

# Sistemi Operativi e Reti

## Specifiche per i progetti assegnati per l'A.A. 2012-13

Data la topologia di rete allegata, si richiede di sviluppare un laboratorio netkit in accordo alle specifiche seguenti.

Determinare per tutti i domini di collisione, laddove mancanti, i seguenti valori:

### Configurazione domini di collisione

1. **N** = Network (Ad esempio, 172.16.0.0 / 12).
2. **NA** = Network Address ( ad esempio 172.16.0.1).
3. **BA** = Broadcast Address (ad esempio, 172.31.255.255).
4. **UIP** = Numero di IP utilizzabili.
5. **R** = Intervallo degli indirizzi IP usabili (esempio, 172.16.0.0 - 172.31.255.255)

Tenere presente che:

- I calcolatori rappresentano punti rete utente localizzati all'interno di un dato dominio di collisione;
- Gli hub (identificati con i pallini verdi) rappresentano i domini di collisione ed etichettati con il nome 'CDn' ( $n = 1, \dots$ ).

Per ogni dominio di collisione, devono essere determinati i valori di cui ai punti 1-5 del precedente elenco;

- I router (identificati con l'etichetta Rn ( $n = 1, \dots$ )) rappresentano le interconnessioni tra i domini di collisione;
- I firewall (identificati con l'etichetta Fn ( $n = 1, \dots$ )) costituiscono i dispositivi di sicurezza presenti nel sistema.

Ogni firewall si comporta anche da router (ovvero connette domini di collisione), e deve essere configurato per soddisfare le specifiche elencate nella sezione **Configurazione Firewall**;

- I server (identificati con l'etichetta Sn ( $n = 1, \dots$ )) rappresentano servizi offerti dalla rete e accessibili dall'esterno. Un server ha normalmente alcune porte di ascolto attive che devono essere raggiungibili. La raggiungibilità di una porta deve essere ottenuta mediante una opportuna configurazione delle regole del firewall.
- I server contrassegnati dall'identificativo SNatted forniscono servizi soggetti a port forwarding da parte

del firewall vicino, che deve essere considerato operante come router NAT. Per questi server è necessario consentire l'erogazione del servizio mantenendo nascosta la reale macchina che lo fornisce evitando, nel contempo, che possa essere possibile accedervi direttamente.

Ogni server è etichettato con i servizi che deve erogare (indicando il nome simbolico del servizio stesso, e.g. 'https'). Più domini di collisione adiacenti formano delle 'aree', che possono essere di tipo DMZ, GREEN e RED.

### Configurazione Firewall

Limitazioni generali sul traffico di rete (in ordine crescente di priorità):

- Le Green Area possono aprire connessioni destinate alle aree RED, DMZ e Internet;
- Le aree DMZ possono aprire connessioni destinate alle aree RED mentre queste ultime non possono aprire connessioni destinate alle altre reti.
- Le aree 'DMZ' devono consentire i seguenti servizi (ANCHE se non è esplicitamente presente il server corrispondente), accessibili dalle sole aree RED:
  - dns sulla porta 53
  - smtp sulla porta 25
  - ftp sulla porta 21
  - msp sulla porta 18
- Per tutti i firewall la politica di default è DROP.