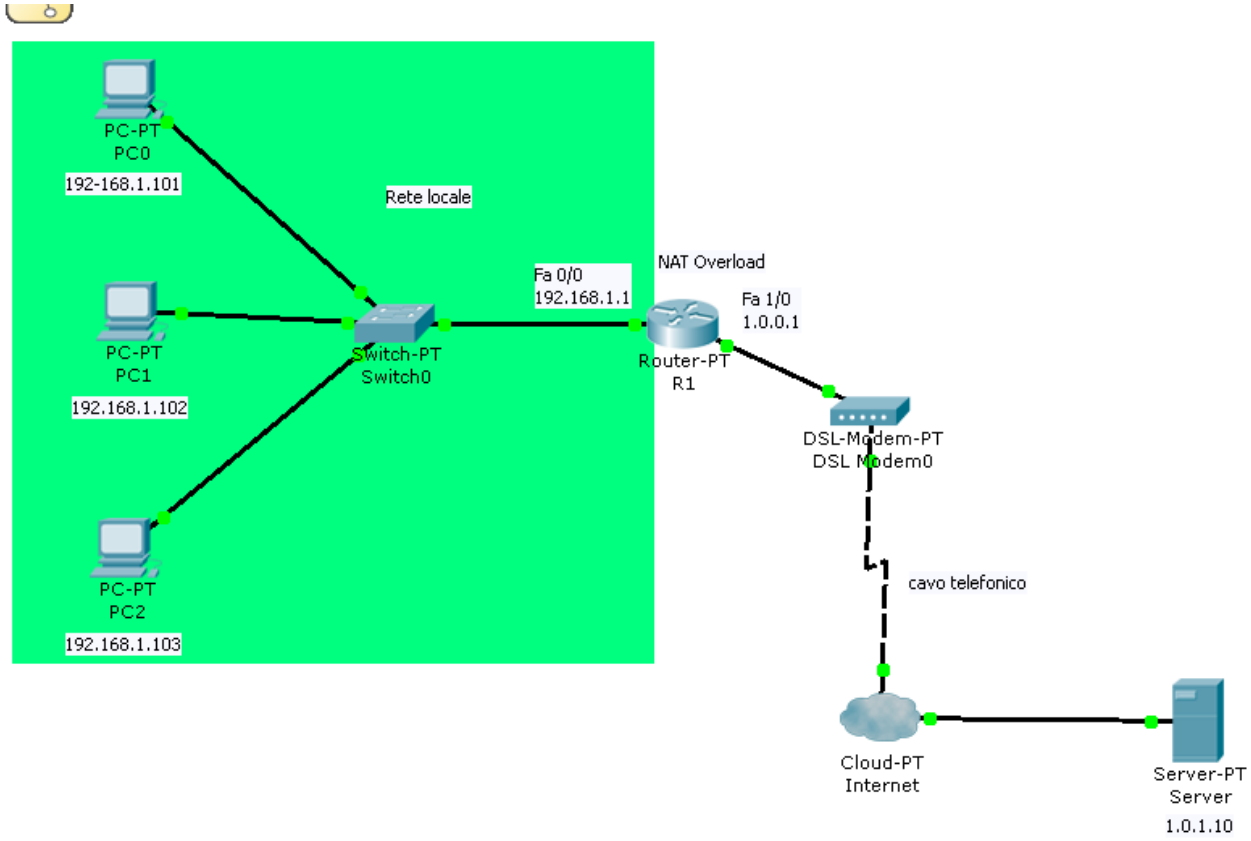
NAT overload dinamico (PAT)

Supponiamo di considerare la rete in figura, e la parte sinistra di essa sia una LAN con indirizzi privati, mentre il resto della rete sia una rete pubblica, a cui, in questo caso, si interfaccia un modem ADSL. Si fa notare che in questo schema il modem ADSL è un dispositivo elementare a tutti gli effetti (ben diverso dai dispositivi multipurpose[1] che di solito si vanno ad acquistare, che conglobano una serie di diverse funzionalità integrate.



Modem ADSL in PT e Cloud PT

Tale modem simulato ha solo le effettive funzionalità di un modem (ADSL), vale a dire entra in esso la linea telefonica, collegata con apparati dell'ISP e captati gli opportuni segnali di linea transla su un cavo Ethernet le comunicazioni in ingresso o in uscita. Possiamo pensarlo quindi come un adattatore di linea su un solo cavo, da cavo telefonico a cavo Ethernet (digitale) e viceversa. Si faccia attenzione anche che la linea telefonica non ha ovviamente numeri di IP (non inserire mai su essa indicazioni IP !), e il capo Ethernet del modem non ha uno specifico numero di IP, in quanto è il router a valle (nella rete dell' ISP) ad averlo. Quindi il solo modem ADSL è solo un dispositivo che opera a livello fisico come l'hub, ed in quanto tale del tutto trasparente alla problematica dei numeri di rete e della loro gestione[2]. La linea telefonica del modem si interfaccia nello schema con un dispositivo di laboratorio, che simula Internet o una rete globale (Cloud). Tale dispositivo ha molteplici tipi di ingresso proprio per

1 In PT esiste però una simulazione di un tipico modem da casa integrato in un unico elemento, qui non utilizzata.
2 Si pensi al cavo telefonico ed al successivo cavo ethernet come ad un solo cavo, continuo, per semplificare.

interfacciare in un tutt'uno più linee entranti in esso (nel cloud). Nel nostro caso è stato necessario regolare il dispositivo a interfacciare la linea modem relativa al nostro ADSL (mappata sull'entrata modem4, all' uscita in Ehternet 6, quella poi collegata al server). Si tratta quindi di un adattatore multiporta, anch'esso non avente un mapping dei numeri di IP alle sue estremità.

NAT statico e NAT dinamico con overload

Il NAT statico è usualmente utilizzato per rendere visibile su una rete esterna pubblica, una macchina con numerazione di IP privata. In questo modo il meccanismo è chiaro: ogni macchina che deve essere visibile sulla rete esterna pubblica avrà un suo numero di IP, che poi viene tradotto tramite NAT sull'ultimo router che confini con la rete privata, di modo da inoltrare alla appropriata macchina tutti i relativi pacchetti[3].

In questo meccanismo la traduzione è 1 a 1, e non ci sono ambiguità o sovrapposizioni. Queste regole di traduzione sono usualmente settate nel router a mano e quindi staticamente[4].

Un diverso sistema per avere possibilità di comunicare su una rete pubblica per macchine presenti su una rete LAN con numerazione privata e il NAT oveloading, detto anche PAT[5].

In questa tecnica invece di avere più IP pubblici che interfacciano altrettante macchine private, si ha solo un indirizzo IP[6] disponibile verso la rete esterna pubblica, e si deve utilizzare quello per interfacciare all'esterno più macchine della rete privata.

In realtà con la logica descritta con il NAT statico questo compito sembrerebbe impossibile, ma non è così. Bisogna viceversa cambiare approccio.

Intanto in questo caso è bene considerare che la tabella di traduzione NAT diviene dinamica e le sue voci durano un tempo molto breve (pochi secondi), dopodichè vengono eliminate, inoltre in questa tabella iniziano a fare la loro comparsa indicazioni che oltre al numero di IP, segnano anche numeri di porta. Tali numeri di porta nel caso di traduzione dell'indirizzo sorgente registrano il numero di porta sorgente. Nel caso tale numero di porta sia unico nelle voci registrate nella tabella di NAT, non c'è motivo di translarlo. Il numero di porta in questa situazione, in questo caso diviene la discriminante per capire a quale indirizzo IP interno corrisponda un certo pacchetto[7].

Bisogna tener presente che nel NAT con overload il numero di IP su cui su basa il NAT è unico. In tal caso, quindi, quando ci sia una coincidenza del numero di porta tra pacchetti in transito provenienti da diversi IP della rete locale, è necessario distinguere i pacchetti, perchè altrimenti essi dovrebbero andare tutti ad una stessa destinazione. In pratica se il pacchetto che proviene da 192.168.1.102:2 con

3 Si ricorda che un indirizzo IP privato è necessariamente ambiguo, essendo ripetuto in innumerevoli LAN nel mondo. Si pensi ad un esempio: in casa ci possiamo chiamare solo con il nome, perchè, presumibilmente, non ci sono ambiguità, dato il basso numero di persone, ma fuori usualmente quando dobbiamo dare le nostre generalità dobbiamo utilizzare il cognome o la combinazione nome + cognome, quindi un "indirizzo" diciamo così pubblico, potenzialmente univoco.

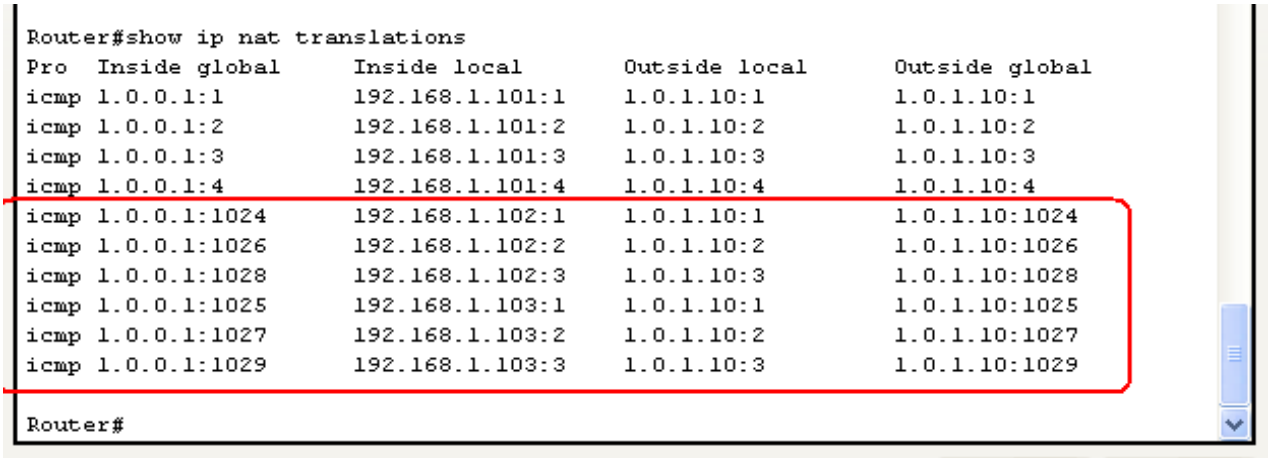
4 Si noti che diverse macchine della sottorete potrebbero non essere in possesso di questa traduzione e quindi della visibilità all'esterno di una LAN.

5 Da Port and Addrees Translator – ossia si hanno traduzioni anche sulle porte in questo caso.

6 Sarebbe infatti troppo oneroso per gli ISP ed in generale per la comunità Internet, data la attuale scarsità di indirizzi IP, mappare ogni macchina privata con un indirizzo IP pubblico ad hoc

7 Questo infatti non è più possibile farlo tramite l'indirizzo di IP pubblico, che è ormai unico per tutti i pacchetti.

porta sorgente 2 dovesse venir tradotto in modo pedissequo, si avrebbe che esso si traduce in 1.0.0.1:2. Siccome però tale ingresso in tabella esiste già, tale traduzione non è univoca (vd. colonna inside global). In questo caso quindi il NAT effettua anche un cambio di porta, di modo da rendere univoca la voce nella colonna Inside global, e da permettere quindi una ritraduzione univoca, che indirizzi, nel nostro esempio al PC 192.168.1.102[8], senza equivoci. Ovviamente con questo meccanismo anche il numero di porta deve essere oggetto di traduzione da parte del NAT, assieme al numero di IP. Si parla infatti di PAT (Port and Address Translation). Il vantaggio di questa metodica è di utilizzare un unico numero di IP pubblico, cosa molto appetibile per gli ISP , per gestire molteplici indirizzi di IP privati.



```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.0.0.1:1         192.168.1.101:1    1.0.1.10:1         1.0.1.10:1
icmp 1.0.0.1:2         192.168.1.101:2    1.0.1.10:2         1.0.1.10:2
icmp 1.0.0.1:3         192.168.1.101:3    1.0.1.10:3         1.0.1.10:3
icmp 1.0.0.1:4         192.168.1.101:4    1.0.1.10:4         1.0.1.10:4
icmp 1.0.0.1:1024      192.168.1.102:1    1.0.1.10:1         1.0.1.10:1024
icmp 1.0.0.1:1026      192.168.1.102:2    1.0.1.10:2         1.0.1.10:1026
icmp 1.0.0.1:1028      192.168.1.102:3    1.0.1.10:3         1.0.1.10:1028
icmp 1.0.0.1:1025      192.168.1.103:1    1.0.1.10:1         1.0.1.10:1025
icmp 1.0.0.1:1027      192.168.1.103:2    1.0.1.10:2         1.0.1.10:1027
icmp 1.0.0.1:1029      192.168.1.103:3    1.0.1.10:3         1.0.1.10:1029

Router#
```

Viceversa se più pacchetti provenienti da un solo numero di IP viaggiano verso la stessa destinazione IP / porta, non vi è motivo di translare anche l'indicazione di porta nella traduzione, e si ha solo una traduzione di indirizzo, come nelle prime righe della tabella di translazione NAT della figura precedente.
La tecnica di traduzione PAT è quella utilizzata anche dai comuni modem / router ADSL casalinghi.
Per mostrare la tabella di traduzione NAT basta dare il comando:

```
show ip nat translations
```

in modalità privilegiata (#).
E' possibile pulire le tabelle di traduzione NAT[9], dando il comando:

```
clear ip nat translation *
```

Settaggi per il NAT overload

Per attivare il NAT overload si dovranno dare i seguenti comandi (ovviamente adattati alle necessità caso per caso). Per prima cosa si definisce un insieme di indirizzi (tecnicamente denominata *access-list*) dai quali sarà ammesso richiedere il NAT. Fuori da tale range di indirizzi, il NAT non potrà essere effettuato. Nel nostro caso:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

si noti il formato delll'istruzione. In coda invece di indicare la net mask si specifica al contrario la parte

8 O al 192.168.1.103, anch'esso oggetto di disambiguazione
9 Operazione utile soprattutto a scopo di test

degli indirizzi host. (in questo caso l' intera sottorete di classe C 192.168.1.0).

L'altra istruzione specifica IOS che definisce come debba essere tradotto tale gruppo di indirizzi è:

```
ip nat inside source list 1 interface FastEthernet1/0 overload
```

che indica che la access list 1 dovrà essere tradotta in NAT in base all' indirizzo IP della interfaccia 1/0 del router in modalità overload (ossia utilizzando qual solo numero di IP, e quindi se necessario effettuando la traslazione delle porte).

In questa sintassi inside indica che gli indirizzi tradotti inizialmente sono quelli interni (*inside*) alla sottorete privata. In precedenza si è definito quale sia l'interfaccia considerata interna (quella verso in numeri di IP privati) e quale quella esterna (verso gli IP pubblici).

L'indicazione *source* invece indica che, nella traduzione verrà tradotto l'indirizzo sorgente (e non quello destinazione).

Si ricorda anche qui che per definire il lato interno (inside) ed esterno (outside) si danno i comandi:

```
R1> enable                modalità standard
R1# config                      modalità privilegiata
R1 (config)# int Fa0/0       modalità configurazione
R1 (config-if)#                   modalità configurazione interfaccia
R1 (config-if)# ip nat inside
R1 (config-if)# exit
R1 (config)# int Fa1/0
R1 (config-if)#
R1 (config-if)#ip nat outside
R1 (config-if)#exit
R1 (config)#
```

iin precedenza si devono assegnare gli IP alle interfacce di rete del router tramite comandi Cisco IOS:

```
R1 (config)# int Fa0/0
R1 (config-if)# ip address 192.168.1.1 255.255.255.0
R1 (config-if)# no shutdown
R1 (config-if)# exit
R1 (config)#
R1 (config)#int Fa1/0
R1 (config-if)# ip address 1.0.0.1 255.0.0.0
R1 (config-if)# no shutdown
R1 (config-if)# exit
R1 (config)#
```

si ricorda che il comando no shutdown attiva l'interfaccia, mentre il comando shutdown la spegne.

Per visionare l'intera configurazione di un router con l'elenco organico dei comandi di regolazione dati, si può digitare il comando (assai utile):

```
R1# show running-config
```