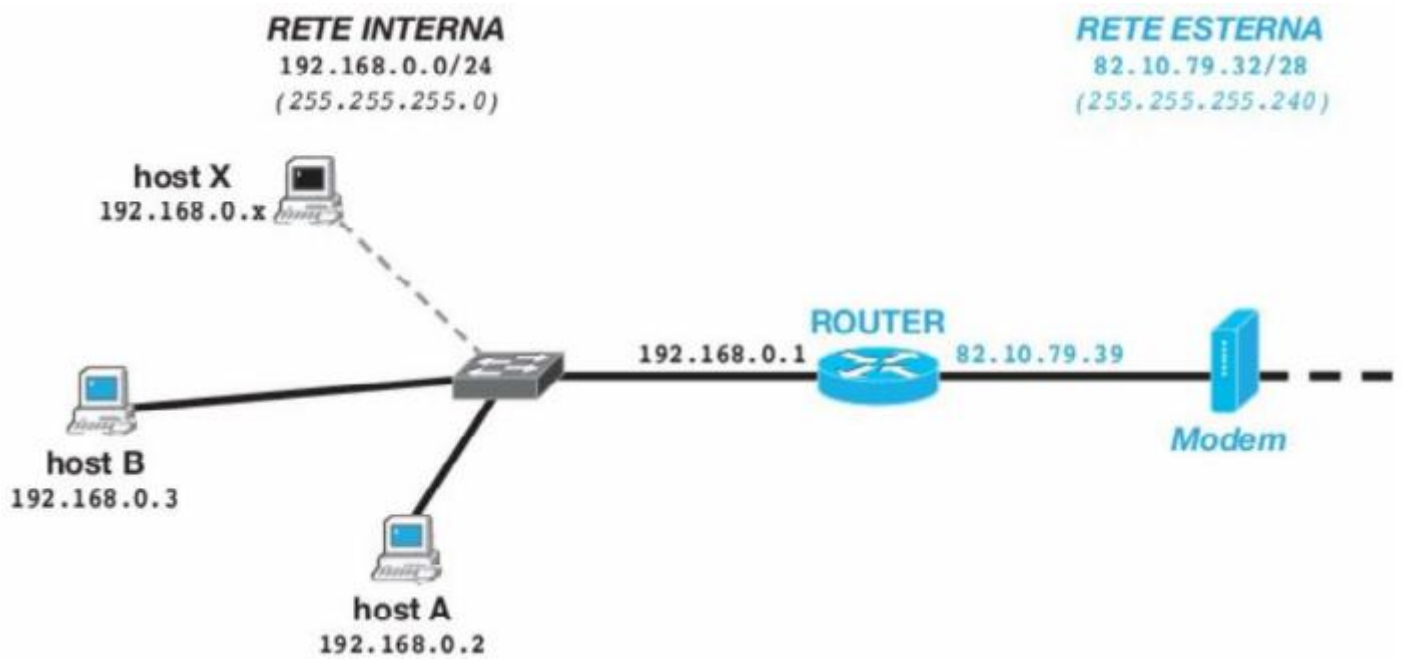
NAT – Network Address Translation

Mattia Pacchin – mattia@v-research.it

V-ReseArch Edu

Internetworking

- La connessione di reti differenti avviene tramite il router (liv. 3)
- Per connettere una rete privata a una rete pubblica, pertanto, è necessario che un router possegga almeno due interfacce:
    1. sulla rete privata
    2. sulla rete pubblica



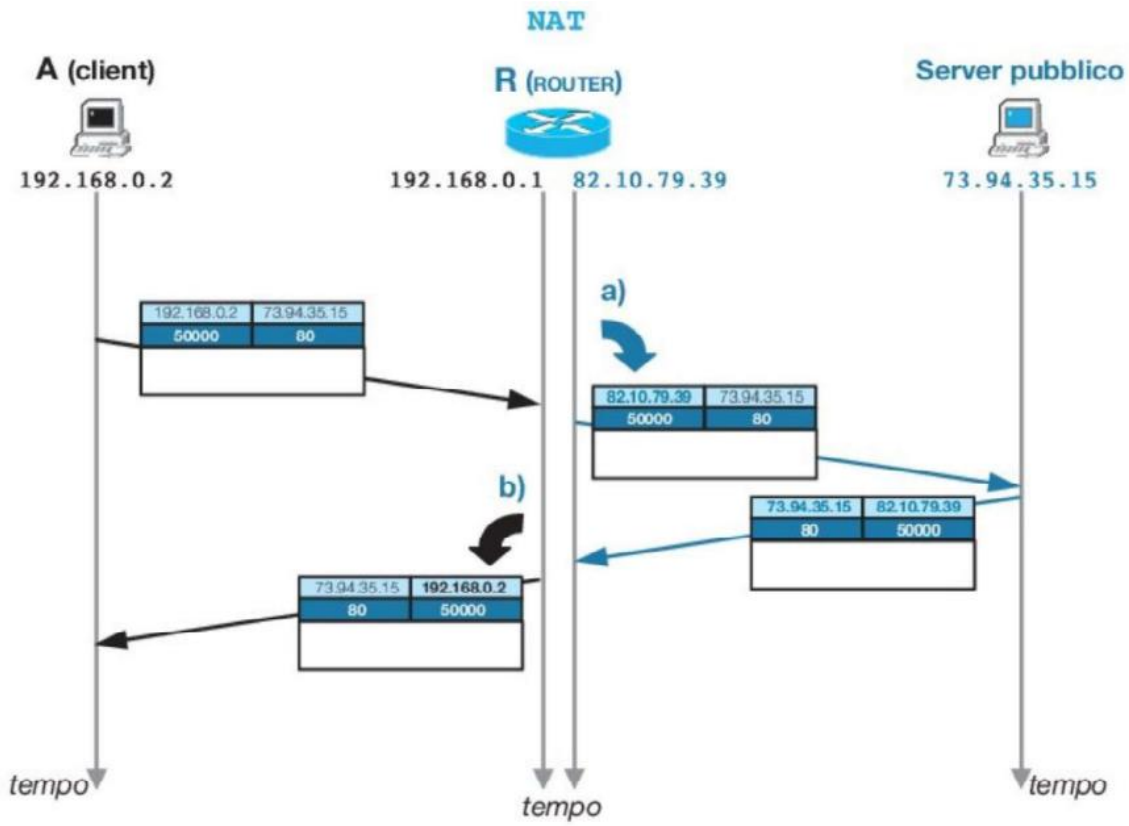
Internetworking

- Scarsità degli indirizzi IP: i molti host di una rete privata non possono essere configurati con indirizzi IP pubblici, nemmeno se ottenuti dinamicamente
- È necessario che una rete privata si doti di un meccanismo che permetta agli host interni di usufruire dei servizi messi a disposizione dalla rete pubblica
- È inoltre estremamente serio il problema della sicurezza: sulla rete pubblica operano milioni di utenze, tra le quali anche quelle ansiose di intercettare, violare o accedere ai dati contenuti nelle reti private che si affacciano al dominio pubblico. È necessario dotare le reti private di sistemi in grado di assicurare la rete da intrusioni indesiderate pur concedendo l'accesso alle utenze legittime (es. firewall)
- Il traffico di una rete privata verso la rete pubblica può essere anche molto sostenuto e variegato; il bitrate di una rete privata è senz'altro superiore al bitrate di una rete pubblica e lo stesso canale di connessione è utilizzato continuamente in contemporanea da numerose utenze

NAT

- Non si tratta di un protocollo, ma di una programma, o meglio, di un processo
- Se un host con un indirizzo IP privato tentasse una connessione TCP/IP verso un host con indirizzo IP pubblico attraversando un router provvisto di NAT, il router potrebbe:
  - cambiare l'IP sorgente (privato) con il proprio IP (pubblico), inoltrare il pacchetto sulla rete pubblica, attendere le risposte e, su queste,
  - sostituire nei pacchetti ricevuti l'indirizzo IP destinazione (proprio) con l'indirizzo IP (privato) dell'host e inoltrarlo a esso sulla rete privata.
  - In questo modo l'host privato ottiene il servizio di rete pubblica

NAT

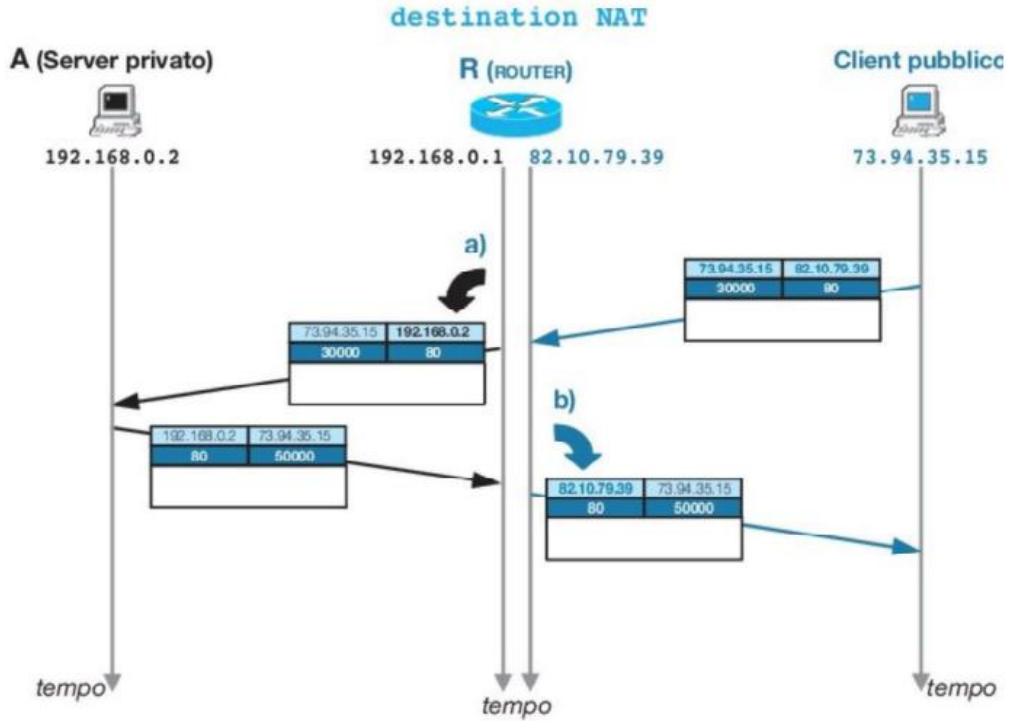


NAT

- Se tutti i client della rete privata intendessero usufruire del NAT, il router sarebbe costretto a mapparne le richieste (per ricordarne le restituzioni) basandosi sul numero di porta effimera utilizzata nei pacchetti client (nel disegno, 50000)
- L'ipotesi più sfavorevole è che due o più client vogliano connettersi sulla stessa porta di un server pubblico (per esempio Google): al router non rimarrebbe che «ricordare» le connessioni in entrata in base alla porta TCP sorgente (la porta effimera), l'unico parametro identificativo del client
- A rigor di logica, anche le porte effimere potrebbero coincidere (sono infatti decise casualmente in locale dai client)
- Un NAT effettivo, quindi, mappa le connessioni sulle porte effimere, e prende il nome di PAT (Port Address Translation, oppure IP masquerading, oppure ancora NAPT, Network Address and Port Translation)
- In questo caso la porta effimera (porta TCP sorgente) viene effettivamente modificata dal server NAT in modo che sia univoca e che possa contraddistinguere i pacchetti di ritorno per la riconsegna all'host originario

NAT

- Naturalmente è possibile che un router effettui l'operazione opposta, ovvero mappi le connessioni provenienti dall'esterno e dirette a un suo indirizzo pubblico verso l'indirizzo privato di un host interno alla rete privata.



V-ReseArch Edu

Sicurezza NAT

- Gli host privati non si presentano mai con il loro reale indirizzo IP sulla rete pubblica e, almeno in teoria, il source NAT impedisce «nativamente» a macchine pubbliche di raggiungere le macchine private della rete
- Inoltre, pur rappresentando un «single point of failure» (un aspetto critico perché il malfunzionamento di un solo elemento della rete determina il malfunzionamento di tutti gli elementi della rete), il server NAT, se ben configurato, riflette automaticamente la sua configurazione di sicurezza a tutti gli host interni senza che questi debbano preoccuparsene espressamente.