VPNs and NAT

Literature:

Forouzan: TCP/IP Protocol Suite : Ch 26

Private Networks

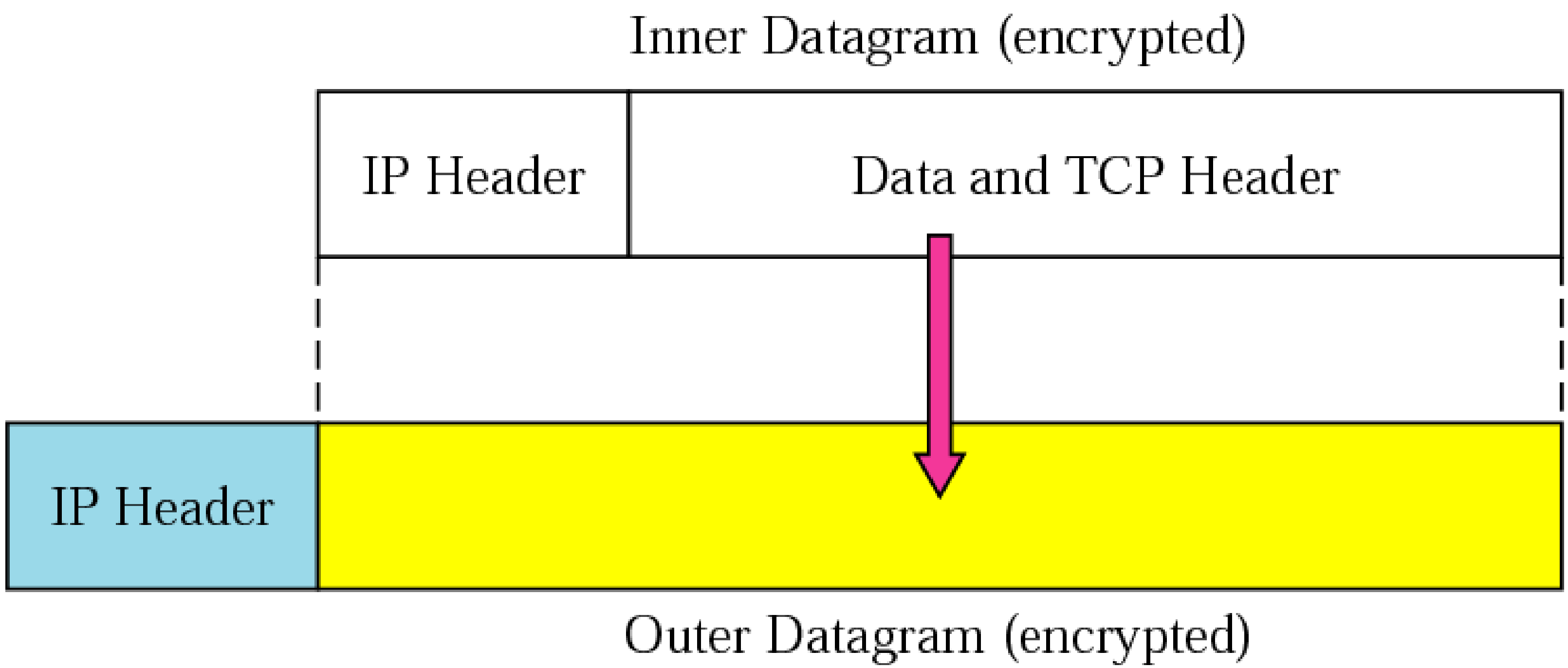
- Designed to be used within an organization
- Access to shared resources
- Provides privacy
- Intranet
  - Access to network limited to users within the organization
- Extranet
  - Some resources may be accessed by specific users outside the organization.
- Addressing
  - Global addresses
    - Future proof - but are not accessible
  - Private addresses
    - Need NAT to access Internet

Motivation and challenges for VPNs

- To build a long distance private network by leased lines is expensive
- Could the same service be offered on top of a public network (Internet)?
- This would be cheaper
  - Existing infrastructure can be re-used
- But to build a VPN we need to address:
  - Privacy
    - others cannot see our data
  - Addressing and routing
    - Internal addresses used within private networks
    - External addresses used on the Internet

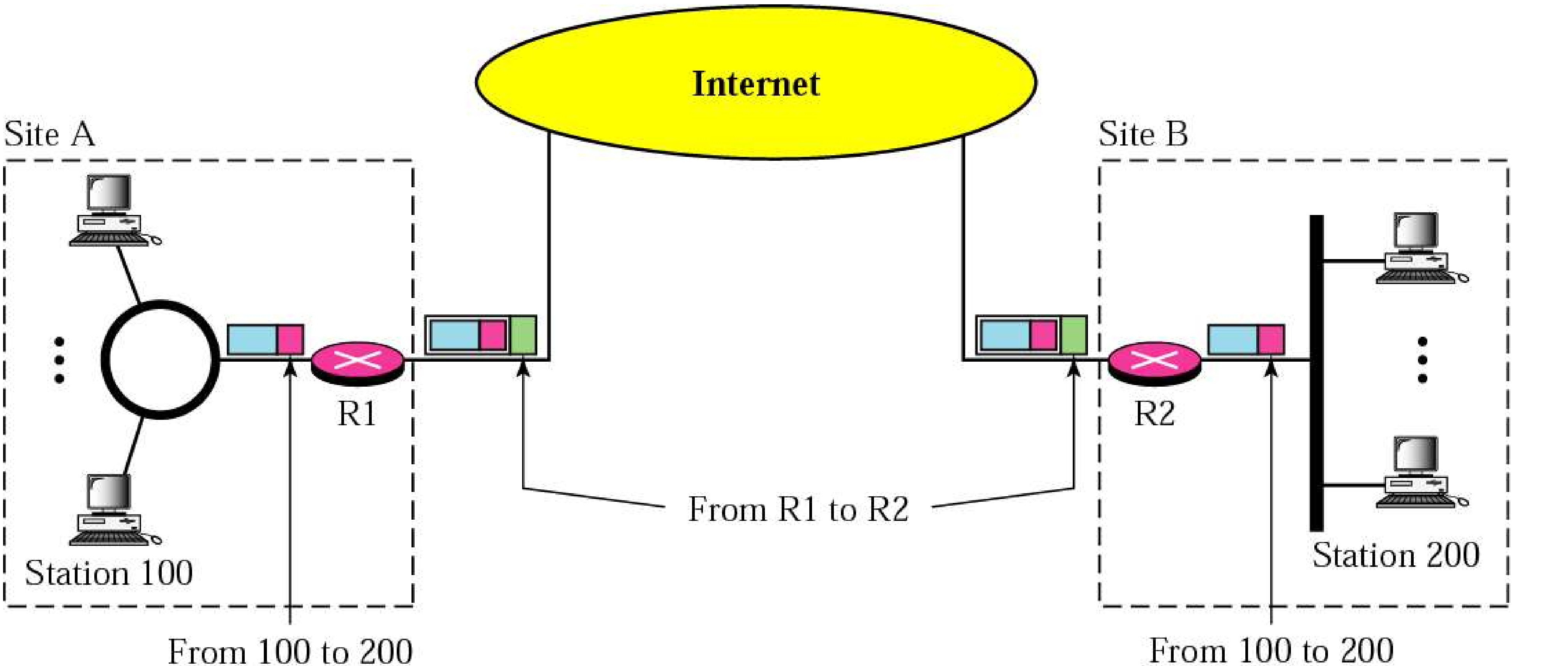
Tunneling and Privacy

- Encapsulate the private datagram within another datagram
- Privacy: encrypt the private datagram
- Problem: Who can you trust to encrypt the data?
  - only yourself
  - the ISP providing the VPN
  - some third party



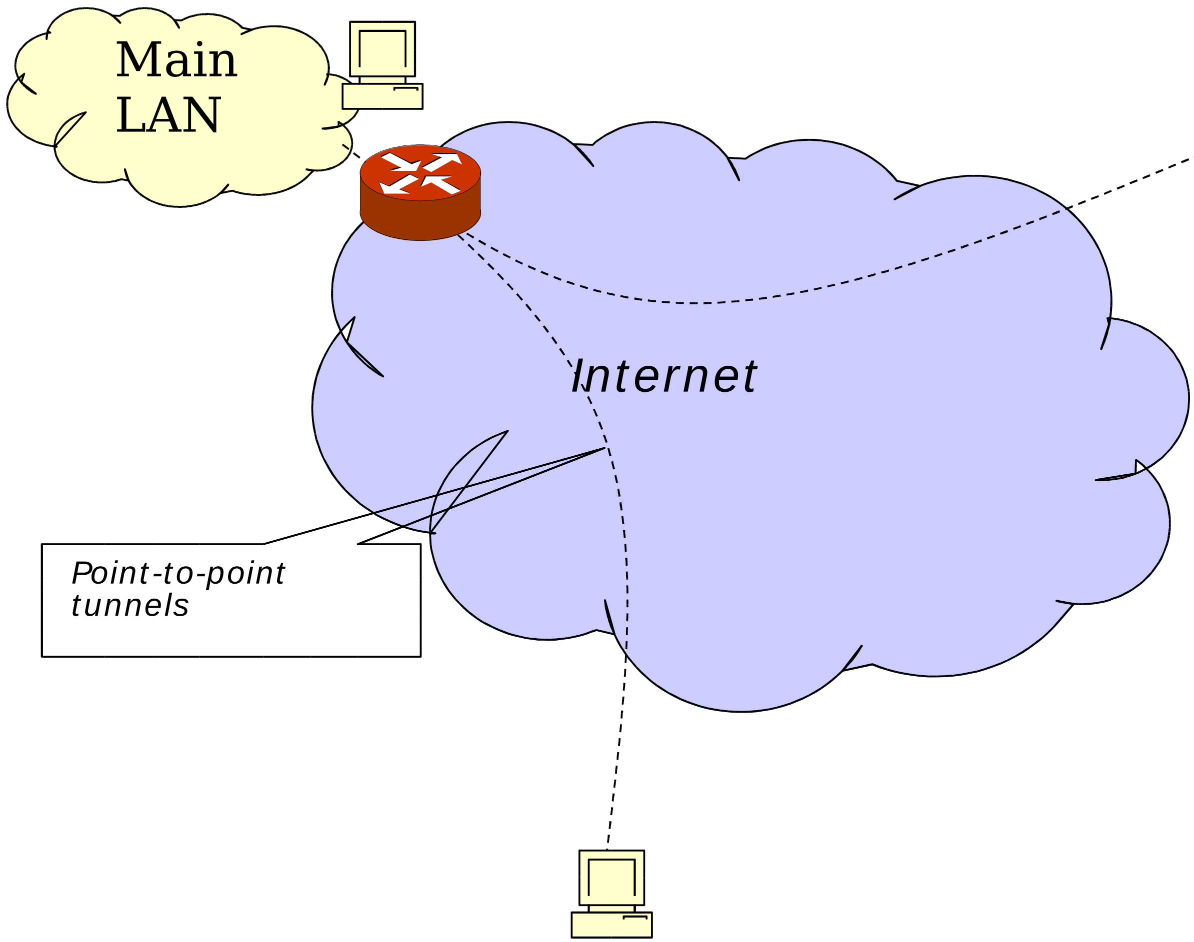
Addressing

- The Internet carries the tunneled datagram from R1 to R2 using public addressing
- R1 encapsulates, R2 decapsulates
- Public versus private addressing



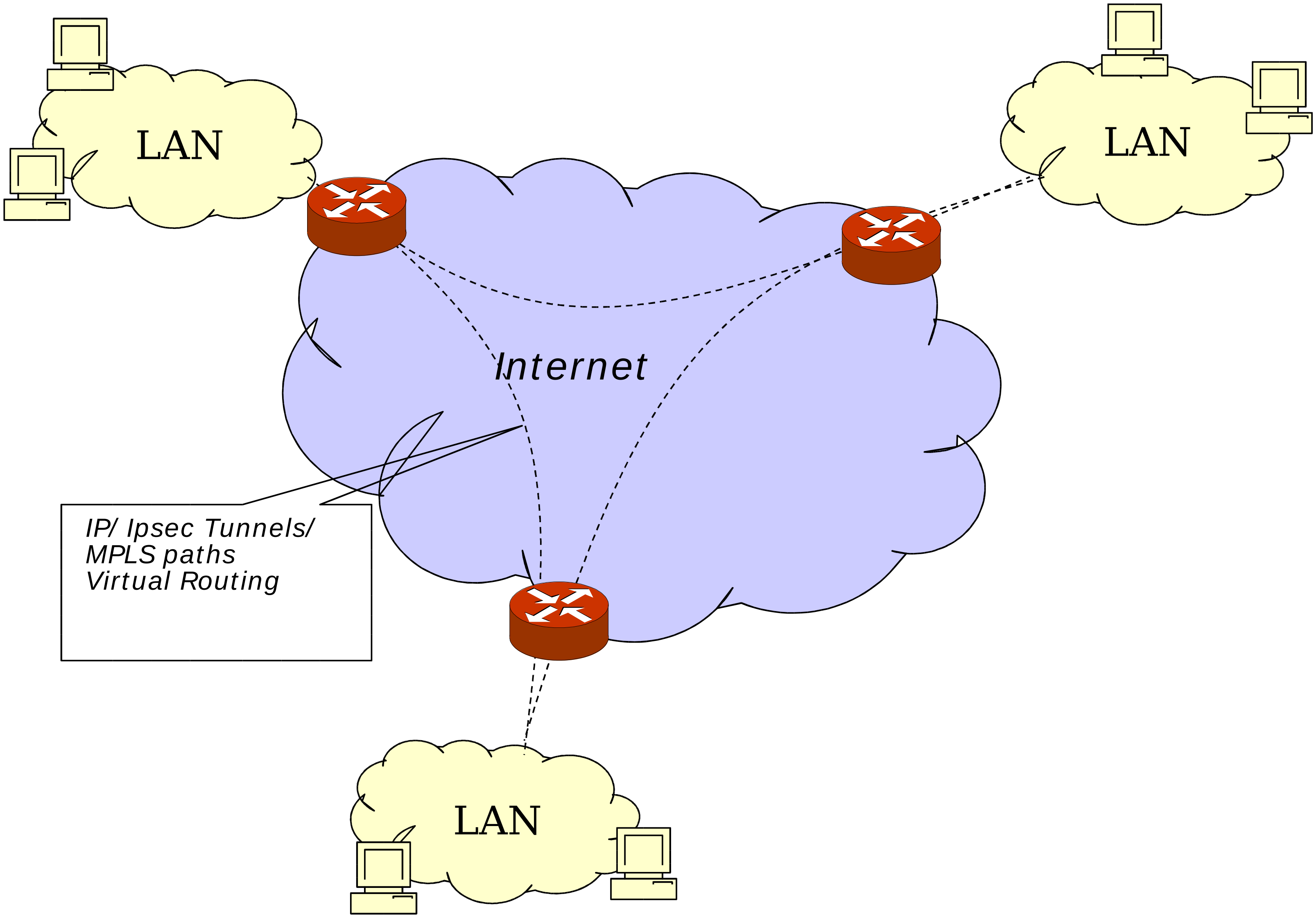
VPN Architecture 1

Connect hosts to central server.



VPN Architecture 2

Connect several LAN “islands”.



L3 VPN

- LANs connect to a router that routes the datagrams between sites.
- IP/IPsec tunnels
  - Point-to-point
  - Full mesh between peers
- Virtual Routing
  - Separate routing tables
  - Different address domains
- MPLS/BGP
  - RFC 2547’’
  - Set up MPLS point-to-point paths over a network
  - Good for Traffic Engineering purposes
  - No need to export customers routing tables into the network

L2VPN

- LAN interconnection may be done by tunneling layer 2 frames (eg Ethernet) over an (IP) network. Most are point-to-point and for dial-up services
- Layer-2 Forwarding (L2F)
- Point-to-point Tunneling Protocol (PPTP)
  - In Windows 95/NT
- Layer Two Tunneling Protocol(L2TP)
  - RFC 2661
  - PPP based
- VPLS
  - Virtual Private LAN Services (IETF PPVPN)
  - Multi LAN

Traffic Engineering

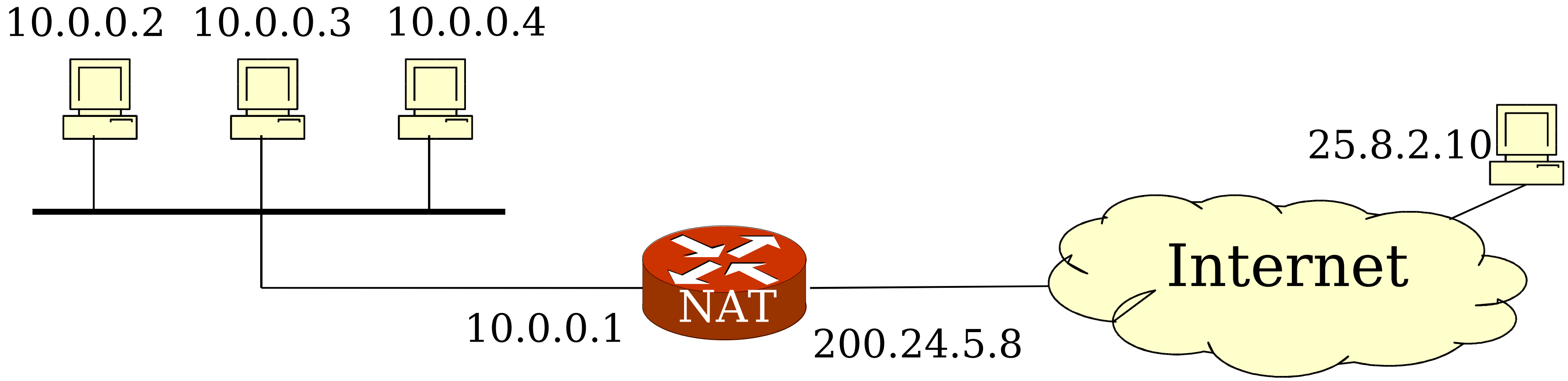
- Many VPN services provides ”QoS”
  - To ensure service for internal traffic
- Provider wants to guarantee a service to VPN customers.
  - No delays
  - No packet loss
  - Eg Telephony over IP (VoIP or tunneled E1:s)
- Typical solution use MPLS
  - Fixed path through a network where resources are allocated
  - RSVP-TE
    - Aggregated traffic with bandwidth guarantees
  - OSPF-TE

Network Address Translation (NAT)

- How can we use private addresses and communicate with the global Internet?
- How can we use more addresses than our ISP assigned us?
  - We may only get one or a pool of IPv4 addresses
  - But we have many local machines
- Solution: IPv6
  - Plenty of addresses
- Or NAT/NAPT

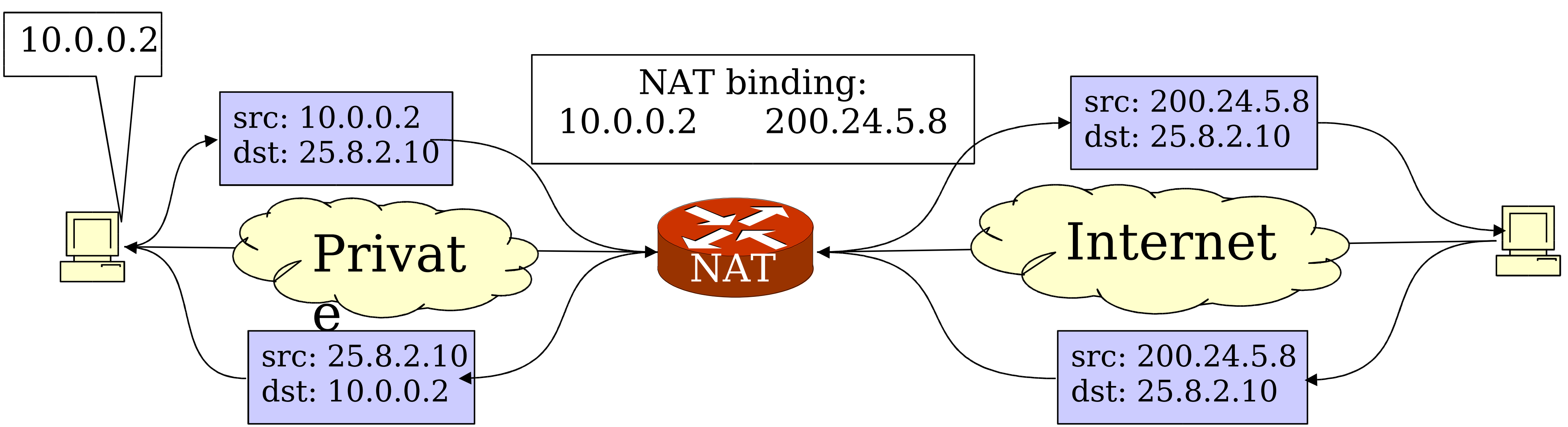
Network Address Translation (NAT)

- Internally, there are many hosts with private addresses
- But the outside world sees only one global address
  - Or a set of global addresses
- The NAT router translates between local (private) and global addresses
  - Typically use private IPv4 addresses, eg 10.0.0.0/8.
  - Translate them to global addresses



Address Translation

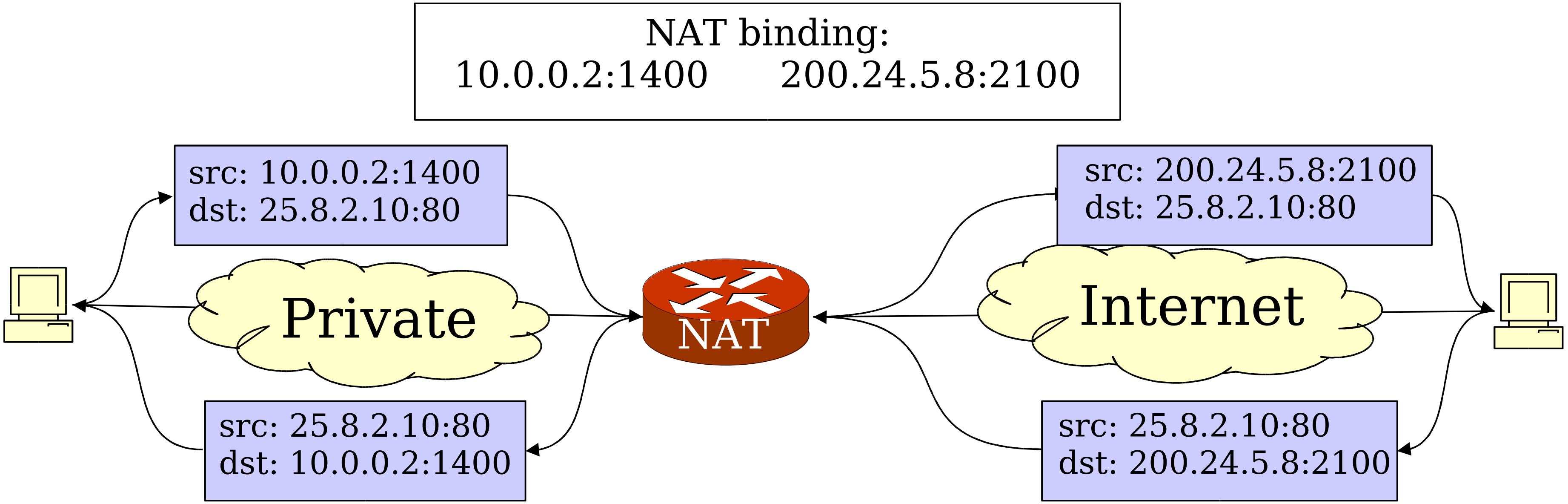
- Eg, a client accesses a global server
- Dynamic table driven from the inside
- Outgoing packets
  - source private address is replaced by global address
- Incoming packets
  - destination global address is replaced by private address



Extending the mapping: NAPT

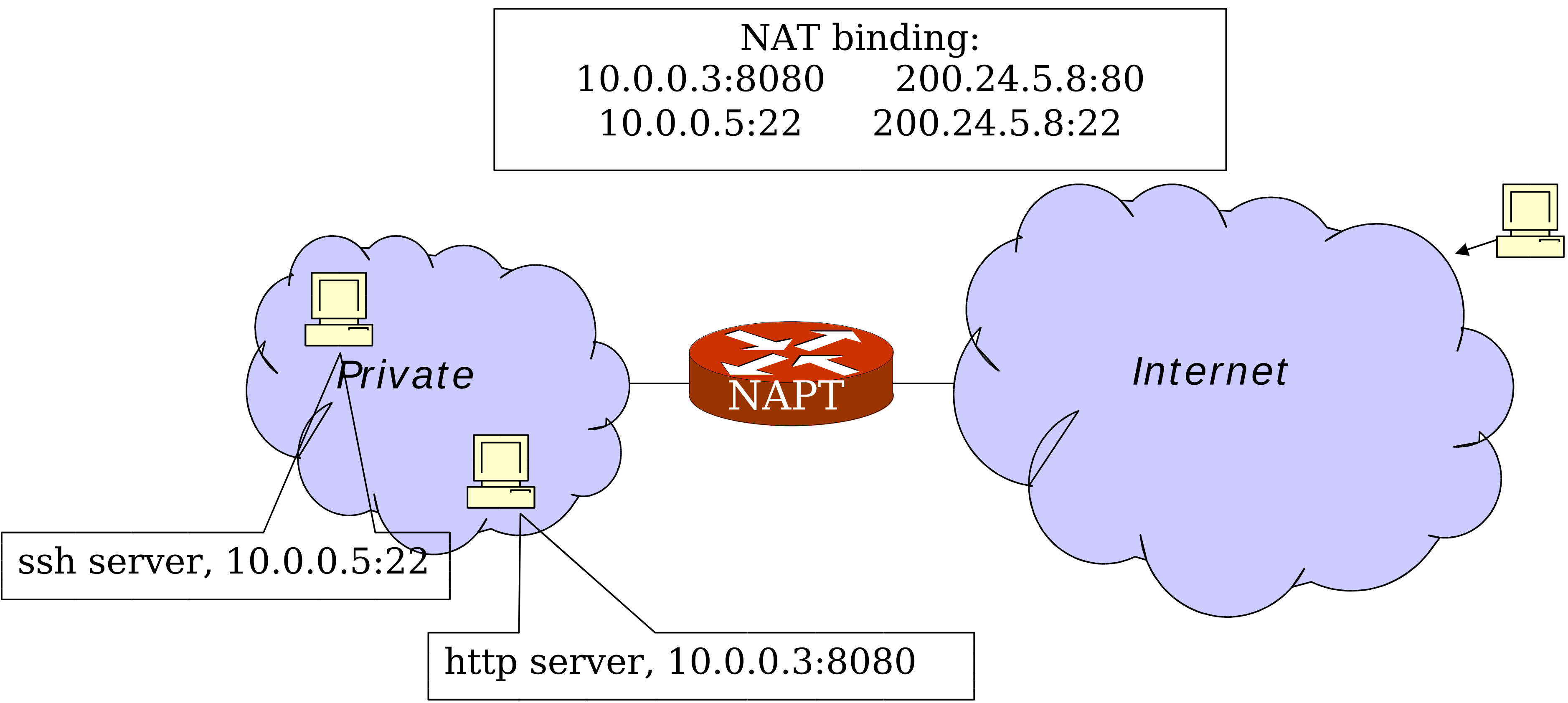
- One-to-one address mapping may be too restrictive and static
- Use the L4 port numbers
- Map local address + port   global address + port
- Network Address Port Translation
- Extends the address space with 2^{16} port numbers
- Limited to TCP/UDP
- Some problems with other protocols and applications

NAPT Example



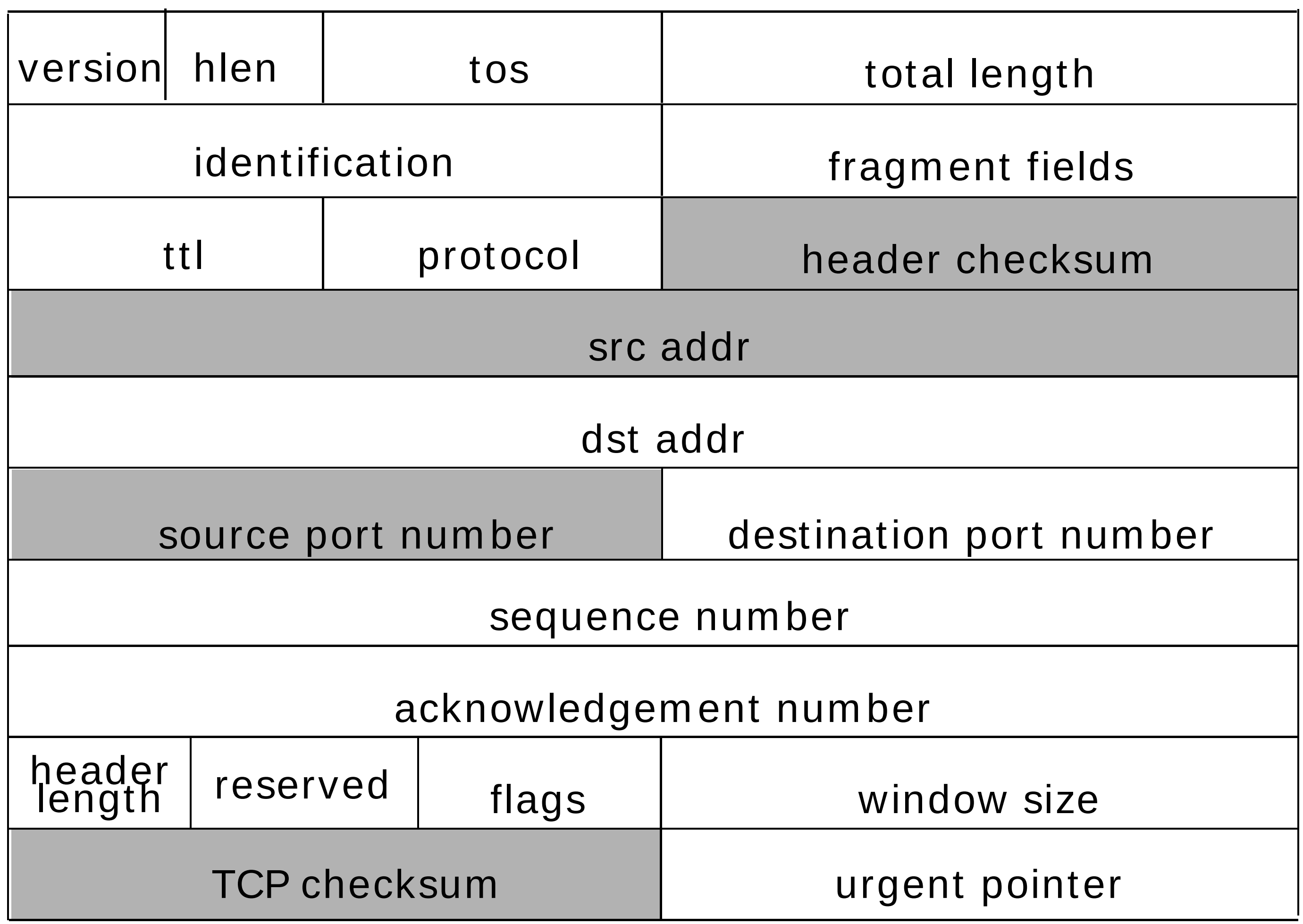
NAPT to access internal servers

- Servers on the inside needs to be accessed from the outside.
  - ssh server at 10.0.0.5
  - http server at 10.0.0.3 (port 8080)



Rewriting of header

Example: TCP packet sent from inside to outside

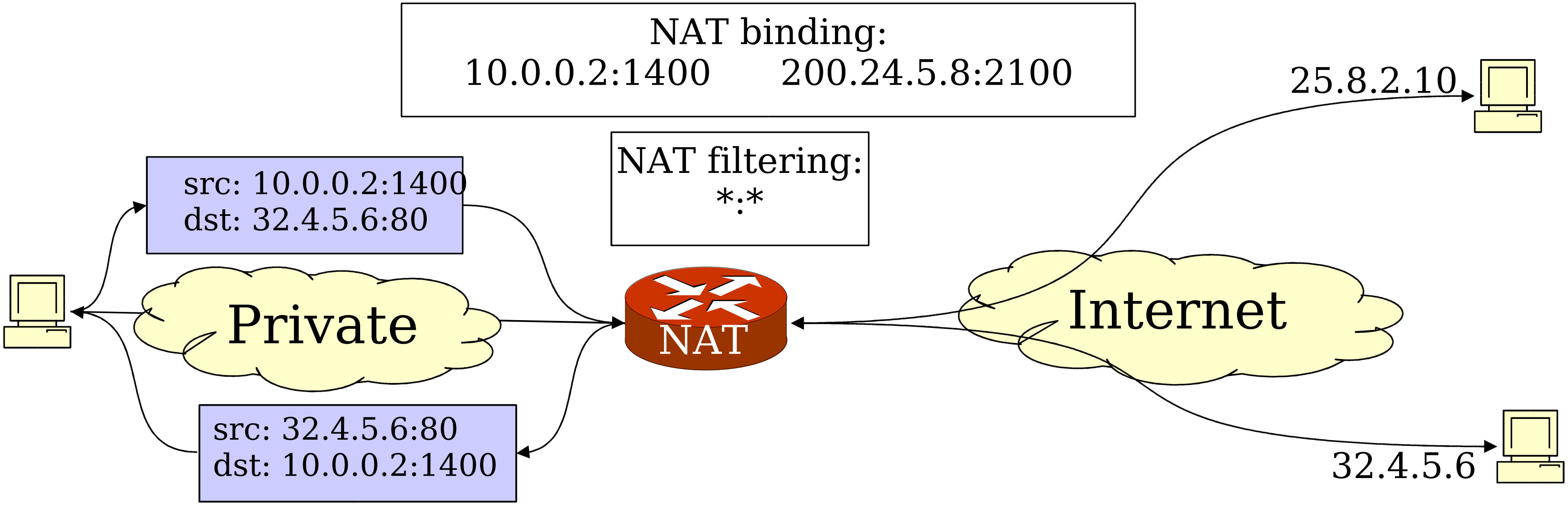


But NATs also filter addresses

- A NAT has also filtering – to restrict which external peers can communicate with the internal host
- So other peers can use the ”hole” in the NAT opened by an initial communication
- This can be used by peer-to-peer applications to make ”NAT-traversal”
  - Otherwise, two hosts behind NATs can never communicate
  - Important for interactive applications eg VoIP
- Only for UDP
  - TCP has state (eg sequence numbers) that can not be re-used

Full Cone

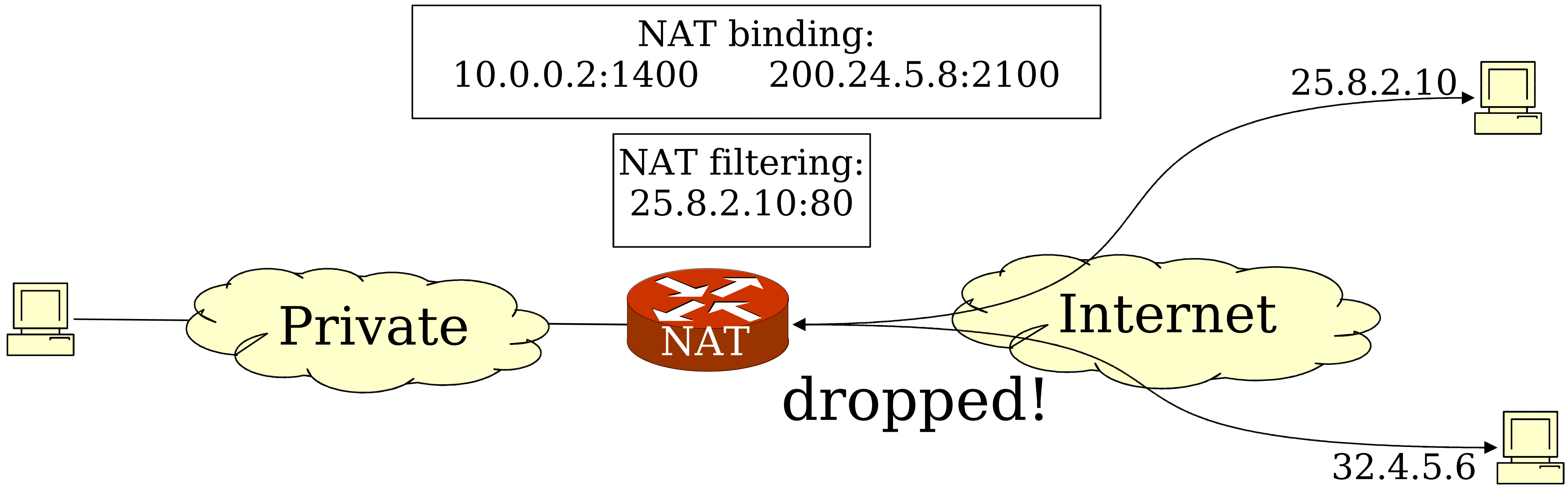
- Full cone – No filtering
  - 32.4.5.6 can use the entry opened by the access to 25.8.2.10



Symmetric NAT

Symmetric NAT

- 32.4.5.6 can not use the entry
- Only 25.8.2.10:80 is accepted as source address



NAPT and Applications

- Problem: address and ports numbers may also be present in payload
  - E.g. FTP and SIP prints the port numbers converted into ASCII in the payload during connection set up
- ICMP
  - echo reply: who should get the reply?
  - redirect: the gateway (NAT box) has an incorrect route?
  - destination unreachable: the payload of the ICMP carries the header from the datagram that could not be delivered.
- Many peer-to-peer applications use special techniques to bypass NAT/NAPT
  - Third party
  - Overloading of well-known ports, eg port 80
- IPsec breaks
  - eg authentication of addresses/ports that are modified