Riepilogo VLAN, RIP2, OSPF1, WEB SERVER, DHCP, ACL, NAT e PAT

1 ISTRUZIONI BASE

1. `enable` → si entra in modalità privilegiata (serve sempre tranne per i comandi `show`, si capisce perché se si è in questa modalità vediamo "#").
2. `config t` → si fa dopo `enable` per modificare impostazioni (si capisce perché si vede "(config)").
3. `show running-config` → si vedono le config del dispositivo (si fa fuori dalla modalità privilegiata, con `space` si vede ciò che non c'è scritto nella pagina).
4. `write m` → per salvare le config (va fatto prima di consegnare su tutti i dispositivi router e switch, deve essere fatto in modalità privilegiata ma non in `config`).

2 Configurazione delle VLAN

2.1 Configurazione di VLAN su switch

1. `Config` → `VLAN database` → scrivere nome e numero di VLAN e aggiungerla
2. per ogni interfaccia di ogni dispositivo indicare in che VLAN appartiene (deve essere di tipo access)
3. per l'interfaccia che va verso il router basta cambiare la modalità in "trunk"

2.2 Configurazione di VLAN su router

attivare cavo del router.
poi nella CLI:

```
Router(config)# interface fastEthernet 0/0.10
Router(config-if)# encapsulation dot1Q 10
Router(config-if)# ip addres ip_gateway netmask (della
    VLAN)
Router(config-if)# no shutdown
Router(config-if)# exit  (ripetere per ogni VLAN)
```

Spiegazione:

- `interface fastEthernet 0/0.10` → accesso all'interfaccia della VLAN 10.
- `encapsulation dot1Q 10` → spiega di incapsulare con dot1Q i messaggi da quella VLAN.

- `ip addres ip_gateway netmask` → indica che ip di gateway ha la VLAN
- `no shutdown` → indica di attivare l'interfaccia in modalità UP

3 RIP Version 2 (RIP v2)

si fa per ogni router, bisogna aggiungere ogni collegamento che ha il router (network..)

3.1 Configurazione base RIP v2

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.10.0 (ip_base
   della rete adiacente)
Router(config-router)# network 192.168.20.0 (ip_base
   della rete adiacente)
Router(config-router)# passive-interface fastEthernet
   0/0.10 (da fare solo per ogni VLAN per evitare il
   traffico di dati inutile)
```

Spiegazione:

- `router rip` → abilita il protocollo RIP sul router.
- `version 2` → usa RIP versione 2 (supporta subnet mask variabili).
- `network X.X.X.X` → indica le reti direttamente collegate che il router deve annunciare agli altri router.
- `passive-interface fastEthernet 0/0.10` → indica che i pacchetti per spiegare ai router i propri vicini non vengono inoltrati alle vlan poiche non gli servono

4 OSPF (Open Shortest Path First)

4.1 Configurazione base OSPF

```
Router(config)# router ospf 1
Router(config)# area 1 stub
Router(config-router)# network 192.168.10.0 0.0.0.255
   area 1 (ip_base della rete adiacente e wild-mask)
Router(config-router)# network 192.168.20.0 0.0.0.255
   area 1 (ip_base della rete adiacente e wild-mask)
Router(config-router)# passive-interface fastEthernet
   0/0.10 (da fare solo per ogni VLAN per evitare il
   traffico di dati inutile)
```

Spiegazione:

- `router ospf 1` → abilita OSPF con ID processo 1.
- `area 1 stub` → crea o entra nell'area 1
- `network <IP> <wildcard> area <area>` → definisce quali reti annunciare in quale area OSPF. - La **wildcard mask** è l'inverso della subnet mask: per /24: 255.255.255.0 → wildcard 0.0.0.255, area 1 indica a quale area aggiungere la rete
- `passive-interface fastEthernet 0/0.10` → indica che i pacchetti per spiegare ai router i propri vicini non vengono inoltrati alle vlan poiche non gli servono

5 Configurazione di un Web Server

Un **server web** è un host configurato per offrire il servizio HTTP/HTTPS. In Packet Tracer si può configurare facilmente:

1. Aggiungere un dispositivo di tipo **Server**.
2. Entrare in **Services** → **HTTP** e abilitare http/https.
3. settare gateway
4. settare ip
5. settare netmask

A questo punto qualsiasi PC della stessa LAN, aprendo il browser e digitando `http://192.168.10.100`, visualizzerà la pagina di default del server.

Per renderlo accessibile dall'esterno (rete pubblica), bisogna configurare il NAT statico sul router.
nella CLI:

```
! Mappatura porta HTTP dal pubblico al server interno
ip nat inside source static tcp 192.168.10.100 80
   203.0.113.50 80

! Configurazione interfacce
interface fastEthernet 0/0
ip address 192.168.10.1 255.255.255.0 (ip del ateway
   del server)
ip nat inside

interface fastEthernet 0/1
ip address 203.0.113.50 255.255.255.0 (ip pubblico, ip
    assegnato all'interfaccia collegata verso l'
   esterrno della rete del router)
ip nat outside
```

Così chi accede a `http://203.0.113.50` dall'esterno, raggiungerà il web server interno.

6 Configurazione di un DHCP Server

Il servizio **DHCP** permette di assegnare automaticamente indirizzi IP ai client della rete. In Packet Tracer, un DHCP server si configura così:

1. Aggiungere un dispositivo di tipo **Server**.
2. Entrare in **Services** → **DHCP** e abilitare il servizio DHCP.
3. settare default gateway: gateway della VLAN dove assegnare gli indirizzi
4. start ip addres: primo ip VLAN destinazione
5. subnet mask: subnet mask VLAN destinazione
6. maximum: wldcard -2
7. salvare
8. sui pc a cui il server deve assegnare gli ip impostare ip in dhcp mode (**Config** → **DHCP**)

Ora bisogna configurare il router in modo che permetta al server di assegnare gli ip.
nella CLI:

```
interface fastEthernet 0/0.10 (interfaccia collegata
   allo switch, indicando la VLAN di destinazione)
ip helper-addres ip_del_server
```

7 Access Control List (ACL)

7.1 Definizione

Una **ACL (Access Control List)** è una lista di regole che un router o uno switch Layer 3 utilizza per controllare il traffico che passa attraverso le interfacce, decidendo cosa è permesso e cosa è bloccato.
ATTENZIONE: sono regole controllate dal router una dopo l'altra, se una regola non viene soddisfatta quelle dopo non vengono manco controllate, per questo generalmente l'ultima è quella di permettere tutto dato che si definisce prima chi non può (o viceversa)

7.2 Tipi di ACL

- **Standard:** filtrano solo in base all'indirizzo IP sorgente. nome comreso tra 1-99
- **Estese:** filtrano in base a sorgente, destinazione, protocollo e porta. nome comreso tra 100-199

7.3 Applicazione

Le ACL si applicano alle interfacce di un router con i comandi:

```
Router(config-if)# ip access-group <numero/nome> in|
   out
```

in indica che le regole sono controllate per il flusso in entrata a quella interfaccia, out che sono controllate per il flusso in uscita.

7.4 Esempio ACL standard per bloccare una VLAN verso un server

componenti:

1. VLAN_1: ip_base: 192.168.10.0 netmask: 0.0.0.255
2. VLAN_2: ip_base: 192.168.20.0 netmask: 0.0.0.255
3. SERVER: ip: 172.16.0.100

cosa fa:

1. nego alla VLAN_1 di accedere al server
2. nego a tutti di accedere al server
3. permetto a tutti di accedere a tutti
4. assegno la ACL al router del server sul cavo in entrata

```
access-list 10 deny 192.168.10.0 0.0.0.255
access-list 10 permit any
interface fastEthernet 0/1
ip access-group 10 out
```

7.5 Esempio ACL estesa per filtrare solo il traffico verso un server specifico

componenti:

1. VLAN_1: ip_base: 192.168.10.0 netmask: 0.0.0.255
2. VLAN_2: ip_base: 192.168.20.0 netmask: 0.0.0.255
3. SERVER: ip: 172.16.0.100

cosa fa:

1. permetto alla VLAN_1 di accedere al server
2. nego a tutti di accedere al server
3. permetto a tutti di accedere a tutti
4. assegno la ACL al router del server sul cavo in entrata

```
access-list 110 permit ip 192.168.10.0 0.0.0.255 host
   172.16.0.100
access-list 110 deny ip any host 172.16.0.100
access-list 110 permit ip any any
interface fastEthernet 0/0
ip access-group 110 in
```

8 NAT e PAT

8.1 NAT base

permette di tradurre tutti gli indirizzi interni con l'indirizzo pubblico del router e viceversa **componenti:**

1. fastEthernet 0/0: interfaccia che collega la rete interna/VLAN al router
2. fastEthernet 0/1: interfaccia che collega la rete esterna al router

cosa fa:

1. dico che 0/0 è la rete interna
2. dico che 0/1 è la rete esterna

```
interface fastEthernet 0/0
ip nat inside
exit
interface fastEthernet 0/1
ip nat outside
exit
```

8.2 NAT dinamico con pool di IP

se invece vogliamo che gli ip interni vengano tradotti con piu ip pubblici si usa il pool di ip che consiste nel dire con quale range di ip bisogna tradurre quelli interni **componenti:**

1. MIO_POOL: nome del pool
2. range di indirizzi pubblici: 203.0.113.10-203.0.113.20, netmask: 255.255.255.0
3. VLAN_1: ip_base: 192.168.10.0, netmask: 0.0.0.255
4. SERVER: ip: 172.16.0.100

cosa fa:

1. setto il nome del pool con il suo range di indirizzi esterni
2. dico quale è l'indirizzo base della VLAN/di un singolo host, da tradurre
3. dico di usare gli ip del pool per tradurre gli indirizzi interni

```
ip nat pool MIO_POOL 203.0.113.10 203.0.113.20 netmask
    255.255.255.0
access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 pool MIO_POOL
```

8.3 PAT dinamico (NAT overload)

si configura in modo che avendo un solo ip pubblico piu host possono uscire con lo stesso ip e non uno alla volta, poiche si usa la loro porta per essere riconosciuti **componenti:**

1. VLAN_1: ip_base: 192.168.10.0 netmask: 0.0.0.255

cosa fa:

1. faccio come per il nat normale
2. dico quale è l'indirizzo base della VLAN/di un singolo host, da tradurre
3. dico di usare l'ip dell'interfaccia 0/1 (router) per tradurre gli indirizzi, overload indica che piu host possono uscire con quell'ip e non uno alla volta
4. assegno la ACL al router del server sul cavo in entrata

```
interface fastEthernet 0/0
ip nat inside
interface fastEthernet 0/1
ip nat outside
access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface fastEthernet 0/1
    overload
```