IIS Ettore Majorana – Cesano Maderno

La sicurezza nelle reti Wi-Fi

Sviluppo di un'infrastruttura di rete wireless attraverso lo standard Wi-FI dell'istituto scolastico IIS Ettore Majorana

Tesina di maturità

Raffaele Defazio

5^TL

Corso ad indirizzo Telecomunicazioni

Anno scolastico 2015/2016

Introduzione

In un’epoca come quella attuale, in cui il bisogno di essere sempre connessi con il mondo è aumentato a tal punto da essere considerata una necessità primaria, gli individui sono alla continua ricerca di un punto d’accesso, di una porta aperta sulle mille risorse che internet può offrire.

Indice

Il **Wi-Fi**

Con il termine Wi-Fi si intendono un insieme di tecnologie di rete che consentono l'accesso via radio, cioè in wireless a risorse condivise, nonché la comunicazione in wireless fra dispositivi posti in rete. Questa tecnologia è usata principalmente per realizzare delle WLAN (*Wireless Local Area Network*). Normalmente una WLAN viene integrata in una LAN cablata e consente di accedere alla LAN stessa, e quindi a tutti i servizi che essa può offrire, quali accesso a internet ad alta velocità e condivisione di hardware e software.
L'ambito delle WLAN è in continua evoluzione. Sono stati sviluppati e si stanno tuttora definendo diversi standard per la realizzazione delle WLAN e l'ente di standardizzazione che si occupa di tutto questo è la IEEE, più precisamente il gruppo di lavoro 802.11.
Tabella riassuntiva di tutti gli standard 802.11 più diffusi in Europa.

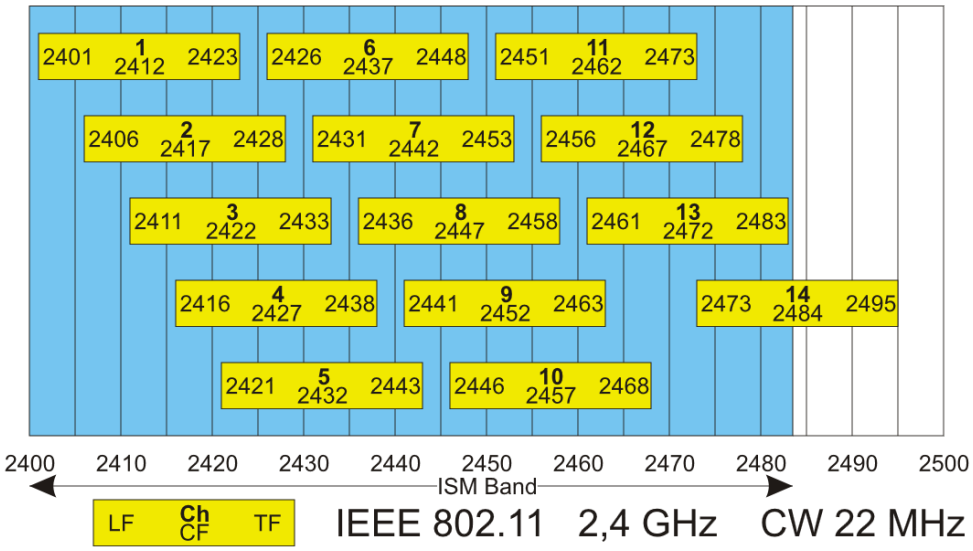
Standard	Frequenza e banda canale	Velocità di trasferimento (Mb/s)	Distanza (metri)	Modulazioni utilizzate
802.11a	5 GHz B = 20 MHz	Fino a 54 Mbit/s	20-40	M-PSK, M-QAM
802.11b	2,4 GHz B = 22 MHz	Fino a 11 Mbit/s	50-100	M-PSK
802.11g	2,4 GHz B = 20 MHz	Fino a 54 Mbit/s	50-80	M-PSK (M=2, 4, 8) M-QAM ($M \geq 16$)
802.11n	Dual band 2,4 GHz, 5 GHz B = 20 MHz o 40 MHz	Fino a 300 Mbit/s (teorico 600 Mbit/s)	Fino ai 120-180[14]	M-PSK (M=2, 4, 8) M-QAM ($M \geq 16$)
802.11ac	5 GHz B = 80 MHz o 160 MHz	1,3 Gbit/s (teorico 3,5 Gbit/s)	10	256-QAM

Quello che differenzia principalmente tutti questi standard, oltre alle velocità di trasferimento e ai tipi di modulazioni usati, è lo stato fisico in quanto definisce le

specifiche relative alle tecniche e alle modalità con cui avviene la ricetrasmissione delle informazioni.

Standard IEE 802.11 b

- Opera a 2,4 GHz con canali aventi banda pari a circa 22 MHz, la cui struttura è riportata nella figura sotto.



- Lo strato fisico supporta una velocità di trasmissione massima pari a 11 Mbit/s.
- Adotta una modulazione a 4 stati denominata QPSK (Quadrature Phase Shift Key).
- Impiega la tecnica di trasmissione DSSS (Direct Sequence Spread Spectrum), che minimizza le interferenze reciproche.
- Può ridurre la velocità, scendendo a 5,5 o 2 o 1 Mbit/s in relazione alle condizioni del canale radio (attenuazioni, disturbi, interferenze) e alle qualità del segnale ricevuto.

Standard IEEE 802.11 g

- Opera a 2,4 GHz con canali aventi banda pari a circa 20 MHz, la cui struttura è riportata nella figura sopra.
- Lo strato fisico supporta una velocità di trasmissione massima pari a 54 Mbit/s.
- Impiega la tecnica di trasmissione a banda larga OFDM (Orthogonal Frequency Division Multiplexing), che consiste nel suddividere la banda di canale a disposizione in 48 sottobande utilizzate in parallelo. Per ottenere la velocità di trasmissione massima, in ciascuna sottobanda si utilizza una modulazione a 64 stati denominata 64-QAM (Quadrature Amplitude Modulation), in grado di trasportare 6 bit per simbolo.
- Può ridurre la velocità, in relazione alle condizioni del canale radio e alla qualità del segnale ricevuto, cambiando il tipo di modulazione, nonché per garantire la compatibilità con apparati conformi allo standard 802.11 b.
- Gli Access Point a standard IEE 802.11 b/g impiegano spesso due antenne, delle quali una viene utilizzata per trasmettere ed entrambe vengono usate per ricevere.

Standard IEEE 802.11 n

Con standard 802.11 n sono stati introdotti diversi miglioramenti sia nello strato fisico sia nello strato MAC.

- Può operare sia nella banda 2,4 GHz sia nella banda (unlicensed) 5 GHz.
- Può operare sia con canali aventi banda 20 MHz sia con canali aventi banda 40 MHz.
- Impiega la tecnica di trasmissione a banda larga OFDM, con un numero di sottocanali maggiore rispetto allo standard 802.11 g (52 sottocanali invece di 48), inoltre è possibile ridurre l'intervallo di guardia tra i simboli trasmessi in OFDM, portandolo da 800 ns a 400 ns. In questo modo si aumenta il throughput in quanto diminuisce l'intervallo di tempo in cui si deve trasmettere nulla.
- Impiega la tecnica MIMO (Multiple In Multiple Out) che consiste nell'impiegare fino a 4 antenne per trasmettere in parallelo dei flussi di bit (fino a 150 Mbit/s per ciascun flusso), raggiungendo così un bit rate totale teorico di 600 Mbit/s. La tecnica MIMO consente inoltre di operare meglio in presenza di ostacoli e di percorsi multipli ovviando al problema del fading.
- Consente di aggregare più PDU e di trasmetterle con un unico header. In questo modo si aumenta il throughput in quanto aumenta il numero di bit informativi trasmessi a parità di bit di servizio (header).
- Supporta la modalità no acknoledgment, che evita l'invio della conferma di corretta ricezione di ogni frame, aumentando così il throughput a discapito dell'affidabilità.
- Supporta il QoS (Quality of Service), che consiste nella possibilità di differenziare il trattamento dei flussi informativi dando delle priorità differenti, per esempio i flussi audio e video possono avere priorità maggiore rispetto al normale traffico dati.
- VLAN (Virtual LAN): gli AP possono essere configurati per creare o estendere delle VLAN anche per i client che accedono in rete in modalità wireless.
- Virtual Access Point e MultiSSID: un unico AP fisico può essere configurato per definire un certo numero di AP virtuali, ciascuno con proprio SSID, in modo da far vedere ai client una molteplicità di WLAN, realizzate però con un unico AP fisico.
- Wireless Intrusion Protection (WIP): l'AP è in grado di monitorare l'ambiente radio per rilevare la presenza di altri AP e mostrarne le caratteristiche così da permettere di rilevare la presenza in rete di AP installati senza autorizzazione.
- Connection Limiti e User Limit: consente di limitare il numero massimo di client che si possono associare a uno stesso AP, in modo da obbligare i client a ripartirsi fra più Access Point (load balancing) nonché aumentare la sicurezza.

Standard IEEE 802.11 ac

- Opera unicamente in banda unlicensed a 5 GHz
- Impiega la tecnica di trasmissione a banda larga OFDM. In ciascun sottocanale si impiega la modulazione QAM con un numero di stati che può arrivare a 256, in grado di trasportare fino a 8 bit per simbolo.
- Può operare con canali aventi banda a 80 MHz fino a 160 MHz.
- Impiega la tecnica MIMO, con un numero di antenne che in teoria può arrivare a 8, per trasmettere fino a 8 flussi di bit in parallelo. Ciascun flusso di bit può supportare una velocità massima di 433 Mbit/s.

- Un AP 802.11 ac equipaggiato con 3 antenne MIMO può così supportare una velocità di trasmissione lorda di8 circa 1300 Mbit/s, mentre se si impiegassero 8 antenne si potrebbe arrivare a circa 3,5 Gbit/s.
- I flussi di bit trasmessi da sistema d'antenna MIMO possono anche essere destinati a client diversi (MU-MIMO, Multi User MIMO) rendendo l'AP funzionalmente simile a uno switch.

Sicurezza degli accessi Wi-Fi

Una WLAN che non implementa l'autenticazione e/o la cifratura è una rete aperta a cui tutti coloro che sono nella zona di copertura radio dell'AP possono accedere.

Poiché la trasmissione delle informazioni avviene via radio è potenzialmente possibile per chiunque sia nella zona di copertura del segnale radio avere un accesso alla WLAN se essa non implementa:

- *Autenticazione*: procedura con la quale si verifica se il dispositivo che vuole accedere alla rete Wi-Fi sia autorizzato.
- *Crittografia*: procedura con la quale si rendono decifrabili le informazioni trasmesse solo da chi possiede una chiave di cifratura ben precisa.

(Esistono due tipi di crittografia quella simmetrica e quella asimmetrica.)

Le tecniche per l'autenticazione e la crittografia nelle WLAN sono:

- **WEP** (Wired Equivalent Privacy) è lo standard originario e prevede due tipi di autenticazione. La Open system che non ha nessun tipo di autenticazione, cioè chiunque si trovi nell'area di copertura radio può tentare di accedere alla rete. Per niente sicura. Il secondo tipo è la Shared key (a chiave condivisa) che consiste nel autenticare quei client, che dopo aver attivato la modalità WEP sono in possesso della chiave di cifratura configurata sull'AP.
  La crittografia WEP impiega una chiave statica, da 64 a 128 bit, preconfigurata sull'Access Point e sui client. Lo standard WEP fornisce una protezione assai debole in quanto, essendo statica, la chiave di cifratura può essere ricostruita da opportuni software (Aircrack-ng). Inoltre l'AP autentica il client e non viceversa e quindi il client non può sapere se si collega all'AP desiderato o ad un AP non autorizzato.
- **WPA** (WiFi Protected Access). Questo standard effettua l'autenticazione reciproca fra AP e client. Esistono due versioni per questo standard: La WPA-PSK (WPA-Pre Shared Key) o WPA personale che viene impiegato nelle piccole reti in cui non è presente un server esterno che gestisce l'autenticazione. Richiede la configurazione di una password nell'AP e nei client che costituisce la chiave di criptazione principale (master key) utilizzata per l'autenticazione e come punto di partenza per generare le chiavi di crittografia le quali cambiano continuamente. E' possibile impostare il tempo di rinnovo delle chiavi di crittografia. Diminuendo il tempo di rinnovo si aumenta la sicurezza della rete in quanto si limita il numero di pacchetti che vengono criptati con la stessa chiave. La WPA Enterprise o WPA Aziendale è uno standard che viene impiegato nelle reti medio-grandi in quanto l'autenticazione viene effettuata da un apposito server denominato RADIUS (Remote Autentichation Dial-In User Service) che coordina tutto il processo di autenticazione. Infatti, nel momento in cui l'Access Point riceve una richiesta di autenticazione, non concede l'accesso ma inoltra

tale richiesta al server RADIUS, che coordina tutto il processo di autenticazione. L'AP e il server RADIUS utilizzano per comunicare tra loro un protocollo denominato EAP (Extensible Autentichation Protocol), per cui negli Access Point va attivata la modalità di autenticazione con protocollo EAP (protocollo per l'autenticazione su reti Ethernet denominato 802.1x.).
- Lo standard **WPA 2** costituisce l'evoluzione dello standard WPA. Esso introduce una forma di crittografia più forte denominata AES (Advanced Encryption Standard), che necessita di un hardware in grado di supportarla. Questo standard funziona come lo standard WPA e quindi sia il client che l'AP vanno configurati con la stessa modalità di autenticazione, lo stesso tipo di crittografia e la stessa chiave o passphrase.

Ulteriori misure di sicurezza

Per aumentare la sicurezza delle reti Wi-Fi si può:

- Ridurre la potenza di emissione dell'AP a valori che limitino la copertura radio, in modo che l'area da servire abbia sufficiente copertura ma si limiti quella dall'esterno.
- Disabilitare la trasmissione in broadcast dell'SSID, limitando così la visibilità della rete, ciò però impone di configurare manualmente l'SSID nei client.
- Utilizzare l'autenticazione WPA2-PSK con crittografia AES. Se vi sono stringenti requisiti di sicurezza si può ridurre il tempo di rinnovo della chiave di crittografia.
- Nel caso vi siano solo alcuni dispositivi client autorizzati ad accedere alla WLAN è possibile abilitare negli AP il filtraggio degli indirizzi MAC. In questo modo l'Access Point può consentire o bloccare l'accesso alla WLAN a client che abbiano un determinato indirizzo MAC. Non fornisce una protezione forte in quanto, soprattutto nei sistemi Linux, se si conosce un indirizzo MAC valido è possibile configurarlo come indirizzo da utilizzare per una certa scheda Wi-Fi.
- Cambiare le password di accesso per la configurazione degli Access Point scegliendone una sufficientemente robusta.

CSMA/CA

Il CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) è un protocollo di accesso multiplo che utilizza il rilevamento della portante in cui i nodi tentano di evitare a priori il verificarsi di collisioni. E' di particolare importanza nei casi in cui il rilevamento delle collisioni non è realizzabile, come avviene nel campo delle reti senza fili. Infatti, oltre all'esistenza del problema dei nodi nascosti, il ricevitore radio di un nodo in una rete senza fili non può rilevare in modo affidabile eventuali trasmissioni provenienti da altri nodi mentre il relativo trasmettitore è attivo. Nel momento in cui una stazione vuole tentare una trasmissione, essa ascolta il canale (Listen-before-Transmit). Se il canale risulta libero la stazione attende per un certo lasso di tempo identificato come DIFS (Distributed Inter Frame Space) trascorso il quale, se il canale continua ad essere libero, la stazione inizia la trasmissione del pacchetto. A trasmissione completata il nodo di trasmissione attende per un tempo detto SIFS (Short Inter Frame Space, di durata inferiore al DIFS) la ricezione di un ACK che conferma dell'avvenuta ricezione da parte della stazione ricevente. Durante la trasmissione e lo SIFS le altre stazioni, trovando il canale occupato, non avvieranno

trasmissioni, evitando in tal modo collisioni. Qualora, invece, la stazione trasmittente rilevi il canale occupato oppure si siano verificate delle prenotazioni da parte di altre stazioni, la stazione attende per una durata casuale (detto tempo di backoff) che il canale si liberi. Questa attesa è implementata per mezzo di un timer che viene decrementato solo durante i periodi di inattività del canale, mentre viene invece congelato durante i restanti periodi di trasmissione sul canale da parte di altre stazioni. Quando il timer raggiunge lo zero la stazione effettua un nuovo tentativo di trasmissione.

Crittografia

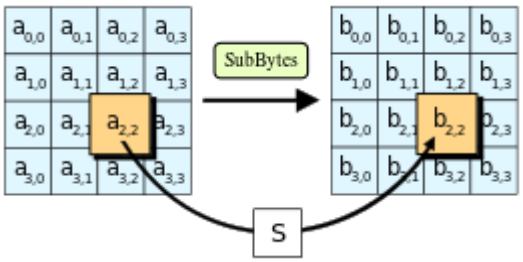
Restando in tema di sicurezza degli accessi e delle informazioni scambiate tra client e Access Point, vi sono due tipi di crittografia:

- La prima è la crittografia simmetrica in cui viene utilizzata una solo chiave per criptare e decriptare i file.
- La seconda è la crittografia asimmetrica in cui ogni utente dispone di due chiavi, una pubblica e una privata. C'è una chiave per crittografare (che chiunque può vedere) e una per decifrare, che conosce solo il destinatario. In altre parole, se Alice vuole ricevere un messaggio segreto da Bob, manda a Bob una scatola vuota con un lucchetto aperto senza chiave. Bob mette dentro il messaggio, chiude il lucchetto, e rimanda il tutto ad Alice, che è l'unica ad avere la chiave. Chiunque può veder passare la scatola ma non può aprirla in quanto non ha la chiave. Alice, deve però tenere al sicuro la chiave privata. Il funzionamento di questo sistema è basato sul fatto che è matematicamente e computazionalmente molto facile moltiplicare due numeri primi (che singolarmente rappresentano la chiave privata, quella che solo Alice conosce per decifrare), ma è invece molto difficile il problema inverso ovvero risalire ai fattori primi del numero ottenuto dal precedente prodotto (che invece rappresenta la chiave pubblica che chiunque può vedere e che si usa per crittografare). Siccome la crittografia asimmetrica è molto lenta se si devono spedire grandi quantità di dati, spesso si usa questo tipo di crittografia per scambiarsi una chiave con cui iniziare una comunicazione in crittografia simmetrica, molto più semplice, veloce e sicura.

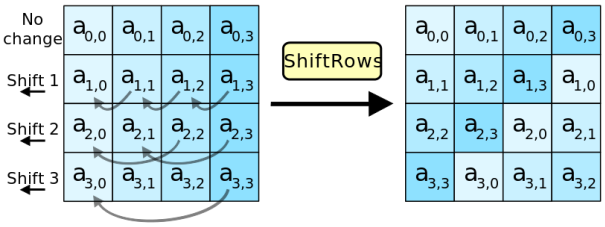
AES

AES fu progettato dai due crittologi Joan Daemen e Vincent Rijmen sulla base di tre caratteristiche fondamentali: resistenza contro tutti gli attacchi, velocità e completezza del codice su un’ampia gamma di piattaforme e semplicità progettuale. AES è un cifrario a blocchi con lunghezza del blocco da 128 bit, può avere chiavi indipendenti con lunghezza variabile di 128, 192 o 256 bit ed effettua una combinazione di permutazioni e sostituzioni.
La prima operazione eseguita dall’algoritmo è quella di prendere i 128 bit del blocco e di disporli in una griglia 4x4 byte. Si procede quindi con la codifica che consiste in un insieme di 10 fasi (rounds) ciascuna composta da 4 trasformazioni. Le 4 trasformazioni sono:

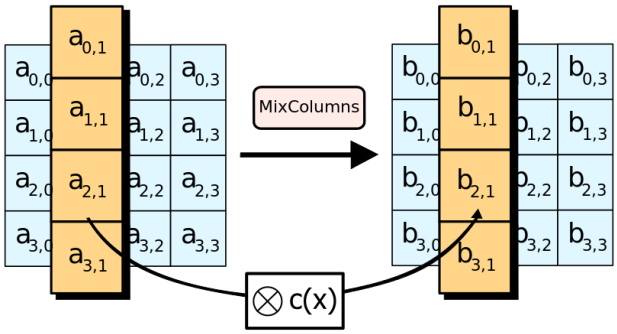
1) Substitute Bytes: ogni bit viene trasformato mediante una permutazione non lineare di byte che vengono mappati tramite una particolare tabella (S-box)



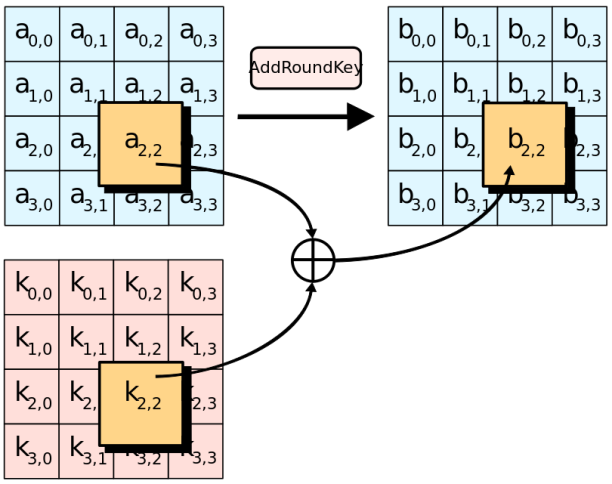
2) Shift Rows: le righe della matrice subiscono uno scorrimento di bytes nell'array state, dove la prima riga rimane invariata, dalla seconda alla quarta viene sempre eseguito uno scorrimento circolare a sinistra di uno, di due e tre bytes rispettivamente.



3) Mix Colums: ogni colonna viene trasformata mediante una operazione che può essere vista come una moltiplicazione matriciale con una particolare matrice generata da un polinomio prefissato.



4) Add Round Key: questa non è altro che la fase in cui viene inserita la chiave segreta che rende il cifrario sicuro. Ogni byte viene combinato in XOR con la chiave da 128 bit. Ad ogni round la chiave aggiunta è diversa e ricavata dalle precedenti ricorsivamente.



AES è il primo standard approvato dall'NSA per comunicazioni Top Secret ed è tutt'ora il cifrario più usato in ambito informatico. Ad oggi non sono conosciuti attacchi in grado di violarlo e l'unico che forse potrebbe farlo (The Square attack) impiegherebbe tempi inaccettabili.

Encryption

Encryption is an essential element in software used for storing or transmitting data which needs to be kept secret like credit card numbers and secure data transmission like government documents. Encryption is divised into 2 stages. The first stage involves the conversion of the original data, called "plaintext", into a form called "ciphertext". The ciphertext can only be read by the receiver of the message. The second stage includes the conversion of the ciphertext into its original form that it is called decryption. A cipher is a code used to keep a message secret. In the past the cipher included the substitution of letters for numbers or the rotation of letters and numbers. Today the cipher is extremely complex and it is created by sophisticated computer algorithms. To recover the original data, the correct decryption key is required. The key is an algorithm and it normally takes the form of a series of characters selected from the 256 ASCII code. The longer and more complex the key is, the harder it is to crack it because of the vast number of different combinations possible, a key just ten characters long could take billions of years to decode. There are two types of encryption: symmetric encryption and asymmetric encryption. Symmetric encryption is the easier encryption because to encrypt and to decrypt the ciphertext one single key is used. Asymmetric encryption requires two different keys. It is a more secure system than symmetric encryption because it requires two separate keys, one for encryption and one for decryption. The public key is used for encrypting the data but you must have the private key to decrypt the data. This method is the basis for most secure communication on the internet.

Modulazioni

I tipi di modulazione usati per la trasmissione di segnali radio sono principalmente due: le modulazioni di fase M-PSK e la modulazione mista di ampiezza e fase M-QAM.

M-PSK

La classe delle modulazioni di fase digitali viene indicata con l'acronimo M-PSK (M-ary Phase Shift Keying). Esse sono modulazioni di fase digitali in cui il valore logico dei bit in ingresso fa assumere alla fase del segnale modulato uno tra M possibili valori, ognuno dei quali corrisponde a uno stato di modulazione che ha associati n=$\log_2 M$ bit.

Ricordiamo che il legame tra bit rate (R_s) e symbol rate (S_R) sia: R_s=$S_R \log_2 M$ bit/s.

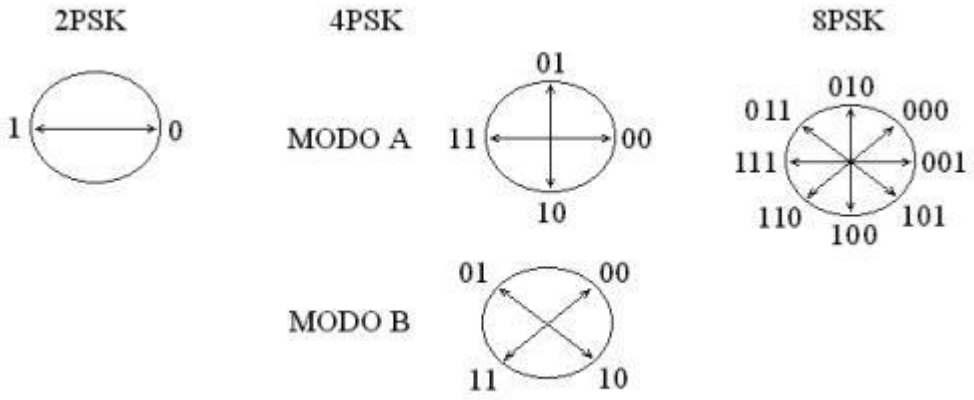
M può assumere i valori 2, 4, 8, per cui sono state realizzate le seguenti modulazioni:

2-PSK: nota anche come BPSK (Binary Phase Shift Keying), modulazione digitale che viene ottenuta associando il valore logico dei bit in ingresso a uno tra due possibili valori di fase che il segnale modulato può assumere, rispetto alla portante.

4-PSK o **QPSK**: è una modulazione digitale in cui il segnale modulato può assumere 4 fasi diverse e ogni fase è associata a una coppia di bit. Viene spesso indicata come QPSK (Quadrature PSK) quando la differenza di fase tra due stati adiacenti è di 90° (sono in quadratura). Poiché la 4-PSK può essere generata con un modulatore I-Q essa viene anche denominata 4-QAM (Quadrature Amplitude Modulation). Rispetto alla 2-PSK è possibile raddoppiare il bit rate a pari symbol rate.

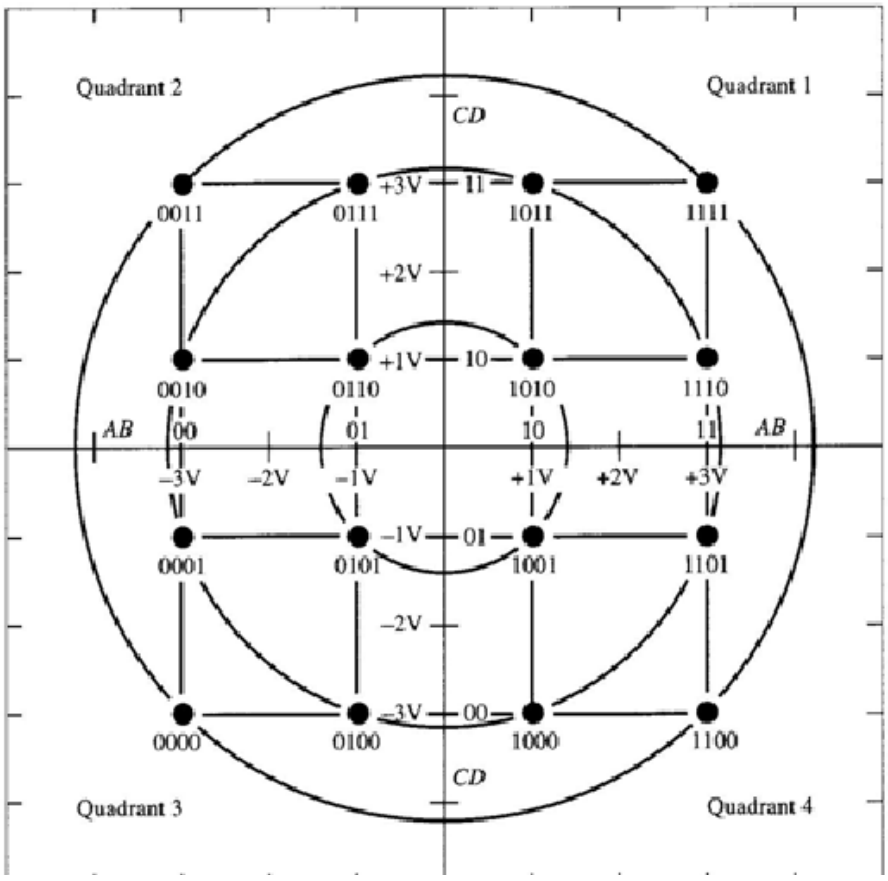
8-PSK: il segnale modulato può assumere 8 fasi differenti e ad ogni fase può essere associato un raggruppamento di tre bit. A pari symbol rate è così possibile triplicare il bit rate generato dalla sorgente rispetto alla 2-PSK.

Le modulazioni PSK sono dette a inviluppo costante poiché attraverso la loro rappresentazione vettoriale si nota che i punti stanno tutti sullo stesso cerchio per cui la lunghezza del vettore è sempre la stessa in tutti gli stati di modulazione. Ciò significa che l'ampiezza del segnale modulato non varia da stato a stato. In prima approssimazione la banda occupata da un segnale M-PSK può essere considerata all'incirca uguale al valore che assume il symbol rate



Modulazione M-QAM

Queste modulazioni sono state sviluppate per superare il limite che le modulazioni M-PSK ponevano sul numero di stati (M). Infatti usando 16 o più fasi e mantenere costante l'inviluppo, cioè posizionando tutti i punti in uno stesso cerchio, si va incontro ad un alta probabilità di errore, in quanto i punti diventano sempre più vicini. Per questo motivo si è pensato di posizionare i punti su un reticolo, oppure su cerchi concentrici di raggio diverso, in modo tale che anche con un numero di punti di modulazione M ≥ 16 essi risultino sufficientemente separati. Così si ottengono le modulazioni M-QAM. In queste modulazioni occorre generare un segnale modulato in cui, a seconda dello stato di modulazione che si determina, variano sia l'ampiezza sia la fase. Uno stato di modulazione è perciò caratterizzato dal valore di ampiezza e fase che assume il segnale modulato in corrispondenza della sequenza di bit a esso associata. In prima approssimazione la banda occupata da un segnale modulato M-QAM può essere considerata all'incirca uguale al valore che assume il symbol rate.



Le frequenze su cui lavorano gli apparati che usano lo standard 802.11 sono frequenze liberalizzate, cioè usabili da tutti senza affittarle. Per evitare interferenze tra i vari apparati si utilizza la tecnica di trasmissione a spettro espanso (spread spectrum). Questa tecnica indica il processo con cui lo spettro di un segnale viene espanso su una banda molto più grande di quella del segnale informativo in ingresso. Questo permette a molti più utenti di operare simultaneamente poiché il segnale non rimane stabile su una singola frequenza. Questa tecnica è molto importante in fatto di sicurezza perché era stata progettata in ambito militare negli anni 50 con lo scopo di proteggere le comunicazioni contro le intercettazioni e le interferenze. Vi sono tre tecniche di spettro espando:

• Con la tecnica DSSS (Direct Sequens Spread Sprectum) lo spreading viene ottenuto moltiplicando I bit in ingresso per una sequenza di codice pseudocasuale, i cui simboli sono denominati chip per distinguerli dai bit ed hanno una durata molto minore di tempo.

• La tecnica FHSS (Frequency Hopping Spread Sprectum) opera suddividendo la banda totale di espansione in k canali, definendo così k frequenze portanti. Ciascun canale ha la larghezza di banda richiesta da una normale modulazione per trasmettere un certo numero di bit. La frequenza portante viene però cambiata ogni Δt(s), per cui trasmette una raffica di n bit (burst) su una frequenza e poi salta su un'altra frequenza per trasmettere il burst successivo.

• La tecnica OFDM (Orthogonal Frequency Division Multiplexing) si basa sulla suddivisione dell'intera banda di canale a disposizione in un numero k elevato di sottobande, in ognuna delle quali si trasmettono i simboli ottenuti modulando una sottoportante ortogonale rispetto alle altre. Si trasmettono così in parallelo blocchi di k simboli su k sottoportanti tra loro ortogonali. Una sottoportante viene definita ortogonale rispetto alle altre quando nel punto in cui il suo spettro presenta il massimo gli spettri delle altre sottoportanti modulate si annullano.

Presentazione progetto

Il progetto che ho deciso di esporre è lo sviluppo e la configurazione dell'infrastruttura di rete wireless del nostro istituto scolastico.

Il progetto si è articolato in più fasi:

- Per prima cosa abbiamo preso in analisi le esigenze del committente e abbiamo proposto dei servizi da offrire tramite Wi-Fi.
- Scelta degli apparati di rete, cioè gli Access Point da utilizzare.
- Impostare la modalità *Site Survey* per l'individuazione dei punti in cui collocare gli AP attraverso Heatmapper e inSSIDer.
- Minimizzare la potenza di trasmissione degli AP per fornire una adeguata copertura radio ma nel contempo limitare l'inquinamento elettro magnetico e aumentare la sicurezza.
- Verifica della copertura radio e del livello di potenza ricevuto.
- Configurazione della sicurezza di rete tramite autenticazione e crittografia.

- Sicurezza degli accessi, autorizzazioni, filtraggio del traffico e controllo dei dispositivi Wi-Fi tramite il servizio Cloud offerto dalla Dashboard di Cisco Meraki.

Lo scopo del progetto è quello di rendere possibile una connessione wireless all'interno dell'istituto scolastico per studenti docenti ed eventuali ospiti. Per renderla fruibile al massimo, bisogna garantire dei requisiti fondamentali:

- *Copertura*: garantire un livello di segnale ottimale in tutto il perimetro scolastico senza che esso sia visibile dall'esterno.
- *Capacità*: essere in grado di servire un gran numero di utenti.
- *Qualità*: offrire e garantire servizi che possono essere sfruttati in maniera fluida senza blocchi o rallentamenti.
- *Flessibilità*: consentire l'accesso alla rete con qualsiasi dispositivo e ovunque nell'istituto.

L'utenza da servire è quella dell'intero complesso scolastico, escludendo l'area laboratori e la biblioteca in quanto già dotati di connessione a Internet cablata. Gli AP copriranno l'atrio, il primo piano, il piano ammezzato e il secondo piano. In base ai diversi tipi di utente sono state create tre differenti SSID tutti con scopi e peculiarità differenti.

- **Rete Ospiti (Majorana-Ospiti):** Rete destinata ad ospiti occasionali. L'SSID di questa rete è nascosto, cioè non viene trasmesso in Broadcast perciò non sarà visibile tramite una scansione. Non vi è nessun tipo di crittografia ma per accedervi bisogna loggarsi tramite una Splash Page con autenticazione tramite SMS. Per accedere a Internet l'ospite dovrà inserire manualmente l'SSID della rete, che verrà fornito tramite un biglietto da visita all'ingresso dell'istituto, e poi il proprio numero di telefono. Il sistema provvederà a inviare un SMS con le credenziali di accesso per connettersi definitivamente. Questo permette anche all'amministratore di rete di registrare l'utente e eventualmente poterlo controllare.
- **Rete Professori (Rete-Professori):** Rete riservata esclusivamente ai docenti, senza limitazioni di banda ma con filtraggio dei contenuti. Anche qui l'SSID è nascosto per una maggior sicurezza. Per l'autenticazione bisogna inserire correttamente l'SSID e la chiave di crittografia WPA2. Una volta aggiunto l'AP bisogna comunque passare attraverso una Splash Page e inserire le proprie credenziali fornite dall'amministratore tramite email. Il Meraki, tramite server RADIUS interno, esamina ogni richiesta e attiva l'accesso solo agli utenti autorizzati.
- **Rete Studenti (Rete-Studenti):** Rete adibita agli studenti che è sia limitata in velocità sia limitata per i contenuti fruibili. Sono stati bloccati, tramite firewall interno dell'AP, tutti i social media, streaming video, videogiochi e tutti gli applicativi che per fine non abbiano scopo didattico. L'SSID è trasmesso in broadcast e la rete non è dotata di chiave di crittografia ma ogni studente dovrà loggarsi usando i dati Meraki forniti in fase di registrazione dall'amministratore di rete. (La segreteria si attiverà richiedendo agli studenti il proprio indirizzo email, con autorizzazione dei genitori in caso fossero minorenni, quindi l'amministratore di rete provvederà in fase di registrazione ad autorizzarli e a fornire loro la password di accesso tramite email).

Per la realizzazione della rete la scelta è caduta sugli:

AP CISCO MERAKI MR26 in quanto permettono di avere in unico apparato tutte le caratteristiche che avevamo bisogno. Inoltre associando tutti gli Access Point ad un unico account sul Cloud Cisco, riusciamo a trasportare la stessa configurazione su ogni Access Point. Questo Access Point può lavorare sia a 2,4GHz che a 5GHZ e può servire fino a 120 host (teorici) contemporaneamente (Standard 802.11 n).
Qui sotto è riportato il datasheet con tutte le informazioni necessarie.

Antenna
Integrated omni-directional antennas
Gain: 3 dBi @ 2.4 GHz, 5 dBi @ 5 GHz

MR26-HW	Cisco Meraki MR26 Cloud Managed AP
MA-INJ-4-XX	Cisco Meraki 802.3at Power over Ethernet Injector (XX = US, EU, UK or AU)
AC-MR-1-XX	Cisco Meraki AC Adaptor for MR Series (XX = US, EU, UK or AU)

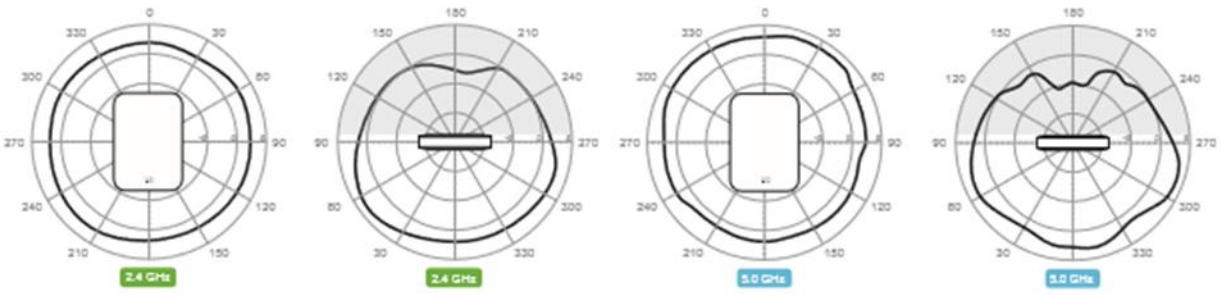
Note: Cisco Meraki Enterprise license required.

RF Performance Table

Operating Band	Operating Mode	Data Rate	TX Power (dBm)	RX Sensitivity
2.4 GHz	802.11b	1 Mb/s 11 Mb/s	22 22	-92 -85
2.4 GHz	802.11g	6 Mb/s 54 Mb/s	21 20	-88 -73
2.4 GHz	802.11n (HT20)	MCS0/8/16 HT20 MCS7/15/23 HT20	22 19	-90 -70
2.4 GHz	802.11n (HT40)	MCS0/8/16 HT40 MCS7/15/23 HT40	21 19	-85 -67
5 GHz	802.11a	6 Mb/s 54 Mb/s	21 19	-89 -71
5 GHz	802.11n (HT20)	MCS0/8/16 HT20 MCS7/15/23 HT20	22 18	-88 -69
5 GHz	802.11n (HT40)	MCS0/8/16 HT40 MCS7/15/23 HT40	20 17	-83 -65

* Maximum hardware capability shown above. Transmit power is configurable in increments of 1 dB and is automatically limited to comply with local regulatory settings.

Signal Coverage Patterns

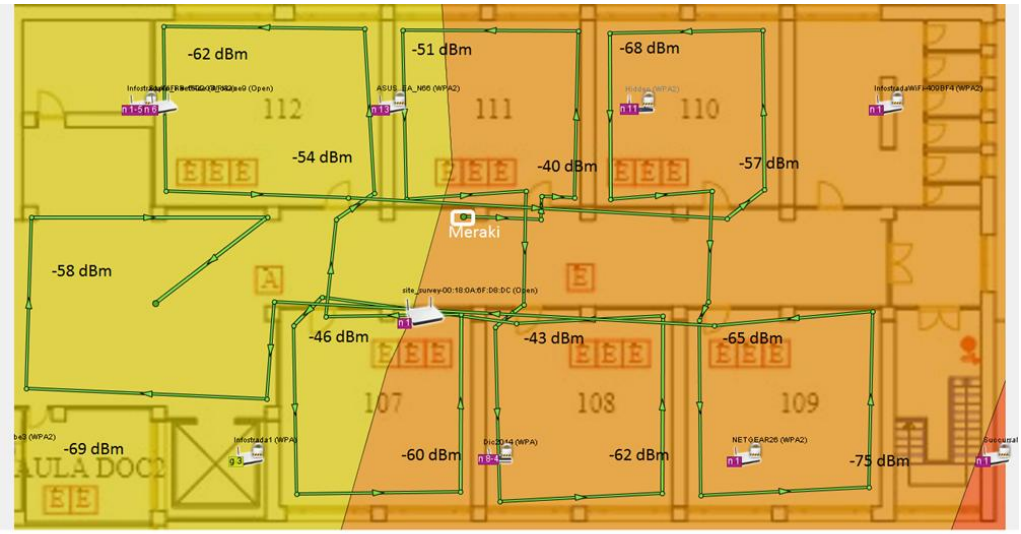


Uno dei punti fondamentali da conoscere su un AP è il guadagno delle antenne, così da poter impostare l'EIRP ed evitare che superi i 20dBm (100mW) che è il limite previsto dalla legge.
Nella figura soprastante possiamo vedere che il guadagno delle antenne è di 3dBm quindi possiamo portare il valore di potenza dell'AP in trasmissione fino a 17dBm. L'importante però è riuscire a coprire tutta l'area necessaria utilizzando la minor potenza trasmissiva possibile così da evitare che il segnale possa uscire all'esterno dell'edificio e quindi evitare a sua volta eventuali intrusioni dall'esterno e limitare le emissioni elettromagnetiche degli AP.

Inoltre per evitare di dover portare l'alimentazione al nostro AP, che arrivasse fino alla presa più vicina, abbiamo deciso di utilizzare un PoE (Power of Ethernet), iniettore che permette di alimentare qualsiasi dispositivo, che "supporti" la tecnologia PoE, tramite cavi di rete in luoghi dove non ci sono prese elettriche (es. soffitto).

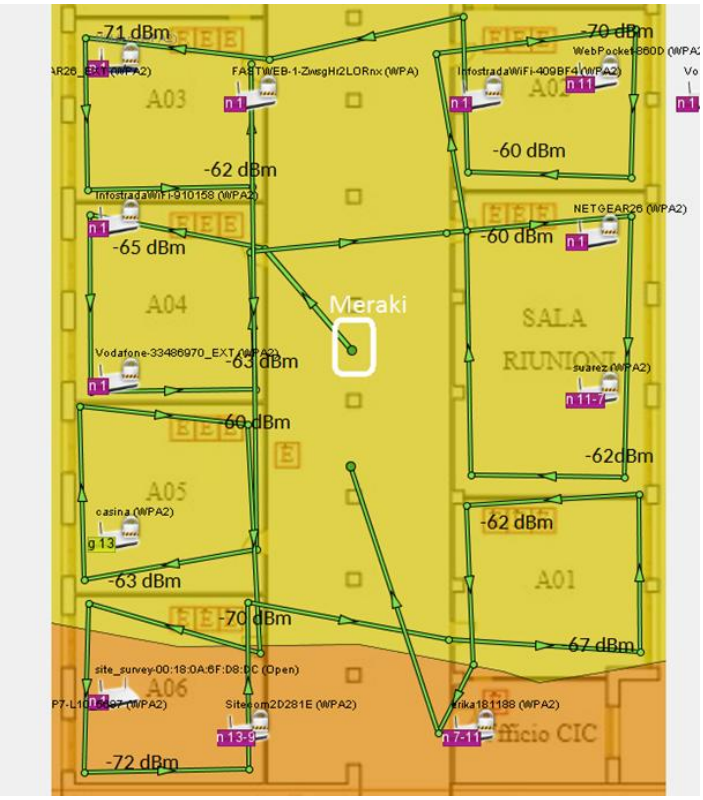
Per l'individuazione dei punti in cui collocare gli AP (HeatMapper) e pianificazione del canale radio utilizzato (inSSIDer) abbiamo attivato la modalità site survey nell'Access Point in modo da poter fare una simulazione delle misure attraverso i software sopra elencati.

Per verificare la copertura (Site Survey) dell'AP, posizionato nei vari posti scelti da noi, abbiamo utilizzato il software HeatMapper che, dopo aver caricato la piantina dell'istituto scolastico fornitaci dal Dirigente Scolastico, ci ha permesso di simulare quella che sarebbe stata la copertura "garantita" dall'AP.



Primo e secondo piano, avendo struttura identica, non hanno nessun tipo di variazione nel test di verifica per la copertura.
Si può notare che l'unico punto in cui la copertura ha un segnale debole è l'angolo in basso a destra (aula 109), in cui arriva un segnale che oscilla tra i -70 dBm e i -75 dBm che è considerata comunque una discreta copertura, dalla stessa azienda produttrice dell'AP, Cisco.

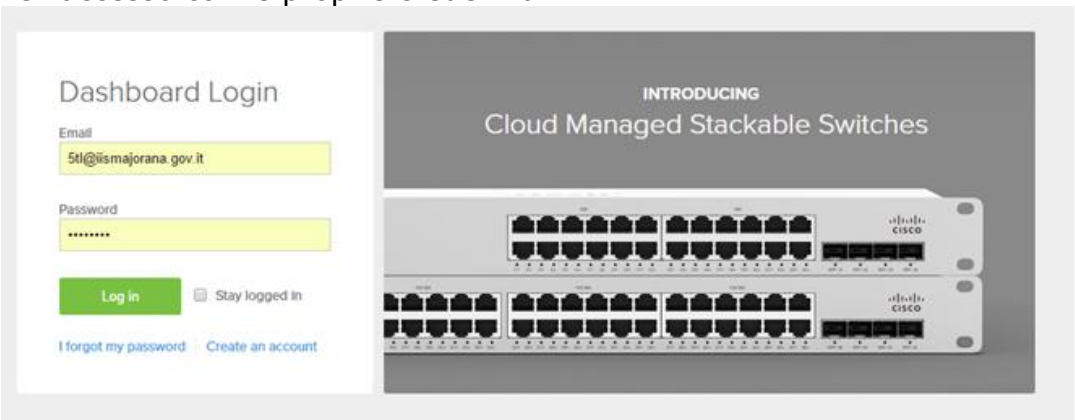
Allo stesso modo abbiamo fatto le misurazioni per il piano ammezzato e per l'atrio:



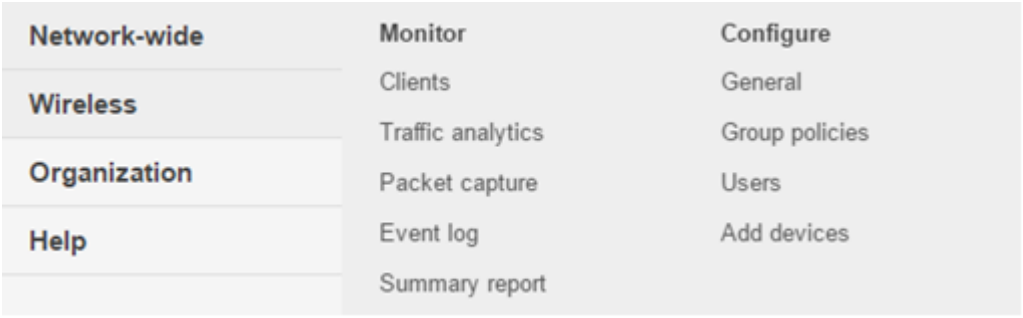
Nel piano ammezzato e nell'atrio abbiamo ottenuto valori assolutamente positivi. A questo punto possiamo affermare che l'AP usato è in grado di coprire tutte le aule necessarie in modo adeguato. L'unico neo riguarda l'angolo in basso a sinistra dove il livello di potenza si aggira intorno ai –72 dBm.
Per quanto riguarda invece il canale radio da utilizzare abbiamo impostato la scelta del canale da utilizzare direttamente dalla dashboard del Meraki in automatico dove sarà l'Access Point autonomamente a scegliersi il canale in base agli Access Point vicini in modo da evitare interferenze.

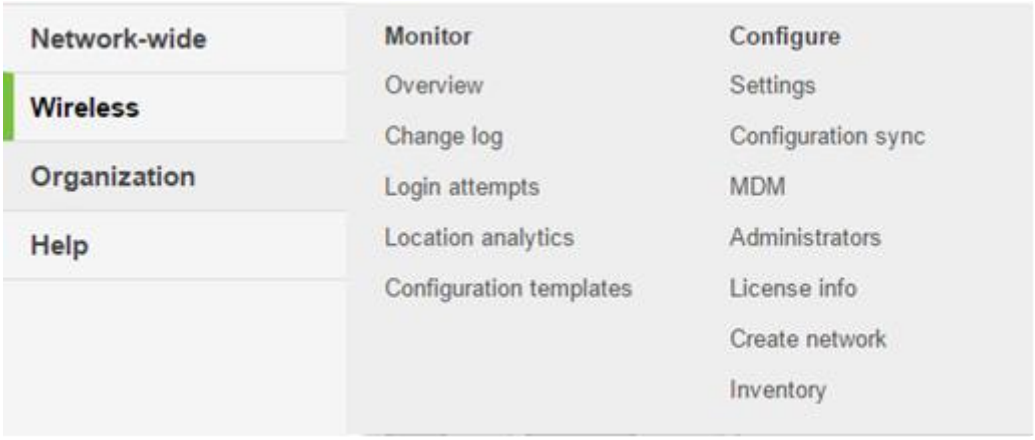
Configurazione completa Access Point tramite dashboard:

Dopo aver scelto la posizione e i servizi da offrire che si andranno ad utilizzare passiamo a quella che è la configurazione vera e propria per tutti i vari accessi che vogliamo rendere disponibili.
Il primo passaggio da effettuare è quello di andare sul link https://n182.meraki.com/login/dashboard_login?go=%2F&sh=182, dove si potrà effettuare l'accesso con le proprie credenziali.



Appena effettuato l'accesso, verremo indirizzati nella schermata principale della nostra Dashboard.
Da qui potremo poi accedere ai vari menù con tutte le loro sotto funzioni.



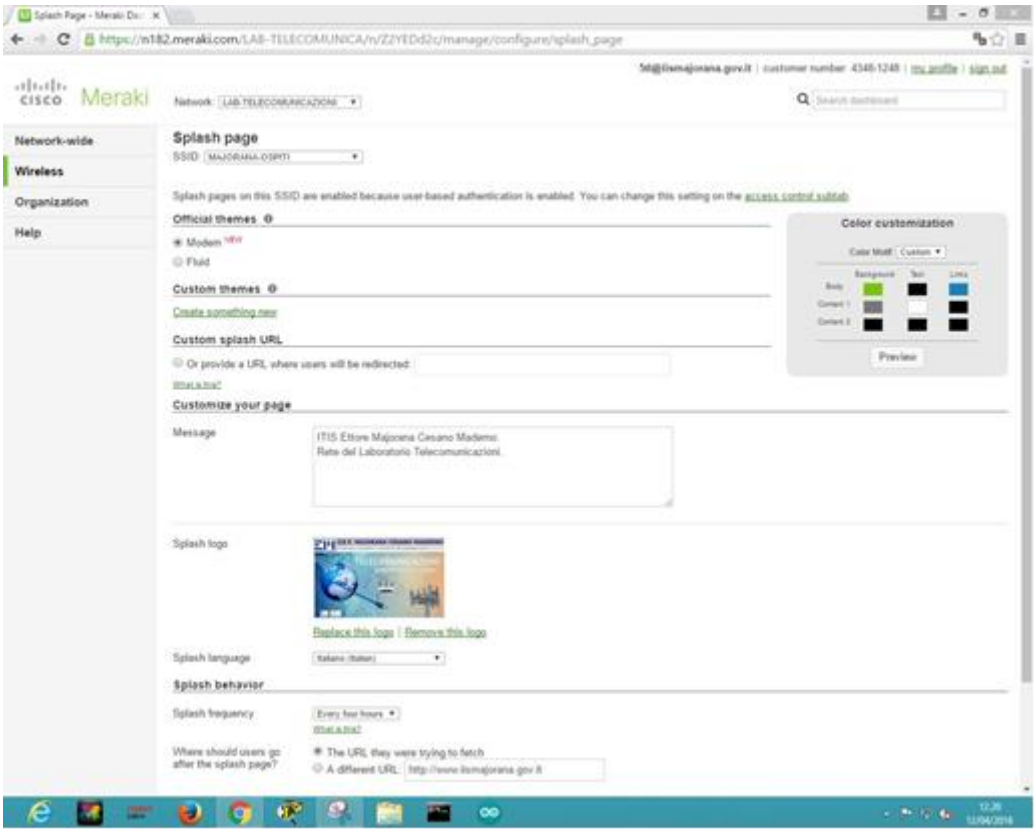


Da questo menù possiamo andare a configurare, modificare e verificare tutte le varie funzioni del nostro AP.
Per prima cosa abbiamo creato 3 SSID differenti e li abbiamo rinominati come si vede in figura.
Ogni SSID è stato settato, in ambito di sicurezza, autenticazione e uso in base a quella che sono i servizi utilizzabili e le richieste del committente.

Da qui si può accedere a quella che è la funzione edit settings che ci porterà in un sotto menù dove poter modificare tutte le varie impostazioni del singolo SSID.

Dato che il Meraki MR26 offre al suo interno anche una funzione firewall abbiamo deciso di sfruttarla per bloccare quelli che sono i siti non inerenti all'ambito scolastico. Per fare ciò è stato sufficiente selezionare l'SSID sulla quale volevamo attivare dei filtri e andare a bloccare tutte le varie applicazioni, siti, indirizzi IP e porte.
Qui in figura la schermata presa dalla sezione firewall della "Rete-Studenti", la rete che ha più restrizioni in quanto è a disposizione di tutti gli studenti dell'istituto e deve essere la più controllata e limitata.

Firewall e Splash page sono due delle funzioni che abbiamo utilizzato per ogni SSID anche se in modi differenti.
La Splash page non è altro che una pagina di autenticazione che viene aperta automaticamente sul dispositivo una volta che si cerca di accedere ad una rete.
Per autenticare gli utenti usiamo il server RADIUS interno del Meraki e una propria Splash page interna opportunamente configurata con il logo del nostro istituto e la rete a cui si sta tentando di accedere.



Il Server **RADIUS** (*Remote Authentication Dial-In User Service*) è un protocollo AAA (*authentication*, *authorization*, *accounting*) utilizzato in applicazioni di accesso alle reti o di mobilità IP. RADIUS è attualmente lo standard de-facto per l'autenticazione remota, prevalendo sia nei sistemi nuovi che in quelli già esistenti ed è implementato in appositi server di autenticazione in una comunicazione con un client che vuole autenticarsi (protocollo client-server). Noi usiamo il server RADIUS integrato nel Meraki per gestire la politica degli accessi alla rete internet irradiata dal nostro Access Point. Il server RADIUS per garantire l'accesso all'utente che lo richiede va ad esaminare all'interno degli users se l'utente è inserito nella sua tabella e se esso è attivo per poter accedere alla rete a cui si vuole collegare e sfruttare. In questo modo non si appoggia a nessun tipo di servizio esterno ed è integrato all'interno dello stesso apparato e in più si può gestire da remoto. Questo garantisce una miglior protezione e una miglior flessibilità. Un utente può essere verificato per accedere alla rete studenti ma nello stesso tempo essere bloccato per accedere alla rete professori nel caso fosse a conoscenza del SSID e della chiave di sicurezza. Questo è molto utile soprattutto essendo una rete per un istituto scolastico in cui qualsiasi tipo di accesso deve essere controllato e nel rispetto delle regole.

Inoltre per evitare un inquinamento elettro magnetico eccessivo abbiamo programmato l'accensione e lo spegnimento dell'Access Point in determinati orari, dopodiché non sarà più possibile connettersi ad una determinata rete.
Qui sotto, per esempio, abbiamo la rete studenti che è disponibile dal lunedì al venerdì dalle 8:00 alle 18:00, il sabato dalle 8:00 alle 14:00 e la domenica non è disponibile.

Bibliografia

"Manuale Cremonese – Informatica e Telecomunicazioni", Zanichelli

Onelio Bertazioli – "Corso di telecomunicazioni (volume 3)", Zanichelli

Luigi Lo Russo/ Elena Bianchi – "Sistemi e Reti (volume 3)", Hoepli

Wikipedia per immagini AES
https://it.wikipedia.org/wiki/Advanced_Encryption_Standard

Introduzione protocollo 802.11
http://www.ucci.it/docs/ICTSecurity-2002-07.pdf

Protocollo CSMA/CA

https://it.wikipedia.org/wiki/CSMA/CA