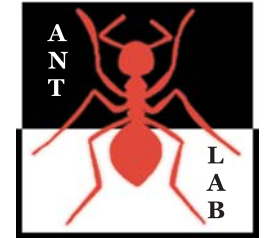




Politecnico di Milano

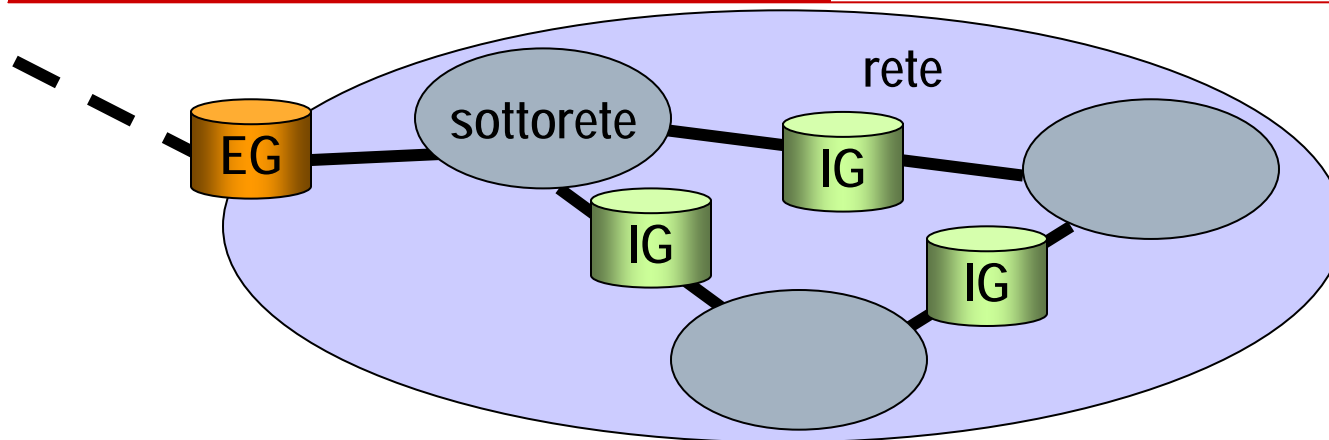
Advanced Network Technologies Laboratory



Il Mondo delle Intranet

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

Reti Private e *Intranet*



- ❑ Le reti private si sono evolute grazie alla tecnologia IP e sono passate da grandi reti collegate a livello 2 (*bridge*) a reti collegate con *router* IP
 - ❑ Una *intranet* non è altro che una rete privata che utilizza tecnologia di interconnessione IP, dotata degli stessi servizi dell'INTERNET come server *www*, server di posta, ecc.
-

Caratteristiche dell Intranet

- L'evoluzione di servizi e protocolli ha però reso le *Intranet* strutturalmente differenti dalle reti pubbliche
 - Problemi di sicurezza
 - Problemi di gestione degli indirizzi
 - Problemi di distinzione tra servizi offerti ai soli utenti della *Intranet* e servizi offerti anche agli utenti di INTERNET
-

Indirizzi

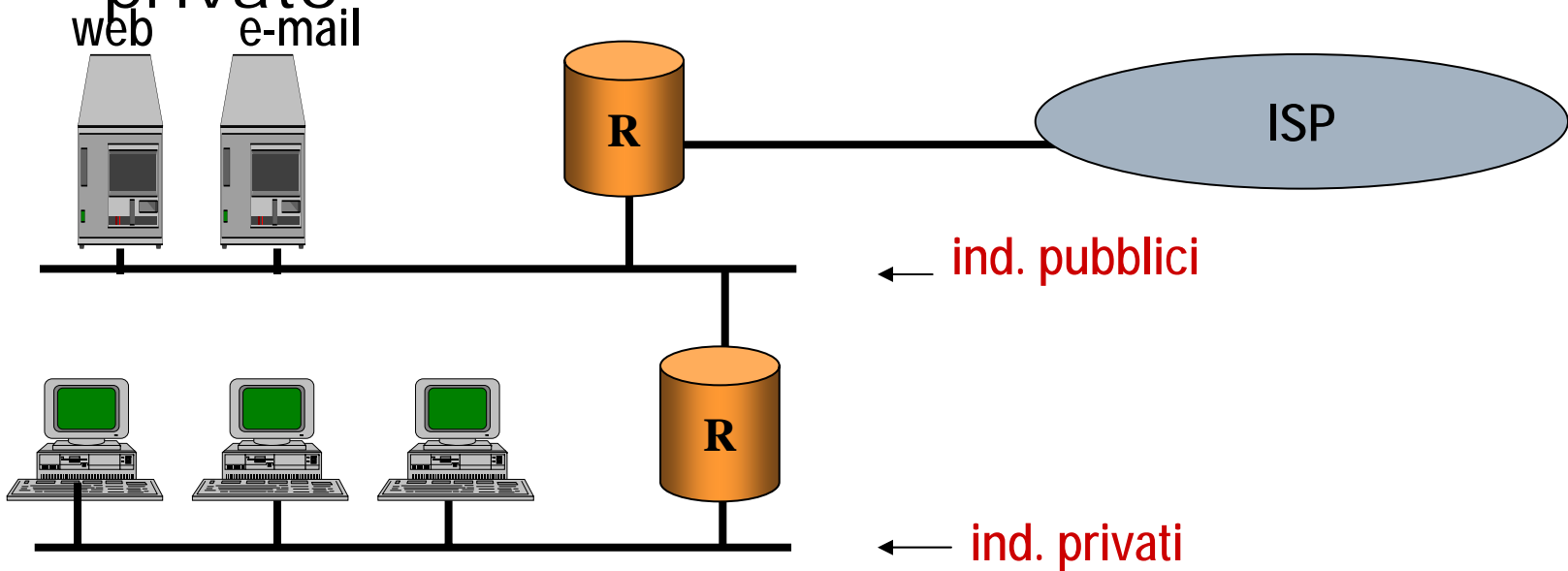
- ❑ L'aumento vertiginoso del numero di host collegati ad INTERNET ha reso il problema della disponibilità di indirizzi IPv4 pressante
 - ❑ E' questo problema che ha spinto alla standardizzazione di IPv6
 - ❑ Nel frattempo però si è trovata un'altra soluzione basata su indirizzi privati
 - ❑ Se una rete IP non è collegata con INTERNET può usare gli indirizzi che gli pare ...
-

Indirizzamento Privato (1)

- Lo sviluppo di particolari tecnologie (*Proxy*, NAT) ha permesso l'utilizzo di indirizzamento privato nelle intranet.
 - Diverse *intranet* possono riusare lo stesso set di indirizzi IP (RFC 1597, *Address Allocation for Private Internets*).
 - classe A: rete 10.xx.xx.xx (16 milioni di indirizzi)
 - classe B: da 172.16.0.0 a 172.31.255.255 (16 reti contigue da 65536 indirizzi)
 - classe C: reti 192.168.xx.xx (256 reti)
 - Non è ammesso che pacchetti con indirizzi privati (sorgente o destinazione) viaggino nella rete pubblica
-

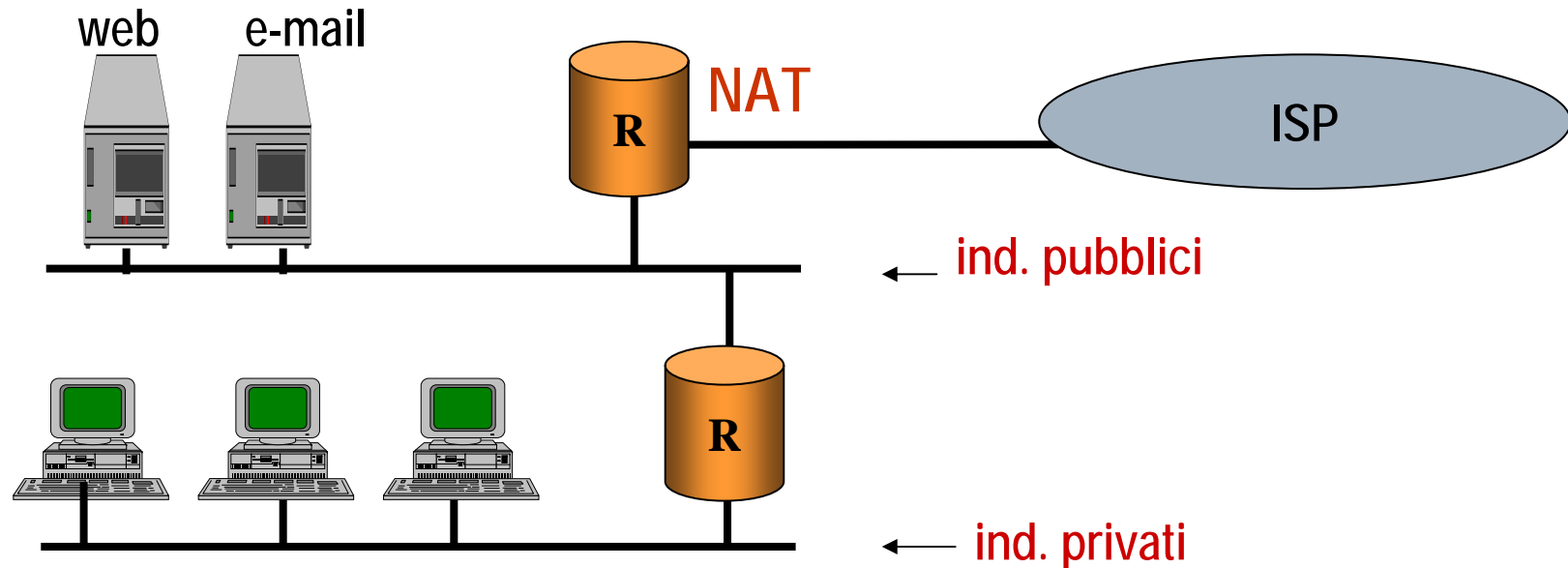
Indirizzamento Privato (2)

- Una rete privata ha normalmente una serie di servizi che sono accessibili dalla rete pubblica
- I *server* per questi servizi devono avere un indirizzo pubblico mentre gli *host* interni alla rete possono avere un indirizzo privato



Indirizzamento Privato (3)

- E' chiaro comunque che in questo modo si impedisce agli *host* della rete privata di aver accesso a tutti servizi di INTERNET
- Prima o poi sorge l'esigenza di consentire lo scambio di pacchetti tra *host* con indirizzo pubblico e *host* con indirizzo privato
- I metodi più comunemente usati per consentire il colloquio sono il *NAT* e i *Proxy*



Connessione

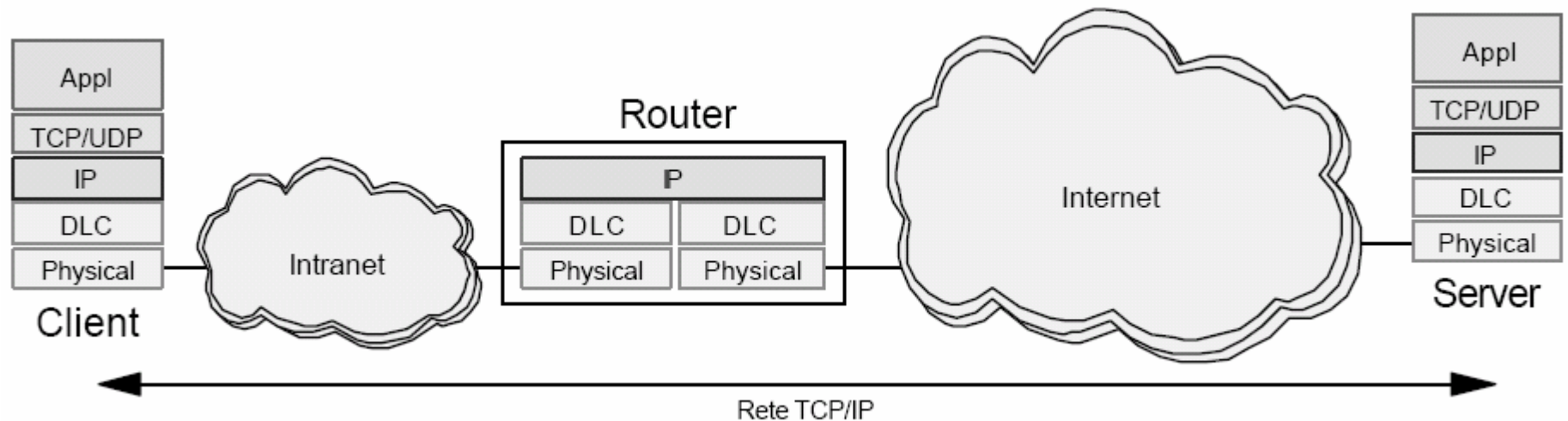
Intranet/Internet

- Intranet che adotta indirizzamento pubblico
 - Proxy applicativi
 - Router semplice (soluzione classica)

 - Intranet che adotta indirizzamento privato
 - NAT
 - Proxy applicativi
-

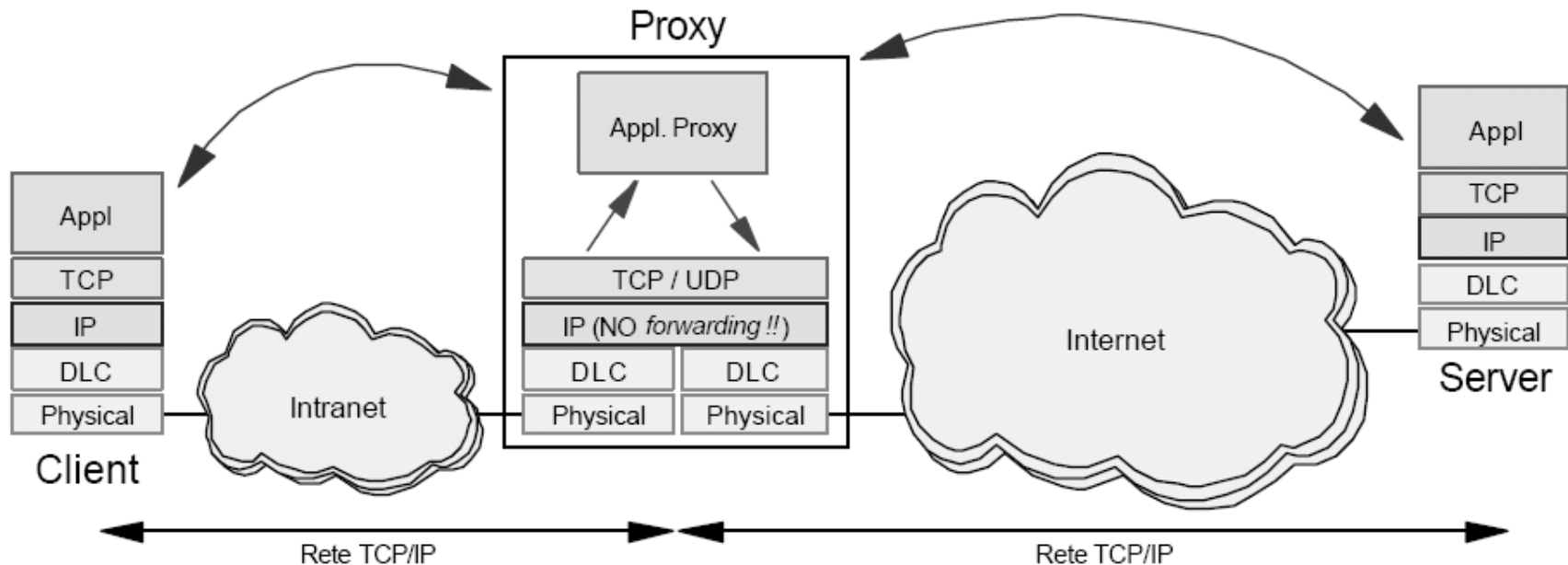
Connessione con Router Semplice

- ❑ L'intranet usa indirizzi IP pubblici
- ❑ Di fatto l'*intranet* scompare (unica rete IPv4 con l'INTERNET)
- ❑ Possibili comunicazioni da e verso l'INTERNET
- ❑ Scarsa sicurezza



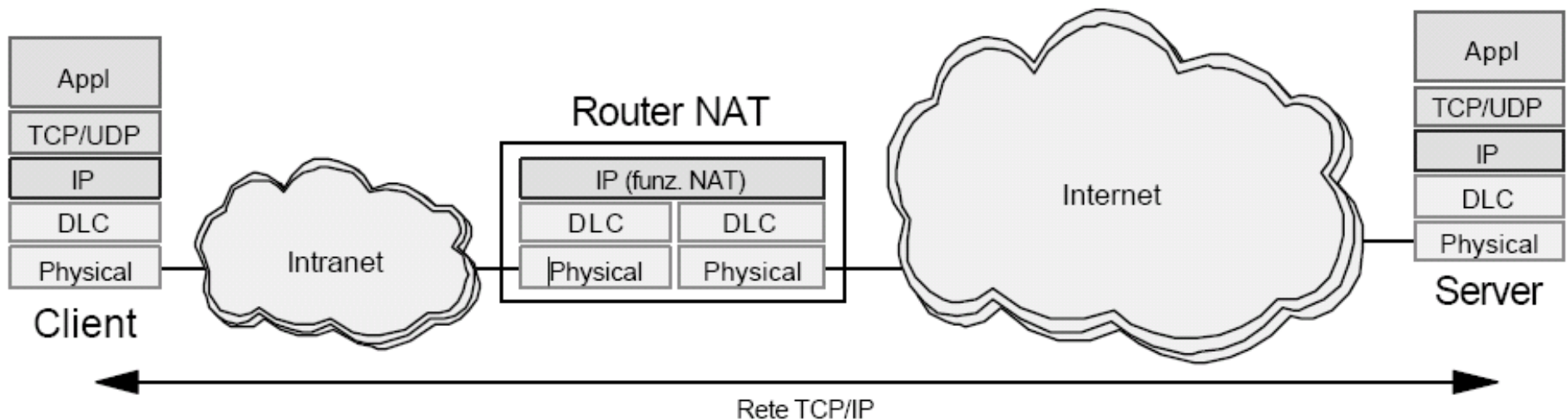
Connessione tramite Proxy Applicativo

- ❑ Funziona sia con indirizzamento pubblico che privato
- ❑ Intranet e INTERNET sono scollegate a livello IP
- ❑ qualunque richiesta viene inviata al *proxy* che la inoltra con il proprio IP *address*



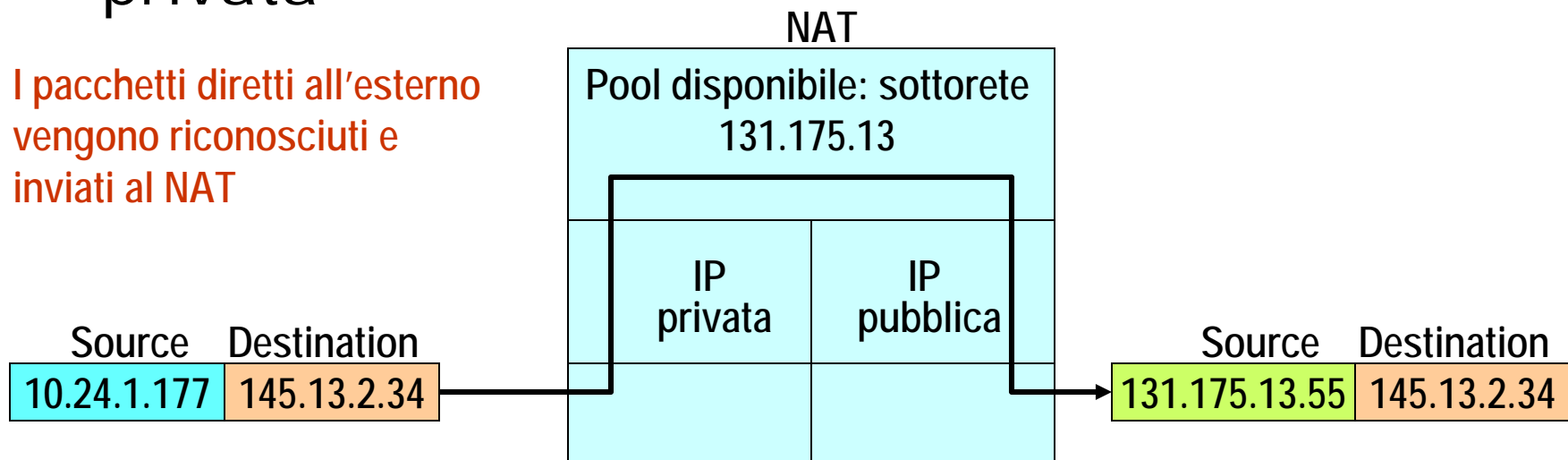
Network Address Translation (NAT)

- I NAT (*Network Address Translation*) hanno tutte le funzionalità dei router classici
- In più sanno gestire anche il *mapping* di uno spazio di indirizzamento (privato) in un altro spazio di indirizzamento (pubblico)



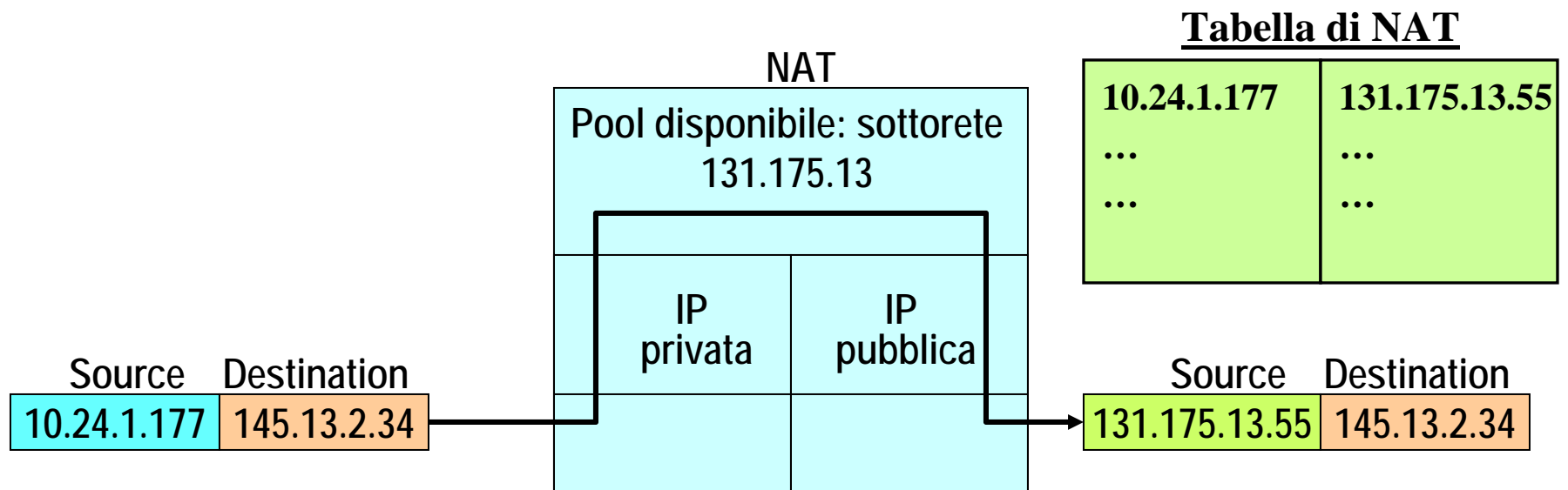
Network Address Translator (NAT)

- ❑ E' un meccanismo reso disponibile su un *router/gateway*
- ❑ Consente di associare, anche temporaneamente, un ridotto numero di indirizzi pubblici, ai numeri della numerazione privata



Possibilità di blocco

NAT – Tabella di NAT



- Perché il colloquio sia bidirezionale occorre mantenere l'associazione tra indirizzo privato e pubblico un una tabella di NAT
 - Corrispondenza statica
 - Corrispondenza dinamica

NAT: Diversi Approcci

- *Traditional NAT*
 - *Basic NAT*
 - *Network Address Port Translation (NAPT)*

 - *Bi-directional NAT*
 - *Twice NAT*
-

Caratteristiche Comuni

- *Transparent Address Translation*
 - Associazione (binding/unbinding) trasparente alle stazioni
 - Due modalità di associazione:
 - Statica (facile ma inefficiente)
 - Dinamica (efficiente ma complessa)
 - *Transparent Routing*
 - Il routing deve essere gestito in maniera coerente all'indirizzamento
 - *ICMP Packet Translation*
 - Porzioni di messaggi ICMP contengono indirizzi IP, quindi vanno mappate
-

NAT – Associazione Dinamica (1)

- L'assegnamento dinamico si basa sul concetto di *sessione*
 - Quando il NAT vede il primo pacchetto di una *sessione* crea l'associazione tra indirizzo privato e pubblico
 - Al termine della sessione l'indirizzo viene rilasciato
 - Cos'è una *sessione*?
 - Dipende dal protocollo utilizzato
 - Per TCP e UDP una sessione viene identificata dall'indirizzo di *socket*
 - Per ICMP dalla terna (IP sorgente, IP destinazione, *Identifier*)
 - Per direzione di una sessione si intende il verso di percorrenza del primo pacchetto
-

NAT – Assegnamento Dinamico (2)

- ❑ Definita la sessione occorre capire quando inizia e quando finisce
 - ❑ Inizio sessione:
 - TCP: pacchetto di SYN
 - UDP, ICMP: sono connectionless, non vi è un metodo unico
 - ❑ Fine sessione:
 - TCP: pacchetti di FIN per entrambe i lati (però possono non arrivare mai ...)
 - Altri prot.: non vi è un metodo univoco
 - Occorrono sempre dei time-out per recuperare situazioni d'errore o perdita di pacchetti
-

NAT – Application Level Gateway

- ❑ Alcune applicazioni trasportano nel Payload dei loro messaggi indirizzi IP (in formato ASCII o binario) e numeri di porta
 - ❑ Gli *Application Level Gateway (ALG)* sono funzionalità aggiuntive che servono per un corretto funzionamento del NAT
 - ❑ Sulla base del tipo di applicazione e del tipo di messaggio si preoccupano di modificare i messaggi applicativi in transito e, se del caso, adattare i segmenti TCP
 - ❑ Simili ai *proxy*, con la differenza che sono trasparenti alle stazioni
-

Traditional NAT (1)

- ❑ Detto anche *Outbound* NAT
 - ❑ Permette solo sessioni iniziate dall'interno (verso della sessione dall'interno verso l'esterno)
 - ❑ Le informazioni di *routing* possono essere distribuite dall'esterno verso l'interno ma non viceversa
 - ❑ 2 sotto-tipi
 - Basic NAT
 - NAT (Network Address and Port Translator)
-

Traditional NAT (2)

□ Basic NAT

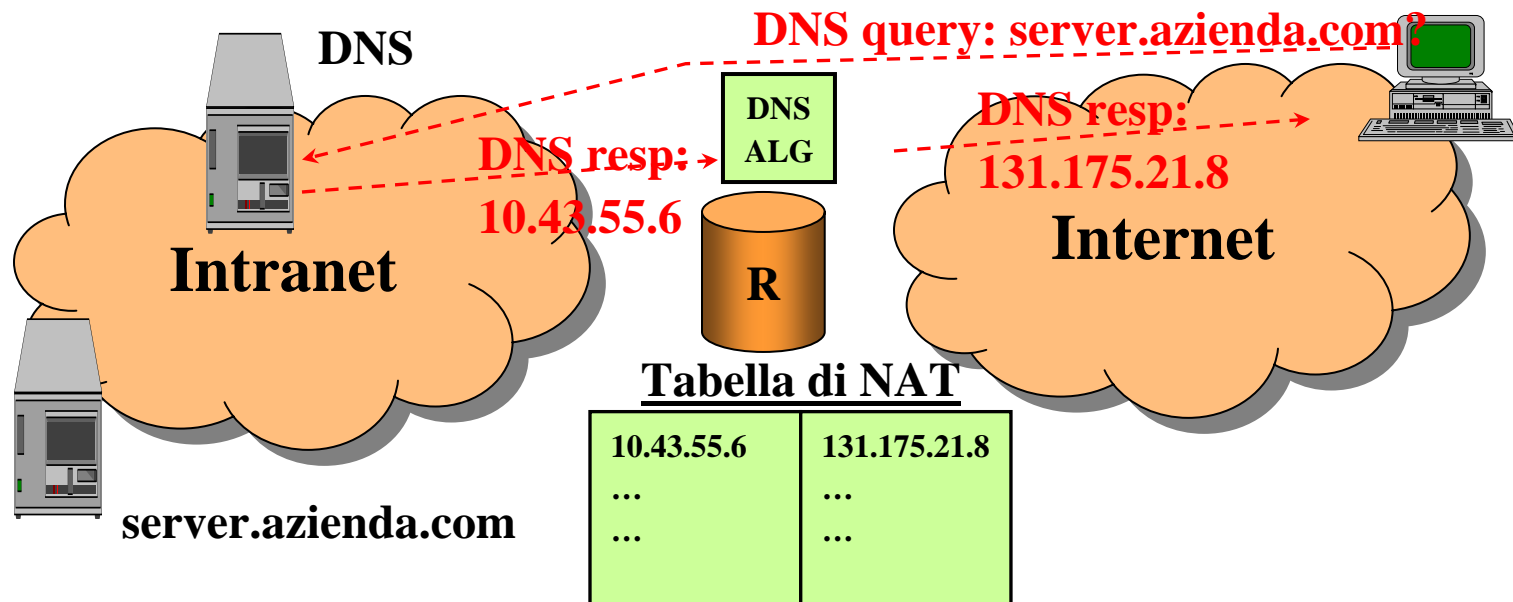
- Viene traslato il solo indirizzo IP
- C'è una corrispondenza uno-a-uno nell'assegnamento degli indirizzi durante una sessione e due host non possono usare lo stesso indirizzo contemporaneamente
- Ci può essere blocco a causa del numero scarso di indirizzi pubblici quando il traffico (numero di sessioni attive) è elevato

□ NAPT

- Viene traslata la coppia (indirizzo, porta)
 - Molti indirizzi interni possono usare lo stesso indirizzo esterno
 - Ci sono problemi con flussi diversi da UDP e TCP (per ICMP si può usare il campo Identifier)
 - Nel caso di frammenti succede un gran casino
-

Bi-Directional NAT

- Si può iniziare una sessione in entrambe i versi
- Problema:
 - Come fa un host pubblico ad iniziare una sessione con un host privato senza avere un indirizzo pubblico a cui raggiungerlo?
 - Occorre usare dei nomi simbolici e il servizio DNS che deve usare un unico spazio dei nomi
 - Corrispondenza statica tra indirizzo pubblico/privato del DNS privato



NAT – Alcune Considerazioni

- Il cambio di indirizzo non è un'operazione indolore
 - Esso impone:
 - Il ricalcolo del *Header Checksum*
 - Sostituzione degli indirizzi dei messaggi ICMP e ricalcolo *header checksum*
 - Il ricalcolo dei *checksum* di TCP o UDP con il nuovo *pseudo-header*
 - Sorgono poi dei problemi con alcuni ALG per via del trasporto degli indirizzi e porte nei messaggi di livello applicativo
 - Chi crea problemi al NAT?
 - Applicazioni che trasferiscono indirizzi IP
 - IPsec e applicazioni di sicurezza
-

NAT – Esempio FTP (1)

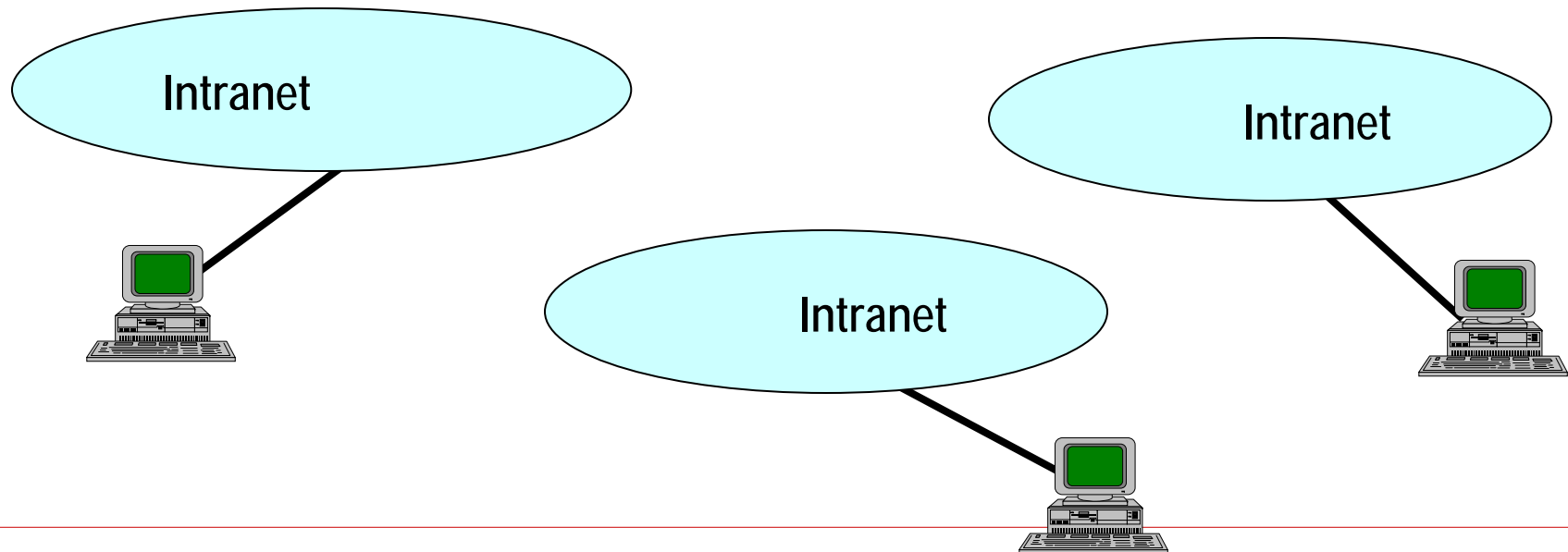
- Il caso del FTP:
 - Sulla connessione di controllo si usano i comandi di PORT e PASV
 - PORT n1,n2,n3,n4,n5,n6 (n1, n2, n3 ,n4 , n5, n6 sono cifrati ASCII)
 - n1.n2.n3.n4 è l'indirizzo IP del client
 - $N5 \times 256 + n6$ = numero di porta del client per la connessione dati
 - Occorre traslare il comando di PORT ma la cosa non è così banale, vediamo il perchè con un esempio.....
-

NAT- Esempio FTP (2)

- Supponiamo di dover mappare 10.43.55.6 (privato) verso 131.175.21.1 (pubblico)
 - Ma FTP è ASCII e
 - nel mapping privato-> pubblico il comando PORT si allunga di 6 byte
 - Nel mapping pubblico->privato il comando PORT si accorcia di 6 byte
 - PORT e PASV cambiano di dimensione -> il payload TCP cambia di dimensione -> si sballa il conteggio dei byte usando i SN e AKN del TCP
 - ALG per FTP deve dunque costruirsi una tabella di mapping anche per i numeri di sequenza e di ACK e i numeri di ACK del TCP, per tutta la durata della connessione FTP!!!
-

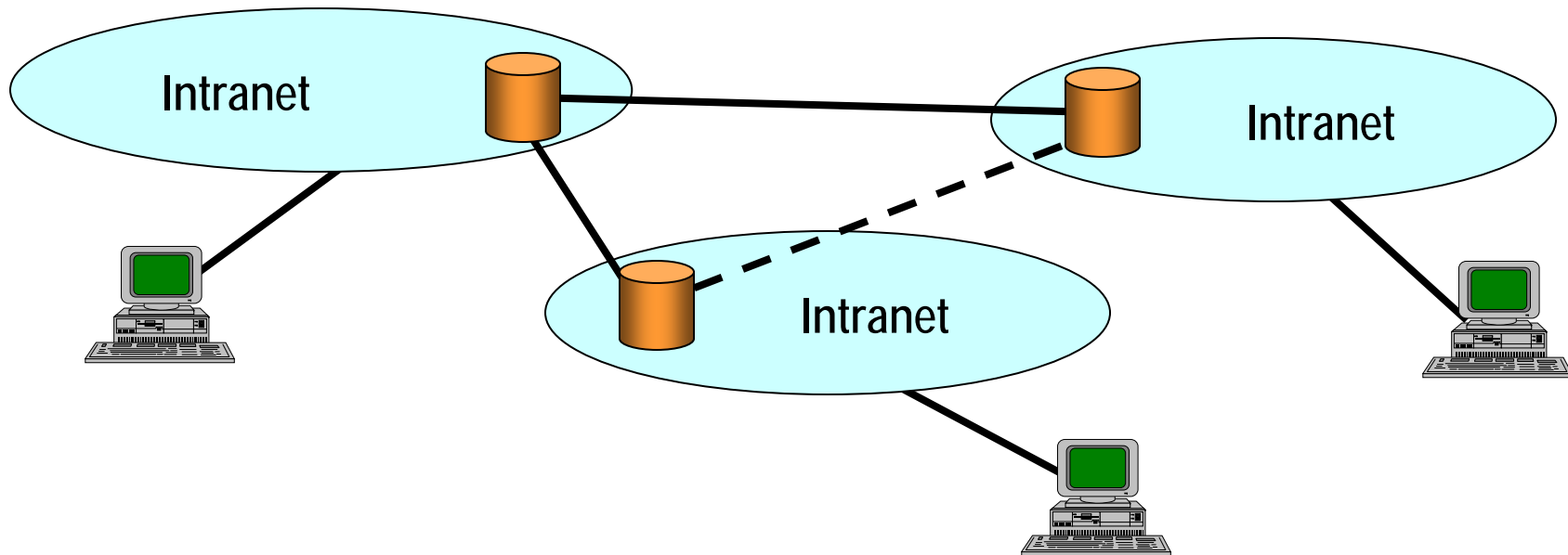
Connessione WAN di intranet remote

- Una volta create le Intranet può sorgere il problema di collegarle tra loro (ad es. sedi diverse di una stessa azienda)
- Problemi:
 - costo
 - uso di indirizzi privati
 - sicurezza



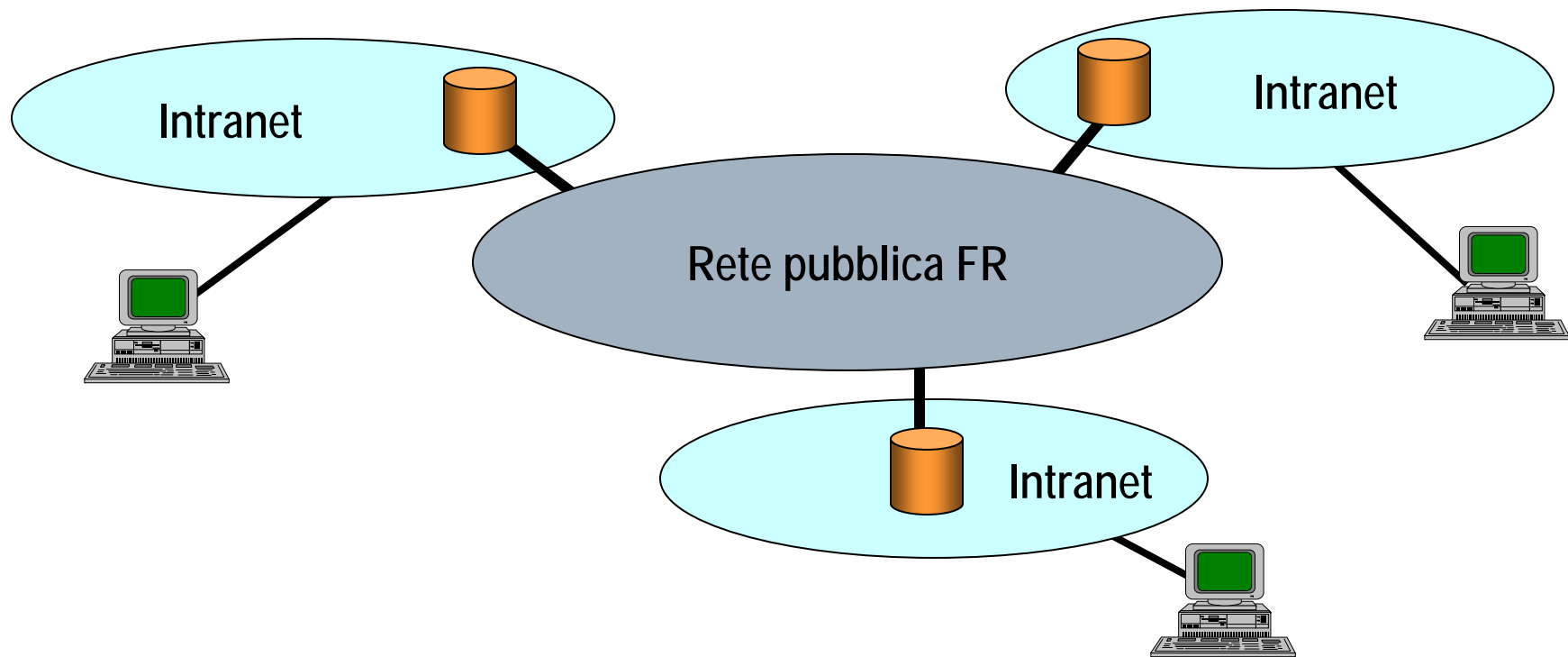
Connessione WAN di intranet remote

- ❑ Uso di canali dedicati
- ❑ Problemi:
 - l'uso può non giustificare il costo elevato



Connessione WAN di intranet remote

- ❑ Uso di reti a pacchetto pubbliche (ad es. Frame Relay)
- ❑ Problemi:
 - l'uso può non giustificare il costo elevato

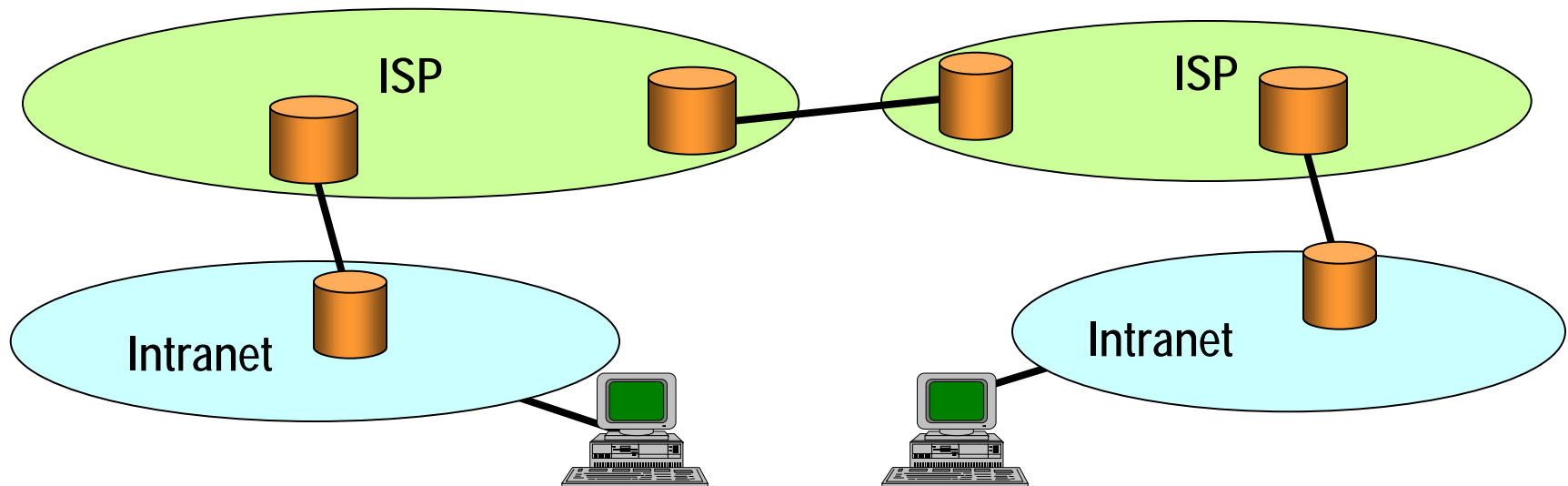


Connessione WAN di intranet remote

- ❑ Uso di INTERNET (Virtual Private Network - VPN)

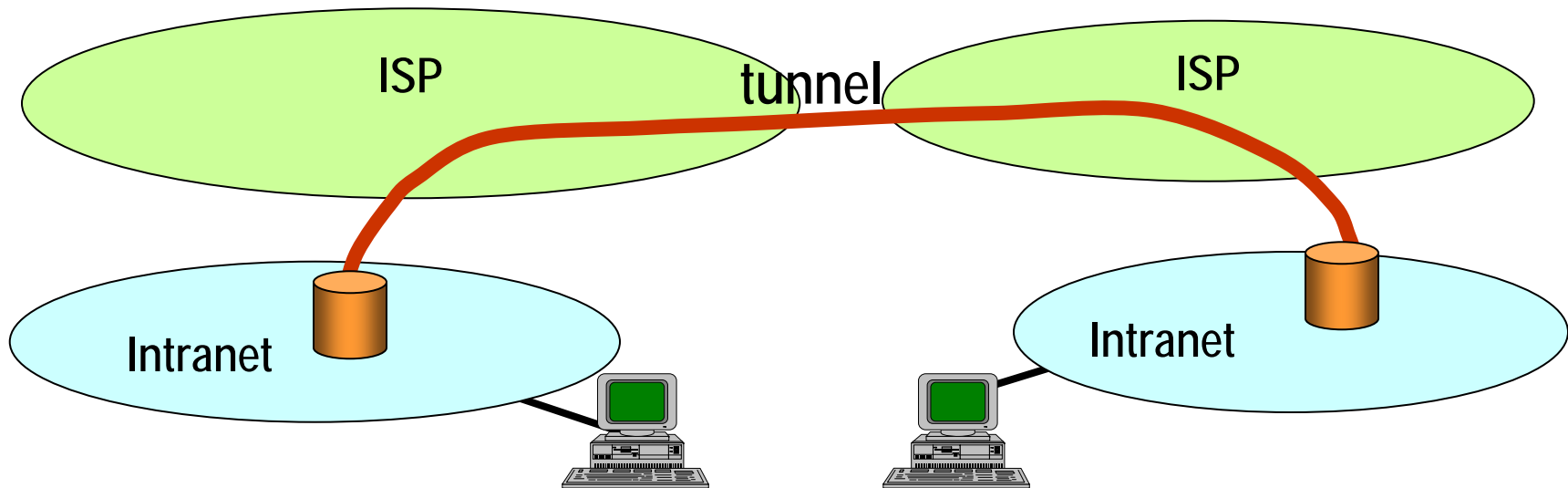
Problemi:

- uso di indirizzi privati
- sicurezza
- prestazioni



Virtual Private Networks

- Tunnel di collegamento



IP tunneling

- ❑ Il tunnel si costruisce incapsulando trame IP in altre trame IP
- ❑ Il payload che viaggia nel segmento pubblico può essere crittato
- ❑ Gli indirizzi A e B possono essere privati

