



NAT

Problema

Si ha a disposizione un numero N di macchine e un numero M di indirizzi IP, con $M < N$.

Gli indirizzi IP, infatti, hanno un costo che, generalmente, risulta tanto più elevato quanto minori sono le caratteristiche del contratto di connettività acquistato.

Si rende pertanto necessario un sistema per consentire alle restanti macchine di collegarsi ad Internet.

Per semplicità, nel seguito, supponiamo di disporre di un solo indirizzo IP.

Reti private

Nell'assegnazione degli indirizzi IP, vi sono alcuni blocchi di indirizzi, descritti in RFC1918, che vengono allocati per reti ad uso privato:

La rete di classe A 10.0.0.0 – 10.255.255.255

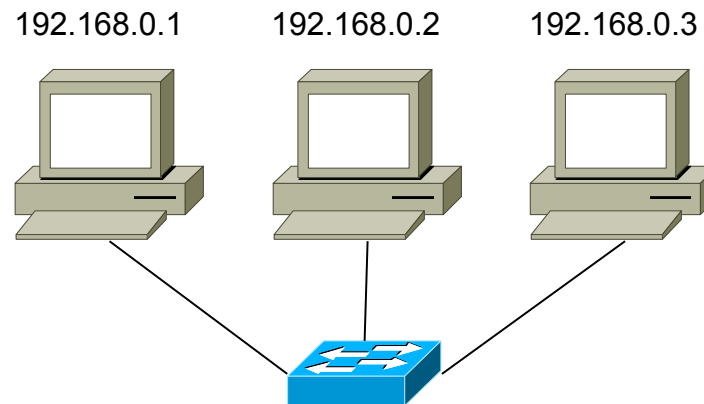
Le 16 reti di classe B 172.16.0.0 – 172.31.255.255

Le 256 reti di classe C 192.168.0.0 – 192.168.255.255

Non esiste in Internet una rete con questi blocchi di indirizzi e i router della rete sono programmati (o, almeno, dovrebbero esserlo) per non instradare pacchetti provenienti da questi indirizzi.

Topologia di una intranet

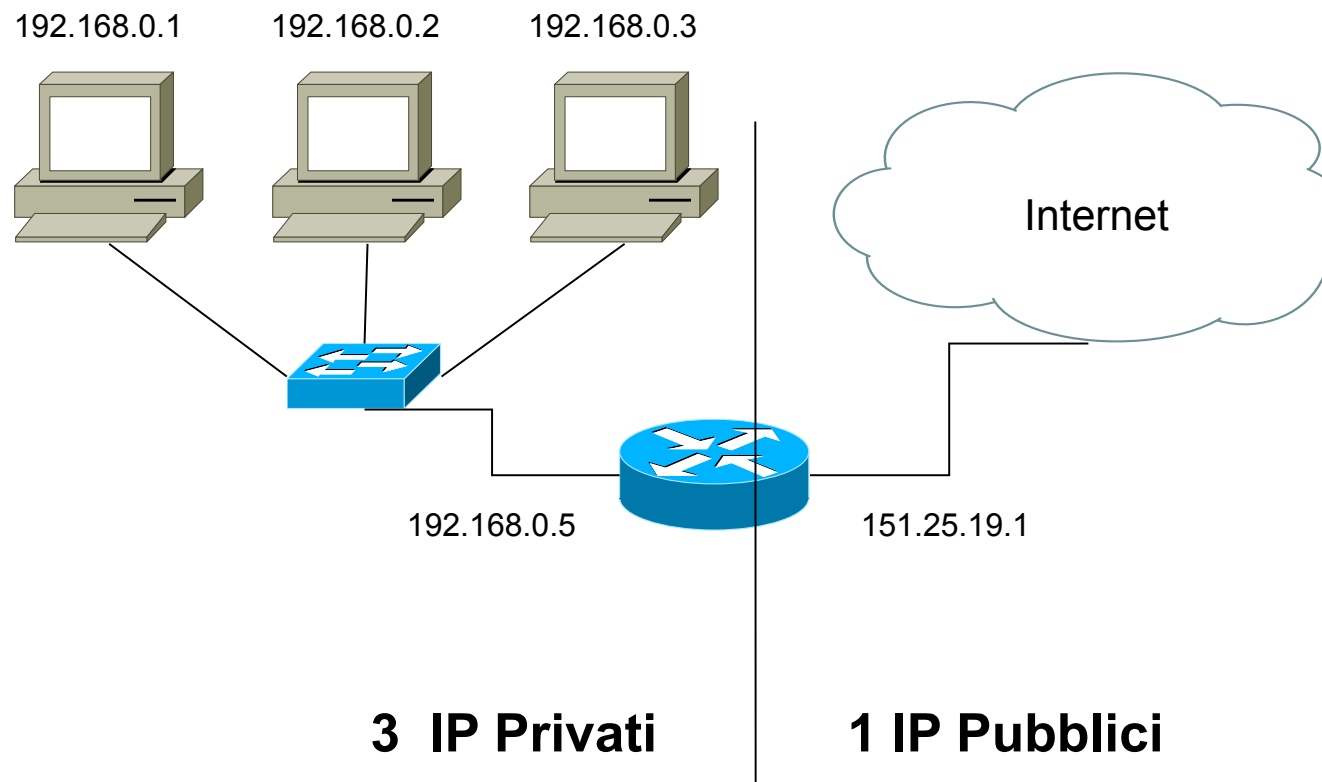
Prendiamo l'esempio di una semplice Intranet senza uscita su Internet.



NAT

Topologia di una intranet

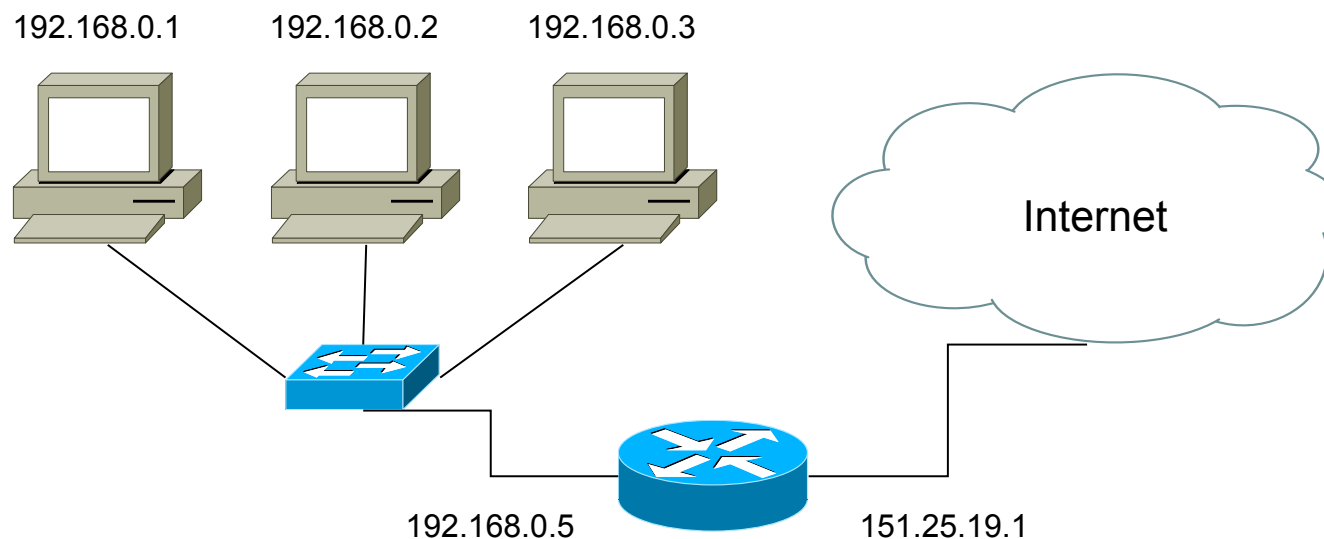
Assegnamo l'unico IP address pubblico disponibile ad un router con due interfacce di rete: una collegata all'intranet e una su internet (extranet).



Topologia di una intranet

Problema: un pacchetto proveniente da 192.168.0.1 non può essere mandato su Internet, in quanto verrebbe automaticamente cancellato dal primo router in rete e, quand'anche così non fosse, la risposta non arriverebbe a destinazione.

L'unica via d'uscita è che un pacchetto esca con 151.25.19.1

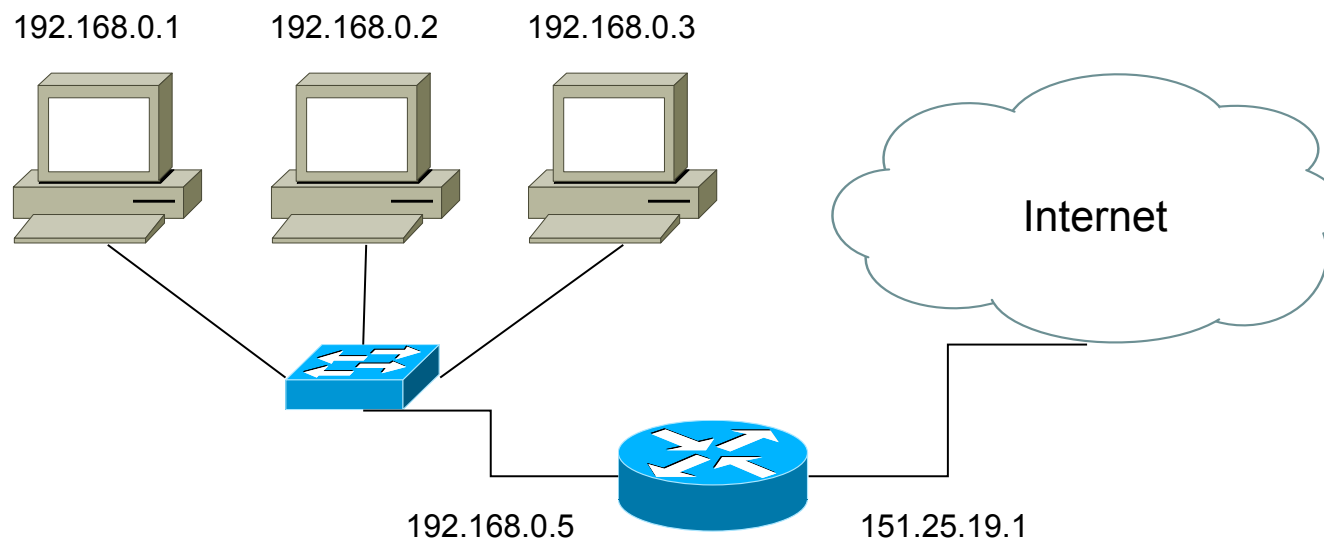


NAT

Network Address Translation

Il router riceve una richiesta di connessione da 192.168.0.1 verso il nodo X. Sostituendosi alla macchina locale, il router effettua la richiesta con il SUO indirizzo IP pubblico.

Ricevuta risposta, la inoltra sulla rete privata per il tramite del suo IP privato e procede così per tutta la durata della connessione.



Network Address Translation

L'intero meccanismo del NAT si regge interamente sull'utilizzo delle porte.

Quando il router riceve una richiesta di instradamento di connessione, effettua la connessione con il proprio IP pubblico e memorizza in una tabella:

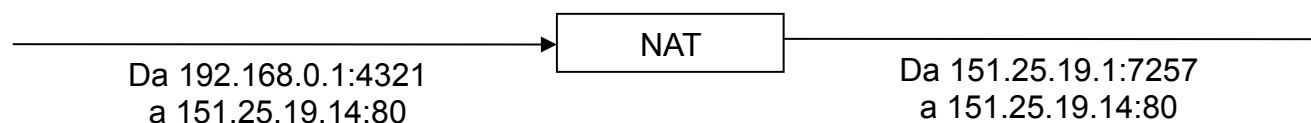
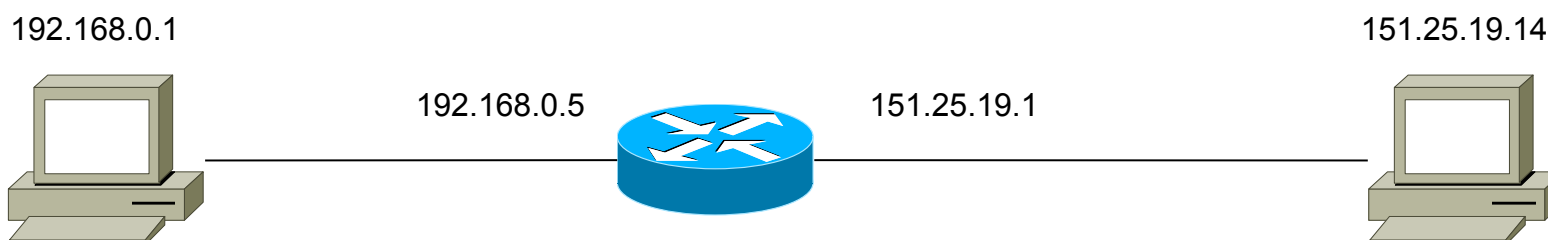
- a) l'indirizzo IP e la porta sorgente locale**
- b) la porta locale con cui effettua la connessione**

Così facendo, è in grado, quando arriva un pacchetto di risposta sulla porta locale, di sapere a quale macchina rigirarlo.

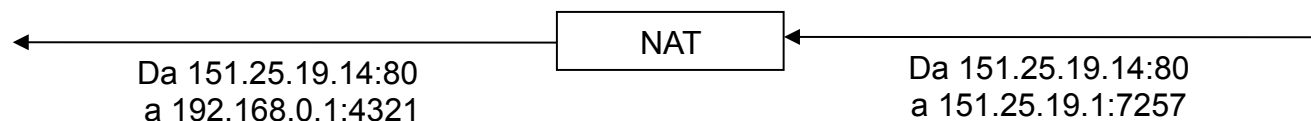
NAT

Network Address Translation

Esempio



NAT Table		
Public port	Local IP	Local port
7257	192.168.0.1	4321



Limitazioni del NAT

Se una macchina di rete interna fa partire una connessione, è possibile, per il NAT, tracciare la connessione e mantenerla attiva fino alla fine.

Se, tuttavia, dall'esterno arriva una richiesta di connessione ad una porta che non è stata precedentemente allocata da una macchina interna tramite una connessione, il NAT non sa a quale delle macchine interne rigirlarla e scarterà il pacchetto.

NAT Table		
Public port	Local IP	Local port
7257	192.168.0.1	4321



Da 151.25.19.13:7534
a 151.25.19.1:4322

NAT

Port Forwarding

E' tuttavia possibile configurare a priori il NAT per far sì che, alla richiesta (dall'esterno) di una connessione su una determinata porta, il NAT invii il pacchetto a una macchina predefinita all'interno della rete.

Una tale configurazione prende il nome di *port forwarding*.

NAT

Port Forwarding

Esempio

