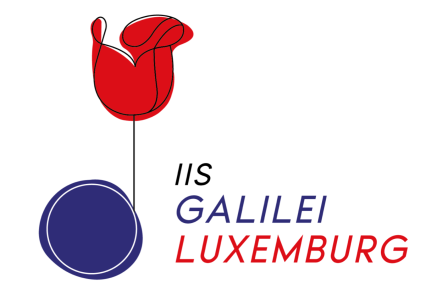
**RELAZIONE CAPOLAVORO**



**CAPOLAVORO REALIZZATO DA:**

**Studenti: Docenti:**

Ivano Hu Piero Greco

Stefano Ichim Marino Torsello

John George Roxas

Simon Isgrò

**INDICE**

[**OBIETTIVO**](#_p54mc7n02bv6) **1**

[**IPOTESI 2**](#_q51g1z1rzp7a)

[**STRUMENTI UTILIZZATI**](#_g65k6nsmbpzi) **3**

[**TABELLA DI INDIRIZZAMENTO**](#_nvz6il1az1w8) **4**

[**STRUTTURA DEL PROGETTO**](#_tjjjpbhjppwf) **5**

[**DESCRIZIONE DEL PROGETTO**](#_jdxl0pv7qtpk) **6**

[**CONCLUSIONE**](#_b4zj33yi8qpv) **7**

# OBIETTIVO:

In questo progetto ci è stato assegnato il primo piano, di cui il nostro compito è di cablare e di inserire i vari device e strumenti elettronici della “Cisco Packet Tracer” necessari per ogni stanza presente nel primo piano dell’Istituto Galileo Galilei in Via Alessandro Paravia, 31 (angolo Via Capecelatro - San Siro) 20148 Milano.

Per sviluppare questo progetto abbiamo usato la versione 8.2.1.0118 della “Cisco Packet Tracer”.

# IPOTESI:

* Stabilire una stanza del piano dove sviluppare i server;
* Sviluppare e impostare l’access point con il collegamento Wi-Fi di 2.4GHz;
* La rete utilizza l’IP di classe C di IPv4: 192.168.1.0;
* Impostare il server DHCP e stabilire il range di IP che vengono associate ai dispositivi. (Range IP: 192.168.1.41 al 192.168.1.255);
* Stabilire i numeri di dispositivi di ogni stanza.
* Stabilire un Router in una stanza qualsiasi per creare una rete interna, e possibilmente anche per creare una rete esterna.
* Aggiungere nel server DNS WEB i protocolli POP e SMTP mettendo come dominio galilux.edu.it
* Aggiungere nel server EMAIL nella sezione EMAIL tre user: **studente**, **docente** e **amministrativa** e stabilire in quali PC assegnare le informazioni dei vari user.
* Stabilire nel server FTP nella sezione FTP Username e Password:

Username: **server\_FTP** Password: **1234**

* Aggiungere in vari corridoi le sirene (allarmi) e macchinetta del caffè. Mentre i printer (stampanti) in alcune stanze in cui c’è n’è bisogno.
* Registrarsi nel sito [www.iot\_galilux1.it](http://www.iot_galilux1.it) con Username e Password per controllare i dispositivi collegati nella stessa rete da remoto:

Username: **galilux\_1** Password: **1234**

* Configurare l’SSID e Password per l’ Access Point per connettere: **dispositivi IoT**, **stampanti** e **vari PC alla stessa rete**.

# STRUMENTI UTILIZZATI:

**Primo corridoio:**

* PC - PT × 5
* Switch 2960 - 24TT × 1
* Access Point - PT × 1
* Router - PT × 1
* Macchinetta del caffè × 1
* Sirena (allarme) × 1

**Secondo corridoio:**

* PC - PT × 8
* Switch 2960 - 24TT × 1
* Access Point - PT × 1
* Server DHCP - DNS - WEB - FTP - EMAIL - IOT- DB
* Printer - PT × 1
* Sirena (allarme) × 1

**Terzo corridoio:**

* PC - PT × 11
* Switch 2960 - 24TT × 2
* Access Point - PT × 2
* Printer - PT × 1
* Sirena (allarme) × 1

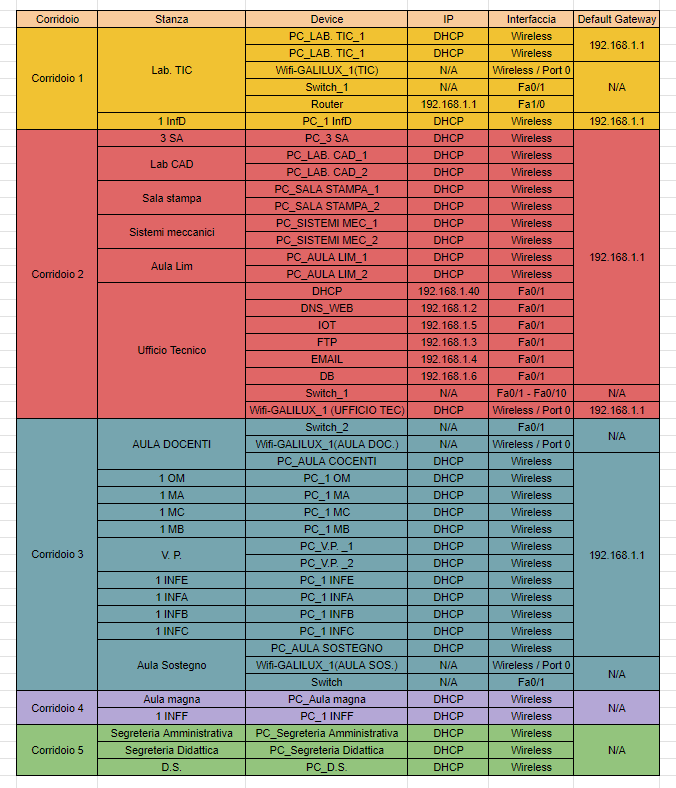
**Quarto corridoio:**

* PC - PT × 2
* Sirena (allarme) × 1

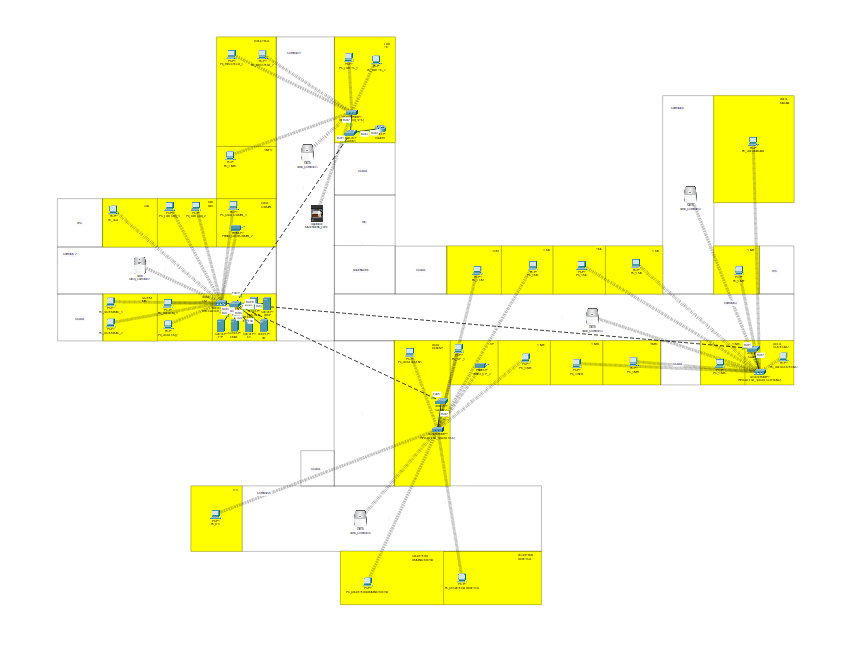
**Quinto corridoio:**

* PC - PT × 3
* Sirena (allarme) × 1

# TABELLA DI INDIRIZZAMENTO:



# STRUTTURA DEL PROGETTO:



# DESCRIZIONE DEL PROGETTO:

In questo progetto abbiamo strutturato il primo piano della scuola Galileo Galilei organizzandoci attraverso le ipotesi che abbiamo stabilito inizialmente.

La nostra idea iniziale sarebbe di stabilire come stanza per sviluppare i **server l’ufficio tecnico**, situato tra il primo e il secondo corridoio. Dopo aver stabilito la stanza per sviluppare i server, abbiamo inserito i vari server tra cui **DHCP - DNS - WEB - FTP - EMAIL - IOT- DB** tutti collegati ad uno **switch**. Attraverso cavi abbiamo collegato lo switch successivamente con gli altri switch, che sono presenti negli altri corridoi del piano per avvenire la comunicazione tra i dispositivi che si trovano in diverse stanze e corridoi, e soprattutto per far si che i server, facessero il loro lavoro ai dispositivi presenti per ogni stanza nei diversi corridoi.

Per ogni switch presente nei diversi corridoi abbiamo collegato un **access point** per consentire ai dispositivi wireless, tra cui PC, stampanti e dispositivi IoT, di connettersi nella stessa rete utilizzando **Wi-Fi di 2.4GHz**. Una volta fatto ciò, dopo aver inserito vari PC su ogni stanza del piano, abbiamo successivamente assegnato a diversi PC e serverindirizzi ipdi classe C di IPv4: **192.168.1.0.** Mentre per quanto riguarda gli altri PC a cui non abbiamo assegnato indirizzi ip staticamente, abbiamo deciso di impostare il server DHCP e stabilire il range di ip che va da **192.168.1.41 a 192.168.1.255**, consentendo ai PC rimanenti senza indirizzo IP di ottenere un indirizzo IP automaticamente dal server DHCP.

Successivamente, dopo aver configurato i vari PC e server, abbiamo aggiunto un **router** nel **laboratorio TIC**, situato nel corridoio 1, per poi successivamente configurarlo. Abbiamo aggiunto questo router per creare una rete interna e possibilmente per creare una rete esterna sul quale lo collegheremo nei diversi piani dell’Istituto.

Una volta fatto ciò abbiamo lavorato con i diversi **server**:

- Sul **server DNS - WEB**, dopo averlo configurato, siamo andati nella sezione DNS dove abbiamo aggiunto i protocolli POP e SMTP che permettono il trasferimento e il ricevimento delle Email tra dispositivi, mettendo come dominio **galilux.edu.it**.

- Di seguito nel **server EMAIL**, nella sezione EMAIL abbiamo aggiunto tre user, mettendo come dominio **galilux.edu.it**, che sarebbero lo **studente, il docente e amministrativa** impostando una password per ciascuno:

- User: studente - Password: studente

- User: docente - Password: docente

- User: amministrativa - Password: amministrativa

Successivamente abbiamo deciso poi di assegnare tre PC sul quale vogliamo inserire le informazioni dei vari user tra cui:

**1**. **PC - PT 3SA** (corridoio 2): studente;

**2**. **PC - PT Aula docenti** (corridoio 3): docente;

**3**. **PC - PT Segreteria amministrativa** (corridoio 5): amministrativa;

Dopo aver inserito le informazioni di indirizzo email di un user a questi 3 PC, questi dispositivi possono inviare e ricevere tra di loro messaggi email, attraverso la crittografia simmetrica e asimmetrica i messaggi che vengono trasferiti da un dispositivo all’altro vengono crittografati, cioè solo il mittente e il destinatario possono visualizzare questi messaggi.

- Sul **server FTP** dopo averlo configurato, siamo andati nella sezione FTP dove abbiamo eliminato le informazioni che non ci servivano e aggiunto nel user setup un username e una password consentendo di scrivere, leggere eliminare e rinominare:

**Username: server\_FTP Password: 1234.**

Di seguito per verificare che il server FTP funziona, a un qualsiasi PC presente nel piano siamo entrati nel pannello di controllo **text editor** dove abbiamo creato un file di testo. Poi successivamente siamo entrati nel pannello di controllo **comand prompt** dove abbiamo digitato una serie di comandi inviando il file usando il comando **put**. Di seguito ad un pc qualsiasi siamo entrati nel pannello di controllo **comand prompt** dove abbiamo usato il comando **get** per prelevare il file, la stessa cosa accade qui, utilizzando la crittografia simmetrica e asimmetrica i dati trasferiti vengono crittografati e solo chi ha la chiave cioè username e la password possono inviare o prelevare i file dal server FTP.

- Sul **server IOT**, dopo aver inserito gli strumenti necessari, tra cui sirene (allarmi) e macchinetta del caffè nei diversi corridoi, abbiamo configurato il server assegnandogli un indirizzo IP, una Subnet Mask, un Default Gateway e il DNS Server. Successivamente siamo tornati nel server DNS - WEB e siamo andati nella sezione relativa al DNS dove abbiamo aggiunto il record del dominio [www.iot\_galilux1.it](http://www.iot_galilux1.it), associandogli l’indirizzo IP che abbiamo assegnato al server IOT.

Di seguito abbiamo attivato la funzionalità IoT sul server IOT e ritornando sul server

**DNS - WEB** siamo entrati nel pannello di controllo web nel sito www.iot\_galilux1.it e ci siamo registrati utilizzando un nome utente e una password, dove attraverso questo sito noi potevamo controllare i dispositivi IoT da remoto:

**Username: galilux\_1 Password: 1234**

Successivamente, tramite gli **access point** presenti per ogni corridoio, abbiamo configurato l’SSID e una password che sarebbero servite per connettere i dispositivi IoT, stampanti e i vari PC alla stessa rete. Per ciascuno di questi strumenti (dispositivi IoT, stampanti e i vari PC), abbiamo inserito l’SSID e la password dell’access point, dopodiché siamo passati alla configurazione delserver IoT di ogni dispositivo IoT, dove abbiamo specificato il nome del sito web ([www.iot\_galilux1.it](http://www.iot_galilux1.it)) e i dati con cui ci siamo registrati sullo stesso sito, ovvero username e password. Questo ha permesso al server di controllare da remoto tutti i dispositivi IoT che sono collegati tramite access point accedendo al sito [www.iot\_galilux1.it](http://www.iot_galilux1.it).

- Sul **server DB**, una volta configurato, abbiamo utilizzato questo server per gestire, memorizzare e recuperare dati in un database.

# CONCLUSIONE:

In conclusione possiamo dire che, seguendo le ipotesi che abbiamo fatto all'inizio, siamo riusciti a cablare e strutturare il primo piano utilizzando strumenti necessari della “Cisco Packet Tracer” e siamo riusciti a verificare che tutti i server che abbiamo utilizzato funzionano.