PROGETTO - RETI CALCOLATORI: PROTOCOLLI

A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

Osvaldo Industries

STUDENTI:

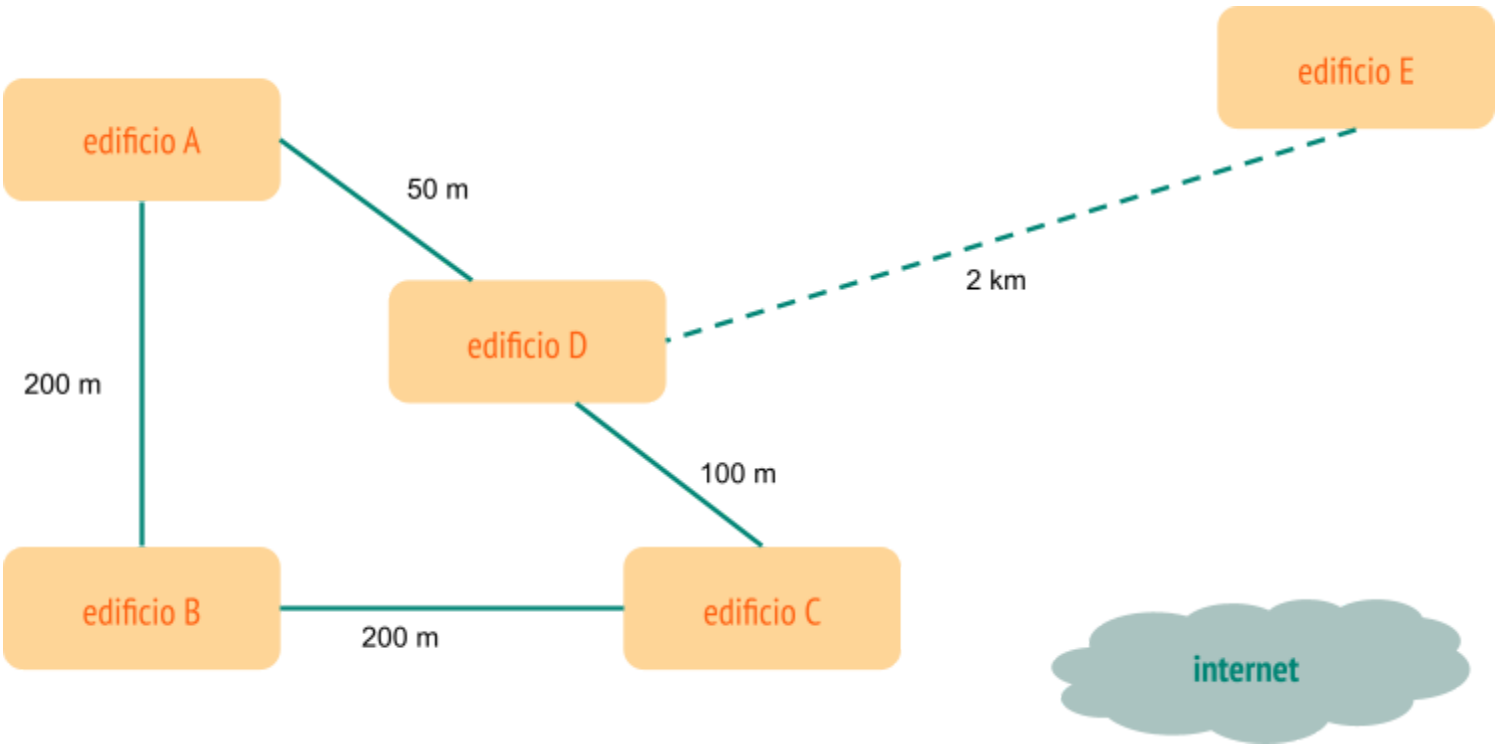
Maria Riommi [315912]
Nicolò Vescera [301838]

DIPARTIMENTO DI
MATEMATICA E
INFORMATICA

Descrizione del progetto

La ditta Osvaldo Industries 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:



Gli edifici sopra rappresentati, hanno le seguenti caratteristiche:

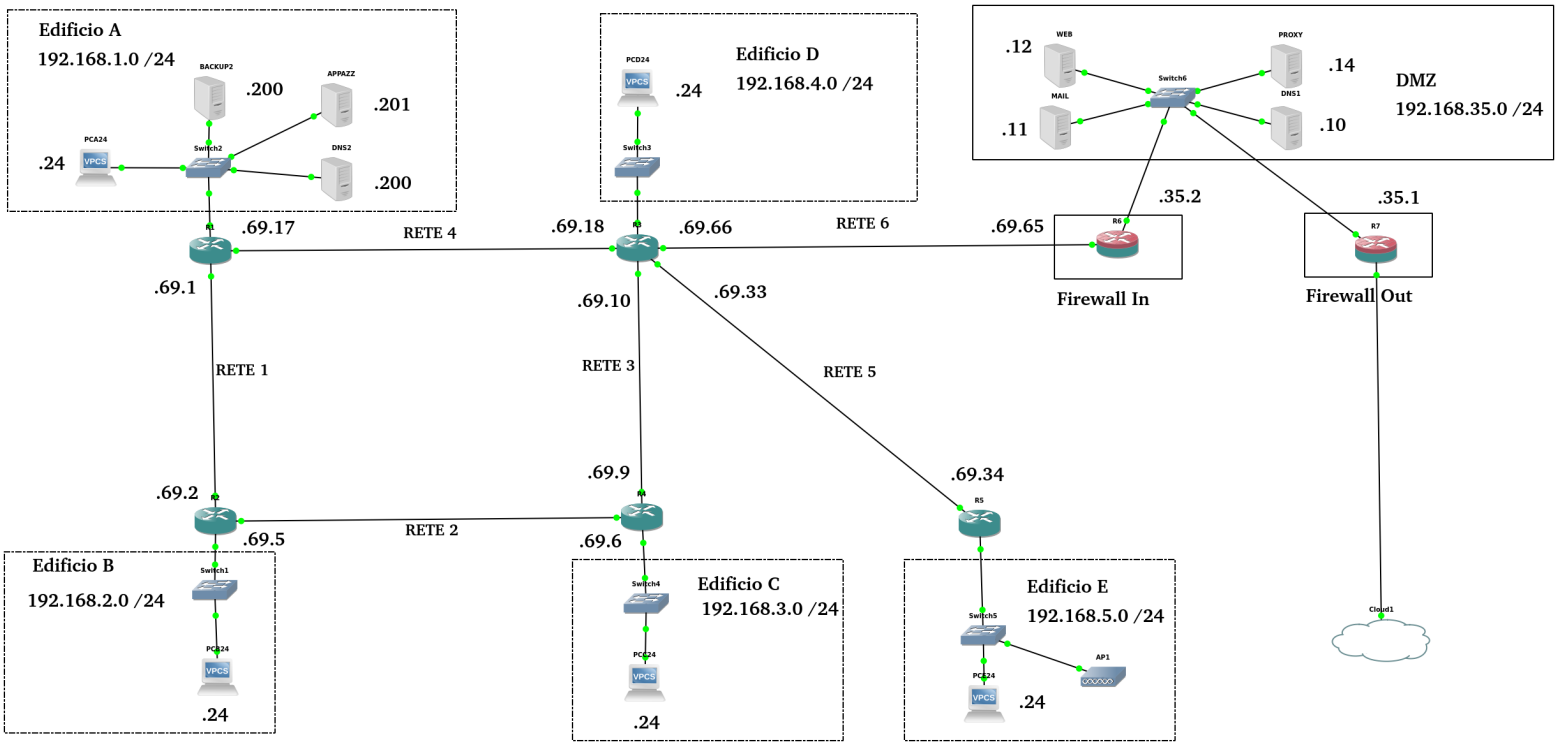
Edificio	Uffici & Reparti	N. Utenti	N. Server	Copertura WiFi
Edificio A	5 reparti da 4 uffici + Server	100	3	NO
Edificio B	5 reparti da 4 uffici	100	0	NO
Edificio C	5 reparti da 4 uffici	100	0	NO
Edificio D	7 reparti da 5 uffici + DMZ	150	4	NO
Edificio E	2 reparti da 5 uffici	50	0	SI

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 di backup	1

La rete prevede una connessione **protetta** ad Internet.

SCHEMA DELLA RETE SU GNS3



Struttura fisica della rete

CONSIDERAZIONI PRELIMINARI

Gli edifici saranno così suddivisi:

- Gli edifici **A**, **B** e **C** avranno **5 piani**, ogni piano sarà suddiviso in **4 stanze** da **5 macchine** ciascuna. Il piano sotterraneo dell'edificio A sarà riservato ai **Server Interni.**
- L'edificio **D** avrà **7 piani**, ogni piano sarà formato da **5 stanz**e con **5 macchine** ciascuna. Il piano sotterraneo sarà riservato alla **DMZ.**
- L'edificio **E** avrà **2 piani**, con **5 stanze** per piano da **5 utenti** l'una.

L' **edificio A** verrà attrezzato per ospitare tutti i server accessibili solo dalla **Rete Interna**:

- **Server DNS Interno**, al quale faranno riferimento solo gli host della rete interna.
- **Server Applicazioni Aziendali**.
- **Server di Backup**, che si occuperà di salvare una copia dei dati di tutti i terminali della rete interna, tale salvataggio avverrà nelle ore notturne per evitare degradazioni delle prestazioni della rete durante le ore di lavoro.

I **Server** che possono essere acceduti dall'esterno sono stati posizionati in una **De-Militarized Zone** in modo da garantire una migliore protezione, in quanto i servizi più "vulnerabili" e potenzialmente insicuri rimangono isolati sia dalla rete interna che dalla rete esterna.
Una struttura di questo tipo viene realizzata inserendo un **firewall-router esterno** che solitamente implementa delle regole di accesso non troppo restrittive ed un **firewall-router interno** che invece opera un controllo maggiore in quanto risulta l'ultima linea di difesa.

L' **edificio D** sarà adibito a contenere le macchine della **DMZ**:

- **Mail Server**.
- **Server Web,** che userà solo la porta 443 per garantire una connessione sicura in https.
- **Server DNS**, che si occuperà di gestire i nomi solo della DMZ.
- **Proxy**, che permetterà la comunicazione tra gli host della rete interna e internet.

CABLAGGIO STRUTTURATO

La realizzazione fisica della rete avverrà con le seguenti tipologie di cavi:

- Il collegamento tra i vari router avverrà tramite un cavo in **Fibra Ottica Multimodale.**
- Ogni router verrà connesso al relativo switch dell'edificio mediante un cavo **STP (Shielded Twisted Pair)**.
- Il link tra lo switch dell'edificio e gli switch dei piani avverrà con un cavo **STP (Shielded Twisted Pair)**.
- La connessione degli switch del piano agli switch della stanza avverrà attraverso un cavo **STP (Shielded Twisted Pair)**.
- Infine i terminali si connetteranno agli switch della stanza per via di un semplice cavo **UTP (Unshielded Twisted Pair)**.

Struttura logica della rete

CLASSI E INDIRIZZI IP

L'**indirizzo ip** usato dall'azienda è di classe C.

La **subnet mask** che abbiamo deciso di usare per la suddivisione degli edifici è la **255.255.255.0** in quanto ci permette di ottenere 254 sottoreti, ognuna delle quali può avere fino ad un massimo di 254 host.
La seguente tabella illustra la suddivisione in **sottoreti degli edifici**:

Edificio	Sottorete
edificio A	192.168.1.0 /24
edificio B	192.168.2.0 /24
edificio C	192.168.3.0 /24
edificio D	192.168.4.0 /24
edificio E	192.168.5.0 /24
DMZ	192.168.35.0 /24

BACKBONE ROUTER - ROUTER

Per la connessione dei vari router tra di loro abbiamo scelto l'indirizzo IP **192.168.69.0.**
Usando la subnet mask **255.255.255.252,** è possibile ottenere sottoreti con un massimo di **2 host** che abbiamo ritenuto più che sufficienti per connettere tra loro tutti i router.

La seguente tabella ne illustra l'utilizzo.

Router- Router	Network
A - B	192.168.69.0 /30
B - C	192.168.69.4 /30
C - D	192.168.69.8 /30
D - A	192.168.69.16 /30
D - E	192.168.69.32 /30
D - Firewall In	192.168.69.64 /30

SWITCH

Per la configurazione degli switch sono state 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.

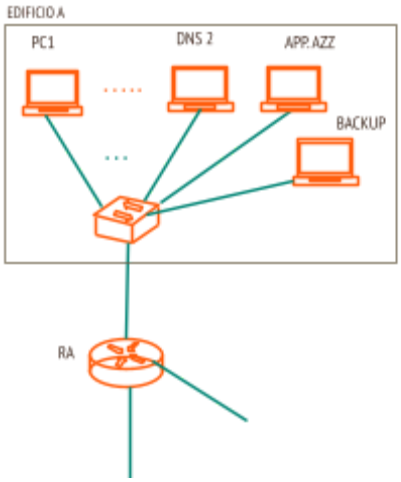
ROUTER

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**: 192.168.1.0/24
- **Collegamenti**: Edificio B, Edificio D

La seguente tabella illustra l'assegnazione degli indirizzi IP

Codice	Tipo Dispositivo	Indirizzo IP
PCA1	host	192.168.1.2
	.....	....
PCA100	host	192.168.1.102
DNS 2	DNS server	192.168.1.200
APP. AZZ	Server	192.168.1.201
BACKUP	Server	192.168.1.202
RA	router	192.168.1.1

CONFIGURAZIONE HOST

Il testo seguente rappresenta la configurazione dell'host 24

```
set pcname PCA24
ip 192.168.1.24/24 192.168.1.1
ip dns 192.168.1.200
```

CONFIGURAZIONE ROUTER

```
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.69.2 255.255.255.252
interface FastEthernet1/0
 ip address 192.168.69.5 255.255.255.252
router rip
 version 2
 network 192.168.2.0
 network 192.168.69.0
 network 192.168.69.4
end

ip domain-lookup
ip name-server 192.168.1.200
```

CONFIGURAZIONE BACKUP

```
set pcname backup
ip 192.168.1.202/24 192.168.1.1
ip dns 192.168.1.200
```

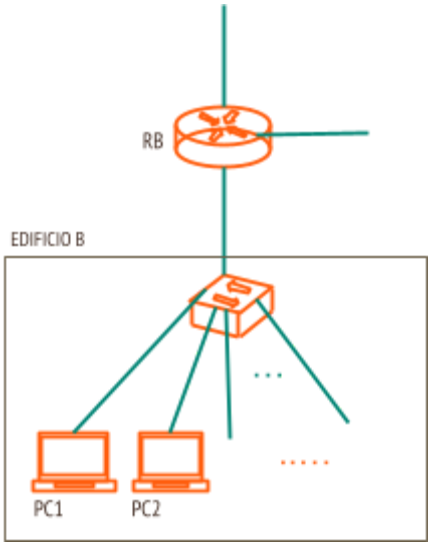
CONFIGURAZIONE DNS INTERNO

```
set pcname DNS2
ip 192.168.1.200/24 192.168.1.1
```

CONFIGURAZIONE APP. AZZ

```
set pcname APPAZZ
ip 192.168.1.201/24 192.168.1.1
ip dns 192.168.1.200
```

EDIFICIO B



- **N° Host**: 100
- **Sottorete**: 192.168.2.0/24
- **Collegamenti**: Edificio A, Edificio C

La seguente tabella illustra l'assegnazione degli indirizzi IP

Codice	Tipo Dispositivo	Indirizzo IP
PCB1	host	192.168.2.2
	.....	....
PCB100	host	192.168.2.102
RB	router	192.168.2.1

CONFIGURAZIONE HOST

Il testo seguente rappresenta la configurazione dell'host 24

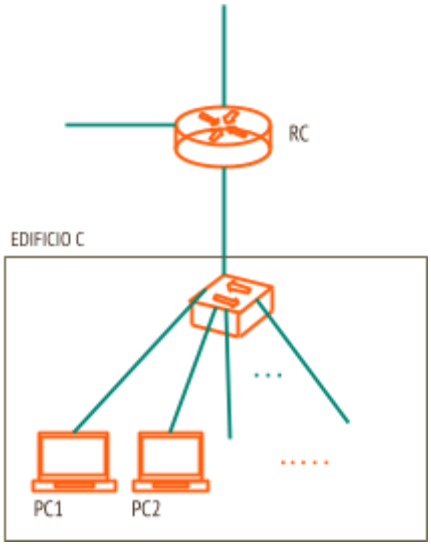
```
set pcname PCB24
ip 192.168.2.24/24 192.168.2.1
ip dns 192.168.1.200
```

CONFIGURAZIONE ROUTER

```
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.69.2 255.255.255.252
interface FastEthernet1/0
 ip address 192.168.69.5 255.255.255.252
router rip
 version 2
 network 192.168.2.0
 network 192.168.69.0
 network 192.168.69.4
end

ip domain-lookup
ip name-server 192.168.1.200
```

EDIFICIO C



- **N° Host**: 100
- **Sottorete**: 192.168.3.0/24
- **Collegamenti**: Edificio B, Edificio D

La seguente tabella illustra l'assegnazione degli indirizzi IP

Codice	Tipo Dispositivo	Indirizzo IP
PCC1	host	192.168.3.2
	.....	....
PCC100	host	192.168.3.102
RC	router	192.168.3.1

CONFIGURAZIONE HOST

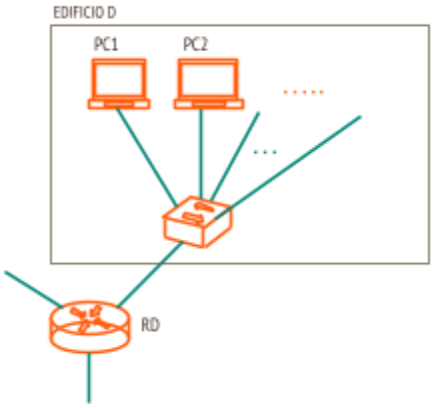
Il testo seguente rappresenta la configurazione dell'host 24

```
set pcname PCC24
ip 192.168.3.24/24 192.168.3.1
ip dns 192.168.1.200
```

CONFIGURAZIONE ROUTER

```
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.69.9 255.255.255.252
interface FastEthernet1/0
 ip address 192.168.69.6 255.255.255.252
router rip
 version 2
 network 192.168.3.0
 network 192.168.69.8
 network 192.168.69.4
end
ip domain-lookup
ip name-server 192.168.1.200
```

EDIFICIO D



- **N° Host**: 150
- **Sottorete**: 192.168.4.0/24
- **Collegamenti**: Edificio A, Edificio C, Edificio E

La seguente tabella illustra l'assegnazione degli indirizzi IP

Codice	Tipo Dispositivo	Indirizzo IP
PCD1	host	192.168.4.2
	.....	....
PCD150	host	192.168.4.152
RD	router	192.168.4.1

CONFIGURAZIONE HOST

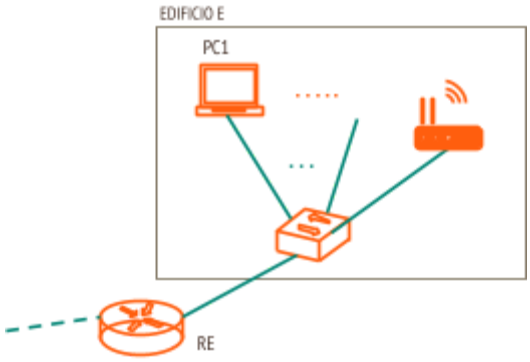
Il testo seguente rappresenta la configurazione dell'host 24

```
set pcname PCD24
ip 192.168.4.24/24 192.168.4.1
ip dns 192.168.1.200
```

CONFIGURAZIONE ROUTER

```
interface FastEthernet0/0
 ip address 192.168.4.1 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.69.10 255.255.255.252
interface FastEthernet1/0
 ip address 192.168.69.18 255.255.255.252
interface FastEthernet1/1
 ip address 192.168.69.33 255.255.255.252
router rip
 version 2
 network 192.168.4.0
 network 192.168.69.8
 network 192.168.69.32
 network 192.168.69.16
end
ip domain-lookup
ip name-server 192.168.1.200
```

EDIFICIO E



- **N° Host**: 50
- **Sottorete**: 192.168.5.0/24
- **Collegamenti**: Edificio D

La seguente tabella illustra l'assegnazione degli indirizzi IP

Codice	Tipo Dispositivo	Indirizzo IP
PCE1	host	192.168.5.2
	.....	....
PCE50	host	192.168.5.102
RE	router	192.168.5.1

CONFIGURAZIONE HOST

Il testo seguente rappresenta la configurazione dell'host 24

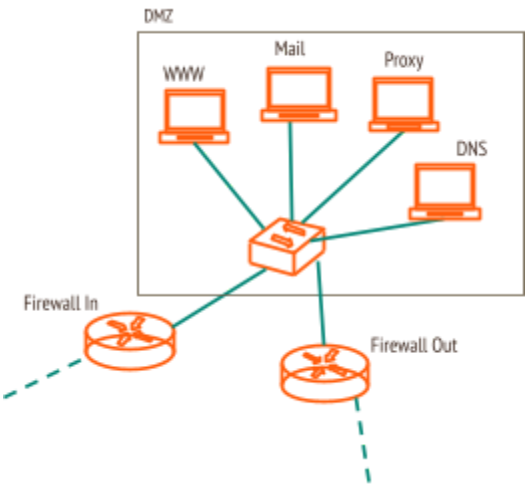
```
set pcname PCE24
ip 192.168.5.24/24 192.168.5.1
ip dns 192.168.1.200
```

```
set pcname PCWIFI
ip dhcp
```

CONFIGURAZIONE ROUTER

```
interface FastEthernet0/0
 ip address 192.168.5.1 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.69.34 255.255.255.252
router rip
 version 2
 network 192.168.5.0
 network 192.168.69.32
end
service dhcp
 ip dhcp excluded-address 192.168.5.1 192.168.5.52
 ip dhcp pool reteE
 network 192.168.5.0 255.255.255.0
 defaulf-router 192.168.5.1
 dns-server 192.168.1.200
 lease 2
exit
ip domain-lookup
ip name-server 192.168.1.200
```

DMZ



- **N° Host**: 5
- **Sottorete**: 192.168.35.0/24
- **Collegamenti**: Firewall In, Firewall Out

La seguente tabella illustra l'assegnazione degli indirizzi IP

Codice	Tipo Dispositivo	Indirizzo IP
DNS	server	192.168.35.10
Mail	server	192.168.35.11
Proxy	server	192.168.35.14
Web	server	192.168.35.12
Firewall Out	router-firewall	192.168.35.1
Firewall In	router-firewall	192.168.35.2

CONFIGURAZIONE DNS

```
set pcname DNS
ip 192.168.35.10/24 192.168.35.1
```

CONFIGURAZIONE MAIL

```
set pcname mail
ip 192.168.35.11/24 192.168.35.1
ip dns 192.168.35.10
```

CONFIGURAZIONE PROXY

```
set pcname proxy
ip 192.168.35.14/24 192.168.35.1
ip dns 192.168.35.10
```

CONFIGURAZIONE WEB SERVER

```
set pcname www
ip 192.168.35.12/24 192.168.35.1
ip dns 192.168.35.10
```

CONFIGURAZIONE ROUTER-FIREWALL

File **firewall In**

```
interface FastEthernet0/0
 ip address 192.168.35.2 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.69.65 255.255.255.252
router rip
 version 2
 network 192.168.35.0
 network 192.168.69.64
end
ip domain-lookup
ip name-server 192.168.1.200
```

File **firewall Out**

```
interface FastEthernet0/0
 ip address 192.168.35.1 255.255.255.0
interface FastEthernet0/1
 ip address dhcp

router rip
 version 2
 network 192.168.35.0
 network 0.0.0.0
 default-information originate
end

ip domain-lookup
ip name-server 192.168.35.10
```

Configurazione Server DNS

DNS INTERNO

File resolv.conf

```
domain osvaldoindustries.it
search osvaldoindustries.it

# DNS Interno
nameserver 192.168.1.200

# DNS DMZ
nameserver 192.168.35.10

# Cloudflare DNS
nameserver 1.1.1.1
nameserver 1.0.0.1
```

File named.conf

```
// Master
// DNS2 e' master per la rete A
zone "reteA.osvaldoindustries.it" {
     type master;
     file "/etc/bind/retea.osvaldoindustries.it.db";
};
zone "1.168.192.in-addr.arpa" {
     type master;
     file "/etc/bind/1.168.192.in-addr.arpa.db";
};

// Slave
zone "osvaldoindustries.it" {
     type slave;
     file "/etc/bind/osvaldoindustries.it.bk";
     masters { 192.168.35.10; };
};
zone "168.192.in-addr.arpa" {
     type slave;
     file "/etc/bind/168.192.in-addr.arpa.bk";
     masters { 192.168.35.10; };
};

// DMZ
zone "dmz.osvaldoindustries.it" {
     type slave;
     file "/etc/bind/dmz.osvaldoindustries.it.bk";
     masters { 192.168.35.10; };
};
zone "35.168.192.in-addr.arpa" {
     type slave;
     file "/etc/bind/35.168.192.in-addr.arpa.bk";
     masters { 192.168.35.10; };
};
```

File named.conf.option

```
acl "trusted-nameservers" {
     localhost;
     192.168.1.200;
     192.168.35.10;
};

acl "trusted-networks" {
     localhost;
     192.168.1.0/24;
     192.168.2.0/24;
     192.166.3.0/24;
     192.168.4.0/24;
     192.168.5.0/24;
     192.168.35.0/24;
};

options {
     directory "/var/cache/bind";
     dnssec-validation auto;
     auth-nxdomain no;
     version "Not disclosed";
     notify yes;
     allow-transfer { trusted-nameservers; };
     allow-query { trusted-networks; };
     forwarders { 1.1.1.1; };
     recursion yes;
};
```

File reteA.osvaldoindustries.it.db

```
$TTL 86400
$ORIGIN reteA.osvaldoindustries.it.
@ IN SOA dns.reteA.osvaldoindustries.it. root.reteA.osvaldoindustries.it. (
     2018112701 ; serial
     43200 ; refresh
     3600 ; retry after 1 hour
     3600000 ; expire after 1000 hours
     2592000 ; default ttl
)

; Definizione dei nameserver e dei server mail
IN NS dns.dmz.osvaldoindustries.it.
IN NS dns.reteA.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.osvaldoindustries.it.

; Host di Rete A
ra IN A 192.168.1.1
dns IN A 192.168.1.200
appazz IN A 192.168.1.201
backup IN A 192.168.1.202
```

File 1.168.192.in-addr.arpa.db

```
$TTL 86400
$ORIGIN 1.168.192.in-addr.arpa.
@ IN SOA dns.reteA.osvaldoindustries.it. root.reteA.osvaldoindustries.it. (
     2018112701 ; serial
     43200 ; refresh
     3600 ; retry after 1 hour
     3600000 ; expire after 1000 hours
     2592000 ; default ttl
)

; Definizione dei nameserver e dei server mail
IN NS dns.dmz.osvaldoindustries.it.
IN NS dns.reteA.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.osvaldoindustries.it.

; Host in rete2.osvaldoindustries.it
1 IN PTR ra.reteA.osvaldoindustries.it.
200 IN PTR dns.reteA.osvaldoindustries.it.
201 IN PTR appazz.reteA.osvaldoindustries.it.
202 IN PTR backup.reteA.osvaldoindustries.it.
```

DNS DMZ

File **resolv.conf**

```
domain osvaldoindustries.it
search osvaldoindustries.it

nameserver 192.168.35.10

nameserver 1.1.1.1
nameserver 1.0.0.1
```

File **named.conf**

```
// Master

zone "osvaldoindustries.it" {
     type master;
     file "/etc/bind/osvaldoindustires.it.db";
};

zone "168.192.in-addr.arpa" {
     type master;
     file "/etc/bind/168.192.in-adr.arpa.db";
};

// DMZ

zone "dmz.osvaldoindustries.it" {
     type master;
     file "/etc/bind/dmz.osvladoindustries.it.db";
};

zone "35.1168.192.in-addr.arpa" {
     type master;
     file "/etc/bind/35.168.192.in-addr.arpa.db";
};
```

File named.conf.option

```
acl "trusted-nameservers" {
     localhost;
     192.168.35.10;
     192.169.1.200;
};

acl "trusted-networks" {
     localhost;
     192.168.35.0/24;
     192.168.1.0/24;
};




options {
     directory "/var/cache/bind";
     dnssec-validation auto;
     auth-nxdomain no;
     version "Not disclosed";
     notify yes;
     allow-transfer { trusted-nameservers; };
     allow-query { "any"; };
     forwarders { 1.1.1.1; };
     recursion yes;
     allow-recursion {any;};
};
```

File dmz.osvaldoindustries.it.db

```
$TTL 86400
$ORIGIN dmz.osvaldoindustries.it.
@ IN SOA dns.dmz.osvaldoindustries.it. root.dmz.osvaldoindustries.it. (
     2018112903 ; serial
     43200 ; refresh
     3600 ; retry after 1 hour
     3600000 ; expire after 1000 hours
     2592000 ; default ttl
)

; Definizione dei nameserver e dei server mail
IN NS dns.dmz.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.dmz.osvaldoindustries.it.

; Host della DMZ
firewallout IN A 192.168.35.1
dns IN A 192.168.35.10
www IN A 192.168.35.12
mail IN A 192.168.35.11
proxy IN A 192.168.35.14
```

File **osvaldoindustries.it.db**

```
$TTL 86400
$ORIGIN osvaldoindustries.it.
@ IN SOA dns.osvaldoindustries.it. root.osvaldoindustries.it. (
     2018112902 ; serial
     43200 ; refresh
     3600 ; retry after 1 hour
     3600000 ; expire after 1000 hours
     2592000 ; default ttl
)

; Definizione dei nameserver e dei server mail
IN NS dns.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.osvaldoindustries.it.

; Sottodomini
dmz IN A 198.168.35.0


; Host
mail IN A 198.168.35.11
dns IN A 198.168.35.10
@ IN A 192.168.35.12
www IN CNAME @
proxy IN A 198.168.35.14
```

File **168.192.in-addr.arpa.db**

```
$TTL 86400
$ORIGIN 168.192.in-addr.arpa.
@ IN SOA dns.osvaldoindustries.it. root.dmz.osvaldoindustries.it. (
     2018112902 ; serial
     43200 ; refresh
     3600 ; retry after 1 hour
     3600000 ; expire after 1000 hours
     2592000 ; default ttl
)

; Definizione dei nameserver e dei server mail
IN NS dns.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.osvaldoindustries.it.

; Sottodomini
0.35 IN PTR dmz.osvaldoindustries.it.


; Host
11.35 IN PTR mail.osvaldoindustries.it.
10.35 IN PTR dns.osvaldoindustries.it.
12.35 IN PTR www.osvaldoindustries.it.
14.35 IN PTR proxy.osvaldoindustries.it.
```

File 35.168.192.in-addr.arpa.db

```
$TTL 86400
$ORIGIN 35.168.192.in-addr.arpa.
@ IN SOA dns.dmz.osvaldoindustries.it. root.dmz.osvaldoindustries.it. (
     2018112903 ; serial
     43200 ; refresh
     3600 ; retry after 1 hour
     3600000 ; expire after 1000 hours
     2592000 ; default ttl
)

; Definizione dei nameserver e dei server mail
IN NS dns.dmz.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.dmz.osvaldoindustries.it.

; Host
1 IN PTR firewallout.dmz.osvaldoindustries.it.
11 IN PTR mail.dmz.osvaldoindustries.it.
10 IN PTR dns.dmz.osvaldoindustries.it.
12 IN PTR www.dmz.osvaldoindustries.it.
14 IN PTR proxy.dmz.osvaldoindustries.it.
```

Configurazione Mail Server

File /etc/mail/access

```
Connect:192.168
GreetPause:192.168
ClientRate:192.168
ClientConn:192.168

REE.STEALTH.MAILER@ REJECT
VIRUS.BANK.MAILER@ REJECT
bounce-special_offer-754905@active.lyris.net REJECT
bounce-special-offer-754905@active.lyris.net REJECT
britneyspearsnude23232@yahoo.com REJECT
bungee369@pacbell.net REJECT
CamCinema@aol.com REJECT
capnet002@excite.com REJECT
casinofdaf6@hotmail.com REJECT
cherryzh@china.com REJECT
con240@pchome.com.tw REJECT
corn441962@catchaplane.net REJECT
osvaldoindustries.it RELAY
192.168 RELAY
```

File /etc/mail/aliases

```
postmaster: sergio
admin: sergio, osvaldo
dmz: dmzgod
dmzgod: damiano, valentina
```

File /etc/mail/local-host-names

```
localhost
mail.osvaldoindustries.it
osvaldoindustries.it
dmz.osvaldoinudstries.it
```

Creazione Utenti

```
useradd --create-home -s /sbin/nologin sergio; passwd sergio
useradd --create-home -s /sbin/nologin osvaldo; passwd osvaldo
useradd --create-home -s /sbin/nologin damiano; passwd damiano
useradd --create-home -s /sbin/nologin valentina; passwd valentina
```

File /etc/mail/sendmail.mc

```
# la riga "DAEMON_OPTIONS('Family=inet, Name=MTA-v4, Port=smtp,
Addr=127.0.0.1')dnl" va sostituita con:

DAEMON_OPTIONS(`Family=inet, Name=MTA-v4, Port=smtp')dnl

# Dopo l'ultimo include del file aggiungiamo

FEATURE(`relay_entire_domain')dnl
```

File /etc/mail/virtusertable

```
osvaldo@osvaldoindustries.it osvaldo
sergio@osvaldoindustries.it sergio
damiano@osvaldoindustries.it damiano
valentina@osvaldoindustires.it valentina
postmaster@osvaldoindustries.it postmaster
admin@osvaldoindustires.it admin
dmz@osvaldoindustries.it dmz
```

Configurazione Firewall

Per la configurazione del firewall abbiamo pensato che la filosofia migliore da applicare fosse la **default deny** in quanto tutto quello che non è espressamente ammesso è proibito, con questo tipo di filosofia gli utenti sono molto ristretti e non possono facilmente rompere la policy di sicurezza.

CONFIGURAZIONE FIREWALL IN

```
# clear chain
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 192.168.35.10 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.10 --dport 53 -j ACCEPT

# Smtp, POP3, IMAP

iptables -A FORWARD -p tcp -d 192.168.35.11 --dport 25 -m limit 100/s -j
ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.11 --dport 110 -m limit 100/s -j
ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.11 --dport 143 -m limit 100/s -j
ACCEPT

# HTTP, HTTPS

iptables -A FORWARD -p tcp -d 192.168.35.14 --dport 80 -m limit 100/s -j
ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.12 --dport 443 -m limit 100/s -j
ACCEPT

iptables -A OUTPUT -m state --state ESTABISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

CONFIGURAZIONE FIREWALL OUT

```
# clear chain
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT

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

# allow SMPT, POP3, IMAP, DNS, HTTPS, HTTP

iptables -A FORWARD -p tcp -d 192.168.35.11 --dport 25 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.11 --dport 110 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.11 --dport 143 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.10 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -d 192.168.35.10 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.12 --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.35.14 --dport 80 -j ACCEPT

iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT
iptables -A FORWARD -p tcp -j REJECT --reject-with tcp-reset

# Redirezione pacchetti mail
iptables -t NAT -A PREROUTING -p tcp --dport 25 -j DNAT --to-destination
198.168.35.11

# Redirezione pacchetti DNS
iptables -t NAT -A PREROUTING -p udp --dport 53 -j DNAT --to-destination
198.168.35.10
iptables -t NAT -A PREROUTING -p tcp --dport 53 -j DNAT --to-destination
198.168.35.10

# Redirezione pacchetti Proxy
iptables -t NAT -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
198.168.35.14

# Redirezione pacchetti Web
iptables -t NAT -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination
198.168.35.12

# Mascheramento ip dei pacchetti uscenti
iptables -t NAT -A POSTROUTING -o eth1 -j MASQUERADE
```

Tecniche di sicurezza adottate

Monitoraggio Rete

Per il monitoraggio dell'intera rete utilizzeremo il seguente software: **OpenNMS**.
E' un'applicazione di gestione della rete di livello aziendale completamente **open source** che offre funzionalità di rilevamento automatizzato, gestione di eventi e notifiche, misurazione delle prestazioni e garanzia del servizio. Include un'app client per smartphone che consente l'accesso in movimento, dando la possibilità di visualizzare interruzioni, nodi, allarmi e aggiungere un'interfaccia per il monitoraggio anche da remoto.

Protezione Server Backup

Il server di Backup verrà posto, come gli altri server presenti nell'edificio A, in una stanza apposita con un elevato sistema di sicurezza e di protezione. In questa stanza potranno accedervi solo gli utenti autorizzati: l'amministratore del sistema e i pochi tecnici incaricati della manutenzione.
Sarà dotata di un sistema anti-incendio all'avanguardia, di un sistema di refrigerazione consono per mantenere una temperatura ideale evitando surriscaldamenti che potrebbero inficiare sulle prestazioni e sull'integrità del server, un sistema di sorveglianza e di un allarme anti-intrusione.

Quando un Hard Disk presenterà segni di malfunzionamento, il tecnico incaricato si preoccuperà di sostituirlo per poi smagnetizzarlo e distruggerlo tramite l'apposita macchina.

Protezione DMZ

I server della DMZ verranno posti in una sala appositamente adibita nel piano interrato dell'edificio D. A questa stanza vi avranno accesso solo l'admin e i pochi tecnici autorizzati.
Sarà dotata di un sistema anti-incendio, un sistema di raffreddamento adeguato per evitare surriscaldamenti e malfunzionamenti dei vari server, un sistema di sorveglianza e un allarme anti-intrusione.

Quando un Hard Disk presenterà segni di malfunzionamento, il tecnico incaricato lo sostituirà, per poi smagnetizzarlo e distruggerlo tramite l'apposita macchina.

Preventivo di spesa

Componente	Quantità	Prezzo unitario	Prezzo totale
Cavo Fibra Ottica Multimodale	2.600 m	€ 2,50/m	€ 6.500,00
Cavo STP	500 m	€ 1,00/m	€ 500,00
Cavo UTP	200 m	€ 0,50/m	€ 100,00
Router	8 pz	€ 120,00/pz	€ 960,00
Switch	135 pz	€ 20,00/pz	€ 2.700,00
Access Point	2 pz	€ 93,50/pz	€ 187,00
Firewall	2 pz	€ 650,00/pz	€ 1.300,00
Dominio	-	€ 12,00/anno	-
Progettazione	50 h (5 h * 10 gg)	€ 22,00/ora	€ 1.100,00
Istallazione	120 h (8 h * 15 gg)	€ 40,00/ora	€ 4.800,00
			TOT: € 18.147,00