



Elaborato di Corbetta Davide

I.I.S. Jean Monnet

a.s. 2020/21



Indice

- **Realtà di interesse (pag. 3-4)**
- **Architettura di rete (pag. 5-10)**
- **Analisi del Database (pag. 11-)**
- **Interrogazioni significative**
- **Struttura funzionale del sistema**



Realtà di interesse

La startup “OneClick Sharing” nata nel settore abbigliamento, adotta un modello di condivisione e scambio seguendo il principio della “sharing economy” (economia della condivisione, promuovendo forme di consumo più consapevoli basate sul riutilizzo) e trasformando un problema in opportunità economica, con benefici ambientali per il sistema ed economici per le famiglie. L’azienda vuole realizzare una piattaforma che permetta di gestire il riciclo di vestiti.

Realizzare:

- Il progetto, anche mediante rappresentazioni grafiche, dell’infrastruttura tecnologica e informatica necessaria a gestire il servizio nel suo complesso, dettagliando:
 - L’architettura della rete e le caratteristiche dei sistemi server
 - Le modalità di comunicazione tra server e dispositivi utilizzati, descrivendo protocolli e servizi software da implementare
- L’analisi della base di dati per la gestione del servizio sopra descritto, in particolare
 - Il modello concettuale
 - Il modello logico;
 - Le interrogazioni significative in linguaggio SQL
 - Il progetto di massima della struttura funzionale del sistema



Studio della realtà di interesse

Dalla richiesta del testo si capisce che si dovrà realizzare sia l'infrastruttura di rete, che la piattaforma web con il Database per la startup "OneClick Sharing", nata con l'obiettivo di creare un modello di condivisione e scambio di abiti di seconda mano.

Per quanto riguarda l'infrastruttura di rete si dovrà creare una rete prima di tutto sicura, gestendo quindi anche le varie autorizzazioni date ai clienti così come agli amministratori che la gestiscono. Inoltre si dovrà considerare anche il fattore scalabilità. Difatti in futuro ci potranno essere ulteriori aggiornamenti alla rete, per questo dovrà essere garantita la possibilità d'incrementare o ridurre le capacità del sistema a seconda delle esigenze del momento.

Oltre a ciò sarà necessario gestire i vari server presenti sulla rete, tra le quali quello per "hostare" la piattaforma web e uno per controllare il Database.

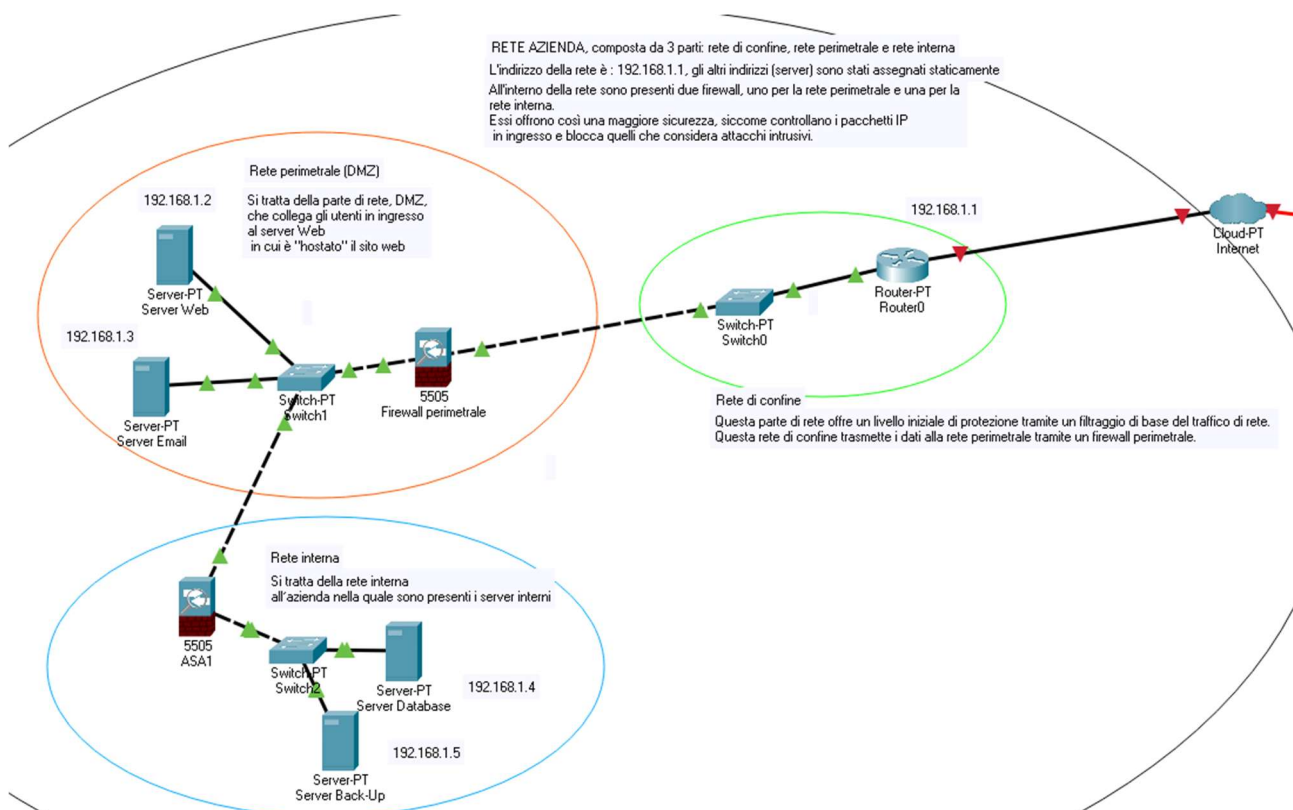
Invece pensando alla piattaforma web, il sito da realizzare dovrà essere "user friendly", quindi di facile utilizzo anche per i nuovi clienti. Dovrà dare la possibilità di scambio dei vestiti di seconda mano e il salvataggio delle informazioni relative in un Database.



Architettura di Rete

Durante la realizzazione dell'architettura di rete si è ritenuto necessario "suddividere" la rete in 3 sezioni in modo tale da creare tre diversi "livelli":

1. Rete esterna (di confine, colorata in verde)
2. Rete perimetrale (DMZ, colorata in arancione)
3. Rete interna (colorata in azzurro)



In questa rete inoltre saranno presenti diversi server con funzioni diverse:

- Un Server per "hostare" la piattaforma web
- Uno di tipo SMTP (Simple Mail Transfer Protocol) per poter gestire l'invio e la ricezione di email
- Un Server per poter gestire il Database nel quale saranno inseriti tutte le informazioni della piattaforma web.
- Un ultimo Server per il Backup in modo da avere una maggiore sicurezza in caso di problemi sulla rete.

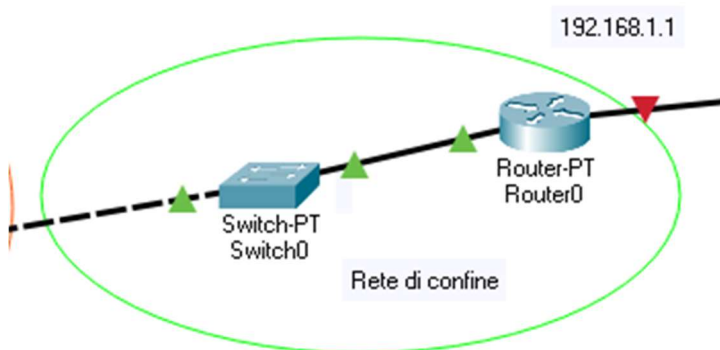


-Rete Esterna (di confine)

Si tratta della parte di rete direttamente connessa a Internet tramite un router che fornisce un livello iniziale di protezione mediante il filtraggio di base del traffico di rete.

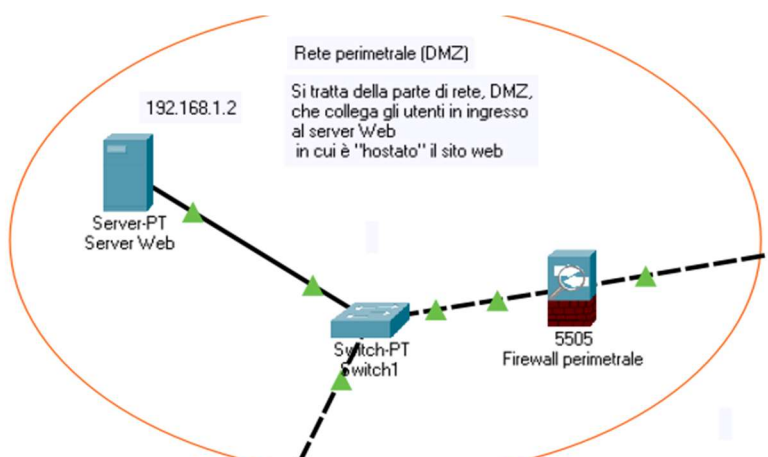
Successivamente il router trasmette i dati alla rete perimetrale tramite l'utilizzo di un firewall perimetrale.

L'indirizzo utilizzato in questa rete è un semplice IP statico di classe C: 192.168.1.1



-Rete Perimetrale (DMZ)

Si tratta della parte di rete marginale, definita come DMZ (Demilitarized Zone), che collega gli utenti in ingresso al Server Web nel quale sarà "hostato" il sito web. Questa sarà l'unica parte di rete visibile completamente all'esterno siccome gli utenti dovranno connettersi sia alla piattaforma web che al server SMTP per l'invio e la ricezione delle email. All'interno inoltre è presente un Firewall perimetrale per un'ulteriore sicurezza.



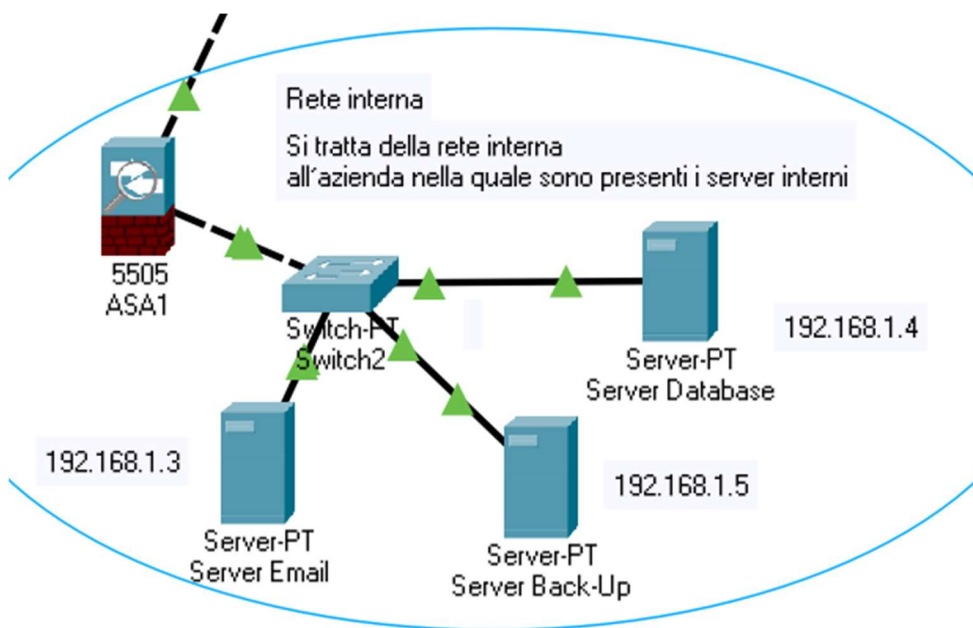


-Rete Interna

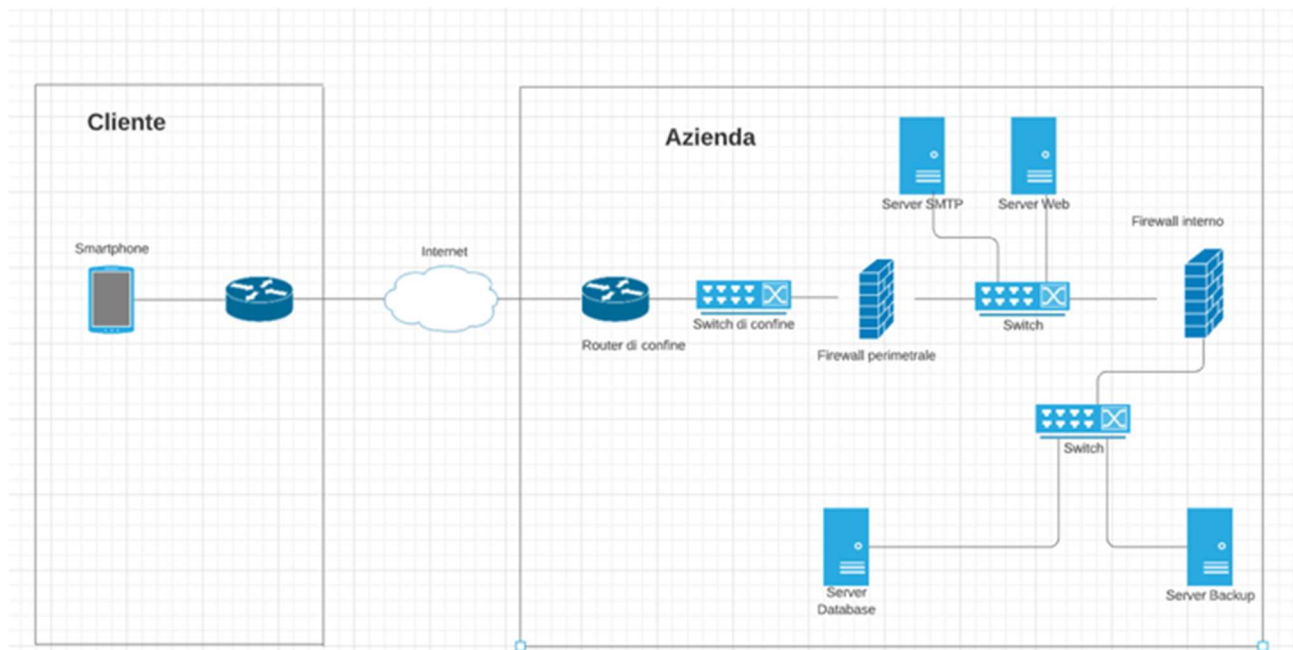
Si tratta della rete più interna all'azienda nella quale sono presenti i server interni (Server per gestire il Database e il Server di Backup).

Questi elementi saranno completamente inaccessibili agli utenti, non avendo alcun permesso. Essa infatti sarà accessibile solo agli amministratori di azienda, che hanno la possibilità di modificare la rete.

In questa parte di rete è presente un altro Firewall per un ulteriore livello di sicurezza.



All'interno della rete saranno utilizzati vari indirizzi statici da un unico indirizzo pubblico di classe C.



In questo caso si può vedere bene la comunicazione tra il cliente e l'azienda, attraverso internet.

Per ottenere buone prestazioni internet sarà necessario l'utilizzo di un buon provider e della fibra ottica almeno di tipo FTTC (Fiber To The Cabinet). In questo modo arriverà un cavo di fibra fino all'armadio stradale esterno e poi verrà esteso tramite cavo di rame.

Con questa soluzione si potranno raggiungere velocità fino a 100 o 200 Mbps (mega bit al secondo), con prestazioni migliori tanto più l'azienda è vicina a un armadio stradale da cui parte l'ultimo tratto della connessione.

Questa tecnologia porta con sé alcuni vantaggi come una migliore convenienza e una facile scalabilità in caso di cambiamenti futuri.

Ovviamente le velocità raggiunte saranno inferiori rispetto alla tecnologia FTTH (con la quale la fibra arriva direttamente in azienda), però anche il costo sarà maggiore.



Architettura e protocolli utilizzati

L'architettura di questa rete è di tipo Client-Server. Abbiamo infatti un server nel quale viene hostato il sito web e i client (utenti) che si connettono ad esso.

HTTP e TCP

La gestione delle richieste e risposte tra client e server avviene tramite protocollo HTTP (HyperText Transfer Protocol) il quale definisce l'interazione (richieste e risposte) tra Client e Server Web. L'HTTP permette l'utilizzo di 4 metodi:

- GET, per restituire la rappresentazione di una risorsa
- PUT, per modificare lo stato di una risorsa
- POST, per creare una nuova risorsa
- DELETE, per eliminare una risorsa

Per instaurare la connessione tra due client e server e gestire la consegna dei pacchetti da un sistema all'altro verrà invece utilizzato il protocollo TCP rispetto al protocollo UDP.

Questo protocollo offre numerosi vantaggi:

- È affidabile, in quanto la ricezione e la conferma dei pacchetti sono garantite.
- È di tipo connection oriented, il che significa che richiede endpoint per stabilire un canale sicuro prima di trasmettere i messaggi.

Ovviamente in futuro potrà essere utilizzato un protocollo più sicuro come quello HTTPS.

Questo permetterebbe di risolvere 3 importanti problemi:

- Crittografia. I dati scambiati verrebbero criptati per proteggerli dalle intercettazioni. Ciò significa che, mentre l'utente consulta un sito web, nessuno può "ascoltare" le sue conversazioni, tenere traccia delle attività svolte in più pagine o carpire le sue informazioni.
- Integrità dei dati. I dati non potrebbero essere più modificati o danneggiati durante il trasferimento, intenzionalmente o meno, senza che ciò venga rilevato.

DNS

In questa rete viene utilizzato un sistema il DNS (Domain Name System). Il DNS aiuta a dirigere il traffico su Internet collegando i nomi di dominio con server web reali. In sostanza, prende una richiesta "human-friendly" (nome di dominio) e lo traduce in un indirizzo IP del Server (che "hosta" la piattaforma web).

In questo modo gli utenti si potranno collegare al sito tramite un nome specifico, senza doversi per forza ricordare un indirizzo IP.



DMZ

La rete perimetrale è definita come rete DMZ (Demilitarized Zone).

Essa è un'area in cui sia il traffico WAN che quello LAN sono fortemente limitati e controllati; in pratica, si tratta di una zona "cuscinetto" tra interno ed esterno, che viene attestata su una ulteriore interfaccia di rete del firewall, oppure viene creata aggiungendo un firewall, come nello schema qui sopra.

Questa sarà l'unica parte di rete accessibile anche ai clienti che si connettono alla piattaforma web. In questo modo gli utenti/clienti collegati alla rete potranno accedere solo al Server Web e non nella rete interna. Di fatti questa parte di rete sarà riservata soltanto agli amministratori d'azienda.

Firewall

In due parti della rete inoltre vengono utilizzati i firewall.

Nella parte DMZ il firewall permetterà l'accesso a tutti mentre nella parte più interna il firewall permetterà un maggiore livello di sicurezza bloccando i tentativi di connessione ai Server interni.

Come specificato prima i server in cui viene "hostato" la piattaforma web e il database sono interni. Questo comporta il non utilizzo del "cloud computing", ovvero l'utilizzo di piattaforme esterne per la gestione del sito internet, database e email.

Ovviamente questo comporta dei vantaggi e degli svantaggi.

Il principale svantaggio è quello che bisogna appoggiarsi a una piattaforma esterna pagandola con un abbonamento.

Un altro svantaggio è quello di affidare dati di moltissimi clienti registrati ad un ente esterno, fidandosi così di loro.

Allo stesso tempo ci sono anche dei vantaggi. Infatti non si dovrà più gestire la rete, siccome sarà tutto esterno e inoltre, in caso di necessità, il gestore potrà espandere o limitare con estrema flessibilità l'infrastruttura.