Progetto – Laboratorio Reti

Azienda: HOPA Inc.

Vitaliy Didyk [379572]
Valentin Racovita [383261]
Docente: Prof. Sergio Tasso
Dipartimento di Matematica e Informatica – Università degli Studi di Perugia

A.A. 2024/2025 – 28 ottobre 2025

Indice

1 Descrizione del progetto

1.1 Scenario e richieste progettuali

La ditta **HOPA Inc.** ha deciso di collegare in rete tutti i suoi reparti ed uffici e ci ha contattato per disegnare, installare e gestire l'intera rete. La rete prevede una connessione **protetta** ad Internet con **unico punto di uscita** presso l'edificio **D**, che ospita anche la **DMZ**. L'edificio **C** è l'unico con copertura **Wi-Fi**.

Edifici e caratteristiche

Edificio	Utenti	Server	Wi-Fi
A	50	–	NO
B	50	–	NO
C	50	–	**SI**
D	150	–	NO
E	50	–	NO

Server richiesti in azienda

Server	#	Note
Posta elettronica	1	in DMZ (D)
Web	1	in DMZ (D)
DNS	≥ 2	DNS interno (master in C) + DNS esterno (slave in DMZ D)
Backup	1	protetto e isolato (edificio E)

Topologia fisica sintetica (mesh parziale) Tra A, B, C, D è presente una **mesh parziale** con i seguenti collegamenti: A–B 500 m, B–C 500 m, C–D 500 m, D–A 500 m, A–C 700 m, B–D 700 m. L'edificio **D** è collegato a **Internet** ed ha un link in **fibra monomodale (SMF)** di 5 km verso **E**, che transita da D per l'accesso alla WAN.

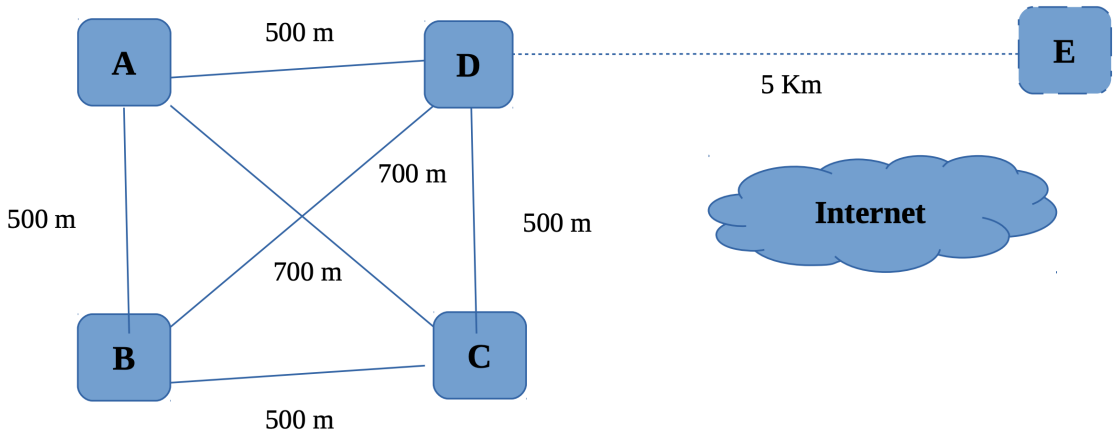

Figura 1: Schema degli edifici e dei collegamenti (mesh parziale A–B–C–D, D gateway/DMZ, collegamento SMF verso E).

1.2 Obiettivi progettuali

- Progettare la **struttura fisica** (topologia, mezzi trasmissivi, apparati).
- Definire la **struttura logica** (sottoreti, piano IP, DMZ in D).
- Configurare **interfacce** (router, server, almeno 1 host Unix per sottorete).
- Impostare il **routing** interno e di frontiera (D come core; R-IN/R-OUT come doppia frontiera DMZ).
- Configurare **DNS** (BIND9) e **posta** (Sendmail).
- Implementare **firewall** (iptables) e **monitoraggio** (Nagios).
- **Proteggere il server di Backup**.
- Redigere un **preventivo** dettagliato.

2 Progettazione struttura fisica della rete

2.1 Topologia adottata

Si adotta una **mesh parziale** tra A, B, C, D per garantire ridondanza dei percorsi; l'edificio **D** funge da **core** (`R-D`) verso gli altri edifici e ospita la **DMZ** con doppia frontiera: `R-IN` (lato LAN) e `R-OUT` (lato Internet). L'edificio **E** è collegato a D tramite **SMF** (5 km).

2.2 Cablaggio e mezzi trasmissivi

- **Backbone inter-sede**: Fibra multimodale per tratte $\leq$ 700 m; **fibra monomodale** D–E (5 km).
- **Cablaggio utente**: rame (Cat5e/Cat6) dagli switch agli host.
- **Rete Wi-Fi**: un Access Point professionale nell'edificio C.

2.3 Dispositivi

- **Router interni**: Cisco serie 7200 (A, B, C, D, E).
- **Frontiera/DMZ**: in D sono presenti `R-IN` e `R-OUT`; tra loro e i server un **switch DMZ** L2.
- **Switch**: Cisco SG350 (28p/8p secondo necessità).
- **AP**: Cisco Aironet serie 2800 (solo C, con DHCP integrato).
- **Server**: Web, Mail, DNS1 (DMZ), DNS2 (interno in C), **Backup (in E)**, Nagios.

3 Progettazione logica della rete

3.1 Suddivisione delle sottoreti

Indirizzi privati con **/24** per ogni sede; **DMZ** dedicata in D su switch L2.

Sede	Sottorete	Capienza	Gateway
A	192.168.10.0/24	$\sim$ 50	192.168.10.1
B	192.168.20.0/24	$\sim$ 50	192.168.20.1
C	192.168.30.0/24	$\sim$ 50	192.168.30.1
D	192.168.40.0/24	$\sim$ 150	192.168.40.1

E	192.168.50.0/24	~ 50	192.168.50.1
DMZ (switch)	**192.168.100.0/24**	servizi	**R-IN: 192.168.100.1 / R-OUT: 192.168.100.**

Piano IP dei server principali

Server	**Posizione**	**IP**
DNS1 (esterno, slave)	DMZ (D)	192.168.100.30
Web	DMZ (D)	192.168.100.40
Mail	DMZ (D)	192.168.100.20
Nagios	DMZ (D)	192.168.100.200
DNS2 (interno, master)	C	192.168.30.30
Backup	**E**	**192.168.50.50**

3.2 Backbone tra router

Collegamenti punto-punto con **/30** (tutti sulla classe 192.168.60.0/24):

- A↔B: 192.168.60.0/30 (A: .1, B: .2)
- B↔C: 192.168.60.4/30 (B: .5, C: .6)
- C↔D: 192.168.60.8/30 (C: .9, D: .10)
- D↔A: 192.168.60.12/30 (D: .13, A: .14)
- A↔C: 192.168.60.16/30 (A: .17, C: .18)
- B↔D: 192.168.60.20/30 (B: .21, D: .22)
- D↔E: 192.168.60.28/30 (D: .29, E: .30)
- **D↔R-IN**: **192.168.60.32/30** (**D: .33, R-IN: .34**)

4 Simulazione

La topologia è stata riprodotta in **Cisco Packet Tracer**.

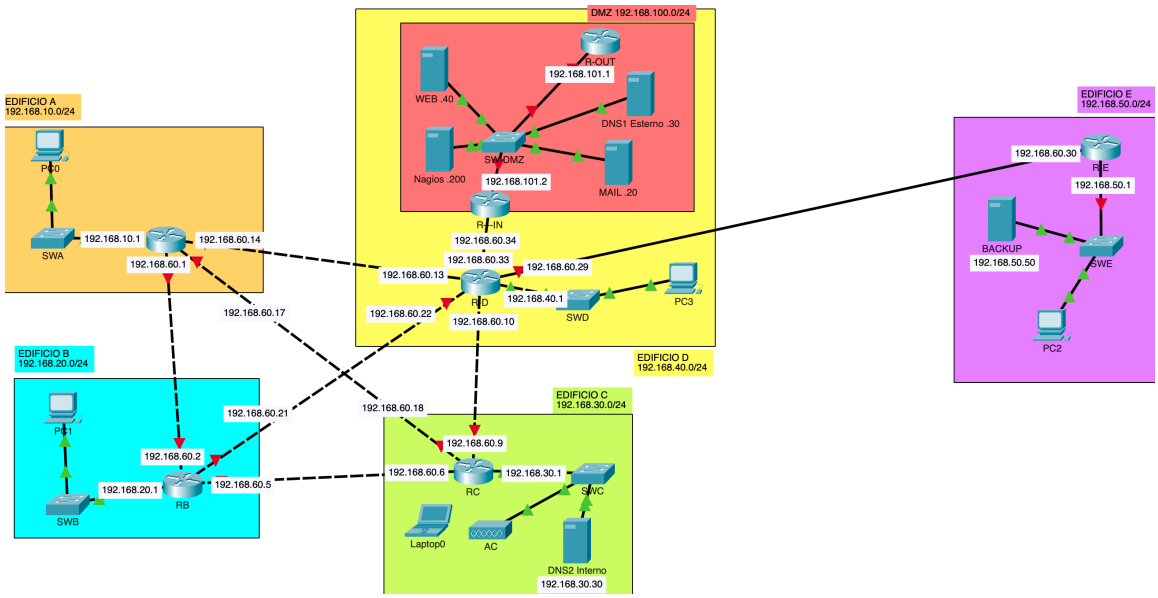

Figura 2: Topologia logica della rete simulata in Cisco Packet Tracer. Tre router in D: R-D (core), R-IN (frontiera interna), R-OUT (frontiera esterna) con DMZ su switch 192.168.100.0/24.

5 Configurazione interfacce di rete

5.1 Host Unix (un esempio per sottorete)

Esempi per A–E con DNS interno 192.168.30.30 e gateway della rispettiva sottorete.

```
# A
set pcname H1.101
ip 192.168.10.101/24 192.168.10.1
ip dns 192.168.30.30
save
# B
set pcname H2.101
ip 192.168.20.101/24 192.168.20.1
ip dns 192.168.30.30
save
# C
set pcname H3.101
ip 192.168.30.101/24 192.168.30.1
ip dns 192.168.30.30
save
# D
set pcname H4.101
ip 192.168.40.101/24 192.168.40.1
ip dns 192.168.30.30
save
# E
set pcname H5.101
ip 192.168.50.101/24 192.168.50.1
ip dns 192.168.30.30
save
```

6 Impostazione Routing

6.1 Routing interno (RIP v2)

Nota generale Tutti i router **interni** (A, B, C, D, E) eseguono RIP v2 con `no auto-summary` e annunciano la propria LAN /24 e i link di backbone (basta un solo `network 192.168.60.0`). **R-IN** e **R-OUT** non partecipano al RIP: usano rotte statiche.

Router A

```
enable
conf t
hostname A
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shut
interface Gi0/1
 ip address 192.168.60.1 255.255.255.252   ! A-B
 no shut
interface Gi0/2
 ip address 192.168.60.14 255.255.255.252  ! D-A
 no shut
interface Gi0/3
 ip address 192.168.60.17 255.255.255.252  ! A-C
 no shut
router rip
 version 2
 no auto-summary
 network 192.168.10.0
 network 192.168.60.0
end
```

Router B

```
enable
conf t
hostname B
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 no shut
interface Gi0/1
 ip address 192.168.60.2 255.255.255.252   ! A-B
 no shut
interface Gi0/2
 ip address 192.168.60.5 255.255.255.252   ! B-C
 no shut
interface Gi0/3
 ip address 192.168.60.21 255.255.255.252  ! B-D
 no shut
router rip
 version 2
 no auto-summary
 network 192.168.20.0
 network 192.168.60.0
end
```

Router C

```
enable
conf t
hostname C
interface FastEthernet0/0
 ip address 192.168.30.1 255.255.255.0
 no shut
interface Gi0/1
 ip address 192.168.60.6 255.255.255.252   ! B-C
 no shut
interface Gi0/2
 ip address 192.168.60.9 255.255.255.252   ! C-D
 no shut
interface Gi0/3
 ip address 192.168.60.18 255.255.255.252  ! A-C
 no shut
router rip
 version 2
 no auto-summary
 network 192.168.30.0
 network 192.168.60.0
end
```

Router D (core)

```
enable
conf t
hostname D
interface FastEthernet0/0
 ip address 192.168.40.1 255.255.255.0     ! LAN D
 no shut
interface Gi0/1
 ip address 192.168.60.10 255.255.255.252  ! C-D
 no shut
interface Gi0/2
 ip address 192.168.60.13 255.255.255.252  ! D-A
 no shut
interface Gi0/3
 ip address 192.168.60.22 255.255.255.252  ! B-D
 no shut
interface Gi0/4
 ip address 192.168.60.29 255.255.255.252  ! D-E
 no shut
interface Gi0/5
 ip address 192.168.60.33 255.255.255.252  ! D-RIN
 no shut
router rip
 version 2
 no auto-summary
 network 192.168.40.0
 network 192.168.60.0
end
```

Router E

```
enable
conf t
hostname E
interface FastEthernet0/0
 ip address 192.168.50.1 255.255.255.0
 no shut
interface Gi0/1
 ip address 192.168.60.30 255.255.255.252   ! D-E
 no shut
router rip
 version 2
 no auto-summary
 network 192.168.50.0
 network 192.168.60.0
end
```

R-IN (frontiera interna, nessun RIP)

```
enable
conf t
hostname R-IN
interface Gi0/0
 ip address 192.168.60.34 255.255.255.252   ! verso R-D (60.32/30)
 no shut
interface Gi0/1
 ip address 192.168.101.2 255.255.255.0     ! DMZ (switch)
 no shut
! Rotte statiche verso le LAN interne attraverso R-D
ip route 192.168.10.0 255.255.255.0 192.168.60.33
ip route 192.168.20.0 255.255.255.0 192.168.60.33
ip route 192.168.30.0 255.255.255.0 192.168.60.33
ip route 192.168.40.0 255.255.255.0 192.168.60.33
ip route 192.168.50.0 255.255.255.0 192.168.60.33
! Default verso Internet tramite R-OUT
ip route 0.0.0.0 0.0.0.0 192.168.100.2
end
```

R-OUT (frontiera esterna, NAT)

```
enable
conf t
hostname R-OUT
interface Gi0/0
 ip address 192.168.101.1 255.255.255.0     ! DMZ (switch)
 no shut
```

6.2 Wi-Fi edificio C e DHCP

Il **DHCP** non è un server dedicato: è integrato nel router/AP dell'edificio C (unico edificio con Wi-Fi).

```
configure terminal
no ip dhcp use vrf connected
```

```
ip dhcp excluded-address 192.168.30.1 192.168.30.50
ip dhcp pool WIFI-C
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.30
 lease 7
end
write memory
```

7 Configurazione dei servizi

7.1 DNS (BIND9)

DNS1 – esterno in DMZ (D)

```
# /etc/resolv.conf
domain hopa.inc
nameserver 192.168.100.30

# /etc/bind/named.conf.options
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;
}

# /etc/bind/named.conf.local
zone "dmz.hopa.inc" {
  type master;
  file "/etc/bind/zones/dmz.hopa.inc.bk";
};
zone "100.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/zones/100.168.192.in-addr.arpa.bk";
};
```

Zone DNS: DMZ

```
$TTL 86400
$ORIGIN dmz.hopa.inc.
@ IN SOA dns.dmz.hopa.inc. root.dmz.hopa.inc. (
        2025102701
        43200
        3600
        3600000
        2592000
```

```
)

; Name Servers
    IN NS dns.dmz.hopa.inc.
    IN NS dns.cloudflare.com.

; MX Record
    IN MX 10 mail.dmz.hopa.inc.

; Host Records
rin      IN A 192.168.101.2
rout     IN A 192.168.101.1
mail     IN A 192.168.100.20
dns      IN A 192.168.100.30
www      IN A 192.168.100.40
nagios   IN A 192.168.100.200

; Aliases

smtp     IN CNAME mail.dmz.hopa.inc.
```

Zone DNS: DMZ Reverse

```
$TTL 86400
$ORIGIN 100.168.192.in-addr.arpa.
@ IN SOA dns.dmz.hopa.inc. root.dmz.hopa.inc. (
        2025102701
        43200
        3600
        3600000
        2592000
)

; Name Server
    IN NS dns.dmz.hopa.inc.

; PTR Records
20   IN PTR mail.dmz.hopa.inc.
30   IN PTR dns.dmz.hopa.inc.
40   IN PTR www.dmz.hopa.inc.
200  IN PTR nagios.dmz.hopa.inc.
```

DNS2 – interno in C

```
# /etc/resolv.conf
domain hopa.inc
nameserver 192.168.100.30
nameserver 192.168.30.30

# /etc/bind/named.conf.options
acl localhost { 127.0.0.1; };
acl trusted { 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; 192.168.100.0/24; };
```

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

# /etc/bind/named.conf.local (estratto)
zone "dmz.hopa.inc" { type master; file "/etc/bind/zones/dmz.hopa.inc.db"; };
zone "100.168.192.in-addr.arpa" { type master; file "/etc/bind/zones/100.168.192.in-
    addr.arpa.db"; };

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

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

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

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

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

File di zona forward Edificio A

```
# /etc/bind/zones/edificioa.hopa.inc.db
$TTL 86400
$ORIGIN edificioa.hopa.inc.
@ IN SOA dns.edificioa.hopa.inc. root.edificioa.hopa.inc. (
        2025102701 ; serial
        43200      ; refresh
        3600       ; retry
        3600000    ; expire
        2592000    ; default ttl
)
```

```
    IN NS dns.edificioa.hopa.inc.
    IN NS dns.dmz.hopa.inc.

    IN MX 10 mail.dmz.hopa.inc.

dns        IN A 192.168.10.200
pc1        IN A 192.168.10.101
pc2        IN A 192.168.10.102
```

File di zona reverse Edificio A

```
$TTL 86400
$ORIGIN 10.168.192.in-addr.arpa.
@ IN SOA dns.edificioa.hopa.inc. root.edificioa.hopa.inc. (
        2025102701
        43200
        3600
        3600000
        2592000
)

    IN NS dns.edificioa.hopa.inc.
    IN NS dns.dmz.hopa.inc.

30  IN PTR dns.edificioa.hopa.inc.
101  IN PTR pc1.edificioa.hopa.inc.
102  IN PTR pc2.edificioa.hopa.inc.
```

7.2 Posta (Sendmail) – server in DMZ (D)

```
# /etc/network/interfaces (estratto)
iface enp0s3 inet static
  address 192.168.100.20
  netmask 255.255.255.0
  gateway 192.168.100.1

# /etc/mail/access (estratto)
Connect:192.168    OK
GreetPause:192.168      1
ClientRate:192.168      100
ClientConn:192.168      100
hopa.inc         RELAY
192.168          RELAY

# /etc/mail/local-host-names (estratto)
localhost
hopa.inc
mail.hopa.inc
dmz.hopa.inc

# /etc/mail/aliases

Creiamo gli alias nel file /etc/mail/aliases
postmaster: vitaliy
admin: vitaliy,valentin
```

```
dmz: admindmz
```

7.3 Web (Apache2) – server in DMZ (D)

```
# /etc/network/interfaces (estratto)
iface enp0s3 inet static
  address 192.168.100.40
  netmask 255.255.255.0
  gateway 192.168.100.1

# /etc/hosts
127.0.0.1 www.hopa.inc

# /etc/apache2/sites-available/hopa.inc.conf
<VirtualHost *:80>
  ServerAdmin admin@hopa.inc
  ServerName hopa.inc
  ServerAlias *.hopa.inc
  DocumentRoot /var/www/hopa.inc
  ErrorLog ${APACHE_LOG_DIR}/hopa.inc/error.log
  CustomLog ${APACHE_LOG_DIR}/hopa.inc/access.log combined
  <Directory /var/www/hopa.inc>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
  </Directory>
</VirtualHost>
```

7.4 Server di Backup (in E)

```
# /etc/network/interfaces (estratto)
iface enp0s3 inet static
  address 192.168.50.50
  netmask 255.255.255.0
  gateway 192.168.50.1
```

8 Firewall

8.1 Iptables (schema di riferimento)

Due livelli: *OUT* (su R-OUT, frontiera Internet/DMZ) e *IN* (su R-IN, frontiera LAN/DMZ). Politiche `DROP` di default, regole per DNS/POSTA/WEB, stato connessioni, NAT su R-OUT.

```
# Esempi (host Linux in DMZ o firewall dedicati)

# Policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Stato connessioni
```

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

# Traffico ammesso verso i servizi DMZ
iptables -A FORWARD -p tcp -d 192.168.100.40 --dport 80  -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.100.40 --dport 443 -j ACCEPT
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 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 connessioni gia 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
```

9 Motivazioni della disposizione dei servizi

Le scelte seguono principi di **sicurezza**, **resilienza** e **manutenibilità**.

9.1 DHCP integrato in C (Wi-Fi)

L'edificio C è l'unico con copertura Wi-Fi. Integrare il servizio DHCP nel router/AP:

- riduce latenza e broadcast superflui per i device mobili;
- semplifica l'operatività (nessun server aggiuntivo);
- mantiene la configurazione vicina al dominio di mobilità.

9.2 DMZ su switch L2 con doppia frontiera

R-IN (lato LAN) e **R-OUT** (lato Internet) insistono sulla stessa LAN **192.168.100.0/24**:

- separazione netta dei domini di fiducia;
- possibilità di policy diverse LAN↔DMZ e Internet↔DMZ;
- semplicità di pubblicazione dei servizi (DNAT su R-OUT).

9.3 DNS master interno in C

Mantiene la risoluzione interna indipendente da eventuali compromissioni della DMZ.

9.4 Backup in E

Sito remoto con collegamento SMF 5 km: riduce il rischio e abilita **disaster recovery**.

10 Preventivo di massima

Componente	**Modello**	**Q.tà**	**Prezzo unitario (€)**	**Totale (€)**
Router	Cisco 7200	7	170	1190
Switch 28p	Cisco SG350-28p	12	420	5040
Switch 8p	Cisco SG350-8p	3	230	690
Access Point Wi-Fi	Cisco Aironet 2800	1	300	300
Server Web	Classe enterprise	1	1200	1200
Server Mail	Classe enterprise	1	1200	1200
Server DNS	Classe enterprise	2	1200	2400
Server Backup	NAS rack	1	2000	2000
Server Nagios	Tower 1U	1	1200	1200
Fibra MM	OM4	-	300	300
Fibra SM	OS2 (5 km)	-	700	700
Rame Cat5e	-	4 km	100	100
Armadio Rack	Rack 42U	1	500	500
Totale stimato				**€ 19.020**

Prezzi indicativi, IVA esclusa.

11 Conclusioni

Il progetto rispetta i vincoli: Wi-Fi solo in C (DHCP integrato), DNS ≥ 2, DMZ in D su switch con doppia frontiera **R-IN/R-OUT**, **backup in E** per DR, routing RIP v2 nei soli router interni, NAT e pubblicazione servizi su R-OUT, policy di firewall coerenti.