

## PROGETTO – Laboratorio reti



A.D. 1308

**unipg**

UNIVERSITÀ DEGLI STUDI  
DI PERUGIA

# BJ Entertainment

### A cura di:

Andrea Jovani [383259]  
Tommaso Babbuini [384518]

### Docente:

Prof. Sergio Tasso

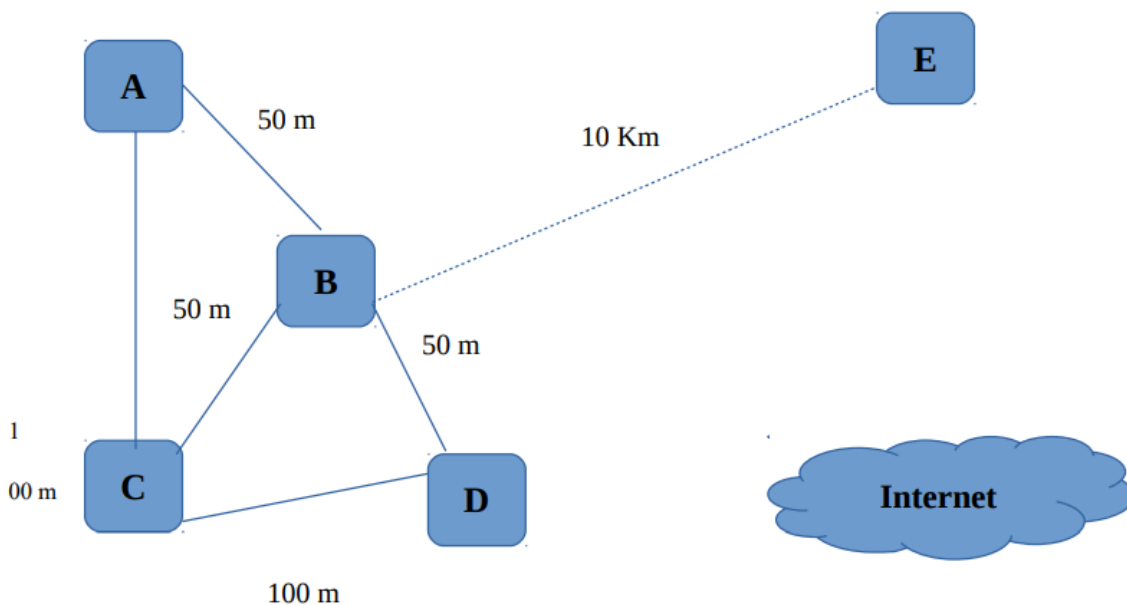
## Indice:

<b>1. Descrizione del progetto</b>	<b>2</b>
1.1. Scenario e obiettivi progettuali	2
1.2. Analisi del progetto	4
<b>2. Progettazione struttura fisica della rete</b>	<b>5</b>
2.1. Struttura e topologia adottata	5
2.2. Cablaggio	5
2.3. Dispositivi usati	6
<b>3. Progettazione logica della rete</b>	<b>7</b>
3.1. Suddivisione delle sottoreti	7
3.2. Importanza delle sottoreti	8
3.3. Indirizzi dei router	8
3.4. Backbone tra router	8
<b>4. Simulazione</b>	<b>9</b>
<b>5. Configurazione interfacce di rete</b>	<b>10</b>
5.1. Configurazione degli host	10
<b>6. Impostazione Routing</b>	<b>16</b>
6.1. Configurazione dei router e protocolli interni	16
6.2. Configurazione rete wireless e DHCP	20
<b>7. Configurazione dei Servizi</b>	<b>21</b>
7.1. Configurazione del server DNS	21
7.2. Configurazione del server di posta elettronica	29
7.3. Configurazione del server Web	30
7.4. Configurazione del server di Backup	32
7.5. Configurazione del server App aziendali	32
<b>8. Firewall e Prevenzione</b>	<b>33</b>
8.1. Configurazione del firewall	33
<b>9. Preventivo</b>	<b>35</b>

# 1. Descrizione del progetto

## 1.1 Scenario e richieste progettuali

La ditta BJ-Entertainment 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:



- Gli edifici sopra rappresentati, hanno le seguenti caratteristiche:

Edifici	Uffici & Reparti	Num. Utenti	Num. Server	Copertura Wi-fi
A	/	100	/	NO
B	/	100	4	NO
C	/	100	3	NO
D	/	100	/	NO
E	/	50	/	SI

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

Server	Numero
Posta elettronica	1
Web	1
DNS	2
Applicazioni aziendali	1
Backup	1

Si richiede pertanto di:

- **Realizzare lo schema fisico della rete**, evidenziando la topologia ed indicando i dispositivi fisici (router, switch, hub, mezzi trasmissivi) da inserire.
- **Realizzare lo schema logico**, evidenziando eventuali suddivisioni della rete in sottoreti.
- **Configurare le interfacce di rete** per tutti i server ed i dispositivi di rete e per almeno un host in ambiente UNIX per ogni rete o sottorete mostrandone tutti i parametri significativi.
- **Impostare il routing** per ogni router interno e di frontiera, riportando eventuali comandi e configurazioni.
- **Configurare dettagliatamente i server DNS e di Posta elettronica.**
- **Implementare e configurare firewall** per la protezione della rete.
- **Indicare quali tecniche si intendono adottare (e come si implementano) per il monitoraggio della rete** al fine di garantire una maggiore sicurezza.
- **Proteggere in maniera particolare il Server di BACKUP.**

## 1.2 Analisi del progetto

Disposizioni generali:

Il numero di utenti massimo possibile è 450, ma l'azienda potrebbe crescere e potenzialmente sarebbe necessario raddoppiare il numero di utenze.

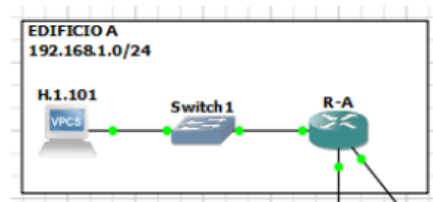
Per rispondere in maniera adeguata alle necessità future ricorriamo ad un ip privato.

Rete: 192.168.X.X

Subnet mask: 255.255.255.0

Per collegare le sedi impieghiamo un router collegato ad uno switch che avrà il compito di dividere la rete tra i vari utenti.

Il tipo di configurazione in figura è la base del resto delle configurazioni per quanto riguarda gli host; verrà usata in tutti gli edifici con piccole variazioni in caso di ulteriori elementi.



L'edificio E avrà una configurazione di un apparecchio wireless (un AP). Sarà indispensabile l'uso di DHCP per gli utenti e i dispositivi che usano quel tipo di connessione.

Le sedi si trovano a breve distanza l'una dall'altra e sono poco numerose, possiamo fare uso di RIP per il routing interno (IGP). Considerando le dimensioni dell'azienda l'utilizzo di RIP è adeguato.

L'accesso alla rete esterna è gestito dall'edificio B che sarà il gateway principale.

In questo modo rendiamo le sedi meno dipendenti possibili l'una dall'altra; l'accesso a risorse esterne e aziendali è centralizzato. La topologia che rispetta meglio le esigenze è a Stella.

La sicurezza è fondamentale per ogni infrastruttura ed, oltre ad una buona configurazione della rete, è necessario usare dei servizi di monitoraggio come Nagios. Per l'accesso a macchine esposte, quali il server web o il server di posta, è indispensabile adottare misure di protezione aggiuntive, come firewall e sistemi di autenticazione robusti.

Il server di Backup lo mettiamo internamente nell'edificio C.

Abbiamo escluso l'edificio E, che ospita la rete Wi-Fi alla quale si possono collegare utenti esterni all'azienda, per minimizzare il rischio di accessi non autorizzati o potenziali compromissioni. La scelta dell'edificio C garantisce una maggiore sicurezza.

## 2. Progettazione struttura fisica della rete

### 2.1 Struttura e topologia adottata

Per realizzare la rete aziendale della BJ Entertainment è stata usata una topologia a stella. Ogni router è collegato direttamente con la sede B.

I dispositivi sono collegati tra loro attraverso uno switch predisposto in ogni sede.

Nella sede E è previsto il montaggio di un Access Point (AP Cisco Aironet 2800) che si occuperà della parte wireless.



Per connettere le varie macchine sono previsti degli switch CISCO (Cisco SG350 - 28p). La dotazione di porte permette di garantire a tutti gli utenti accesso alla rete. Nelle sedi con un centinaio di utenti andranno collegati 4 switch a catena per coprire tutte le connessioni.






Gli switch sono collegati a diversi Router CISCO (C7200) interconnessi tra loro con cavi in fibra.

Nella figura a fianco viene riportato il router CISCO usato nelle simulazioni; è necessario aggiungere componenti aggiuntivi per aumentare le capacità. Per la simulazione con GNS3 abbiamo utilizzato il router CISCO c3725 ma essendo fuori produzione per l'azienda in questione abbiamo scelto il c7200



### 2.2 Cablaggio

Per collegare i vari edifici è stata usata la fibra ottica per garantire la massima velocità. Le connessioni dei vari host agli switch usiamo cavi rame a seconda delle esigenze con dei cavi in rame. Tra le sedi c'è una backbone per ciascun collegamento.

Fibra ottica multimodale	
Fibra ottica monomodale	
Cablaggio in rame	

## 2.3 Dispositivi usati

Dispositivi	Modello	Quantità
Router	Cisco C7200	x 6
Switch	Cisco SG350 - 28p	x 18
Switch	Cisco SG350 - 8p	x 2
AP	Cisco Aironet 2800	x 1
Server Web	Dell PowerEdge R650xs	x 1
Server Mail	Dell PowerEdge R650xs	x 1
Server DNS	Supermicro SYS-5019S-M	x 2
Server Backup	Synology Rackstation RS1221+	x 1
Server Nagios	Lenovo ThinkSystem SR250 V2 (7D7QA02QEA)	x 1
Server Aziendale	Dell PowerEdge R650xs	x 1
Fibra ottica multimodale	OM4	0,4 km
Fibra ottica monomodale	OS2	10 km
Cablaggio rame	FTP Cat5e	4,5 km
Armadio	APC NetShell SX	x 1

### 3. Progettazione logica della rete

#### 3.1 Suddivisione delle sottoreti

Data la numerosità degli utenti abbiamo deciso di adottare indirizzi ip privati, abbiamo usato 192.168.0.0/24 come ip principale per la diffusione degli ip.

Sede	Sottorete	Capienza
A	192.168.1.0/24	~ 100
B	192.168.2.0/24	~ 100
B (DMZ)	192.168.100.0/24	/
C	192.168.3.0/24	~ 100
D	192.168.4.0/24	~ 100
E	192.168.5.0/24	~ 50

L'edificio B presenta vari server. A seguito un elenco che fa da Mappa per gli ip dei server presenti

Sede	Server	IP dei server
B	Posta elettronica	192.168.100.20
B	Web	192.168.100.40
B	DNS 1	192.168.100.30
B	Nagios	192.168.100.200
C	Applicazioni aziendali	192.168.3.10
C	DNS 2	192.168.3.30
C	Backup	192.168.3.50



### 3.2 Importanza delle sottoreti

Dividere in sottoreti ci permette di isolare in aree definite.

Possiamo proteggere eventuali porzioni, riducendo notevolmente le aree raggiungibili.

Uno degli aspetti più importanti da considerare è che semplifica la ricerca di eventuali problemi, possiamo monitorare ogni parte isolata localizzando meglio eventuali errori.

La maschera di sottorete è /24, che consente all'azienda di disporre di un numero abbondante di indirizzi IP, lasciando margine all'azienda per espansioni future.

### 3.3 Indirizzi dei router

Router	Sede	Sottorete
R-A	A	192.168.1.1
R-B	B	192.168.2.1
R-OUT	B	192.168.100.1
R-C	C	192.168.3.1
R-D	D	192.168.4.1
R-E	E	192.168.5.1

### 3.4 Backbone tra router

Per far comunicare i router presenti è necessario associare degli indirizzi per la comunicazione tra le varie sottoreti.

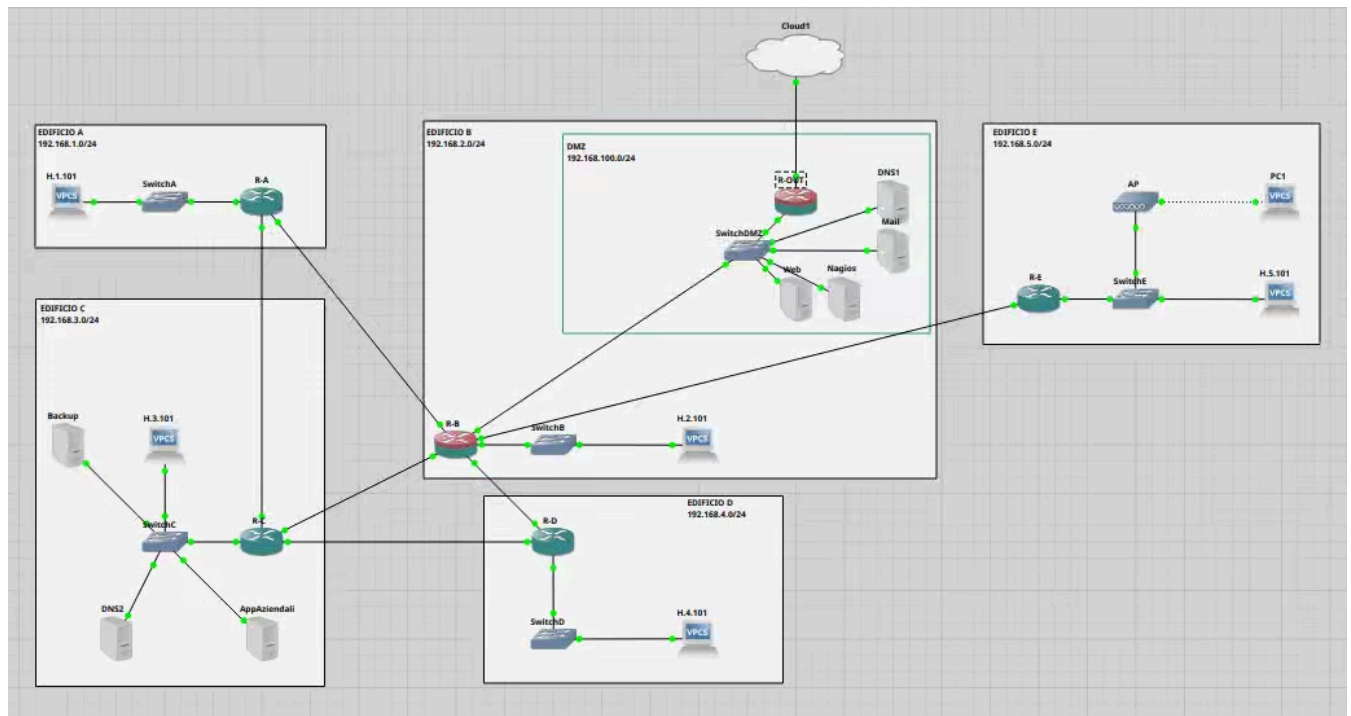
Per connettersi tra loro i router hanno bisogno di un indirizzo che segue la seguente regola:

10.[sede mittente].[sede destinataria \* 10].0/30

Usando la subnet mask 255.255.255.252, si ottengono sottoreti con un massimo di 2 host connessi (ovvero i due router).

## 4. Simulazione

In seguito troviamo lo schema fisico di rete che abbiamo realizzato con GNS3.



## 5. Configurazione interfacce di rete

### 5.1 Configurazione degli host

#### Configurazione IP statici degli Host dell'edificio A:

Riepilogo dati:

Rete	192.168.1.0/24
IP Host	192.168.1.101 - 192.168.1.201
IP DNS2	192.168.3.30

# Il DNS1 (192.168.100.30) è opzionale.

- **Host nella simulazione di GNS3:**

```
set pname H1.101
ip 192.168.1.101/24 192.168.1.1
ip dns 192.168.3.30
save
```

- **Host in una configurazione reale:**

```
~# sudo nano /etc/network/interfaces
```

```
#iface enp0s3 inet dhcp
iface enp0s3 inet static          # Connessione calata
address 192.168.1.101            # IP statico
netmask 255.255.255.0           # Subnet mask
gateway 192.168.1.1              # Gateway
dns-nameservers 192.168.3.30     # DNS
```

```
~# sudo systemctl restart networking | echo Configurazione ricaricata
```

## Configurazione edificio B:

Riepilogo dati:

Rete	192.168.2.0/24
IP Host	192.168.2.101 - 192.168.2.201
IP DNS2	192.168.3.30

# Il DNS1 (192.168.100.30) è opzionale.

- **Host nella simulazione di GNS3:**

```
set pcname H2.101
ip 192.168.2.101/24 192.168.2.1
ip dns 192.168.3.30
save
```

- **Host in una configurazione reale:**

```
~# sudo nano /etc/network/interfaces
```

```
#iface enp0s3 inet dhcp
iface enp0s3 inet static          # Connessione calata
address 192.168.2.101            # IP statico
netmask 255.255.255.0            # Subnet mask
gateway 192.168.2.1              # Gateway
dns-nameservers 192.168.3.30     # DNS
```

```
~# sudo systemctl restart networking | echo Configurazione ricaricata
```

## Configurazione edificio B (DMZ):

Riepilogo dati:

Rete	192.168.2.0/24
IP Host	192.168.2.101 - 192.168.2.201
IP DNS2	192.168.3.30

# Il DNS1 (192.168.100.30) è opzionale.

- **Host nella simulazione di GNS3:**

```
set pcname H2.101
ip 192.168.2.101/24 192.168.2.1
ip dns 192.168.3.30
save
```

- **Host in una configurazione reale:**

```
~# sudo nano /etc/network/interfaces
```

```
#iface enp0s3 inet dhcp
iface enp0s3 inet static      # Connessione calata
address 192.168.2.101        # IP statico
netmask 255.255.255.0        # Subnet mask
gateway 192.168.2.1          # Gateway
dns-nameservers 192.168.3.100 # DNS
```

```
~# sudo systemctl restart networking | echo Configurazione ricaricata
```

## Configurazione edificio C:

Riepilogo dati:

Rete	192.168.3.0/24
IP Host	192.168.3.101 - 192.168.3.201
IP DNS2	192.168.3.30

# Il DNS1 (192.168.100.30) è opzionale.

- **Host nella simulazione di GNS3:**

```
set pcname H3.101
ip 192.168.3.101/24 192.168.3.1
ip dns 192.168.3.30
save
```

- **Host in una configurazione reale:**

```
~# sudo nano /etc/network/interfaces
```

```
#iface enp0s3 inet dhcp
iface enp0s3 inet static          # Connessione calata
address 192.168.3.101           # IP statico
netmask 255.255.255.0          # Subnet mask
gateway 192.168.3.1             # Gateway
dns-nameservers 192.168.3.30    # DNS
```

```
~# sudo systemctl restart networking | echo Configurazione ricaricata
```

## Configurazione edificio D:

Riepilogo dati:

Rete	192.168.4.0/24
IP Host	192.168.4.101 - 192.168.4.201
IP DNS2	192.168.3.30

# Il DNS1 (192.168.100.30) è opzionale.

- **Host nella simulazione di GNS3:**

```
set pcname H4.101
ip 192.168.4.101/24 192.168.4.1
ip dns 192.168.3.30
save
```

- **Host in una configurazione reale:**

```
~# sudo nano /etc/network/interfaces
```

```
#iface enp0s3 inet dhcp
iface enp0s3 inet static      # Connessione calata
address 192.168.4.101        # IP statico
netmask 255.255.255.0        # Subnet mask
gateway 192.168.4.1          # Gateway
dns-nameservers 192.168.3.30 # DNS
```

```
~# sudo systemctl restart networking | echo Configurazione ricaricata
```

## Configurazione edificio E:

Riepilogo dati:

Rete	192.168.5.0/24
IP Host	192.168.5.101 - 192.168.5.201
IP DNS2	192.168.3.30

# Il DNS1 (192.168.100.30) è opzionale.

- **Host nella simulazione di GNS3:**

```
set pcname H5.101
ip 192.168.5.101/24 192.168.5.1
ip dns 192.168.3.30
save
```

- **Host in una configurazione reale:**

```
~# sudo nano /etc/network/interfaces
```

```
#iface enp0s3 inet dhcp
iface enp0s3 inet static          # Connessione calata
address 192.168.5.101           # IP statico
netmask 255.255.255.0           # Subnet mask
gateway 192.168.5.1             # Gateway
dns-nameservers 192.168.3.30    # DNS
```

```
~# sudo systemctl restart networking | echo Configurazione ricaricata
```



## 6. Impostazione Routing

### 6.1 Configurazione del routing e protocolli interni

Abbiamo configurato per ogni edificio i vari router e il protocollo RIP:

#### Edificio A:

```
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown

interface GigabitEthernet0/1
ip address 10.1.20.1 255.255.255.252
no shutdown

interface GigabitEthernet1/0
ip address 10.1.30.1 255.255.255.252
no shutdown

router rip
version 2
network 192.168.1.0
network 10.1.20.0
network 10.1.30.0

end
ip domain-lookup
ip name-server 192.168.3.30
```

## Edificio B:

```
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
no shutdown

interface GigabitEthernet0/1
ip address 10.1.20.2 255.255.255.252
no shutdown

interface GigabitEthernet1/0
ip address 10.2.30.1 255.255.255.252
no shutdown

interface GigabitEthernet1/1
ip address 10.2.40.1 255.255.255.252
no shutdown

interface GigabitEthernet1/2
ip address 10.2.50.1 255.255.255.252
no shutdown

interface GigabitEthernet1/3
ip address 10.2.100.1 255.255.255.252
no shutdown

router rip
version 2
network 192.168.2.0
network 10.1.20.0
network 10.2.30.0
network 10.2.40.0
network 10.2.50.0
network 10.2.100.0

end
ip domain-lookup
ip name-server 192.168.3.30
```

## Edificio C:

```
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
no shutdown
```

```
interface GigabitEthernet0/1
ip address 10.1.30.2 255.255.255.252
no shutdown
```

```
interface GigabitEthernet1/0
ip address 10.2.30.2 255.255.255.252
no shutdown
```

```
interface GigabitEthernet1/1
ip address 10.3.40.1 255.255.255.252
no shutdown
```

```
router rip
version 2
network 192.168.2.0
network 10.1.30.0
network 10.2.30.0
network 10.3.40.0
```

```
end
ip domain-lookup
ip name-server 192.168.3.30
```

### **Edificio D:**

```
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
no shutdown

interface GigabitEthernet0/1
ip address 10.2.40.2 255.255.255.252
no shutdown

interface GigabitEthernet1/0
ip address 10.3.40.2 255.255.255.252
no shutdown

router rip
version 2
network 192.168.2.0
network 10.1.30.0
network 10.2.30.0

end
ip domain-lookup
ip name-server 192.168.3.30
```

### **Edificio E:**

```
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
no shutdown

interface GigabitEthernet0/1
ip address 10.2.50.2 255.255.255.252
no shutdown

router rip
version 2
network 192.168.2.0
network 10.2.50.0

end
ip domain-lookup
ip name-server 192.168.3.30
```

### Edificio B (DMZ):

```
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
no shutdown

interface GigabitEthernet0/1
ip address 10.2.100.2 255.255.255.252
no shutdown

router rip
version 2
network 192.168.2.0
network 10.2.100.0

end
ip domain-lookup
ip name-server 192.168.100.30
```

### 6.2 Configurazione rete wireless e DHCP

Nell'edificio "E" è presente un access point (AP) quindi è stato configurato il DHCP secondo questi parametri:

```
configure
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.5.101 192.168.5.151
ip dhcp excluded-address 192.168.5.1
ip dhcp pool AP1-E
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
lease 7
exit
write memory
```

## 7. Configurazione dei servizi

### 7.1 Configurazione DNS

#### Server DNS1 (Esterno)

**resolv.conf:**

```
domain bj.com

// Name Server primario DNS1
nameserver 192.168.100.30
```

**named.conf**

```
options {
    directory "/var/cache/bind";
    dnssec-validation auto;
    auth-nxdomain no;
    version "Not disclosed";
    notify yes;
    allow-transfer { none; };
    allow-query { any; };
    forwarders {
        1.1.1.1;
        8.8.8.8;
    };
    recursion no;
};

// DNS1 è slave di DNS2
zone "dmz.bj.com" {
    type slave;
    file "/etc/bind/zones/dmz.bj.com.bk";
    masters { 192.168.3.30; };
};

// reverse mapping per bj.com
zone "100.168.192.in-addr.arpa" {
    type slave;
    file "/etc/bind/zones/100.168.192.in-addr.arpa.bk";
    masters { 192.168.3.30; };
};
```

## Server DNS2 (Interno)

### resolv.conf:

```
domain bj.com

// Name Server primario DNS1
nameserver 192.168.100.30

// Name Server secundario DNS2
nameserver 192.168.3.30
```

### named.conf

```
acl localhost {
    127.0.0.1;
};

acl dmz {
    192.168.100.0/24;
};

acl trusted-networks {
    192.168.1.0/24;
    192.168.2.0/24;
    192.168.3.0/24;
    192.168.4.0/24;
    192.168.5.0/24;
};

options {
    directory "/var/cache/bind";
    dnssec-validation auto;
    auth-nxdomain no;
    version "Not disclosed";
    notify yes;
    allow-transfer { none; };
    allow-query { localhost; trusted-networks; };
    forwarders {
        1.1.1.1;
        8.8.8.8;
    };
    recursion yes;
    max-cache-size 512M;
    query-timeout 10;
};
```

**// DMZ**

```
zone "dmz.bj.com" {  
    type master;  
    file "/etc/bind/zones/dmz.bj.com.db";  
};
```

```
zone "100.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/zones/100.168.192.in-addr.arpa.db";  
};
```

**// Edificio a**

```
zone "edificioa.bj.com" {  
    type master;  
    file "/etc/bind/zones/edificioa.bj.com.db";  
};
```

```
zone "1.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/zones/1.168.192.in-addr.arpa.db";  
};
```

**// Edificio b**

```
zone "edificiob.bj.com" {  
    type master;  
    file "/etc/bind/zones/edificiob.bj.com.db";  
};
```

```
zone "2.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/zones/2.168.192.in-addr.arpa.db";  
};
```

**// Edificio c**

```
zone "edificioc.bj.com" {  
    type master;  
    file "/etc/bind/zones/edificioc.bj.com.db";  
};
```

```
zone "3.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/zones/3.168.192.in-addr.arpa.db";  
};
```



```

        allow-transfer { none; };
};

// Edificio d
zone "edificiod.bj.com" {
    type master;
    file "/etc/bind/zones/edificiod.bj.com.db";
};

zone "4.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/4.168.192.in-addr.arpa.db";
};

// Edificio e
zone "edificioe.bj.com" {
    type master;
    file "/etc/bind/zones/edificioe.bj.com.db";
};

zone "5.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/5.168.192.in-addr.arpa.db";
};

```

## **/etc/bind/zones/dmz.bj.com.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com.
(
    2025060101 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400      ; Minimum TTL
)

@ IN NS dns1.dmz.bj.com.
@ IN NS dmz.bj.com.
@ IN MX 10 mail.bj.com.

dns1 IN A 192.168.100.30
nagios IN A 192.168.100.200
web IN A 192.168.100.40
mail IN A 192.168.100.20
```

## **/etc/bind/zones/100.168.192.in-addr.arpa.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com.
(
    2025060101 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400      ; Minimum TTL
)

@ IN NS dns1.dmz.bj.com.
@ IN NS dmz.bj.com.

200 IN PTR nagios.dmz.bj.com.
40 IN PTR web.dmz.bj.com.
30 IN PTR dns1.dmz.bj.com.
20 IN PTR mail.dmz.bj.com.
```

### **/etc/bind/zones/edificioa.bj.com.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com. (
    2025060101 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400 )     ; Minimum TTL
```

```
IN NS dns1.dmz.bj.com.
```

```
gw      IN A 192.168.1.1
h.1.101 IN A 192.168.1.101
h.1.102 IN A 192.168.1.102
```

### **/etc/bind/zones/1.168.192.in-add.arpa.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com. (
    2025060101 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400 )     ; Minimum TTL
```

```
IN NS dns1.dmz.bj.com.
```

```
1      IN PTR gateway
101    IN PTR h.1.101
102    IN PTR h.1.102
```

### **/etc/bind/zones/edificio.bj.com.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com. (
    2025060202 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400 )     ; Minimum TTL

IN NS dns1.dmz.bj.com.
```

```
gw      IN A 192.168.2.1
H.2.101 IN A 192.168.2.101
H.2.102 IN A 192.168.2.102
```

### **/etc/bind/zones/2.168.192.in-add.arpa.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com. (
    2025060202 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400 )     ; Minimum TTL

IN NS dns1.dmz.bj.com.
```

```
1      IN PTR gateway
101    IN PTR H.2.101
102    IN PTR H.2.102
```

### **/etc/bind/zones/edificioc.bj.com.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com. (
    2025060202 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400 )     ; Minimum TTL

IN NS dns1.dmz.bj.com.
```

```
gw      IN A 192.168.3.1
H.2.101 IN A 192.168.3.101
H.2.102 IN A 192.168.3.102
```

### **/etc/bind/zones/3.168.192.in-add.arpa.db**

```
$TTL 86400
@ IN SOA dns1.dmz.bj.com. admin.bj.com. (
    2025060202 ; Serial
    3600       ; Refresh
    1800       ; Retry
    1209600    ; Expire
    86400 )     ; Minimum TTL

IN NS dns1.dmz.bj.com.

1      IN PTR gateway
101    IN PTR H.3.101
102    IN PTR H.3.102
```

## 7.2 Configurazione del Server Mail:

```
~# sudo nano /etc/network/interfaces
#iface enp0s3 inet dhcp          # Assegnazione IP dinamica
iface enp0s3 inet static         # Connessione calata
address 192.168.100.20          # Ip statico
netmask 255.255.255.0          # Subnet Mask
network 192.168.100.0           # Rete
broadcast 192.168.100.255       # Broadcast
gateway 192.168.100.1           # Gateway

~# sudo systemctl restart networking | echo Configurazione ricaricata
```

Dopo aver installato sendmail impostiamo i permessi e controlli per i client che si connettono al server di posta in /etc/mail/access:

```
Connect:192.168 // Permette di scambiare mail nella rete
GreetPause:192.168 // Antispam
ClientRate:192.168 // Limite alle connessioni
ClientConn:192.168
FREE.STREALTH.MAILER@ 550 Non si accettano mail da spammers
bj.com RELAY
192.168 RELAY
```

Creiamo gli alias nel file /etc/mail/aliases

```
postmaster: tommaso
admin: tommaso, andrea
dmz: admin dmz
rete: admin rete
reteb: admin retea
retec: admin retea
reted: admin retea
retee: admin retea
admin dmz: andrea
admin rete: dembélé, hakimi
admin retea: andrea, yildiz
admin retec: tommaso, doue
admin retea: doue, hakimi
admin retee: dembélé, doue
```

Configuriamo nomi di dominio gestiti dal server /etc/mail/local-host-names

```
localhost
bj.com
```

```
mail.bj.com
dmz.bj.com
rete.bj.com
reteb.bj.com
ret.ec.bj.com
reted.bj.com
retee.bj.com
```

Configuriamo /etc/mail/sendmail.mc  
Inviamo una mail a tutti gli utenti nel dominio  
FEATURE('relay\_entire\_domain')dnl''

Creazione di utenti che scrivono solo testo sulla console  
useradd --create-home -s /sbin/nologin tommaso; passwd tommaso  
useradd --create-home -s /sbin/nologin andrea; passwd andrea

Configuriamo la tabella degli utenti virtuali /etc/mail/virtusertable

```
root@bj.com root
postmaster@bj.com postmaster
admin@bj.com admin
dmz@bj.com dmz
rete@bj.com rete
reteb@bj.com retea
ret.ec@bj.com ret.ec
reted@bj.com reted
retee@bj.com retee
tommaso@bj.com tommaso andrea@bj.com andrea
```

cd /etc/mail  
make  
service sendmail restart  
nano /etc/network/interfaces

### 7.3 Configurazione del Server Web:

```
~# sudo nano /etc/network/interfaces
#iface enp0s3 inet dhcp           # Assegnazione IP dinamica
iface enp0s3 inet static          # Connessione calata
address 192.168.100.40            # Ip statico
netmask 255.255.255.0             # Subnet Mask
network 192.168.100.0             # Rete
broadcast 192.168.100.255         # Broadcast
gateway 192.168.100.1            # Gateway

~# sudo systemctl restart networking | echo Configurazione ricaricata
```

Come prima cosa dobbiamo aggiungere l'ip del nostro sito web (/etc/hosts).  
Inseriamo questa riga: **127.0.0.1 www.bj.com**

Dobbiamo installare apache2, uno dei servizi web più utilizzati al mondo.  
Per gestire le richieste al sito web va configurato, è possibile farlo attraverso **apache2.conf** nella cartella: **/etc/apache2/**

Nel file /etc/apache2/sites-available/**000-default.conf** aggiungiamo le righe:  
**ServerName www.bj.com**  
**UseCanonicalName Off**

Ci creiamo una cartella per ospitare il sito in:  
**/var/www/bj.com/it**

Per la sicurezza del server possiamo gestire i permessi in questo modo:  
Nella cartella **"/var/www/bj.com/it/"** impostiamo i permessi in questo modo:

L'owner delle cartelle nella directory a 7 (tutti i permessi),  
il gruppo e tutti gli altri a 5 (lettura ed esecuzione) **755**

Mentre per tutti i file l'accesso dell'admin è 6 (scrittura e lettura),  
per il gruppo e gli altri 4 (sola lettura) **644**

In fine impostiamo l'**admin** come proprietario della cartella **/var/www/bj.com**

Sempre ai fini della sicurezza del sito possiamo configurare i log di apache2.  
Creiamo una cartella per i log in **/var/apache2/bj.com**  
Cambiamo il proprietario la cartella **/var/log/apache2/bj.com**  
Creiamo un file che crea i log **bj.com.conf**.

Intera configurazione del file:

```
<VirtualHost *:80>
```

```
    ServerAdmin babbujova@bj.com
```

```
    ServerName bj.com
```

```
    ServerAlias *.bj.com
```

```
    DocumentRoot /var/www/bj.com
```

```
    ErrorLog ${APACHE_LOG_DIR}/bj.com/error.log
```

```
    CustomLog ${APACHE_LOG_DIR}/bj.com/access.log combined
```

```
<Directory /var/www/bj.com>
```

```
    Options Indexes FollowSymLinks
```

```
    AllowOverride All
```



```
Require all granted
</Directory>
</VirtualHost>
```

```
sudo a2ensite bj.com.conf
sudo systemctl reload apache2
sudo systemctl restart apache2
```

#### 7.4 Configurazione Server Backup:

- Configurazione su macchina reale:  
~# sudo nano /etc/network/interfaces  
#iface enp0s3 inet dhcp # Assegnazione IP dinamica  
iface enp0s3 inet static # Connessione calata  
address 192.168.3.50 # Ip statico  
netmask 255.255.255.0 # Subnet Mask  
network 192.168.3.0 # Rete  
broadcast 192.168.3.255 # Broadcast  
gateway 192.168.3.1 # Gateway  
  
~# sudo systemctl restart networking | echo Configurazione ricaricata
- Configurazione su GNS3  
ip 192.168.3.50/24 192.168.3.5  
ip dns 192.168.3.30  
save

#### 7.5 Configurazione Server App Aziendali:

- Configurazione su macchina reale:  
~# sudo nano /etc/network/interfaces  
#iface enp0s3 inet dhcp # Assegnazione IP dinamica  
iface enp0s3 inet static # Connessione calata  
address 192.168.3.10 # Ip statico  
netmask 255.255.255.0 # Subnet Mask  
network 192.168.3.0 # Rete  
broadcast 192.168.3.255 # Broadcast  
gateway 192.168.3.1 # Gateway  
  
~# sudo systemctl restart networking | echo Configurazione ricaricata
- Configurazione su GNS3  
ip 192.168.3.10/24 192.168.3.1  
ip dns 192.168.3.30  
save

## 8. Firewall e prevenzione

### 8.1 Configurazione firewall:

Abbiamo due firewall, uno interno, che implementa più misure di protezione essendo appunto interno alla nostra rete; e uno esterno, il quale avrà meno misure di protezione dovendo essere accessibile dall'esterno.

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 IN:

Regole per DNS2:

```
iptables -A FORWARD -p udp -d 192.168.100.30 --dport 53 -j ACCEPT
```

```
iptables -A FORWARD -p tcp -d 192.168.100.30 --dport 53 -j ACCEPT
```

Regole per Posta Elettronica:

```
iptables -A FORWARD -p tcp -d 192.168.100.20 --dport 25 -m limit 100/s -j ACCEPT
```

```
iptables -A FORWARD -p tcp -d 192.168.100.20 --dport 110 -m limit 100/s -j ACCEPT
```

```
iptables -A FORWARD -p tcp -d 192.168.100.20 --dport 143 -m limit 100/s -j ACCEPT
```

Regole per Web:

```
iptables -A FORWARD -p tcp -d 192.168.100.40 --dport 443 -m limit 100/s -j ACCEPT
```

Regole per connessioni già stabilite:

```
iptables -A OUTPUT -m state --state ESTABLISHED,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:

Regole per DNS1, Posta Elettronica e Web:

```
iptables -A FORWARD -p tcp -d 192.168.100.20 --dport 25 -j ACCEPT
```

```
iptables -A FORWARD -p tcp -d 192.168.100.20 --dport 110 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.100.20 --dport 143 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.100.30 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -d 192.168.100.30 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.100.40 --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
```

Regole per NAT:

```
iptables -t NAT -A PREROUTING -p tcp --dport 25 -j DNAT --to-destination 198.168.100.20
iptables -t NAT -A PREROUTING -p udp --dport 53 -j DNAT --to-destination 198.168.100.30
iptables -t NAT -A PREROUTING -p tcp --dport 53 -j DNAT --to-destination 198.168.100.30
iptables -t NAT -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination 198.168.100.40
```

# Mascheramento ip dei pacchetti uscenti

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

### **Prevenzione:**

```
sudo iptables -A FORWARD -d -j DROP
// Da fare
```

## 9. Preventivo

Componente	Modello	Quantità	Prezzo unitario	Prezzo totale
Router	Cisco c7200	6	350€	2.100€
Switch	Cisco SG350 - 28p	18	250€	4.500€
Switch	Cisco SG350 - 8p	2	80€	160€
AP	Cisco Aironet 2800	1	42€	42€
Server Web	Dell PowerEdge R650xs	1	3.900€	3.900€
Server Mail	HPE ProLiant DL360 Gen10 Plus	1	3.200€	3.200€
Server DNS	Supermicro SYS-5019S-M	2	800€	1.600€
Server Backup	Synology Rackstation RS1221+	1	1.000€	1.000€
Server Nagios	Lenovo ThinkSystem SR250 V2 (7D7QA02QEA)	1	1.300€	1.300€
Server Aziendale	Dell PowerEdge R650xs	1	3.900€	3.900€
Fibra ottica multimodale	OM4	0,4 km	1,99€/m	795€
Fibra ottica monomodale	OS2	10 km	0,84€	8.415€
Cablaggio rame	FTP Cat5e	4,5 km	0,52€	2.340€
Armadio	APC NetShell SX	1	2.950€	2.950€
<b>TOT:</b>	<b>36.204€</b>			