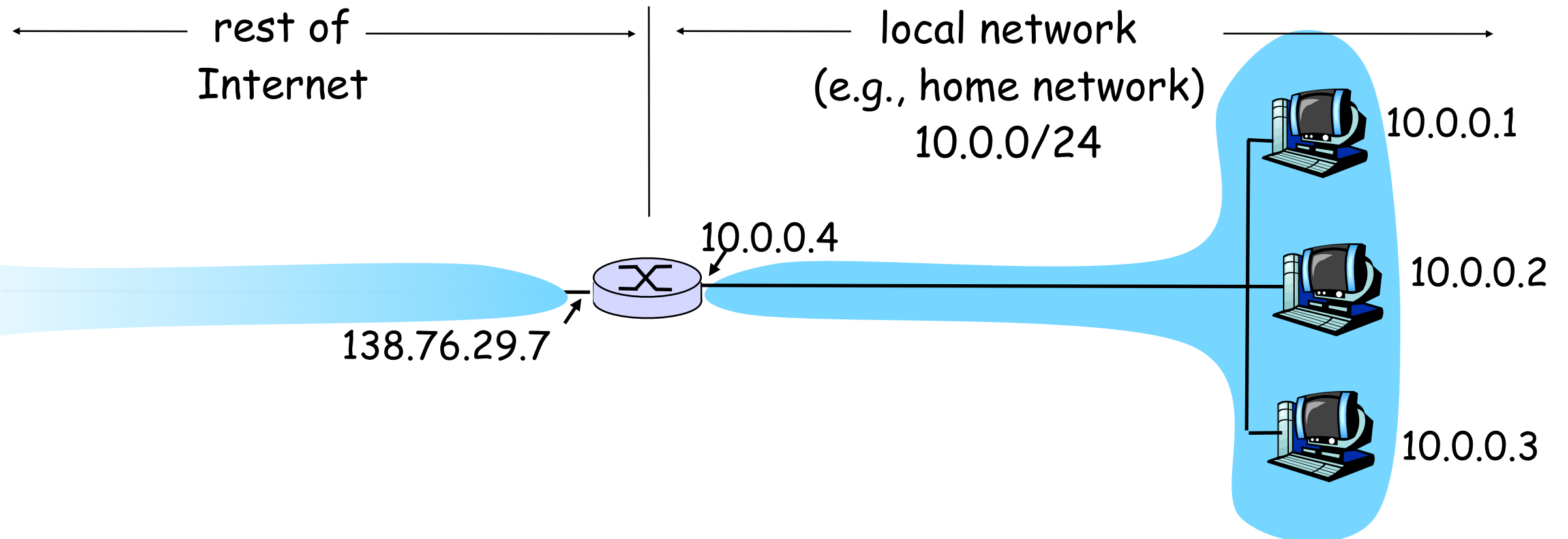
All datagrams **leaving** local network have **same** single source NAT IP address: 138.76.29.7.

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

NAT: Network Address Translation

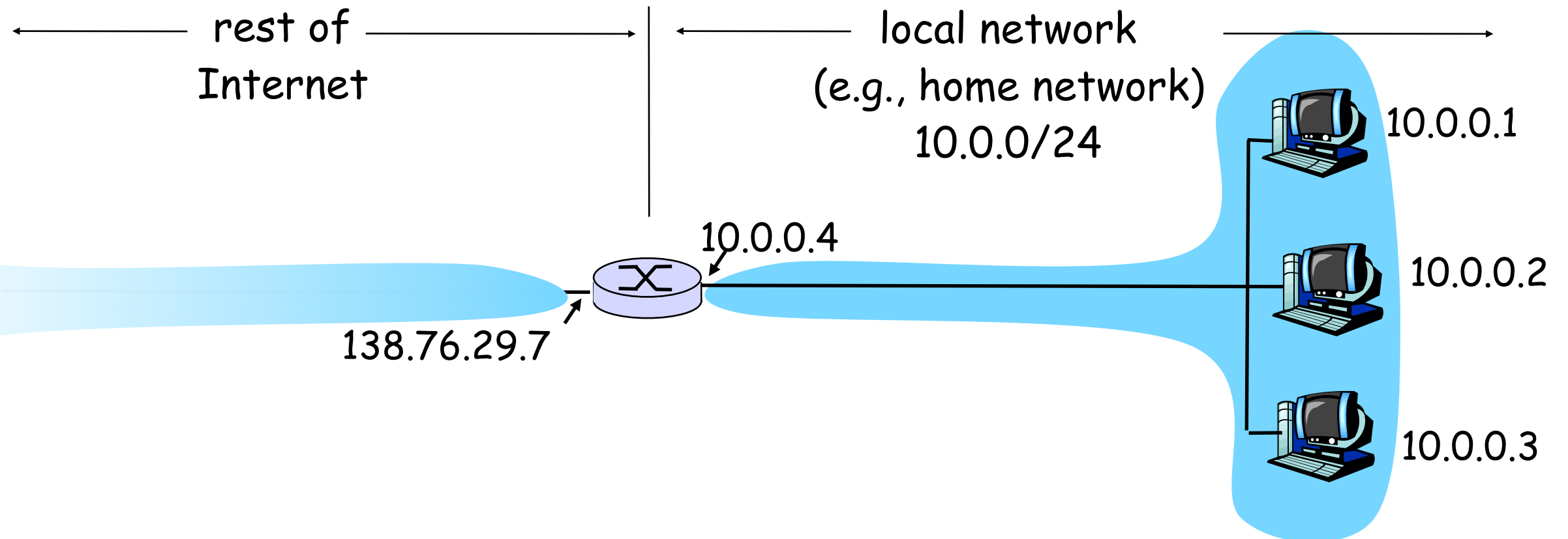


NAT: Network Address Translation



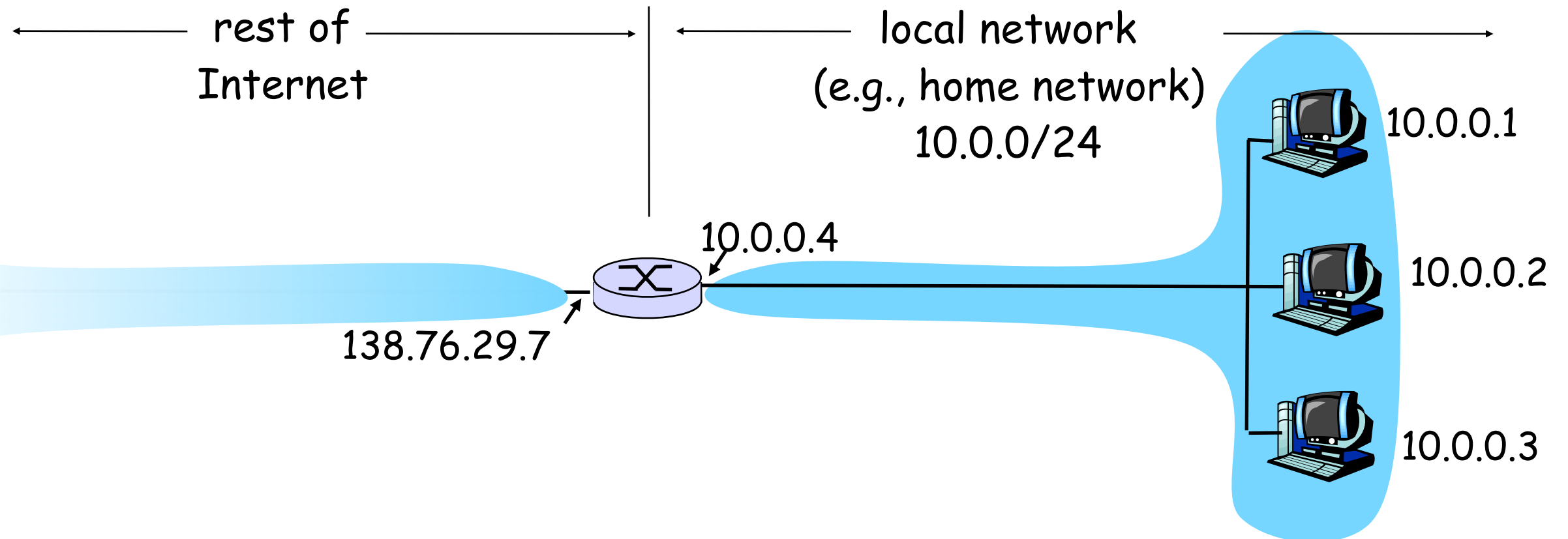
❖ How does the router get its external address?

NAT: Network Address Translation



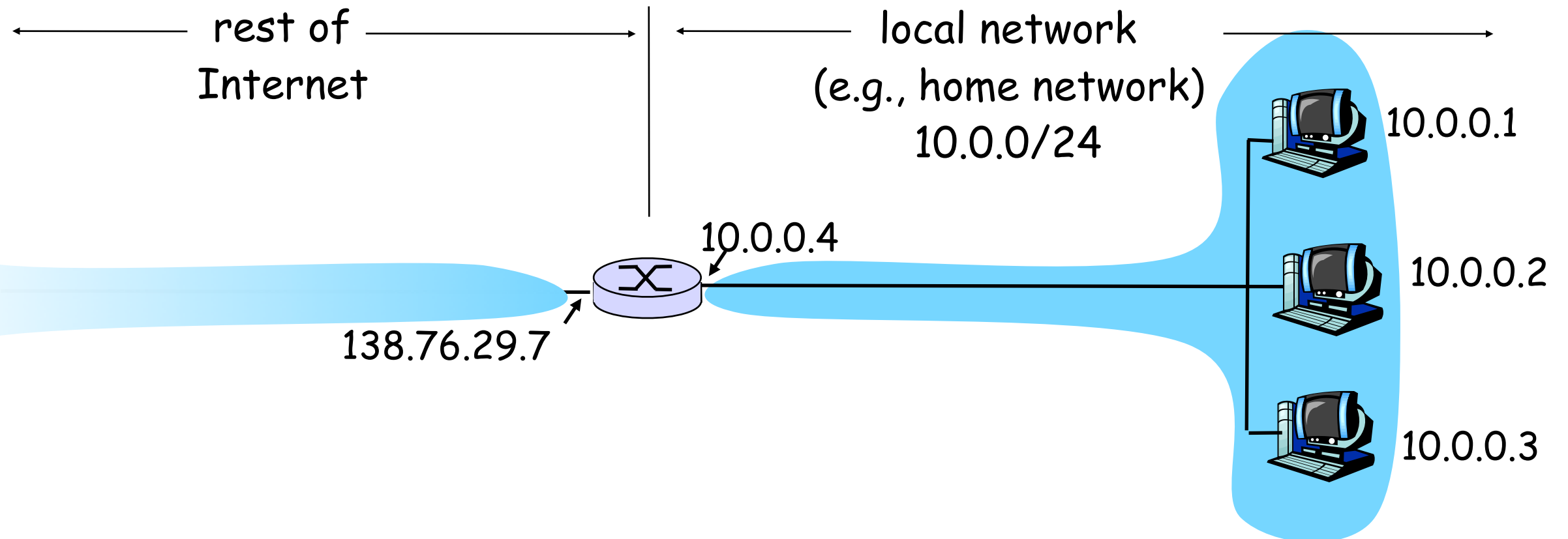
- ❖ How does the router get its external address?
 - ❖ From ISP

NAT: Network Address Translation

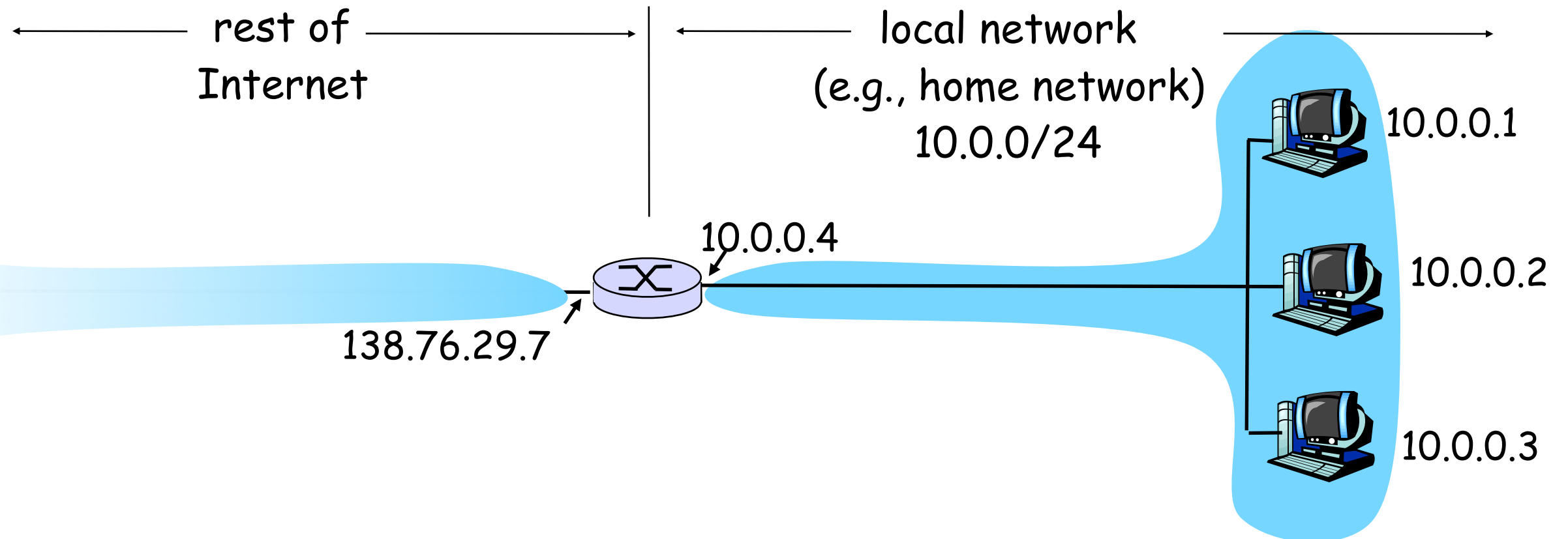


- ❖ How does the router get its external address?
 - ❖ From ISP
 - ❖ Static or DHCP

NAT: Network Address Translation

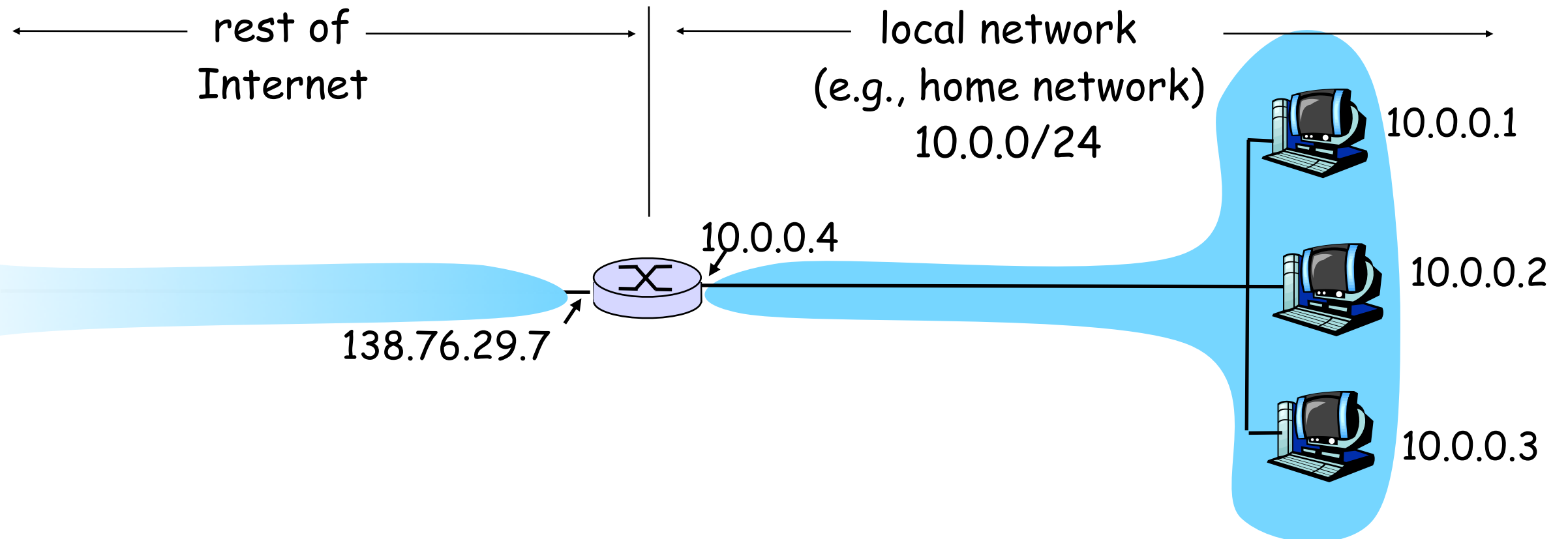


NAT: Network Address Translation



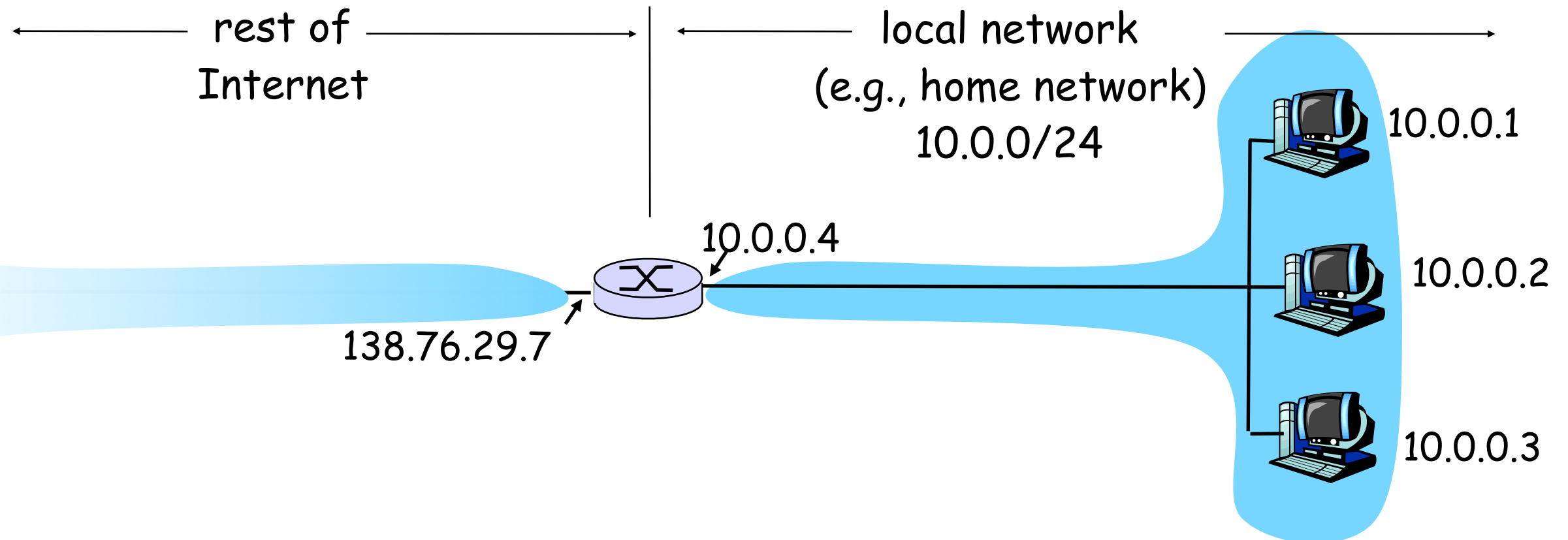
❖ What are these 10.x.x.x addresses?

NAT: Network Address Translation



- ❖ What are these 10.x.x.x addresses?
 - ❖ Explicitly private address space

NAT: Network Address Translation



- ❖ What are these 10.x.x.x addresses?
 - ❖ Explicitly private address space
 - ❖ 10/8, 192.168/16, 172.16/12, 100.64/10

NAT: Network Address Translation

NAT: Network Address Translation

- ❖ **Motivation:** local network uses just one IP address as far as outside world is concerned:

NAT: Network Address Translation

- ❖ **Motivation:** local network uses just one IP address as far as outside world is concerned:
 - range of addresses not needed from ISP: just one IP address for all devices

NAT: Network Address Translation

- ❖ **Motivation:** local network uses just one IP address as far as outside world is concerned:
 - range of addresses not needed from ISP: just one IP address for all devices
 - can change addresses of devices in local network without notifying outside world

NAT: Network Address Translation

- ❖ **Motivation:** local network uses just one IP address as far as outside world is concerned:
 - range of addresses not needed from ISP: just one IP address for all devices
 - can change addresses of devices in local network without notifying outside world
 - can change ISP without changing addresses of devices in local network

NAT: Network Address Translation

- ❖ **Motivation:** local network uses just one IP address as far as outside world is concerned:
 - range of addresses not needed from ISP: just one IP address for all devices
 - can change addresses of devices in local network without notifying outside world
 - can change ISP without changing addresses of devices in local network
 - devices inside local net not explicitly addressable, visible by outside world (a security plus).

NAT: Network Address Translation

NAT: Network Address Translation

Implementation: NAT router must:

NAT: Network Address Translation

Implementation: NAT router must:

- **outgoing datagrams:** replace client source IP address of every outgoing datagram with NAT IP address
... remote clients/servers will respond using the NAT's external IP address as destination addr.

NAT: Network Address Translation

Implementation: NAT router must:

- **outgoing datagrams:** replace client source IP address of every outgoing datagram with NAT IP address
... remote clients/servers will respond using the NAT's external IP address as destination addr.
- **incoming datagrams:** replace NAT's external IP address in dest field of every incoming datagram with the client's internal IP address

NAT: Network Address Translation

NAT: Network Address Translation

Implementation: NAT router must:

NAT: Network Address Translation

Implementation: NAT router must:

- **outgoing datagrams: replace** (client source IP address, port #) of every outgoing datagram with (external NAT IP address, new port #)
 - ... remote clients/servers will respond using (external NAT IP address, new port #) as destination addr.

NAT: Network Address Translation

Implementation: NAT router must:

- **outgoing datagrams: replace** (client source IP address, port #) of every outgoing datagram with (external NAT IP address, new port #)
... remote clients/servers will respond using (external NAT IP address, new port #) as destination addr.
- **remember (in NAT translation table)** every (source IP address, port #) to (NAT IP address, new port #) translation pair

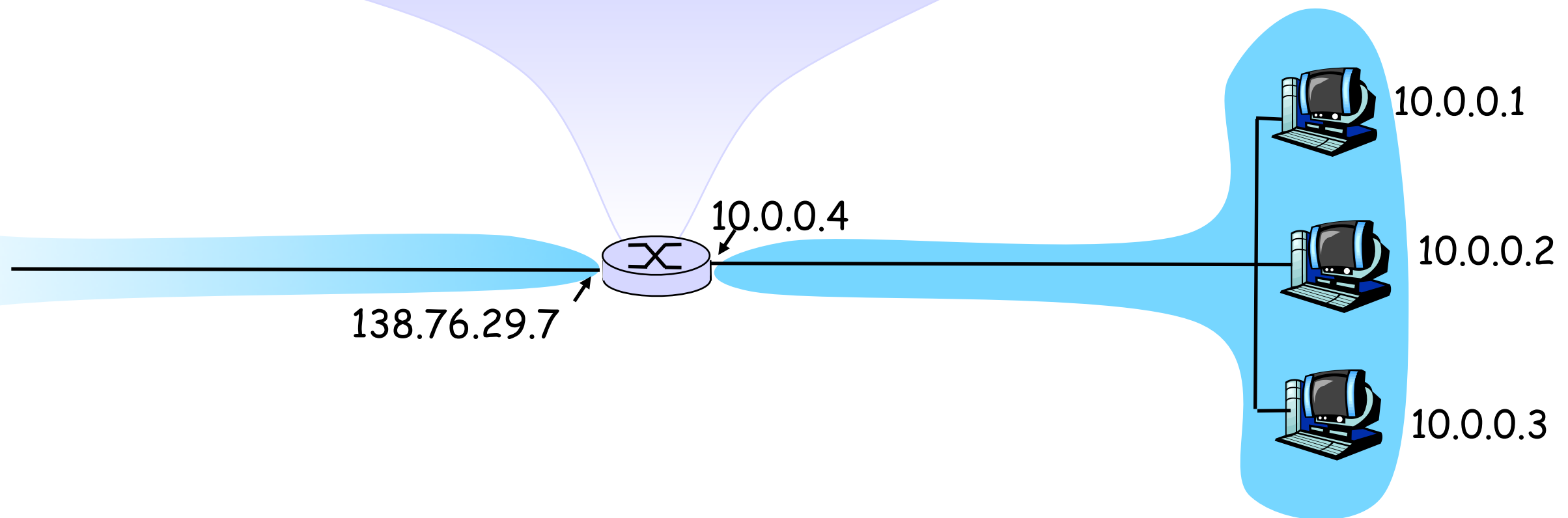
NAT: Network Address Translation

Implementation: NAT router must:

- **outgoing datagrams: replace** (client source IP address, port #) of every outgoing datagram with (external NAT IP address, new port #)
... remote clients/servers will respond using (external NAT IP address, new port #) as destination addr.
- **remember (in NAT translation table)** every (source IP address, port #) to (NAT IP address, new port #) translation pair
- **incoming datagrams: replace** (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT: Network Address Translation

NAT translation table	
WAN side addr	LAN side addr



NAT: Network Address Translation

NAT translation table	
WAN side addr	LAN side addr

1: host 10.0.0.1
sends datagram to
128.119.40.186, 80

S: 10.0.0.1, 3345
D: 128.119.40.186, 80

1

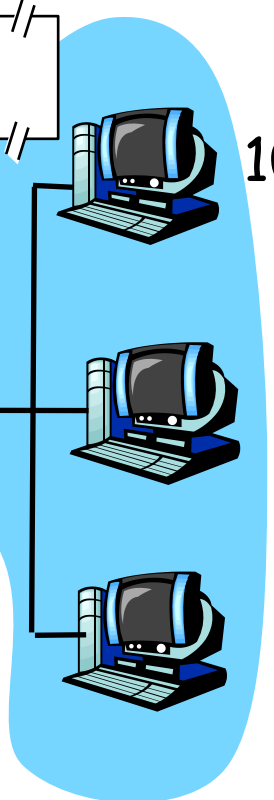
10.0.0.1

10.0.0.2

10.0.0.3

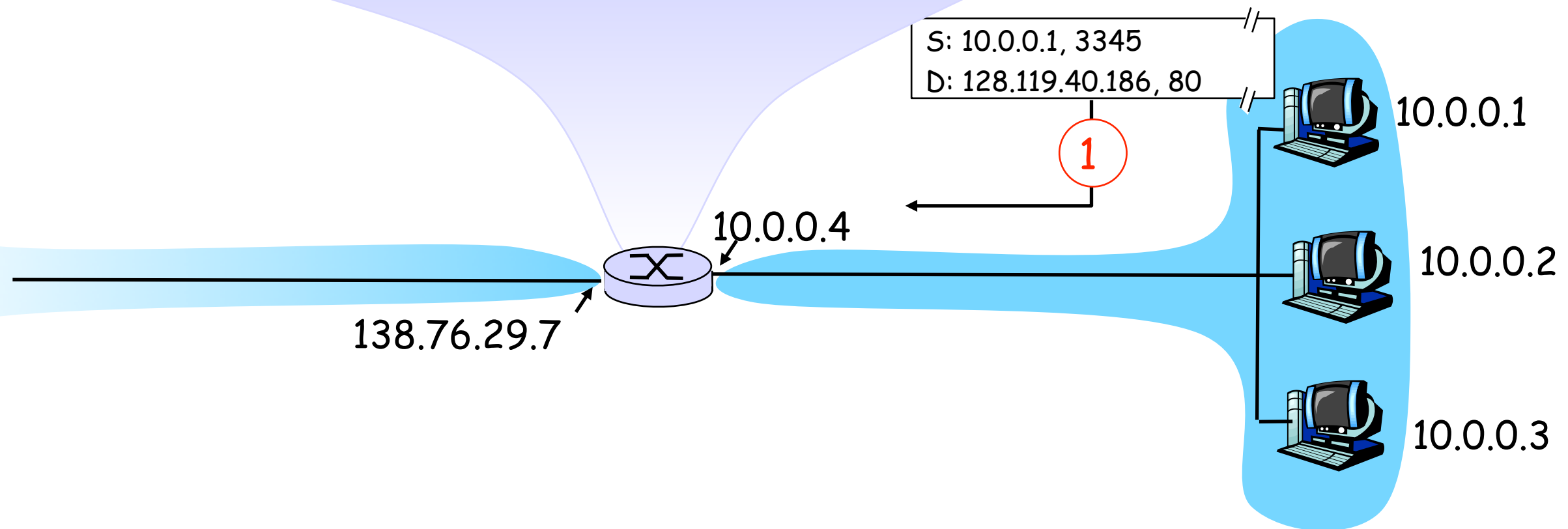
138.76.29.7

10.0.0.4



NAT: Network Address Translation

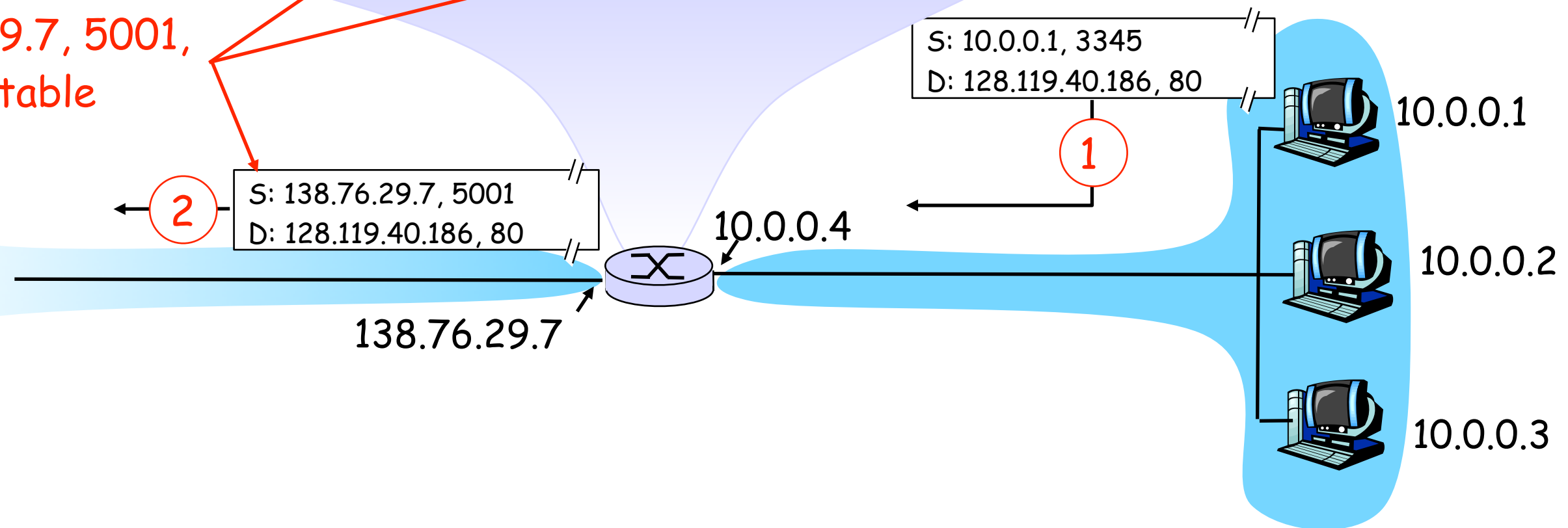
NAT translation table	
WAN side addr	LAN side addr



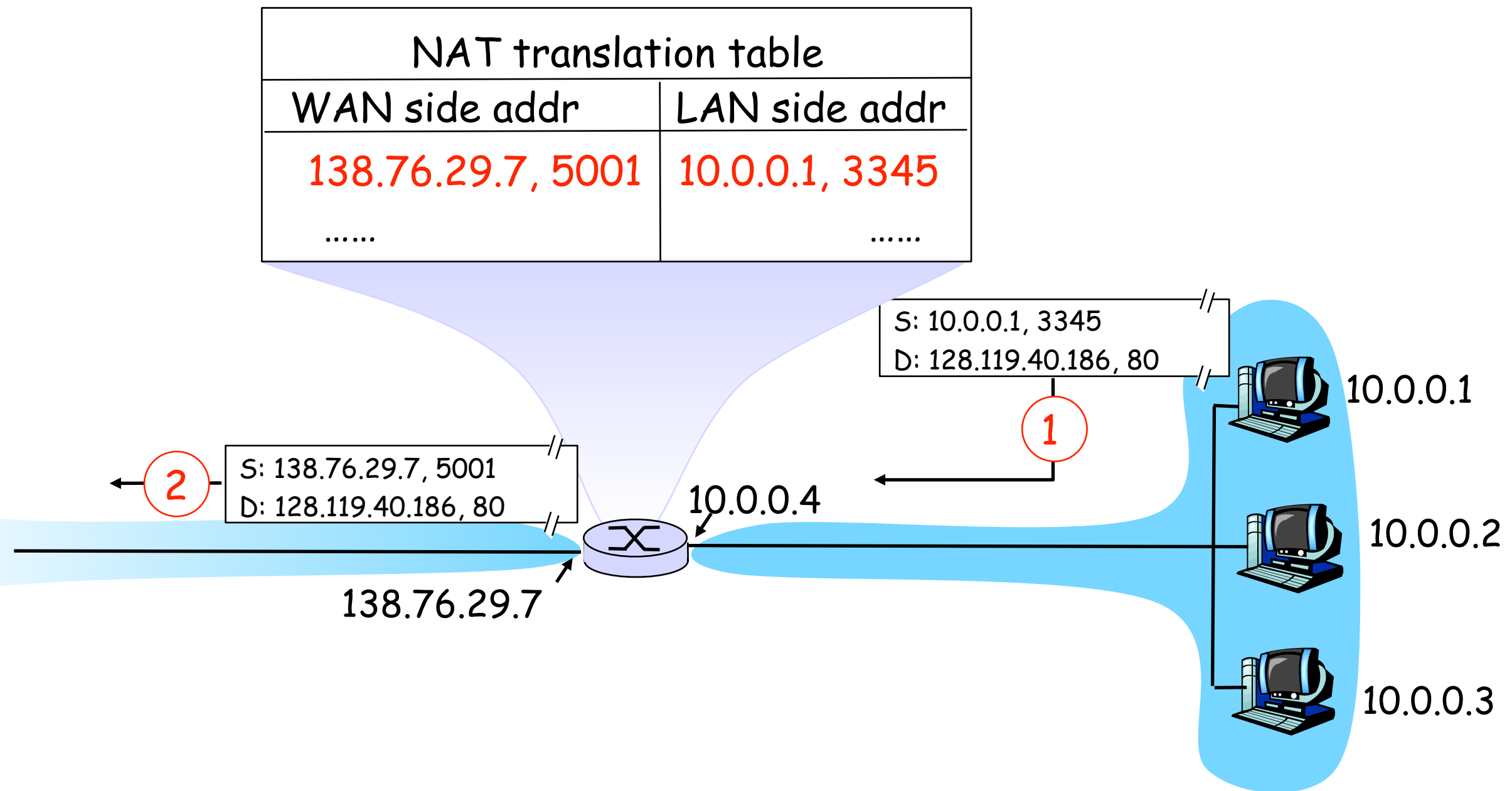
NAT: Network Address Translation

2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

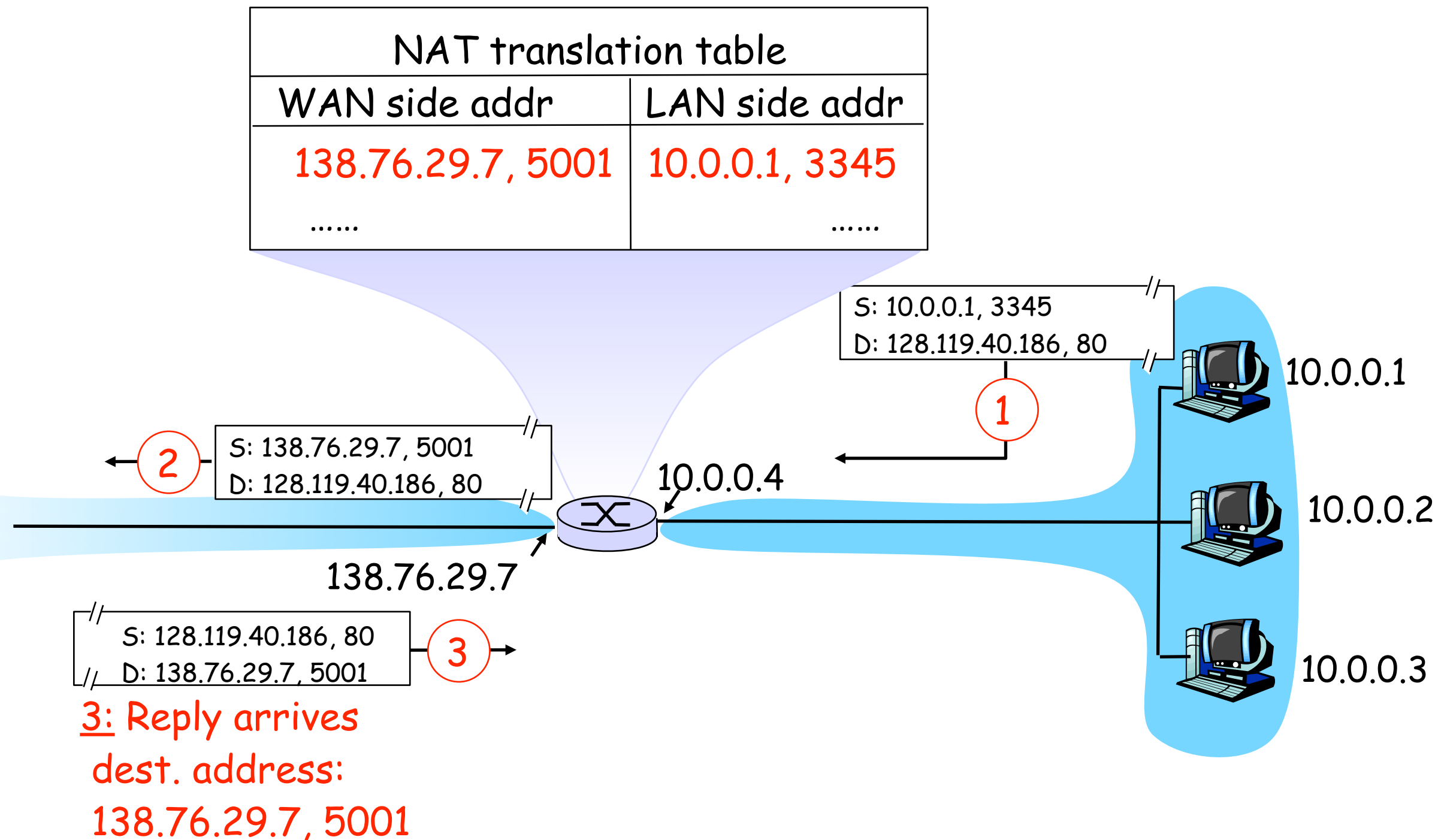
NAT translation table	
WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
.....



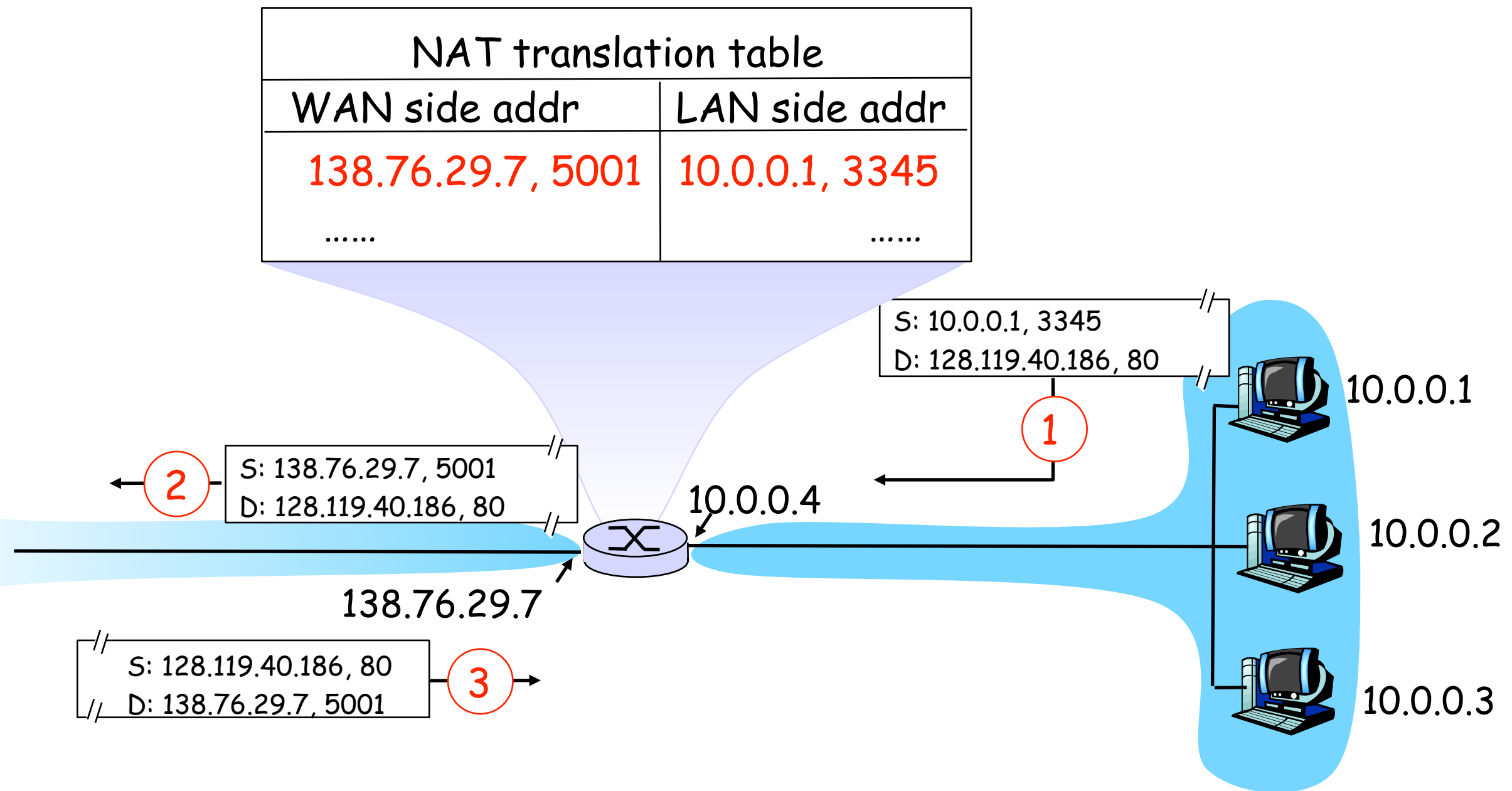
NAT: Network Address Translation



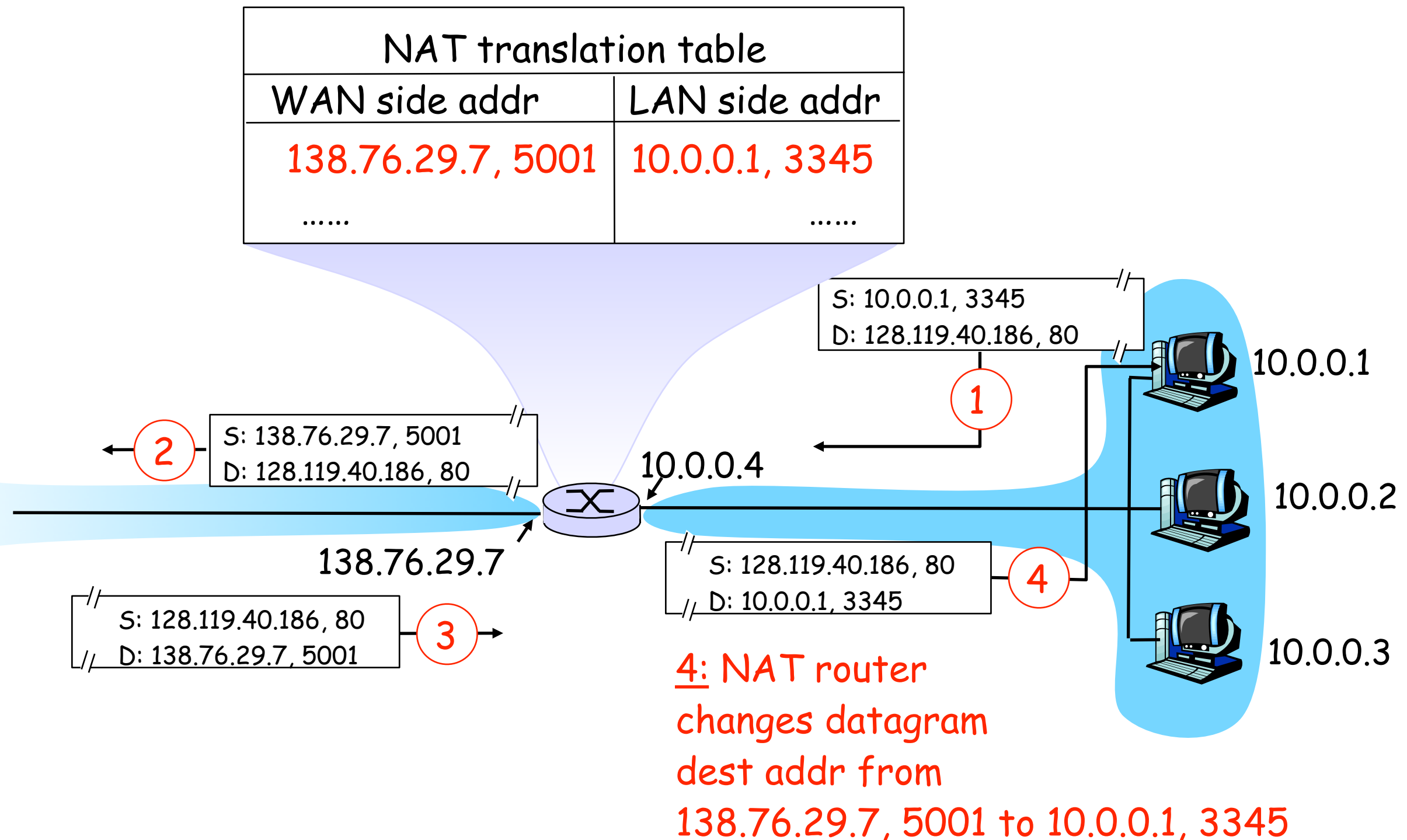
NAT: Network Address Translation



NAT: Network Address Translation



NAT: Network Address Translation



NAT: Network Address Translation

NAT: Network Address Translation

- ❖ 16-bit port-number field:
 - 60,000+ simultaneous connections with a single LAN-side address!

NAT: Network Address Translation

- ❖ 16-bit port-number field:
 - 60,000+ simultaneous connections with a single LAN-side address!
- ❖ NAT is (was?) controversial:

NAT: Network Address Translation

- ❖ 16-bit port-number field:
 - 60,000+ simultaneous connections with a single LAN-side address!
- ❖ NAT is (was?) controversial:
 - routers should only process up to layer 3

NAT: Network Address Translation

- ❖ 16-bit port-number field:
 - 60,000+ simultaneous connections with a single LAN-side address!
- ❖ NAT is (was?) controversial:
 - routers should only process up to layer 3
 - violates end-to-end argument
 - NAT possibility must be taken into account by app designers, e.g., P2P applications

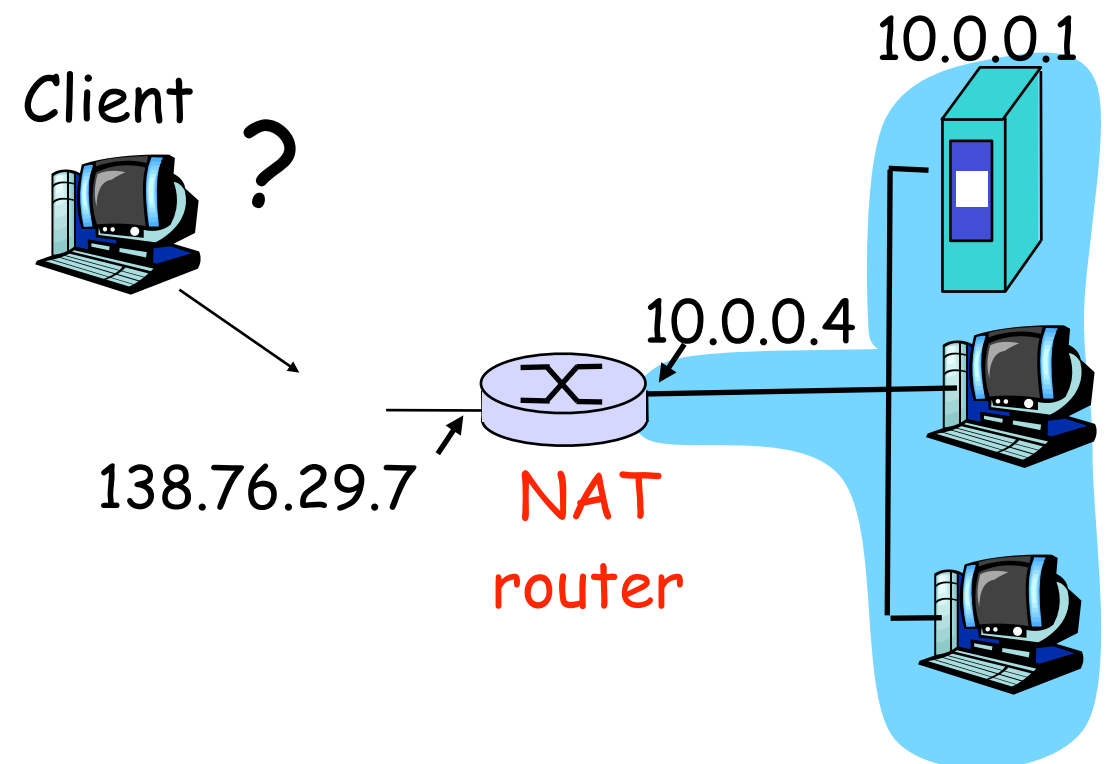
NAT: Network Address Translation

- ❖ 16-bit port-number field:
 - 60,000+ simultaneous connections with a single LAN-side address!
- ❖ NAT is (was?) controversial:
 - routers should only process up to layer 3
 - violates end-to-end argument
 - NAT possibility must be taken into account by app designers, e.g., P2P applications
 - address shortage should instead be solved by IPv6

NAT traversal problem

❖ client wants to connect to server with address 10.0.0.1

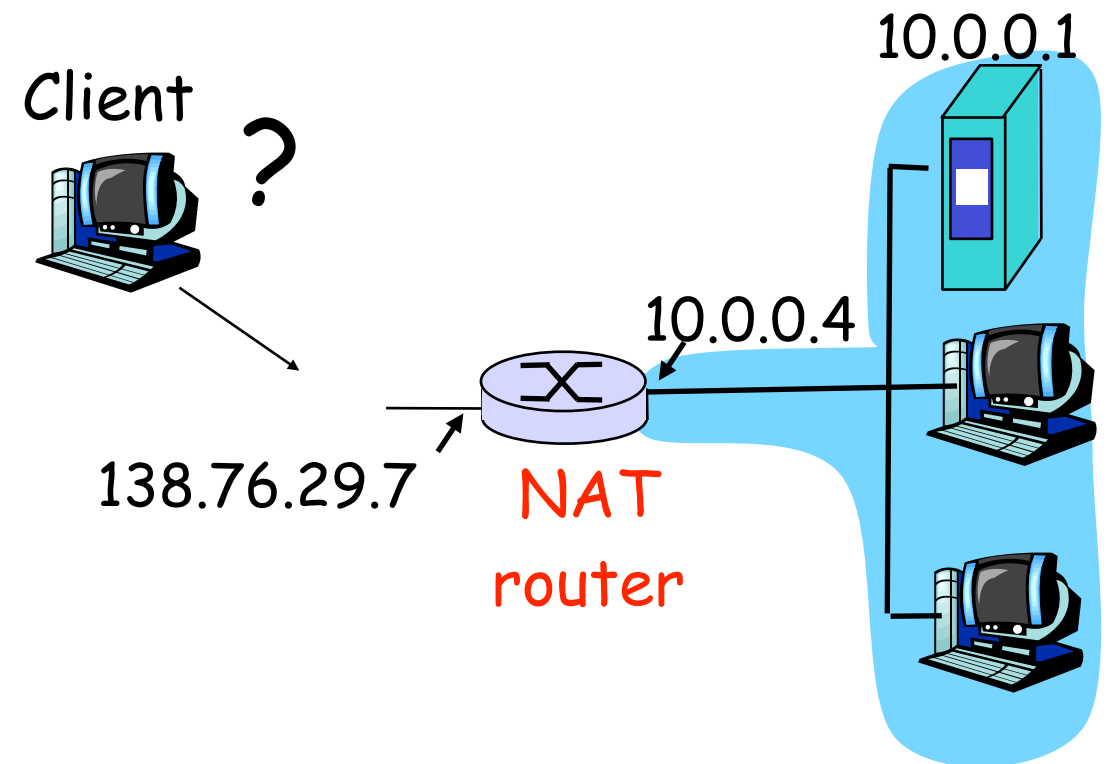
- server address 10.0.0.1 local to LAN (client can't use it as destination addr)
- only one externally visible NATed address: 138.76.29.7



NAT traversal problem

❖ solution 1: statically configure NAT to forward incoming connection requests at given port to server

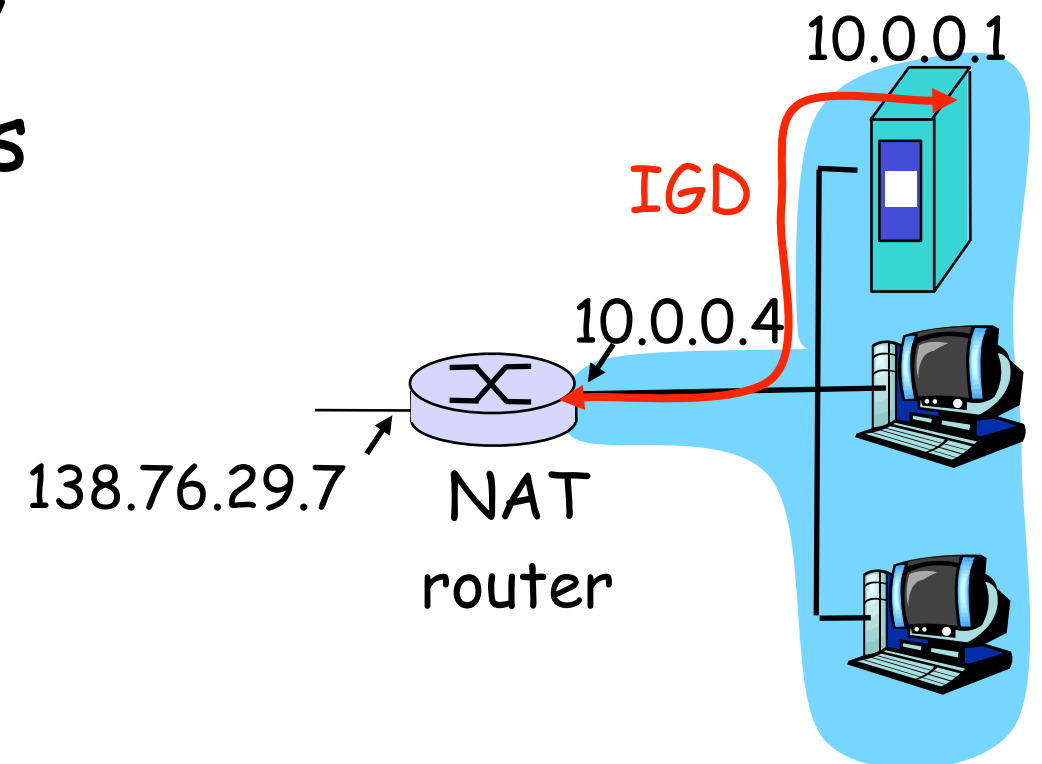
- e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000



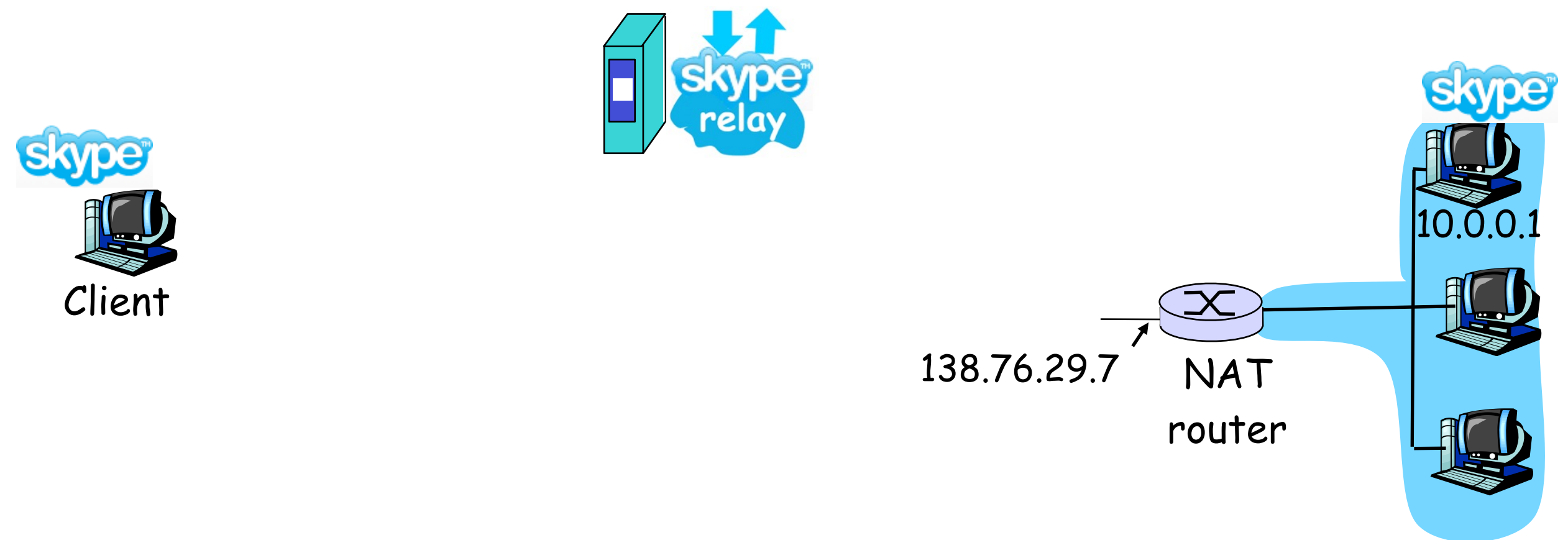
NAT traversal problem

- ❖ solution 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATed clients to:
- ❖ learn public IP address (138.76.29.7)
- ❖ add/remove port mappings (with lease times)

i.e., automate static NAT port map configuration

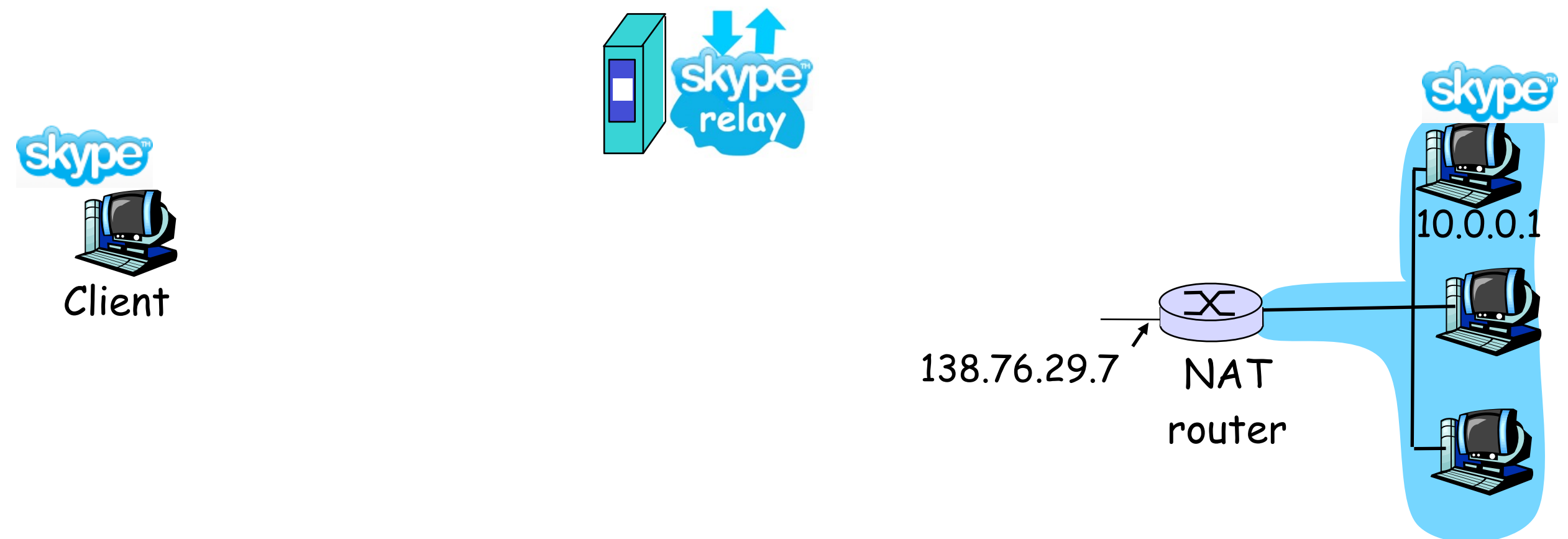


NAT traversal problem



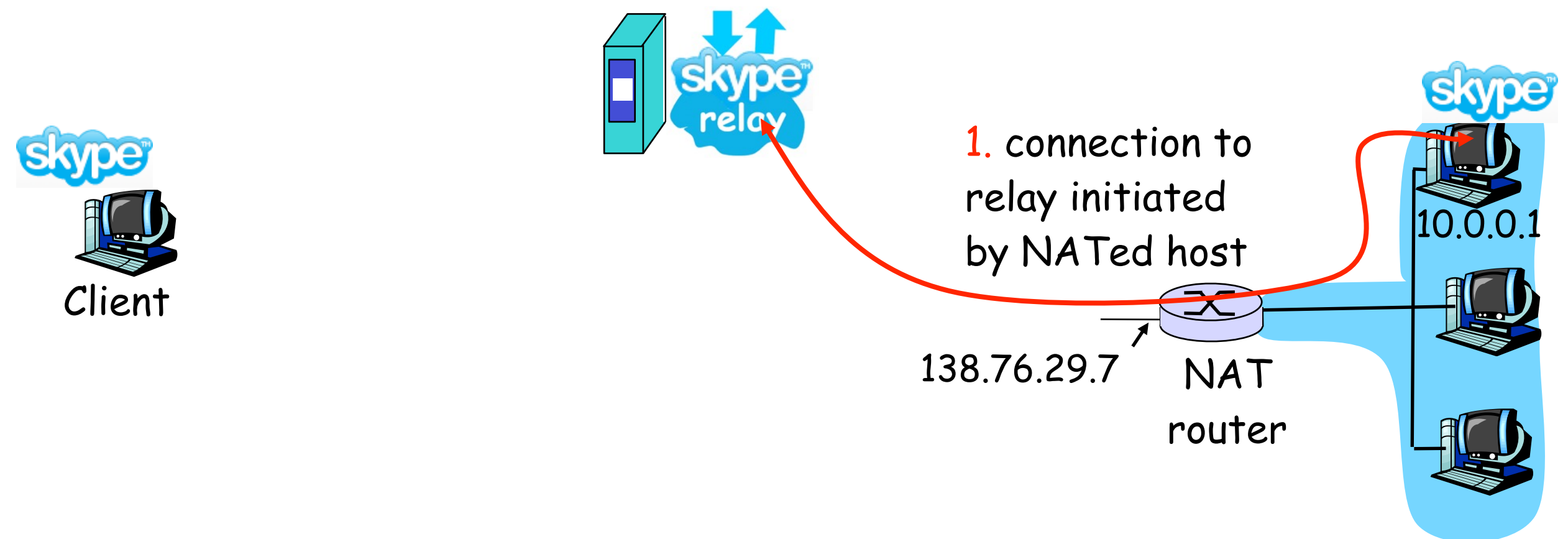
NAT traversal problem

❖ solution 3: relaying (used in Skype)



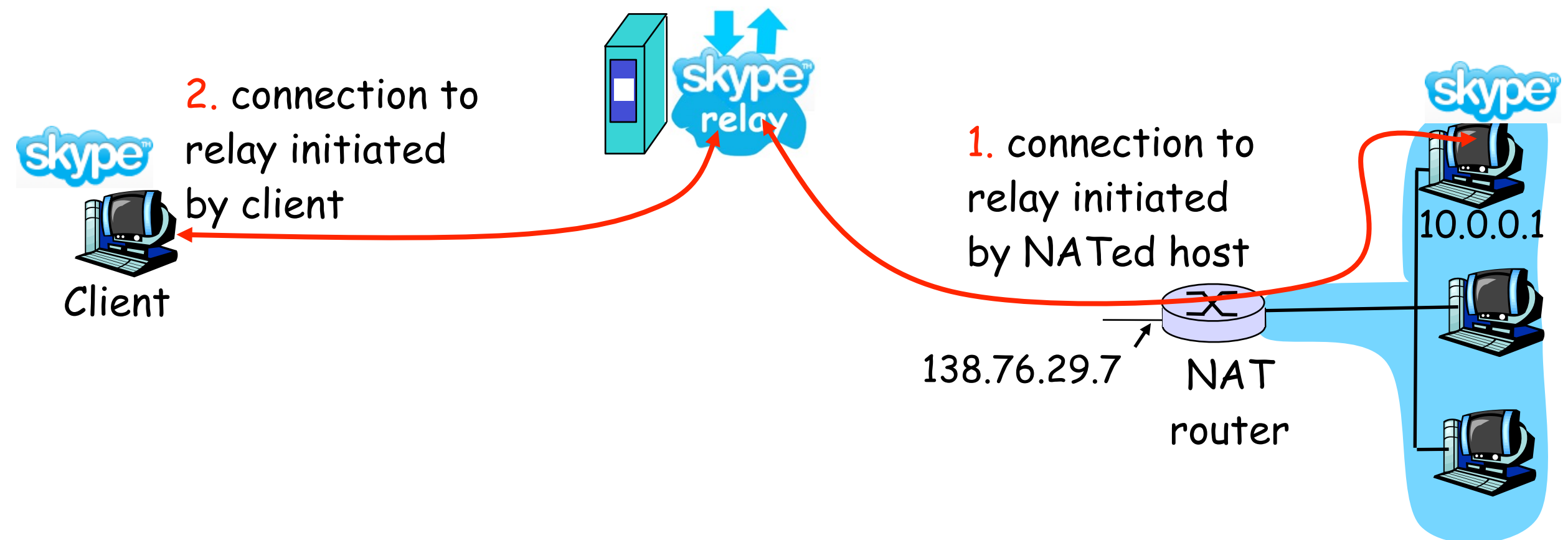
NAT traversal problem

- ❖ solution 3: relaying (used in Skype)
 - NATed client establishes connection to relay



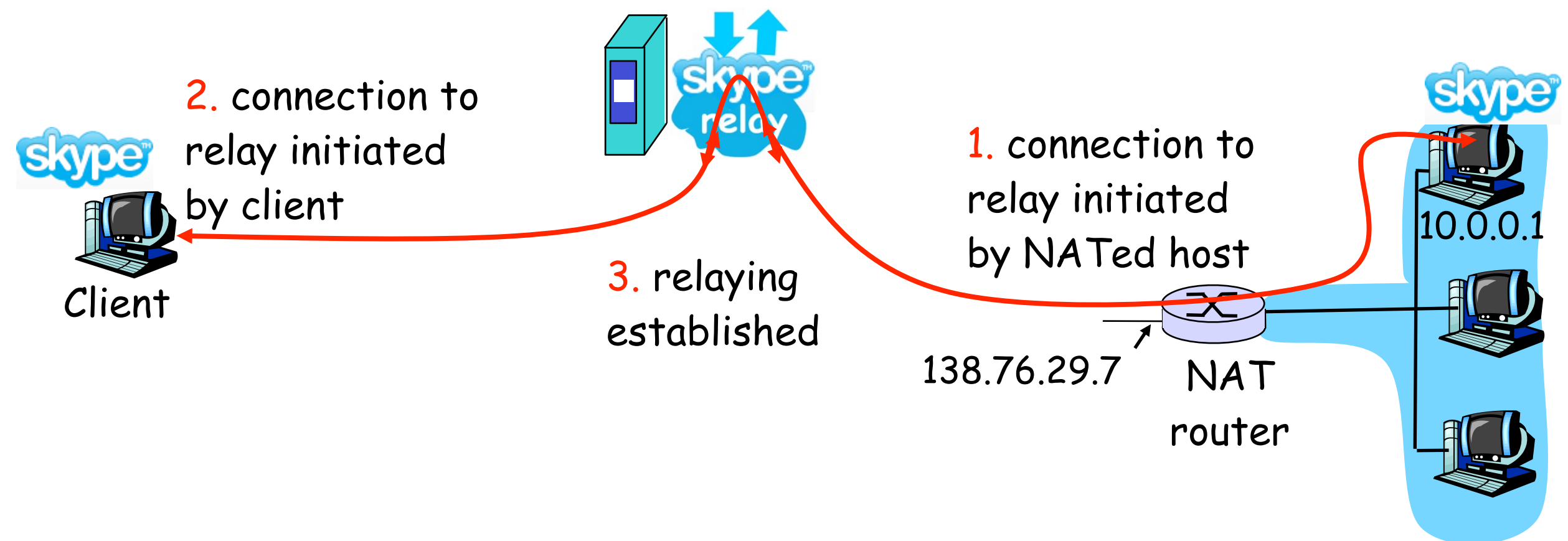
NAT traversal problem

- ❖ solution 3: relaying (used in Skype)
 - NATed client establishes connection to relay
 - External client connects to relay



NAT traversal problem

- ❖ solution 3: relaying (used in Skype)
 - NATed client establishes connection to relay
 - External client connects to relay
 - relay bridges packets between to connections



NATs Here ... NATs There!

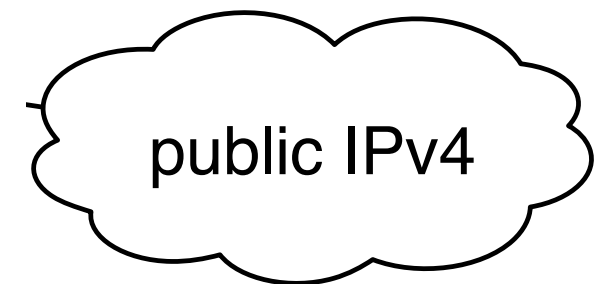
Subscribers

|

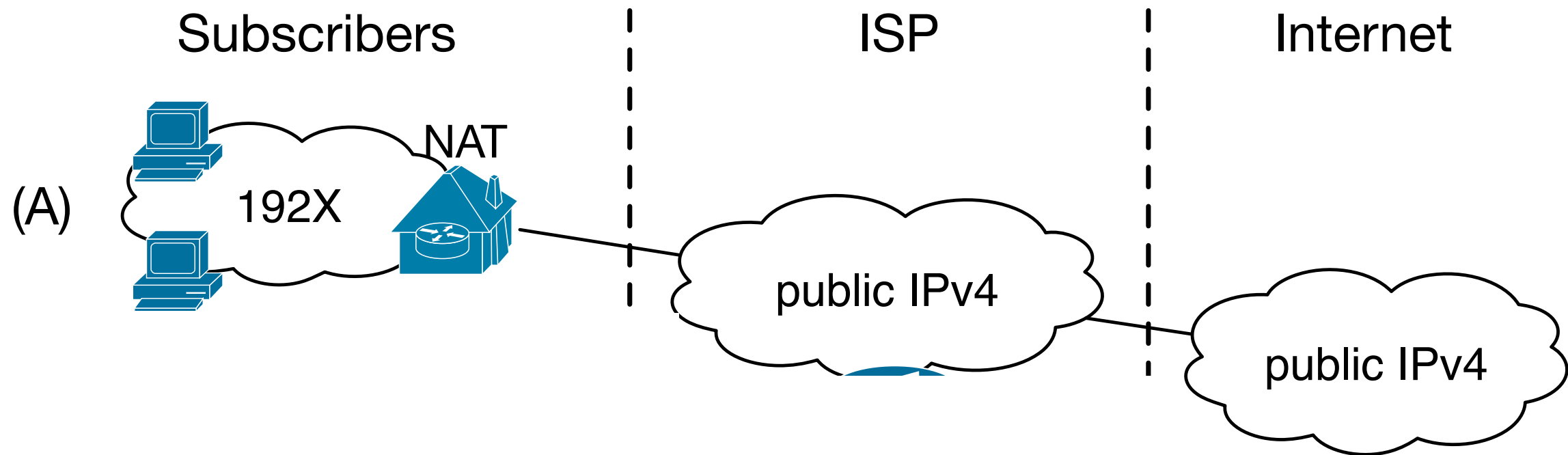
ISP

|

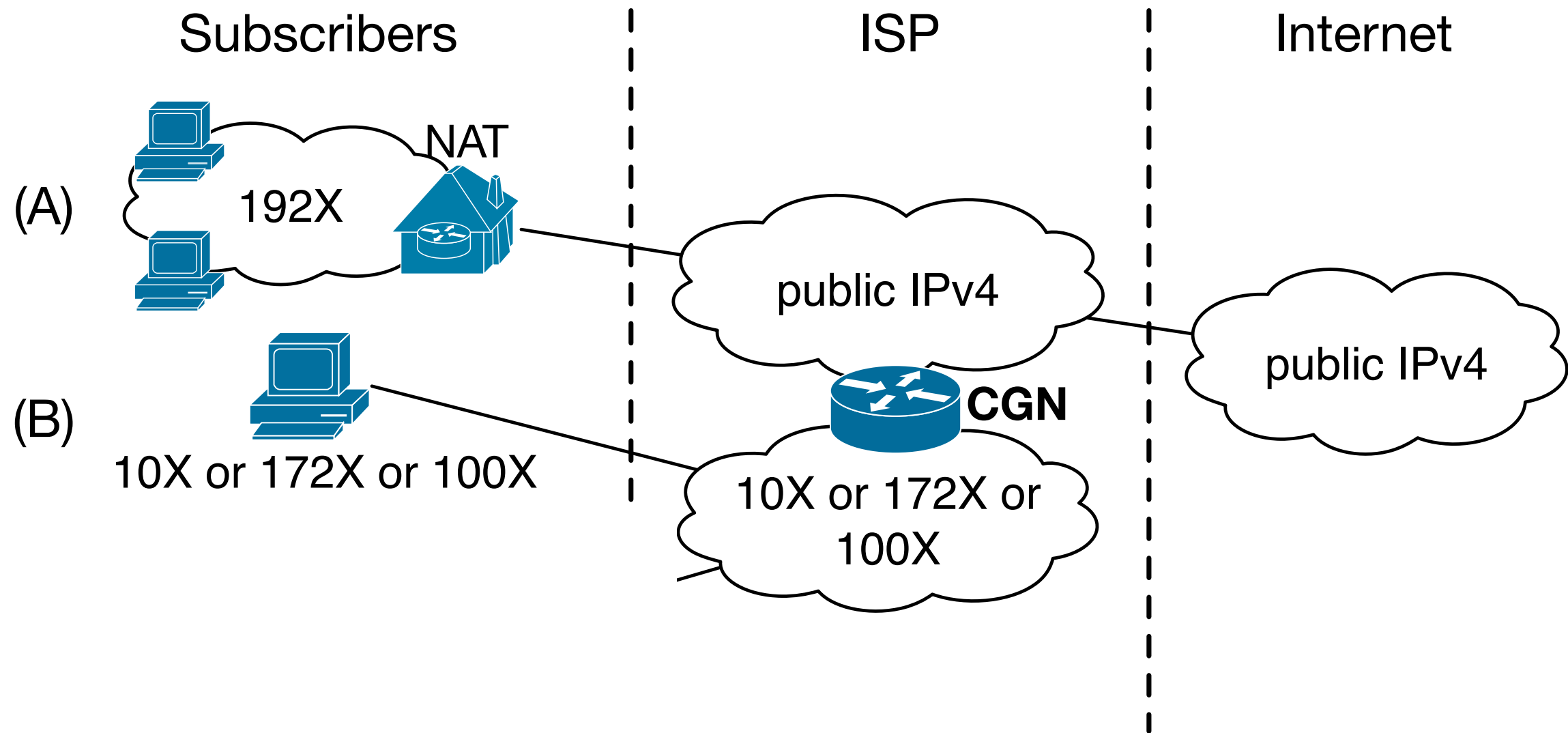
Internet



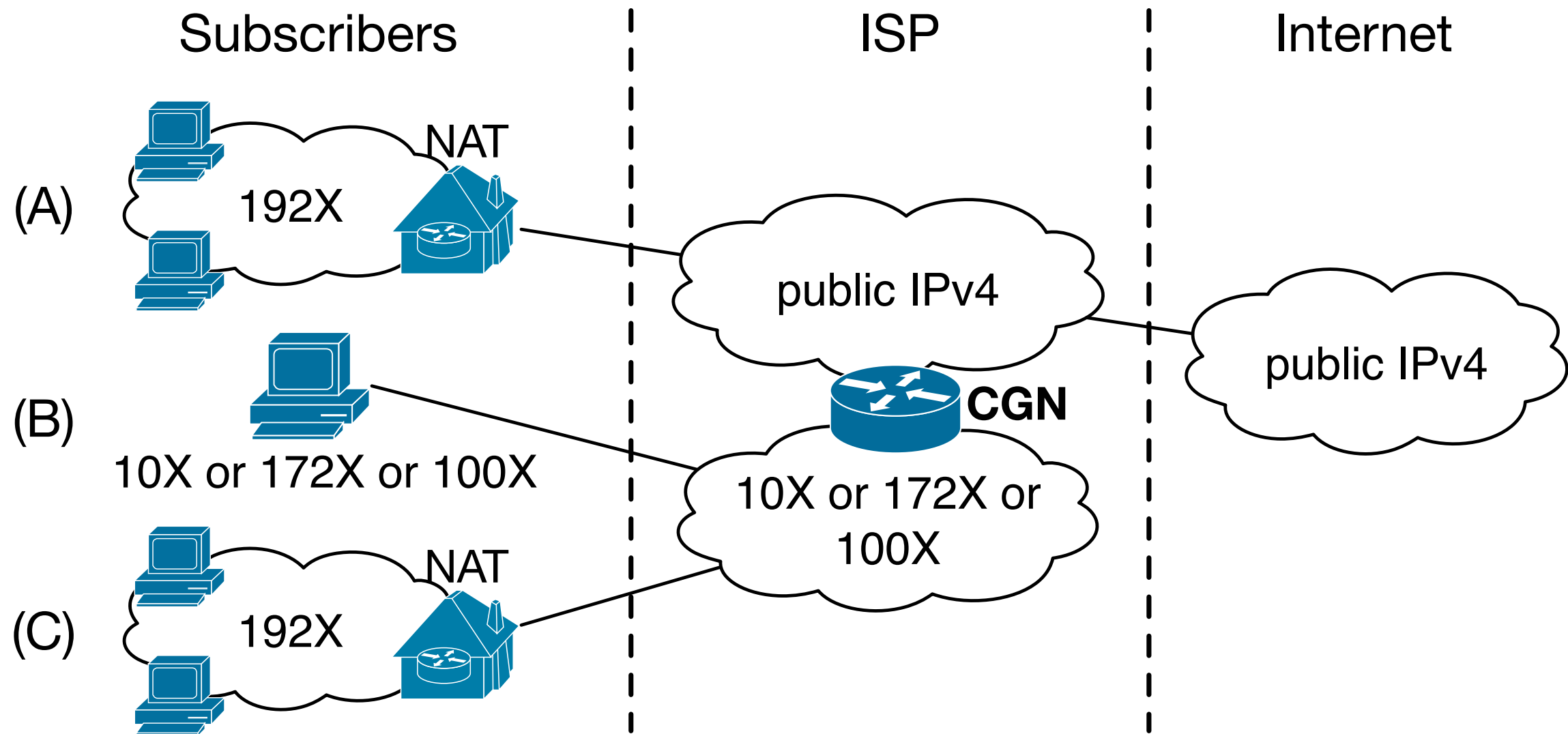
NATs Here ... NATs There!



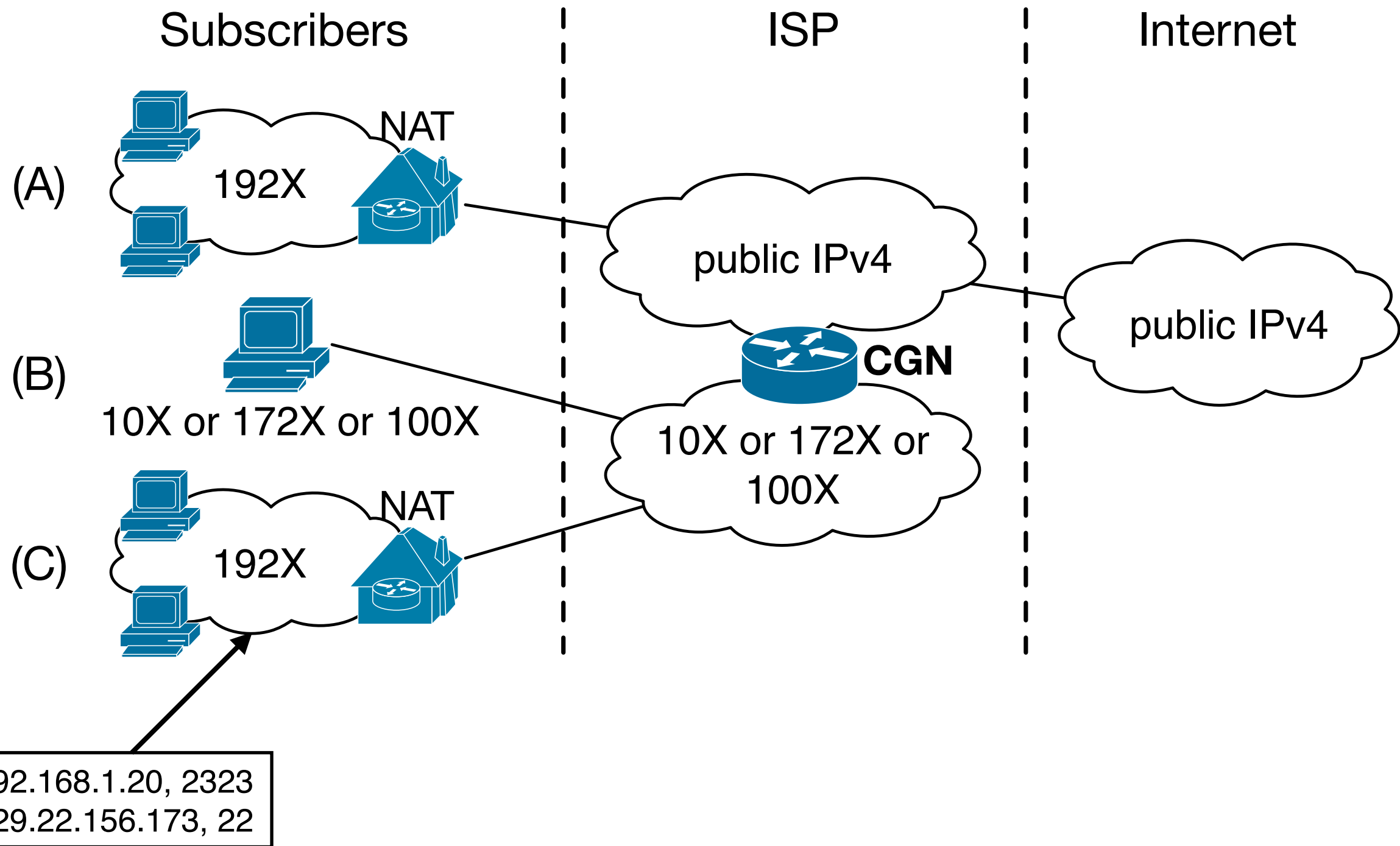
NATs Here ... NATs There!



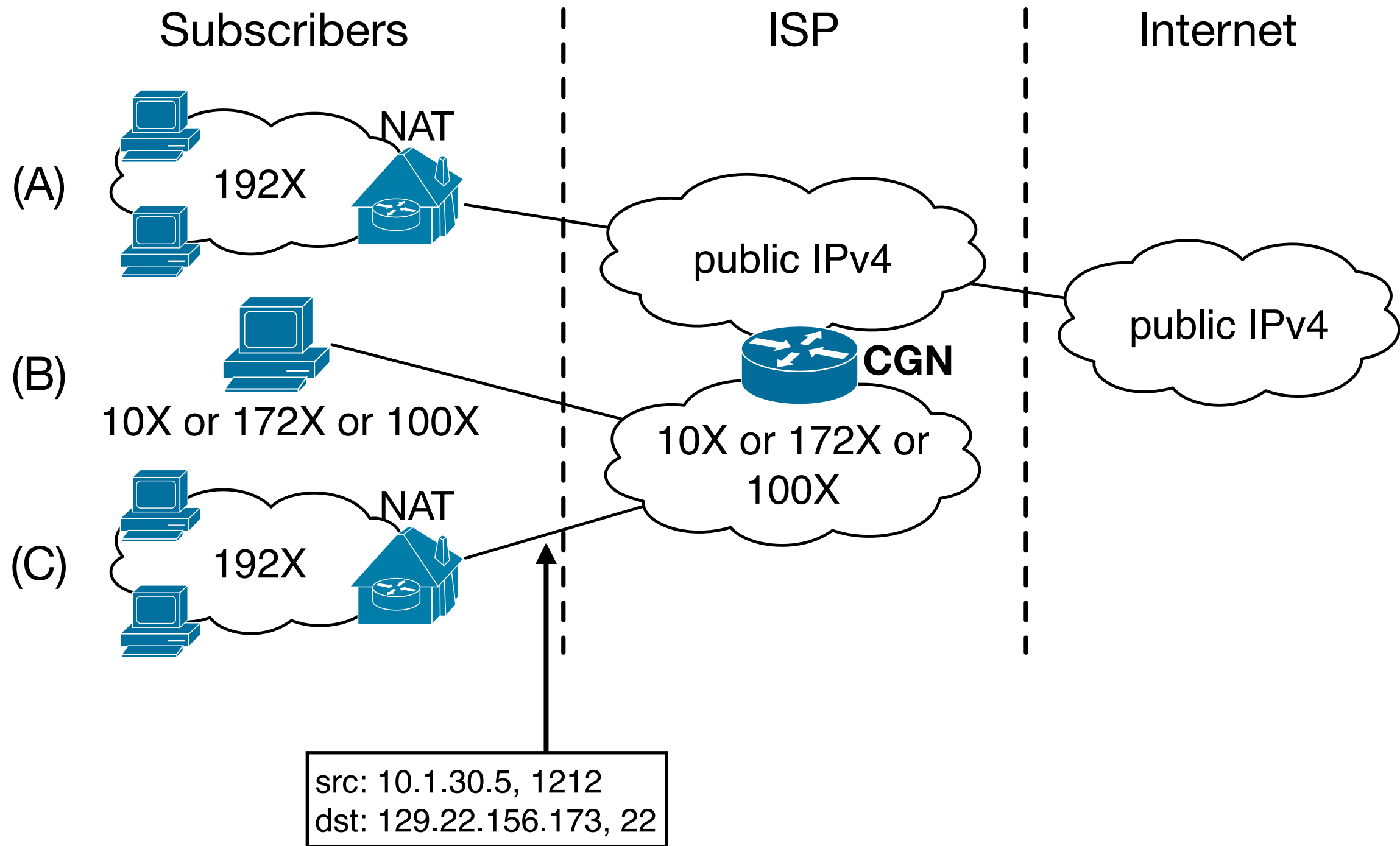
NATs Here ... NATs There!



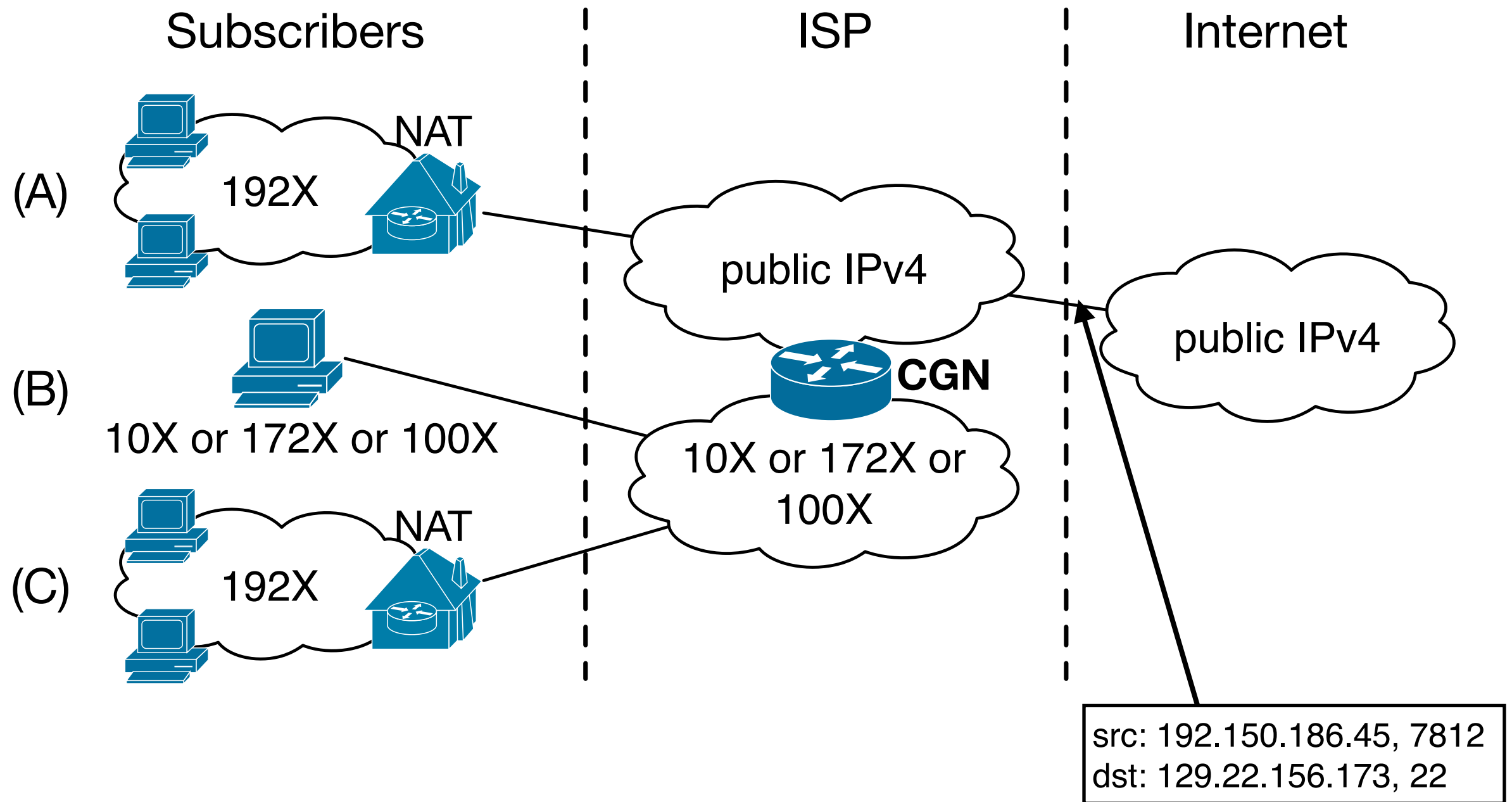
NATs Here ... NATs There!



NATs Here ... NATs There!



NATs Here ... NATs There!

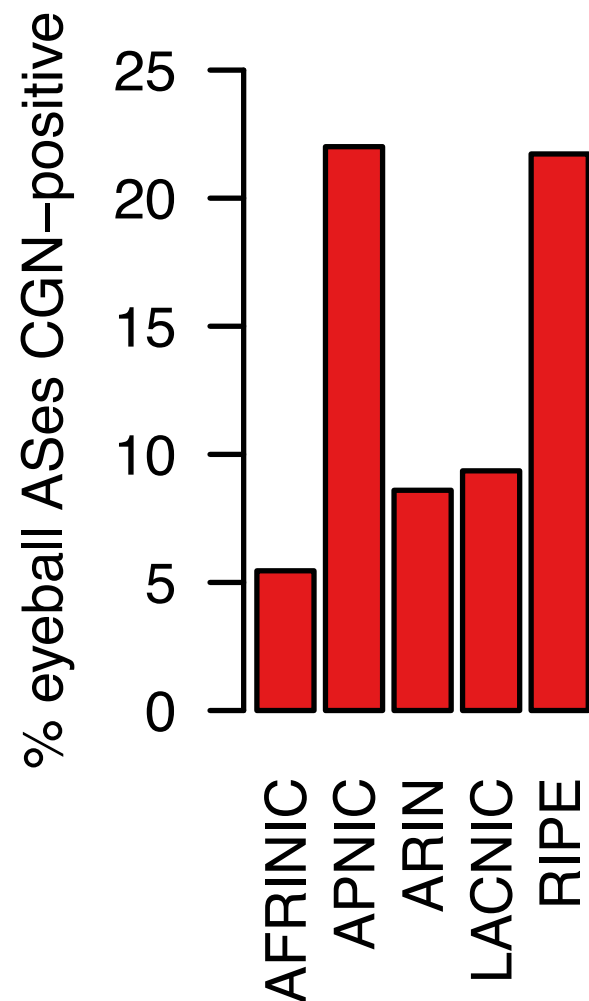


Carrier Grade NAT Deployment

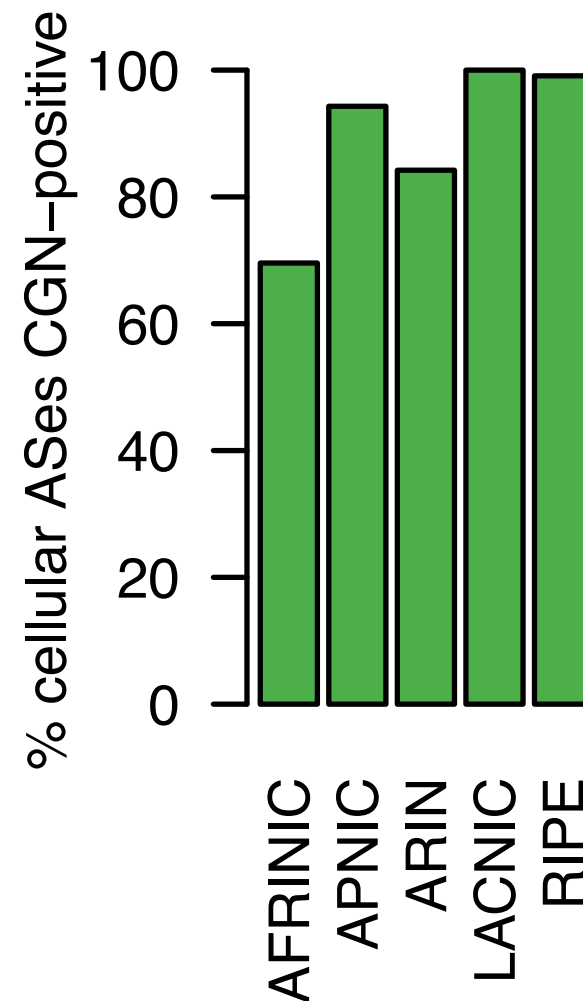
	routed ASes (N=52K)		eyeball ASes, PBL (N=2.9K)		eyeball ASes, APNIC (N=3.1K)	
	covered	CGN-positive	covered	CGN-positive	covered	CGN-positive
BitTorrent	2,724 (5.2%)	254 (9.40%)	1,673 (57.7%)	180 (10.8%)	1,824 (59.6%)	204 (11.2%)
Netalyzr non-cellular	1,367 (2.6%)	195 (14.3%)	866 (29.8%)	151 (17.4%)	929 (30.4%)	174 (18.7%)
BitTorrent \cup Netalyzr	3,166 (6.0%)	421 (13.3%)	1,791 (61.7%)	306 (17.1%)	1,946 (63.6%)	350 (18.0%)
Netalyzr cellular	218 (0.4%)	205 (94.0%)	175 (6.0%)	162 (92.6%)	171 (5.6%)	161 (94.2%)

- ❖ 13-18% of non-cellular eyeball ASes now use CGNs
- ❖ 92-94% of cellular ASes now use CGNs

Carrier Grade NAT Deployment



(b) eyeball ASes
CGN-positive



(c) cellular ASes
CGN-positive

Carrier Grade NAT Deployment

Results from

Philipp Richter, Florian Wohlfart, Narseo Vallina-Rodriguez, Mark Allman, Randy Bush, Anja Feldmann, Christian Kreibich, Nicholas Weaver, Vern Paxson. *A Multi-perspective Analysis of Carrier-Grade NAT Deployment*. ACM Internet Measurement Conference, November 2016.

<http://www.icir.org/mallman/pubs/RWV+16/>

CGNs ... So What?

CGNs ... So What?

❖ Is there a problem with adding CGNs to the mix?

CGNs ... So What?

- ❖ Is there a problem with adding CGNs to the mix?
- ❖ CGNs exacerbate the NAT traversal problem

CGNs ... So What?

- ❖ Is there a problem with adding CGNs to the mix?
- ❖ CGNs exacerbate the NAT traversal problem
 - configuring a port mapping in a local NAT is not enough

CGNs ... So What?

- ❖ Is there a problem with adding CGNs to the mix?
- ❖ CGNs exacerbate the NAT traversal problem
 - configuring a port mapping in a local NAT is not enough
 - configuring a port mapping in a NAT controlled by the ISP is not likely to be allowed

CGNs ... So What?

- ❖ Is there a problem with adding CGNs to the mix?
- ❖ CGNs exacerbate the NAT traversal problem
 - configuring a port mapping in a local NAT is not enough
 - configuring a port mapping in a NAT controlled by the ISP is not likely to be allowed
 - ... which leaves relaying ...

NATs and CGNs ... Summary

NATs and CGNs ... Summary

- ❖ Benefit: extends a finite resource in a backwards compatible way

NATs and CGNs ... Summary

- ❖ Benefit: extends a finite resource in a backwards compatible way
- ❖ Cost: makes reachability more difficult
 - and often impossible

NATs and CGNs ... Summary

- ❖ Benefit: extends a finite resource in a backwards compatible way
- ❖ Cost: makes reachability more difficult
 - and often impossible
 - so much for the dumb middle and the thin waist!