# Some special IP addresses

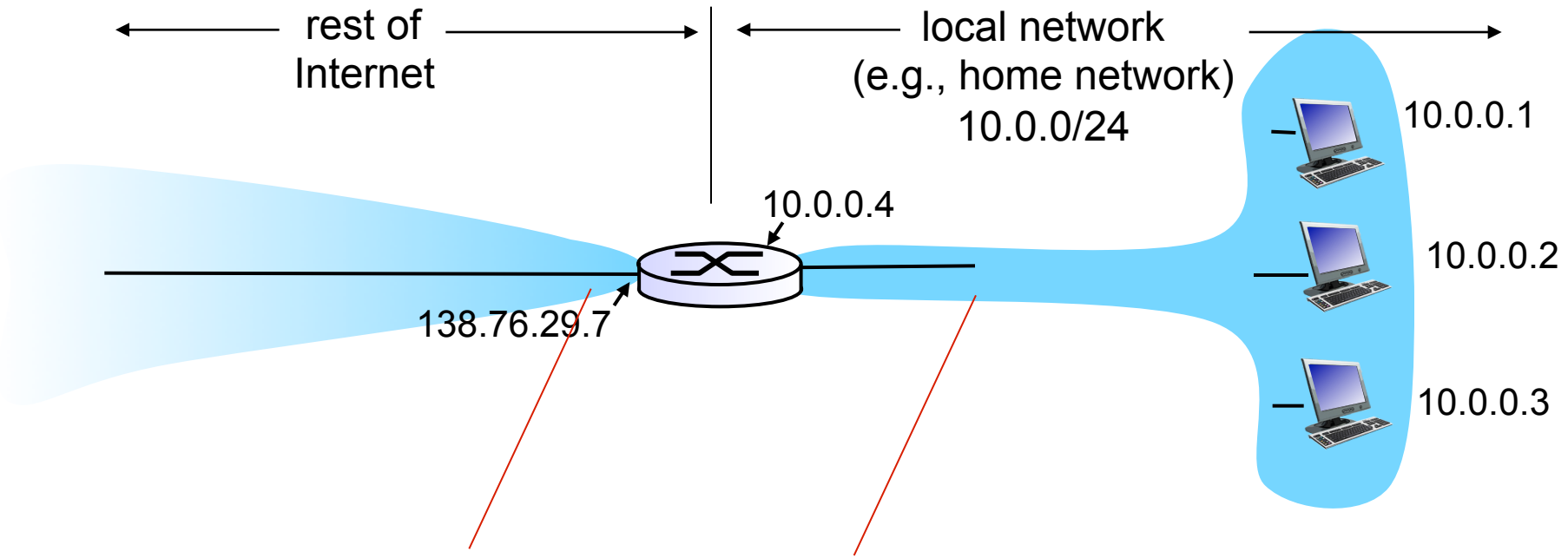
- 127.0.0.1: localhost
- 0.0.0.0: loopback
- IP addresses used for private networks
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - …

# Private networks to the Internet

- How do hosts in private networks, e.g., in your home, communicate with the outside world?

NAT: network address translation

# NAT: network address translation




*all* datagrams *leaving* local network have *same* single source NAT IP address: 138.76.29.7,different source port numbers

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

# NAT: network address translation

*motivation:* local network uses just one IP address as far as outside world is concerned:

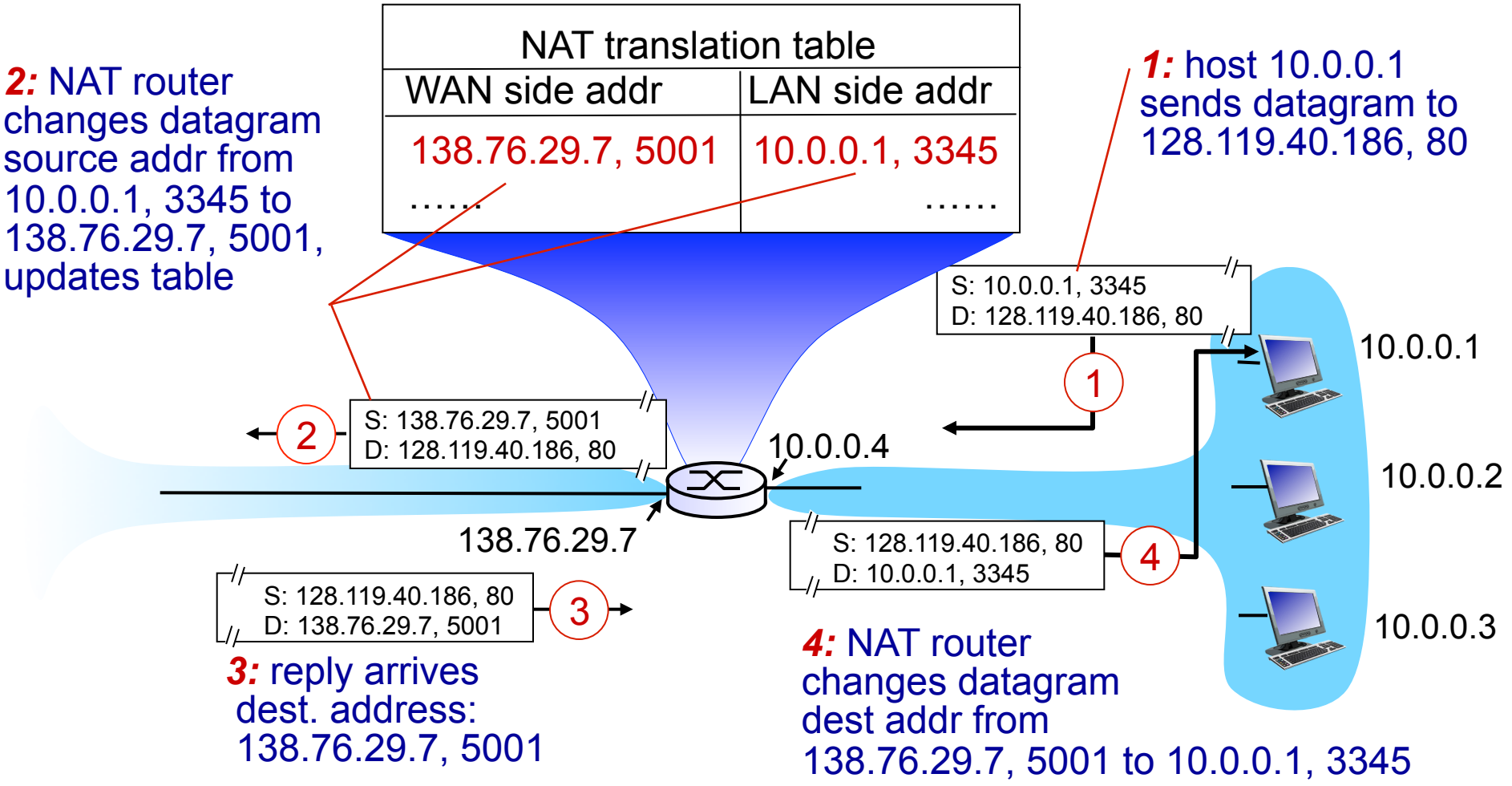
- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible by outside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

# NAT: network address translation

*implementation:* NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
  - . . . remote clients/servers will respond using (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



Assume a host in a local network with IP address of 10.0.0.5 open a TCP connection on port 1234 to connect to a web server at 131.30.123.5 (port 80), what is a possible row for this connection in the NAT translation table?

A. <131.30.123.5,80> ⬅➡ <10.0.0.5, 1234>

B. <138.125.10.10, 5025> ⬅➡ <10.0.0.5, 1234>

C. <10.0.0.5, 1234> ⬅➡ <131.30.123.5,80>

D. <10.0.0.5, 80> ⬅➡ <131.30.123.5,80>

# NAT: network address translation

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

# Can we run a server, e.g. web server within a NAT?

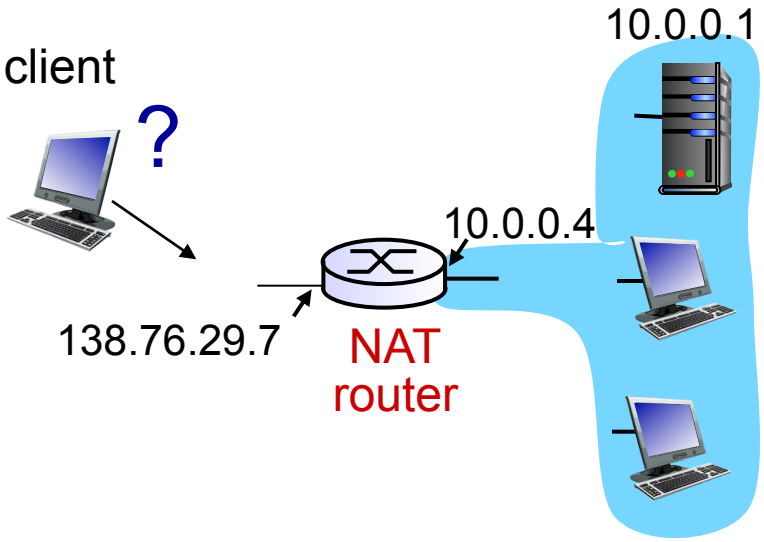
A. Yes

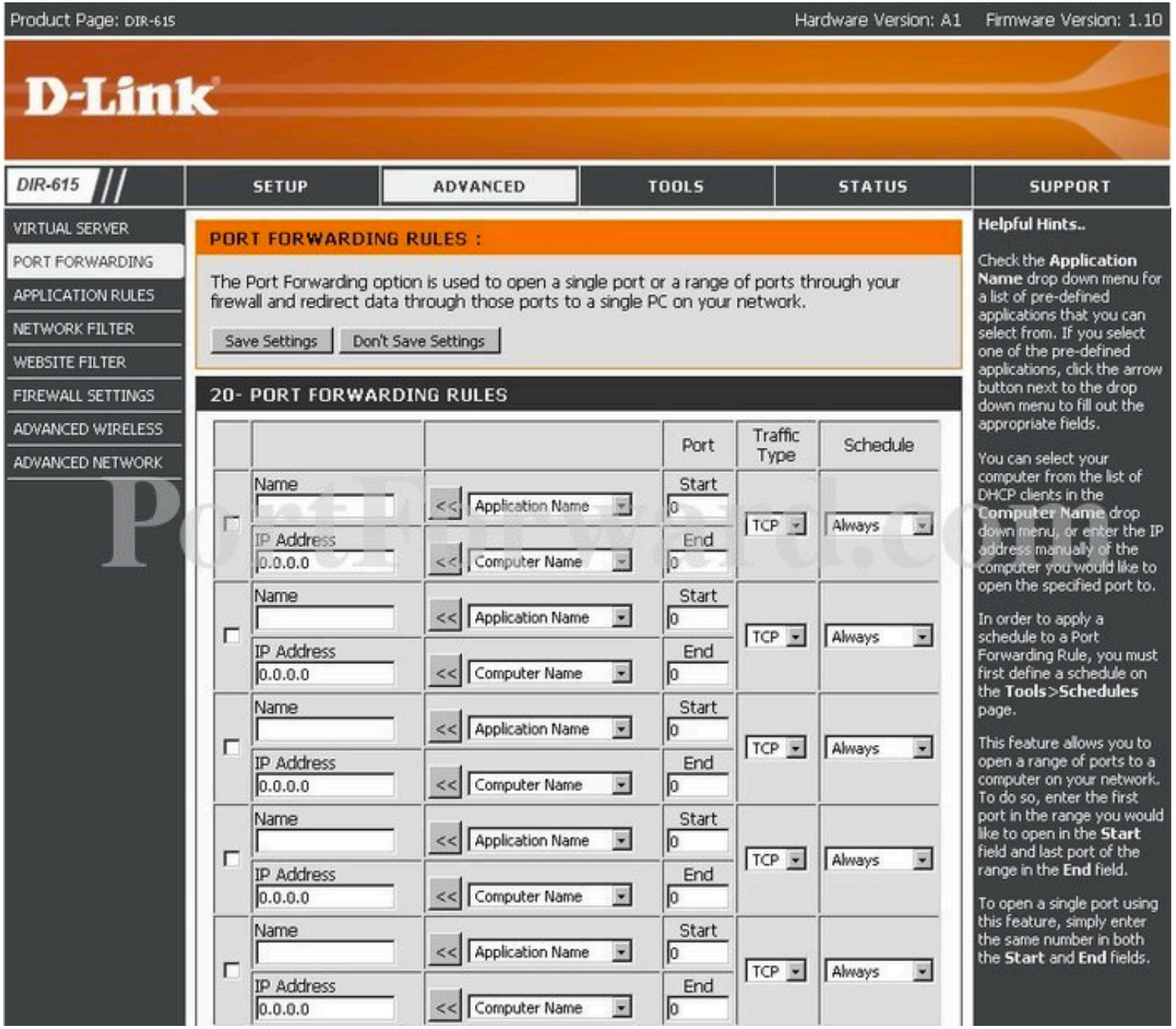
B. Yes, but it can only communicate (send/ receive) with hosts within the private network

C. No

# 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
- *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




Product Page: DIR-615
Hardware Version: A1
Firmware Version: 1.10
D-Link
DIR-615
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
VIRTUAL SERVER
PORT FORWARDING
APPLICATION RULES
NETWORK FILTER
WEBSITE FILTER
FIREWALL SETTINGS
ADVANCED WIRELESS
ADVANCED NETWORK
PORT FORWARDING RULES :
The Port Forwarding option is used to open a single port or a range of ports through your firewall and redirect data through those ports to a single PC on your network.
Save Settings
Don't Save Settings
20- PORT FORWARDING RULES
Name
IP Address
0.0.0.0
Application Name
Computer Name
Port
Start
End
Traffic Type
TCP
Schedule
Always
Helpful Hints..
Check the Application Name drop down menu for a list of pre-defined applications that you can select from. If you select one of the pre-defined applications, click the arrow button next to the drop down menu to fill out the appropriate fields.
You can select your computer from the list of DHCP clients in the Computer Name drop down menu, or enter the IP address manually of the computer you would like to open the specified port to.
In order to apply a schedule to a Port Forwarding Rule, you must first define a schedule on the Tools>Schedules page.
This feature allows you to open a range of ports to a computer on your network. To do so, enter the first port in the range you would like to open in the Start field and last port of the range in the End field.
To open a single port using this feature, simply enter the same number in both the Start and End fields.

# Can a P2P app like BitTorrent run in NATed networks?

A. Yes

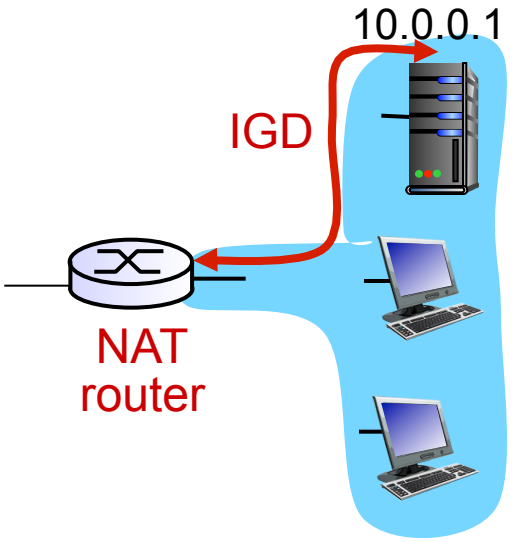
B. Yes, but it can only communicate (send/receive) with hosts within the private network

C. No

# NAT traversal problem

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

  i.e., automate static NAT port map configuration



# Can we run multiple e.g., web servers within a NATed network?

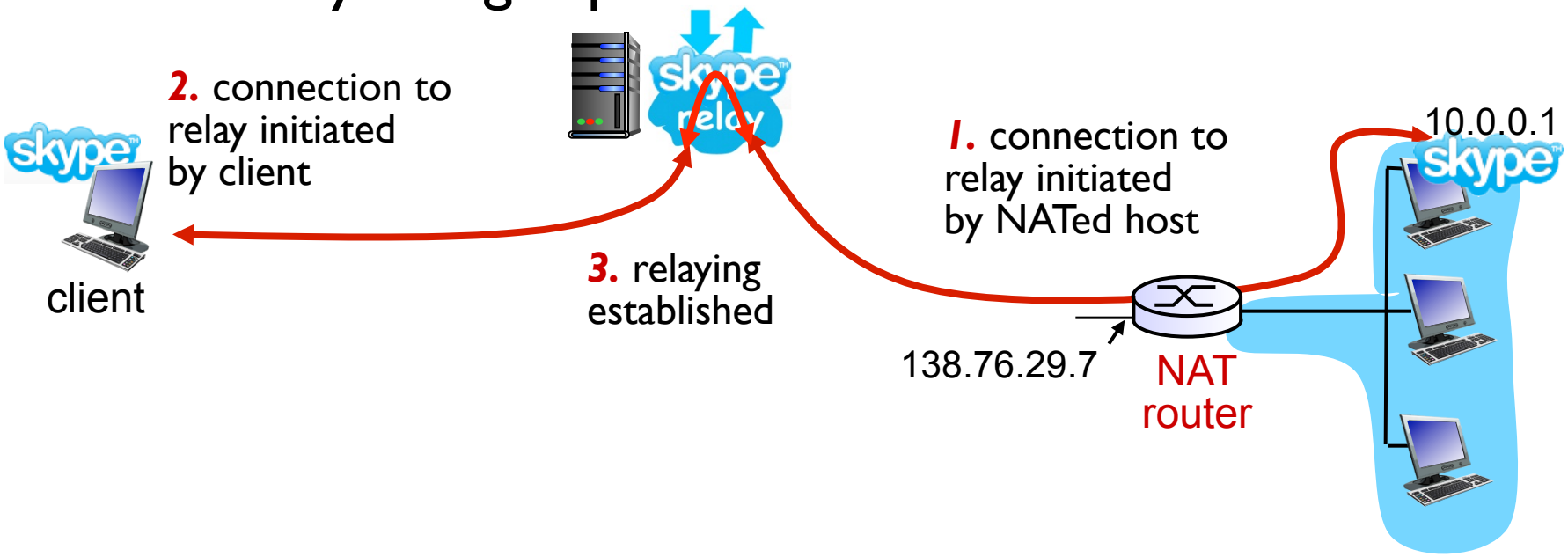
A. Yes

B. No

C. Something else (to be discussed)

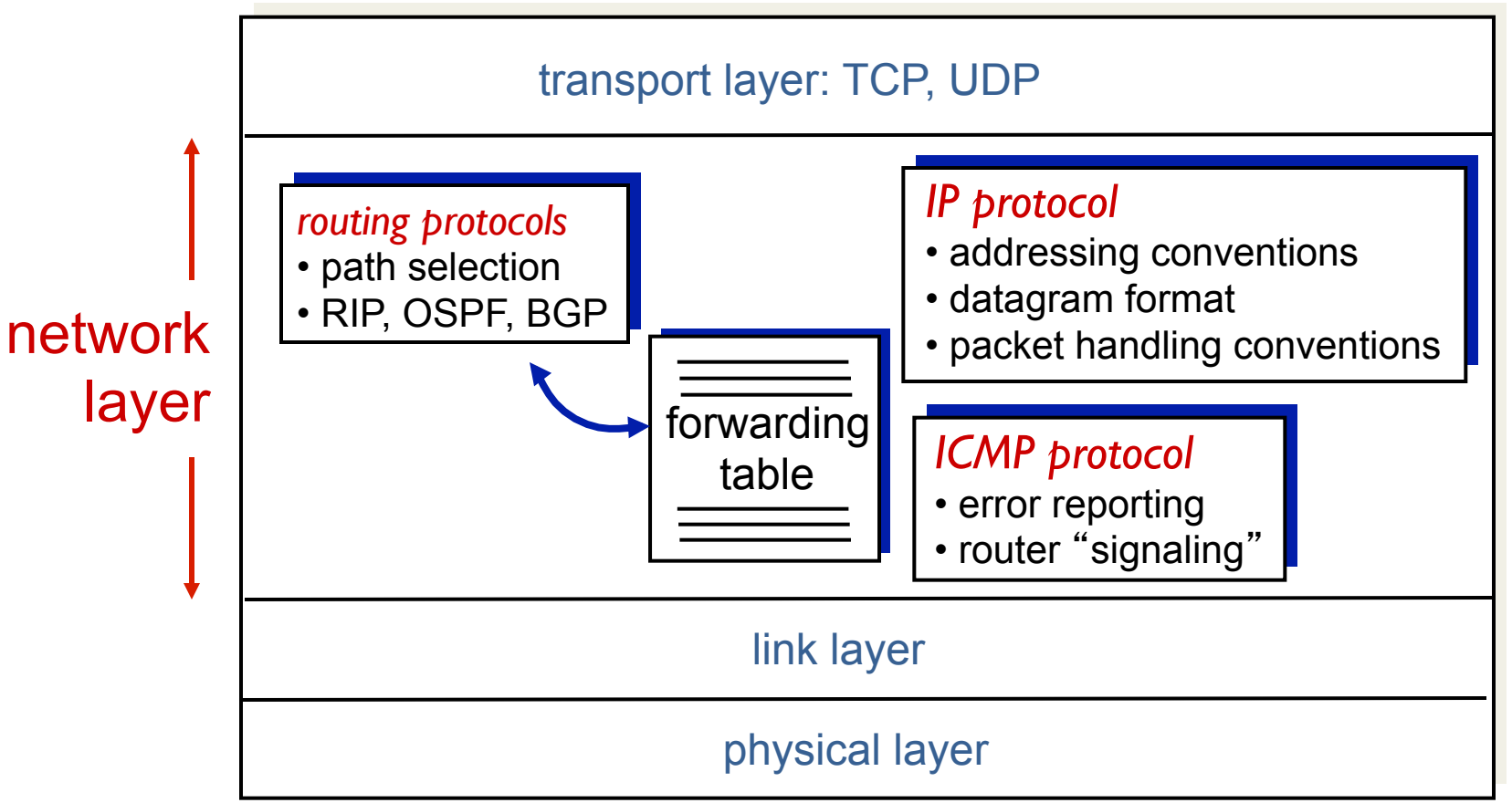
# NAT traversal problem

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



# The Internet network layer

host, router network layer functions:



# ICMP: internet control message protocol

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

| Type | Code | description |
|---|---|---|
| 0 | 0 | echo reply (ping) |
| 3 | 0 | dest. network unreachable |
| 3 | 1 | dest host unreachable |
| 3 | 2 | dest protocol unreachable |
| 3 | 3 | dest port unreachable |
| 3 | 6 | dest network unknown |
| 3 | 7 | dest host unknown |
| 4 | 0 | source quench (congestion control - not used) |
| 8 | 0 | echo request (ping) |
| 9 | 0 | route advertisement |
| 10 | 0 | router discovery |
| 11 | 0 | TTL expired |
| 12 | 0 | bad IP header |

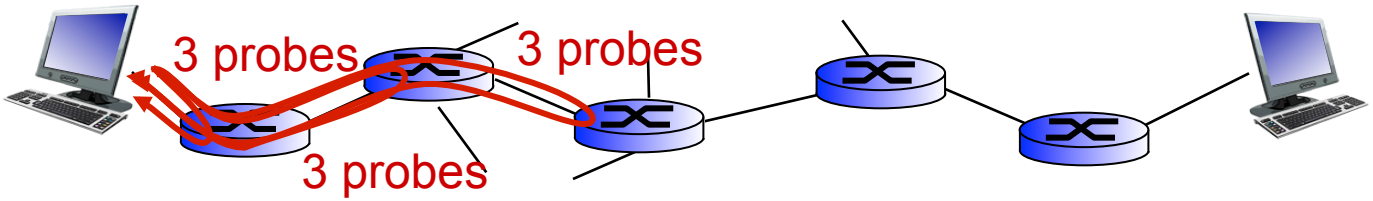
# Traceroute and ICMP

- source sends series of UDP segments to dest
  - first set has TTL =1
  - second set has TTL=2, etc.
  - unlikely port number
- when *n*th set of datagrams arrives to nth router:
  - router discards datagrams
  - and sends source ICMP messages (type 11, code 0)
  - ICMP messages includes name of router & IP address

- when ICMP messages arrives, source records RTTs

*stopping criteria:*

- UDP segment eventually arrives at destination host
- destination returns ICMP "port unreachable" message (type 3, code 3)
- source stops



# Next lecture

- IPv6
  - 4.4.4