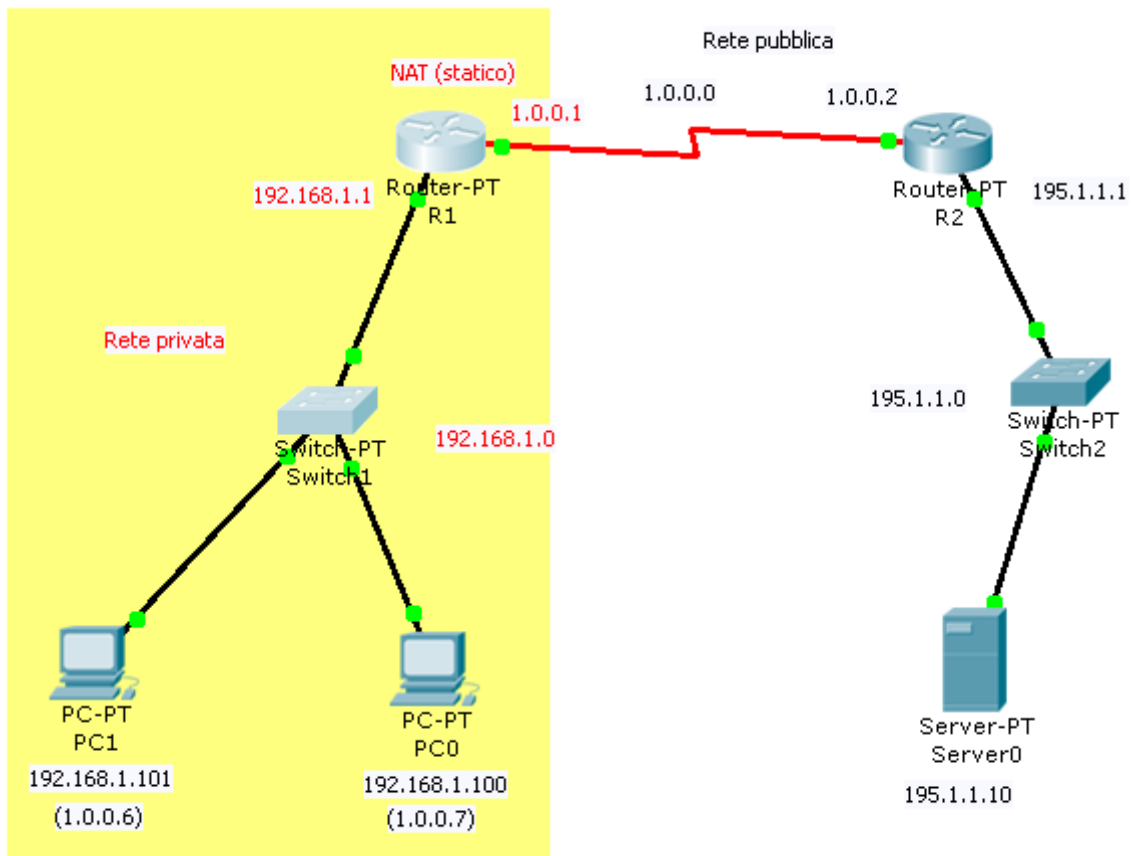


Rete con NAT¹ statico



In questa esercitazione PT consideriamo una rete che utilizza il cosiddetto NAT statico.

Si suppone nello schema che a sinistra sia presente una rete locale privata (infatti dotata di IP privati in classe C) al centro (schematizzata, in questo caso, con il collegamento seriale a lunga distanza) la rete Internet, mentre a destra, dopo il router R2, un fornitore di servizi.

Per NAT statico si intende una traduzione statica (quindi fissata) degli indirizzi dei pacchetti IP di una sottorete di origine (in questo caso) transitanti nel router in degli indirizzi IP disponibili presi tra quelli della sottorete confinante, nel nostro caso 1.0.0.0 (data la netmask definita 255.0.0.0 è rete, pubblica, di classe A). In pratica il NAT statico è stato effettuato su R1 con la seguente regola:

Rete 192.168.1.0	Rete 1.0.0.0
(PC0) 192.168.1.100	1.0.0.6
(PC1) 192.168.1.101	1.0.0.7

Da notare che la traduzione settata è a tutti gli effetti bidirezionale, ossia avendo in arrivo un pacchetto giungente al router R1 con indirizzo di destinazione 1.0.0.7 ad esso viene applicata la regola di

¹ NAT stà per Network Address Translator, in italiano traducibile con traduttore di indirizzi di rete.

traduzione indicata e l'indirizzo IP di destinazione viene modificato in 192.168.1.101 presente nella sottorete di destinazione. In pratica con tale meccanismo tramite indirizzi pubblici fissi (nella tabella nella colonna di destra, PC0 e PC1 possono, volendo essere contattati dall'esterno della rete privata agli indirizzi IP oggetto della traduzione (1.0.0.6 e 1.0.0.7).

Per prima cosa per abilitare le funzioni di NAT sul router bisogna dare i comandi:

```
R1(config)# int fa0/0
R1(config-if)# ip nat inside
R1(config-if)# exit
R1(config)# int se2/0
R1(config-if)# ip nat outside
R1(config-if)# exit
```

Questi comandi definiscono che la porta Fa0/0 è interna² alla zona sottoposta a NAT e quella seriale Se2/0 è verso l'esterno del NAT.

Successivamente gli effettivi settaggi di NAT sono effettuabili e visibili tramite i comandi³:

```
R1(config)#ip nat inside source static 192.168.1.100 1.0.0.6
R1(config)#ip nat inside source static 192.168.1.101 1.0.0.7
R1(config)#exit
R1#
*SYS-5-CONFIG_I: Configured from console by console

R1#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  1.0.0.6              192.168.1.100    ---                ---
---  1.0.0.7              192.168.1.101    ---                ---
```

Il NAT qui applicato è il *source NAT*,⁴ ossia il router R1 cambia l'indirizzo sorgente dei pacchetti che escono dal NAT e, di conseguenza, l'indirizzo di destinazione dei pacchetti che vanno verso⁵ la zona di NAT. Questa operazione simmetrica è ovviamente necessaria, in quanto i pacchetti che arrivano all'interfaccia seriale del router R1 hanno indirizzi di destinazione (ritorno), pubblici quindi tradotti, ed essi devono essere ritradotti.

Gli altri settaggi dei router sono analoghi a quelli dello schema classico con due router, tranne per il fatto che al router R2 mancano le indicazioni di instradamento verso la sottorete 192.168.1.0 in quanto costituita da comuni indirizzi privati. Nel nostro caso, ad R2, per produrre pacchetti di ritorno a tali macchine basta instradare sulla contigua e quindi conosciuta 1.0.0.0⁶, per poi riuscire a raggiungere le macchine della 192.168.1.0 grazie a NAT.

2 I successivi comandi indicano di tradurre l'indirizzo sorgente secondo la regola data, ma specificano anche che si tratta di un pacchetto proveniente dall'"interno". Questi comandi hanno lo scopo di specificare quale sia il lato interno e quale sia il lato esterno del NAT.

3 Sono due comandi simili, perchè sono stati mappati due indirizzi IP della rete privata tramite NAT. Si noti che almeno con questa metodica non è detto che tutti gli indirizzi della sottorete debbano essere mappati all'esterno e quindi possiamo avere macchine effettivamente a tutti gli effetti irraggiungibili dalla rete pubblica.

4 Viceversa si potrebbero cambiare i numeri di destinazione del pacchetto, e in questo caso si avrebbe un cosiddetto *destination NAT*

5 Ossia entranti.

6 Grazie al fatto che sulla rete pubblica circolano pacchetti con indirizzi tradotti (e a loro volta pubblici).

In realtà non ha senso che, viceversa, qualche rete indirizzi i suoi router sui numeri privati della sottorete 192.168.1.0. In quanto privati, infatti, questi numeri hanno molteplici corrispondenze nel mondo e non sono quindi univoci. Non ha quindi significato, in questo contesto che R2, instradi pacchetti verso la sottorete 192.168.1.0, che ha innumerevoli istanze nel mondo (verso quale quindi instradare effettivamente ??).

Una conseguenza pratica di questa situazione è che i computer interni alla rete sotto NAT possono contattare i computer delle reti esterne, senza problema, con i loro numeri di IP opportunamente tradotti in indirizzi pubblici, mentre viceversa i computer esterni non sono in grado di contattare i computer sottoposti a NAT, senza conoscere con precisione gli IP pubblici tramite il quale vengono mappati gli IP privati.

In ultimo mostro la schermata dell' analizzatore di pacchetti di PT, nelle quali risultano evidenti le traduzioni di indirizzi nel verso di andata (da 192.168.1.101 a 1.0.0.7) e di ritorno (da 1.0.0.7 a 192.168.1.101):

Andata

Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.1.101, Dest. IP: 1.0.0.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 1.0.0.7, Dest. IP: 1.0.0.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 00D0.BA44.4874 >> 000B.BE1E.90D7	Layer 2: HDLC Frame HDLC
Layer 1: Port FastEthernet0/0	Layer 1: Port(s): Serial2/0

Ritorno

Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 1.0.0.2, Dest. IP: 1.0.0.7 ICMP Message Type: 0	Layer 3: IP Header Src. IP: 1.0.0.2, Dest. IP: 192.168.1.101 ICMP Message Type: 0
Layer 2: HDLC Frame HDLC	Layer 2: Ethernet II Header 000B.BE1E.90D7 >> 00D0.BA44.4874
Layer 1: Port Serial2/0	Layer 1: Port(s): FastEthernet0/0