**Esercitazione SeR #2**

**“Impostazione servizi con NAT dinamico”**

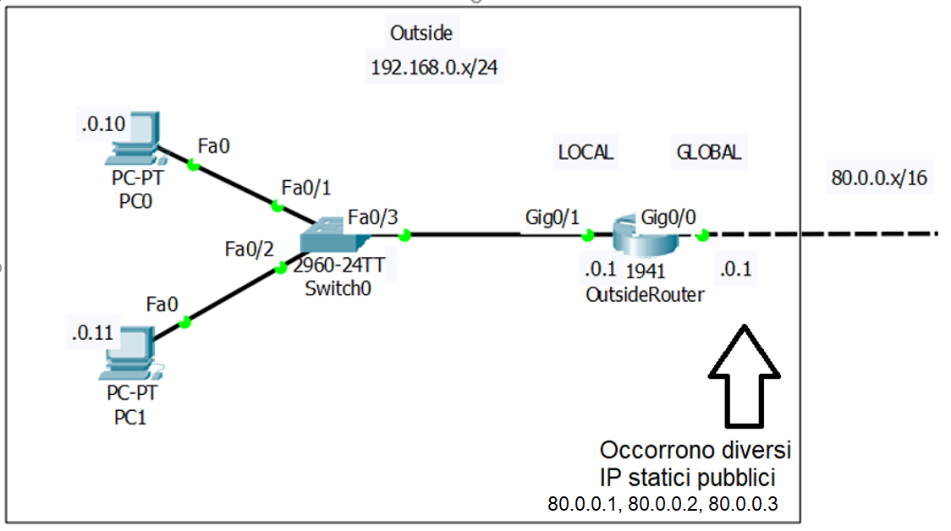
classe 5G – a.s. 2017/2018

**Premessa:** nell’esercitazione precedente i server della rete INSIDE avevano solo un indirizzo IP pubblico (80.0.0.20) a disposizione per “esporre” i propri servizi. Visto che un indirizzo IP può essere associato univocamente ad un solo server/PC, ne consegue che per consentire la contemporanea fruibilità di tutti i servizi/server dall’esterno, impedendo l’utilizzo degli IP privati/locali, avremmo bisogno di diversi IP pubblici statici (teoricamente uno per ciascun server).

In questo esercizio ribaltiamo la problematica sulla rete OUTSIDE, considerando i vari PC che vogliono navigare sui siti del ServerWeb, rimanendo visibili sulla rete pubblica solamente attraverso IP pubblici.

Gli indirizzi IP pubblici assegnabili alla rete OUTSIDE tuttavia:

1. sono limitati (in quanto IPv4) e non sempre sono ottenibili dal provider di accesso alla rete pubblica (Internet)
2. se fossero ottenibili comunque, inciderebbero considerevolmente in termini di costo sulla soluzione finale
3. nel caso di una LAN con centinaia/migliaia di calcolatori, sarebbe una soluzione impraticabile (ben difficilmente il provider ci assegnerà mille indirizzi IPv.4 statici)
4. sarebbe comunque uno spreco di soldi/risorse in quanto la situazione di accesso alla rete pubblica spesso non è permanente (es. i vari PC non navigano in Internet contemporaneamente e costantemente 24/24 ore).

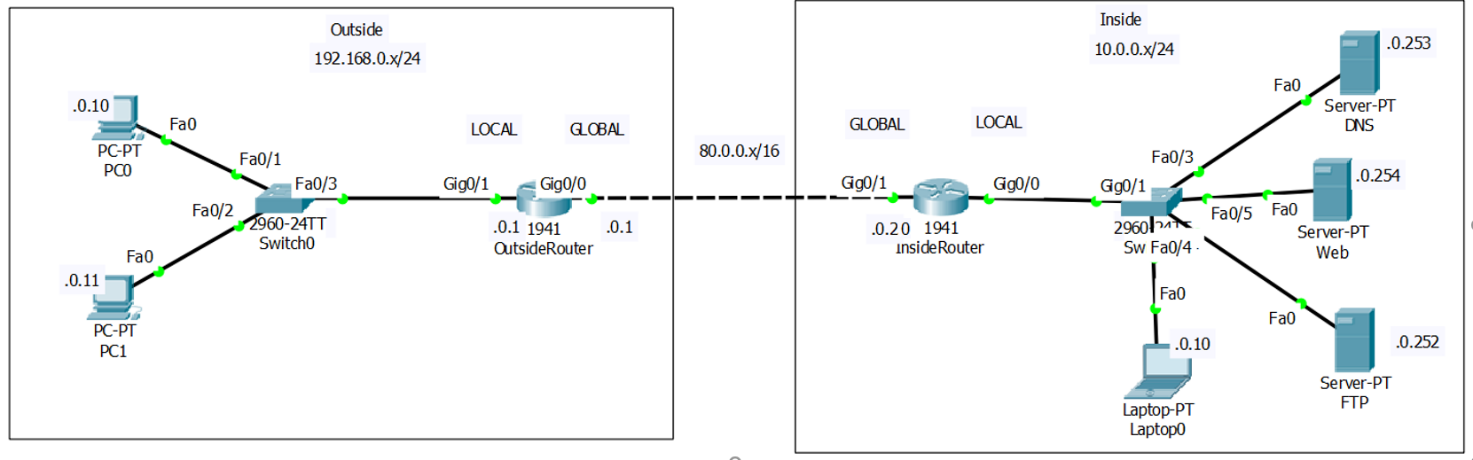
****

**Obiettivo generale**: fare in modo che i PC della rete OUTSIDE possano navigare sfruttando le risorse del ServerWeb della rete INSIDE, utilizzando un pool (insieme) costituito da più IP “pubblici” (in numero comunque inferiore al numero di PC della rete OUTSIDE). Gli indirizzi IP pubblici disponibili verranno “utilizzati dinamicamente” ai pacchetti dei PC secondo le loro esigenze di accesso alla rete pubblica.

**Scopo**: incrementare il livello di **sicurezza** dei client web, ridurre i costi connessi al loro accesso alla rete pubblica.

**Occorre**

* realizzare la topologia di rete schematizzata in figura.
* verificarne la connettività ed il funzionamento dei singoli servizi rendendoli fruibili anche dalla rete remota attraverso il **pool di indirizzi IP** ( 80.0.0.1, 80.0.0.2, 80.0.0.3 )



**Svolgimento**

* Per applicare il **NATTING dinamico** e “pubblicare” i server interessati all’utenza esterna (ovvero renderli visibili attraverso più indirizzi IP pubblici disponibili) occorre, con riferimento al ROUTER della rete OUTSIDE (**OutsideRouter**), fare quanto segue:

1. definire l’interfaccia interna (INSIDE) ed esterna (OUTSIDE) del router
2. definire il pool di indirizzi IP pubblici a disposizione
3. stabilire quali PC potranno accedere agli IP pubblici, definendo una “lista di accesso” (Access Control List o ACL)
4. Associare il pool alla lista di accesso

Definire l’interfaccia interna di Natting (IP NAT INSIDE)

OutsideRouter(config)#**interface** gi0/1

OutsideRouter(config-if)#**ip nat inside**

Definire l’interfaccia esterna di Natting (IP NAT OUTSIDE)

OutsideRouter(config)#**interface** gi0/0

OutsideRouter(config-if)#**ip nat outside**

Definire il pool di indirizzi IP pubblici ( 80.0.0.1, 80.0.0.2, 80.0.0.3 )

OutsideRouter(config)#**ip nat pool pubip\_pool 80.0.0.1 80.0.0.3 netmask 255.255.0.0**

**Nota2**: **pubip\_pool** è il nome arbitrario del pool

**Nota2**: tutti gli IP compresi tra il primo valore (80.0.0.1) e l’ultimo (80.0.0.3) sono compresi nel pool

Definire la lista (ACL) dei Server/PC che potranno accedere agli IP pubblici

OutsideRouter(config)#**access-list 10 permit 192.168.0.0 0.0.0.255**

**Nota1**: il valore 10 è un valore numerico identificativo dell’ACL

**Nota2**: si osservi che per specificare “tutti i calcolatori” della rete 192.168.0.0/24 si usa l’indirizzo di rete

**Nota3**: si osservi che la **SUBNET MASK** è sostituita dalla **WILD CARD MASK** che ha una notazione complementare alla precedente

Associare il pool all’ACL

OutsideRouter(config)#**ip nat inside source list 10 pool pubip\_pool**

Per visualizzare lo stato della NAT TABLE sul router, impostare il seguente comando

OutsideRouter#**show ip nat translations**

Pro Inside global Inside local Outside local Outside global

Notare che appena impostato il NAT la **NAT table risulta vuota**.

Esempio di contenuto della NAT TABLE dopo un certo periodo di attività svolta sulla rete

