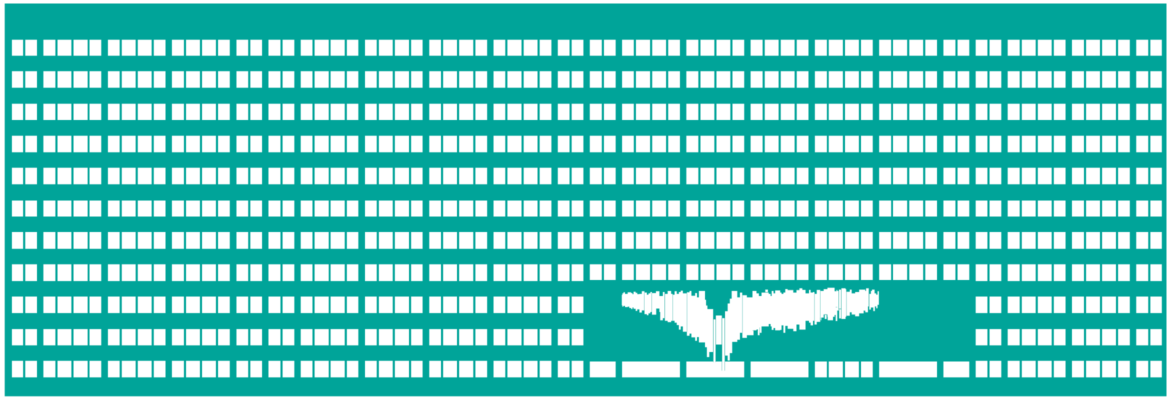
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Network Address Translator (NAT, RFC 3022)



Computer Networks
Lecture 5

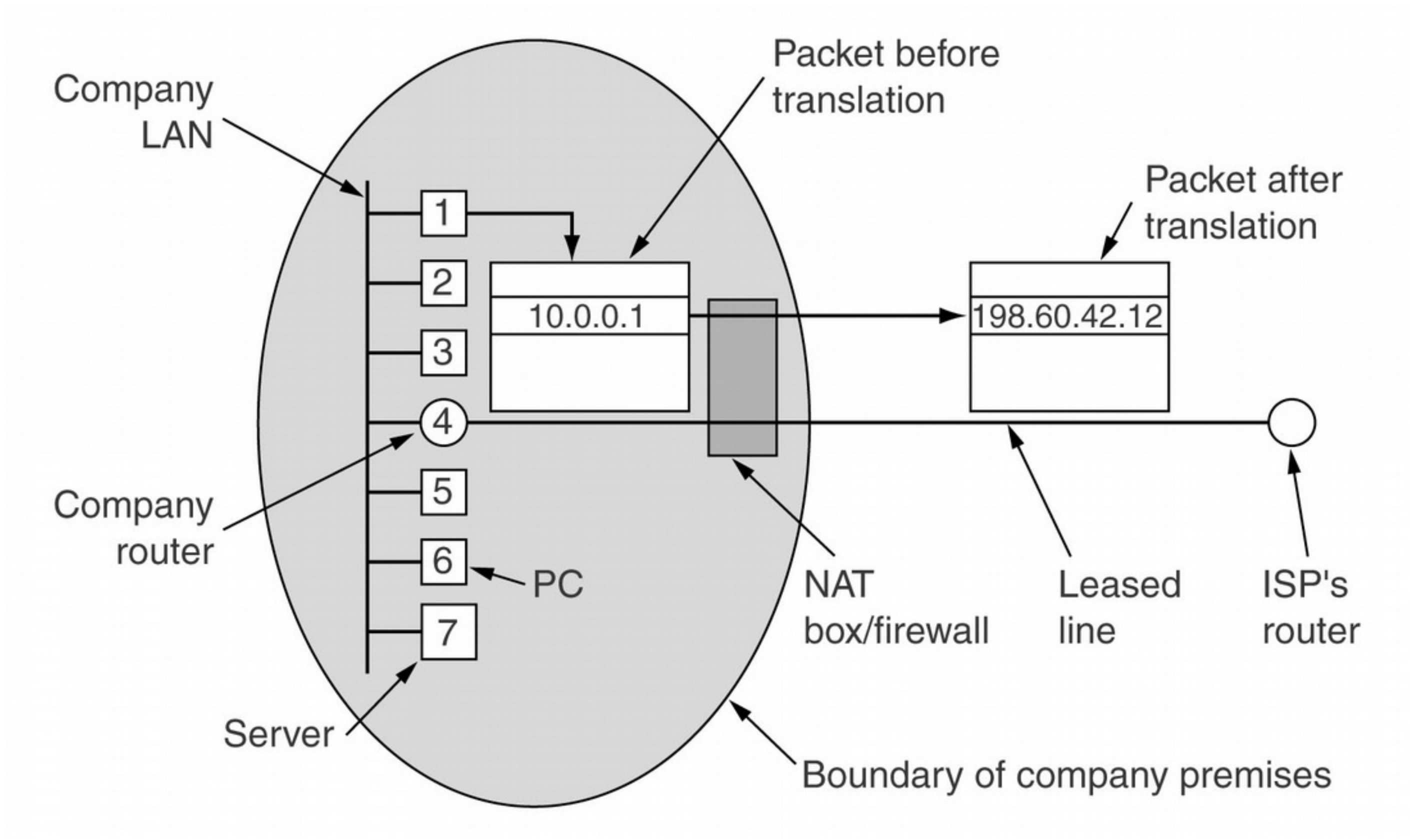
Purpose of NAT

- Only a limited set of public addresses (or a single address) is used for a potentially large number of stations
    - Stations may dynamically borrow addresses from the public address pool (or masquerade beyond interface IP address)
- Reducing the usage of public IP address space
    - and related expenses
- A disadvantage of NAT is that it limits the communication coming from the Internet
    - Often misunderstood as a security solution
        - NAT punching and other techniques to get inside of the network…

NAT Principle

- NAT device translates the source and destination IP addresses
  - Routers, firewalls (generally L3 devices)
- Uses the NAT translation table
  - Records may be configured manually or automatically created/removed dynamically
- The NAT device typically translates between inside addresses of the internal network and public addresses of the Internet

Typical NAT Usage Scenario



NAT Modes

- Full-cone NAT (one-to-one NAT)
  - When the internal address is mapped to an external address, any external host can send packets to any port of internal address by using the external one
- (Address)-restricted-cone NAT
  - Outside host can send packets to any port on internal host once a packet came to it from the external address corresponding to the internal address.
- Port-restricted cone NAT
  - Like (A)RC NAT, but limited to the port as well
- Symmetric NAT
  - Requests from the same internal address and port to different outside hosts are mapped to different external address/port pairs, PRC NAT rules apply

Static and Dynamic NAT

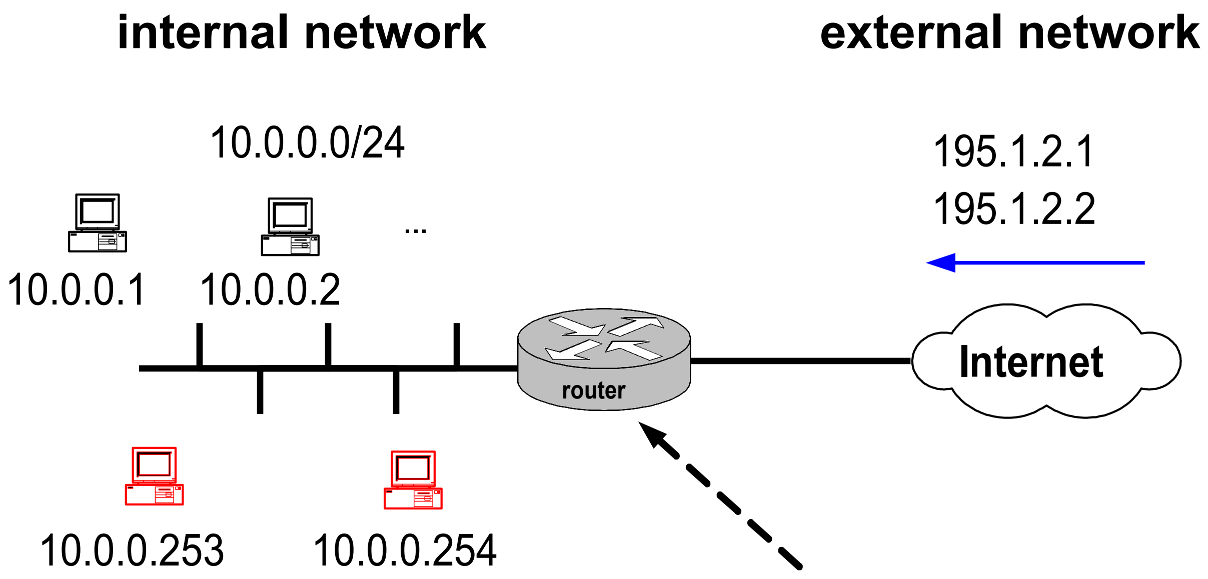
- Static NAT
  - The translation table is preconfigured manually
- Dynamic NAT
  - The contents of the translation table is created dynamically according to the network traffic
  - Public addresses are allocated to individual conversation from the public address pool

- Typically a combination of both approaches nowadays

Usages of Static NAT

- Static translation of (a private) inside source address to (a global) address of the outside network
- Static translation of (a global) outside destination address to a particular (private) address of the inside network
  - „port forwarding“ – making internal server with inside address accessible from outside
    - port preservation – the same (TCP/UDP) port for inside and outside address, not always possible

Static NAT
Basic (One-to-one) NAT Example



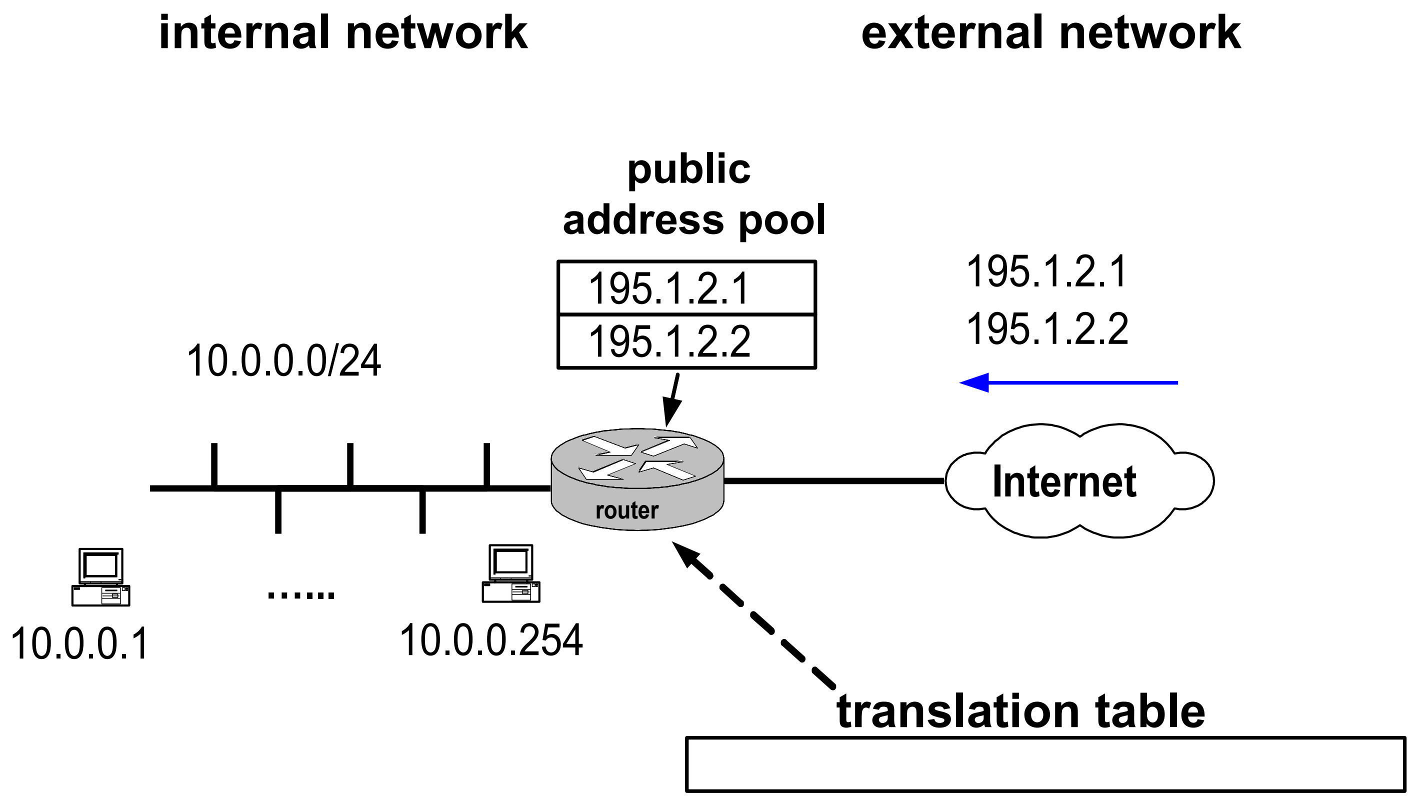
src 10.0.0.253 -> src 195.1.2.1
src 10.0.0.254 -> src 195.1.2.2
dst 195.1.2.1 -> dst 10.0.0.253
dst 195.1.2.2 -> dst 10.0.0.254

Static translation table

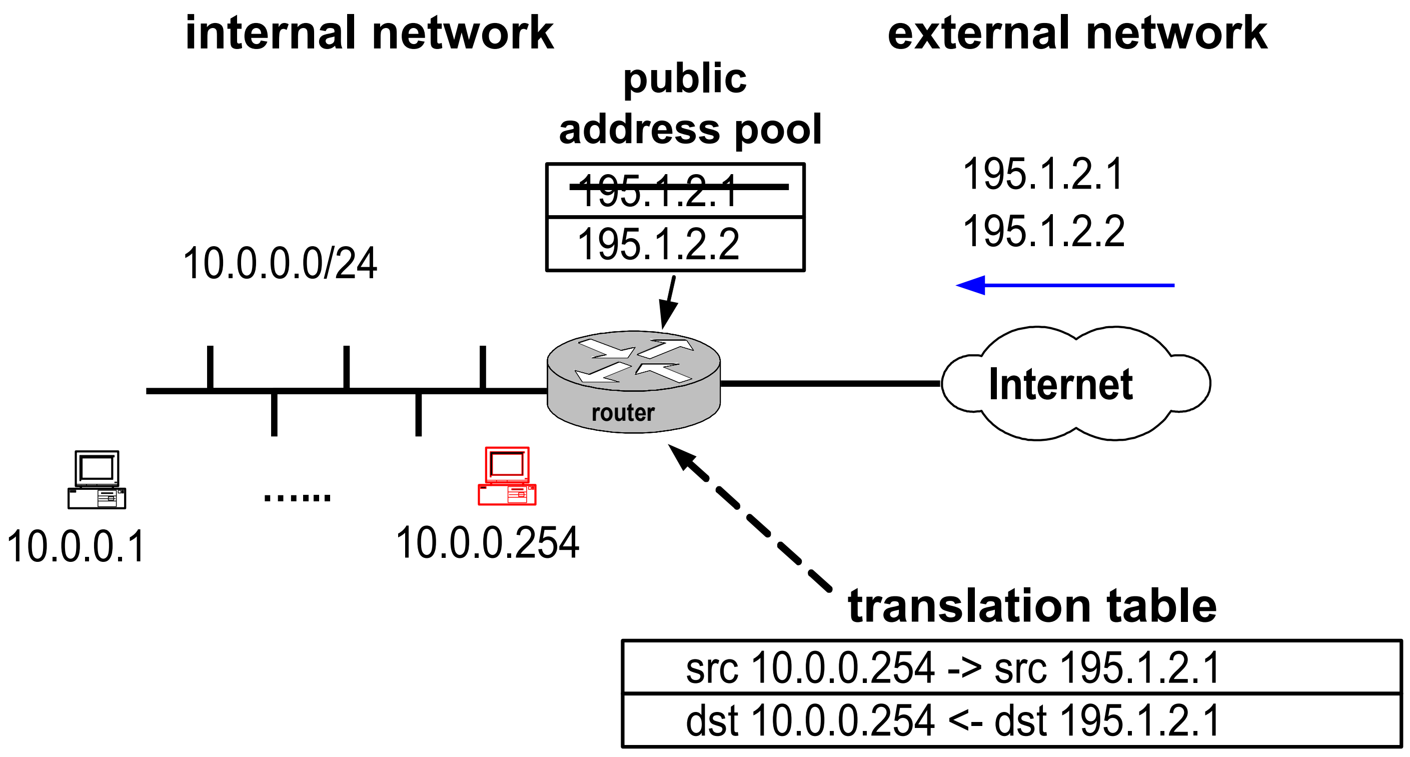
Principle of Dynamic NAT

- M public addresses are assigned to a network with N>M stations that needs to access the outside network
    - at most M stations at the same time (basic NAT)
- The NAT device maintains the currently available public addresses in a pool
- If a inside station S sends a packet from internal to external network, NAT device borrows it address V from the pool (if there is still some address available)
    - A record in the translation table that maps IP address of the station S to V is automatically created
    - A source address of the station S is rewritten in the outgoing packet to V (that is unique and routable in the outside network)
    - After the response packet comes to address V, the translation table is consulted and the destination address translated back to S. The packet is then forwarded to the inside network.

Dynamic NAT – An Example (1)

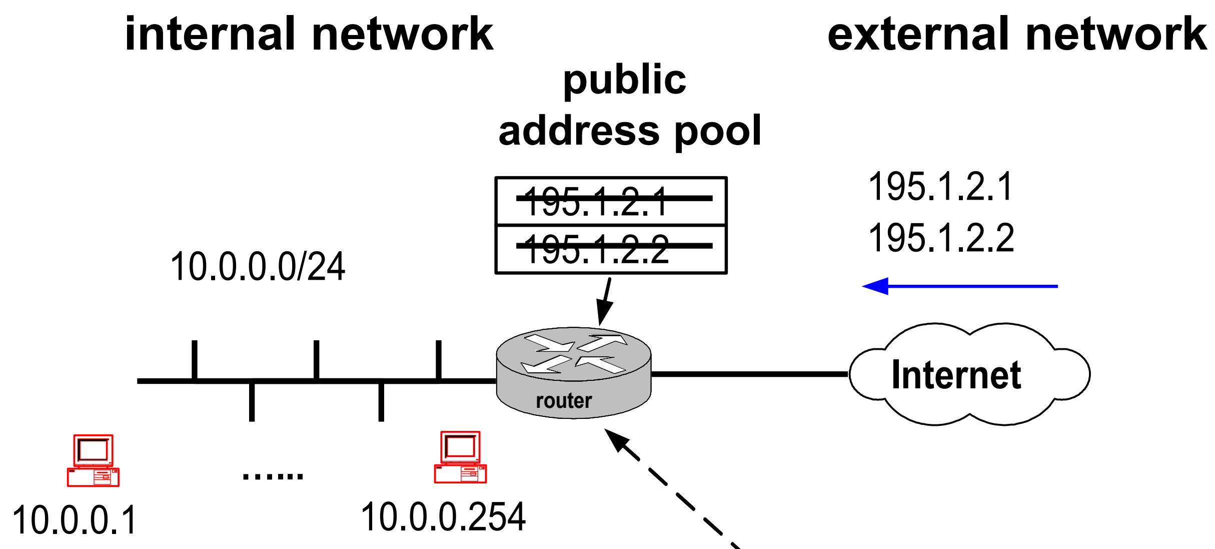


Dynamic NAT – An Example (2)



10.0.0.254 -> 158.196.1.10

Dynamic NAT – An Example (3)



translation table

src 10.0.0.254 -> src 195.1.2.1
dst 10.0.0.254 <- dst 195.1.2.1
src 10.0.0.1 -> src 195.1.2.2
dst 10.0.0.1 <- dst 195.1.2.2

10.0.0.1 -> 158.196.1.10

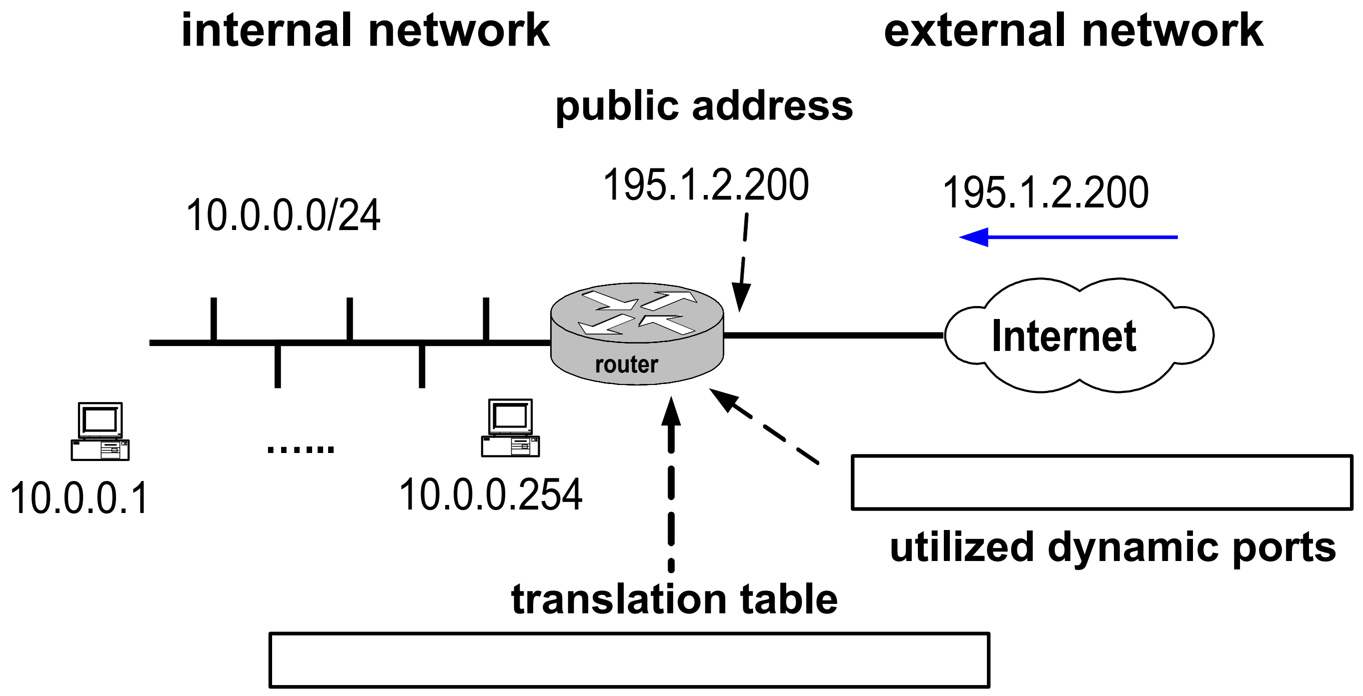
Aging of Dynamic NAT Translation Table Records

- To allow N stations to share M<N outside addresses, the lifetime of the dynamically created records of the translation table is limited
  - Related to the time when the record was last used
- After the expired record is removed from the table, the borrowed outside address is returned back to the pool

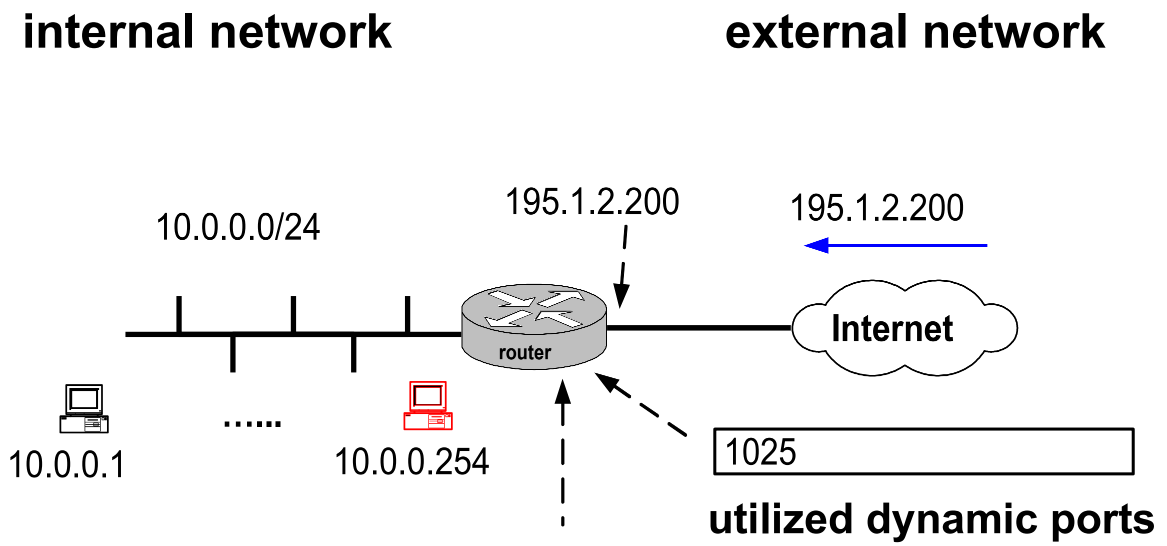
Network Address and Port Translation

- NAPT
    - „Masquerading“ in Linux terminology
    - Port Address Translation (PAT)
    - NAT overload
    - many-to-one NAT
- Multiple nodes are hidden beyond a single IP address, they are distinguished based on different port numbers
    - Dynamically assigned source ports → a translation table mapping ports to internal IP addresses is being built.

NAPT – An Example (1)



NAPT – An Example (2)

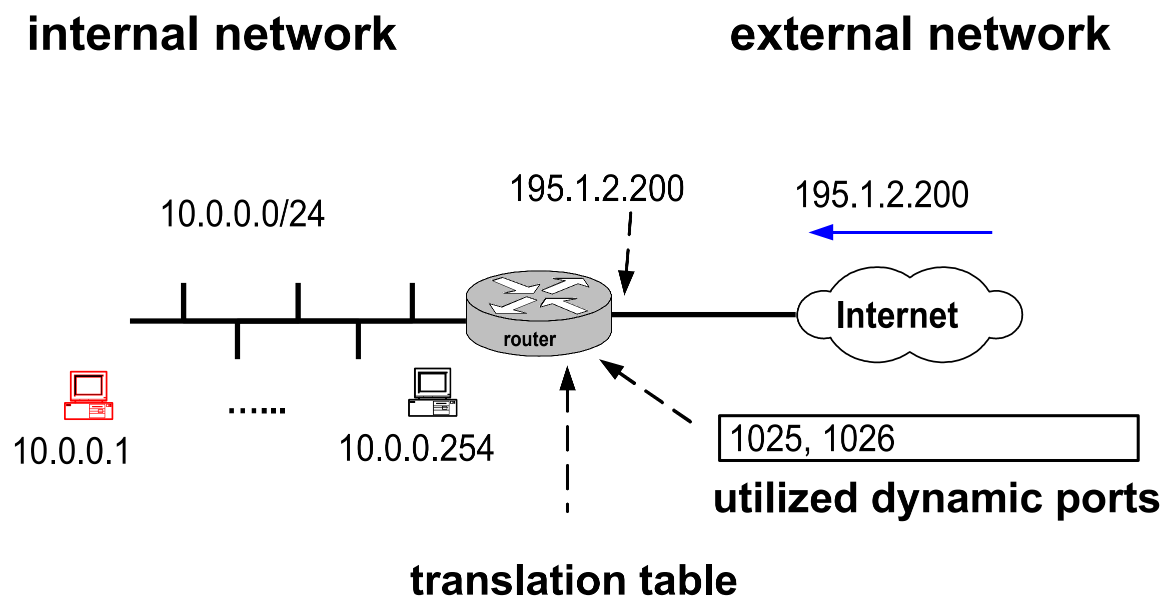


translation table

src 10.0.0.254:2000 -> src 195.1.2.200:1025	
dst 10.0.0.254:2000 <- dst 195.1.2.200:1025	

10.0.0.254:2000 -> 158.196.1.10:80

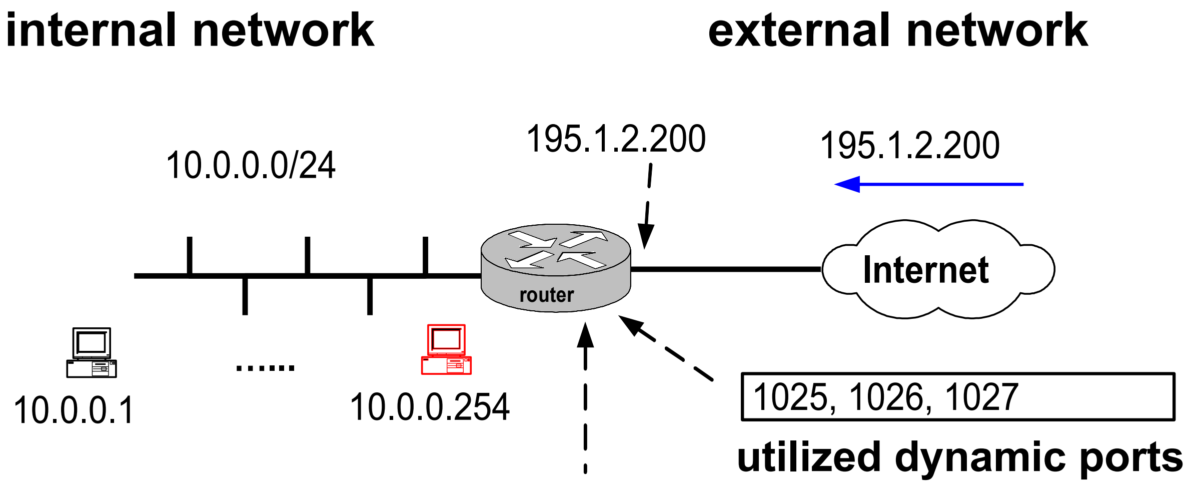
NAPT – An Example (3)



src 10.0.0.254:2000 -> src 195.1.2.200:1025
dst 10.0.0.254:2000 <- dst 195.1.2.200:1025
src 10.0.0.1:3000 -> src 195.1.2.200:1026
dst 10.0.0.1:3000 <- dst 195.1.2.200:1026

10.0.0.1:3000 -> 158.196.1.10:80

NAPT – An Example (4)



translation table

src 10.0.0.254:2000 -> src 195.1.2.200:1025
dst 10.0.0.254:2000 <- dst 195.1.2.200:1025
src 10.0.0.1:3000 -> src 195.1.2.200:1026
dst 10.0.0.1:3000 <- dst 195.1.2.200:1026
src 10.0.0.254:2001 -> src 195.1.2.200:1027
dst 10.0.0.254:2001 <- dst 195.1.2.200:1027

10.0.0.254:2001 -> 158.196.1.10:80

Routing and NAT

- Routers in the outside network knows nothing about NAT presence
- But they have to know about the outside address pool used by NAT device
  - The prefix has to be advertised to the routing protocol so that the returning traffic can be delivered back to the NAT device

NAT Disadvantages

- Limits the universal connectivity
  - Only clients may reside in the internal network
    - Today's network designs take that into account
- Stateful device in the data path
  - Problem arises in case of the state information loss (e.g. NAT device reboot)
- Problematic usage with asymmetric routing (e.g. the network connected to the outside world by more than 1 router)
  - the incoming traffic may return through the other router than the corresponding outgoing traffic