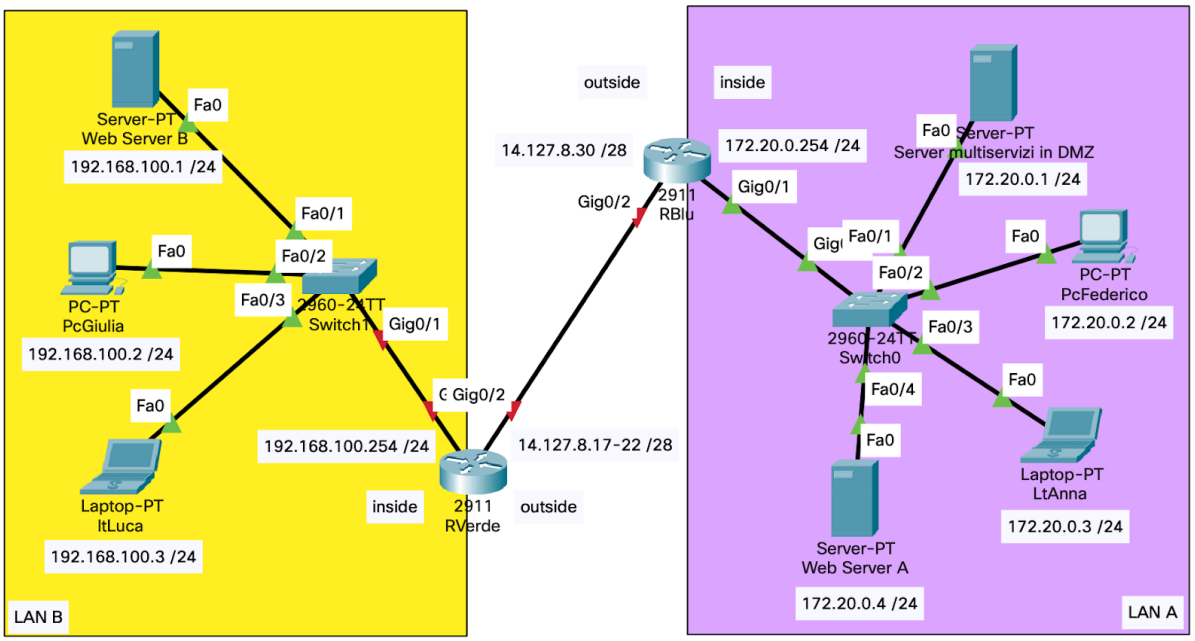
NAT - *Network Address Translation Static & Dynamic*

In questa sezione si intende mostrare il funzionamento di 4 classici tipi di **NAT** che possono essere configurati sui router Cisco:

1. **Static Translation 1-to-1**
2. **Port Address Translation 1-to-1 Port *X*** ← *dove X indica una porta a scelta, ad esempio 80*
3. **NAT Overload Translation (PAT - Port Address Translation)** ← *NAT classico di casa/ufficio*
4. **Dynamic Translation (NAT pool)** ← *Quando si ha un router con più indirizzi pubblici*

Lo schema Packet Tracer dove verranno fatte le configurazioni è il seguente. Sono presenti due LAN private collegate per semplicità da soli due router. Tali router hanno due interfacce: una verso l'interno (verso la LAN) con indirizzo privato e una verso l'esterno con indirizzo pubblico. Nella realtà potrebbe esserci una rete geografica grande a piacere che separa le due LAN.



Gli obiettivi sono i seguenti e verranno realizzati rispettivamente con i 4 tipi di NAT:

1. Il Server Multiservizi in DMZ della LAN A, deve poter essere raggiunto su qualsiasi porta tramite l'indirizzo pubblico 14.127.8.**29**
   Ogni porta espone un servizio diverso ← HTTP, FTP, DNS, ...
2. Il Web Server A della LAN A, deve poter essere raggiunto solo sulla porta 80 tramite l'indirizzo pubblico 14.127.8.**30**
3. Gli host della LAN A sebbene abbiano un indirizzo IP privato, devono poter uscire dalla propria rete sfruttando l'unico indirizzo IP pubblico del router RBlu.
4. Gli host della LAN B sebbene abbiano un indirizzo IP privato, devono poter uscire dalla propria rete sfruttando l'insieme (*pool*) di indirizzi IP pubblici del router RVerde.

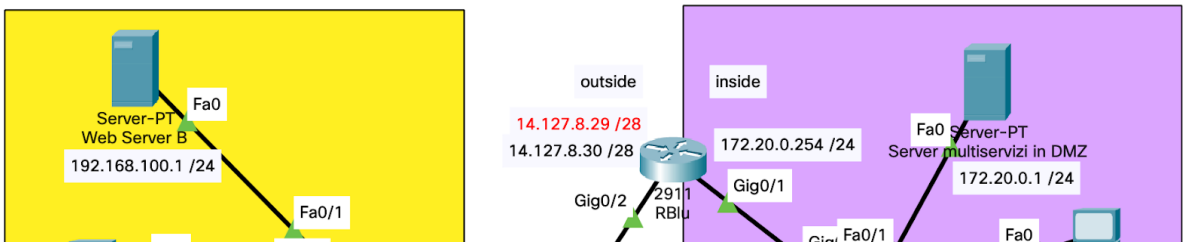
Si omette per semplicità la configurazione degli indirizzi IP statici sui vari dispositivi e l'accensione delle porte sui routers. Si ricorda che /28 rappresenta la maschera 255.255.255.240 e rappresenta reti con 14 indirizzi IP utilizzabili (più altri 2 per *netID* e *broadcast*).
Si aggiungono per comodità i *default gateway* ai due routers per permettere alcuni test di funzionamento. Quando verranno configurati completamente i NAT, non saranno più necessari.

RBlu(config)#**ip route 0.0.0.0 0.0.0.0 14.127.8.17**
RVerde(config)#**ip route 0.0.0.0 0.0.0.0 14.127.8.30**

Risulta ovvio che le macchine di una LAN non possono raggiungere le macchine dell'altra. Questo perchè nel caso reale gli indirizzi privati non sono ammessi sulla rete pubblica, ma anche perchè in ogni caso i due routers nascondono le reti private all'esterno (non si vogliono utilizzare tecniche di routing statico o dinamico).

1. Server Multiservizi in DMZ - *Static Translation 1-to-1*

L'ipotesi è che il *Server Multiservizi* esponga appunto molteplici servizi che devono essere raggiunti dall'esterno della rete locale con un indirizzo IP pubblico differente da quello configurato sull'interfaccia Gigabit 0/2 del router RBlu. La traduzione da indirizzo pubblico a privato deve essere fatta *1-a-1*.



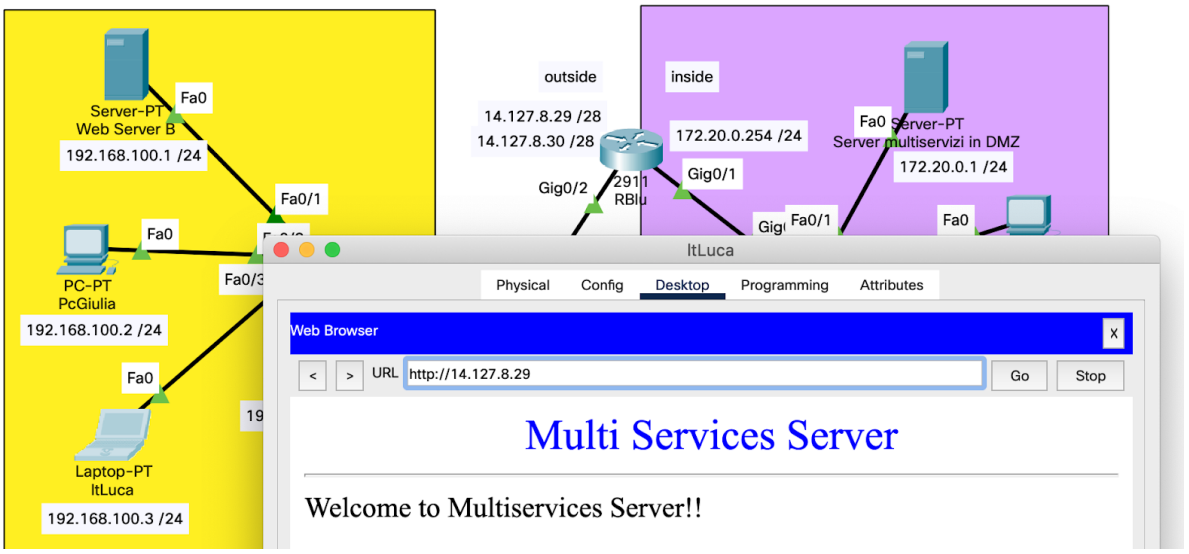
Si inizia sul router RBlu indicando quali interfacce sono interne alla rete locale e quali sono esterne. La Gigabit 0/1 è interna, mentre la Gigabit 0/2 è esterna.

RBlu(config)#**interface gigabitEthernet 0/1**
RBlu(config-if)#**ip nat inside**
RBlu(config-if)#**exit**
RBlu(config)#**interface gigabitEthernet 0/2**
RBlu(config-if)#**ip nat outside**
RBlu(config-if)#**exit**

Si procede quindi con la configurazione statica della traduzione da indirizzo pubblico a privato.
RBlu(config)#**ip nat inside source static 172.20.0.1 14.127.8.29**

Facendo un test di funzionamento dal router RVerde si nota che il nuovo indirizzo IP è raggiungibile:
RVerde#**ping 14.127.8.29**
[...] Sending 5, 100-byte ICMP Echos to 14.127.8.29, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Avendo aggiunto il *default gateway* sui due routers è possibile testare il funzionamento di uno dei servizi esposti dal server multiservizi (ad esempio il web server) da un PC dell'altra LAN (laptop Luca).



2. WEB Server - Port Address Translation 1-to-1 Port *X*

Si desidera rendere accessibile il solo servizio di Server Web (basato su TCP) sulla porta **80** direttamente con l'indirizzo IP pubblico del router. Tutto il traffico diverso deve essere bloccato.
Si inizia sul router RBlu indicando quali interfacce sono *interne* alla rete locale e quali sono *esterne*. La Gigabit 0/1 è interna, mentre la Gigabit 0/2 è esterna.

RBlu(config)#**interface gigabitEthernet 0/1**
RBlu(config-if)#**ip nat inside**
RBlu(config-if)#**exit**
RBlu(config)#**interface gigabitEthernet 0/2**
RBlu(config-if)#**ip nat outside**
RBlu(config-if)#**exit**

Si procede quindi con la configurazione statica della traduzione da indirizzo pubblico a privato per il solo protocollo TCP sulla porta **80**.

RBlu(config)#**ip nat inside source static tcp 172.20.0.4 80 14.127.8.30 80**

Il comando quindi è molto simile al caso precedente.
E' possibile testare il funzionamento del WEB Server da un PC dell'altra LAN (laptop Luca).

NB
Se invece si prova ad utilizzare il protocollo *HTTPS* che opera sulla porta *443*, il servizio non sarà raggiungibile anche se abilitato e attivo.

3. NAT standard - **Metodo che utilizza un solo IP pubblico per tutti gli host della LAN**

Si desidera permettere a tutti gli host della LAN A di uscire dalla rete locale e poter navigare all'esterno facendo in modo che il router RBlu si faccia carico delle loro richieste.

Si inizia sul router RBlu indicando quali interfacce sono *interne* alla rete locale e quali sono *esterne*. La Gigabit 0/1 è interna, mentre la Gigabit 0/2 è esterna.

RBlu(config)#**interface gigabitEthernet 0/1**
RBlu(config-if)#**ip nat inside**
RBlu(config-if)#**exit**
RBlu(config)#**interface gigabitEthernet 0/2**
RBlu(config-if)#**ip nat outside**
RBlu(config-if)#**exit**

Si procede quindi con un utilizzo molto semplice delle **ACL** - *Access Control List* per permettere che il traffico dell'intera rete privata 172.20.0.0 /24 (LAN A) possa transitare sul router.
Si configura una *ACL standard* con numerazione a piacere (in questo caso), ad esempio 55. Ricordare che le ACL vengono considerate in ordine crescente. Avendone solo una, il valore può essere scelto casualmente tra 1 e 99 (*ACL standard*). Successivamente si imposta la regola del NAT che utilizza tale ACL in **overload**. Grazie al *sovraccarico* il router può sfruttare le porte di livello 4 per mappare le richieste dei vari host privati e inoltrarle fuori dalla rete privata tramite il proprio indirizzo IP pubblico.

RBlu(config)#**access-list 55 permit 172.20.0.0 0.0.0.255** ← *Uso di Wild Card: subnetmask invertita*
RBlu(config)#**ip nat inside source list 55 interface gigabitEthernet 0/2 overload**

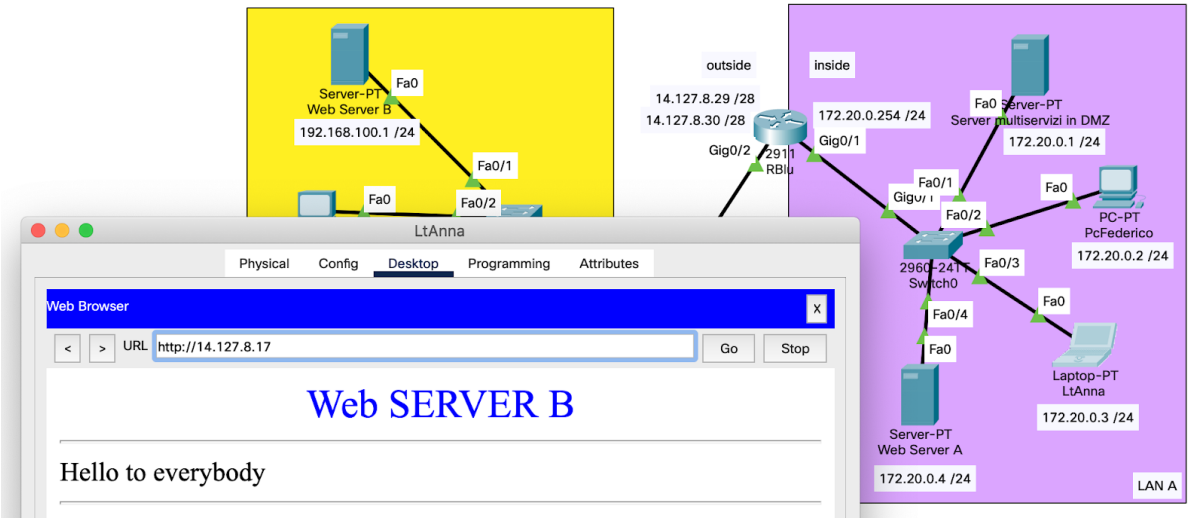
Al fine di testare il funzionamento, si configura il router RVerde per esporre il Web Server B all'esterno della LAN B.

RVerde(config)#**interface gigabitEthernet 0/1**
RVerde(config-if)#**ip nat inside**
RVerde(config-if)#**exit**
RVerde(config)#**interface gigabitEthernet 0/2**
RVerde(config-if)#**ip nat outside**
RVerde(config-if)#**exit**

Si procede quindi con la configurazione statica della traduzione da indirizzo pubblico a privato per il solo protocollo TCP sulla porta **80**.

RVerde(config)#**ip nat inside source static tcp 192.168.100.1 80 14.127.8.17 80**

Come mostrato, il Web Server della LAN B è raggiungibile usando l'indirizzo IP pubblico del RVerde (14.127.8.17) attraverso il browser di un host della rete LAN A.



Con il comando show è possibile vedere tutte le traduzioni di indirizzi tramite NAT.

RBlu#**show ip nat translations**

Protocol	Inside global	Inside local	Outside local	Outside global
---	14.127.8.29	172.20.0.1	---	---
tcp	14.127.8.30:1025	172.20.0.3:1025	14.127.8.17:80	14.127.8.17:80
tcp	14.127.8.30:80	172.20.0.4:80	---	---

4. NAT pool - Metodo che utilizza i vari IP pubblici per gli host della LAN

Per la configurazione di questo tipo di NAT ci si concentra sulla LAN B e si opera quindi sul router RVerde. Ancora una volta si indicano le interfacce interne e quelle esterne.

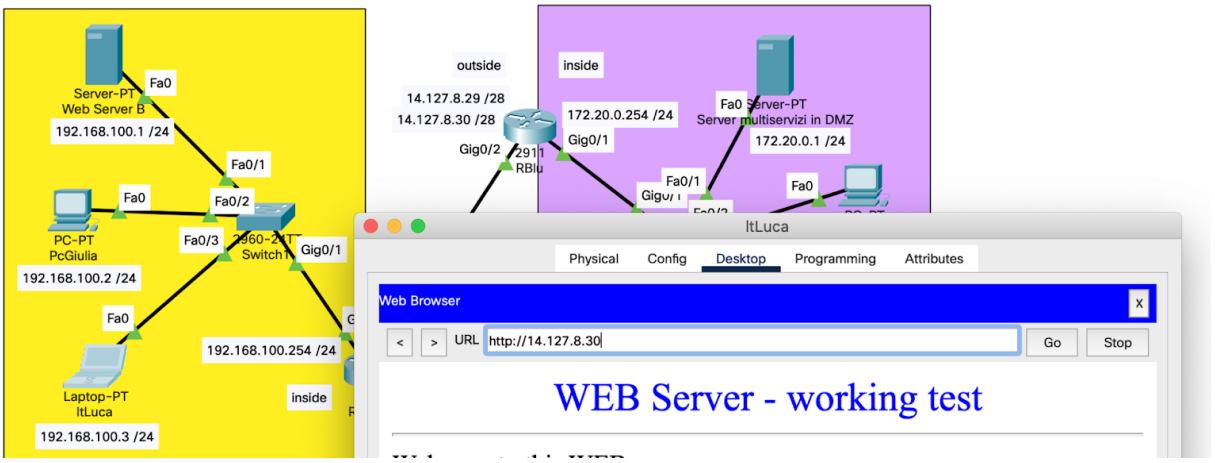
RVerde(config)#**interface gigabitEthernet 0/1**
RVerde(config-if)#**ip nat inside**
RVerde(config-if)#**exit**
RVerde(config)#**interface gigabitEthernet 0/2**
RVerde(config-if)#**ip nat outside**
RVerde(config-if)#**exit**

Si procede quindi con un utilizzo molto semplice delle **ACL** - *Access Control List* per permettere che il traffico dell'intera rete privata 192.168.100.0 /24 (LAN A) possa transitare sul router.
Si configura una *ACL standard* con numerazione a piacere (in questo caso), ad esempio 22. Ricordare che le ACL vengono considerate in ordine crescente. Avendone solo una, il valore può essere scelto casualmente tra 1 e 99. Successivamente si imposta la regola del NAT che utilizza tale ACL in

overload. Grazie al *sovraccarico* il router può sfruttare le porte di livello 4 per mappare le richieste dei vari host privati e inoltrarle fuori dalla rete privata tramite il proprio **pool** di indirizzi IP pubblici.

RVerde(config)#**access-list 22 permit 192.168.100.0 0.0.0.255** ← *Wild Card: subnetmask invertita*
RVerde(config)#**ip nat pool MyPool 14.127.8.17 14.127.8.22 netmask 255.255.255.240**
RVerde(config)#**ip nat inside source list 22 pool MyPool overload**

Come mostrato, tale configurazione permette di raggiungere il WebServer della LAN A all'indirizzo 14.127.8.30 da un host della LAN B.



Con il comando *show ip nat translations* sul router RVerde è possibile vedere le traduzioni applicate.

RVerde#**show ip nat translations**

Protocol	Inside global	Inside local	Outside local	Outside global
tcp	14.127.8.17:80	192.168.100.1:80	---	---
tcp	14.127.8.18:1025	192.168.100.3:1025	14.127.8.30:80	14.127.8.30:80