Progettazione e configurazione di una rete aziendale

Filippo Mariani, Giorgio Mazza

22 aprile 2018

Indice

1 Requisiti del progetto e finalità

Un'azienda di onoranze funebri richiede la progettazione e configurazione di una rete aziendale in grado di interconnettere i vari edifici di suddetta azienda. Gli edifici sono i seguenti:

Nome edificio	Numero utenti
Agenzia	50
Barificio	260
Cremino	200
Destinazione	50
Epitaffio	30

Tabella 1: Edifici

ed è richiesto il seguente schema di collegamenti:

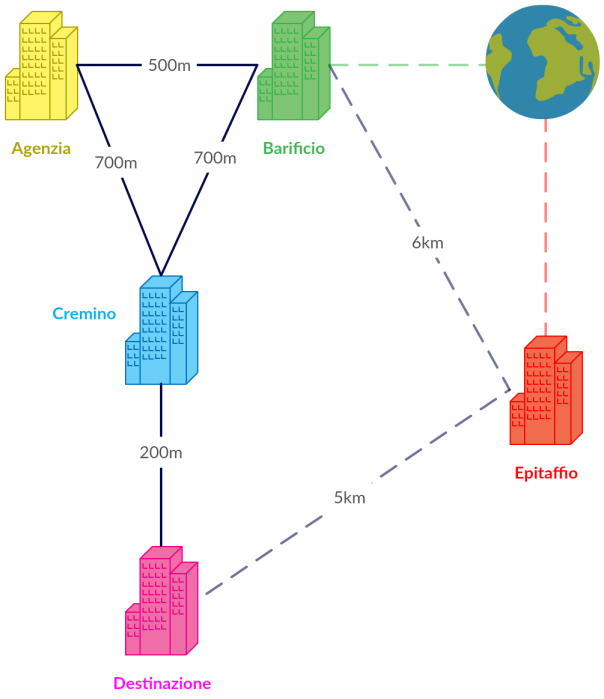

Figura 1: Schema Fisico

Sono richiesti:

- accesso protetto a Internet
- copertura WiFi nell'edificio C
- un server di posta elettronica
- un server di backup
- un server adibito alle applicazioni aziendali (da proteggere con particolare attenzione)

In oltre, in base a quanto richiesto, si è deciso di configurare:

- tre server DNS
- un server proxy
- un server DHCP

I vari server forniscono servizi agli utenti della rete e servono per il funzionamento stesso della rete.
Il **Server Mail** si occupa di fornire servizi per la posta elettronica, il **Server Web** permette a tutte le postazioni della rete di poter accedere alla rete Internet.
Nel **Server per le applicazioni aziendali** risiedono programmi applicativi in uso all'Azienda.
I tre **Server DNS** si occupano di tradurre un indirizzo della forma `http://www.mazziamari.it`, in uno espresso in forma numerica (richiesta per l'accesso ad Internet). Per questo motivo tutte le macchine che accedono ad Internet devono avere specificato il loro DNS Server.
Nel **Server di Backup** verranno salvati i dati generati dai vari programmi applicativi in uso in modo da garantire una copia di sicurezza.
I sopracitati server sono così disposti:

Nome edificio	**Server**
Agenzia	-
Barificio	DNS, Mail, Web, Proxy
Cremino	DNS, DHCP, App. aziendali
Destinazione	-
Epitaffio	DNS, Backup

Tabella 2: Dislocazione Server

2 Schema Logico della rete

La topologia della rete diverge dallo schema fisico della stessa: i quattro edifici più vicini - Agenzia, Barificio, Cremino e Destinazione) sono collegati tramite fibra ottica, così da garantire un servizio veloce, efficente ed affidabile.
In quanto all'edificio Epitaffio, dato che è molto distante dagli altri, si è deciso di connetterlo ai restanti tramite Virtual Private Network (**VPN**): ciò permette di costruire una rete privata virtuale su un'infrastruttura pubblica, usando una rete non dedicata (in questo caso Internet). L'uso di VPN per l'edificio EPitaffio, rende la soluzione di gran lunga più economica, semplice e sicura rispetto all'uso di altre tecnologie come la fibra ottica.

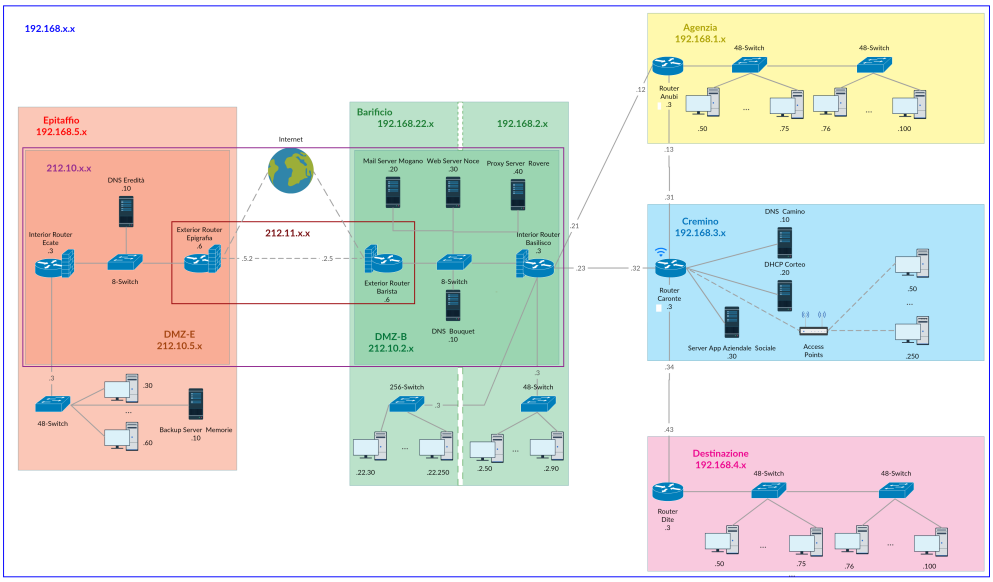

Figura 2: Schema Logico

Struttura della rete Alla rete principale è stato assegnato l'IP di classe B **192.168.0.0/24**, al quale corrisponde il nome di dominio **http://www.mazziamari.it**; Questa è stata suddivisa in sottoreti, ognuna corrispondente a ciascun edificio:

- Agenzia: 192.168.1.0/24
- Barificio: 192.168.2.0/24 e 192.168.22.0/24
- Cremino: 192.168.3.0/24
- Destinazione: 192.168.4.0/24
- Epitaffio: 192.168.5.0/24

DMZ Per il collegamento a internet degli edifici Barificio ed Epitaffio, si è deciso di introdurre una De-Militarized Zone (DMZ), posta per l'appunto agli estremi della rete, a svolgere funzioni di sicurezza e per contenere i server che forniscono servizi accessibili anche dall'esterno della rete. Questa rete sarà trattata in dettaglio successivamente nei singoli edifici che la contengono.

2.1 A: Agenzia

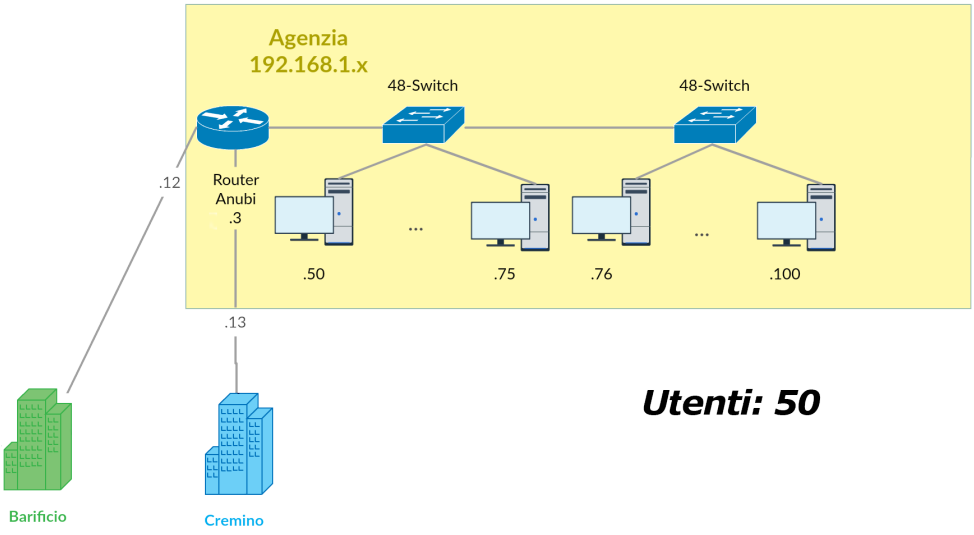

Figura 3: Dettaglio sottoreterete 1

All'edificio Agenzia è stata assegnata la sottorete con indirizzo **192.168.1.0/24** (unica sottorete per l'edificio, visto il numero esiguo di utenti che deve ospitare)
Questa è raggiungibile tramite il router **Anubi** con indirizzo **192.168.1.3**, tramite le interfacce *192.168.2.12* per *Barificio* e *192.168.3.13* per *Cremino*.

Dispositivo	Nome	IP
Router	Anubi	192.168.1.3
Host 1	agenzia01	192.168.1.50
...	...	...
Host 50	agenzia50	192.168.1.100

Tabella 3: Riepilogo A

2.2 B: Barificio

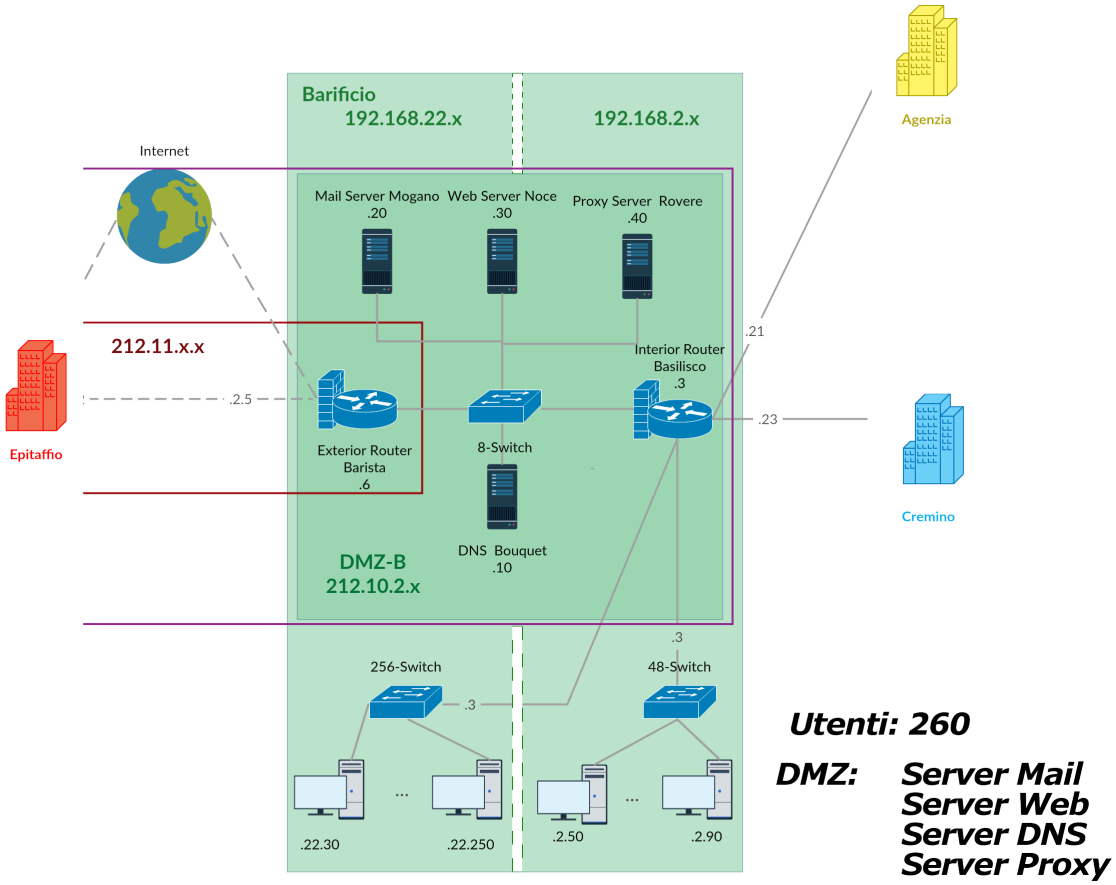

Figura 4: Dettaglio sottoreterete 2

All'edificio Barificio sono state assegnate le sottoreti con indirizzo **192.168.2.0/24** e **192.168.22.0/24** (due sottorete per l'edificio B, visto il numero cospicuo di utenti che deve ospitare)
Queste sono raggiungibili tramite il router **Basilisco** con indirizzo 212.10.2.3, tramite le interfacce *192.168.1.21* per *Agenzia* e *192.168.3.23* per *Cremino*, che comunica cone le due sottoreti mediante le sue interfacce **192.168.2.3** e **192.168.22.3**.

Dispositivo	Nome	IP
Interfaccia1	Basilisco	192.168.2.3
Host 1	barificio01	192.168.2.50
...	...	...
Host 50	barificio40	192.168.2.90
Interfaccia2	Basilisco	192.168.22.3
Host 51	barificio41	192.168.22.30
...	...	...
Host 260	barificio260	192.168.22.260

Tabella 4: Riepilogo B

2.2.1 DMZ

Nell'edificio B è presente anche la DMZ, nella quale sono inclusi i server che devono risultare accessibili anche dall'esterno della rete. Alla DMZ è stata assegnata la rete **212.10.2.0/24**.
Agli estremi della DMZ sono presenti **due router / firewall** che svolgono funzione di filtraggio e protezione per la rete:

- il firewall-router interno **Basilisco** con indirizzo **212.10.2.3** protegge la DMZ dagli accessi provenienti dalla LAN
- il firewall-router esterno **Barista**, che comunica con internet, con indirizzo **212.10.2.6** protegge la DMZ dagli accessi esterni.

In particolare il firewall collocato tra la LAN e la DMZ filtra i pacchetti in transito mediante le due catene *dmzlan e landmz*, svolgendo anche la funzione di NAT.
Allo stesso modo il firewall esterno usa le due catene *inetdmz e dmzinet* per effettuare *packet filtering* tra Internet e la DMZ.

Dispositivo	Nome	IP
Firewall/Router Interno	Basilisco	212.10.2.3
Firewall/Router Esterno	Barista	212.10.2.6
DNS server	Bouquet	212.10.2.10
Mail server	Mogano	212.10.2.20
Web server	Noce	212.10.2.30
Proxy server	Rovere	212.10.2.40

Tabella 5: Riepilogo B

2.3 C: Cremino

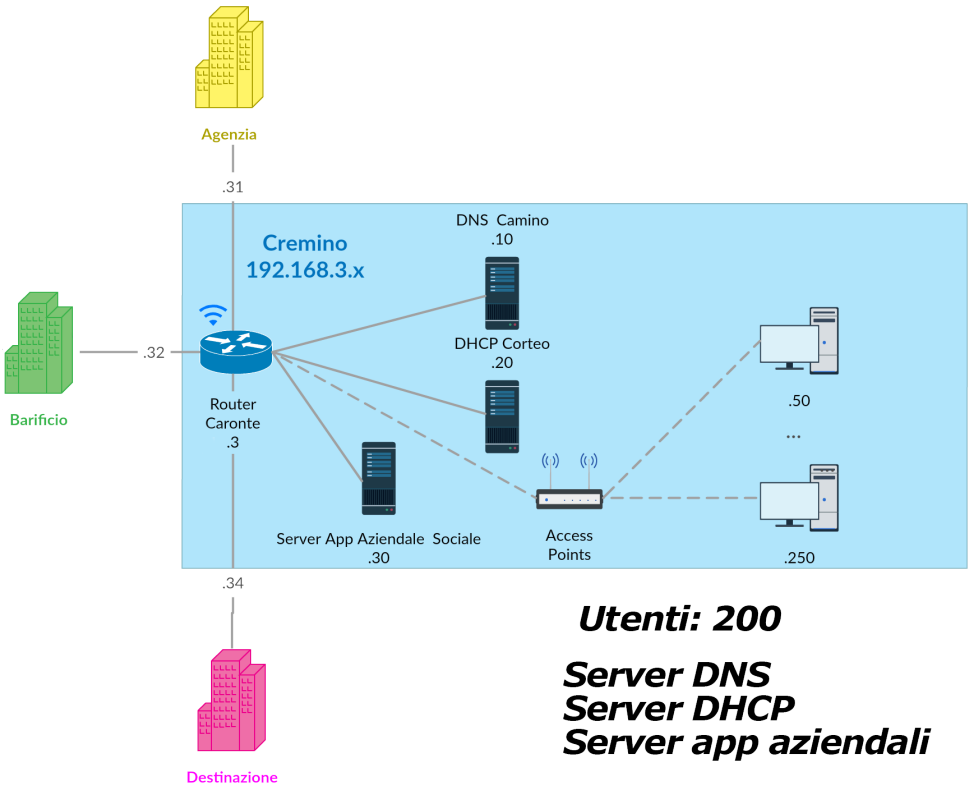

Figura 5: Dettaglio sottoreterete 3

All'edificio Cremino è stata assegnata la sottorete con indirizzo **192.168.3.0/24** Questa è raggiungibile tramite il router **Caronte** con indirizzo **192.168.3.3**, tramite le interfacce *192.168.1.31* per *Agenzia*, *192.168.2.32* per *Barificio* e *192.168.4.34* per *Destinazione*.
La sottorete è usufruibile dagli host in forma wireless, mediante gli access points collocati in vari punti dell'edificio; E' una rete che può presentare un numero variabile di hosts (max 200) in base a quanti utenti vi si connettono. Per questo motivo, si è deciso di assegnare agli hosts presenti un **indirizzo dinamico** tramite DHCP in un range che varia da 192.168.3.50 a .250.
Di conseguenza, nel suddetto edificio sarà presente un **server DHCP** (e un server per le applicazioni aziendali).
Infine è presente un server DNS interno, adibito alla risoluzione dei nomi degli host della LAN.

Dispositivo	Nome	IP
Router	Caronte	192.168.3.3
DNS server	Camino	192.168.3.10
DHCP server	Corteo	192.168.3.20
Server app aziendali	Social	192.168.3.30
Host 1	agenzia01	192.168.3.50
...	...	...
Host 50	agenzia50	192.168.3.250

Tabella 6: Riepilogo C

2.4 D: Destinazione

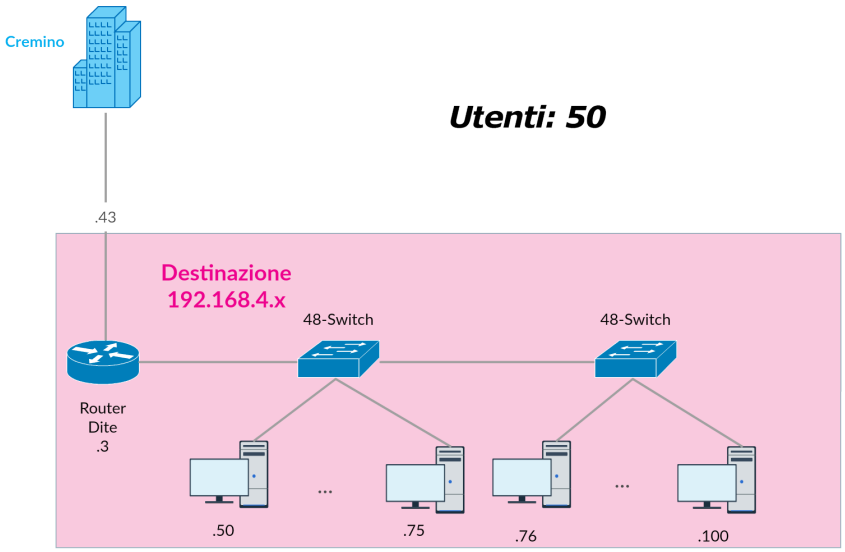

Figura 6: Dettaglio sottoreterete 4

All'edificio Destinazione è stata assegnata la sottorete con indirizzo **192.168.4.0/24** (unica sottorete per l'edificio, visto il numero esiguo di utenti che deve ospitare)
Questa è raggiungibile tramite il router **Dite** con indirizzo **192.168.3.3**, tramite l'interfaccia *192.168.3.43* per *Cremino*.

Dispositivo	**Nome**	**IP**
Router	Dite	192.168.3.3
Host 1	destinazione01	192.168.3.50
...	...	...
Host 50	destinazione50	192.168.3.100

Tabella 7: Riepilogo D

2.5 E: Epitaffio

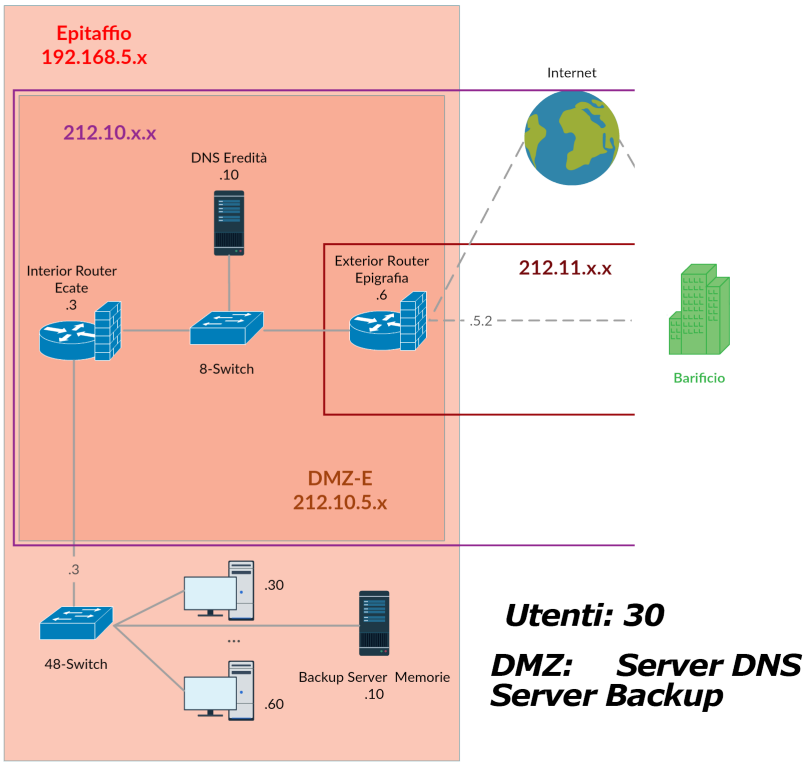

Figura 7: Dettaglio sottoreterete 5

All'edificio Epitaffio è stata assegnata la sottorete con indirizzo **192.168.5.0/24** (unica sottorete per l'edificio, visto il numero esiguo di utenti che deve ospitare)

Dispositivo	Nome	IP
Interfaccia	Ecate	192.168.5.3
Host 1	epitaffio01	192.168.5.30
...	...	...
Host 30	epitaffio40	192.168.5.60
Backup server	Memorie	192.168.5.10

Tabella 8: Riepilogo E

2.5.1 Rete intermedia

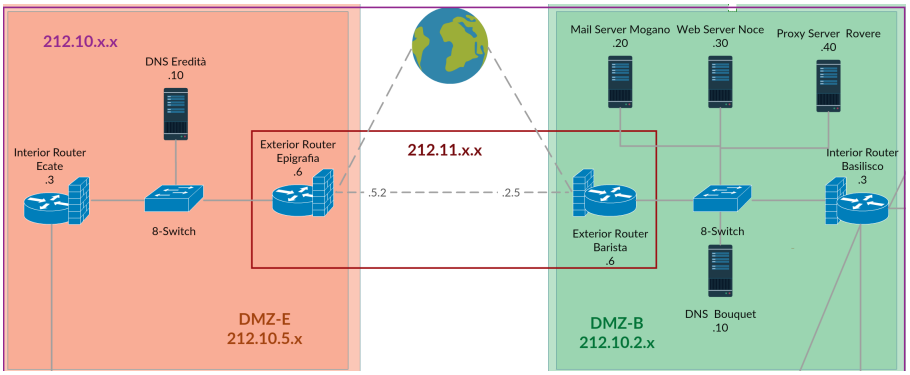

Figura 8: Dettaglio rete intermedia delle DMZ

L'edificio E deve poter essere raggiunto sia dall'edificio B che dall'edificio D: data la distanza da essi, si è deciso di farli comunicare mediante **VPN**.
A tal scopo abbiamo deciso di far comunicare E direttamente con internet (con opportuna aggiunta di DMZ) ed abbiamo creato una rete privata che connette la DMZ di E con la DMZ di B, corrispondente all'indirizzo **212.11.0.0/16**. Ciò è reso possibile facendo comunicare l'interfaccia *212.11.5.2* del router esterno di E **Epigrafia** con indirizzo **212.10.5.6**, con l'interfaccia *212.11.2.5* del router esterno di B.
Così facendo, E può comunicare con B mediante suddetta rete e con D passando per B e C.

2.5.2 DMZ

Nell'edificio E è presente anche la DMZ, nella quale è presente il server DNS.
Alla DMZ è stata assegnata la rete **212.10.5.0/24**.
Agli estremi della DMZ sono presenti **due router / firewall** che svolgono funzione di filtraggio e protezione per la rete:

- il firewall-router interno **Ecate** con indirizzo **212.10.5.3** protegge la DMZ dagli accessi provenienti dalla LAN
- il firewall-router esterno **Epigrafia**, che comunica con internet, con indirizzo **212.10.5.6** protegge la DMZ dagli accessi esterni.

I firewall lavorano in modo analogo a quelli della DMZ dell'edificio B.

Dispositivo	Nome	IP
Firewall/Router Interno	Ecate	212.10.5.3
Firewall/Router Esterno	Epigrafia	212.10.5.6
DNS server	Eredità	212.10.5.10

Tabella 9: Riepilogo DMZ E

3 Routing

Per quanto riguarda il routing all'interno della rete:

- Per gli edifici A, B, C si è deciso di utilizzare un routing dinamico configurando il protocollo **RIP** (Routing Information Protocol), un protocollo di routing interno basato su metrica vettore-distanza, gestito nel nostro caso dal demone *gated*.
- Per gli edifici E, D e la rete intermedia 212.11.0.0 si è deciso di utilizzare un routing statico tramite il comando **route add**, essendoci una sola strada percorribile per giungervi.

4 DNS

Nella rete sono presenti tre server DNS: due esterni, che risiedono nelle due DMZ, ed uno interno.

- I DNS esterni sono situati nella DMZ dell'edificio B (*Bouquet*) e in quella dell'edificio E (*Eredità*) e sono
  - master dei server della DMZ (i due DNS traducono in nomi gli indirizzi dei server cui si accede dall'esterno - ciò permette la presenza online dell'azienda)
  - slave tra di loro per la risoluzione dei nomi di internet
- Il DNS interno, posto nell'edificio C (*Camino*), è:
  - master delle reti interne (esso permette di accedere più comodamente alle varie macchine in rete)
  - slave dei due DNS esterni (chiede ai precedenti per quanto riguarda i server della DMZ e per la risoluzione dei nomi di internet)

Ciò rende anche più sicura l'intera rete in quanto dall'esterno non è possibile accedere ai nomi interni.

5 Sicurezza

5.1 Firewalls

Per soddisfare gli standard minimi di sicurezza, si è scelto di adoperare due firewall distinti per DMZ (quattro in totale), configurati tramite `iptables`, integrati rispettivamente nei due router Barificio e nei due router di Epitaffio. Grazie ad essi, la DMZ risulta protetta sia dagli accessi provenienti dalla rete locale che da quelli esterni, come sopra spiegato.

5.2 Hardening: il server per applicazioni aziendali

La sicurezza del server per applicazioni aziendali è stata rafforzata filtrando i pacchetti TCP con un wrapper e facendovi girare il superserver `xinetd`, che a sua volta monitora le richieste ai servizi telnet, SSH e NFS talvolta, come nel caso di telnet, disabilitandoli completamente.

6 Preventivo di spesa

Componente	**Quantità**	**Prezzo cad.**	**Prezzo tot.**
TP-Link TL-SF1048 Switch 48 Porte	4	154.34 EUR	926.04 EUR
WiFi access point	3	130 EUR	390 EUR
Fibra ottica	2100 m	6.34 EUR/m	13314 EUR
Cavo UTP	3000 m	2.65 EUR/m	7950 EUR
VPN		300 EUR annui	300 EUR annui
		TOTALE:	**22880.04 EUR**

Tabella 10: Costo delle componenti hardware

Al costo della componentistica va sommato il costo dell'installazione, pari a 20.000 euro, per un totale complessivo di 42880.04 euro.