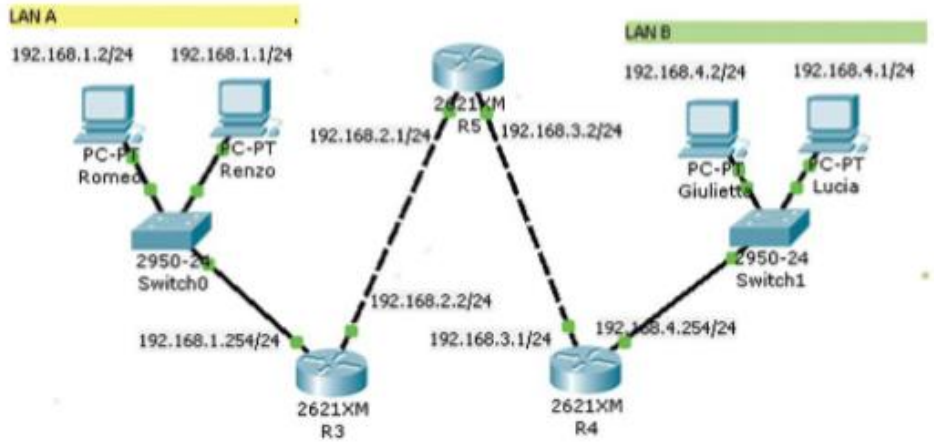
Esercizio sulla VPN

2 ESERCIZI IN LABORATORIO

REALIZZIAMO UNA VPN CON PACKET TRACER

Per poter definire una VPN è necessario avere a disposizione una rete sulla quale operare: realizziamo quella riportata nella figura seguente.



Per la LAN A connettiamo due PC a uno switch, con la seguente Addressing Table:

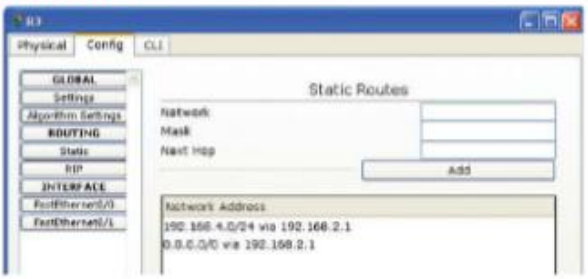
DEVICE	IP ADDRESS	SUBNET MASK	DEFAULT GATEWAY
Romeo	192.168.1.2	255.255.255.0	192.168.1.254
Renzo	192.168.1.1	255.255.255.0	192.168.1.254

Per la LAN B connettiamo due PC a uno switch, con la seguente Addressing Table:

DEVICE	IP ADDRESS	SUBNET MASK	DEFAULT GATEWAY
Giulietta	192.168.4.2	255.255.255.0	192.168.4.254
Lucia	192.168.4.1	255.255.255.0	192.168.4.254

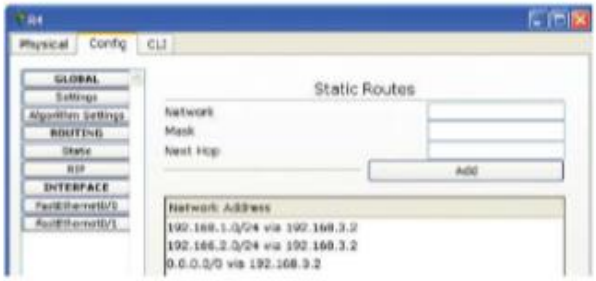
La configurazione dei router non richiede particolari accorgimenti: riportiamo per comodità solo le tabelle statiche.

Router R3

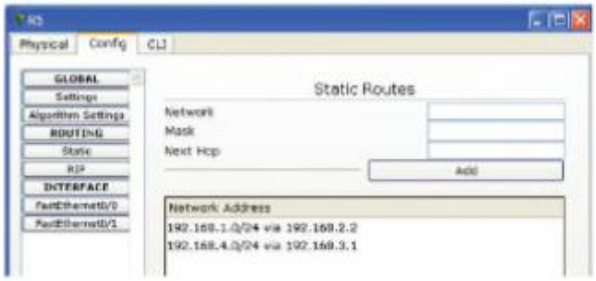


ESERCIZI IN LABORATORIO 2

Router R4



Router R5



VPN – crittografia

Dopo avere collaudato il funzionamento della rete verificando che i pacchetti della rete LAN A giungano alla LAN B, procediamo con la creazione di un tunnel tramite il quale i pacchetti scambiati tra il router R3 e il router R4 vengano cifrati, così da garantire l'integrità e la riservatezza delle comunicazioni per fare in modo che il router R5 non venga a conoscenza del loro contenuto.

Comandi per il router R4

Analizziamo il comando da inserire nel router in due parti: nella prima fase introduciamo le impostazioni per effettuare lo scambio delle chiavi e utilizzare il protocollo **ISAKMP** per identificare l'algoritmo di hashing e il metodo di autenticazione.

ISAKMP
The Internet Security Association and Key Management Protocol (ISAKMP) defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA).

È anche necessario indicare "la terminazione" del tunnel, che nel nostro caso è sul router R4 di indirizzo 192.168.3.1.

```
crypto isakmp policy 10
hash md5
authentication pre-share // utilizza la chiave di cifratura definita in seguito
crypto isakmp key P5NM address 192.168.3.1    //chiave di cifratura
isakmp ccm
```

2 ESERCIZI IN LABORATORIO

Procediamo creando `IPsec` definendo la trasformazione che chiamiamo `SEGRETO` con l'indicazione del protocollo di crittografia che deve essere diverso da quello utilizzato da IKE.

```
crypto ipsec transform-set SEGRETO esp-3des esp-md5-hmac
mode transport
crypto ipsec df-bit clear
```

Possiamo anche definire un gruppo e richiedere le credenziali per l'utilizzo della VPN.

```
crypto isakmp client configuration group AMICI
key AMICI
```

Impostiamo infine la crittomappa che verrà utilizza nel sistema.

```
crypto map MIAMAPPA 10 ipsec-isakmp     // definizione di una crittomappa
set peer 192.168.3.1                    // estremo del tunnel
set transform-set SEGRETO               // abilitiamo la trasformazione
match address 101                       // origine-destinazione dei pacchetti
crypto map MIAMAPPA                     // attiva la crittomappa
```

Comandi per il router R3

I comandi per il router R3 sono identici a quelli sopra descritti per il router R4: cambia solamente l'indirizzo di fine tunnel, che è 192.168.2.2.

METTITI ALLA PROVA

- Programmare i router Cisco in CLI
- Applicare una VPN

Inserisci nei router i comandi sopra descritti e verifica il funzionamento, analizzando i pacchetti che attraversano il router R5.