Network Address Translation (NAT)

Relates to Lab 7.
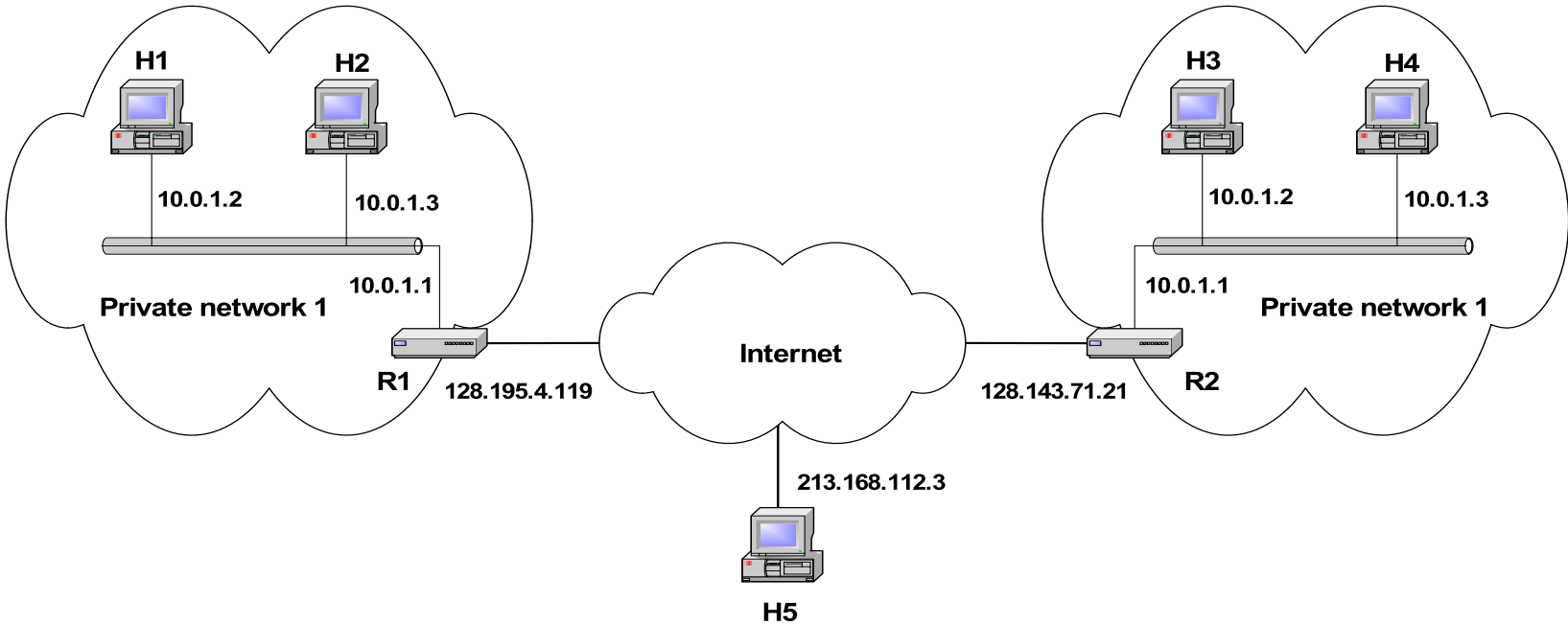
Module about private networks and NAT.

Taken from http://www.cs.virginia.edu/~itlab/
book/slides/module17-nat.ppt

Private Network

- *Private IP* network is an IP network that is not directly connected to the Internet

- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique

- Generally, private networks use addresses from the following experimental address ranges (*non-routable addresses*):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
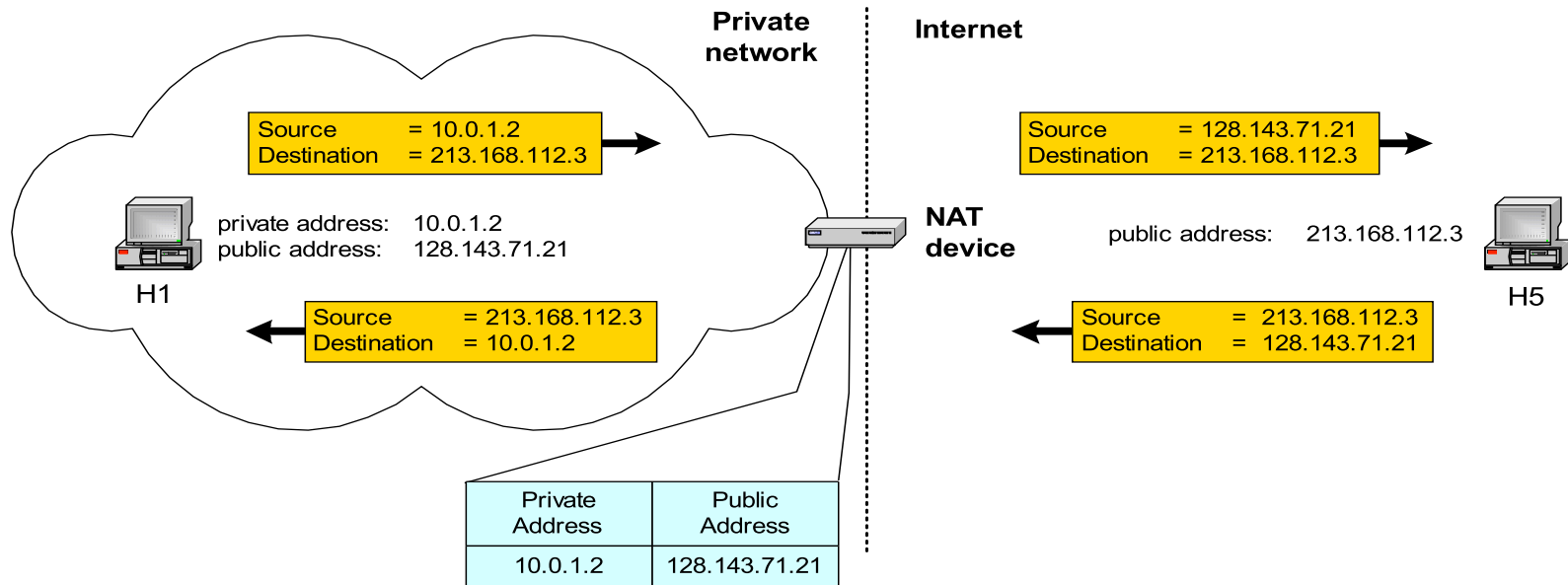 - 192.168.0.0 – 192.168.255.255

Private Addresses

H1   **H2**

10.0.1.2   10.0.1.3

10.0.1.1

Private network 1

R1   128.195.4.119

Internet

128.143.71.21   **R2**

H3   **H4**

10.0.1.2   10.0.1.3

10.0.1.1

Private network 1

213.168.112.3

H5

Network Address Translation (NAT)

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network

- NAT is a method that enables hosts on private networks to communicate with hosts on the Internet

- NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.
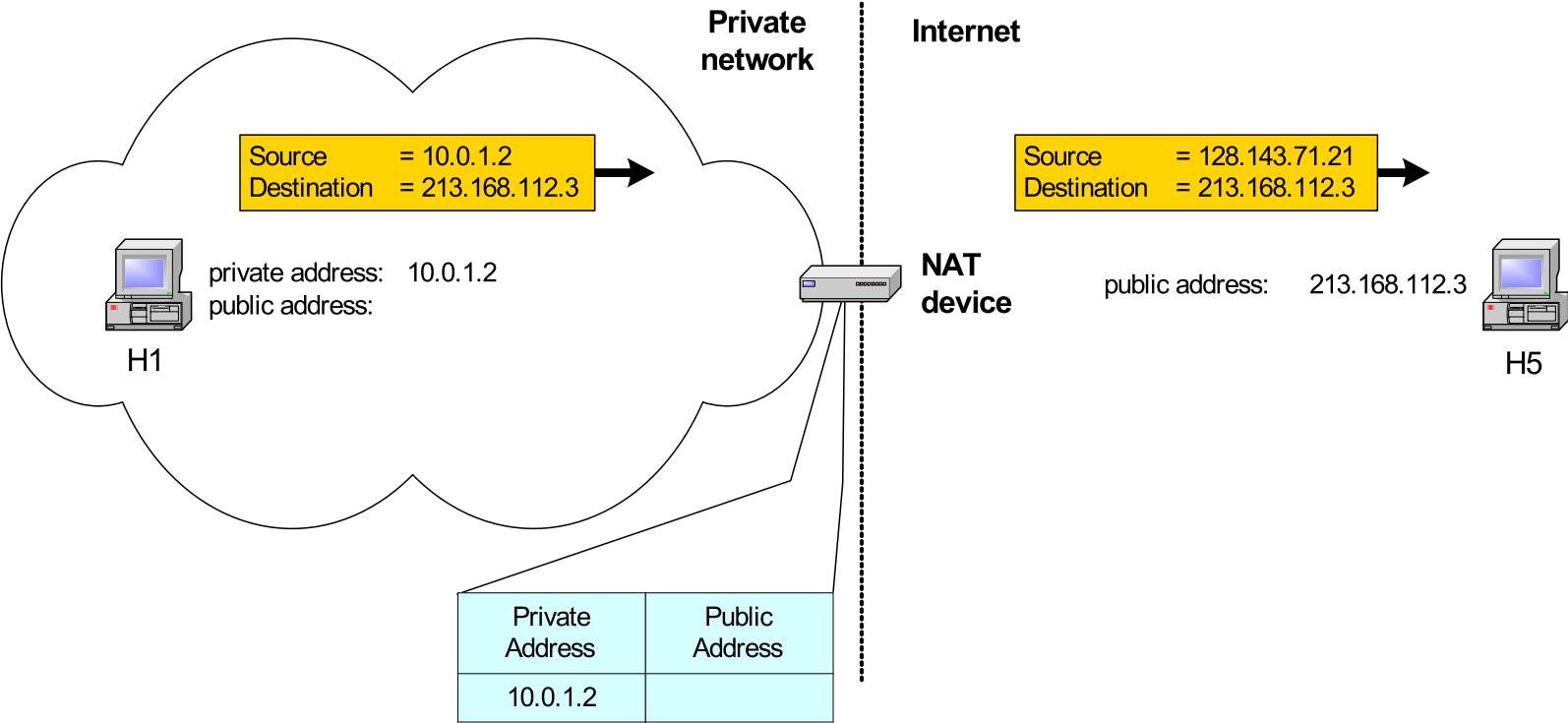
Basic operation of NAT

Private network | Internet

Source = 10.0.1.2
Destination = 213.168.112.3

Source = 128.143.71.21
Destination = 213.168.112.3

private address: 10.0.1.2
public address: 128.143.71.21

NAT device

public address: 213.168.112.3

H1

H5

Source = 213.168.112.3
Destination = 10.0.1.2

Source = 213.168.112.3
Destination = 128.143.71.21

Private Address	Public Address
10.0.1.2	128.143.71.21

- NAT device has address translation table

5

Pooling of IP addresses

- **Scenario:** Corporate network has many hosts but only a small number of public IP addresses

- **NAT solution:**
  - Corporate network is managed with a private address space
  - NAT device, located at the boundary between the corporate network and the public Internet, manages a pool of public IP addresses
  - When a host from the corporate network sends an IP datagram to a host in the public Internet, the NAT device picks a public IP address from the address pool, and binds this address to the private address of the host

Pooling of IP addresses

Private network   **Internet**

Source = 10.0.1.2
Destination = 213.168.112.3

Source = 128.143.71.21
Destination = 213.168.112.3

NAT device

H1

private address: 10.0.1.2
public address:

public address: 213.168.112.3

H5

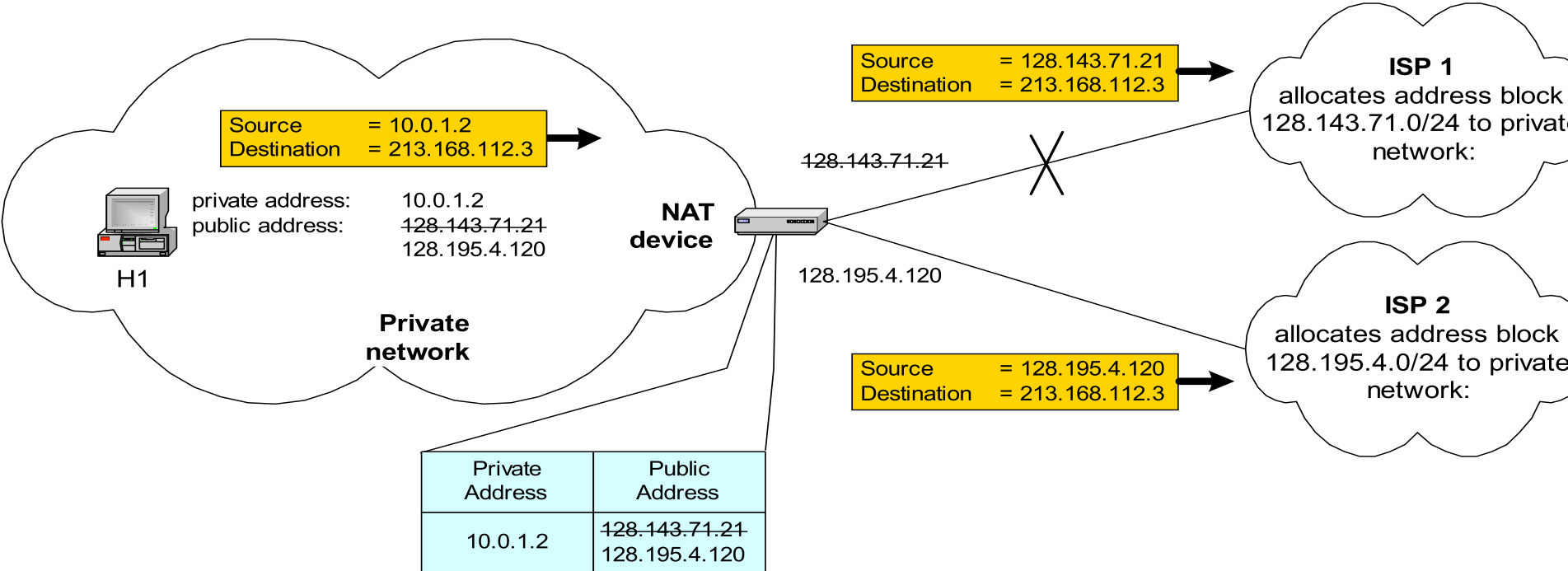| Private Address	Public Address
10.0.1.2	

Pool of addresses: 128.143.71.0-128.143.71.30

Supporting migration between network service providers

- **Scenario:** In CIDR, the IP addresses in a corporate network are obtained from the service provider. Changing the service provider requires changing all IP addresses in the network.

- **NAT solution:**
  - Assign private addresses to the hosts of the corporate network
  - NAT device has static address translation entries which bind the private address of a host to the public address.
  - Migration to a new network service provider merely requires an update of the NAT device. The migration is not noticeable to the hosts on the network.

  Note:
  - The difference to the use of NAT with IP address pooling is that the mapping of public and private IP addresses is static.

Supporting migration between network service providers

Source = 128.143.71.21
Destination = 213.168.112.3

Source = 10.0.1.2
Destination = 213.168.112.3

private address: 10.0.1.2
public address: ~~128.143.71.21~~
128.195.4.120

128.143.71.21

128.195.4.120

NAT device

H1

Private network

ISP 1
allocates address block
128.143.71.0/24 to private
network:

ISP 2
allocates address block
128.195.4.0/24 to private
network:

Source = 128.195.4.120
Destination = 213.168.112.3

Private Address	Public Address
10.0.1.2	~~128.143.71.21~~ 128.195.4.120

9

IP masquerading

- **Also called: Network address and port translation (NAPT), port address translation (PAT).**
- **Scenario:** Single public IP address is mapped to multiple hosts in a private network.
- **NAT solution:**
  - Assign private addresses to the hosts of the corporate network
 - NAT device modifies the port numbers for outgoing traffic

IP masquerading

Private Address	Public Address
10.0.1.2/2001	128.143.71.21/2100
10.0.1.3/3020	128.143.71.21/4444
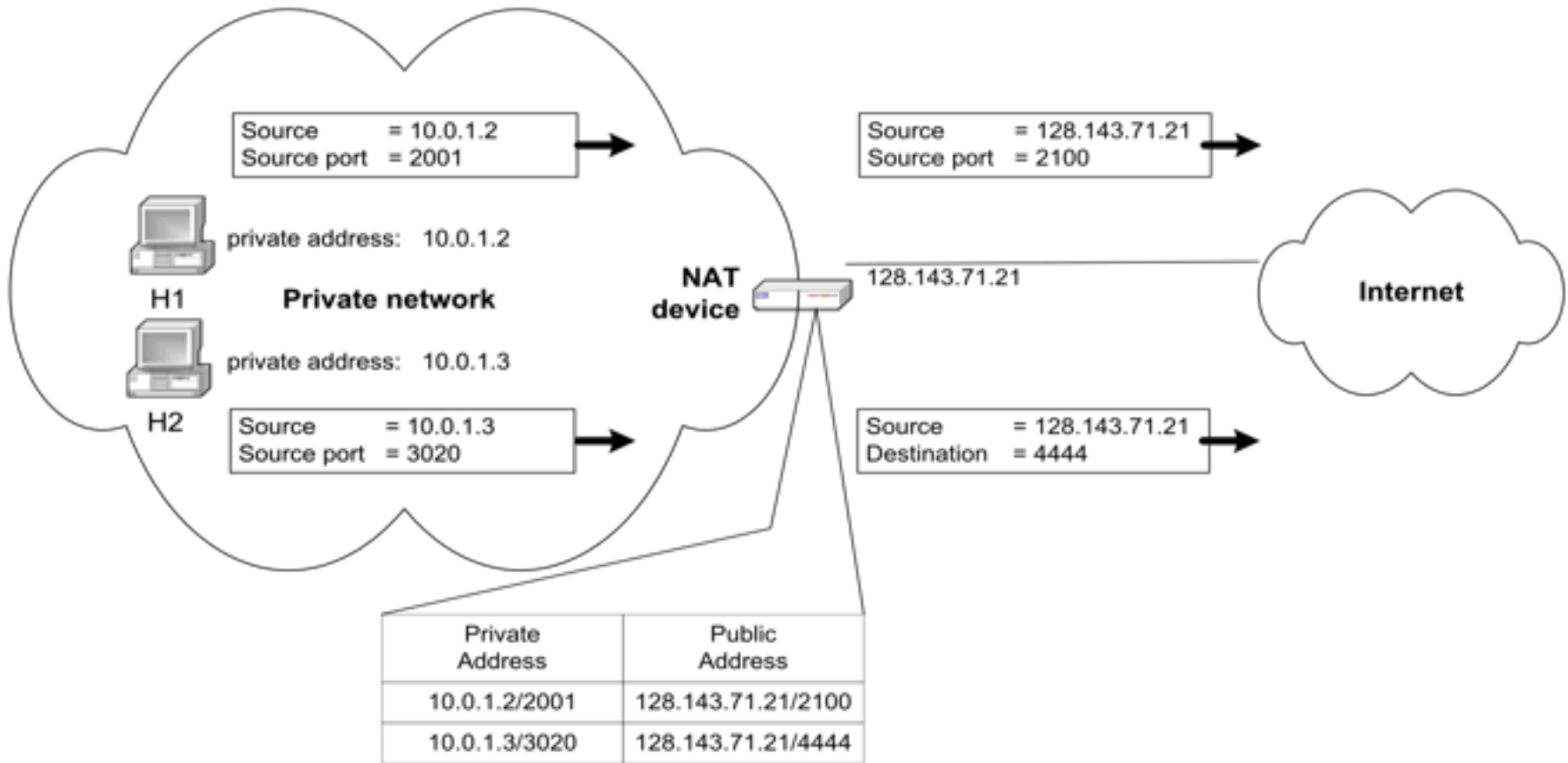
Load balancing of servers

- **Scenario:** Balance the load on a set of identical servers, which are accessible from a single IP address

- **NAT solution:**
  - Here, the servers are assigned private addresses
  - NAT device acts as a proxy for requests to the server from the public network
  - The NAT device changes the destination IP address of arriving packets to one of the private addresses for a server
  - A sensible strategy for balancing the load of the servers is to assign the addresses of the servers in a round-robin fashion.

Load balancing of servers
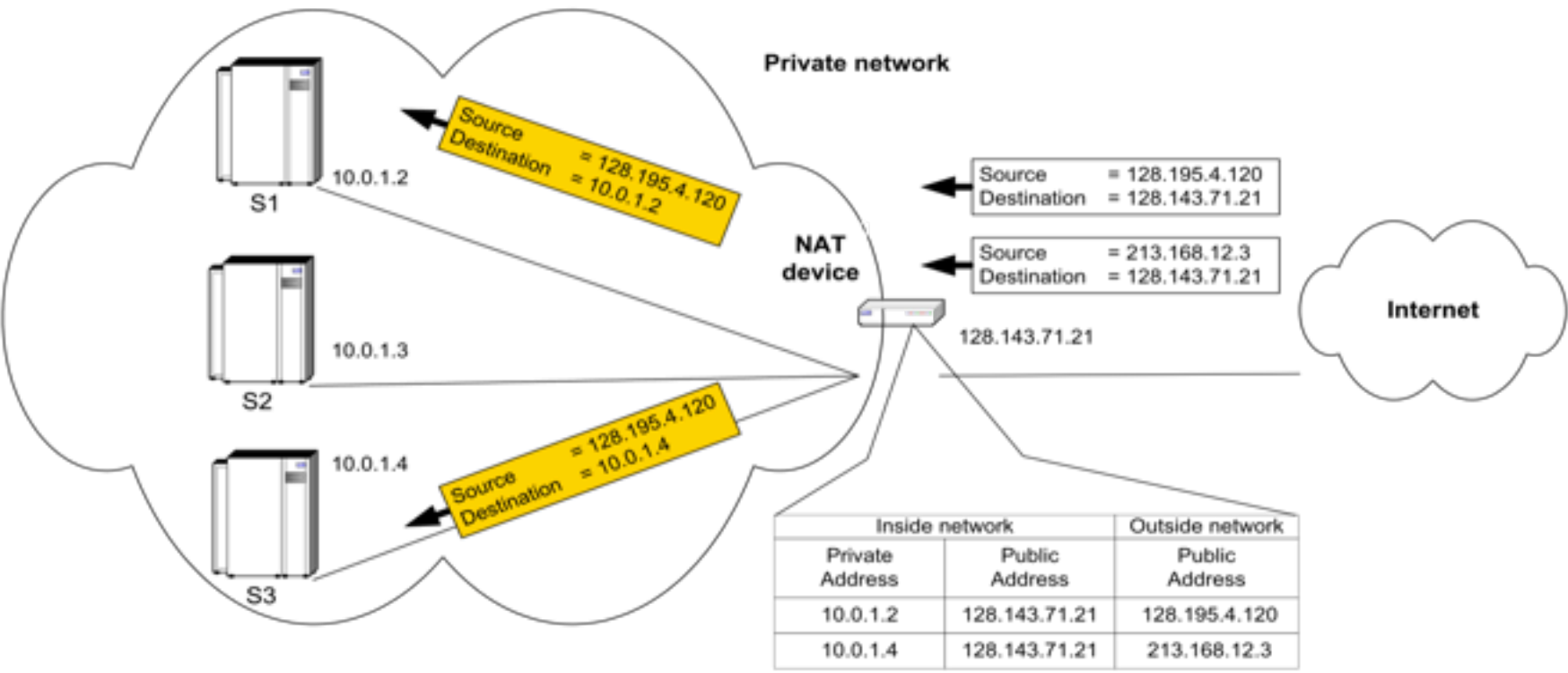
Concerns about NAT

- **Performance:**
  - Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum
  - Modifying port number requires that NAT boxes recalculate TCP checksum
- **Fragmentation**
  - Care must be taken that a datagram that is fragmented before it reaches the NAT device, is not assigned a different IP address or different port numbers for each of the fragments.

Concerns about NAT

- **End-to-end connectivity:**
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - The problem is worse, when two hosts that are in a private network need to communicate with each other.

Concerns about NAT

- **IP address in application data:**
  - Applications that carry IP addresses in the payload of the application data generally do not work across a private-public network boundary.
  - Some NAT devices inspect the payload of widely used application layer protocols and, if an IP address is detected in the application-layer header or the application payload, translate the address according to the address translation table.

NAT and FTP
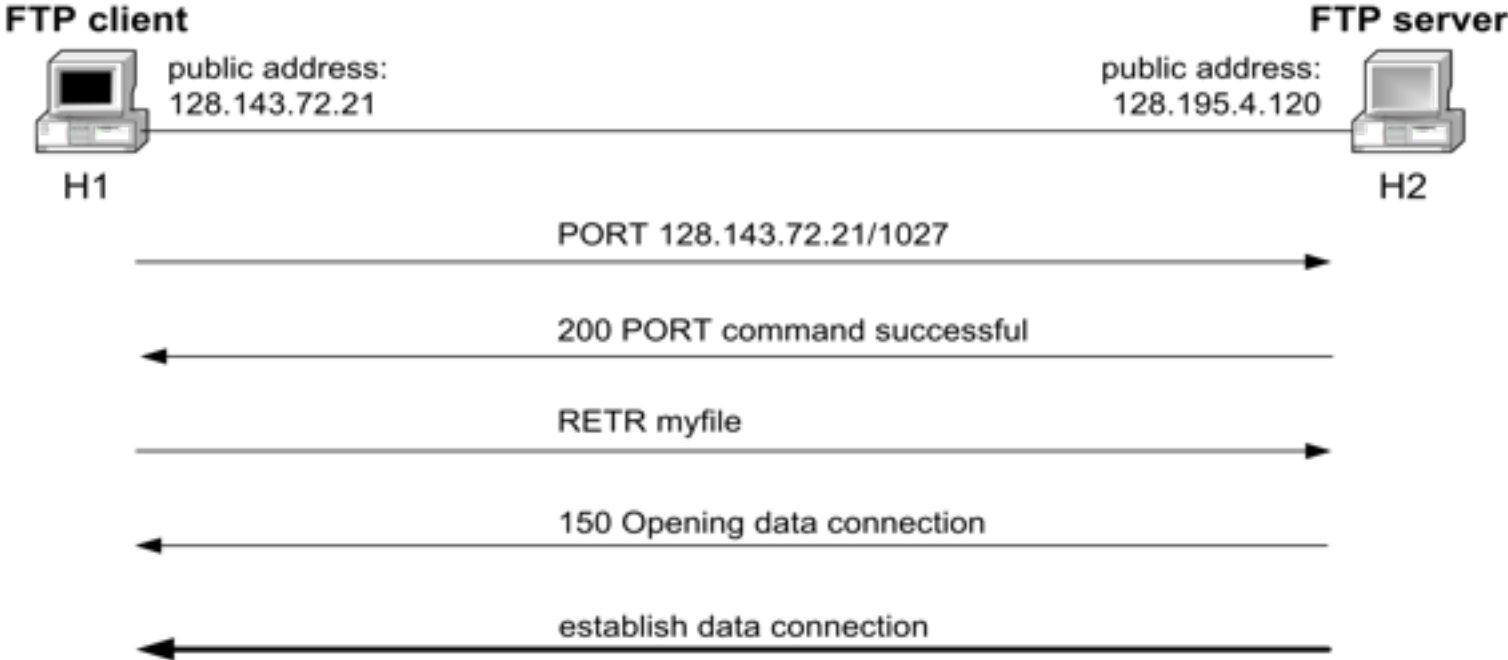
- Normal FTP operation

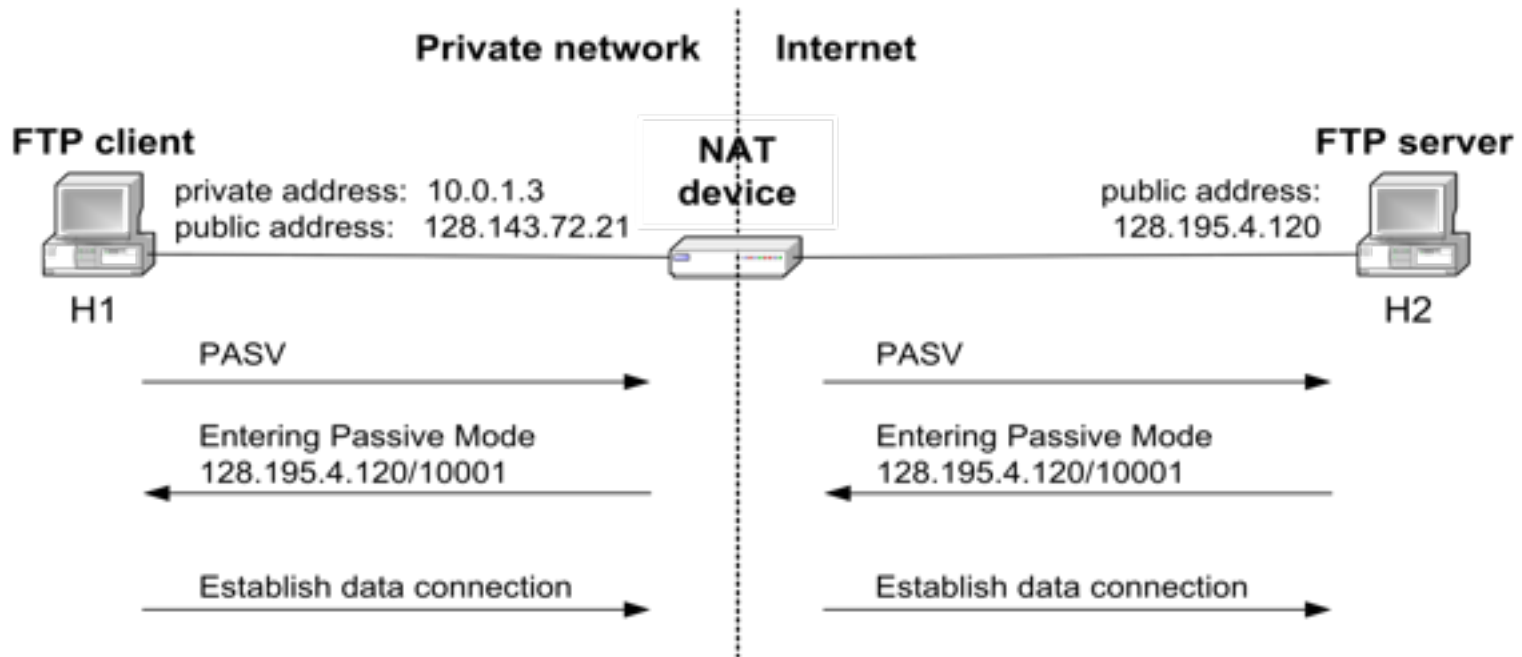# NAT and FTP
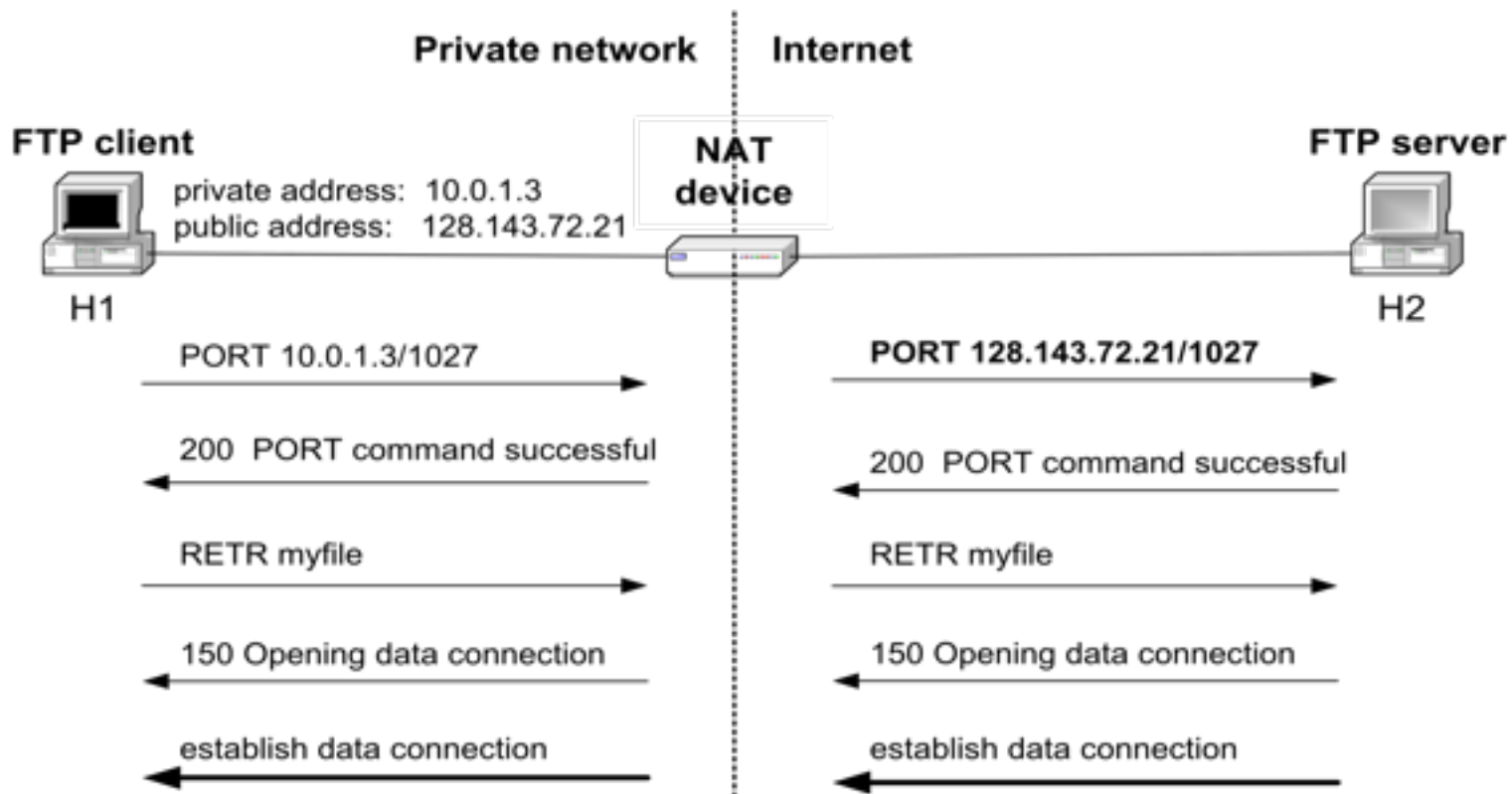
- NAT device with FTP support

NAT and FTP

- FTP in passive mode and NAT.