NAT Network Address Translation

NAT enables a user to have a large set of addresses internally and one or small set of addresses externally.

- To separate the address used inside and ones used in internet , will be use the private addresses .
- Any organization can use an address of this set without permission from Internet authorities. They are unique inside of organization but they are not unique globally.
- No router will forward a packet that has one these addresses as the destination address.
- The router has to run NAT software.

Range	*Total*
10.0.0.0 to 10.255.255.255	2^{24}
172.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0 to 192.168.255.255	2^{16}

Private addreses

*There are reserved three blocks of the IP address space for **private networks**:*

1 * Class A

*Class A network IP address range = **10.0.0.0 - 10.255.255.255***

For one Class A network: Subnet mask = 255.0.0.0

Network address length = 8 bit ; Computer address length = 24 bit

16 * Class B

Class B network IP address range = 172.16.0.0 - 172.16.255.255

...

Class B network IP address range = 172.31.0.0 - 172.31.255.255

For each of the 16 Class B networks: Subnet mask = 255.255.0.0

Network address length = 16 bit ; Computer address length = 16 bit

*Alternatively, 16 * Class B combined*

*Combined Class B networks IP address range = **172.16.0.0 - 172.31.255.255***

For all 16 Class B networks combined: Subnet mask = 255.240.0.0

Network address length = 12 bit ; Computer address length = 20 bit

256 * Class C

Class C network IP address range = 192.168.0.0 - 192.168.0.255

...

Class C network IP address range = 192.168.255.0 - 192.168.255.255

For each of the 256 Class C networks: Subnet mask = 255.255.255.0

Network address = 24 bit ; Computer address = 8 bit

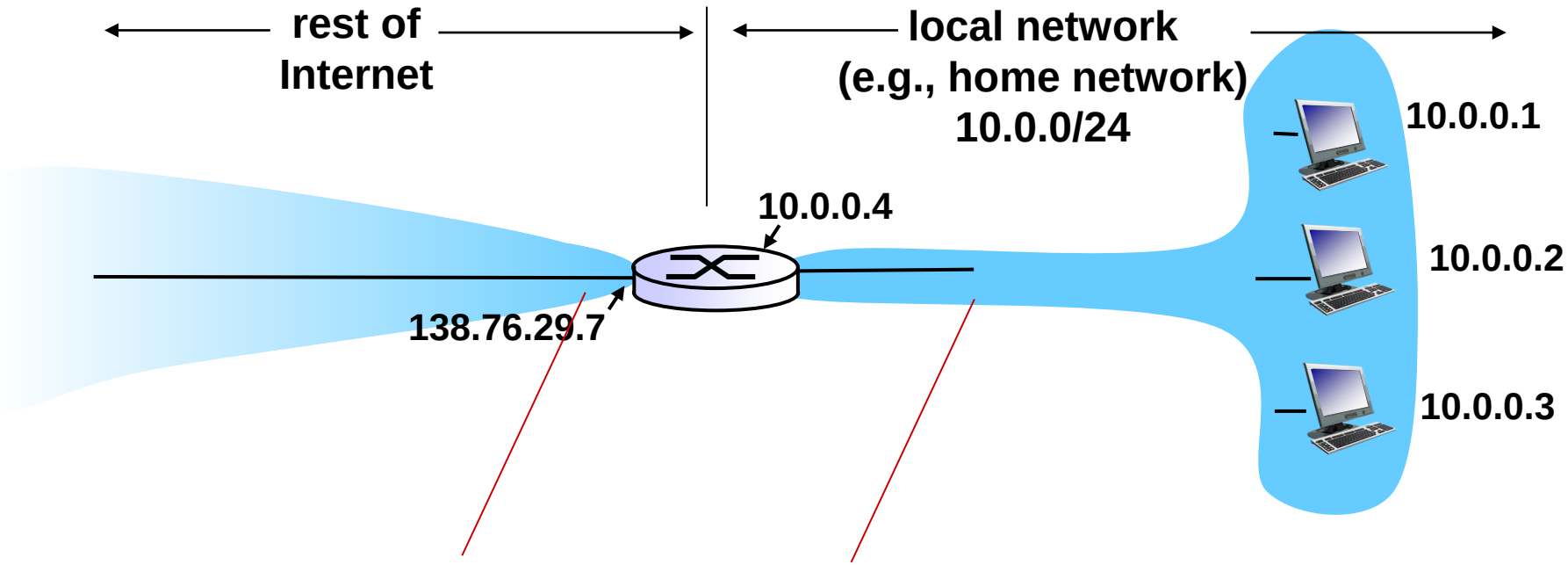
*Alternatively, 256 * Class C combined*

*Combined Class C networks IP address range = **192.168.0.0 - 192.168.255.255***

For all 256 Class C networks combined: Subnet mask = 255.255.0.0

Network address length = 16 bit; Computer address length = 16 bit

NAT: network address translation



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

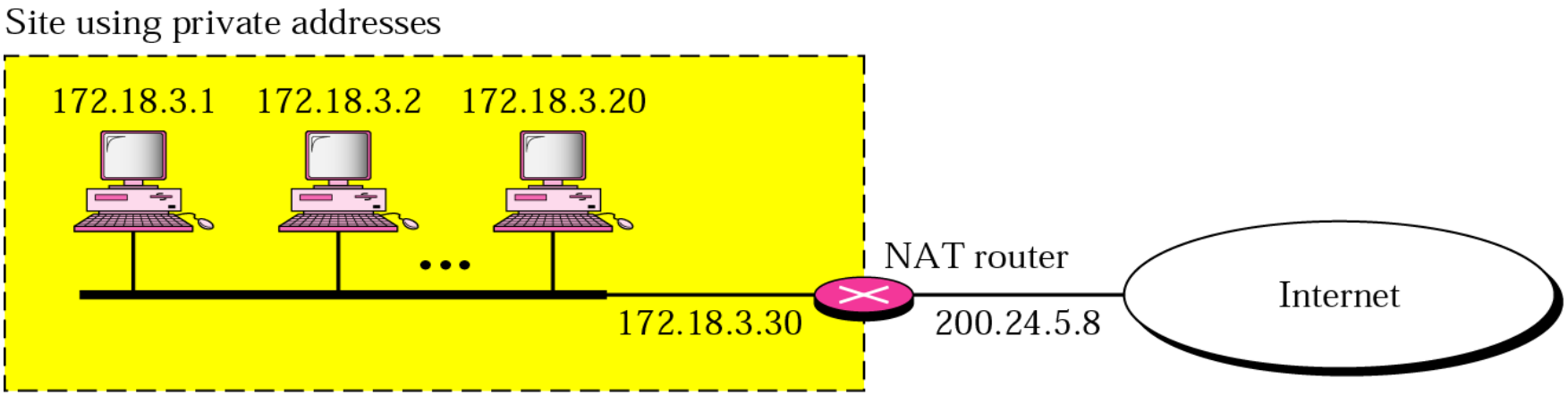
datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT: network address translation

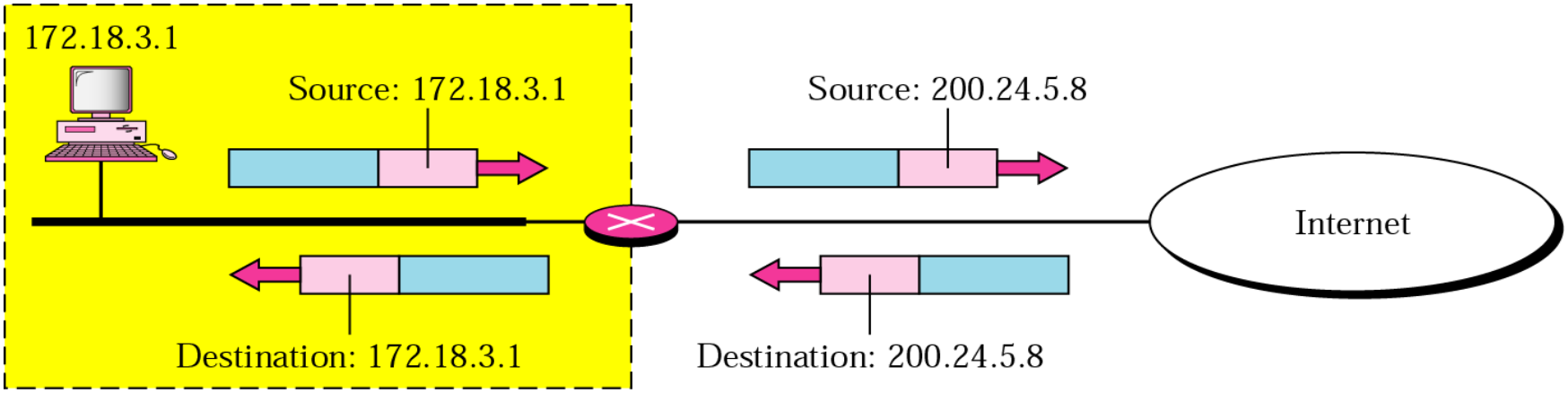
motivation: local network uses **just one IP address** as far as outside world is concerned:

- 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



Address translation

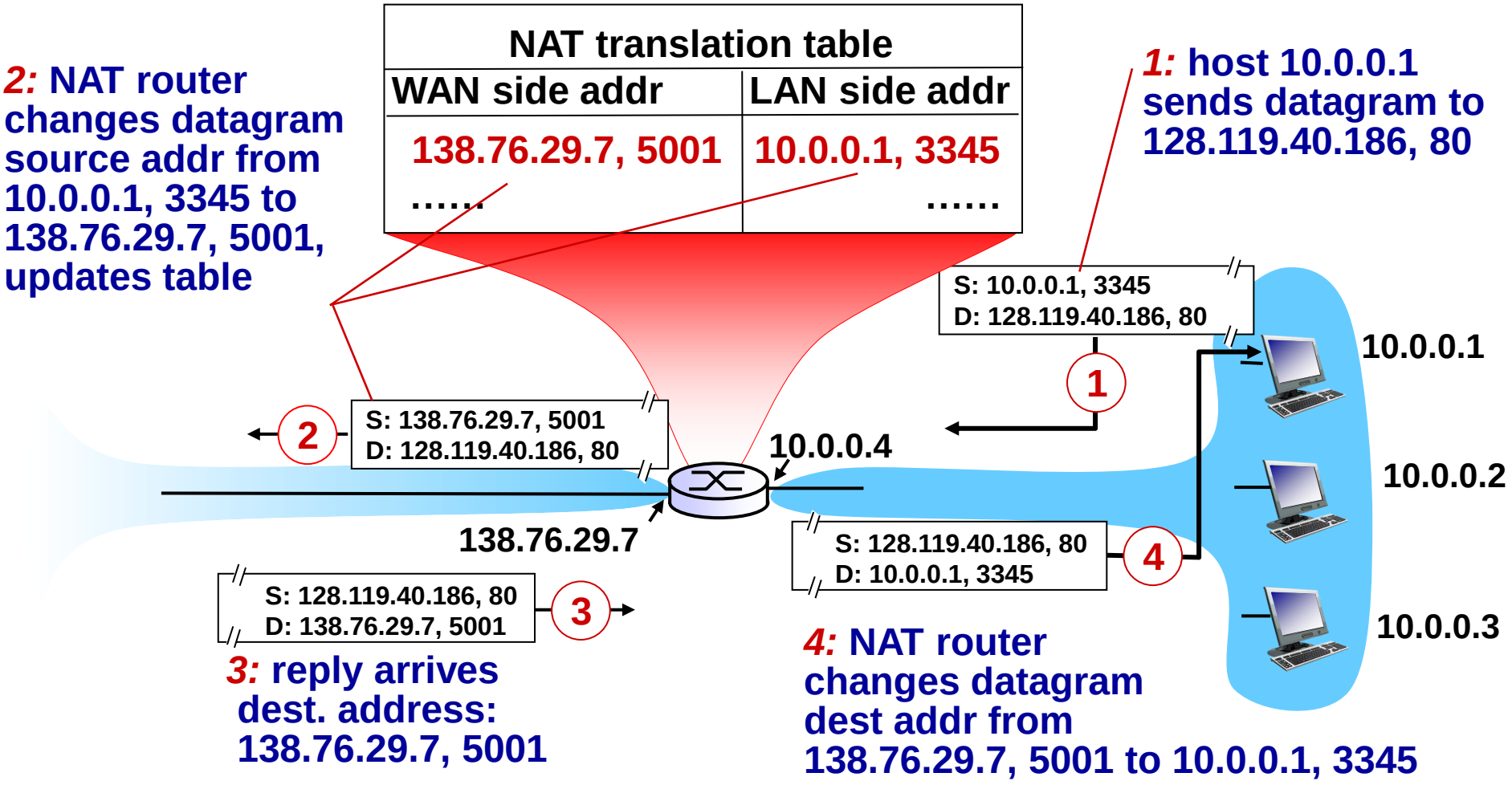


NAT: network address translation

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

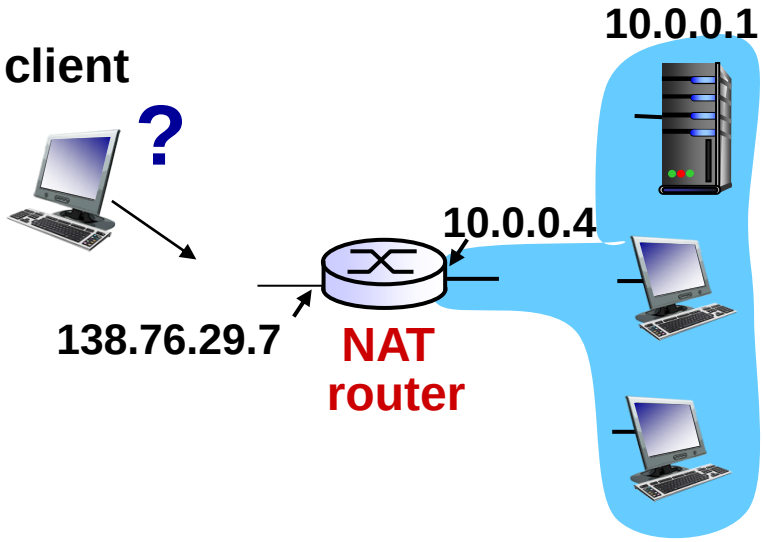


NAT: network address translation

- 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

NAT traversal problem

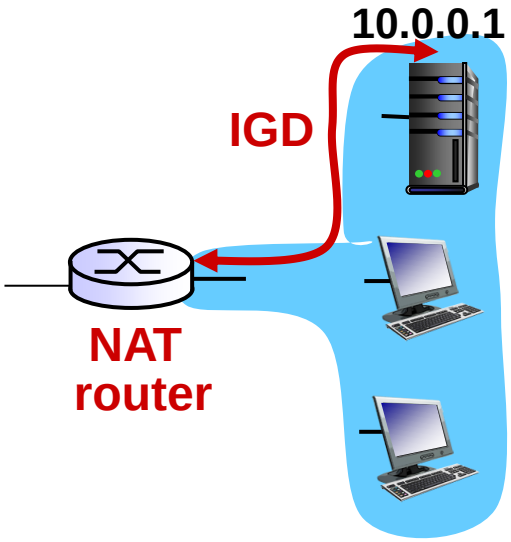
- client wants to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can't use it as destination addr)
  - only one externally visible NATed address: 138.76.29.7



NAT traversal problem

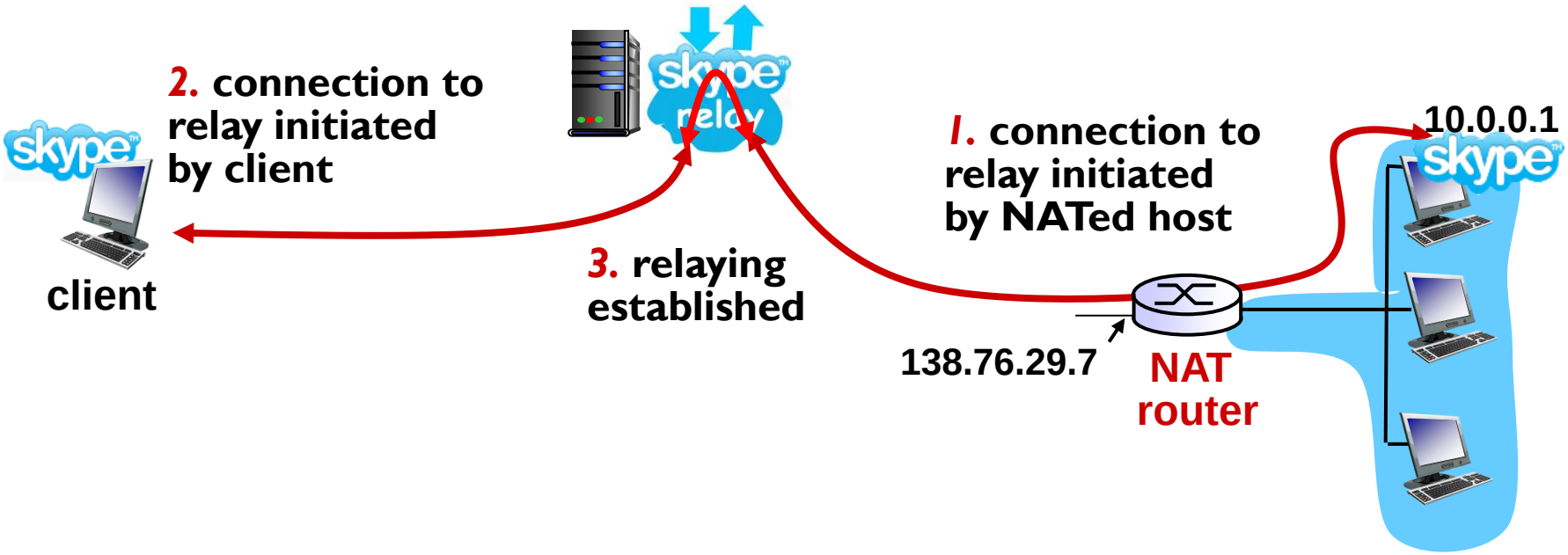
- *solution1:* statically configure NAT to forward incoming connection requests at given port to server
  - e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000
- *solution 2:*
- Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATed host to:
  - learn public IP address (138.76.29.7)
  - add/remove port mappings (with lease times)

  i.e., automate static NAT port map configuration



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



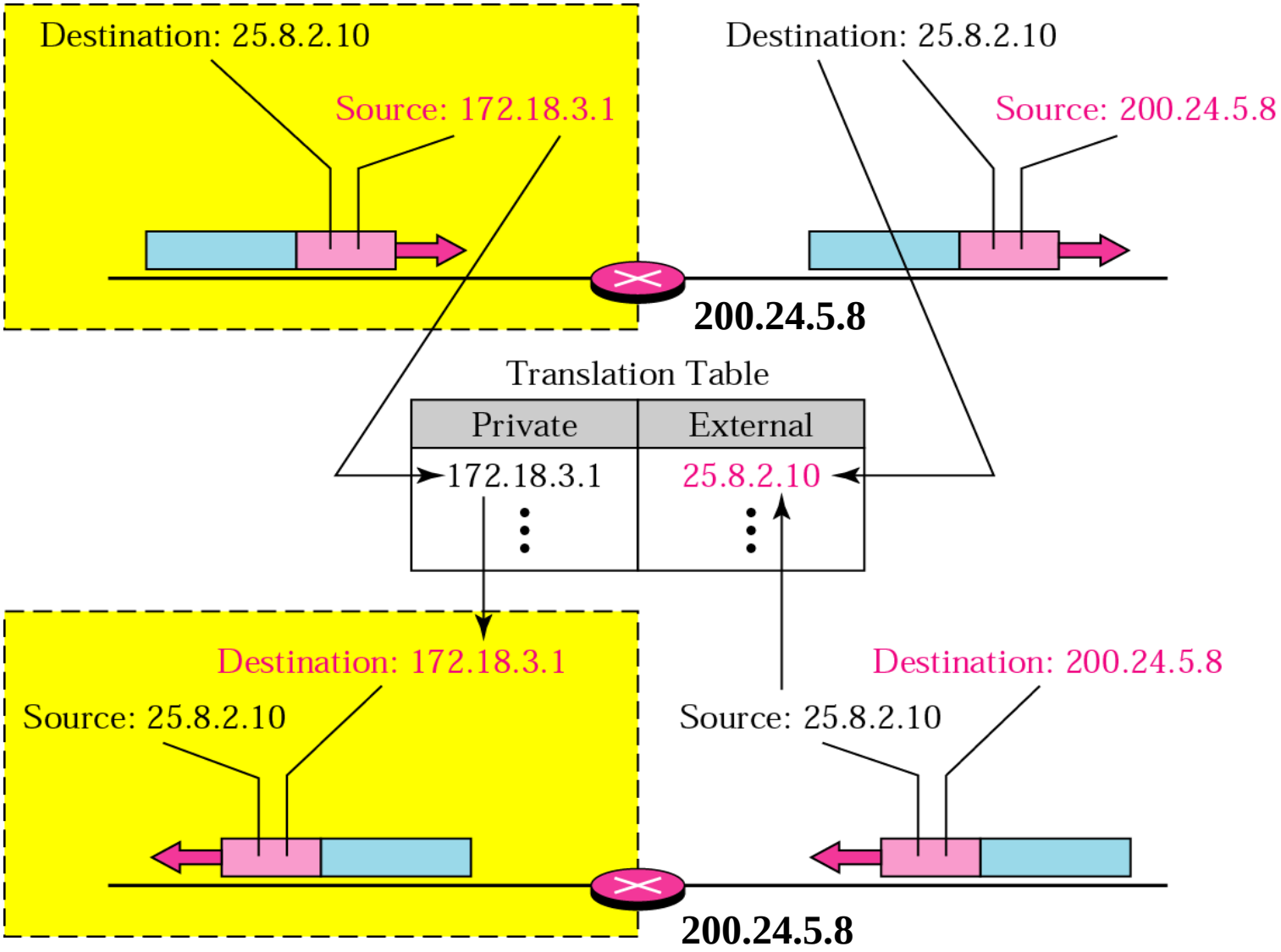
How NAT works

- The network address translation (NAT) process will be active on a router, or firewall security system, that typically connects to the Internet.
- This process on a router, or firewall, is called an application proxy.
- The generic use of the term "application proxy" is when the router/firewall receives a data packet, checks its payload, manipulates it and then redirects it—in short, acts as a middleman.
- NAT performs a one-to-one IP address mapping from a private to a registered "real" IP address.
  - In each data packet that is bound for the Internet, the NAT process looks at the destination and source IP addresses.
  - The process strips off any private addressing and replaces it with one of the "real" registered IP addresses from the pool.
- The NAT process will keep track, through an internal mapping process, of the assigned registered IP addresses to private addresses.
- When the remote Internet server replies, the NAT router receives in inbound Internet packet and re-addresses the packet to the original private address.

How PAT works

- Port Address Translation (PAT) process is similar to NAT process: a registered IP address merely replaces the private address in an outgoing Internet session.
- As both Internet-bound data packets traverse the PAT router, the private source IP addresses (on both packets) are replaced with the singular registered IP address.
- Additionally, the PAT router alters a specific field in the outgoing data packet, the port acknowledgment field.
  - The PAT router tracks the new unique port assignment issued to each of the packets.
  - Both Internet hosts receive their respective packets, reply to the address and then specify the different unique acknowledgment ports.
- The PAT router receives these packets, relates them, and then converts the acknowledgment ports to the original private IP address and original port assignment.

Translation using translation table



Five-column translation table

Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
…	…	…	…	…

Using booth IP Address and PORT numbers

To allow a many to many relationship between private network hosts and external server programs, we need more information in the translation table.

Disadvantages

- **Application limitations:**
- Many new applications have problems negotiating a path across an application proxy such as NAT/PAT.
- As described previously, NAT/PAT functions by replacing the IP addressing portion in the data packet.
- Some of the advanced applications, to function properly, have source-IP addressing buried within the actual data portion (payload) of the data packet.
- The NAT/PAT process doesn't typically check this payload field unless an Application Level Gateway (ALG) function is enabled (if supported). An ALG is designed to allow the proxy process determine what kind of packet is being examined and if the packet's payload needs to be adjusted.

Disadvantages

- H.323 causes a problem with NAT because it uses two Transmission Control Protocol (TCP) connections and several User Datagram Protocol (UDP) sessions for a single call.
- The response IP addressing information needed for the H.323 session is placed within these data packet's payload also causes problems with proper NAT H.323 support mechanisms.
- H.323, further, uses an encoding in the packet's payload called Abstract Syntax Notation (ASN) which is too complex for a standard NAT process to decode.
- H.323 uses ephemeral (dynamic and greater than 1024) ports in its connection call setup process which PAT has difficulty supporting.
- Outside session setup must also be allowed for external network call inquires. This will require static address relation tables or firewall conduits to be constructed which increases the management overhead of supporting H.323 applications through a NAT system.