

Relazione esercitazione 6 Laboratorio di reti

Configurazione di un router CISCO

Franco Masotti Danny Lessio

June 8, 2015

Contents

I	Consegna	2
II	Configurazione del router	3
1	Collegamento al router	3
2	Ripristino della password	3
3	Ripristino dell'immagine	3
4	Access lists	4
5	Configurazioni delle interfacce seriali	5
6	Rotte statiche	5
7	Rotte dinamiche	6
III	Listati	7
8	running-config OSPF	7

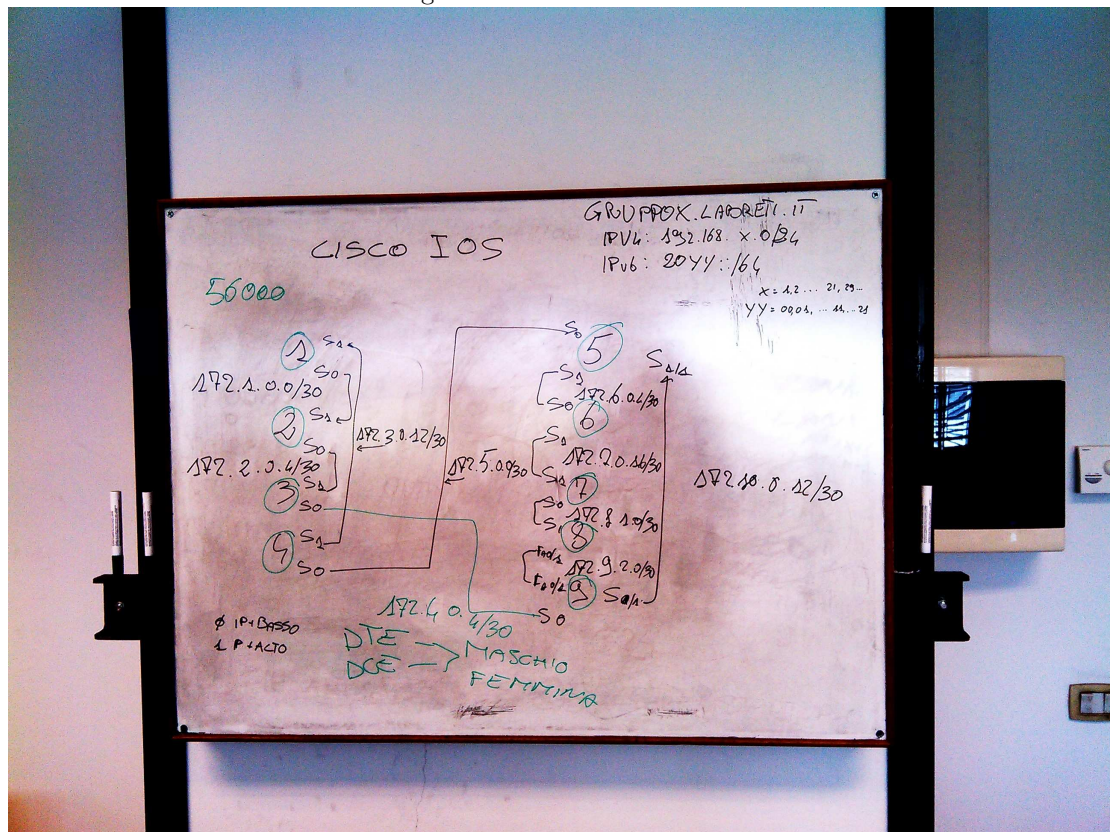
Part I

Consegna

Questa esercitazione consiste nella configurazione di un router CISCO in modo effettuare il recovery della password e dell'immagine del sistema. Inoltre abbiamo abilitato le rotte statiche e poi quelle dinamiche (con vari algoritmi di routing).

Di seguito é rappresentato lo schema dei collegamenti tra le seriali di tutti i router:

Figure 1: Connessioni seriali



⁰networks-lab Copyright (C) 2016 frnmst (Franco Masotti), dannylessio (Danny Lessio). This document comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to redistribute it under certain conditions; see LICENSE file for details.

Part II

Configurazione del router

1 Collegamento al router

Al contrario degli switch i nostri router si trovano in una postazione remota. Il collegamento in seriale non é quindi piú possibile. In questo caso ci colleghiamo ad un gateway attraverso ethernet con `telnet`:

```
telnet 192.168.0.100 7002
```

dove la porta 7002 corrisponde al router del nostro gruppo. Abbiamo inserito il nostro username e password¹.

Successivamente abbiamo configurato il router allo stesso modo dello switch (escludendo ovviamente la parte delle VLAN che qui non é presente) e abbiamo abilitato il telnet.

2 Ripristino della password

Dopo aver salvato la nostra nuova configurazione sul computer² abbiamo salvato anche l'immagine del sistema³. A questo punto abbiamo settato un valore nel registro di sistema in modo che al riavvio del router, questo ignori la configurazione precedentemente salvata in nvram (`nvram:/startup-config`):

```
enable
configure terminal
confreg 0x0
end
```

Riavviamo il router con `reload`. Abbiamo poi copiato la vecchia configurazione ed impostato la nuova password:

```
confreg 0x2142
copy startup-config running-config
configure terminal
enable password labreti
```

Infine abbiamo settato il valore del registro con quello originale:

```
confreg 0x2102
```

3 Ripristino dell'immagine

Se l'immagine del sistema operativo é corrotta, allora é possibile ripristinarla. Ricordandoci che abbiamo salvato l'immagine precedentemente (assumendo che quella non abbia problemi) per prima cosa dobbiamo cancellare l'immagine corrente:

¹labreti2

²copy running-config tftp:

³copy c2600-adventerprisek9-mz.124-16b.bin tftp:

```
enable
cd flash:/
delete c2600-adventerprisek9-mz.124-16b.bin
```

Adesso riavviamo il router con `reload`. Una volta riavviato il router, noteremo che questo é entrato in recovery mode. Per ripristinare l'immagine bisogna assegnare manualmente le informazioni per l'interfaccia ethernet⁴. Per visualizzare le variabili settate prima di lanciare il comando `tftpdnld` é possibile lanciare il comando `set`:

```
IP_ADDRESS=192.168.0.101
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=192.168.0.101
TFTP_SERVER=192.168.0.100
TFTP_FILE=c2600-adventerprisek9-mz.124-16b.bin
```

Abbiamo poi lanciato il comando `tftpdnld` e abbiamo risposto `y` a tutte le domande. Per salvare le variabili `ROMmon` in memoria non volatile `NVRAM` abbiamo lanciato il comando `sync`. Infine abbiamo cancellato la nostra configurazione per i prossimi gruppi:

```
delete nvram:/startup-config
reload
```

4 Access lists

La parte successiva dell'esercitazione consiste nell'applicazione di access list per inibire l'accesso all'interfaccia amministrativa telnet a certe reti ed host piuttosto che altri. Abbiamo provato due casi differenti.

Per applicare le access list:

```
enable
configure terminal
ip access-list extended VTY_ACCESS
```

Il primo caso consiste nel permettere l'accesso a tutti gli host della sottorete escluso il computer corrente:

```
10 permit tcp 192.168.2.0 0.0.0.255 any eq telnet
20 deny tcp host 192.168.2.1 any eq telnet
```

Il secondo caso invece permette l'accesso solo dal computer corrente mentre inibisce l'accesso da tutti gli altri host.

```
10 permit tcp host 192.168.2.1 any eq telnet
20 deny tcp 192.168.2.0 0.0.0.255 any eq telnet
```

Per testare queste configurazioni abbiamo usato i due indirizzi `192.168.2.1` e `192.168.2.2` a seconda dei casi.

⁴Avendo avuto problemi con il server tftp sul computer abbiamo usato quello interno della rete sia per salvare l'immagine sia per effettuare il ripristino.

5 Configurazioni delle interfacce seriali

Una delle parti critiche nella fase di setup di ogni router é la selezione dei cavi seriali. I device che comunicano attraverso interfaccia seriale vengono suddivisi in due categorie: DCE e DTE. I primi forniscono il segnale di clock per permettere la comunicazione all'interno del bus. Il DTE può essere visto come "maschio" mentre il DCE viene visto come "femmina".

Il router a noi affidato era provvisto di due DTE, non abbiamo dunque avuto bisogno di assegnare il clockrate ed il bandwidth.

I router sono collegati tra di loro attraverso queste interfacce seriali. Per poter effettuare il collegamento fra il nostro router e quelli adiacenti (vedi schema connessioni) é necessario assegnare due indirizzi di sottoreti rispettivamente alle due interfacce. Per convenzione la maschera della sottorete é /30, quindi abbiamo solo 4 indirizzi disponibili di cui uno usato per identificare la sottorete (172.1.0.0 ed 172.2.0.4) ed uno per il broadcast (172.1.0.3 ed 172.2.0.7). Lo scopo finale é quello di poter pingare i router adiacenti⁵. Come da schema abbiamo assegnato l'indirizzo 172.2.0.5 alla Serial0/0 e 172.1.0.1 alla Serial0/1:

```
enable
configure terminal
interface Serial0/0
ip address 172.2.0.5 255.255.255.252
no shut
exit
configure terminal
interface Serial0/1
ip address 172.1.0.1 255.255.255.252
no shut
```

A questo punto, é stato possibile pingare i router vicini (gruppo1 e gruppo3) attraverso interfaccia seriale con successo:

```
ping 172.1.0.2
ping 172.2.0.6
```

6 Rotte statiche

L'instradamento deve avvenire dal gruppo1 verso il gruppo9. Dev'essere possibile pingare tutti i 9 router della rete interna. Nella nostra situazione, seguendo lo schema, abbiamo settato la tabella di routing indirizzando i pacchetti relativi alla sottorete 192.168.1.0 al router numero 1, mentre tutti gli altri vengono gestiti dal router numero 3:

```
ip route 192.168.1.0 255.255.255.0 172.1.0.2
ip route 0.0.0.0 0.0.0.0 172.2.0.6
```

A questo punto é stato possibile raggiungere ogni altro router a partire dal nostro.

Ovviamente, agendo sulle nostre singole macchine ed impostando il nostro router (192.168.2.100) come default gateway é stato possibile raggiungere le macchine degli altri gruppi collegate ai rimanenti 8 router locali.

⁵Nel nostro caso il gruppo 1 ed il gruppo 3.

7 Rotte dinamiche

Abbiamo applicato tre algoritmi di routing sia di tipo distance vector, sia di tipo link state⁶:

- RIPv2

- É di tipo distance vector quindi impiega il numero di hop come metrica. RIP evita i routing loop adottando un limite massimo di hop dalla sorgente verso la destinazione. Il numero massimo di hop consentito é 15. Questo numero di hop limita in ogni caso il diametro della rete consentito da RIP. Un numero di hop equivalente a 16 viene considerato come metrica infinita per indicare le rotte inaccessibili che non verranno installate in tabella di routing. Questa versione "v2" include il trasporto di informazioni nella maschera di sottorete. Ecco i comandi per abilitarlo:

```
router rip
version 2
network ip-address mask
```

- OSPF

- É di tipo link state, cioè i link sono scelti in base alle condizioni della rete. OSPF non é un protocollo proprietario. Aggiunge proprietà aggiuntive rispetto ai protocolli di tipo link state quali il bilanciamento del carico, aggiunge un grado di gerarchia nei domini ed implementa l'autenticazione dei messaggi. Ecco i comandi per abilitarlo:

```
router ospf process_id
network ip_address mask area area_id
```

- EIGRP

- Il protocollo proprietario della CISCO ha gli aspetti migliori di un protocollo link state e distance vector. Ecco i comandi per abilitarlo:

```
router eigrp autonomous-system
network network-number
```

⁶Il comando network di ogni protocollo va applicato per tutte e 3 le interfacce. vedi listato OSPF.

Part III

Listati

Abbiamo inserito la sola configurazione del protocollo OSPF, le altre due configurazioni mancanti sono quasi identiche in quanto cambiano solo le informazioni relative al protocollo.

8 running-config OSPF

running-config

File di configurazione principale del router configurato per il routing OSPF. Da notare **area 12** che deve essere uguale per tutti i router.

```
!  
! running-config-ospf  
!  
! Copyright (C) 2016 frnmst (Franco Masotti) <franco.  
    masotti@student.unife.it>  
!  
!             dannylessio (Danny Lessio)  
!  
! This file is part of networks-lab.  
!  
! networks-lab is free software: you can redistribute it and/or  
    modify  
! it under the terms of the GNU General Public License as  
    published by  
! the Free Software Foundation, either version 3 of the License,  
    or  
! (at your option) any later version.  
!  
! networks-lab is distributed in the hope that it will be useful,  
! but WITHOUT ANY WARRANTY; without even the implied warranty of  
! MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the  
! GNU General Public License for more details.  
!  
! You should have received a copy of the GNU General Public  
    License  
! along with networks-lab. If not, see <http://www.gnu.org/  
    licenses/>.  
!  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname gruppo2  
!  
boot-start-marker
```



```

log-adjacency-changes
network 172.1.0.0 0.0.0.3 area 12
network 172.2.0.4 0.0.0.3 area 12
network 192.168.2.0 0.0.0.255 area 12
!
!
!
no ip http server
no ip http secure-server
!
ip access-list extended VTY_ACCESS
deny tcp host 192.168.2.1 any eq telnet
permit tcp 192.168.2.0 0.0.0.255 any eq telnet
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
access-class VTY_ACCESS in
password 7 03085A09140A3545
login
!
!
end

```