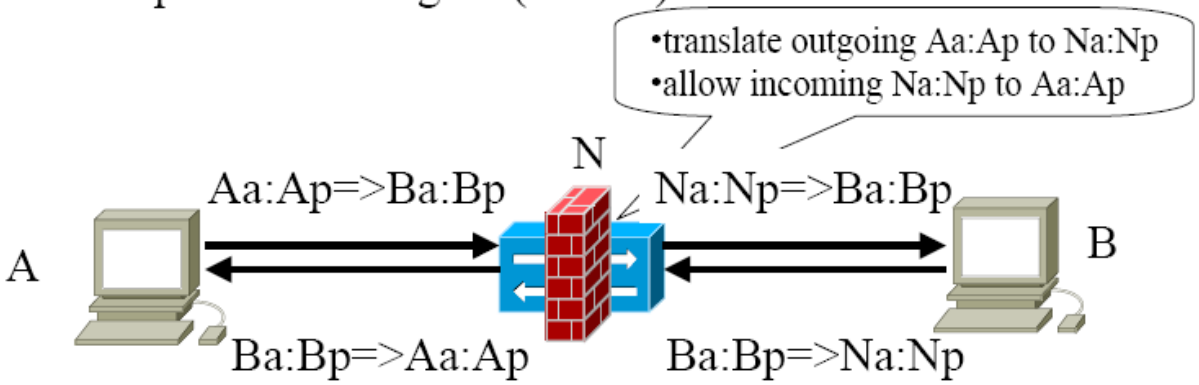
Communication: NAT

Firewalls and NAT

Firewalls and NATs

- firewalls and NATs usually work hand-to-hand
- firewalls: packet filtering w/ (known) rules

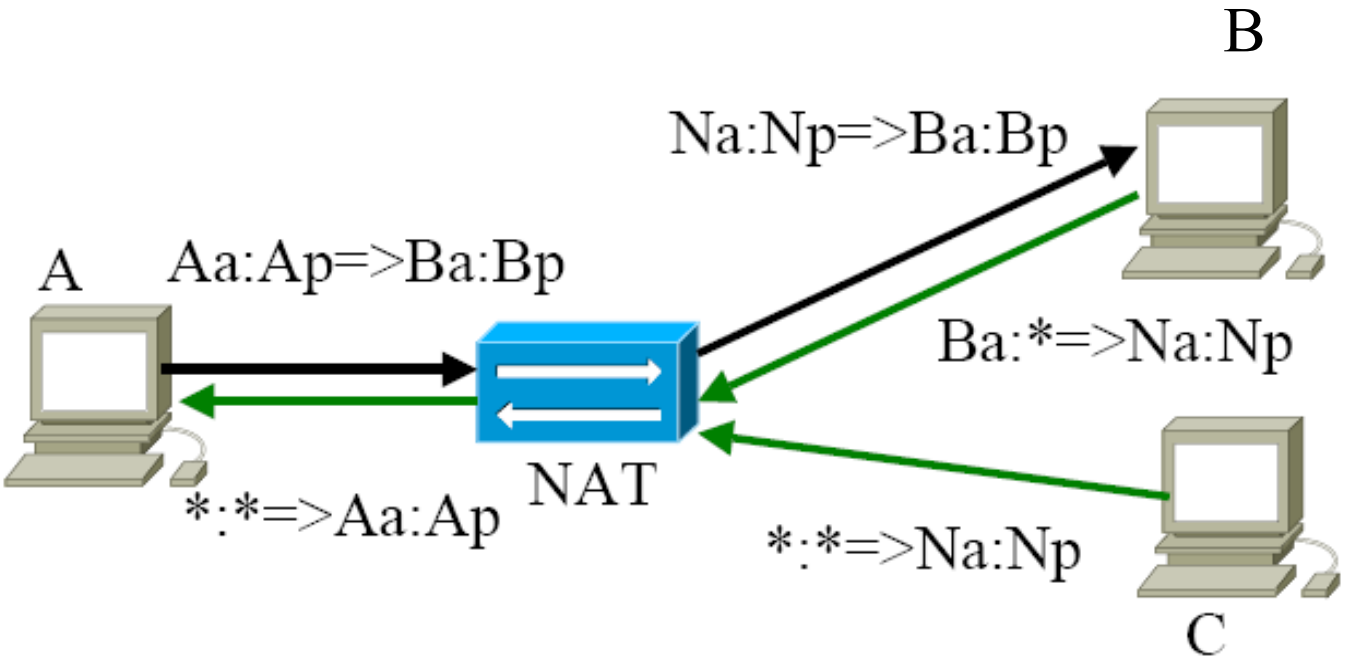


- NATs: initially as a *quick-fix* to IPv4 address shortage
- now pervasive in every networking scenario
- translate source/destination address/port
- update other related information (checksum etc.)

Four Types of NAT

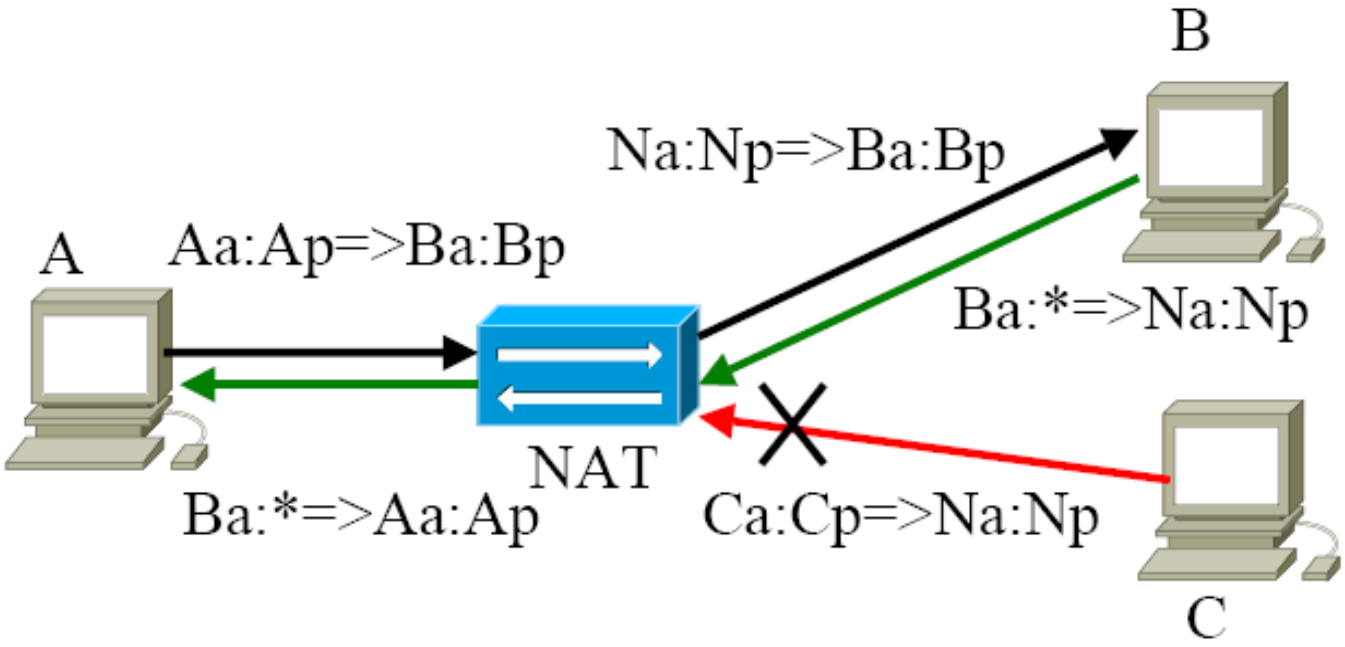
1. Full Cone NAT
2. IP Restricted NAT
3. Port Restricted NAT
4. Symmetric NAT

Full Cone: not very restricted



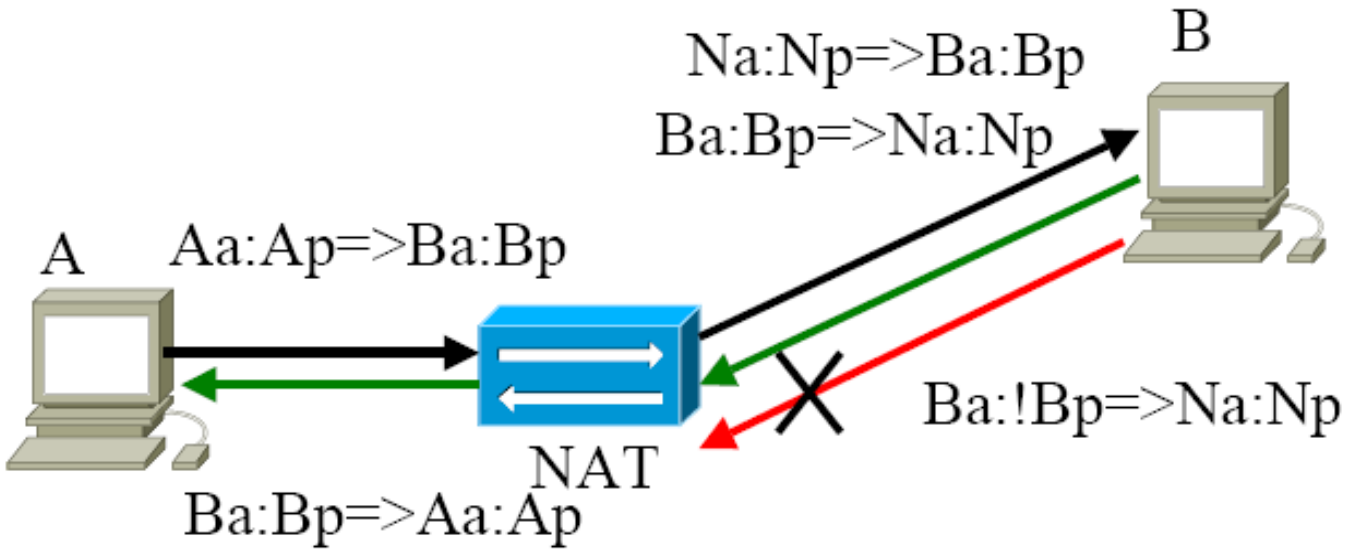
IP Restricted NAT

- Has restrictions on incoming IP



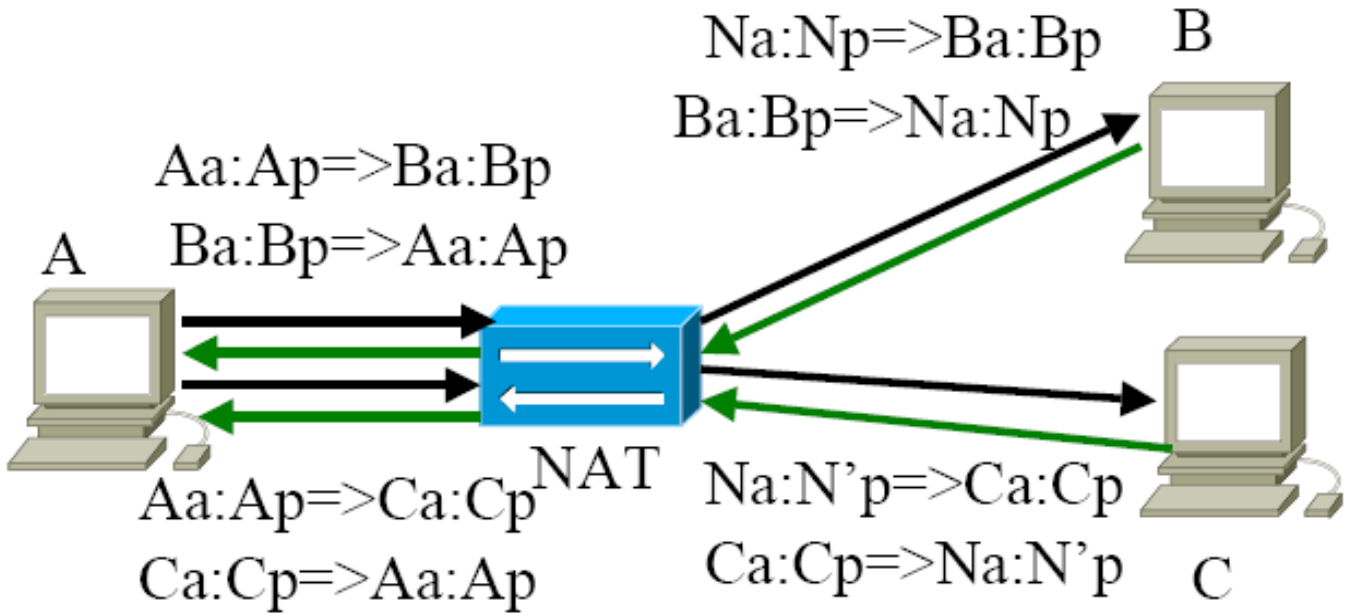
Port Restricted NAT

- Not only has restrictions on IP, but also on Port

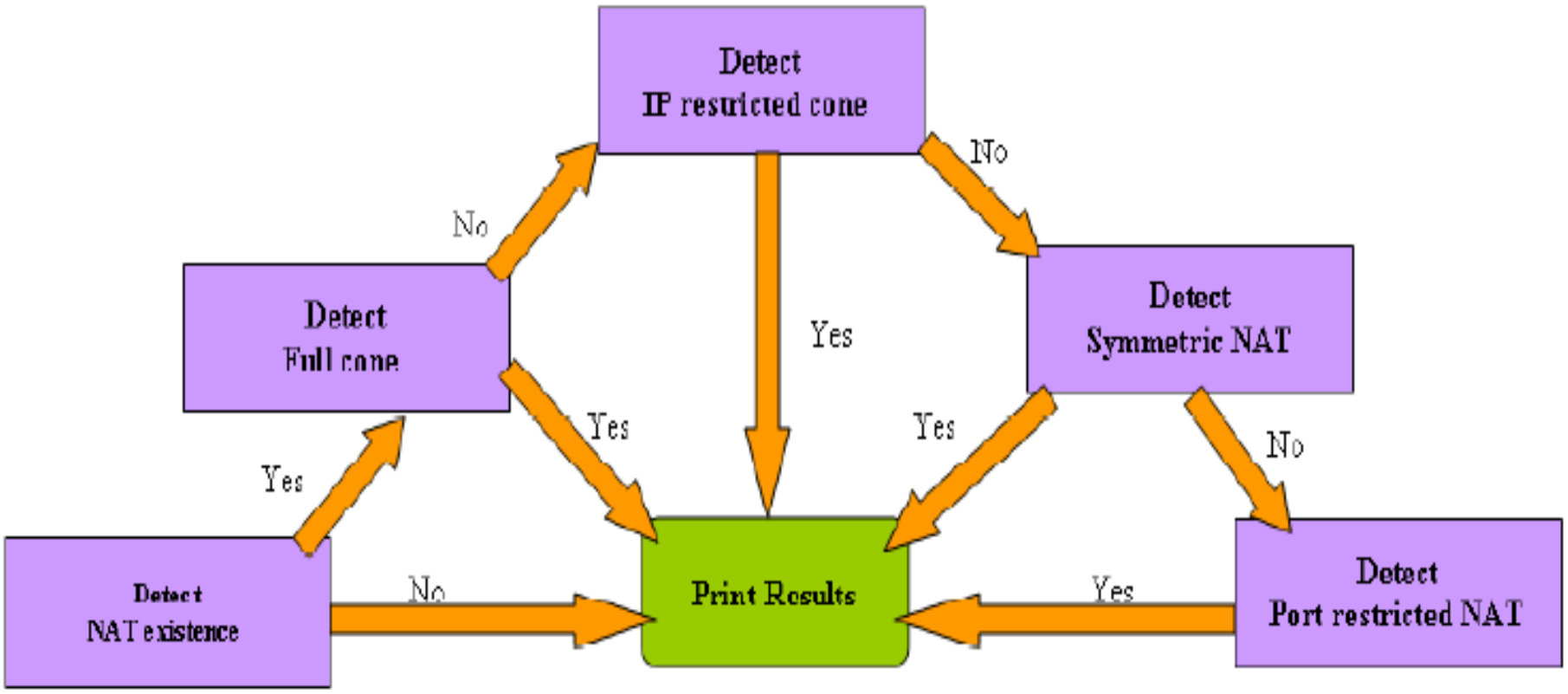


Symmetric NAT

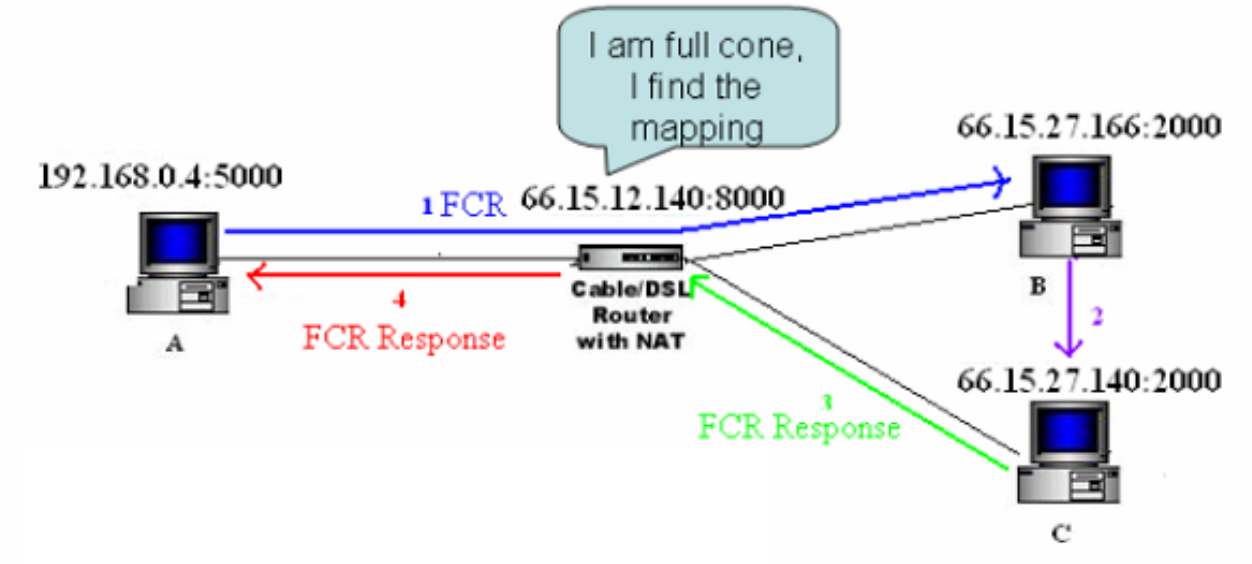
- Very restricted. New mapping for each different connection.



NAT Detection Flow



Example: Full Cone Detection

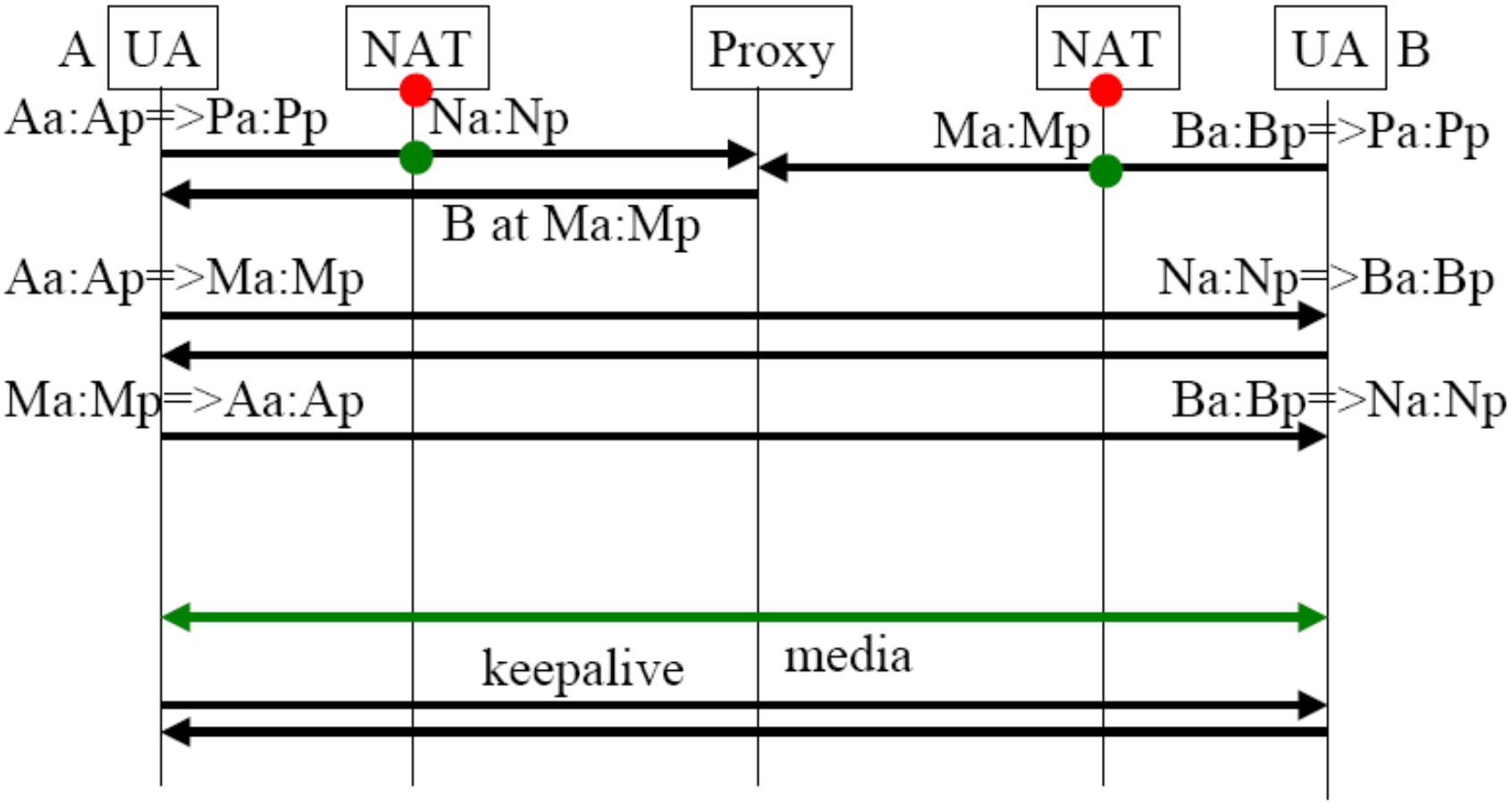


NAT Traversal

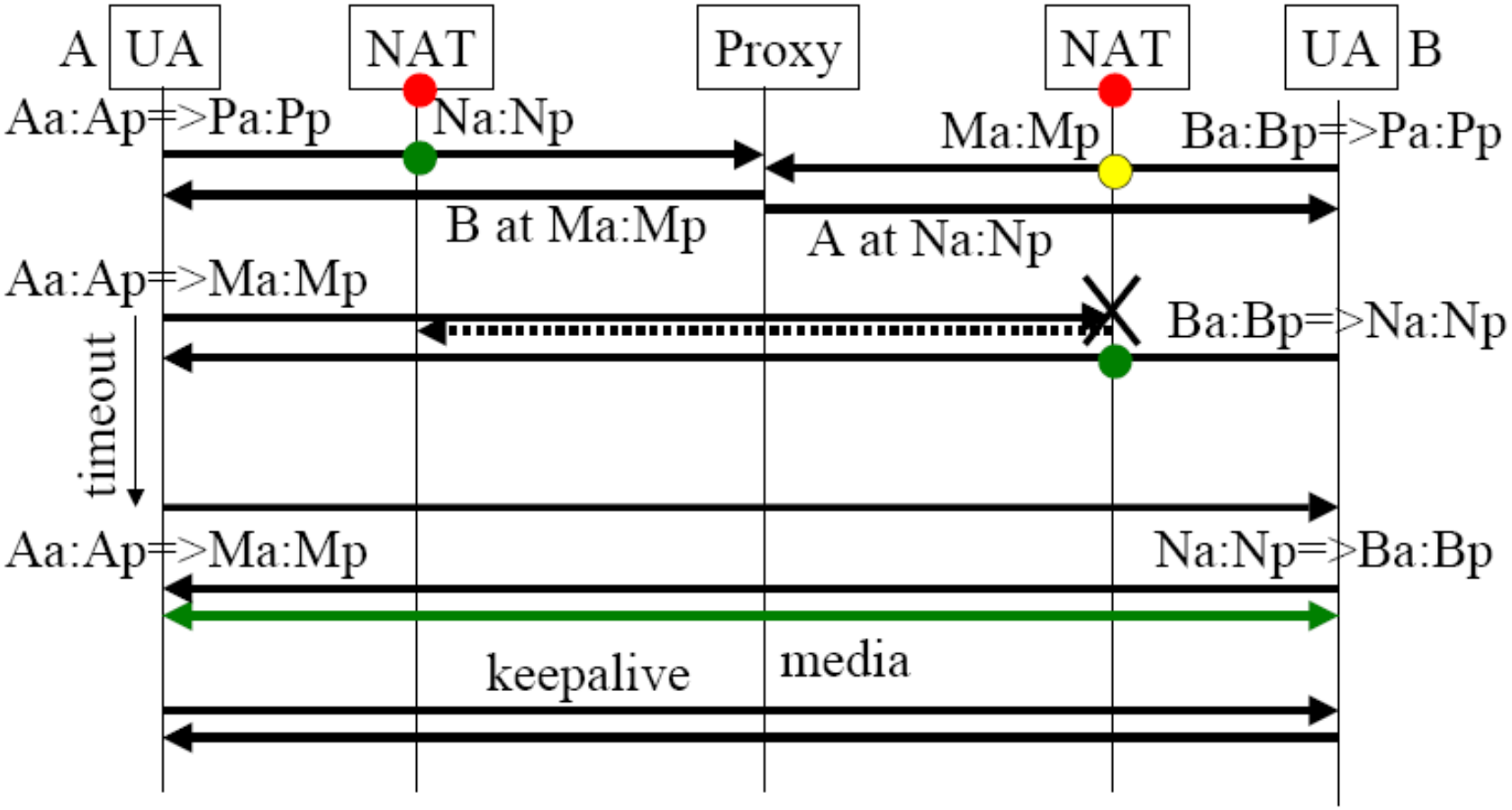
- NAT Traversal

A \ B	full cone	IP restricted	port restricted	symmetric
full cone	√	√	√	√
IP restricted		√	√	√
port restricted			√	?
symmetric				?

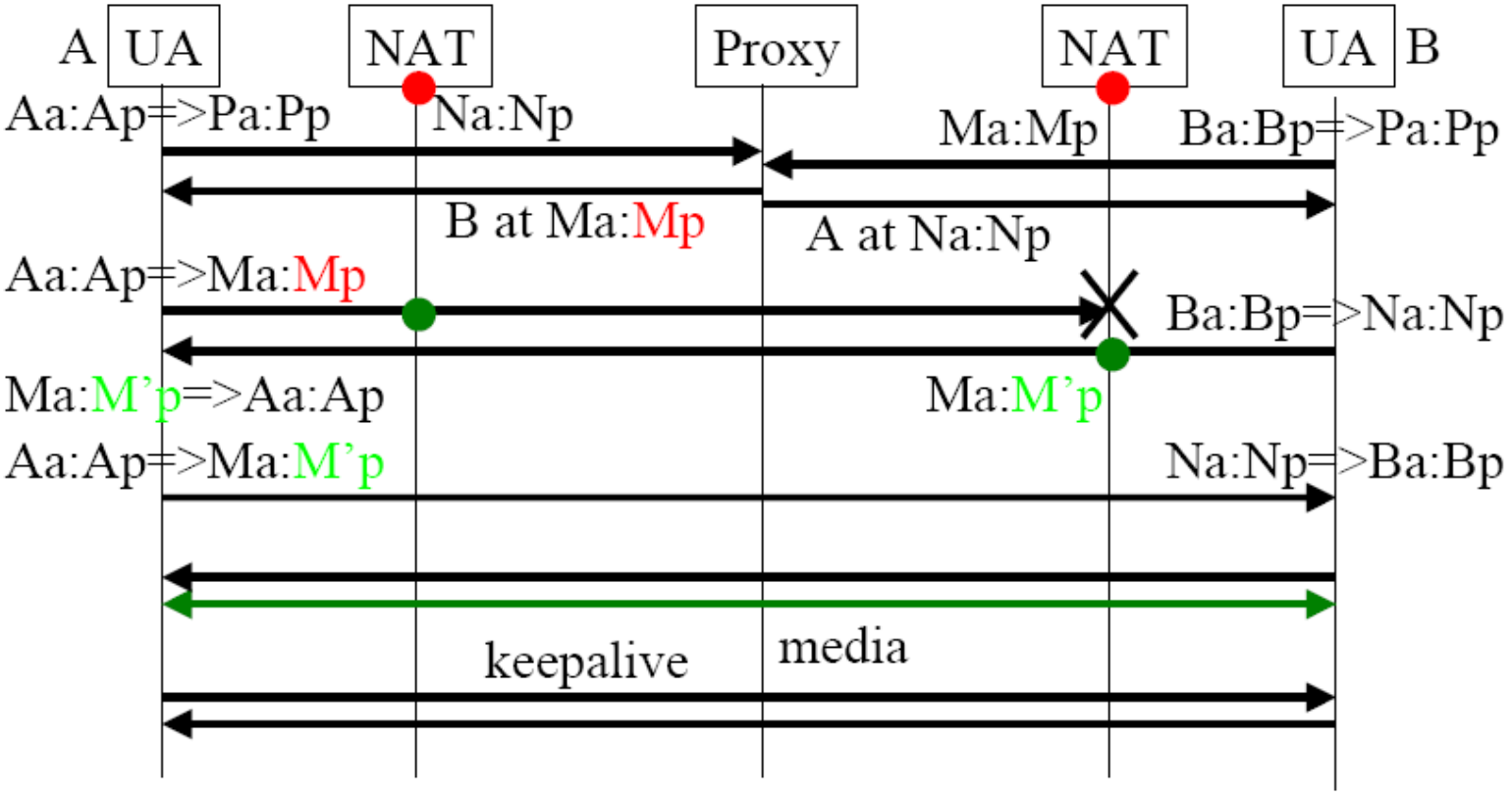
Full Cone-Full Cone



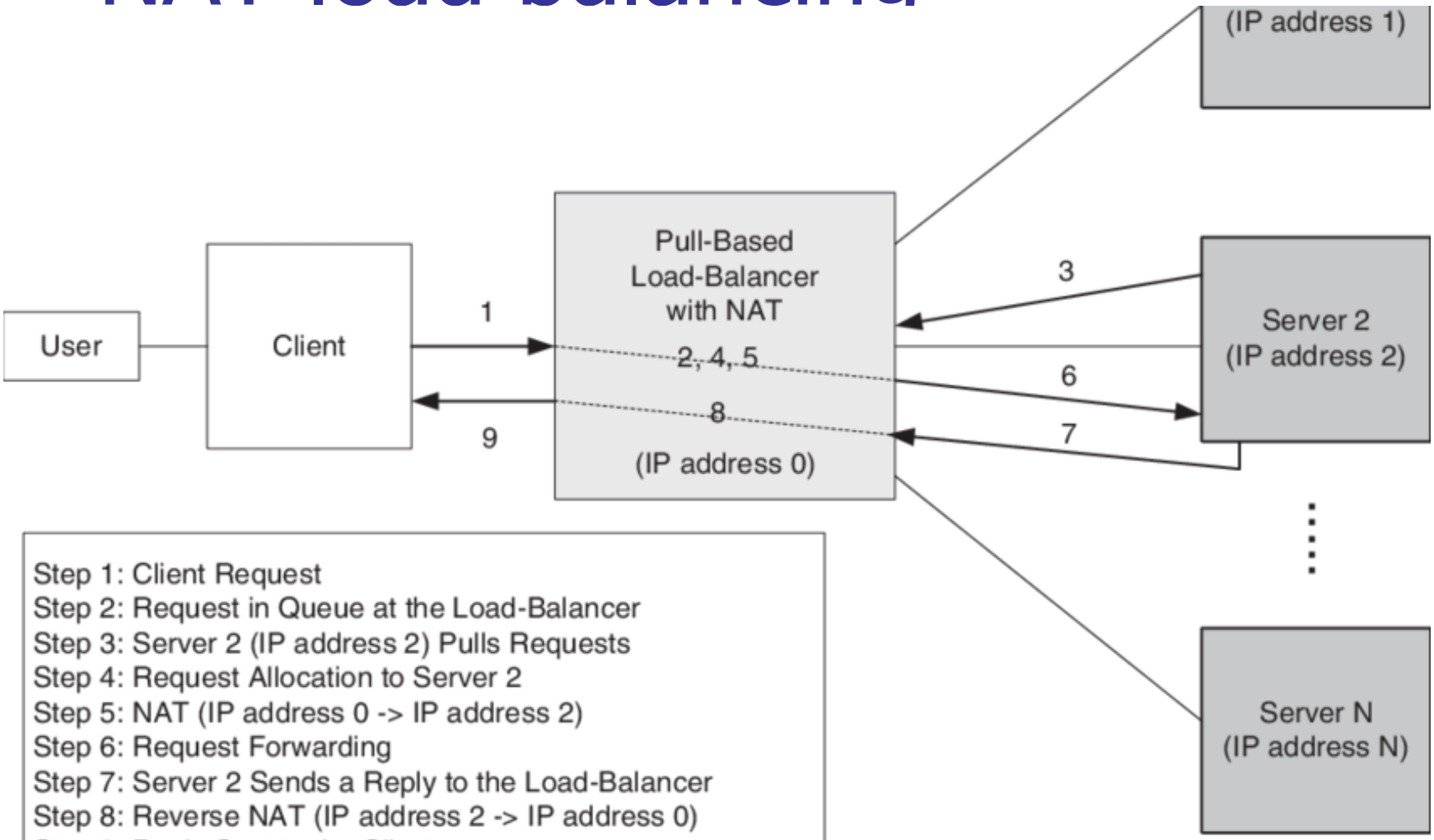
Full cone/IP restricted



Full cone/Port restricted-symmetric

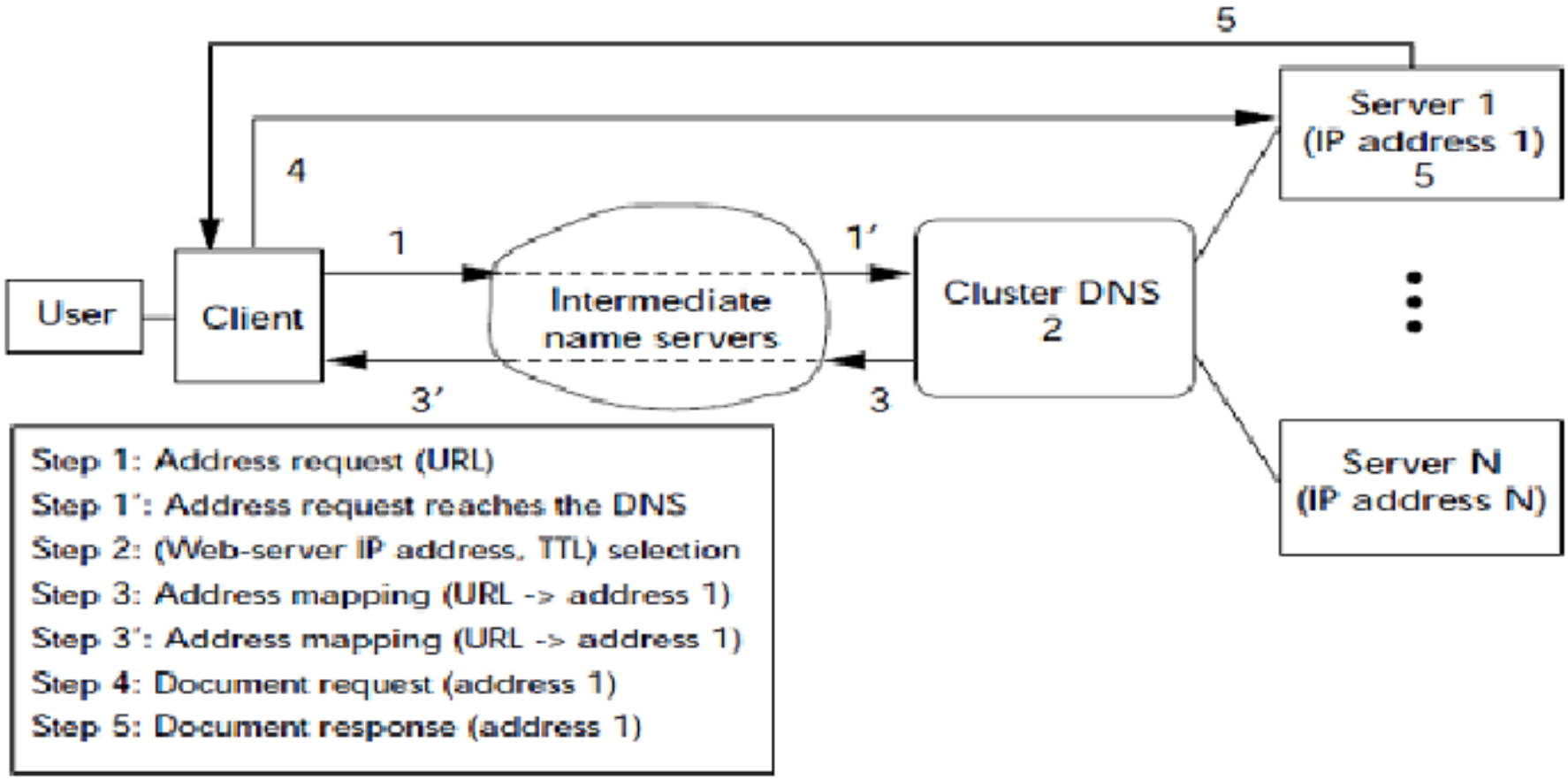


NAT load balancing

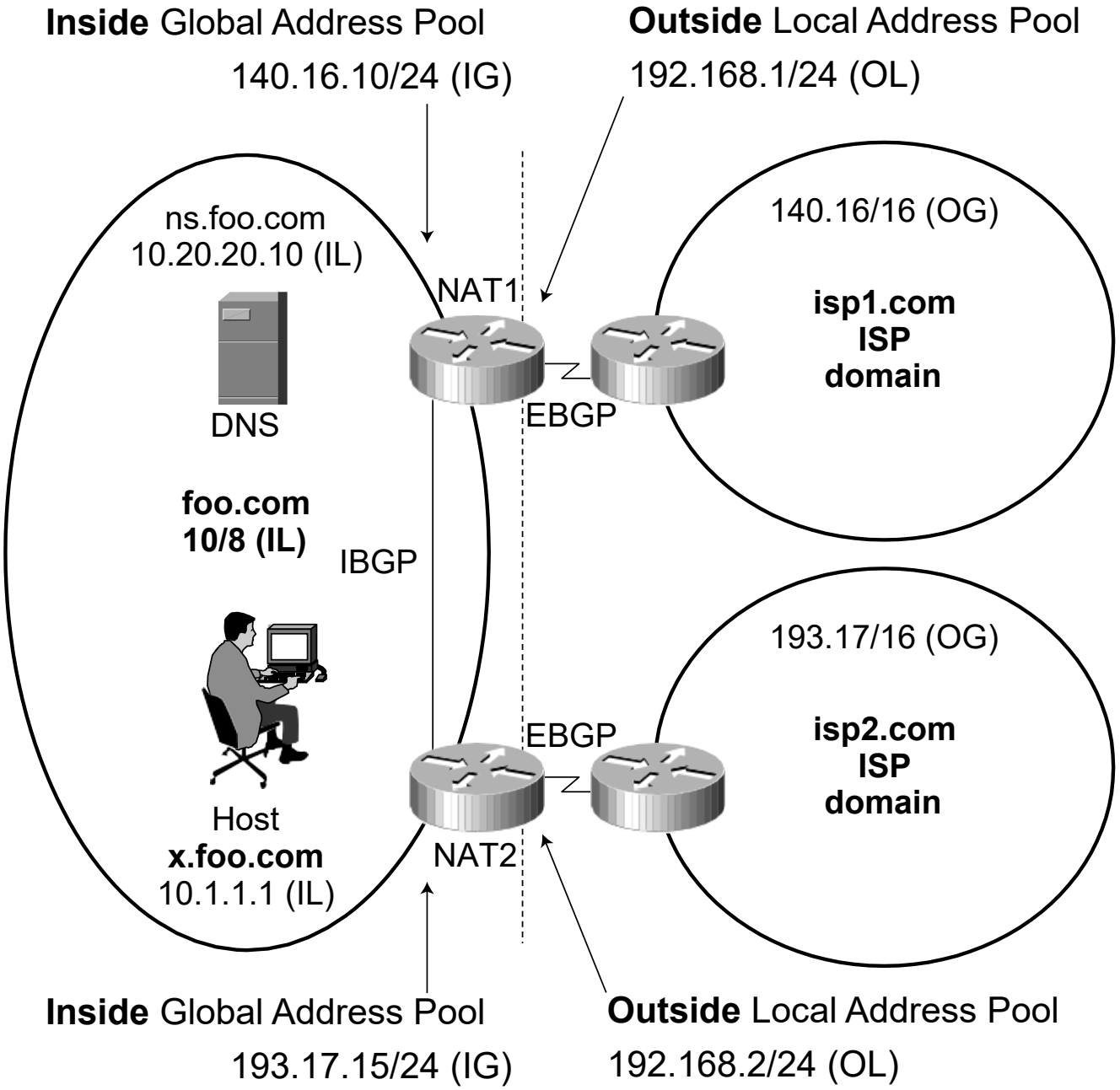


Step 1: Client Request
Step 2: Request in Queue at the Load-Balancer
Step 3: Server 2 (IP address 2) Pulls Requests
Step 4: Request Allocation to Server 2
Step 5: NAT (IP address 0 -> IP address 2)
Step 6: Request Forwarding
Step 7: Server 2 Sends a Reply to the Load-Balancer
Step 8: Reverse NAT (IP address 2 -> IP address 0)
Step 9: Reply Sent to the Client

DNS load balancing

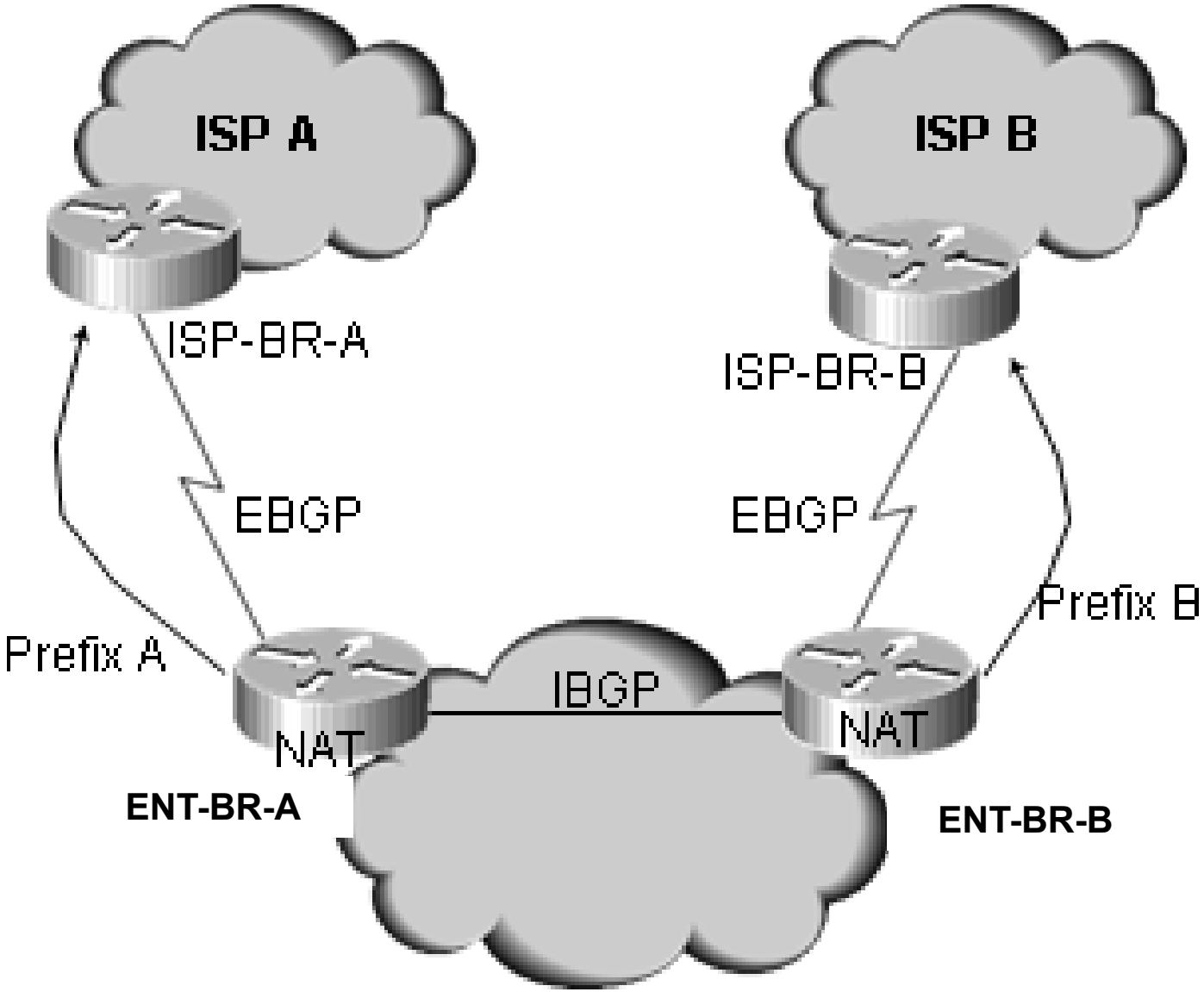


NAT MULTIHOMING



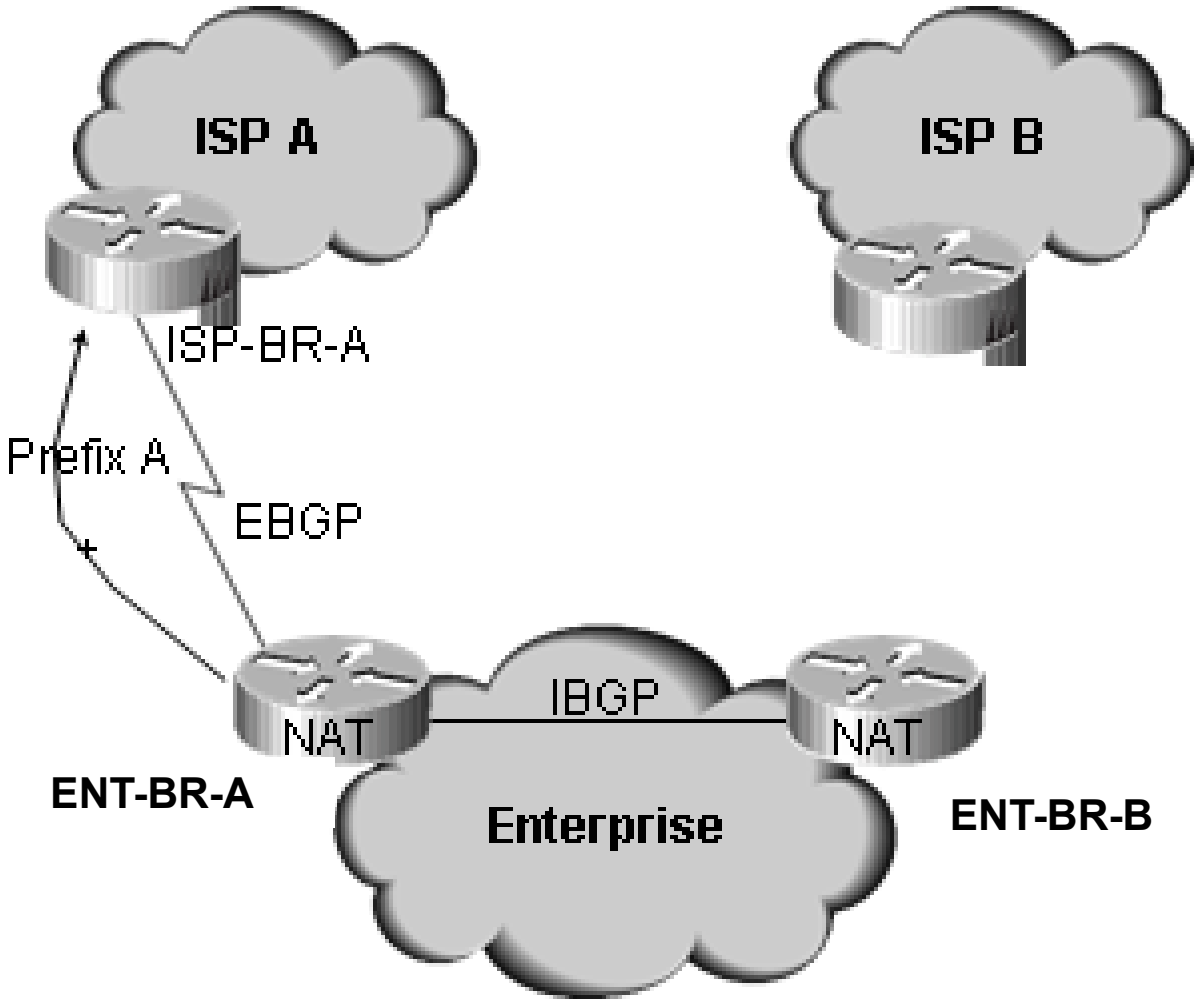
NAT MULTIHOMING

Auto route injection – steady state



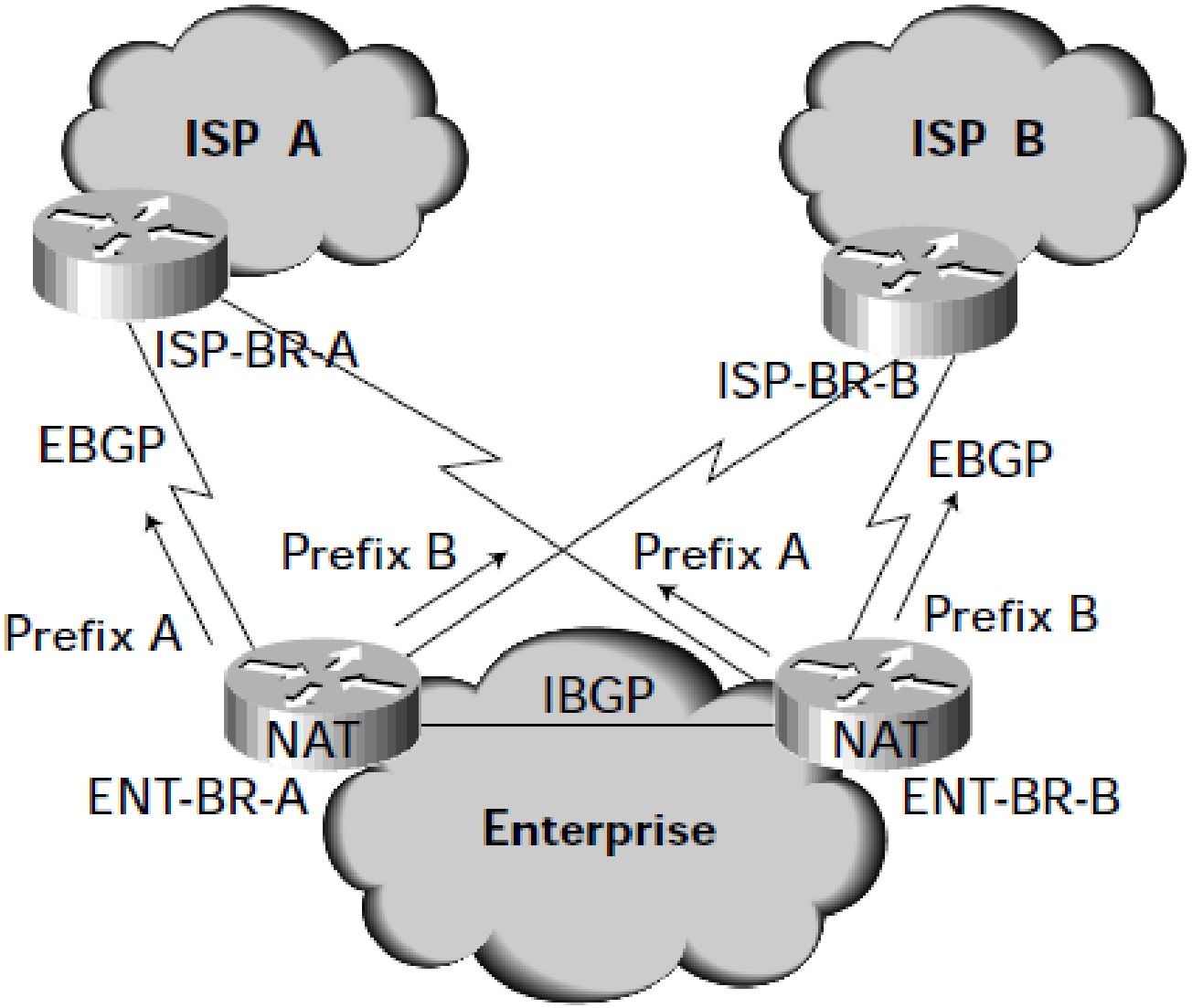
NAT MULTIHOMING

Auto route injection – broken connection



NAT MULTIHOMING

Non-Direct EBGP peering – steady state



Non-Direct EBGP peering – broken connection

NAT MULTIHOMING