A.D. 1308

unipg

UNIVERSITÀ DEGLI STUDI
DI PERUGIA

Tad&Apd srl

Studenti:

Christian Angileri [330925]

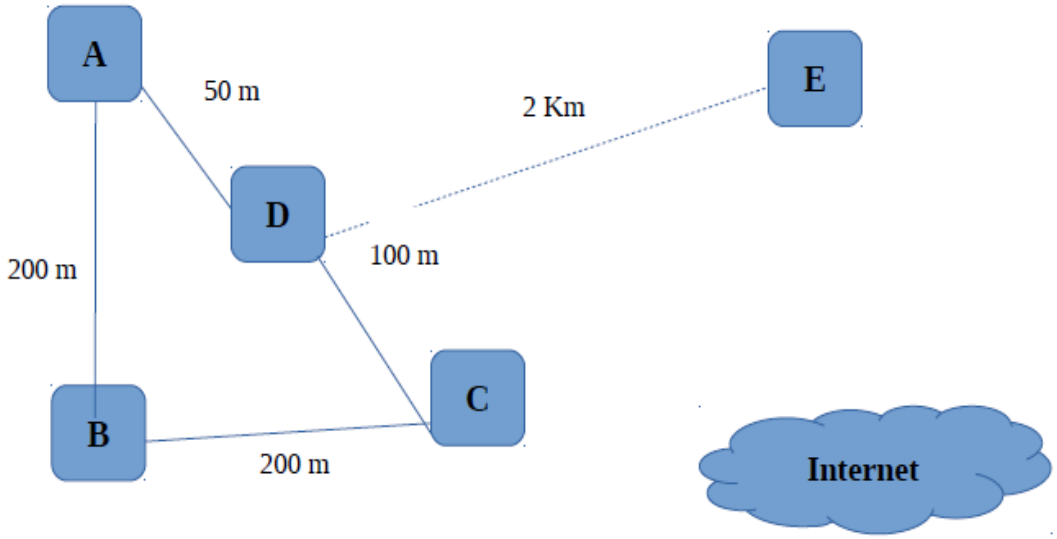
Alessio Cassieri [324396]

DIPARTIMENTO DI
MATEMATICA E
INFORMATICA

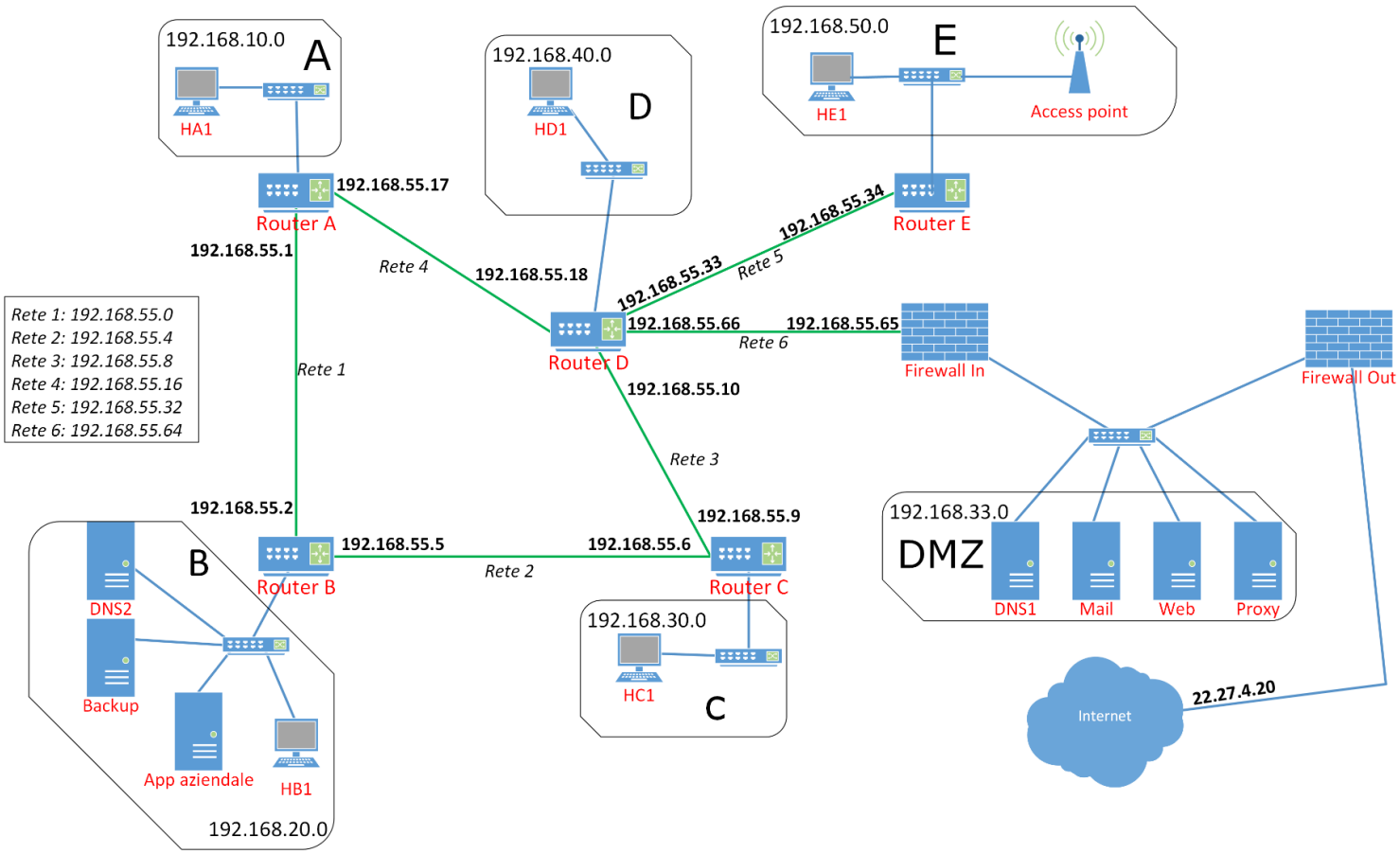
Descrizione del Progetto

La ditta Tad&Apd srl ha deciso di collegare in rete tutti i suoi reparti ed uffici e vi ha contattato per disegnare, installare e gestire l'intera rete. Quest'ultima può essere così schematizzata:

Schema fisico della rete:



Struttura generale della rete



Ogni edificio sopra viene rappresentato in questo modo:

Edificio	Uffici & Reparti	N. utenti	N. Server	Wi-fi
A	4 reparti + 5 uffici da 5 pc l'uno	100	0	No
B	4 reparti + 5 uffici da 5 pc l'uno + server	100	3	No
C	4 reparti + 5 uffici da 5 pc l'uno	100	0	No
D	6 reparti + 5 uffici da 5 pc l'uno + server	150	4	No
E	2 reparti + 5 uffici da 5 pc l'uno	50	0	Si

All'interno dell'azienda devono essere presenti i seguenti Server:

Tipo di server	Numero
Server di posta elettronica	1
Server Web	1
Server DNS	2
Server per applicazioni aziendali	1
Server Proxy	1
Server Backup	1

La rete prevede una connessione protetta ad internet

Struttura fisica della rete:

CONSIDERAZIONI PRELIMINARI:

Gli edifici saranno suddivisi:

- A e C avranno 4 piani composti da 5 uffici l'uno al cui interno ci saranno 5 pc;
- B avrà 4 piani composti da 5 uffici l'uno al cui interno ci saranno 5 pc. Il piano sotterraneo conterrà i server interni;
- D avrà 6 piani composti da 5 uffici l'uno al cui interno ci saranno 5 pc. Il piano sotterraneo conterrà la DMZ;
- E avrà 2 piani composti da 5 uffici l'uno al cui interno ci saranno 5 pc.

L'**edificio B** è attrezzato per ospitare i server accessibili dalla **rete interna**, che sono:

- **Server DNS Interno**, dove potranno accedervi solo gli host della rete interna;
- **Server Applicazione Aziendale**;
- **Server di Backup**, che svolge il compito di salvare ed effettuare una copia di tutti i terminali della rete interna, il salvataggio viene effettuato di notte per evitare l'aumento di carico nella rete, che può causare degradazione delle prestazioni nelle ore diurne, ma può essere effettuato anche a comando.

Cablaggio rete

Il collegamento fisico della rete avverrà con i seguenti cavi:

- **Fibra ottica** multimodale per il collegamento tra i vari router;
- Cavo **STP**(Shielded Twisted Pair) per collegamento tra router e switch dell'edificio;
- Cavo **STP** per collegamento tra switch dell'edificio e gli switch dei vari piani dell'edificio;
- Cavo **STP** per collegamento tra switch del piano e gli switch delle stanze;
- Infine, i terminali si connetteranno agli switch della stanza attraverso un cavo **UTP** (Unshielded Twisted Pair).

Struttura logica della rete

Classi ed indirizzi IP

La classe di indirizzi IP utilizzata è la C.
La **subnet mask** utilizzata per suddividere gli edifici è la 255.255.255.0, che ci permette di avere 254 sottoreti, ognuna delle quali con 254 host.

La tabella seguente specifica la suddivisione degli edifici:

Edificio	Sottorete
A	192.168.10.0 /24
B	192.168.20.0 /24
C	192.168.30.0 /24
D	192.168.40.0 /24
E	192.168.50.0 /24
DMZ	192.168.33.0 /24

Connessione tra Router:

I vari router comunicano tra di loro tramite l'indirizzo IP: 192.168.55.0
Utilizziamo la sub-net mask 255.255.255.252, ottenendo così un massimo di 2 host per sottorete, i quali sono sufficienti per connettere tra di loro tutti i router.

La tabella seguente rappresenta quanto affermato prima:

Router-Router	Network
A - B	192.168.55.0 /30
B - C	192.168.55.4 /30
C - D	192.168.55.8 /30
D - A	192.168.55.16 /30
E - D	192.168.55.32 /30
D – Firewall in	192.168.55.64 /30

SWITCH

Gli **switch** sono stati messi in modo da avere un prezzo minore nel conteggio finale, questo però ci fa inserire molti switch per edificio, dato che è presente 1 switch per la connessione con un router, poi uno switch per piano e poi uno switch per ufficio.

Per la configurazione degli switch vengono seguite le seguenti convenzioni:
- L'interfaccia 0/0 è stata usata per la connessione con il router.
- L'ultima interfaccia verrà usata per una eventuale connessione con il Firewall Out.
- Le altre interfacce sono utilizzate per la connessione con gli host.

ROUTER

Per la configurazione del router sono state scelte le seguenti convenzioni:
- L'interfaccia 0/0 è usata per la connessione allo Switch dei vari edifici (sulla porta 0/0), l'IP sarà X.X.X.1.
- Le altre interfacce sono usate per connettersi con gli altri router.
- Il protocollo di Routing che abbiamo ritenuto più adeguato è RIP_v2 in quanto la rete da noi progettata non crea problemi ai suoi limiti di convergenza e numero massimo di hop possibili (max 15).

Configurazione:

Edificio A

N° host: 100
Sottorete: 192.168.10.0 /24
Collegamento edifici: B,D

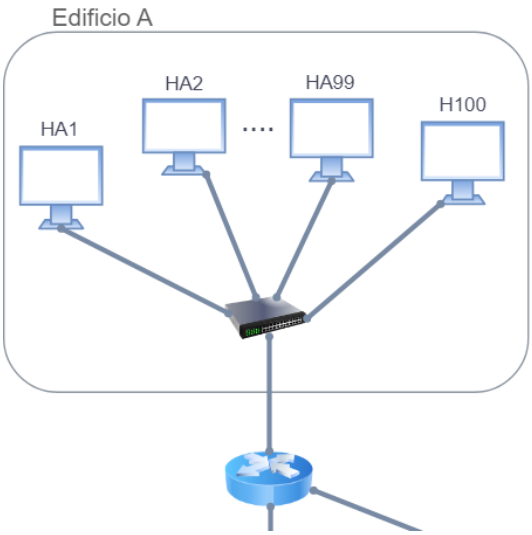


Tabella assegnazione indirizzi IP:

Codice	Tipologia dispositivo	Indirizzo IP
HA1	Host	192.168.10.2
HA2	Host	192.168.10.3
....	....	....
HA99	Host	192.168.10.100
HA100	Host	192.168.10.101
Router A	Router	192.168.10.1

Edificio B

N° host: 100
Sottorete: 192.168.20.0 /24
Collegamento edifici: A,C

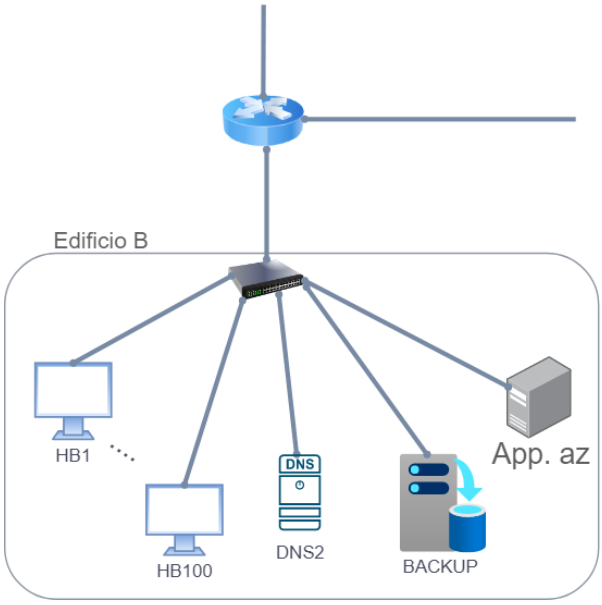


Tabella assegnazione indirizzi IP:

Codice	Tipologia dispositivo	Indirizzo IP
HB1	Host	192.168.20.2
HB2	Host	192.168.20.3
....	....	....
HB99	Host	192.168.20.100
HB100	Host	192.168.20.101
Router B	Router	192.168.20.1
DNS2	DNS server	192.168.20.200
BACKUP	Server	192.168.20.201
App. aziendale	Server	192.168.20.202

Edificio C

N° host: 100
Sottorete: 192.168.30.0 /24
Collegamento edifici: A,D

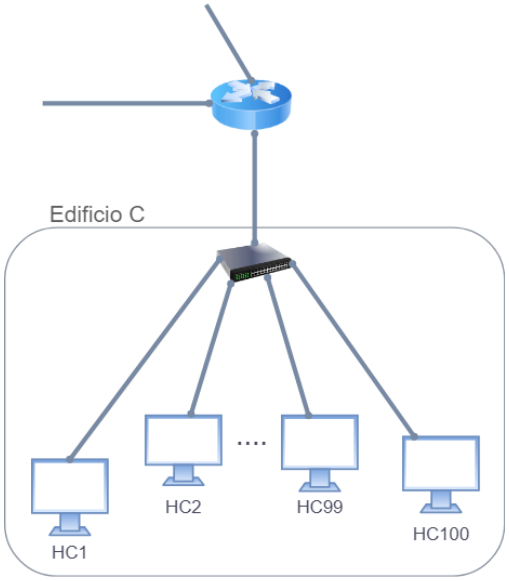


Tabella assegnazione indirizzi IP:

Codice	Tipologia dispositivo	Indirizzo IP
HC1	Host	192.168.30.2
HC2	Host	192.168.30.3
....	....	....
HC99	Host	192.168.30.100
HC100	Host	192.168.30.101
Router C	Router	192.168.30.1

Edificio D

N° host: 150
Sottorete: 192.168.40.0 /24
Collegamento edifici: A,C,E

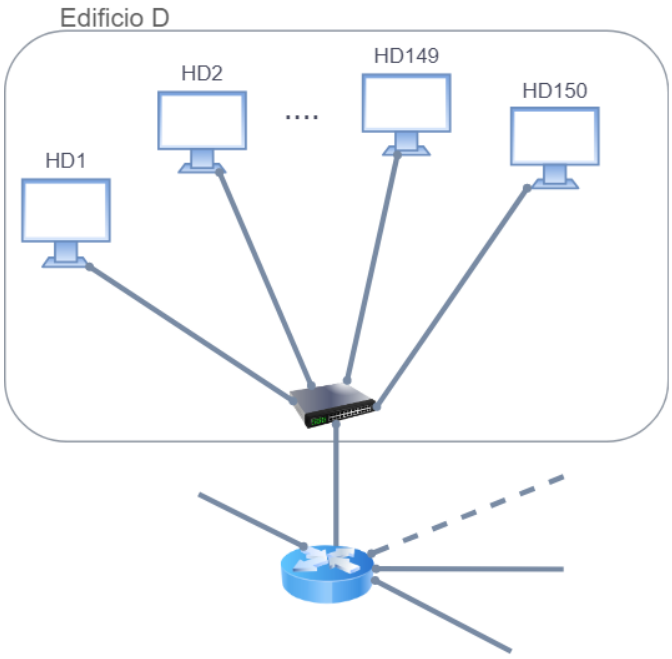


Tabella assegnazione indirizzi IP:

Codice	Tipologia dispositivo	Indirizzo IP
HD1	Host	192.168.40.2
HD2	Host	192.168.40.3
....	....	....
HD149	Host	192.168.40.150
HD150	Host	192.168.40.151
Router D	Router	192.168.40.1

Edificio E

N° host: 50
Sottorete: 192.168.50.0 /24
Collegamento edifici: D

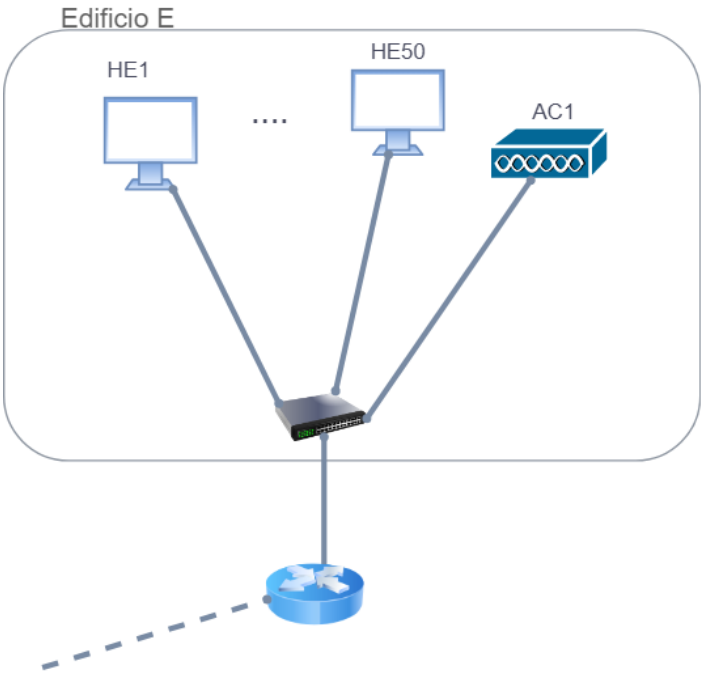


Tabella assegnazione indirizzi IP:

Codice	Tipologia dispositivo	Indirizzo IP
HE1	Host	192.168.50.2
HE2	Host	192.168.50.3
....	....	....
HE49	Host	192.168.50.50
HE50	Host	192.168.50.51
Router E	Router	192.168.50.1
Wlan0	Access point	192.168.50.77

DMZ

N° host: 0
Sottorete: 192.168.33.0 /24
Collegamento edifici: D
Collegamento Internet

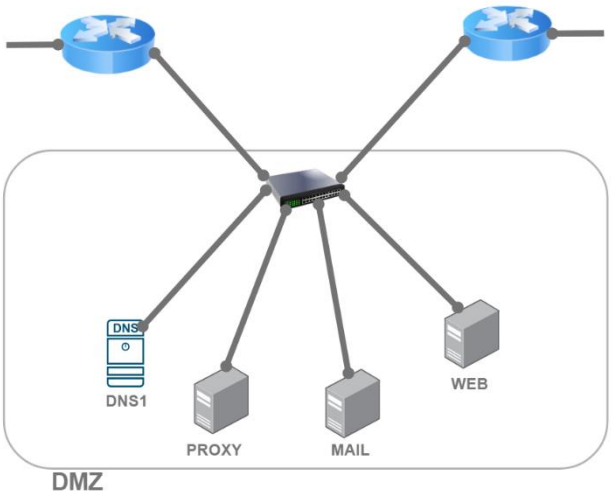


Tabella assegnazione indirizzi IP:

Codice	Tipologia dispositivo	Indirizzo IP
SZ200	Server DNS1	192.168.33.200
SZ201	Server Web	192.168.33.201
SZ202	Server Proxy	192.168.33.202
SZ203	Server Mail	192.168.33.203

Configurazione:

Interfacce router

default 255.255.255.0
mask 255.255.255.252

Router A:

ifconfig	*a0*	*192.168.10.1*	*netmask*	*default*	*broadcast*	*192.168.10.255*
ifconfig	*a1*	*192.168.55.1*	*netmask*	*mask*	*broadcast*	*192.168.55.3*
ifconfig	*a2*	*192.168.55.17*	*netmask*	*mask*	*broadcast*	*192.168.55.19*

Router B:

ifconfig	*b0*	*192.168.20.1*	*netmask*	*default*	*broadcast*	*192.168.20.255*
ifconfig	*b1*	*192.168.55.2*	*netmask*	*mask*	*broadcast*	*192.168.55.3*
ifconfig	*b2*	*192.168.55.5*	*netmask*	*mask*	*broadcast*	*192.168.55.7*

Router C:

ifconfig	*c0*	*192.168.30.1*	*netmask*	*default*	*broadcast*	*192.168.30.255*
ifconfig	*c1*	*192.168.55.6*	*netmask*	*mask*	*broadcast*	*192.168.55.7*
ifconfig	*c2*	*192.168.55.9*	*netmask*	*mask*	*broadcast*	*192.168.55.11*

Router D:

ifconfig	*d0*	*192.168.40.1*	*netmask*	*default*	*broadcast*	*192.168.40.255*
ifconfig	*d1*	*192.168.55.10*	*netmask*	*mask*	*broadcast*	*192.168.55.11*
ifconfig	*d2*	*192.168.55.18*	*netmask*	*mask*	*broadcast*	*192.168.55.19*
ifconfig	*d3*	*192.168.55.33*	*netmask*	*mask*	*broadcast*	*192.168.55.35*
ifconfig	*d4*	*192.168.55.66*	*netmask*	*mask*	*broadcast*	*192.168.55.67*

Router E:

ifconfig e0 192.168.50.1 netmask default broadcast 192.168.50.255

ifconfig e1 192.168.55.34 netmask mask broadcast 192.168.55.35

Firewall In:

ifconfig fi0 192.168.33.2 netmask default broadcast 192.168.33.255

ifconfig fi1 192.168.55.65 netmask mask broadcast 192.168.55.67

Firewall Out:

22.27.4.20 Ip pubblico statico assegnato dal provider

ifconfig fo0 192.168.33.1 netmask default broadcast 192.168.33.255

ifconfig fo1 22.27.4.20 netmask default broadcast 22.27.4.20

Interfacce host:

default 255.255.255.0

Rete A 192.168.10.0:

ifconfig HA1 192.168.10.2 netmask default broadcast 192.168.10.255

ifconfig HA2 192.168.10.3 netmask default broadcast 192.168.10.255

...

ifconfig HA100 192.168.10.101 netmask default broadcast 192.168.10.255

Rete B 192.168.20.0:

ifconfig HB1 192.168.20.2 netmask default broadcast 192.168.20.255

ifconfig HB2 192.168.20.3 netmask default broadcast 192.168.20.255

...

ifconfig HB100 192.168.20.101 netmask default broadcast 192.168.20.255

Rete C 192.168.30.0:

ifconfig HC1 192.168.30.2 netmask default broadcast 192.168.30.255

ifconfig HC2 192.168.30.3 netmask default broadcast 192.168.30.255

...

ifconfig HC100 192.168.30.101 netmask default broadcast 192.168.30.255

Rete D 192.168.40.0:

ifconfig HD1 192.168.40.2 netmask default broadcast 192.168.40.255

ifconfig HD2 192.168.40.3 netmask default broadcast 192.168.40.255

...

ifconfig HD150 192.168.40.151 netmask default broadcast 192.168.40.255

Rete E 192.168.50.0:

ifconfig HE1 192.168.50.2 netmask default broadcast 192.168.50.255

ifconfig HE2 192.168.50.3 netmask default broadcast 192.168.50.255

...

ifconfig HE50 192.168.50.51 netmask default broadcast 192.168.50.255

Interfacce server:

default 255.255.255.0

Dentro Edificio B

Server DNS2:

ifconfig SB200 192.168.20.200 netmask default broadcast 192.168.20.255

Server Backup:

ifconfig SB201 192.168.20.201 netmask default broadcast 192.168.20.255

Server App aziendale:

ifconfig SB202 192.168.20.202 netmask default broadcast 192.168.20.255

Dentro DMZ

Server DNS1:

ifconfig SZ200 192.168.33.200 netmask default broadcast 192.168.33.255

Server Web:

ifconfig SZ201 192.168.33.201 netmask default broadcast 192.168.33.255

Server Proxy:

ifconfig SZ202 192.168.33.202 netmask default broadcast 192.168.33.255

Server Mail:

ifconfig SZ203 192.168.33.203 netmask default broadcast 192.168.33.255

Interfaccia Access Point:

default 255.255.255.0

Server Access Point Wi-Fi E:

ifconfig wlan0 192.168.50.77 netmask default broadcast 192.168.50.255

Routing

Per quanto riguarda il routing interno verrà configurato innanzitutto un **routing statico** che sarà utile nel caso in cui il routing dinamico riscontri problemi. Questa tipologia di routing rende impossibile l'aggiornamento della rete senza dover mettere mano al file di configurazione.

Per quanto riguarda il routing dinamico verrà utilizzato il **RIP** che utilizza come metrica i salti tra i router (hop) con un massimo di 15, sufficienti per questo tipo di rete. Per il routing esterno abbiamo configurato **EGP** sull'unico router che comunica con internet.

Router A:

route –n add	*/192.168.10.0*	*/192.168.10.1*	*1*
route –n add	*default*	*192.168.55.17*	*1*
route –n add	*192.168.55.0*	*192.168.55.1*	*1*
route –n add	*192.168.55.16*	*192.168.55.17*	*1*
route –n add	*192.168.20.0*	*192.168.55.1*	*2*

route –n add	*192.168.40.0*	*192.168.55.17*	*2*
route –n add	*192.168.55.4*	*192.168.55.1*	*2*
route –n add	*192.168.55.8*	*192.168.55.17*	*2*
route –n add	*192.168.55.32*	*192.168.55.17*	*2*
route –n add	*192.168.55.64*	*192.168.55.17*	*2*
route –n add	*192.168.30.0*	*192.168.55.17*	*3*
route –n add	*192.168.50.0*	*192.168.55.17*	*3*
route –n add	*192.168.33.0*	*192.168.55.17*	*3*

Router B:

route –n add	*/192.168.20.0*	*/192.168.20.1*	*1*
route –n add	*default*	*192.168.55.5*	*1*
route –n add	*192.168.55.0*	*192.168.55.2*	*1*
route –n add	*192.168.55.4*	*192.168.55.5*	*1*
route –n add	*192.168.10.0*	*192.168.55.2*	*2*
route –n add	*192.168.30.0*	*192.168.55.5*	*2*
route –n add	*192.168.55.8*	*192.168.55.5*	*2*
route –n add	*192.168.55.16*	*192.168.55.2*	*2*
route –n add	*192.168.55.32*	*192.168.55.5*	*3*
route –n add	*192.168.55.64*	*192.168.55.5*	*3*
route –n add	*192.168.40.0*	*192.168.55.5*	*3*
route –n add	*192.168.50.0*	*192.168.55.5*	*4*
route –n add	*192.168.33.0*	*192.168.55.5*	*4*

Router C

route –n add	*/192.168.30.0*	*/192.168.30.1*	*1*
route –n add	*default*	*192.168.55.9*	*1*
route –n add	*192.168.55.4*	*192.168.55.6*	*1*
route –n add	*192.168.55.8*	*192.168.55.9*	*1*
route –n add	*192.168.20.0*	*192.168.55.6*	*2*
route –n add	*192.168.40.0*	*192.168.55.9*	*2*

route –n add	*192.168.55.0*	*192.168.55.6*	*2*
route –n add	*192.168.55.16*	*192.168.55.9*	*2*
route –n add	*192.168.55.32*	*192.168.55.9*	*2*
route –n add	*192.168.55.64*	*192.168.55.9*	*2*
route –n add	*192.168.10.0*	*192.168.55.9*	*3*
route –n add	*192.168.50.0*	*192.168.55.9*	*3*
route –n add	*192.168.33.0*	*192.168.55.9*	*3*

Router D

route –n add	*/192.168.40.0*	*/192.168.40.1*	*1*
route –n add	*default*	*192.168.55.66*	*1*
route –n add	*192.168.55.16*	*192.168.55.18*	*1*
route –n add	*192.168.55.8*	*192.168.55.10*	*1*
route –n add	*192.168.55.64*	*192.168.55.66*	*1*
route –n add	*192.168.55.32*	*192.168.55.33*	*1*
route –n add	*192.168.30.0*	*192.168.55.10*	*2*
route –n add	*192.168.10.0*	*192.168.55.18*	*2*
route –n add	*192.168.55.4*	*192.168.55.10*	*2*
route –n add	*192.168.55.0*	*192.168.55.18*	*2*
route –n add	*192.168.33.0*	*192.168.55.66*	*2*
route –n add	*192.168.50.0*	*192.168.55.33*	*2*
route –n add	*192.168.20.0*	*192.168.55.10*	*3*

Router E

route –n add	*/192.168.50.0*	*/192.168.50.1*	*1*
route –n add	*default*	*192.168.55.34*	*1*
route –n add	*192.168.55.32*	*192.168.55.34*	*1*
route –n add	*192.168.55.8*	*192.168.55.34*	*2*
route –n add	*192.168.55.64*	*192.168.55.34*	*2*
route –n add	*192.168.40.0*	*192.168.55.34*	*2*
route –n add	*192.168.55.16*	*192.168.55.34*	*2*

route –n add	*192.168.30.0*	*192.168.55.34*	*3*
route –n add	*192.168.10.0*	*192.168.55.34*	*2*
route –n add	*192.168.55.4*	*192.168.55.34*	*3*
route –n add	*192.168.55.0*	*192.168.55.34*	*3*
route –n add	*192.168.33.0*	*192.168.55.34*	*3*
route –n add	*192.168.20.0*	*192.168.55.34*	*4*

Firewall out

route –n add	*default*	*22.27.4.20*	*1*
route –n add	*192.168.33.0*	*192.168.33.1*	*1*

Firewall in

route –n add	*default*	*192.168.55.65*	*1*
route –n add	*192.168.33.0*	*192.168.33.2*	*1*

Routing dinamico RIP:

Router A:

//La parola chiave passive sta ad indicare che, essendo l'unica interfaccia di rete di A, gated non deve cancellare questa interfaccia dalla routing table anche quando l'interfaccia è down.

```
interfaces{
        interface 192.168.10.1 passive;
}
rip yes{
        broadcast;
        interface 192.168.10.1{
                version 2;
```

```
            multicast;
            authentication simple "RIPauth";
};
        interface 192.168.55.1{
            version 2;
            multicast;
            authentication simple "RIPauth";
        };
        interface 192.168.55.17{
            version 2;
            multicast;
            authentication simple "RIPauth";
        };
};
```

Router B:

```
Interfaces {
         Interface 192.168.20.1 passive;
}

rip yes{
        broadcast;
        interface 192.168.20.1{
            version 2;
            multicast;
            authentication simple "RIPauth";
};
        interface 192.168.55.5{
            version 2;
            multicast;
            authentication simple "RIPauth";
        };
        interface 192.168.55.2{
            version 2;
            multicast;
            authentication simple "RIPauth";
        };
};
```

Router C:

```
Interfaces {
        Interface 192.168.30.1 passive;
}

rip yes{
        broadcast;
        interface 192.168.30.1{
                version 2;
                multicast;
                authentication simple "RIPauth";
};
        interface 192.168.55.6{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.55.9{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};
```

Router D:

```
Interfaces {
        Interface 192.168.40.1 passive;
}

rip yes{
        broadcast;
        interface 192.168.40.1{
                version 2;
                multicast;
                authentication simple "RIPauth";
};
        interface 192.168.55.18{
                version 2;
                multicast;
                authentication simple "RIPauth";
```

```
        };
        interface 192.168.55.10{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
         interface 192.168.55.66{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
         interface 192.168.55.33{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };


};
```

Router E:

```
Interfaces {
         Interface 192.168.50.1 passive;
}

rip yes{
        broadcast;
        interface 192.168.50.1{
                version 2;
                multicast;
                authentication simple "RIPauth";
};
        interface 192.168.55.34{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};
```

Firewall in

```
Interfaces {
        Interface 192.168.55.65 passive;
        Interface 192.168.33.2 passive;

}

rip yes{
        broadcast;
        interface 192.168.55.65{
                version 2;
                multicast;
                authentication simple "RIPauth";
};
        interface 192.168.33.2{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};
```

Firewall out

```
//Routing dinamico EGP

Autonomoussystem 224;
Options gendefault;
Routerid 22.27.4.20;

ospf no;

Interfaces {
        Interface 192.168.33.1 passive;
        Interface 22.27.4.20 passive;

}

rip yes{
        broadcast;
        interface 192.168.33.1{
                version 2;
                multicast;
```

```
                authentication simple "RIPauth";
};
        interface 22.27.4.20{
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};


egp yes {
                  packetsize 12288;
                  group minhello 2:30 minpoll 10:00{};
                  //dichiarazione di un gruppo di EGP vicini
};

#esporta le route esterne da altri AS all'interno

export proto rip{
proto rip as 224{all};
};
```

Configurazione Server DNS:

DNS1 Primario DMZ:

Configurazione del file named.conf

```
options {
        acl “tad_apd”{
                        192.168.33.0;
                        };
        directory           "/etc/named";   //directory
        pid-file            "named.pid";    //Put pid file in working dir
        allow-query         { "tad_apd"; };
        recursion           no;
};

zone        “.” IN {
            type hint;
            file “named.ca”;
};

zone        “localhost” IN {
            type master;
            file “localhost.zone”;
};
zone        “0.0.127.in.addr.arpa” IN {
            type master;
            file “localhost.rev”;
};
```

```
zone    "tad_apd.it" IN {
        type master;
        file "tad_apd.rev";
        allow-transfert {192.168.20.200;};
};
zone    "168.192" IN {
        type master;
        file "tad_apd.rev";
        allow-transfert {192.168.20.200;};
};
```

Zone files

localhost.zone

```
@           .       IN      SOA     @root(
                                        2023010100 ;    serial
                                        43200 ;         refresh
                                        3600 ;          retry
                                        3600000 ;       expire
                                        2592000 ;       default ttl
                                        );
IN      NS      @
IN      PTR     127.0.0.1
```

localhost.rev

```
@           .       IN      SOA     dns1.tad_apd.it root.localhost(
                                        2023010100 ;    serial
                                        43200 ;         refresh
                                        3600 ;          retry
```

```
                                        3600000 ;       expire
                                        2592000 ;       default ttl
                                        );
        IN      NS      dns1.tad_apd.it;
1       IN      PTR     localhost;
```

tad_apd.zone

```
@               .       IN      SOA     dns1.tad_apd.it root.localhost(
                                        2023010100 ;    serial
                                        43200 ;         refresh
                                        3600 ;          retry
                                        3600000 ;       expire
                                        2592000 ;       default ttl
                                        );
IN      NS      dns1.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      NS      proxy.tad_apd.it;
IN      MX      mail.tad_apd.it;
dns1    IN      A       192.168.33.200;
web     IN      A       192.168.33.201;
proxy   IN      A       192.168.33.202;
mail    IN      A       192.168.33.203;
www.tad_apd.it          IN      CNAME           web;
mail.tad_apd.it         IN      CNAME           mail;
```

tad_apd.rev

```
@               .       IN      SOA     dns1.tad_apd.it root.localhost(
                                        2023010100 ;    serial
                                        43200 ;         refresh
                                        3600 ;          retry
```

```
                                        3600000 ;       expire
                                        2592000 ;       default ttl
                                        );
IN      NS      dns1.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      NS      proxy.tad_apd.it;
IN      MX      mail.tad_apd.it;

33.200  IN      PTR     dns1;
33.201  IN      PTR     web;
33.202  IN      PTR     proxy;
33.203  IN      PTR     mail;
```

DNS2 Primario interno rete:

Configurazione del file named.conf

```
options {
    acl “tad_apd”{
         localhost;
        192.168.10.0/24;
        192.168.20.0/24;
        192.168.30.0/24;
        192.168.40.0/24;
        192.168.50.0/24;
        192.168.33.0/24;
        };
    directory       "/etc/named";   //directory
    pid-file        "named.pid"; // Put pid file in working dir
```

```
    allow-query     { "tad_apd"; };
    recursion       no;
};

zone    "." IN {
            type hint;
            file "named.ca";
};

zone    "localhost" IN {
            type master;
            file "localhost.zone";
};
zone    "0.0.127.in.addr.arpa" IN {
            type master;
            file "localhost.rev";
};

zone    "tad_apd.it" IN {
            type slave;
            file "tad_apd.zone";
            masters {192.168.33.200;};
};
zone    "168.192.in.addr.arpa" IN {
            type slave;
            file "tad_apd.rev";
            masters {192.168.33.200;};
};
```

```
zone    "produzione.tad_apd.it" IN {
        type master;
        file "produzione.zone";
};
zone    "10.168.192.in.addr.arpa" IN {
        type master;
        file "produzione.rev";
};

zone    "management.tad_apd.it" IN {
        type master;
        file "management.zone";
};
zone    "20.168.192.in.addr.arpa" IN {
        type master;
        file "management.rev";
};

zone    "marketing.tad_apd.it" IN {
        type master;
        file "marketing.zone";
};
zone    "30.168.192.in.addr.arpa" IN {
        type master;
        file "marketing.rev";
};

zone    "tecnici.tad_apd.it" IN {
        type master;
```

```
        file "tecnici.zone";
};
zone    "40.168.192.in.addr.arpa" IN {
        type master;
        file "tecnici.rev";
};

zone    "segreteria.tad_apd.it" IN {
        type master;
        file "segreteria.zone";
};
zone    "50.168.192.in.addr.arpa" IN {
        type master;
        file "segreteria.rev";
};

zone    "dmz.tad_apd.it" IN {
        type master;
        file "dmz.zone";
};
zone    "33.168.192.in.addr.arpa" IN {
        type master;
        file "dmz.rev";
};
```

Zone files

localhost.zone

```
@               .       IN      SOA     @root(
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
                                                3600000 ;       expire
                                                2592000 ;       default ttl
                                                );
IN      NS      @
IN      PTR     127.0.0.1
```

localhost.zone

```
@               .       IN      SOA     dns2.tad_apd.it @root.localhost(
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
                                                3600000 ;       expire
                                                2592000 ;       default ttl
                                                );
        IN      NS      dns2.tad_apd.it;
1       IN      PTR     localhost;
```

produzione.zone

```
@               .       IN      SOA     produzione.tad_apd.it
                                        root_produzione.tad_apd.it (
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
```

```
                                        3600000 ;       expire
                                        2592000 ;       default ttl
                                        );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

HA1     IN      A       192.168.10.2;
....
HA100   IN      A       192.168.10.101;
```

produzione.rev

```
@               .       IN      SOA     produzione.tad_apd.it
                                        root_produzione.tad_apd.it (
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
                                                3600000 ;       expire
                                                2592000 ;       default ttl
                                                );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

2       IN      PTR     HA1;
....
101     IN      PTR     HA100;
```

management.zone

```
@                .       IN      SOA     management.tad_apd.it
                                         root_management.tad_apd.it (
                                                 2023010100 ;    serial
                                                 43200 ;         refresh
                                                 3600 ;          retry
                                                 3600000 ;       expire
                                                 2592000 ;       default ttl
                                                 );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

HB1                     IN      A       192.168.20.2;
....
HB100                   IN      A       192.168.20.101;

dns2                    IN      A       192.168.20.200;
dns2.tad_apd.it         IN      CNAME   dns2;
backup                  IN      A       192.168.20.201;
app.aziendale           IN      A       192.168.20.202;
```

management.rev

```
@                .       IN      SOA     management.tad_apd.it
                                         root_management.tad_apd.it (
                                                 2023010100 ;    serial
                                                 43200 ;         refresh
                                                 3600 ;          retry
```

```
                                        3600000 ;       expire
                                        2592000 ;       default ttl
                                        );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

2       IN      PTR     HB1;
....
101     IN      PTR     HB100;

200     IN      PTR     dns2;
201     IN      PTR     backup;
202     IN      PTR     app.aziendale;
```

marketing.zone

```
@               .       IN      SOA     marketing.tad_apd.it
                                        root_marketing.tad_apd.it (
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
                                                3600000 ;       expire
                                                2592000 ;       default ttl
                                                );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;
```

```
HC1        IN      A       192.168.30.2;
....
HC100      IN      A       192.168.30.101;
```

marketing.rev

```
@                  .          IN      SOA     marketing.tad_apd.it
                                               root_marketing.tad_apd.it (
                                                     2023010100 ;     serial
                                                     43200 ;          refresh
                                                     3600 ;           retry
                                                     3600000 ;        expire
                                                     2592000 ;        default ttl
                                                     );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

2       IN      PTR     HC1;
....
101     IN      PTR     HC100;
```

tecnici.zone

```
@                  .          IN      SOA     tecnici.tad_apd.it
                                               root_tecnici.tad_apd.it (
                                                     2023010100 ;     serial
                                                     43200 ;          refresh
                                                     3600 ;           retry
```

```
                                        3600000 ;       expire
                                        2592000 ;       default ttl
                                        );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

HD1     IN      A       192.168.40.2;
....
HD150   IN      A       192.168.40.151;
```

tecnici.rev

```
@               .       IN      SOA     tecnici.tad_apd.it
                                        root_tecnici.tad_apd.it (
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
                                                3600000 ;       expire
                                                2592000 ;       default ttl
                                                );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

2       IN      PTR     HD1;
....
151     IN      PTR     HD150;
```

segreteria.zone

```
@                .        IN      SOA     segreteria.tad_apd.it
                                         root_segreteria.tad_apd.it (
                                                 2023010100 ;    serial
                                                 43200 ;         refresh
                                                 3600 ;          retry
                                                 3600000 ;       expire
                                                 2592000 ;       default ttl
                                                 );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

HE1             IN      A       192.168.50.2;
....
HE50            IN      A       192.168.50.51;

acc.point       IN      A       192.168.50.77;
```

segreteria.rev

```
@                .        IN      SOA     segreteria.tad_apd.it
                                         root_segreteria.tad_apd.it (
                                                 2023010100 ;    serial
                                                 43200 ;         refresh
                                                 3600 ;          retry
                                                 3600000 ;       expire
                                                 2592000 ;       default ttl
                                                 );
```

```
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

2       IN      PTR     HE1;
....
51      IN      PTR     HE50;

77      IN      PTR     acc.point;
```

dmz.zone

```
@               .       IN      SOA     dmz.tad_apd.it
                                        root_dmz.tad_apd.it (
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
                                                3600000 ;       expire
                                                2592000 ;       default ttl
                                                );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

dns1    IN      A       192.168.33.200;
web     IN      A       192.168.33.201;
proxy   IN      A       192.168.33.202
mail    IN      A       192.168.33.203;
```

dmz.rev

```
@               .       IN      SOA     dmz.tad_apd.it
                                        root_dmz.tad_apd.it (
                                                2023010100 ;    serial
                                                43200 ;         refresh
                                                3600 ;          retry
                                                3600000 ;       expire
                                                2592000 ;       default ttl
                                                );
IN      NS      dns1.tad_apd.it;
IN      NS      dns2.tad_apd.it;
IN      NS      web.tad_apd.it;
IN      MX      mail.tad_apd.it;

200     IN      PTR     dns1;
201     IN      PTR     web;
202     IN      PTR     proxy;
203     IN      PTR     mail;
```

Configurazione Server Mail

Abbiamo deciso di utilizzare “**Sendmail**” come programma per il trasporto della posta elettronica.

Sendmail riceve da un programma di posta dell'utente un messaggio, interpreta l'indirizzo di posta elettronica, riscrive tale indirizzo in un formato apposito per il programma di spedizione e instrada il messaggio al programma di spedizione appropriato.

Inoltre riceve e spedisce posta SMTP (Simple Mail Transfer Protocol) e fornisce alias di posta molto grandi che permettono l'inserimento di mailing list.
Sendmail ha dunque bisogno di alias per funzionare. Si configurano con il file "/etc/aliases".

Configurazione Aliases

root: root@tad_apd.it
Guido : guido_snt@segreteria_tad_apd.it
Paulo : paulo_dbl@segreteria_tad_apd.it
Jacopo : jacopo_bst@tad_apd.it
....
Informazioni : info@tad_apd.it

Configurazione Mailing List

Root: root, Jacopo, Informazioni.

Segreteria: Guido, Paulo.

...

Dal file aliases si crea un database. Per crearlo occorre lanciare il comando "**sendmail -bi**" grazie al quale inizializziamo il database.
Se si invoca il comando dopo aver aggiornato il file aliases occorre verificare che i nuovi aliases siano stati accettati.
La configurazione vera e propria di sendmail si fa attraverso il file "/etc/sendmail.cf". Andiamo a definire tutte le macro in questo file (macro obbligatorie: "e,j,l,n,o,q").

Configurazione Sendmail.cf

```
Dwweb                   //Hostname del sito       (web)
DDtad_apd.it            //Dominio                 (tad_apd.it)
Dj$w.$D                 //NomeUfficialeDominio    (web.tad_apd.it)

De$j Sendmail $v ready at $b    //MessaggioIniziale     v=versione    b=dataCorr
DlFrom $g $d                    //UnixFromLine          g=mittente    d=dataCorr
DnMAILER-DEAMON                 //NomeDemoneMessErrore
Do.:%\@!^=/                     //InsiemeOperatoriIndirizzi
Dq$g$?x ($x)$.                  //FormatoIndirizzoDefaultMittente

//UtentiTrusted
Troot
Tdeamon
Tuucp

//DefaultPrecedenza
Pfirst-class=0
Pspecial-delivery=100
Pbulk=-60
Pjunk=-100

//HeaderMail
H?P?Return-Path: <$g>                       //PathMailer
HReceived: $?sfrom $s $.by $j ($v/$Z)       //Mittente
H?D?Resent-Date: $a                         //DataPartenza
H?D?Date: $a
H?F?Resent-From: $q                         //Forward
H?F?From: $q                                //NomeMittente
H?x?Full-Name: $x                           //ImpostazioneFullName
```

Hsubject:

H?M?Resent-Message-Id: <$t.$i@$j> *//ora_att.id@NomeUfficialeDom*

H?M?Message-Id: <$t.$i@$j>

//Mailer

Mlocal, P=/bin/mail, F=rlsDFMmn, S=10, R=20, A=mail -d $u *//PostaLocale*

Mprog, P=/bin/sh, F=lsDFMe, S=10, R=20, A=sh -c $u *//Programmi*

Mtcpld, P=[ICP], F=mDFMueXLC, S=17, R=27, A=IPC $h, E=\r\n *//TCP/IP a local*

Mtcp, P=[ICP], F=mDFMueXLC, S=14, R=24, A=IPC $h, E=\r\n *//TCP/IP a Net.*

Muucp, P=/usr/bin/uux, F=DFMhuU, S=13, R=23, M=100000, //uucp

A=uux - -r -z -a$f -gC $h!rmail ($u)

Configurazione Firewall

Per la configurazione dei firewall abbiamo pensato che la miglior soluzione fosse utilizzare la **default deny**, dove tutto quello che non è espressamente ammesso viene bloccato, questo fa si che la politica di sicurezza sia più solida.
Abbiamo posizionato i 2 firewall nella zona di accesso ed uscita della DMZ, questo per far si che ogni pacchetto che entra ed esce dalla rete sia controllato.

Il **Firewall Esterno** implementerà delle regole di accesso non troppo restrittive mentre **Firewall Interno** che invece opererà un controllo maggiore in quanto sarà l'ultima linea di difesa.

Tramite iptables andremo ad effettuare la nostra configurazione

Firewall In:

```
# pulisce i router da eventuali catene rimaste
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT

# default drop
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

# dns
iptables -A FORWARD -p udp -d 192.168.33.200 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.33.200 --dport 53 -j ACCEPT

# mail SMTP, POP3, IMAP anche con SSL
iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 25 -m limit 100/s -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 465 -m limit 100/s -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 110 -m limit 100/s -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 143 -m limit 100/s -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 993 -m limit 100/s -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 995 -m limit 100/s -j ACCEPT

# web e proxy
iptables -A FORWARD -p tcp -d 192.168.33.201 --dport 80 -m limit 100/s -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.33.202 --dport 443 -m limit 100/s -j ACCEPT
```

Firewall Out:

 # dns, mail, web e proxy

iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 25 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 456 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 587 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 110 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 993 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 143 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.203 --dport 995 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.200 --dport 53 -j ACCEPT

iptables -A FORWARD -p udp -d 192.168.33.200 --dport 53 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.201 --dport 80 -j ACCEPT

iptables -A FORWARD -p tcp -d 192.168.33.202 --dport 443 -j ACCEPT

 # regole per connessioni già stabilite

iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT

iptables -A FORWARD -p tcp -j REJECT --reject-with tcp-reset

 # NAT

iptables -t NAT -A PREROUTING -p tcp --dport 25 -j DNAT --to-destination 198.168.33.203

iptables -t NAT -A PREROUTING -p udp --dport 53 -j DNAT --to-destination 198.168.33.200

iptables -t NAT -A PREROUTING -p tcp --dport 53 -j DNAT --to-destination 198.168.33.200

iptables -t NAT -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 198.168.33.201

iptables -t NAT -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination 198.168.33.202

 # mascheramento pacchetti uscenti

iptables -t NAT -A POSTROUTING -o eth1 -j MASQUERADE

Host hardening

Proponiamo un'altra soluzione per proteggere la rete, per farlo è necessario utilizzare due soluzioni:

- **TCP wrappers**;
- **xinetd**;

i quali ci permettono di inserire un livello di protezione a livello host.

TCP wrappers

Bisogna configurare due file, /etc/hosts.allow e deny, con priorità dall'alto verso il basso, dove il primo contiene informazioni su quali indirizzi è permesso l'accesso e il secondo file invece specifica l'accesso bloccato.

/etc/hosts.allow (per tutti gli host che non hanno funzione di server)

in.ftpd: ALL :/bin/date %c >> /var/log/in.http.log

in.http: ALL :/bin/date %c >> /var/log/in.http.log/in

in.sshd: ALL : /bin/date %c >> /var/log/in.ssh.log

in.htmld: ALL : /bin/date %c >> /var/log/in.html/log

in.whois: tad_apd.it

in.pop3,imap,smtp: tad_apd.it

/etc/hosts.deny

in.telnetd: ALL

ALL

ALL: ALL: SPAWN (
echo -e "\n
TCP Wrappers\: Connection refused\n
By\: $(uname -n)\n
Process\: %d (pid %p)\n
User\: %u\n
Host\: %c\n
Date\: $(date)\n
" | /usr/bin/mail -s "Connection to %d blocked" root)

XINETD

XINETD è un demone che estende le funzionalità del internet daemon inetd aggiungendo nuove ed avanzate metodologie di controllo dei servizi internet. Abilitiamo questo servizio per tutti gli host presenti nella rete interna e pure per i server aziendali.

Regole generali per host con inclusi i file per i protocolli TCP, UDP e SSH

/etc/xinetd.d

defaults
{
instances = 20
log_type = SYSLOG authpriv
log_on_success = HOST PID

log_on_failure= HOST

cps =10 30

}

includedir /etc/xinetd.d/wu-tcp

includedir /etc/xinetd.d/wu-udp

includedir /etc/xinetd.d/wu-ssh

/etc/xinetd.d/wu-tcp

service tcp

{

socket_type = dgram

wait = no

user = tcp

server = /usr/sbin/in.tcpd

log_on_success += DURATION USERID

log_on_failure += USERID

access_times = 08:00-19-00

}

/etc/xinetd.d/wu-udp

service udp

{

socket_type = dgram

wait = no

user = udp

server = /usr/sbin/in.udpd

log_on_success += DURATION USERID

log_on_failure += USERID

access_times = 08:00-19-00

}

/etc/xinetd.d/wu-ssh

service ssh

{

socket_type = stream

wait = no

user = ssh

server = /usr/sbin/in.sshd

log_on_success += DURATION USERID

log_on_failure += USERID

access_times = 08:00-19-00

}

Tramite questi file possiamo definire i servizi per l'utente semplice, dove ha un accesso dalle 8 di mattina alle 7 di sera, questi file sono presenti su ogni host. Nel caso di un attacco hacker interno, cioè effettuato da un computer aziendale, quest'ultimo può essere effettuato soltanto durante i turni di lavoro di un dipendente, di modo che sia più facile rendersi conto dell'attacco.

Regole generali per i server

/etc/xinetd.d

defaults

{

instances = 500

log_type = SYSLOG authpriv

log_on_success = HOST PID

log_on_failure= HOST

cps =200 30

}

includedir /etc/xinetd.d

Preventivo spese finali

Componente	Quantità	Prezzo unitario	Prezzo totale
Cavo fibra ottica	2600 m	€4,00/m	€10.400,00
Switch 5p TP-Link TL-SF1005D	3	€8	€24
Switch 8p TP-Link TL-SF1008D	123	€13	€1.599
Switch 16p TP-Link TL-SF1016D	1	27,82	€27,82
Firewall	2	€547,86	€1.095,72
Access Point TP-Link	1	€60	€60
Router TP-Link	5	€95	€475
Cavo STP	500 m	€ 1,00/m	€500,00
Cavo UTP	200 m	€ 0,50/m	€100,00
Progettazione	50 h (5h * 10 gg)	€22,00/ora	€1.100,00
Installazione	120 h (8h * 15 gg)	€40,00/ora	€4.800,00
		Totale:	€20.181,54