**Esercitazione SeR #3**

**“Impostazione servizi con PAT/NAT overload”**

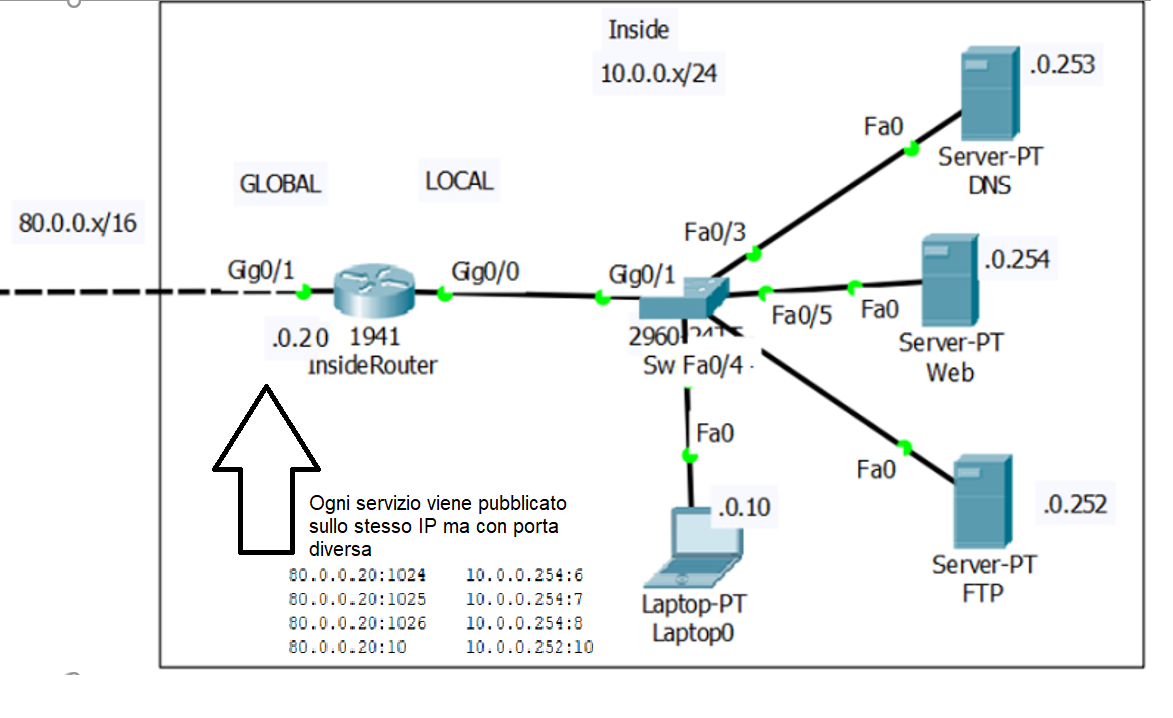
classe 5G – a.s. 2017/2018

**Premessa:** nell’esercitazione #1 l’esigenza è stata quella di “far vedere”, all’esterno di una rete locale, l’indirizzo IP locale di un solo server, per mezzo di un indirizzo IP pubblico. Abbiamo visto che questo è fattibile configurando il **NAT statico** sul router d’ “interfaccia” tra “rete locale-rete pubblica” e realizzando una mappatura (traduzione) uno-uno tra indirizzo IP pubblico ed indirizzo IP privato.

Questa tecnica tuttavia non è applicabile nel caso di **più server** che vogliono “esporre” pubblicamente i propri servizi in quanto l’unico indirizzo IP pubblico è già in uso.

Un metodo per superare questo inconveniente è stato analizzato nell’esercitazione #2: nel caso in cui ci vengano **assegnati più IP pubblici**, si può configurare il router “interfaccia” nella modalità di **NAT Dinamico**.

Quando però non è possibile avere a disposizione più IP pubblici (ma uno solo) la soluzione per affrontare il problema è quella di assegnare sullo stesso indirizzo IP pubblico, ma su porte diverse, i vari servizi da esporre su rete pubblica. In questo caso si parla di **Port Address Translation (PAT)** o **NAT con OVERLOAD**, in quanto **un unico IP pubblico viene “sovraccaricato” di più possibili connessioni interne, ciascuna associata univocamente ad una porta diversa**.

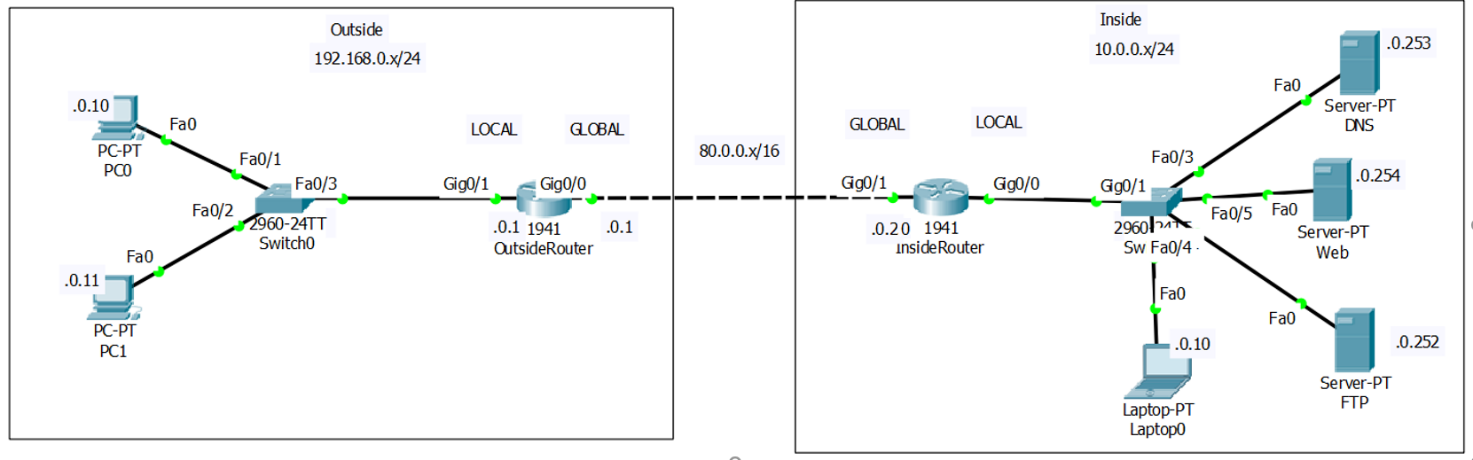


**Obiettivo generale**: fare in modo che **tutti i servizi/server** della rete INSIDE siano raggiungibili dalla seconda rete OUTSIDE utilizzando l’unico indirizzo IP “pubblico” dell’ INSIDE (80.0.0.20) in modo da non consentire ad utenze esterne alla rete INSIDE di interagire con indirizzi IP locali.

**Scopo**: incrementare il livello di **sicurezza** di accesso a tutti i server, offrire una soluzione più economica in termini di IP pubblici richiesti e quindi di costo, rispetto al NAT Dinamico

**Occorre**

* Realizzare la topologia di rete schematizzata in figura.
* Verificarne la connettività ed il funzionamento dei singoli servizi rendendoli fruibili anche dalla rete remota



**Svolgimento**

* Per applicare il NAT/PAT interno ed esterno e “pubblicare” i server interessati all’utenza esterna (ovvero renderli visibili attraverso un unico indirizzo IP pubblico, occorre, nell’ambito della rete INSIDE configurare **InsideRouter** come segue.

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

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

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

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

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

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

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

OutsideRouter(config)#**access-list 10 permit 10.0.0.0 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 10.0.0.0/24 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 ed abilitare il PAT/NAT con overload

OutsideRouter(config)#**ip nat inside source list 10 interface Gi0/1 overload**

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

**Nota2**: Gi0/1 è la denominazione dell’interfaccia pubblica del router InsideRouter valida solo per questo esempio

**Nota3**: il termine **overload** abilita il PAT

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

