Dynamic Address Configuration

- Each computer that is attached to the internet must have the following information:
  - IP address
  - Subnet mask
  - IP address of a router
  - IP address of a name server
- This information is usual stored in a configuration file and accessed by the computer during bootstrap process.

DHCP – Dynamic Host Configuration Protocol

- DHCP is a protocol design to provide the information dynamically. DHCP assign address to a host dynamically.
- DHCP is client server program
- Basically DHCP has two databases
  - Database statically binds physical addresses to IP addresses.
  - Database dynamically makes DHCP dynamic
- When a DHCP client request temporary IP address the DHCP server goes to the pool of available unused IP addresses and assign an IP for a negotiable period of time.
- DHCP server first check its static database

DHCP States

- 1. **Initializing state:**
  - The client broadcasts a DHCP_DISCOVER message on its local physical subnet. The DHCP_DISCOVER message may include options that suggest values for the network address and lease duration. BOOTP relay agents may pass the message on to DHCP servers not on the same physical subnet.

- 2. **Selecting State**
  - Each server may respond with a DHCP_OFFER message that includes an available IP address and a lease duration (default 1hour).
  - The server that sends a DHCP_OFFER lock the offered IP address so that it is not available to any other clients. The client chooses one of the offers and sends DHCP_REQUEST message to the selected server.
  - If the client receive no DHCP_OFFER message it tries fore more times, each with a span of 2 sec. If there is no reply to any of these DHCP_DISCOVER the client sleep for 5 min before trying again.

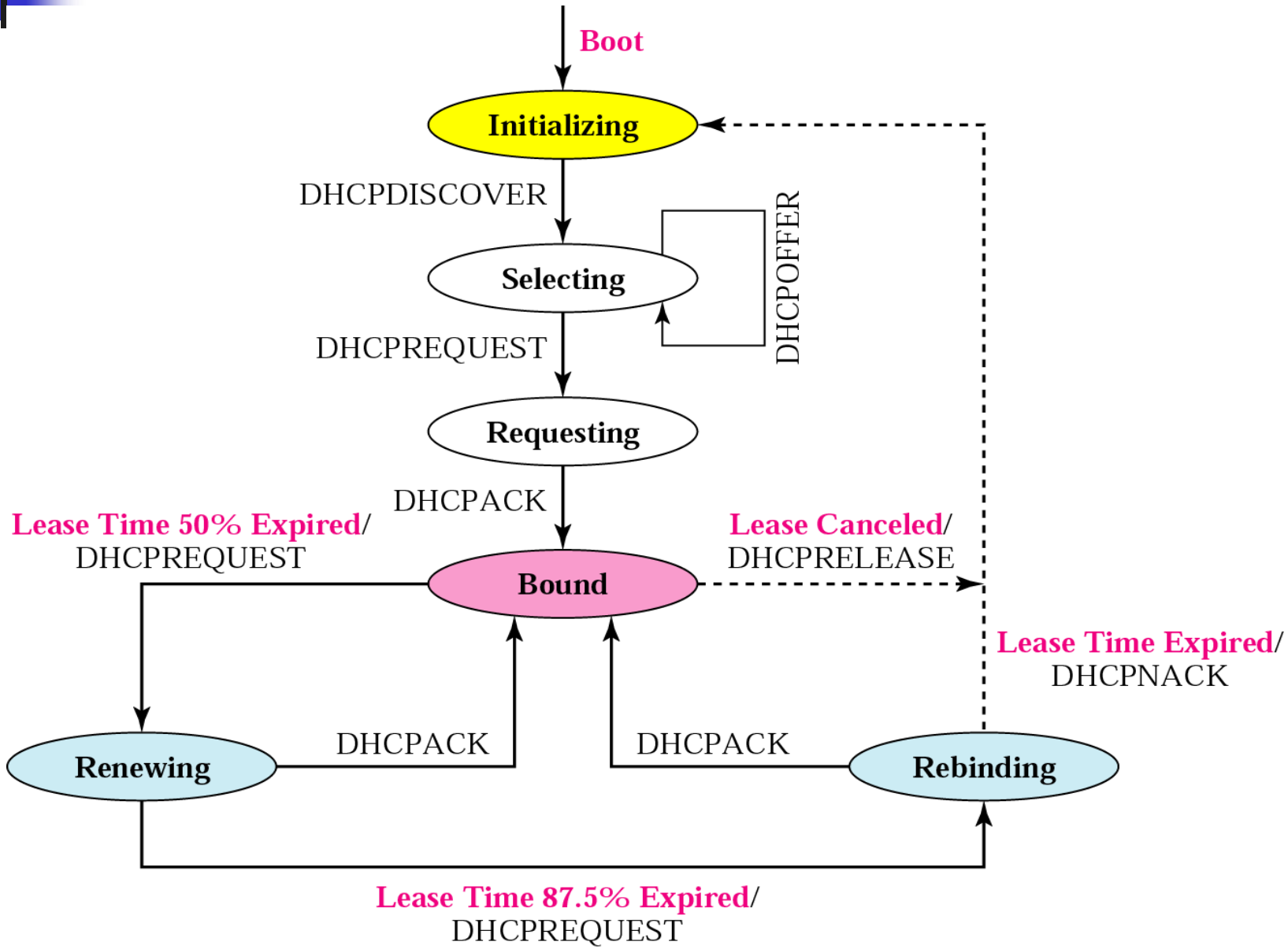
DHCP States cont'

- **3 Requesting State**
  - **The client remains in the requesting state until it receives a DHCP_ACK message from the server which creates the binding between the client's physical address and its IP address.**
- **4 Bound State**
  - **The client use the IP address until the lease expire. When 50% of the lease period is reached the client sends another DCHP_REQUEST to ask for renewal.**
- **5 Renewing State**
  - **The client remains in the renewing state**
  - **If receives a DHCP_ACK renew the lease agreement. Reset the timer and goes back to the bound state**
  - **If DHCP_ACK is not received and 87.5% of the lease time expire the client goes to the rebinding state**
- **6 Rebinding State**
  - **If receives DHCP_NACK or the lease time expires , the client goes back to the Initializing State**
  - **IF receives DHCP_ACK it goes to the bound state and reset the timer.**

DHCP messages

- DHCP_DISCOVER - Client broadcast to locate available servers.
- DHCP_OFFER - Server to client in response to DHCP_DISCOVER with offer of configuration parameters.
- DHCP_REQUEST - Client broadcast to servers requesting offered parameters from one server and implicitly declining offers from all others.
- DHCP_ACK - Server to client with configuration parameters, including committed network address.
- DHCP+NACK - Server to client refusing request for configuration parameters (e.g., requested network address already allocated).
- DHCP_DECLINE - Client to server indicating configuration parameters (e.g., network address) invalid.
- DHCP_RELEASE - Client to server relinquishing network address and canceling remaining lease.

DHCP transition diagram



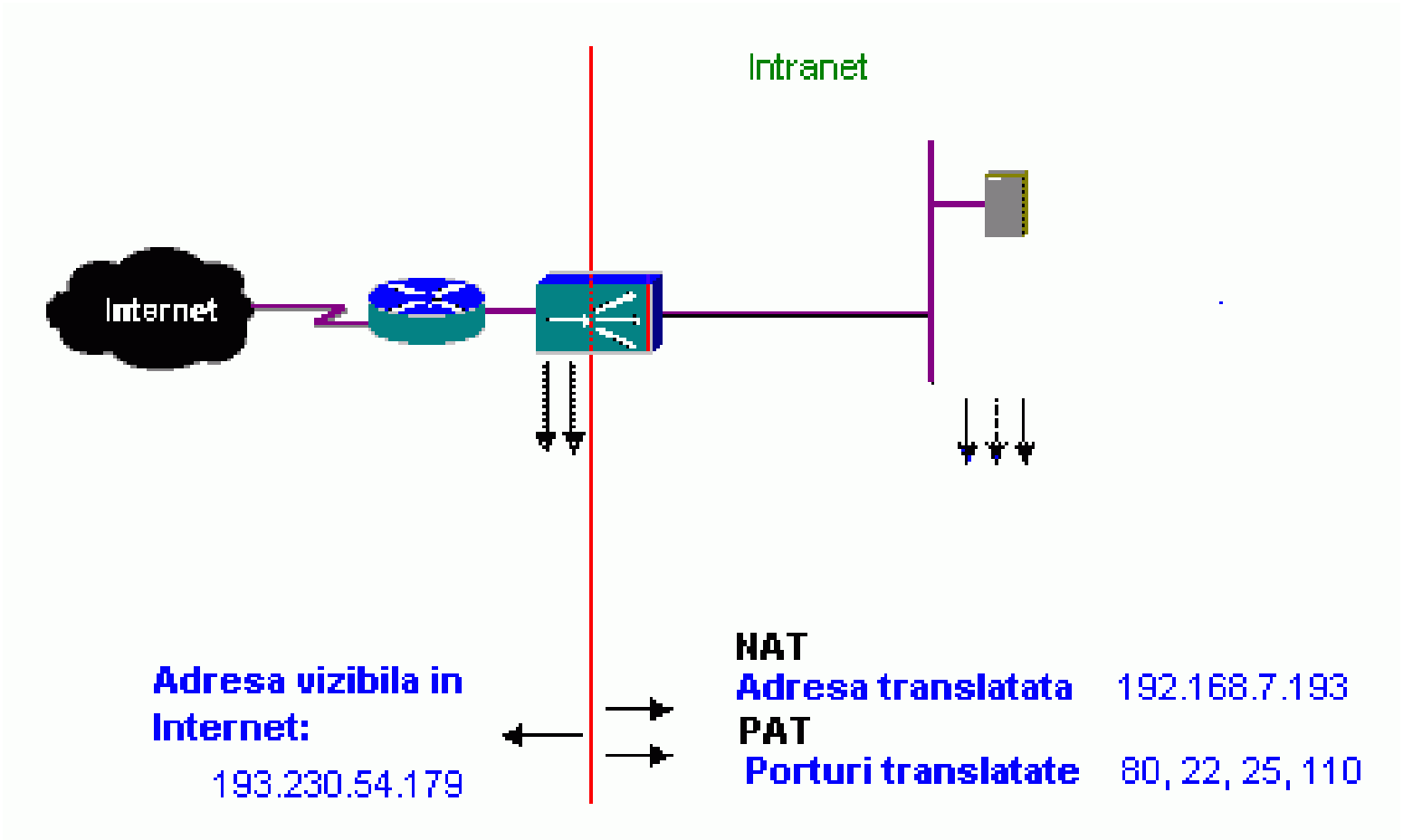
Internet Assigned Number Authority

- The commercialization of the Internet, however, has consumed nearly all of the unique TCP/IP address space. The fact that nearly all private and public entities are moving to establish an Internet connection has created a serious IP address shortage.
- The Internet Assigned Number Authority (IANA), the organization responsible for resolving the problem, proposed to conserve the unique addressing space by blocking out (reserving) a large addressing space (private space) that may be replicated in multiple private local area networks (LANs).
- This pool of set-aside addresses would also be non-routable on the Internet.

NAT / PAT

Network Address Translation/Port Address Translation

- NAT si PAT sunt 2 tehnologii care permit unui echipament - server, router - sa schimbe una sau ambele adrese IP folosite in tranzactie.
- In Internet, doua masini interconectate prin protocolul TCP/IP au fiecare adrese unice, ceea ce permite rutarea traficului intre ele.
- Adresele se regasesc in antetul fiecarui pachet rutat in Internet.


Intranet
Internet
Adresa vizibila in Internet:
193.230.54.179
NAT
Adresa translatata 192.168.7.193
PAT
Porturi translatate 80, 22, 25, 110

- Prin NAT se schimba la plecare, una din adrese, in alta adresa unica. La returul traficului, adresa schimbata, se reface pentru a ajunge la masina originala. Se poate astfel:
  - asigura un prim nivel de securitate - adresa reala IP a unei masini, nu e cunoscuta in afara
  - economisi adrese pretioase IP, ascunzand in spatele routerului care face NAT, o intreaga retea, translatata in exterior printr-o singura adresa, sau un grup de adrese.
- Prin PAT, se schimba portul TCP/IP adresat unei masini din spatele routerului, in alt port, cunoscut numai in interiorul retelei. Se realizeza astfel:
  - un al doilea nivel de redirectare, ca masura de securitate
  - se permite accesul din Internet, la o masina aflata in spatele routerului, pe anumite porturi
- Folosite combinat, cele 2 tehnologii permit ascunderea unei intregi retele interioare, in spatele unei singure adrese IP, sau grup de adrese IP, vizibile in Internet, cu asigurarea accesului dinspre Internet, spre anumite masini din reteaua interioara, pentru care se permite accesul (servere Web, E-mail, Ftp, etc.).

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}

How NAT works

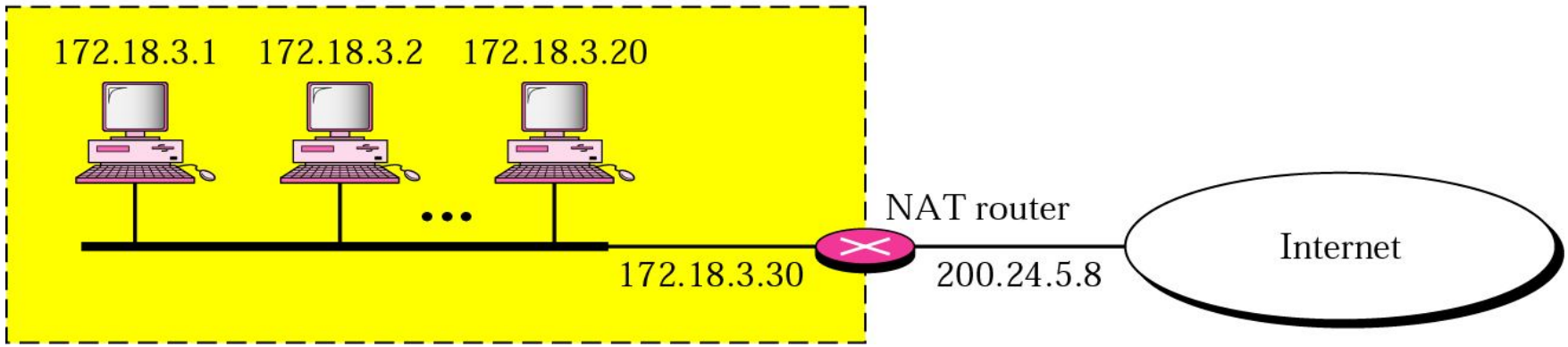
- The network address translation (NAT) process will be active on a router, or firewall security system, that typically connects to the Internet.
- This process on a router, or firewall, is called an application proxy.
- The generic use of the term "application proxy" is when the router/firewall receives 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

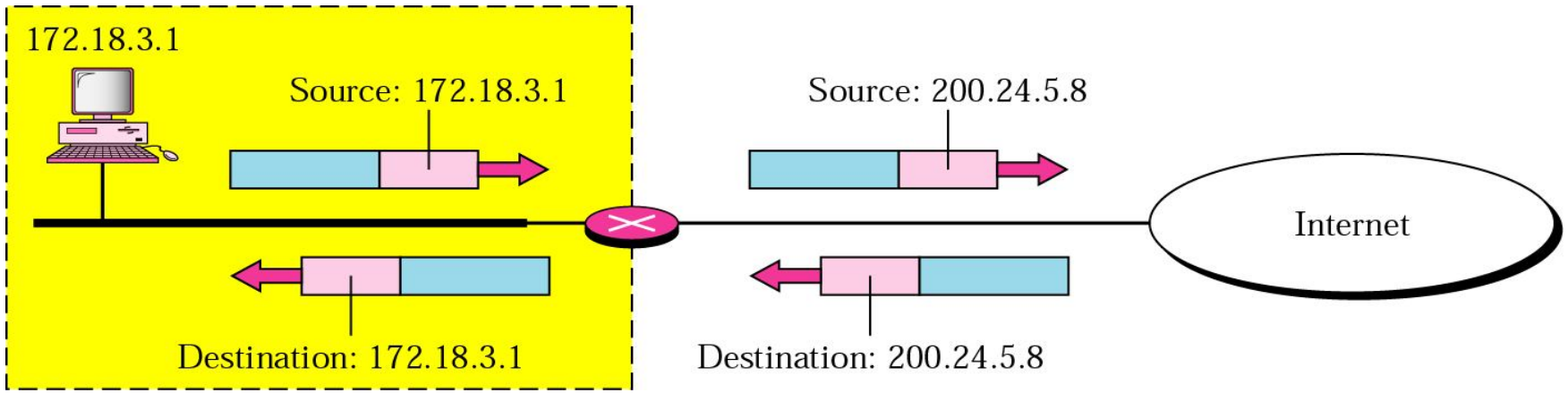
- Port Address Translation (PAT) process is similar to NAT process: a registered IP address merely replaces the private address in an outgoing Internet session.
- As both Internet-bound data packets traverse the PAT router, the private source IP addresses (on both packets) are replaced with the singular 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.

NAT

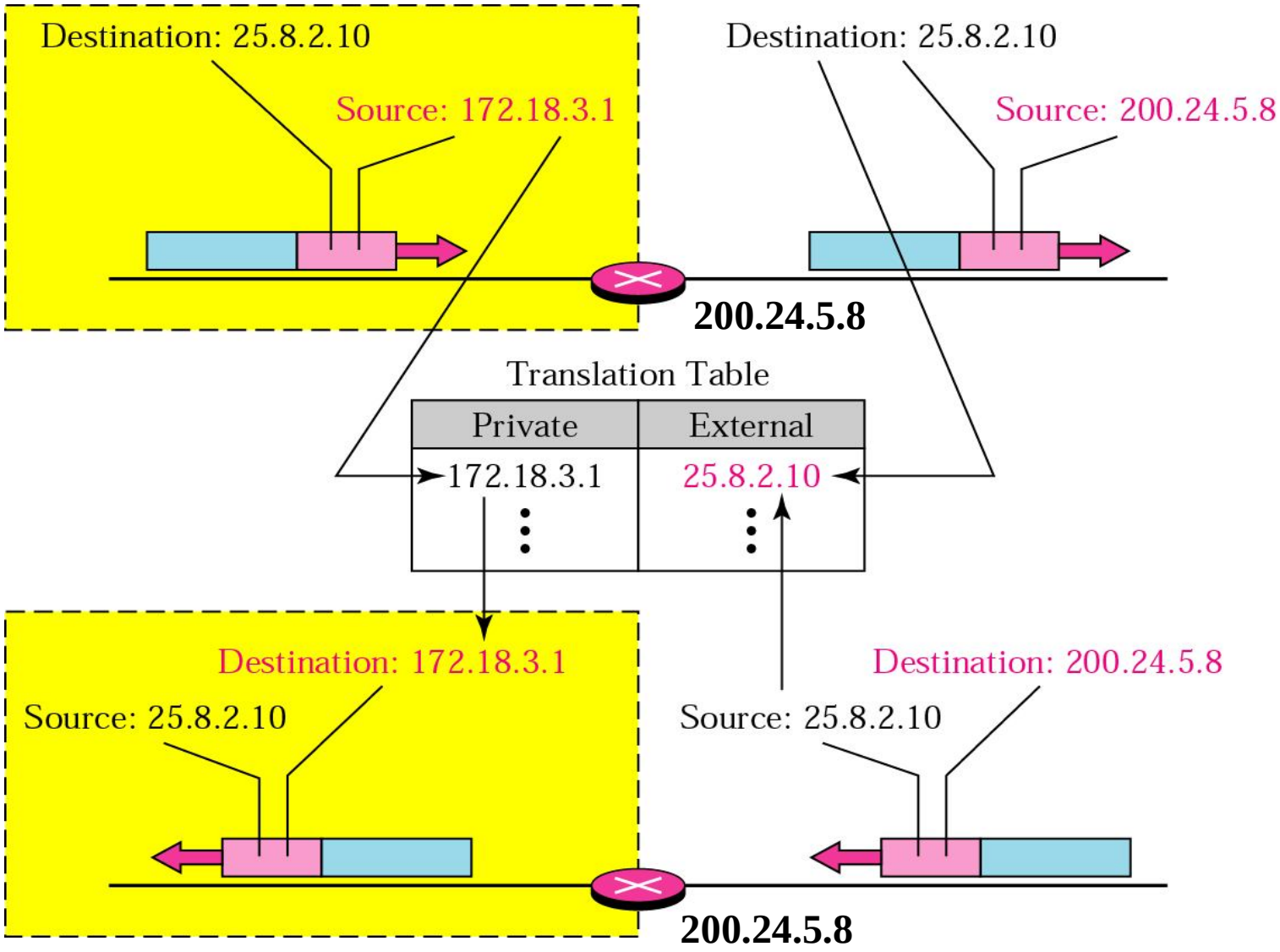
Site using private addresses



Address translation



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.