

Corso di Fondamenti di Reti e Sicurezza Informatica

Prova di laboratorio 20 Luglio 2023

Durata Prova **90 minuti**

ISTRUZIONI

Lo svolgimento della prova consiste nello sviluppo e simulazione di una rete locale (Firewalling + Routing + Configurazione).

1. **Rinomina** la cartella chiamata "Cognome-Nome-Matricola" che hai trovato sul Desktop e in cui hai trovato questa traccia, sostituendo "Cognome" "Nome" e "Matricola" con i tuoi dati personali e lasciando i trattini;
2. Configura la topologia lasciando tutti i file necessari nella cartella di cui sopra.

Istruzioni per il confezionamento dei file di configurazione:

1. I domini di collisione dovranno essere elencati all'interno del file `CDs` già presente all'interno della cartella **Cognome-Nome-Matricola**.

```
## ESEMPIO DI CD ##
CD1
  network 10.0.0.0/24
  netmask 255.255.255.0
  broadcast 10.0.0.255

CD2
  network 10.0.7.0/30
  netmask 255.255.255.252
  broadcast 10.0.7.3

CDX
...

# Accorpamento RED
RED
  network 10.0.0.0/23
  netmask 255.255.254.0
  broadcast 10.0.1.255
```

2. La risposta ai quesiti deve essere scritta all'interno del file `Quesiti` situato all'interno della directory **Cognome-Nome-Matricola**. Il formato dovrà essere uguale a quello dell'esempio sottostante:

NON SPEGNERE IL PC A FINE ESAME

```
1.
2. comando -xaz
3. altroComando -x -a -z
```

3. Le rotte dell'intero progetto potranno essere specificate all'interno di un file dal nome **rotte.sh** debitamente commentato. Per semplificare, è possibile usare la notazione *networkAreaRed/22* per indicare ad esempio, il network e la maschera di una determinata area o dominio di collisione (evitando dunque di riportare l'intero indirizzo del network del dominio) e *R1[eth0]* per indicare, ad esempio, l'indirizzo ip relativo alla scheda di rete *eth0* del router *R1*. La stessa convenzione può essere utilizzata anche nelle regole di firewalling se necessario e lo si ritiene opportuno.

Si noti che per ogni risposta è riportato il numero del quesito a cui ci si riferisce. Se non si vuole dare alcuna risposta ad una determinata domanda basta scrivere il numero del quesito e lasciare in bianco la riga.

Non è consentito l'uso di alcun altro tipo di materiale (appunti, esempi, libri, calcolatrice, dati trasferiti tramite USB).

N.B. Per il superamento della prova è necessario completare correttamente i **primi 3 punti** specificati all'interno della sezione **[REQUISITI]**.

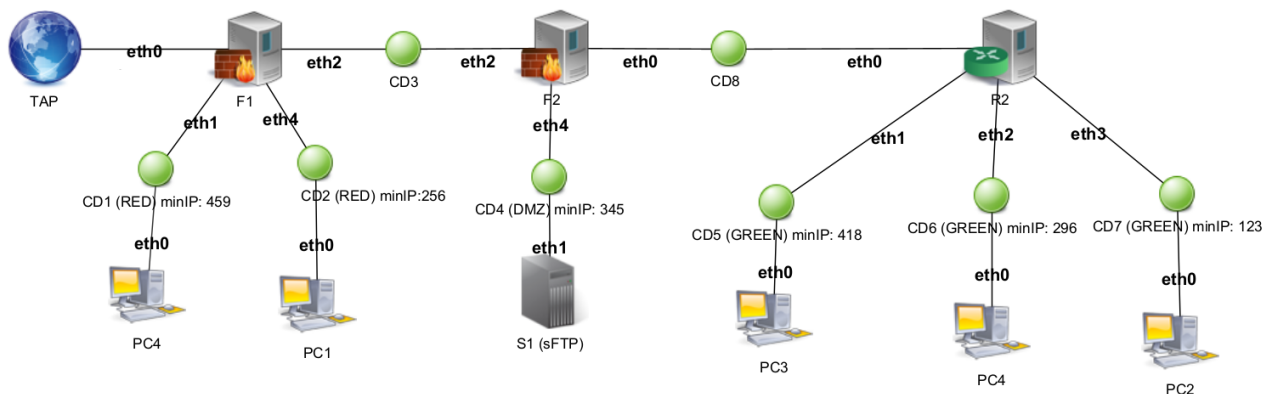
Quando finisci NON spegnere il PC.

SALVA SPESSO il tuo lavoro

NON SPEGNERE IL PC A FINE ESAME

ESERCIZIO 1 (22 punti)

Si ha a disposizione una rete di **classe A** (10.0.0.0/8). Si deve progettare/simulare una rete locale seguendo le specifiche riportate nella figura sottostante.



REQUISITI:

REQUISITI:

1. **(4pt)** È necessario accorpare i domini di collisione contigui della stessa tipologia (Green, Red o DMZ)
2. **(4pt)** È richiesto di minimizzare il più possibile lo spreco di indirizzi IP (**annotare sul foglio, per ogni dominio di collisione, gli indirizzi network, maschera e broadcast**)
3. **(3pt)** È necessario, in una prima fase, che tutta la rete sia completamente connessa e funzionante e che tutti gli host siano in grado di comunicare con tutti gli altri hosts (Es. I PC in CD1 devono poter raggiungere e pingare i PC di CD6 e viceversa)
4. **(8pt)** Successivamente applicare le seguenti regole di firewalling (**default policy DROP**):
 - a. **(1pt)** L'area GREEN può aprire comunicazioni verso tutti; l'area RED può aprire nuove comunicazioni verso INTERNET e DMZ; l'area DMZ può ricevere nuove comunicazioni da tutti
 - a. **(2pt)** Si abiliti l'uso di `icmp` tra l'area GREEN e l'area RED. L'area GREEN potrà effettuare nuove richieste ping (echo-request) mentre l'area RED potrà solo rispondere alle richieste pervenute (echo-reply).
 - b. **(2pt)** Il firewall F2 mette a disposizione un servizio postfix/mail sulla porta 2525. Tale servizio deve essere accessibile da INTERNET, e quindi dall'esterno della rete locale. Si scrivano le opportune regole di firewall a tal fine.

c. **(3pt)** Natting:

- i. Si crei una regola che effettui il port forwarding dei seguenti pacchetti:
 - 1. Se il pacchetto arriva in input sulla scheda di rete *eth0* di **F1** e la sua porta destinazione è la **1234**, il pacchetto dovrà essere rediretto in **S1** sulla nuova porta **25**.
 - 2. Se il pacchetto arriva in input sulla scheda di rete *eth0* di **F1** e la sua porta destinazione è la **4567**, il pacchetto dovrà essere rediretto in **S1** sulla nuova porta **7654**.
- i. Si scriva una regola per mascherare l'indirizzo ip sorgente di tutte le connessioni provenienti dall'interno della rete e dirette verso internet con uno dei seguenti indirizzi ip: 10.1.2.3, 10.1.2.4 o 10.1.2.5

N.B.: La regola è da inserire nel firewall F1 e sarà F1 stesso a decidere con quale dei 2 possibili indirizzi ip mascherare la connessione.

- 5. **(1pt)** Modificare il file host di F1 affinché sia possibile contattare il pc R1 tramite il suo hostname (ovvero, eseguendo il comando: `ping R1`)
- 6. **(1pt)** Scrivere i comandi usati (*lato client e server*) per misurare le prestazioni di rete tra 2 hosts
- 7. **(1pt)** Scrivere il comando usato per visualizzare in tempo reale il contatore dei pacchetti accettati/droppati dal firewall F1.

ESERCIZIO 2 (8 pt)

Si scriva, in linguaggio Python o Perl, uno script che esegua periodicamente (con frequenza 30 minuti) il comando “arp” individuando eventuali gruppi di indirizzi IP con MAC address ripetuto. Supponendo che tale script giri sul gateway di default della rete, si impartisca dinamicamente una regola iptables che filtri (*blocchi*) il traffico proveniente da tutti gli indirizzi IP in conflitto. Allo scadere dei 30 minuti, le regole di firewall eventualmente inserite dovranno essere eliminate automaticamente.

È parte integrante dello script conoscere i comandi e le opzioni utili a ricavare le informazioni relative agli indirizzi ip associati ad un mac address nella macchina locale e al numero di connessioni instaurate tra 2 hosts.