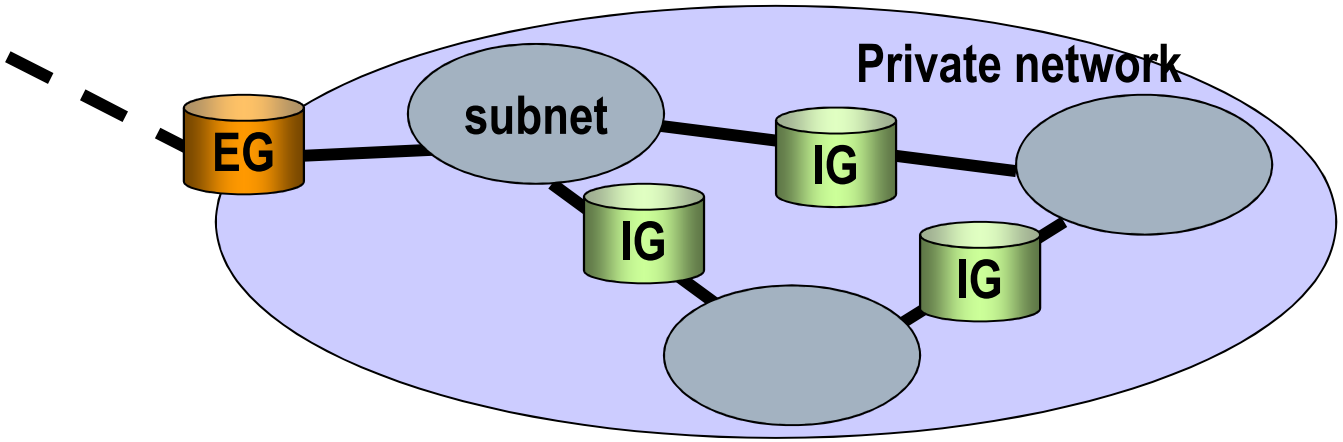
POLYTECH
PARIS-SUD

Intranets

- *Network Address Translation* (NAT)
- *Virtual Private Networks* (VPN)

Private networks and *Intranets*



- Private networks have evolved based on IP technology.
- Private networks are usually partitioned using layer-2 switches, VLAN and IP routers.
- An *intranet* is just a private network using IP technology for LAN (or VLAN) interconnection, and providing some services on the INTERNET (web server, mail server, etc.).

Characteristics of Intranets

- The evolution of services and protocols made Intranets quite different from public IP networks
  - Security issues
  - Address management
  - Differentiation of services offered to *Intranet* users and INTERNET users.
  - etc.

Addresses

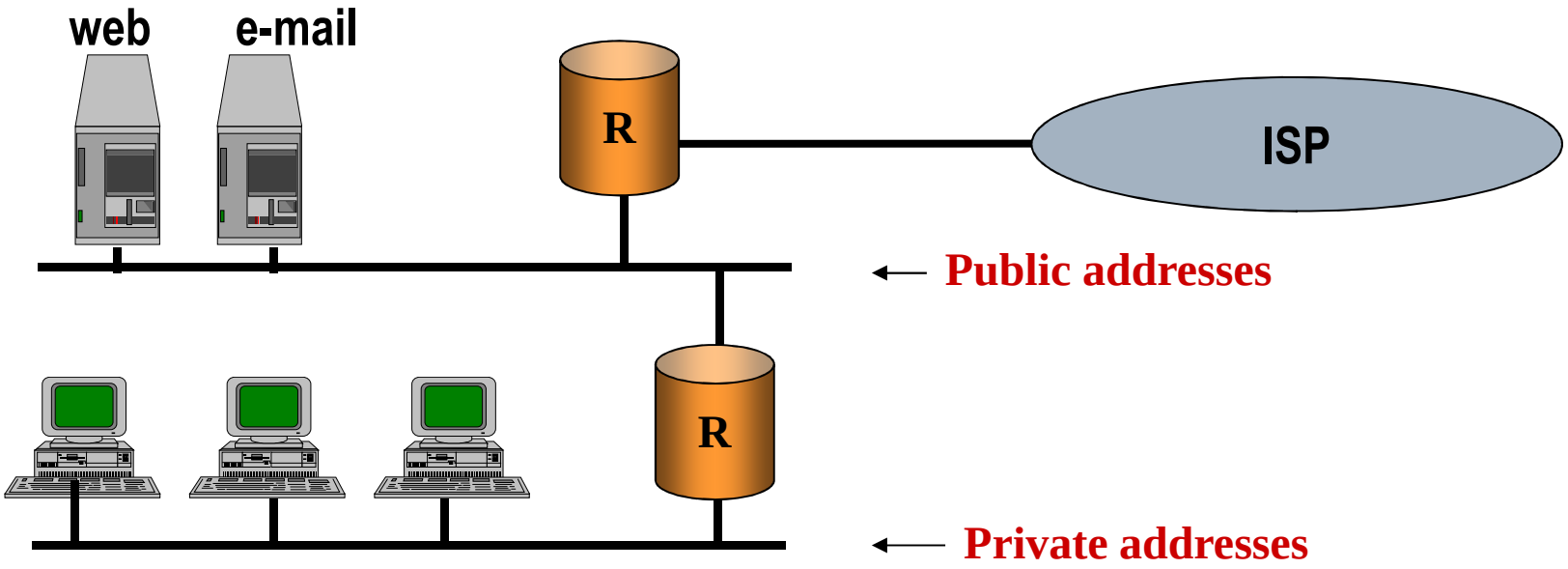
- The exponential increase of the number of hosts in the Internet makes the availability of IPv4 addresses a real problem
- This problem has pushed the standardization of IPv6
- In the meanwhile, another solution has been found by means of *private addresses*
- If an IP network is not connected to the Internet, it can use any arbitrary addressing plan ...

Private addressing (1)

- Different *intranets* can reuse the same set of IP addresses (RFC 1597, *Address Allocation for Private Internets*).
  - class A: net 10.xx.xx.xx (16 millions addresses)
  - class B: from 172.16.0.0 to 172.31.255.255 (16 nets with 65536 addresses each)
  - class C: nets 192.168.xx.xx (256 nets with 254 addresses each)
- It's not allowed that packets with private addresses (source or destination addresses) travel in the public Internet
- The development of some technologies like *Proxy* and *NAT* allowed the use of private addressing even to intranets connected to the Internet

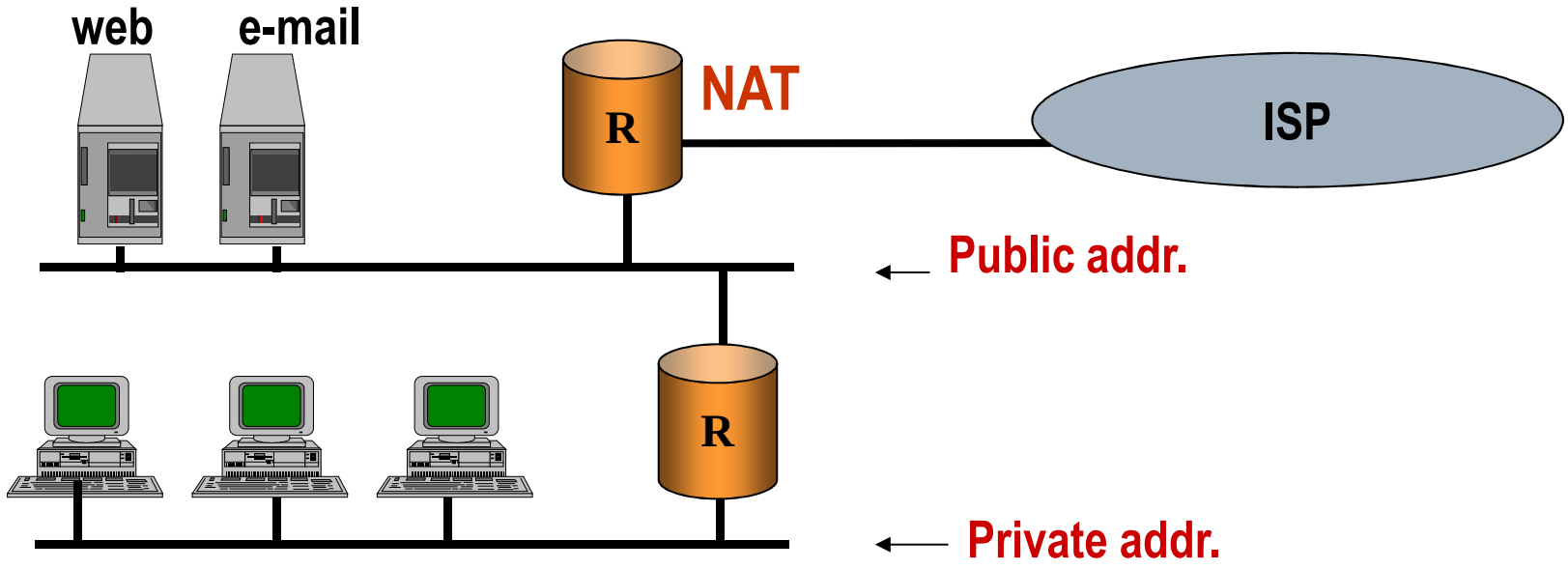
Private addressing (2)

- A private network has usually some services that can be accessed from the public Internet
- *Servers* of these services need a *public address,* while internal hosts can use a private address



Private addressing (3)

- Whitout an interconnection mechanism between private and public world, private hosts cannot access to Internet services
- Commonly adopted methods for interconnection are *NAT and Proxy*

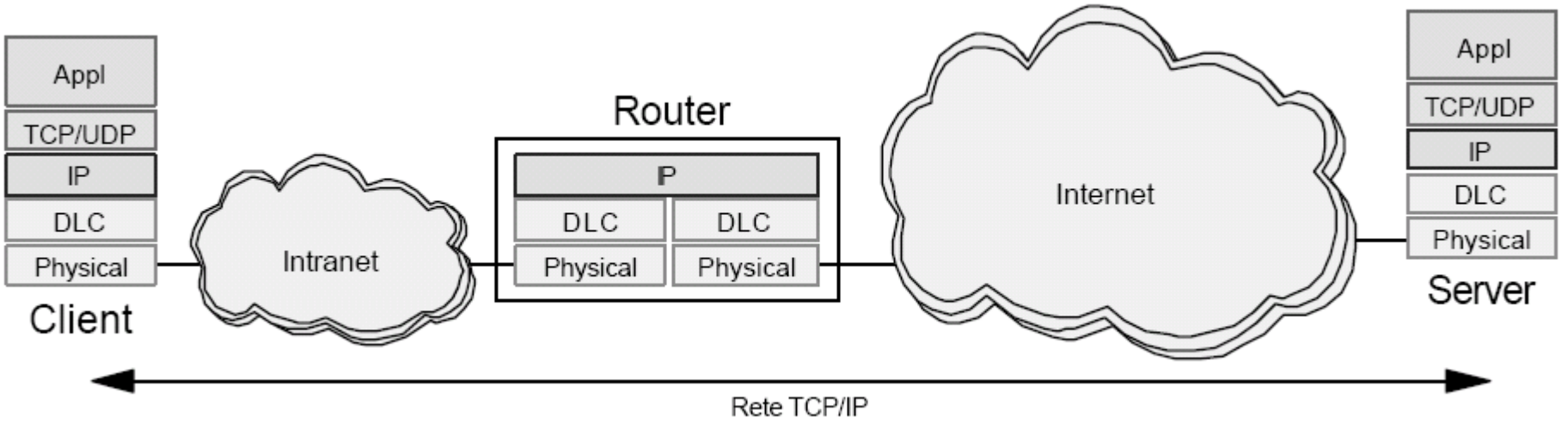


Connection *Intranet/Internet*

- Intranet using public addresses
  - Application Proxy
  - Simple Router
- Intranet using private addresses
  - NAT
  - Application Proxy

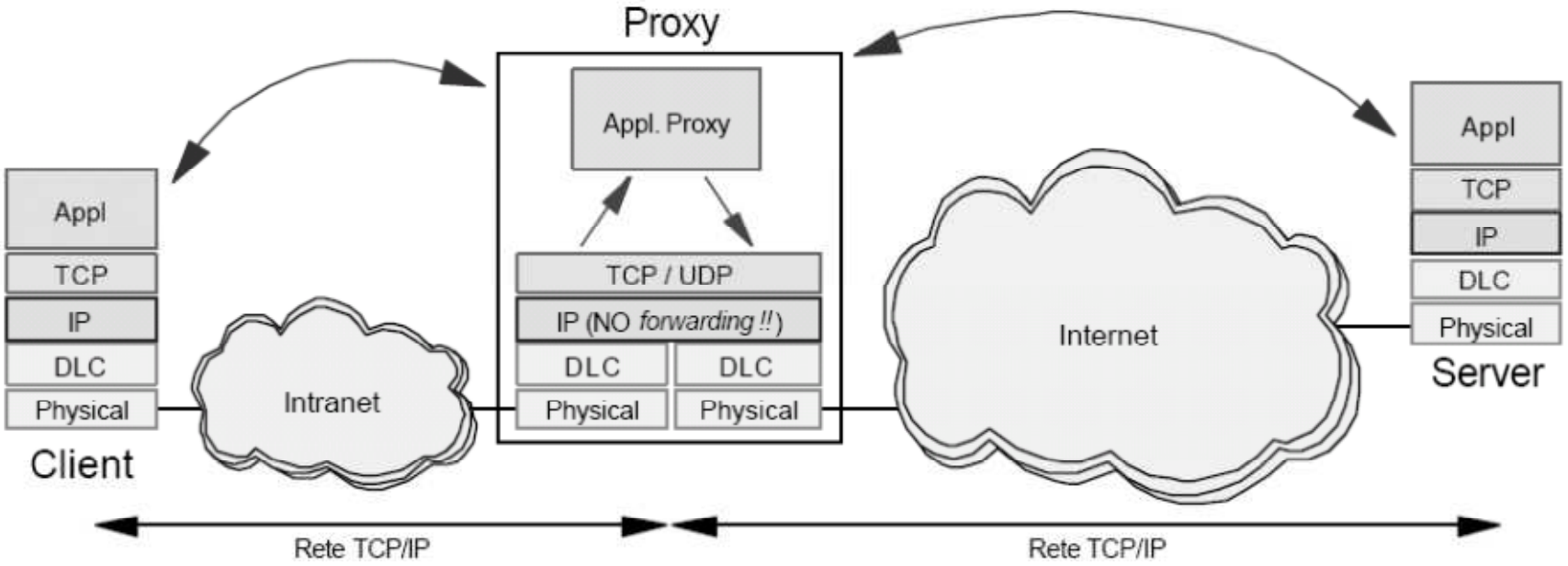
Connection with a simple Router

- The intranet uses public IP addresses
- The *intranet* is actually a part of the big Internet
- Communications are always possible
- Low security

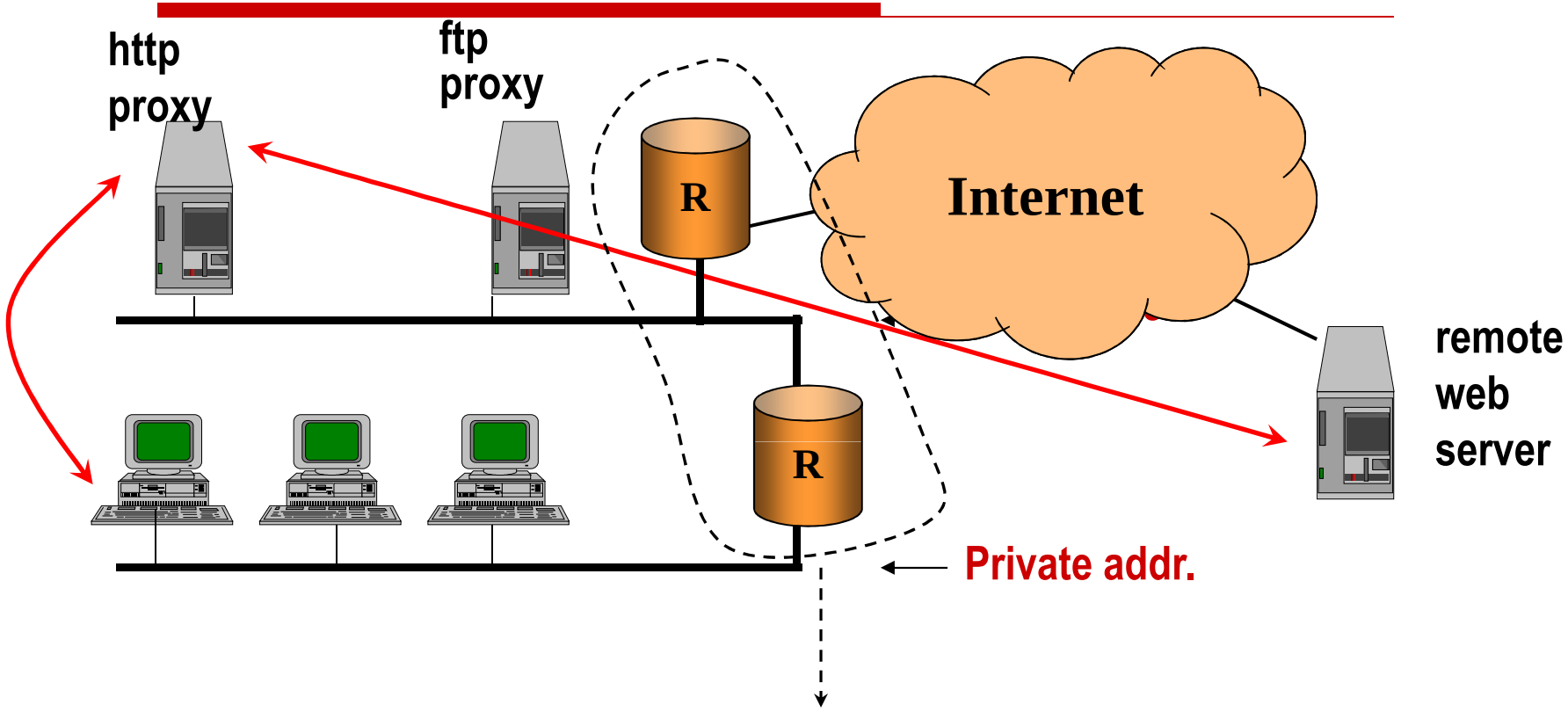


Connection through an application Proxy

- This solution works either with public or private addresses
- Intranet and INTERNET are not connected at the IP layer
- Any request (application layer) is forwarded to the *proxy* that forwards it to the Internet using its public IP address
- A proxy for *each application* is required



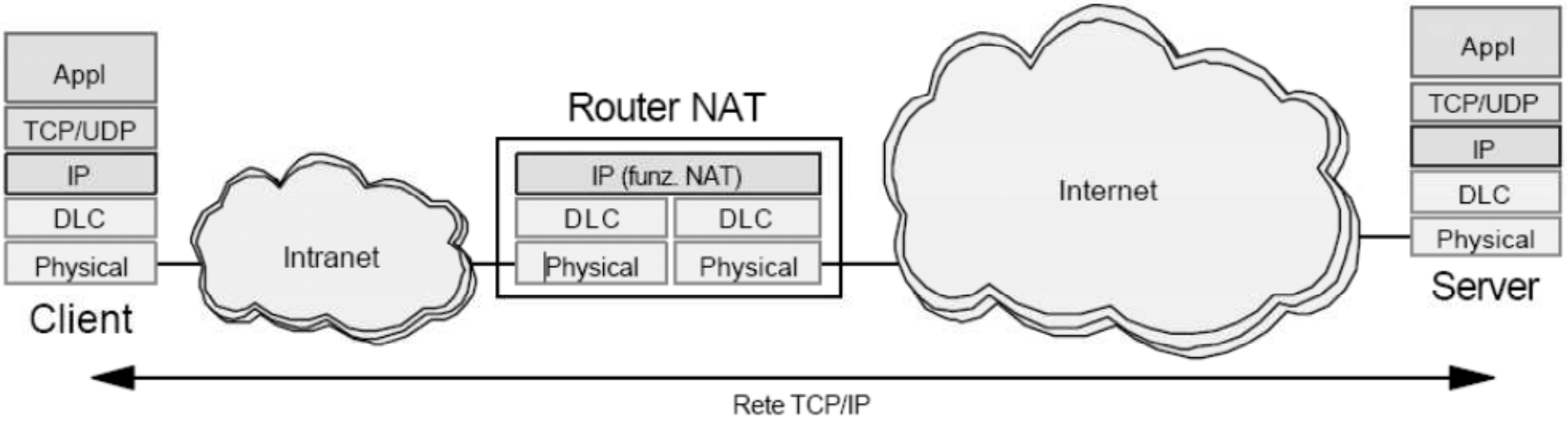
Application Proxy



- Routing tables with public and private addresse

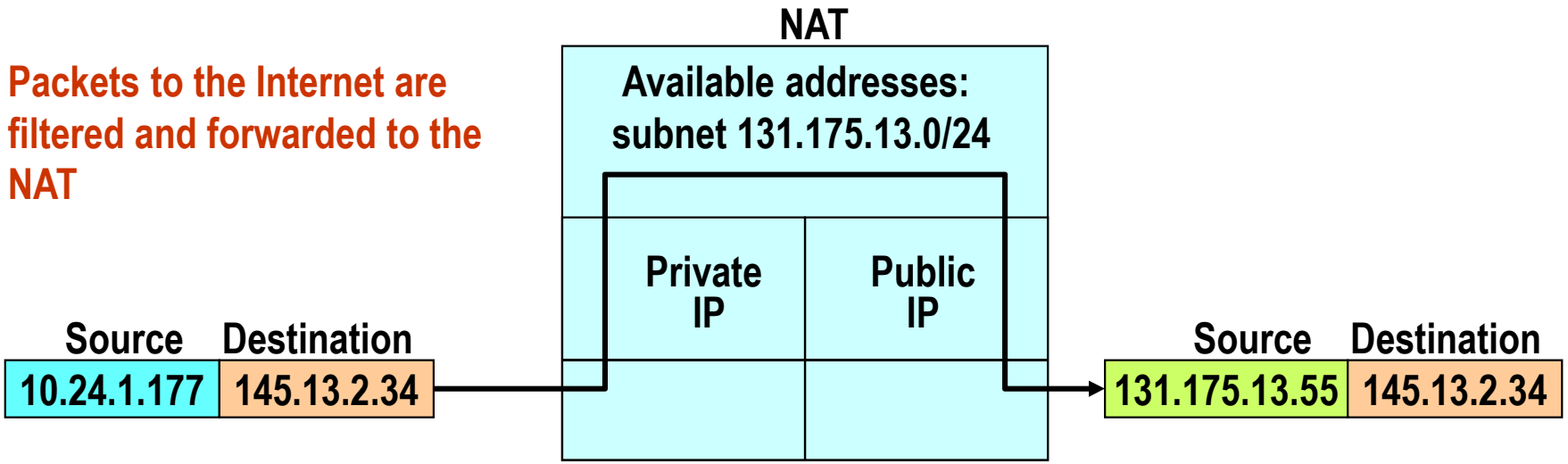
Network Address Translation (NAT)

- NAT (*Network Address Translation*) routers have all classical functionalities of IP routers …
- … and in addition they can *map* a (private) addressing space into another (public) addressing space.

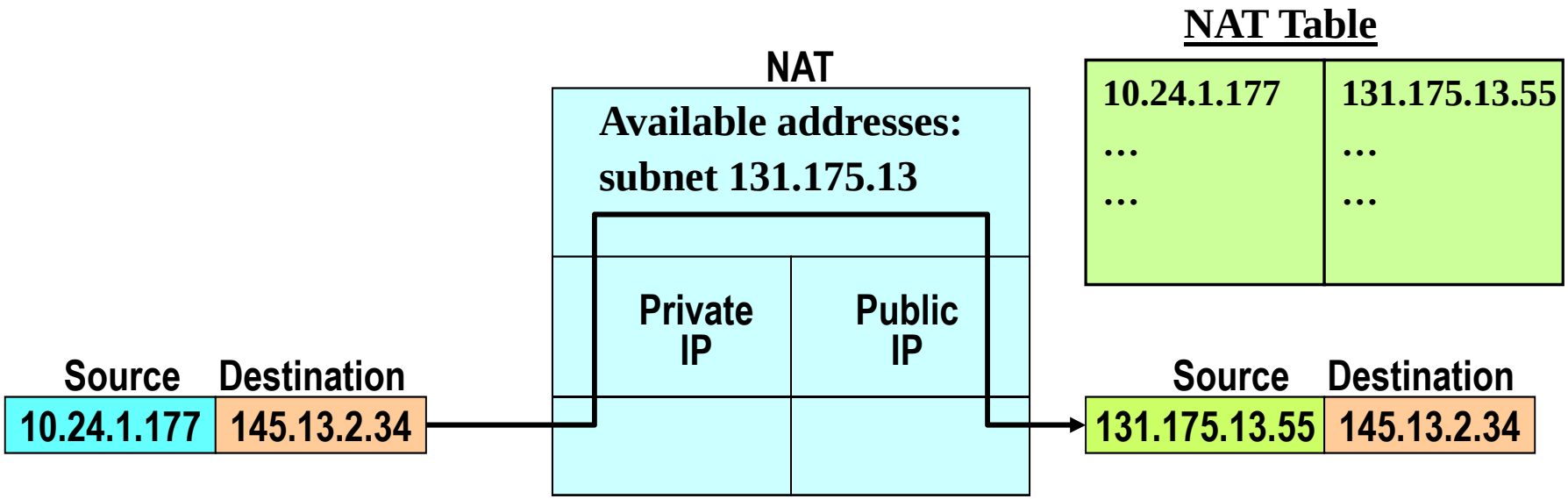


Network Address Translator (NAT)

- NAT permits to associate (usually temporarily) a *private* address to a *public* address. The set of private addresses is usually much larger than that of public addresses.



NAT Table



- To allow bidirectional connections, a mapping table is required:
  - Static mapping
  - Dynamic mapping

NAT methods

- *Traditional* NAT
  - *Basic* NAT (a.k.a. one-to-one NAT)
    - Only the IP addresses, IP header checksum and any higher level checksums that include the IP address are changed, the rest of the packet is left untouched
  - *Network Address and Port* Translation (a.k.a. One-to-many NAT, NAPT)
    - To avoid ambiguity in the handling of returned packets, a one-to-many NAT must alter *higher level information* such as TCP/UDP ports in outgoing communications and must maintain a translation table so that return packets can be correctly translated back
- *Bi-directional* NAT
  - *Twice* NAT

Common features

- *Transparent Address Translation*
  - Association (binding/unbinding) trasparent to hosts
  - Two association modes:
    - Static (easy but inefficient)
    - Dynamic (efficient but complex)
- *Transparent Routing*
  - Routing must be managed according to the address type (private addressing plans must not be redistributed to the public network)
- *ICMP Packet Translation*
  - Portions of ICMP messages include IP addresses, therefore they have to be translated

NAT – Dynamic association (1)

- Dynamic assignment is based on the concept of *session*
- When NAT receives the first packet of a session, it creates the association between public and private addresses
- At the end of the session the public address is released
- What's a session?
  - Its definition is protocol-dependent
  - For TCP and UDP a session is based on the *socket*
  - For ICMP, a set of three addresses (source IP, destination IP, Protocol Identifier)
  - The direction of a session is the direction of the first packet

NAT – Dynamic association (2)

- Once defined the session, we have to assess when it starts and ends
- Session start:
  - TCP: SYN packet
  - UDP, ICMP: connectionless, there is not a unique method
- Session end:
  - TCP: FIN packets or RESET
  - Other protocols: there is not a unique method
  - Timers are always required to recover from error states.

NAT – Application Level Gateway (ALG)

- Several applications include IP addresses in the messages (ASCII or binary formats) and port numbers
- *Application Level Gateways* (*ALG*) add some functionalities to NATs for a correct operation with such applications
- Based on the application and messages type, not only IP headers but also message contents are translated, and if needed TCP segments are modified accordingly
- ALG are similar to *proxy*, but they are transparent to hosts

Traditional NAT (1)

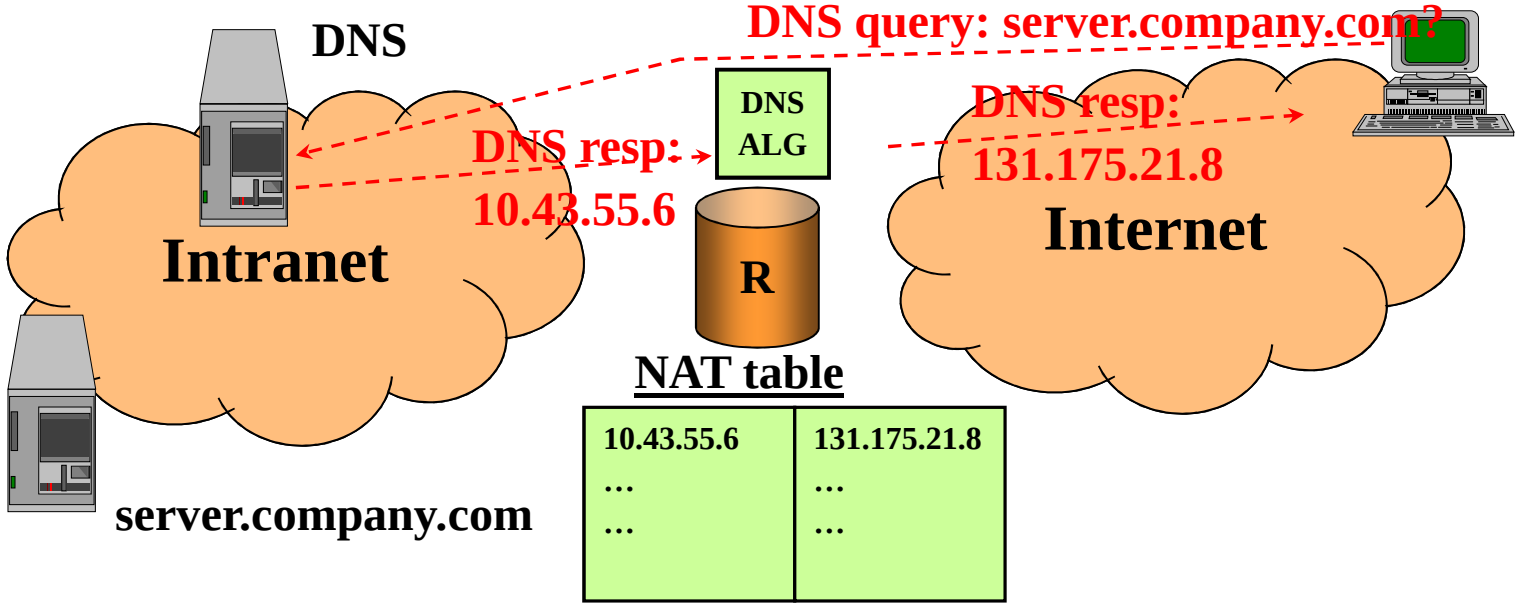
- Also named *Outbound* NAT
- It allows only sessions initiated from the private network (from the Intranet → to the Internet)
- Routing information is redistributed from the Internet to the Intranet, but not in the opposite direction
- 2 sub-types
  - Basic NAT
  - NAPT (*Network Address and Port Translator*)

Traditional NAT (2)

- Basic NAT
  - Only the IP address is translated
  - There is a one-to-one mapping during a session and two hosts cannot use the same public address at the same time
  - Requests can be blocked due to the limited number of available public addresses
- NAPT
  - The couple (IP, port) is translated
  - Many private addresses can be mapped on the same public address at the same time
  - Some problems arise with flows not using UDP or TCP (with ICMP it is possible to use the protocol identifier field)
  - With fragments it does not work

Bi-Directional NAT

- A session can start in any direction
- Problem:
  - How can a public host start a session with a private host without a public address?
  - Symbolic names must be used and the DNS service must support the NAT

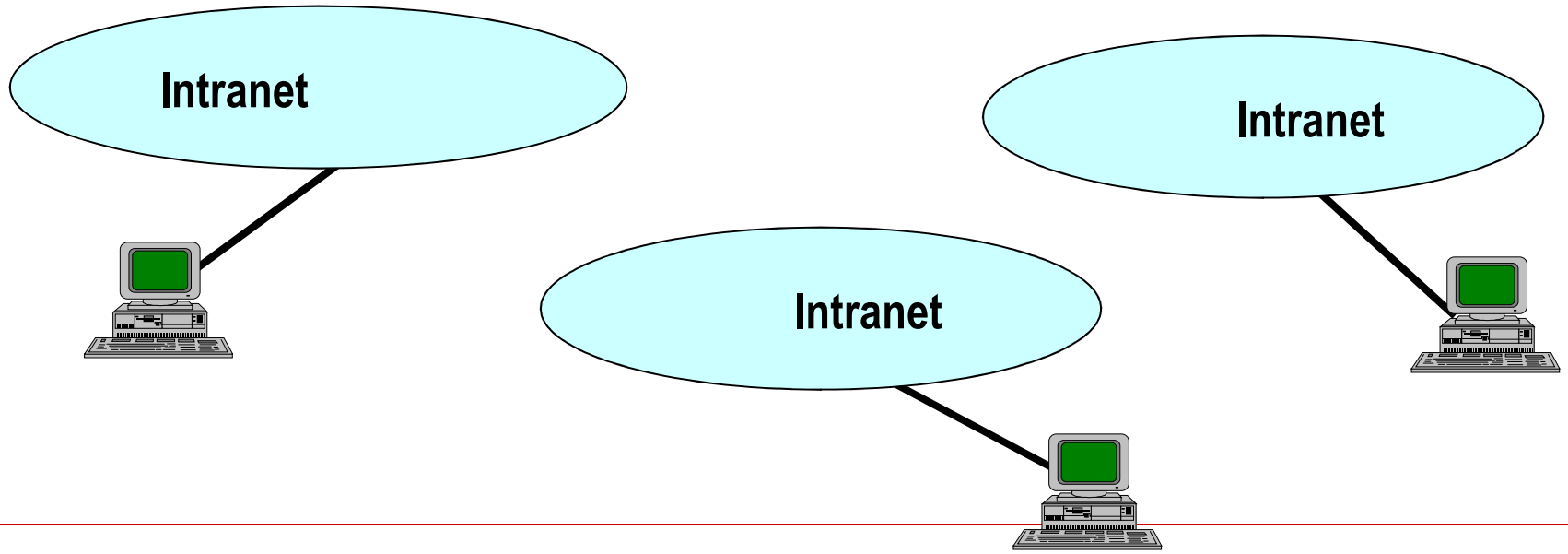


NAT – Some comments

- Address mapping is not an easy task
- It requires
  - To recalculate the *Header Checksum*
  - To replace address into ICMP message and to recalculate the *header checksum*
  - To recalculate the *checksum* of TCP or UDP with the new *pseudo-header*
- ALG are required with applications including addresses or ports into application messages
- IPsec and all security protocols are difficult to manage

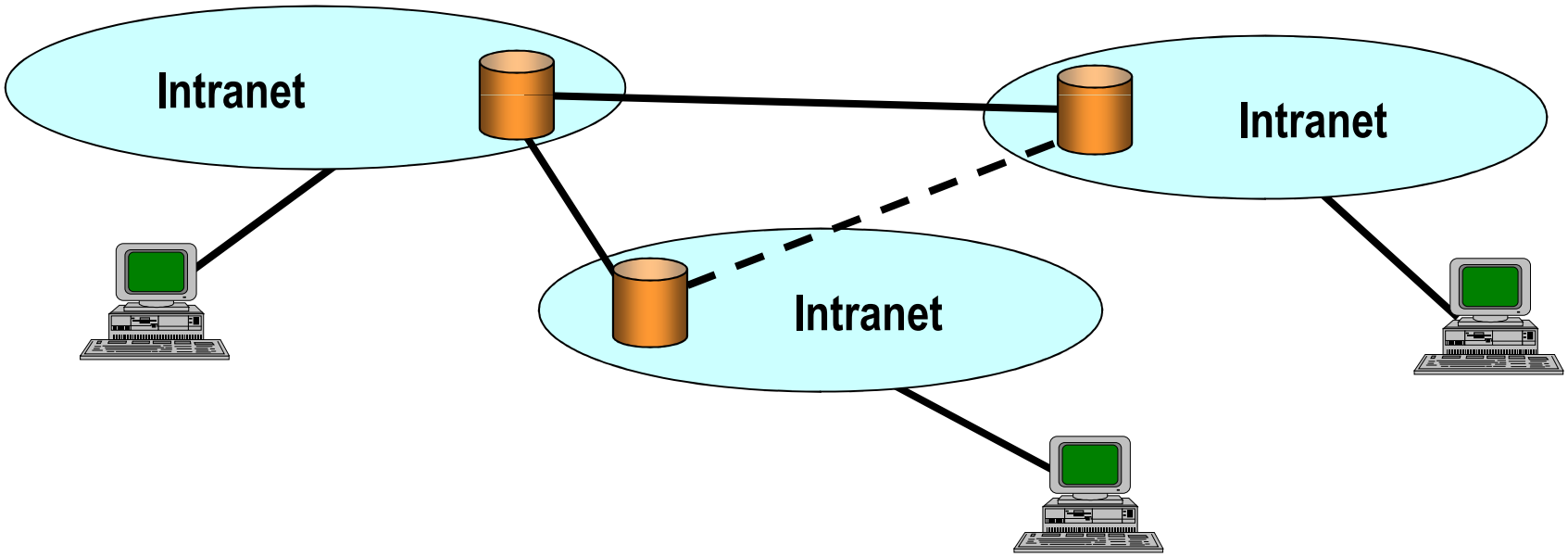
WAN connection of remote intranets (1)

- Different Intranets (of the same organization/company) can be connected together
- Problems:
  - cost
  - use of private addresses
  - security



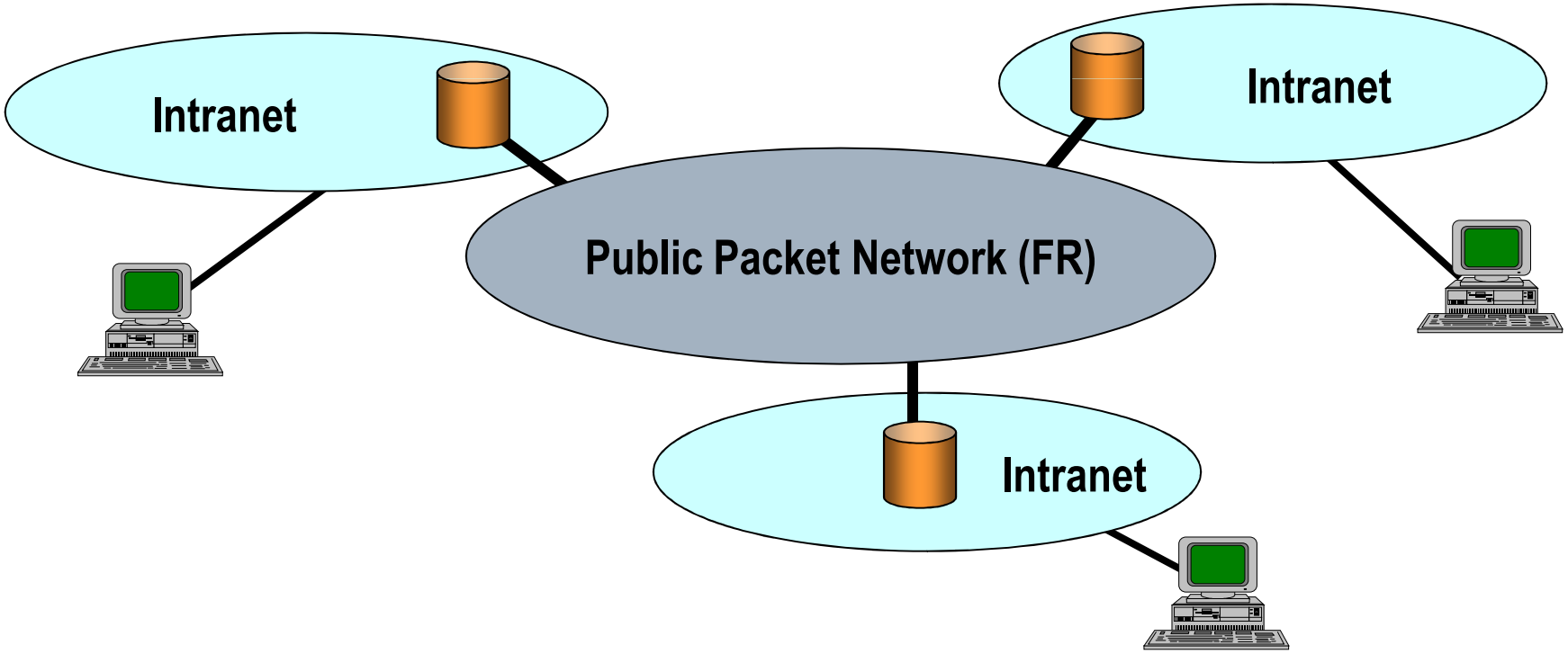
WAN connection of remote intranets (2)

- Dedicated channels
- Problem:
  - Very high cost



WAN connection of remote intranets (3)

- Public packet networks (e.g. Frame Relay)
- Problems:
  - Quite high cost

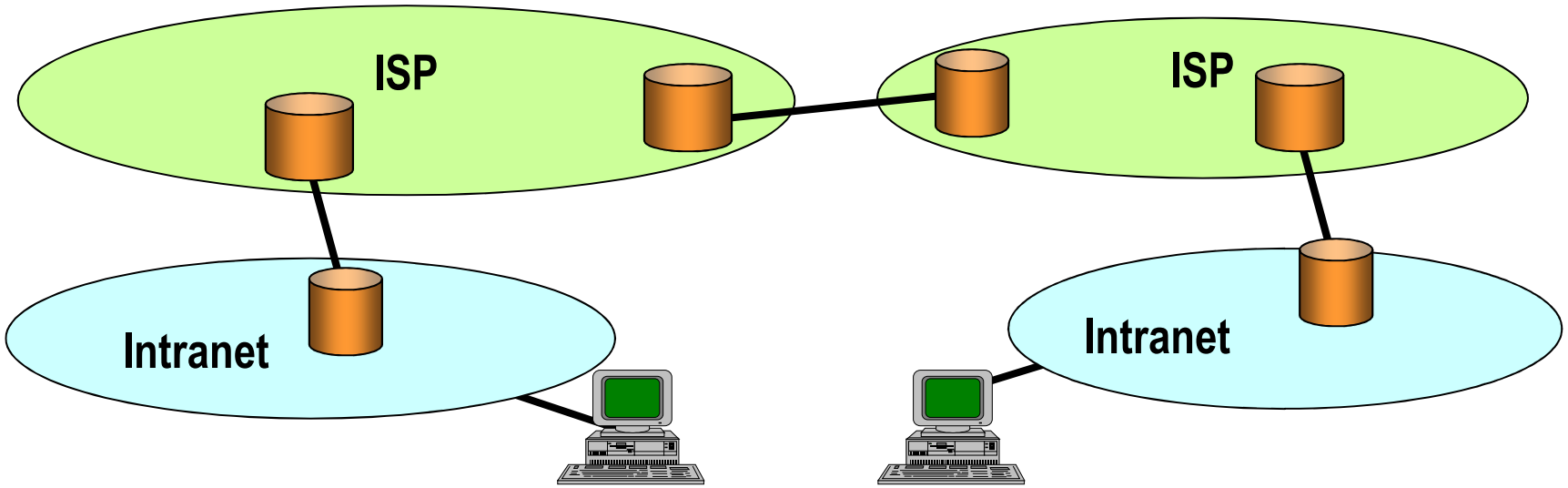


WAN connection of remote intranets (4)

- INTERNET (Virtual Private Network - VPN)

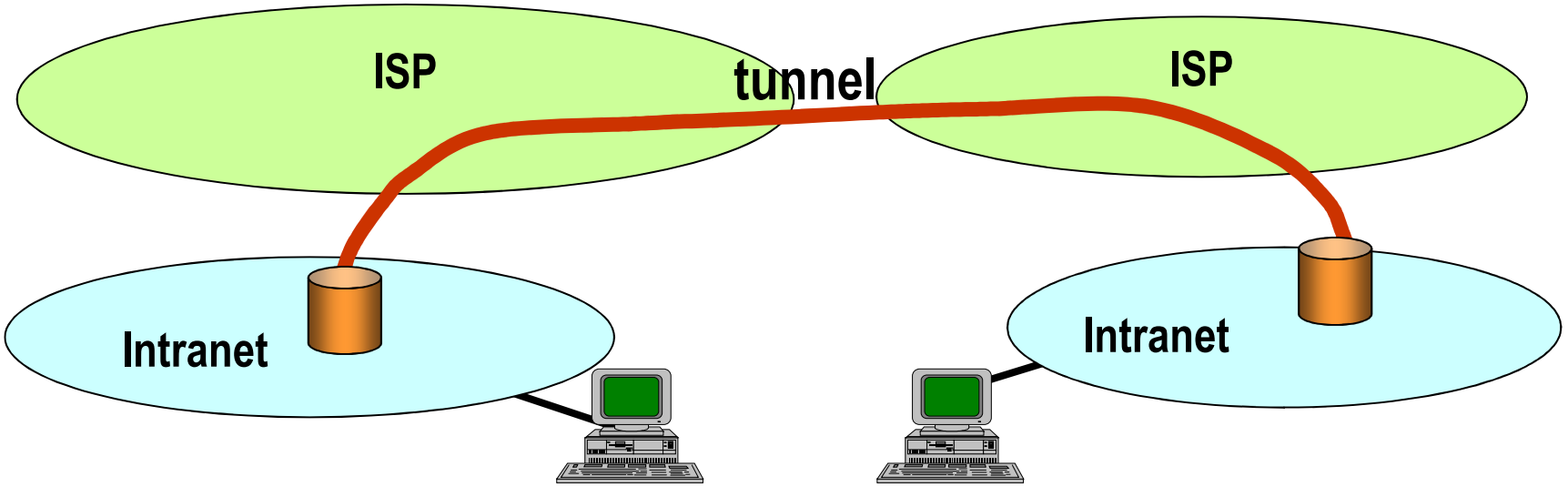
Problems:

- Private addresses
- security
- performance



Virtual Private Networks

- Tunnels



IP tunneling

- Tunnel can be created through encapsulation of IP packets into IP packets
- The payload traveling in the public network can be encrypted (IPsec)
- Addresses in the remote intranets are usually private