Network Address Translation (NAT)

Petr Grygárek

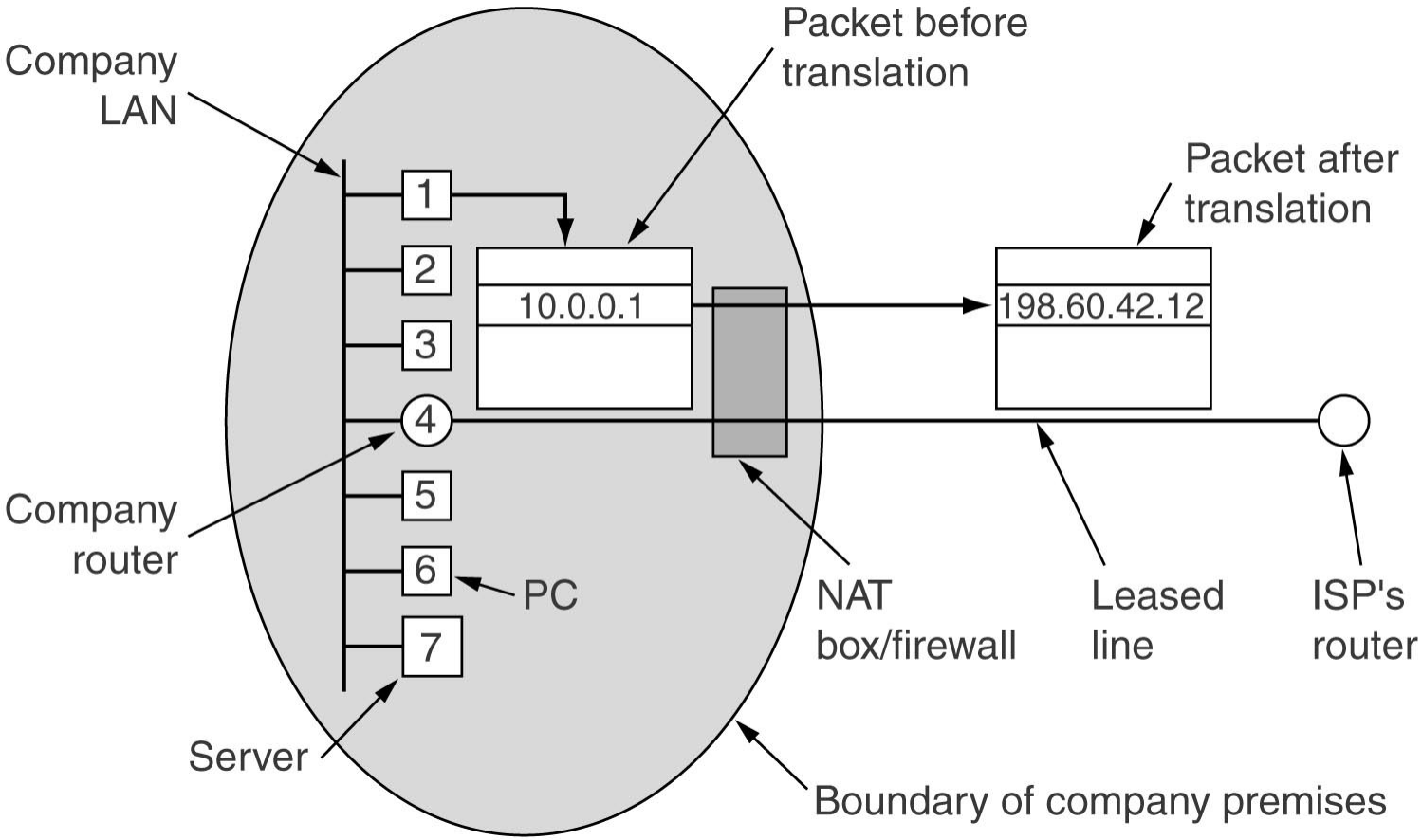
© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Network Address Translation (RFC 1631)

- translation of source/destination IP addresses
  - performed by L3 devices (router, firewall)
- utilizes NAT translation table
  - entries configured statically or automatic dynamic creation
- translation commonly implemented between "inside" network with private addresses and "outside" network with global unique addresses

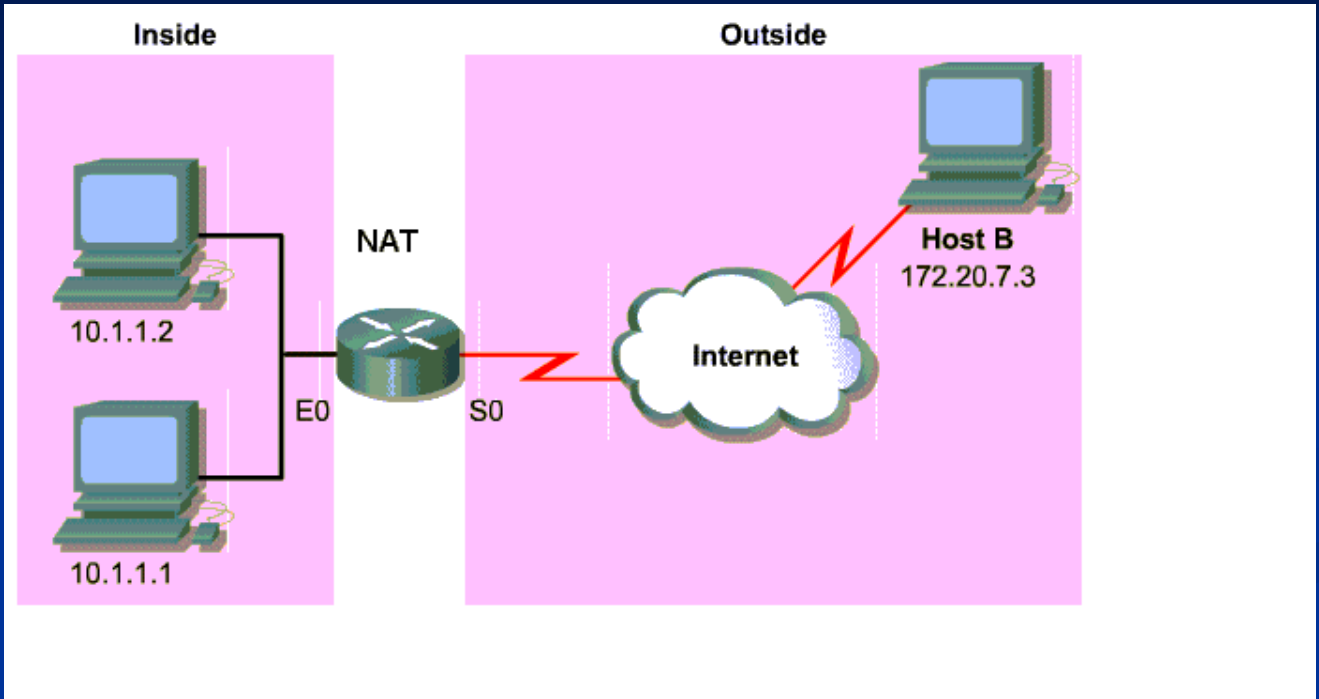
© 2005 Petr Grygarek, Advanced Computer Networks Technologies

NAT usage scenario



© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Inside and outside interfaces



- Multiple interfaces can be designated as inside
- Some interfaces can be neither inside or outside
  - traffic through them not manipulated by NAT

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Address classification

- Inside Local
  - addresses in inside network as viewed in inside network (i.e. configured on stations of inside network)
- Inside Global
  - addresses in inside network as viewed from outside network
- Outside Global
  - public (globally assigned and unique) addresses configured on stations of outside network (as viewed in outside and probably also in inside network)
- Outside Local
  - addresses in outside network as viewed from inside network
    - (differ from Outside Global addresses in special cases like overlapping address range NAT-ing)

NAT translation table

- Implemented and maintained by device performing NAT
- Entries specify which source/destination addresses should be manipulated and how
  - Entry format

    < inside local, inside global, outside local, outside global >
    (source and destination ports may be manipulated also)
- Every packet arriving at inside or outside interface is checked against NAT translational table entries and manipulated if some entry requires to do that
  - SRC/DST IP address and ports change
  - Packet arriving at inside (or outside in special cases) interface may cause translation table entry creation

Static and dynamic NAT

- Static NAT
  - NAT translation table statically configured
- Dynamic NAT
  - NAT translation table entries created dynamically based on passing traffic
  - (Outside source) addresses temporarily borrowed from pool of (outside global) addresses
    - other scenarios also possible, for example for load balancing between multiple servers in inside network

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Static NAT principle (typical usage)

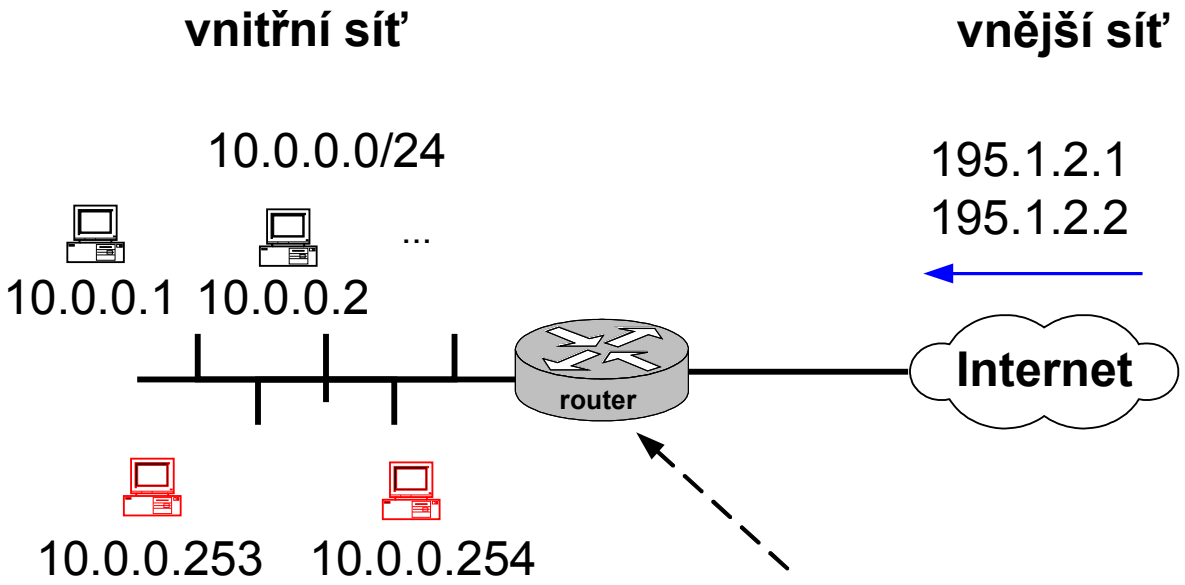
- Translation of a given (private) source inside address to given outside source address (public and routable in outside network)
  - + translation of public destination address to corresponding private destination address in opposite direction
- Translation of given outside (public) destination address to given (private) destination inside address in case of publicly available services in inside network
  - + translation of private source address to corresponding public source address in opposite direction

Addresses/ports to translate from and to are given by static configuration

Typically used to make server in inside network with private addresses available to the public under globally unique address.

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Static NAT



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

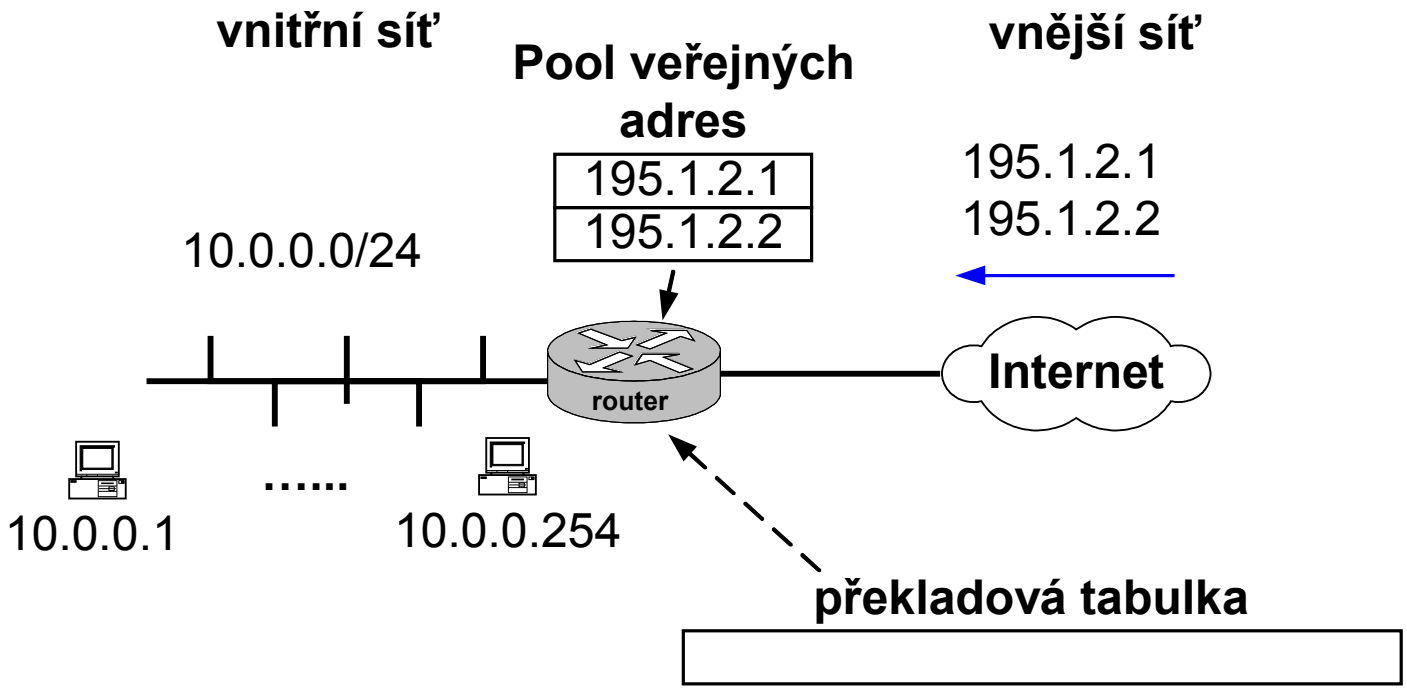
Statická překladová tabulka

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

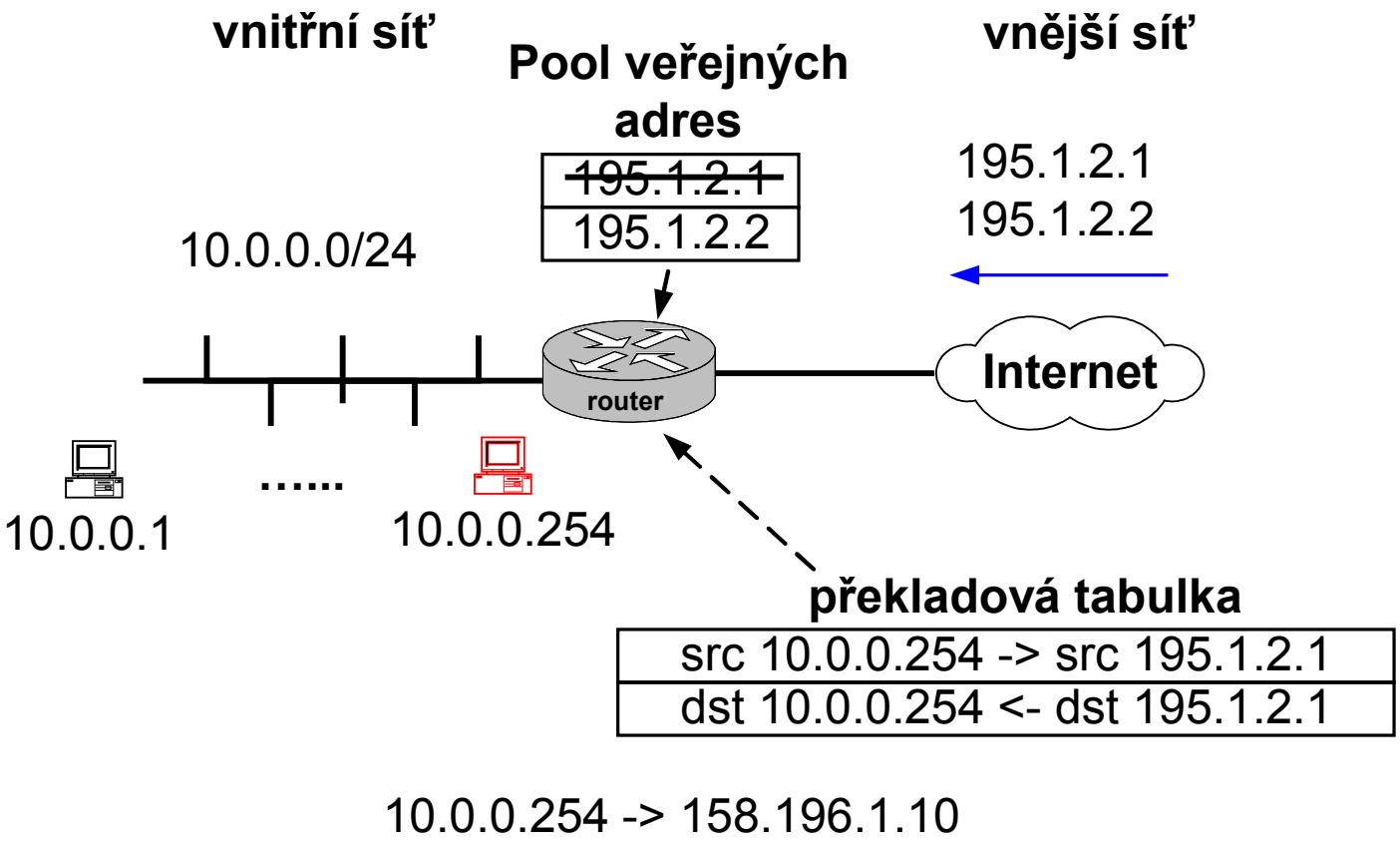
Dynamic NAT principle (typical usage)

- NAT-ed network is assigned M public addresses
- Customer wants to place N>M stations at internal network and allow them to access outside network
  - (but at most M stations at the same time)
- Available public addresses are placed and maintained in pool on the NAT device
- If station S at inside network sends packet to outside network, it is temporarily assigned some (source) address V from address pool (if there is still some address remaining)
  - entry mapping station address S to address V is created in translation table
  - source address S is replaced with V in outgoing packet (V is routable and unique in outside network)
  - when reply packet arrives to address V, translation table is searched and destination address V is replaced with destination address S. Then the packet is sent to inside network.

Dynamic NAT (1)

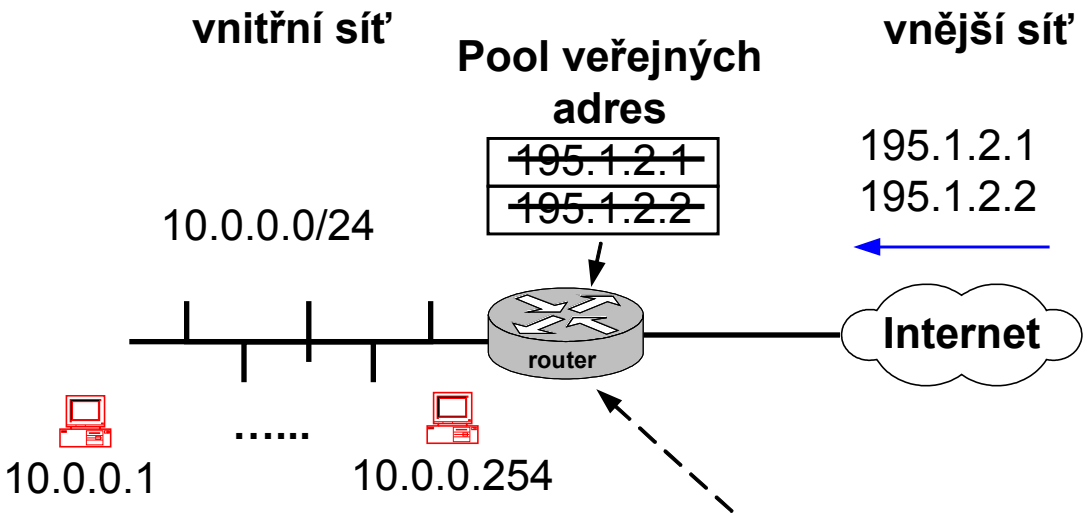


Dynamic NAT (2)



© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Dynamic NAT (3)



10.0.0.1 -> 158.196.1.10

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Timing of dynamic NAT

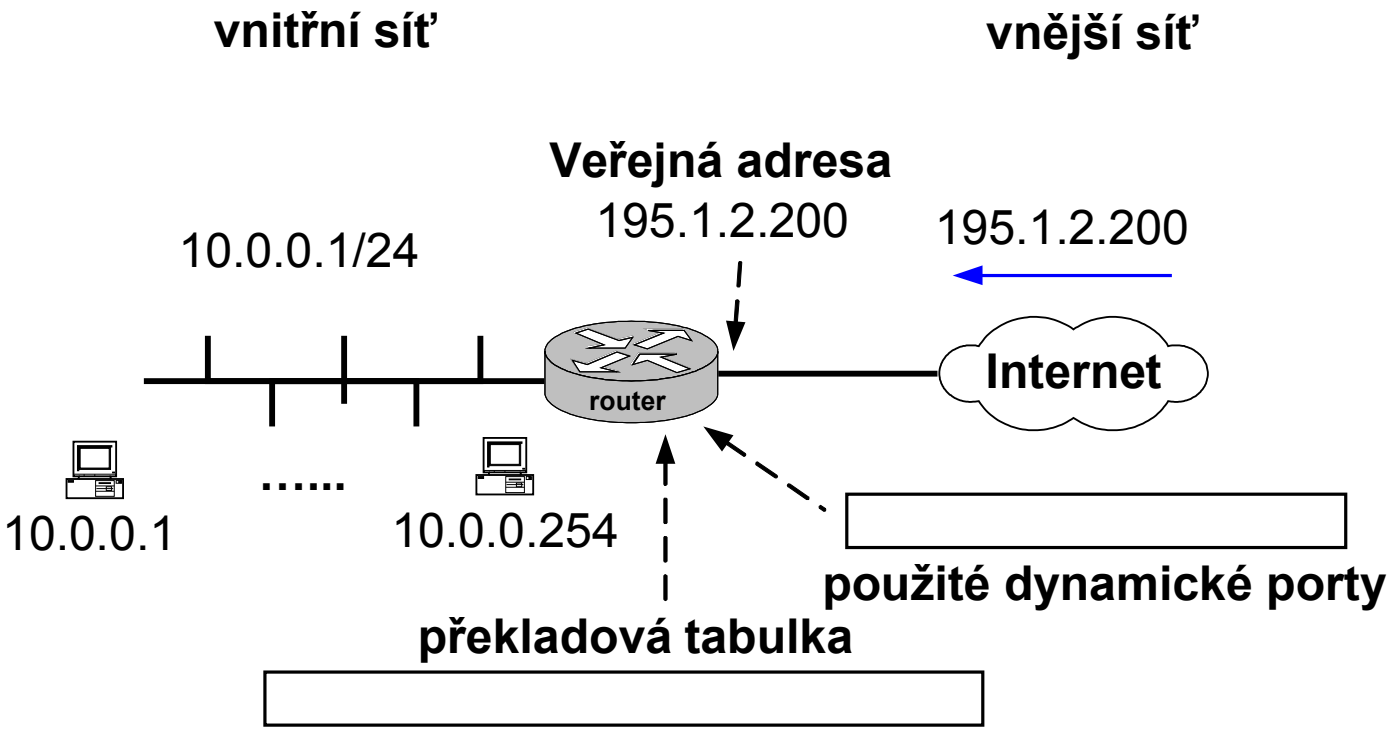
- To allow N stations to share M public addresses, dynamically created entries in translation table have limited lifetime
  - timeout measured from time the entry was used last time for packet header manipulation
- When translation table entry removed on timeout expiration, public address returned back to address pool
- Timeout setting – based on typical session inactivity duration
  - risk of session loss vs. need of quick pool addresses "recycling"

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

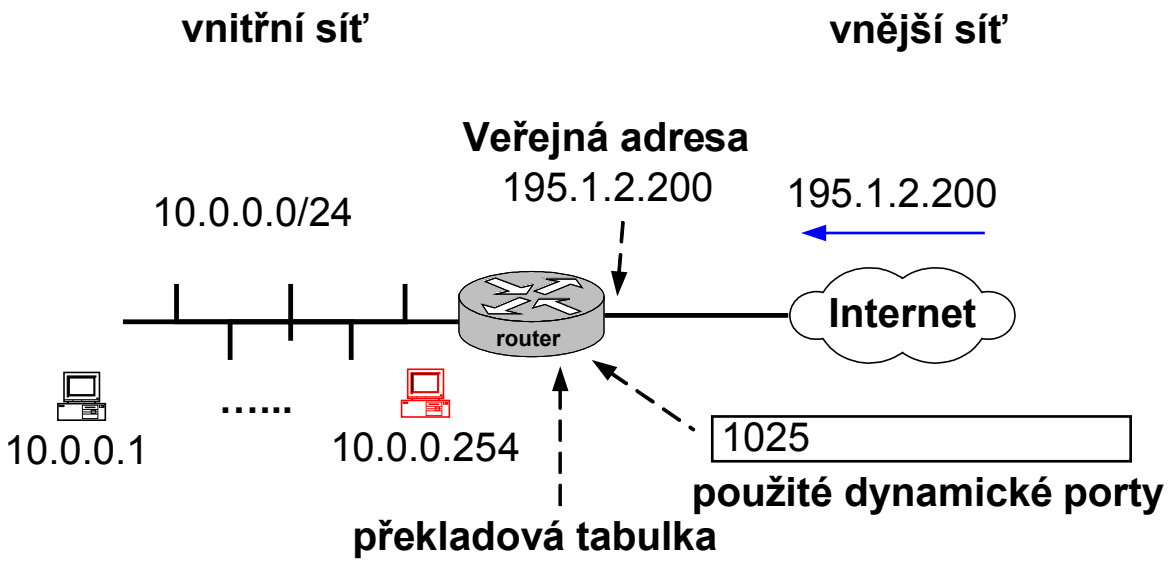
Port Address Translation

- „Masquarading“ in Linux terminology
- Hides multiple (client) station IP addresses behind single public IP address
- Stations differentiated by various L4 ports of the public address
  - Source ports of public address assigned dynamically
  - Dynamic NAT translation table entries contain mapping of public address's ports to inside network station addresses
  - Usable only for UDP/TCP
    - there exist a way how to use ICMP through PAT (matching of outgoing and incoming packets using ICMP sequence numbers)
  - Multiple public addresses can be PATed

PAT (1)


vnitřní síť
vnější síť
Veřejná adresa
195.1.2.200
195.1.2.200
10.0.0.1/24
router
Internet
.....
10.0.0.1
10.0.0.254
použité dynamické porty
překladová tabulka

PAT (2)

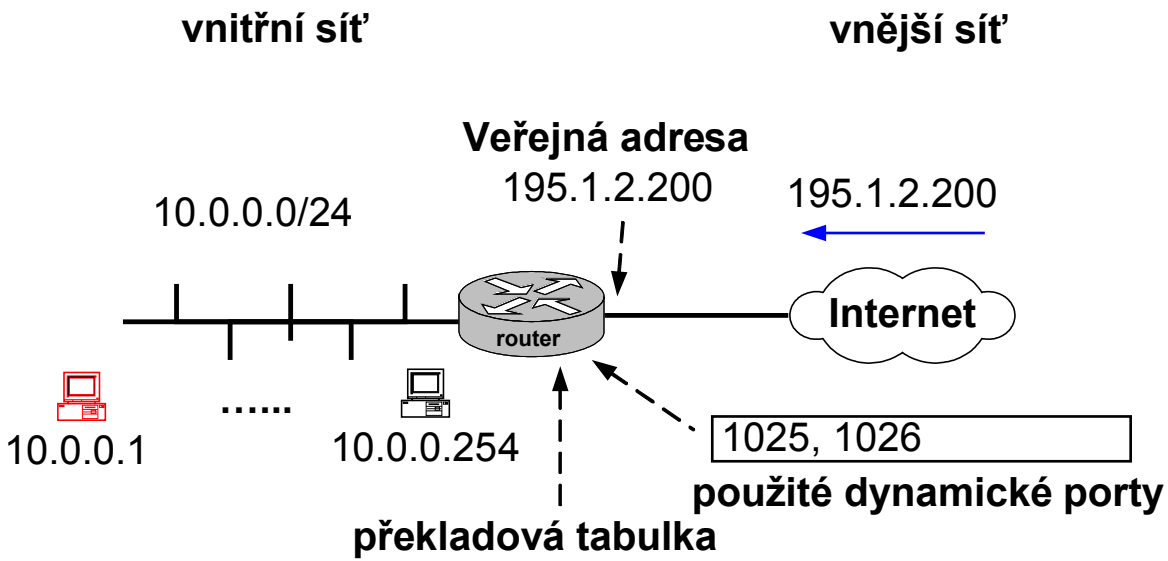


src 10.0.0.254:2000 -> src 195.1.2.200:1025
dst 10.0.0.254:2000 <- dst 195.1.2.200:1025

10.0.0.254:2000 -> 158.196.1.10:80

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

PAT (3)

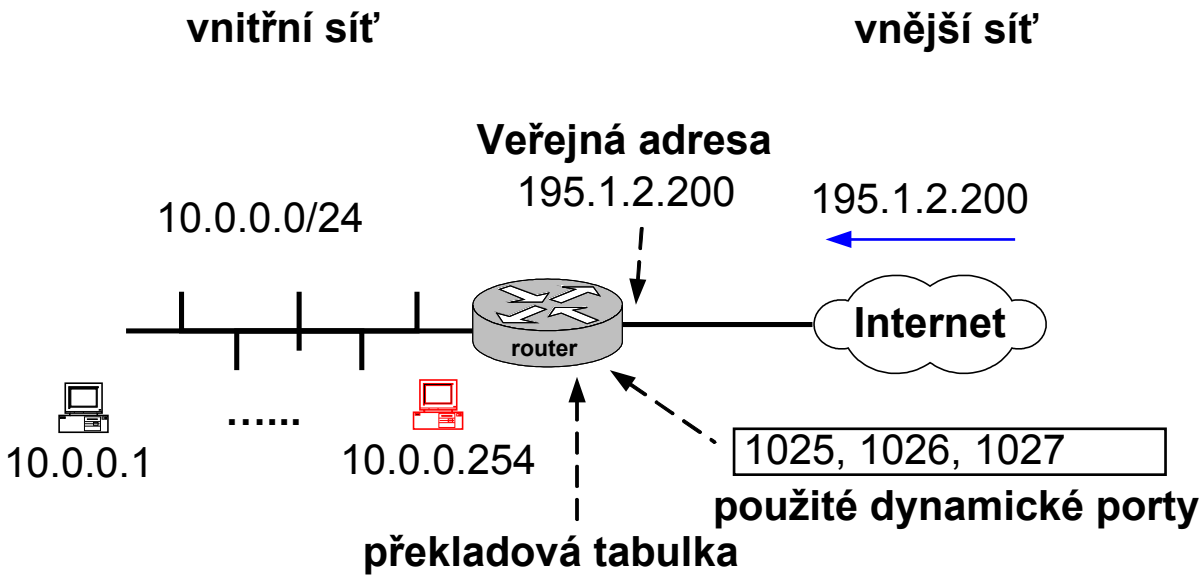


src 10.0.0.254:2000 -> src 195.1.2.200:1025
dst 10.0.0.254:2000 <- dst 195.1.2.200:1025
src 10.0.0.1:3000 -> src 195.1.2.200:1026
dst 10.0.0.1:3000 <- dst 195.1.2.200:1026

10.0.0.1:3000 -> 158.196.1.10:80

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

PAT (4)



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

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

NAT advantages

- Solves cases where addressing scheme would have be changed and there is a reason not to do that on all network devices (including stations)
  - address prefix change (when changing ISP)
  - Interconnection of multiple network with overlapping ranges of private addresses
- Saves IP addresses
  - which is a reason why providers love NAT so much
- Increases security

NAT usage limitation

- Limits global connectivity and global addressability of devices (original Internet architecture developers' intent)
- Inside network has to be connected with single NAT-router – no redundancy
  - maybe some sort of source-based load balancing to multiple NAT devices is possible
- No publicly available services in internal network can be operated if pure dynamic NAT is used
  - no fixed "outside global" address for service servers
  - can be worked around using static destination NAT (or port forwarding)
    - if provider agrees to configure it for us on the NAT box
- Routing updates cannot traverse NAT

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Advanced NAT topics

- NAT performed multiple times
- Ca be NAT detected ?
- IP addresses and ports in application-level data
  - FTP (PASV, PORT commands)
  - IP Telephony protocols
  - NetBIOS over TCP/IP
  - DHCP
  - SNMP

  NAT device may fix some specific protocol problems (application data inspection required)
- Manipulation with DNS responses in networks with overlapping address ranges
  - A, DNS records

NAT usage for load balancing

Load balancing between servers in inside network known by single address in outside network

- Addresses of servers in server farm placed into pool of (destination) addresses
- Single virtual public IP address allocated
- Connections (data streams) arriving to virtual address mapped in round-robin fashion to addresses from pool of destination addresses

© 2005 Petr Grygarek, Advanced Computer Networks Technologies

Security and NAT

NAT is often considered a mechanism to increase security of inside (internal) network

- Internal network address structure is hidden
- Using dynamic NAT, attacker in outside network may contact only stations for which (dynamic) entry in NAT translation table currently exists
  - but address (/port) representing station of attacker's interest is still changing in poorly predictable way, depending on traffic pattern from inside to outside network

Linux IPChains terminology: SNAT & DNAT

- SNAT = SOURCE NAT
  - source address translation (commonly to dynamic range)
    - for returning traffic (outside-to-inside), destination address has to be translated also (on outside interface), but source address translation is primary as it creates dynamic entries in translation table
- DNAT = DESTINATION NAT
  - destination address/port forwarding
    - for returning traffic (inside-to-outside), source address has to be translated also (on inside interface), but destination address translation is primary as it creates dynamic entries in translation table

Do not confuse with static and dynamic NAT.

© 2005 Petr Grygarek, Advanced Computer Networks Technologies