Network Layer (3): Network Address Translation (NAT)

Required reading:
Kurose – Section 4.3.4

EECS 3214, Winter 2020
Instructor: N. Vlajic

Network Address Translation – NAT

Network Address Translation (NAT) – allows a number of hosts in a private network to share a single (limited number of) globally valid IP addresses

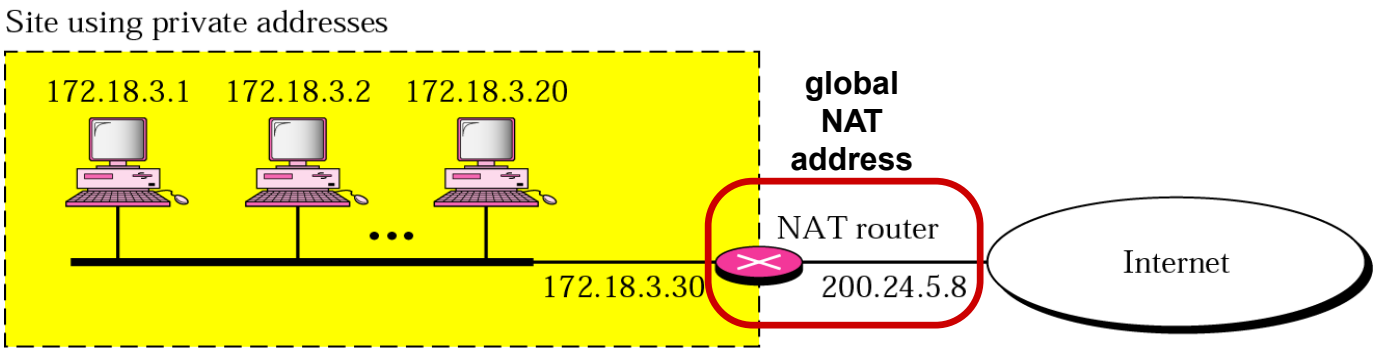
- individual host addresses are unique inside private network, but they are not unique globally!

NAT Advantages

(1) host addresses in private network can be changed and new computers added without notifying outside world ☺

(2) ISP can be changed without changing host addresses in private network ☺

(3) local devices are not explicitly visible or addressable from outside (improved security+!) ☺

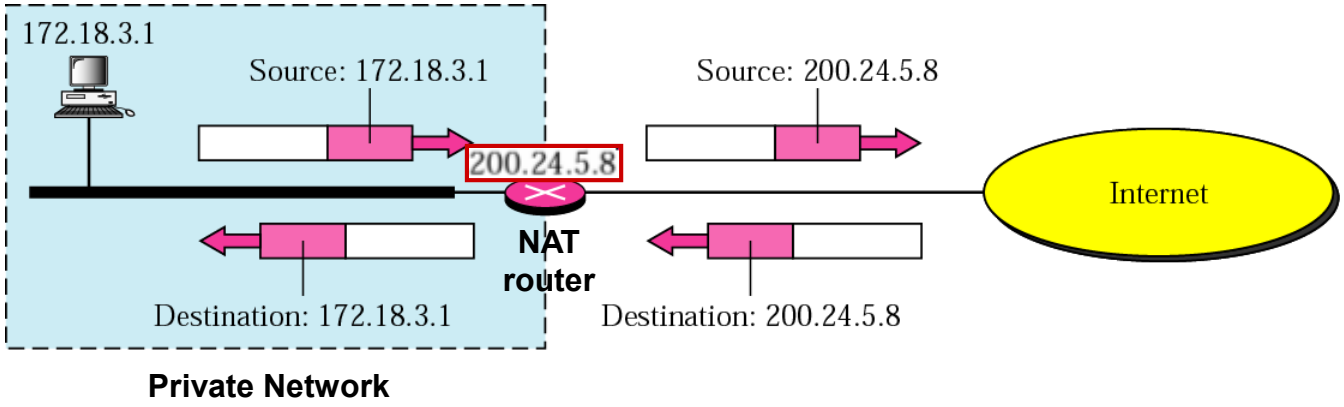


Network Address Translation (cont.)

Address Translation – **minimum set of operations performed by NAT router**

(1) replace the *source address* of all outgoing packets with the *global NAT address*

(2) replace the *destination address* of all incoming packets with the appropriate *private address*



Translating the source address for an outgoing packet is straightforward.

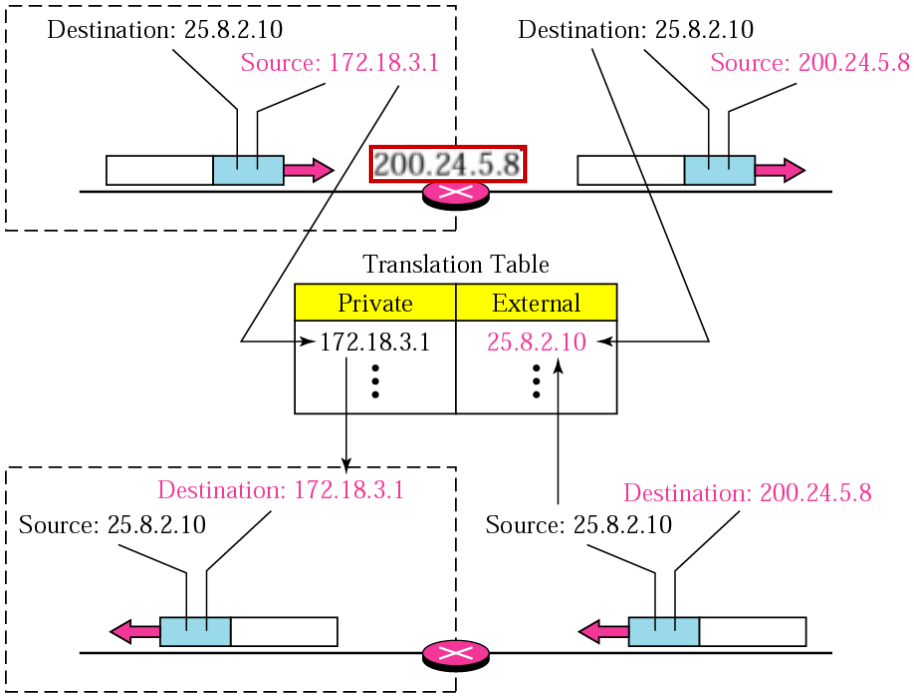
But, how does the NAT router know the destination address for a packet coming from the Internet?!

There may be tens or hundred of private addresses sharing a single globally valid address.

Network Address Translation (cont.)

NAT Tables – **NAT routers create translation tables "on the fly" (dynamically)**

- **in simplest form, a translation table has two columns: the private and external / destination address – when an outgoing packet is received an entry is made in the table if one does not exist already**
- **when response comes back from the destination, router looks up source address in translation tables to find corresponding private address of the packet**
- **unused entry are removed after an idle timeout, e.g. 2-3 minutes**



What if there is the same applications running between 2 different sources, inside NAT, and the same destination?!

What if there are 2 copies of the same application running between the same source and the same destination?!!!

Network Address Translation (cont.)

NAT Table Entries

each table entry uniquely identified with corresponding port number

Source Computer Address	Source Computer Port	NAT Router's IP	NAT Router's Port	Destination Computer Address	Destination Computer Port	Transport Protocol
172.18.3.1	1400	200.24.5.8	5001	25.8.3.2	80	TCP
172.18.3.1	1401	200.24.5.8	5002	25.8.3.2	80	TCP
172.18.3.2	1400	200.24.5.8	5003	25.8.3.2	80	TCP
...	...			...	...	...

(1) The router receives an IP/TCP packet from a computer on the NAT domain.

(2.a) In the IP packet/header router replaces the sending computer's non-routable IP address with the router's IP address.

(2.b) The router generates a new port number and uses it to replaces the sending computer's source port number in the TCP packet/header. (unique identifier for this connection!)

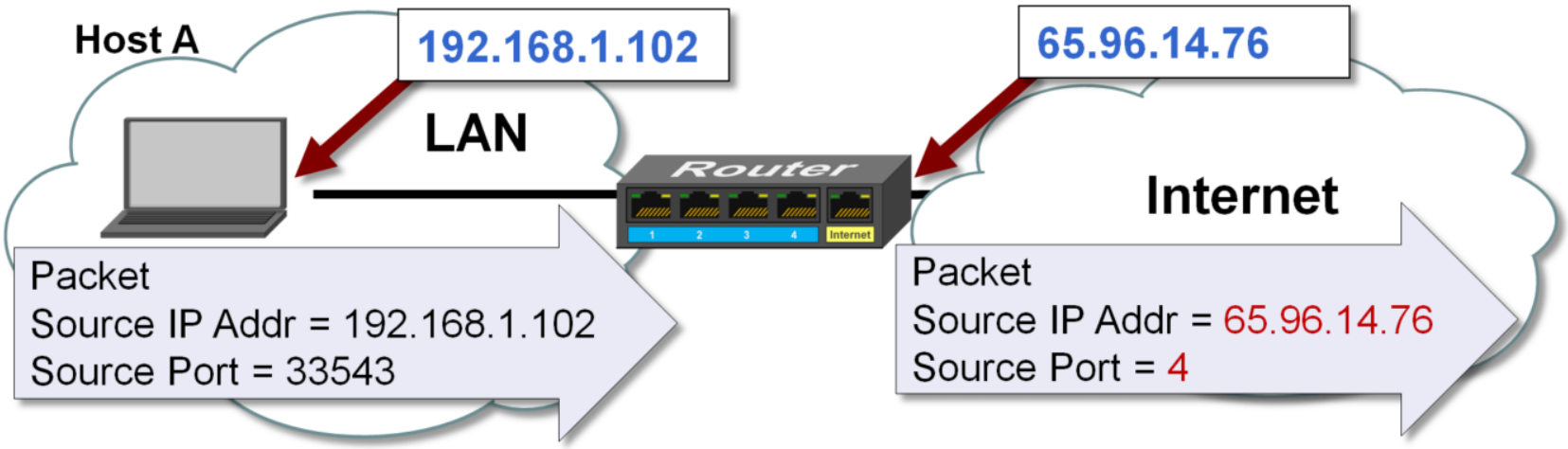
(2.b) The router adds a new entry corresponding to this packet to the NAT table.

(3) When a packet comes back from the destination computer, the router checks the destination port in the packet, and then looks in the translation table to see which computer and application on the stub domain the packet belongs to.

(4) It changes the destination address and destination port to the one saved in the address translation table and sends it to that computer.

Network Address Translation (cont.)

Example **[packet modification in NAT]**



NAT Translation Table

	Local IP Address	Source Port #		Internet IP Address	Source Port #
process X, Host A →	192.168.1.101	54,847	=	65.96.14.76	1
Host B →	192.168.1.103	24,123	=	65.96.14.76	2
process Y, Host A →	192.168.1.101	42,156	=	65.96.14.76	3
Host C →	192.168.1.102	33,543	=	65.96.14.76	4

Network Address Translation (cont.)

NAT Cons – **main NAT drawbacks include**

- **additional switching delays caused by NAT translations**
- **NAT routers becomes "single point of failure" for NAT networks connected to the Internet**
- **when the data is encrypted within the IP packet (including port number), it is impossible for NAT to perform the internal packet address translation (example: IPSec)**
- **difficulty to use services that required the initiation of TCP/UDP connections from outside network**

  (example: P2P applications, where any participating Peer should be able to initiate a TCP connection to any other participating Peer)
- **loss of end-to-end IP traceability - much harder to trace packets that undergo numerous packet changes over multiple NAT hops**