PROGETTO - RETI CALCOLATORI: PROTOCOLLI

OSVALDO INDUSTRIES

STUDENTI:

Maria Riommi

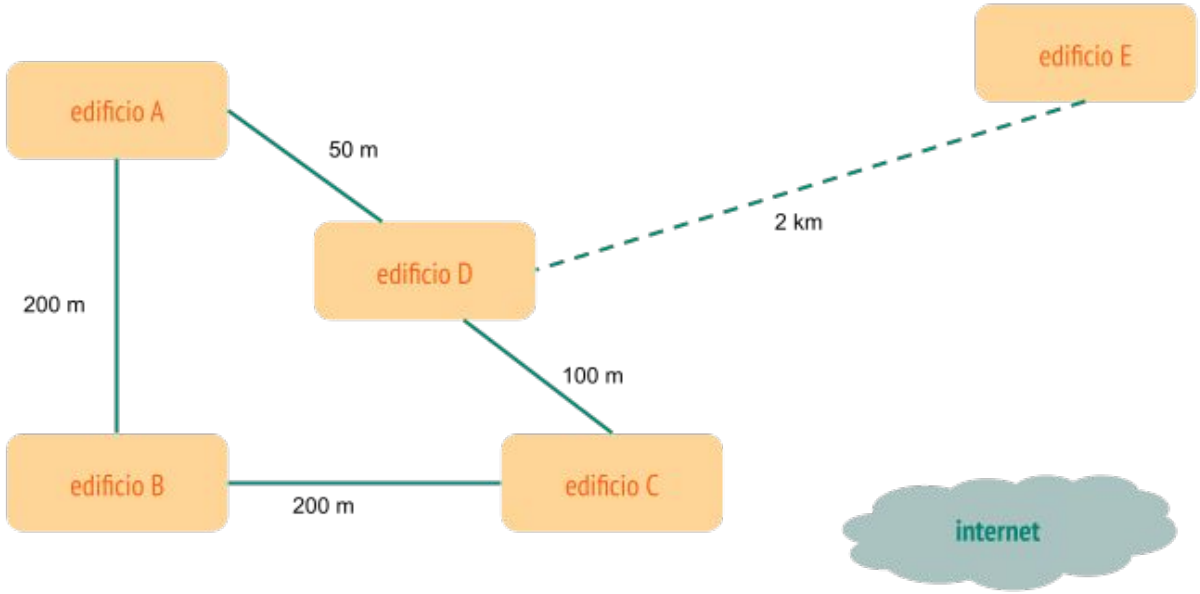
Nicolò Vescera

DIPARTIMENTO DI MATEMATICA E INFORMATICA

A.D. 1308 unipg UNIVERSITÀ DEGLI STUDI DI PERUGIA

DESCRIZIONE DEL PROGETTO

La ditta Osvaldo Industry 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:



DESCRIZIONE DEL PROGETTO

ABOUT OSVALDO INDUSTRIES ENTERPRISE

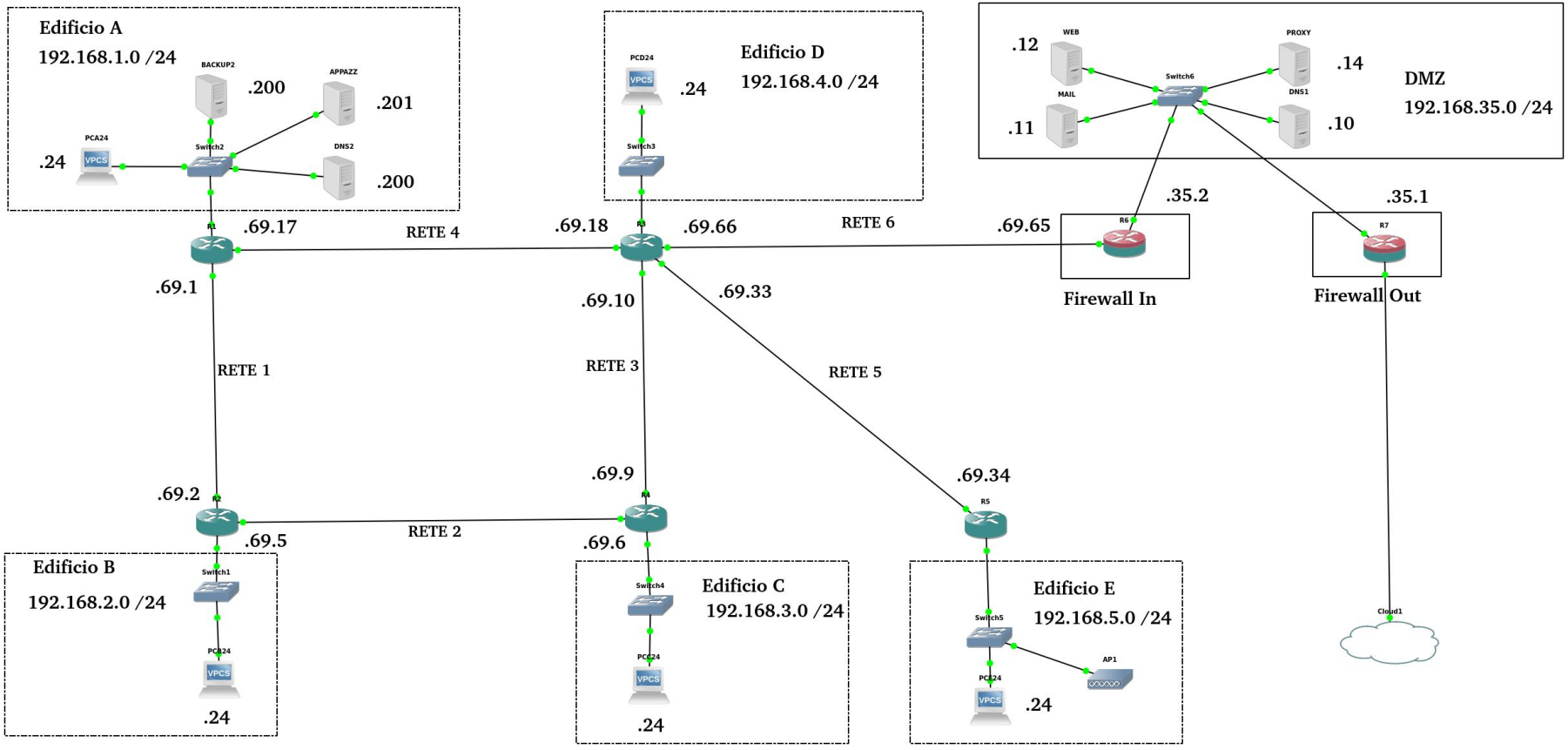
La Osvaldo Industries Entreprise è l'Azienda **leader** nel settore **E-LEARNING** in Italia.
Ha spopolato grazie a vari software per semplificare la Didattica a Distanza (**DaD**) in modo da rendere la vita migliore sia agli studenti che ai docenti di tutti gli ordini e gradi.

Questa azienda pone al centro della sua attività la **Sicurezza dei Dati** dei suoi utenti rispettando a pieno il Regolamento Generale per la Protezione dei Dati Personali (**GDPR**).

La O.I.E è completamente proiettata nel mondo **OpenSoruce** e predilige e sviluppa software che rispettano tale filosofia.

O.I.E
Osvaldo Industires Enterpise

SCHEMA DELLA RETE SU GNS3



STRUTTURA FISICA

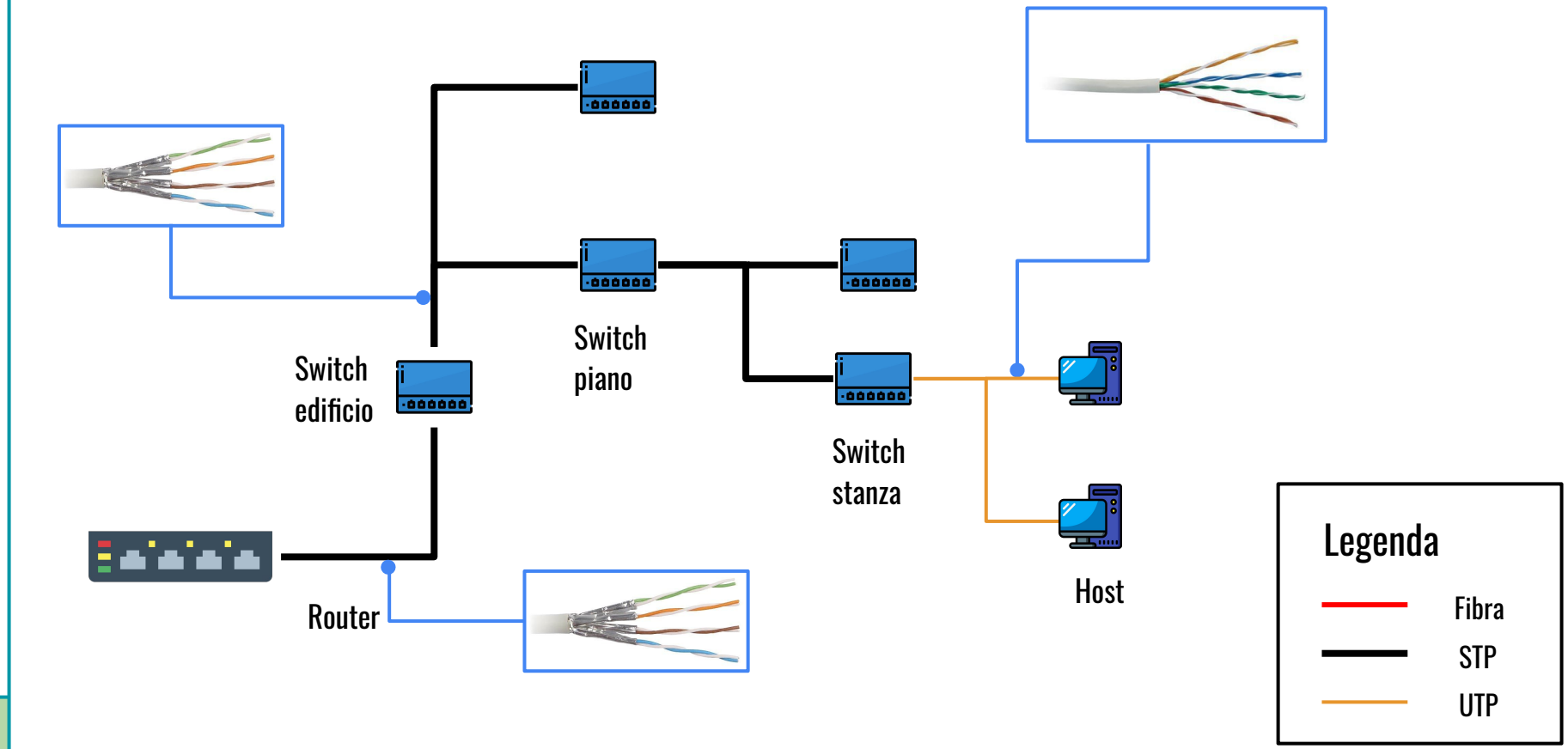
STRUTTURA FISICA

L'Azienda sarà formata da 5 edifici che verranno rinominati con le lettere dell'alfabeto e saranno così strutturati:

Edificio	Piani	Stanze	Utenti per Stanza
A	5	4	5
B	5	4	5
C	5	4	5
D	7	5	5
E	2	5	5

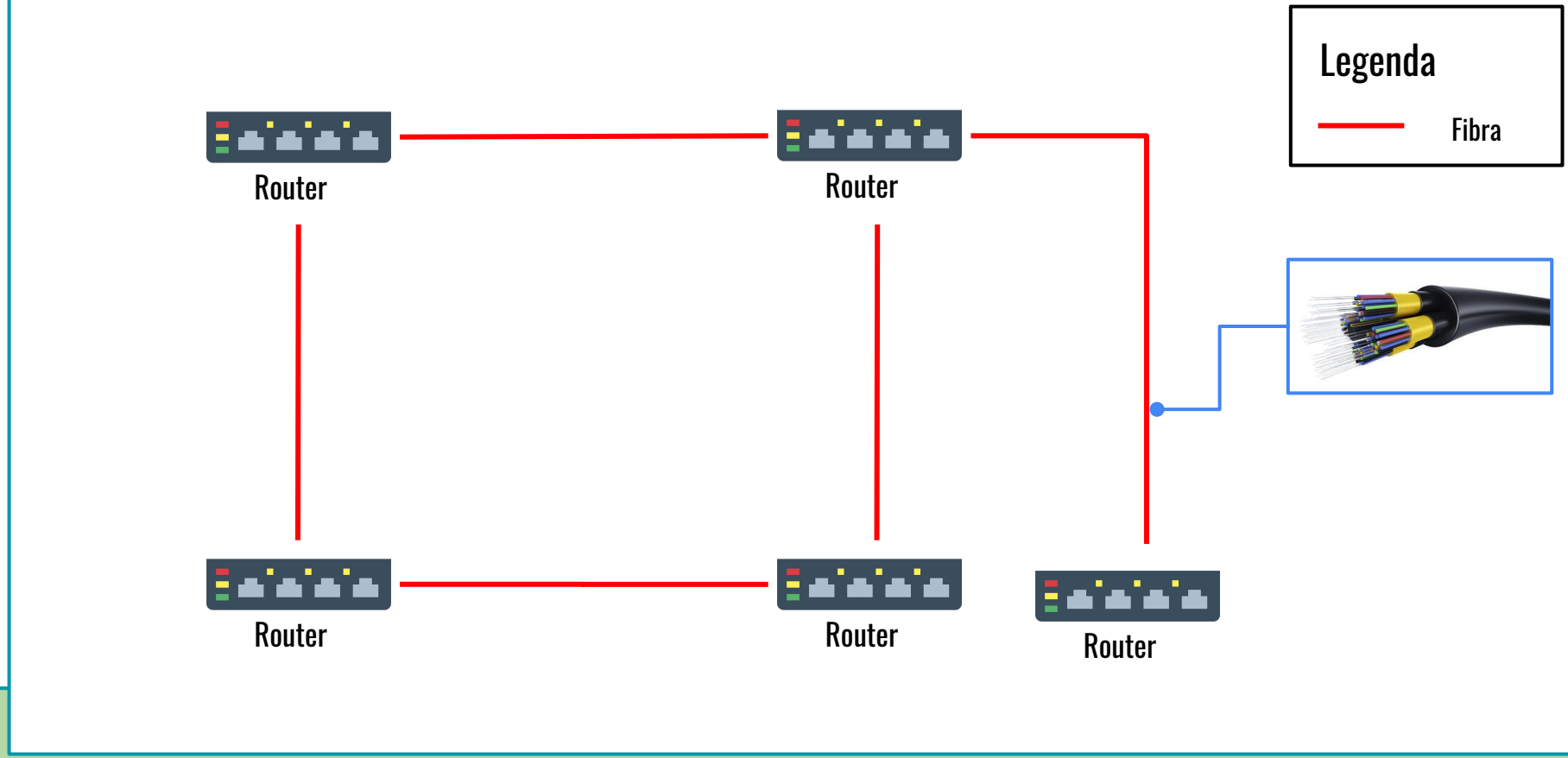
STRUTTURA FISICA

CABLAGGIO STRUTTURATO



STRUTTURA FISICA

CABLAGGIO STRUTTURATO



STRUTTURA LOGICA

STRUTTURA LOGICA

IP EDIFICI

Gli Edifici avranno un indirizzo IP di classe C e saranno assegnati come illustrato nella seguente tabella:

Edificio	Rete	Subnet mask
A	192.168.1.0	255.255.255.0 (/24)
B	192.168.2.0	255.255.255.0 (/24)
C	192.168.3.0	255.255.255.0 (/24)
D	192.168.4.0	255.255.255.0 (/24)
E	192.168.5.0	255.255.255.0 (/24)
DMZ	192.168.35.0	255.255.255.0 (/24)

STRUTTURA LOGICA

IP Router - Router

Per connettere i Router tra di loro è stato scelto l'indirizzo IP 192.168.69.0.
Utilizzando la subnet mask 255.255.255.252 (/30) otteniamo sottoreti con un massimo di 2 host in modo tale da evitare il più possibile spreco di indirizzi.

Router - Router	Rete	Subnet mask
A - B	192.168.69.0	255.255.255.252 (/30)
B - C	192.168.69.4	255.255.255.252 (/30)
C - D	192.168.69.8	255.255.255.252 (/30)
D - A	192.168.69.16	255.255.255.252 (/30)
D - E	192.168.69.32	255.255.255.252 (/30)
D - Firewall In	192.168.69.64	255.255.255.252 (/30)

STRUTTURA LOGICA

CONVENZIONI

Per la realizzazione della struttura logica abbiamo seguito le seguenti convenzioni:

Switch:

- 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.

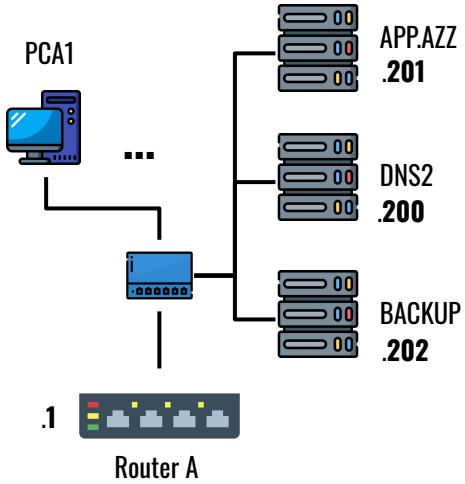
Router:

- 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 sarà **RIP_v2**.

CONFIGURAZIONE EDIFICI

EDIFICIO A

192.168.1.0 /24



L'**Edificio A** è strutturato in 5 piani con 4 stanze ciascuno le quali ospiteranno 5 utenti.

In particolare il **piano sotterraneo** verrà riservato per i **Server** a cui potranno accedervi solo gli utenti della Rete Aziendale.

Il Router di questo edificio sarà connesso direttamente a quelli dell'**Edificio B e D**

EDIFICIO A

CONFIGURAZIONE HOST

Configurazione dell'host PCA24

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

EDIFICIO A

CONFIGURAZIONE ROUTER

```
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.69.1 255.255.255.252
interface FastEthernet1/0
 ip address 192.168.69.17 255.255.255.252
router rip
 version 2
 network 192.168.1.0
 network 192.168.69.0
 network 192.168.69.16
end

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

EDIFICIO A

CONFIGURAZIONE SERVER

Configurazione Server Backup

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

Configurazione Server DNS Interno

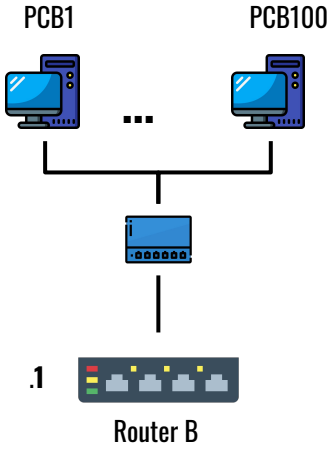
```
set pcname DNS2
ip 192.168.1.200/24 192.168.1.1
```

Configurazione Server Applicazioni Aziendali

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

EDIFICI B, C, E

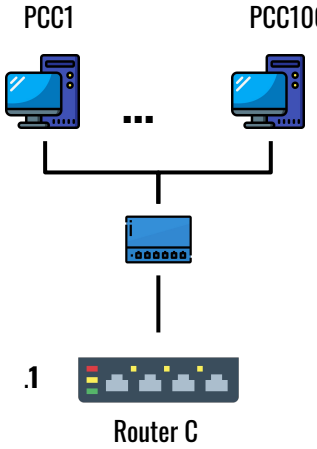
192.168.2.0 /24



L'**Edificio B** è strutturato in 5 piani con 4 stanze ciascuno le quali ospiteranno 5 utenti.

Il Router di questo edificio sarà connesso direttamente a quelli dell'**Edificio A e C**

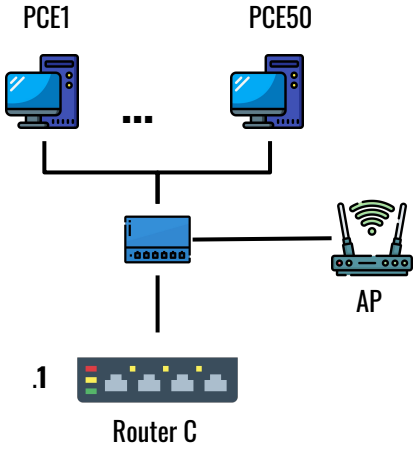
192.168.3.0 /24



L'**Edificio C** è strutturato in 5 piani con 4 stanze ciascuno le quali ospiteranno 5 utenti.

Il Router di questo edificio sarà connesso direttamente a quelli dell'**Edificio B e D**

192.168.5.0 /24



L'**Edificio E** è strutturato in 5 piani con 4 stanze ciascuno le quali ospiteranno 5 utenti.

Il Router di questo edificio sarà connesso direttamente a quelli dell'**Edificio D.**

EDIFICI B, C, E

CONFIGURAZIONE HOST

Configurazione dell'host PCB24

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

Configurazione dell'host PCC24

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

Configurazione dell'host PCE24

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

```
set pcname PCWIFI
ip dhcp
```

EDIFICI B e C

CONFIGURAZIONE ROUTER B e C

Configurazione Router B

```
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 Router C

```
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
```

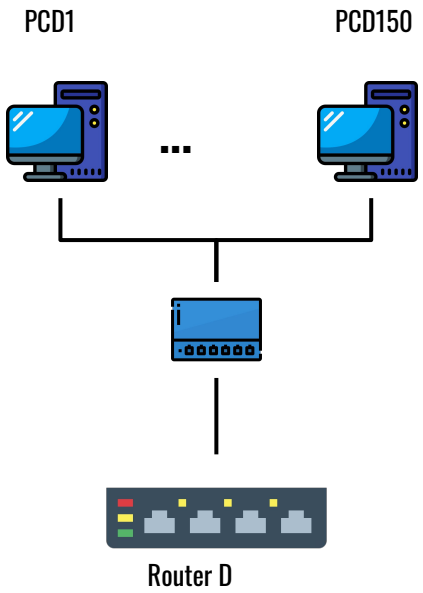
EDIFICIO E

CONFIGURAZIONE ROUTER E

```
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
```

EDIFICIO D

192.168.4.0 /24



L'**Edificio D** è strutturato in 5 piani con 4 stanze ciascuno le quali ospiteranno 5 utenti.

In particolare il **piano sotterraneo** verrà riservato ai **Server** presenti nella **DMZ**.

Il Router di questo edificio sarà connesso direttamente a quelli dell'**Edificio A, C e E**

EDIFICIO D

CONFIGURAZIONE HOST

Configurazione dell'host PCD24

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

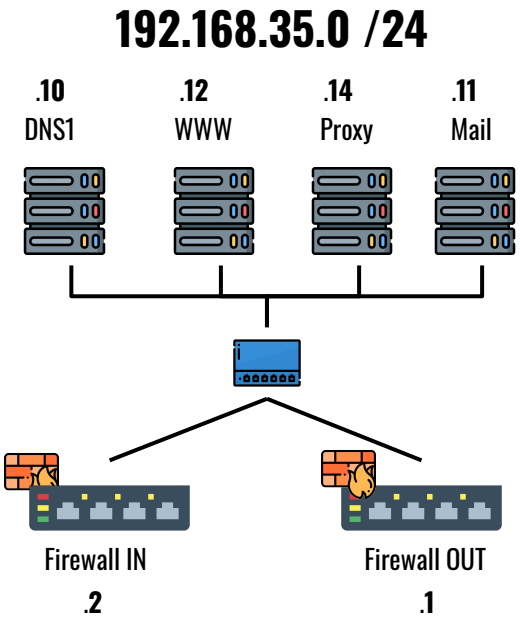
EDIFICIO D

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 D

DMZ



La **De-Militarized Zone** conterrà tutti i server accessibili solo dall'esterno.

Una struttura di questo tipo viene realizzata inserendo due **Firewall-Router** uno esterno ed uno interno.

DMZ

CONFIGURAZIONE SERVER

Configurazione Server DNS1

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

Configurazione Server Mail

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

Configurazione Server Proxy

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

Configurazione Server Web

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

DMZ

CONFIGURAZIONE ROUTER

Configurazione 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
```

Configurazione 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 DNS

CONFIGURAZIONE DNS INTERNO

Il DNS Interno (DNS2) si occuperà di gestire i nomi della Rete A e sarà il DNS a cui tutti gli host della Rete Aziendale interna faranno riferimento.

```
// Master
zone "reteA.osvaldoindustries.it" {
      type master;
      file "/etc/bind/retea.osvaldoindustries.it.db";
};
```

named.conf

Si appoggerà al DNS Esterno (DNS1) per risolvere i nomi dei Server posti all'interno della DMZ.

```
// Slave
zone "dmz.osvaldoindustries.it" {
      type slave;
      file "/etc/bind/dmz.osvaldoindustries.it.bk";
      masters { 192.168.35.10; };
};
```

named.conf

CONFIGURAZIONE DNS

CONFIGURAZIONE DNS INTERNO

Verranno definiti i namserver nel seguente modo:

```
IN NS dns.dmz.osvaldoindustries.it.
IN NS dns.reteA.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.osvaldoindustries.it.
```

Di seguito le configurazioni per la risoluzione Diretta e la risoluzione Inversa:

```
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
```

reteA.osvaldoindustries.it.db

```
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.
```

1.168.192.in-addr.arpa.db

CONFIGURAZIONE DNS

CONFIGURAZIONE DNS DMZ

Il DNS DMZ (DNS1) si occuperà di gestire solo i nomi dei server presenti all'interno della De-Militarized Zone.

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

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

named.conf

CONFIGURAZIONE DNS

CONFIGURAZIONE DNS DMZ

Verranno definiti i namserver nel seguente modo:

```
IN NS dns.osvaldoindustries.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.osvaldoindustries.it.
```

Di seguito le configurazioni per la risoluzione Diretta:

```
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
```

dmz.osvaldoindustries.it.db

```
; Sottodomini
dmz IN A 198.168.35.0

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
```

osvaldoindustries.it.db

CONFIGURAZIONE DNS

CONFIGURAZIONE DNS DMZ

Di seguito le configurazioni per la risoluzione Inversa:

```
; 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.
```

168.192.in-addr.arpa.db

```
; 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.
```

35.168.192.in-addr.arpa.db

CONFIGURAZIONE MAIL SERVER

CONFIGURAZIONE MAIL SERVER

La **Osvaldo Industries** è particolarmente attenta alla sicurezza dei suoi dipendenti !
In particolare con la seguente configurazione vengono ignorati tutti i tentativi di spam provenienti dai seguenti indirizzi:

```
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
…
```

/etc/mail/access

CONFIGURAZIONE MAIL SERVER

Con la seguente configurazione vengono definiti gli alias

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

/etc/mail/aliases

mentre con il seguente file si specifica la lista degli host per i quali sendmail accetta posta

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

/etc/mail/local-host-names

CONFIGURAZIONE MAIL SERVER

Con i seguenti comandi verranno creati alcuni utenti a cui verranno assegnate le mail personali:

```
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
```

```
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 dmzz
```

/etc/mail/virtusertable

Infine verranno applicate le seguenti modifiche per abilitare la ricezione delle email anche da altri host:

```
# 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
```

/etc/mail/sendmail.mc

CONFIGURAZIONE FIREWALL

CONFIGURAZIONE FIREWALL

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.

Verrà applicata una filosofia di **Default Deny** per garantire una sicurezza elevata in quanto tutto quello che non è esplicitamente consentito sarà automaticamente negato.

Lo strumento software che andremo ad utilizzare sarà **iptables**.

```
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

CONFIGURAZIONE FIREWALL

CONFIGURAZIONE FIREWALL IN

Regole per 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
```

Regole per Mail:

```
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
```

Regole per Web e Proxy:

```
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
```

Regole per connessioni già stabilite:

```
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

CONFIGURAZIONE FIREWALL OUT

Regole per DNS, Mail, Proxy e Web:

```
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
```

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
```

Regole per NAT:

```
iptables -t NAT -A PREROUTING -p tcp --dport 25 -j DNAT --to-destination 198.168.35.11
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
iptables -t NAT -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 198.168.35.14
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
```

SICUREZZA

TECNICHE DI SICUREZZA ADOTTATE

Monitoraggio Rete

Per il monitoraggio dell'intera rete utilizzeremo il seguente software: **OpenNMS**.

Sicurezza dei Server

- posti in una sala appositamente adibita nel piano interrato
- Accesso esclusivo per l'admin e tecnici autorizzati.
- Sistema anti-incendio,
- Sistema di raffreddamento adeguato
- Sistema di sorveglianza
- Allarme anti-intrusione.
- HD Care

Server BackUp

- Funzionamento notturno

PROGETTO - RETI CALCOLATORI: PROTOCOLLI

FINE