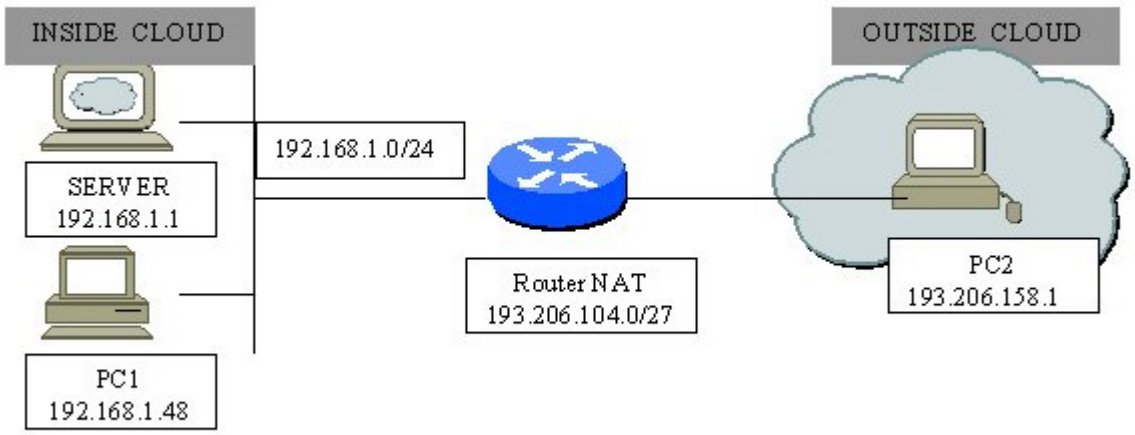
NAT (Network Address Translation)

L'implementazione del NAT su un router Cisco, comporta una problematica per la cui soluzione è richiesta la conoscenza di alcune specificità che, di seguito, vengono indicate, divise per colorazioni: verde per la configurazione di base con NAT dinamico, blu per l'aggiunta del NAT statico nel caso si abbiano dei server all'interno della LAN, rosso per indicare una soluzione per i problemi di routing loop.

Di seguito sono riportati, uno schema tipico, la relativa configurazione da utilizzare nonché le problematiche associate a tale configurazione in caso di traffico, generato sia dall'interno che dall'esterno.

Schema

Nell'esempio che segue il NAT è definito sul range di indirizzi validi (pubblici) 193.206.104.2-193.206.104.31.
La classe C interna (privata) utilizzata è la **192.168.1.0/24**.
Consideriamo un solo server interno.



La conseguente configurazione sarà:

ip nat pool prova-pool 193.206.104.2 193.206.104.31 prefix-lenght 24

!definisce il NAT pool chiamato prova-pool con un range di indirizzi pubblici da utilizzare x internet

ip nat inside source list 1 pool prova-pool [overload]

!indica che ogni pacchetto ricevuto sulla inside interface e ammesso dalla acl-1 avra` una corrispondenza tra l'indirizzo privato "source" e un indirizzo pubblico "out" del NAT pool "prova-pool". La keyword "overload" abilita il NAT ad associare piu` indirizzi privati su un singolo ip pubblico del pool, in questo caso il router mantiene una ulteriore informazione dai protoccolli di livello superiore (per esempio, i numeri di porta TCP o UDP) per tradurre dall'indirizzo globale il corretto indirizzo locale.

interface eth0
ip address 192.168.1.2

ip nat inside
!definisce la eth0 come inside interface

interface ser0
ip address 193.206.104.32

ip nat outside
!definisce la ser0 come NAT outside interface

ip route 193.206.104.0 255.255.255.0 null0
!necessaria con NAT !!!

ip nat inside source static 192.168.1.1 pool 193.206.104.1
!definiamo una statica per il server

access-list 1 deny host 192.168.1.1
access-list 1 permit 192.168.1.0 0.0.0.255
!acl che indica il range da utilizzare all'interno della lan, in questo caso una /24

ip route 0.0.0.0 0.0.0.0 serial 0

Esempio di traffico generato tramite un ping:

Vediamo cosa accade quando si genera traffico dall'interno della lan.
Effettuando un ping da PC1 (192.168.1.48) verso PC2 (193.206.158.1, un qualsiasi pc esterno). Il NAT-router associa al 192.168.1.48 un ip del prova-pool ad esempio 193.206.104.10, questa corrispondenza va nella translation-table. Quindi il pacchetto arriva sulla etho (inside) e viene inviato alla ser0 (outside).
Al ritorno tale pacchetto ha come destination ip 193.206.104.10, e sara` quindi convertito in 192.168.1.48 perche` gia` presente nella translation-table.
Ciò significa che il pacchetto arriva sulla ser0 (in) e viene inviato sulla eth0 (out).
Il ping tra pc1(interno) e pc2(esterno) a questo punto termina con successo.

Il problema nasce quando il traffico va in senso contrario. E` importante sapere che quando c'e` NAT se il traffico va dall'esterno verso l'interno prima viene controllata la translation-table e poi viene effettuato il routing, invece quando il traffico va dall'interno verso l'esterno accade il contrario e cioe` prima viene controllata la routing table e poi viene cambiato l'ip.
Vediamo cosa puo` accadere se PC2 prova a comunicare con un indirizzo di destinazione non presente nella translation-table (ad esempio un ip pubblico del prova-pool). Lo scenario e` lo stesso ma il ping parte questa volta da PC2 (193.206.158.1) verso un IP pubblico ad es. 193.206.104.10. In questa circostanza il router non trova nessuna entry nella translation-table per il pacchetto in questione, e quindi lo rimanda dietro sulla ser0.
Questo causa un loop che nella maggior parte dei casi manda down la seriale.
Quindi la statica per gli indirizzi pubblici con next hop a null0 serve proprio ad evitare questo tipo di routing loop.

A questo punto e` chiaro che tutti i pacchetti che viaggiano dall'interno verso l'esterno vengono conservati con il rispettivo ip pubblico nella translation-table almeno fino allo scadere di un determinato timeout.
Nel caso in cui vogliamo offrire dei servizi che necessitano di ricevere pacchetti originati dall'esterno (www, email, ecc.) allora siamo obbligati ad implementare anche il NAT statico. In questo modo la corrispondenza tra ip pubblico e privato viene forzata nella translation-table in maniera definitiva.