INTERNET OF THINGS - A.A. 2021/2022

Sommario

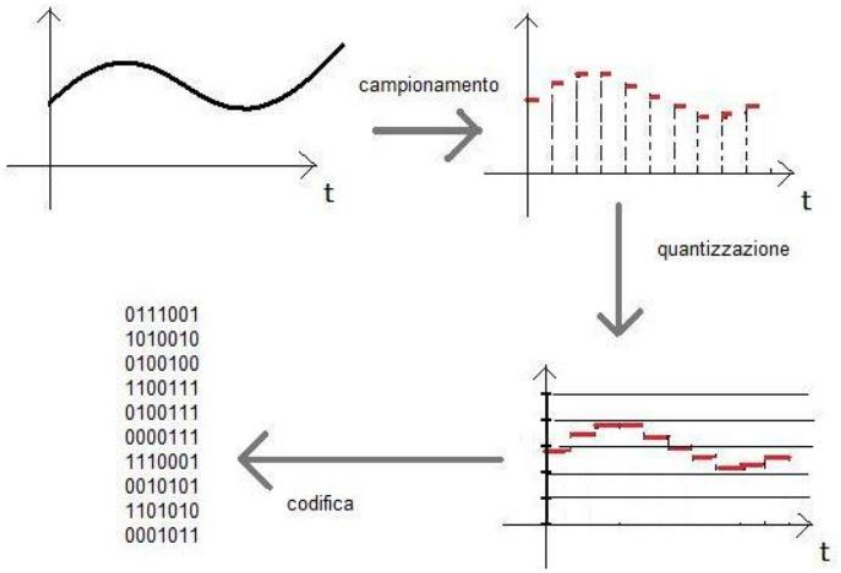
L1:

Le componenti di un sistema di comunicazione sono le seguenti:

- Conversione analogico-digitale e digitale-analogico;
- Codifica e decodifica;
- Modulazione e demodulazione;
- Multiplexing e demultiplexing;
- Accesso multiplo;
- Canale di trasmissione dati.

Per effettuare correttamente una conversione da una grandezza analogica ad una valore digitale è necessario stabilire:

1. Con quale frequenza si vuole registrare il valore della grandezza analogica → questa fase prende il nome di **Campionamento**;
2. Con quale precisione, ovvero in quanti livelli diversi si vuole suddividere i valori assunti dalla grandezza analogica → questa fase prende il nome di **Quantizzazione**;
3. In quale modo si vuole trasformare i valori ottenuti in valori numeri → questa fase prende il nome di **Codifica**.

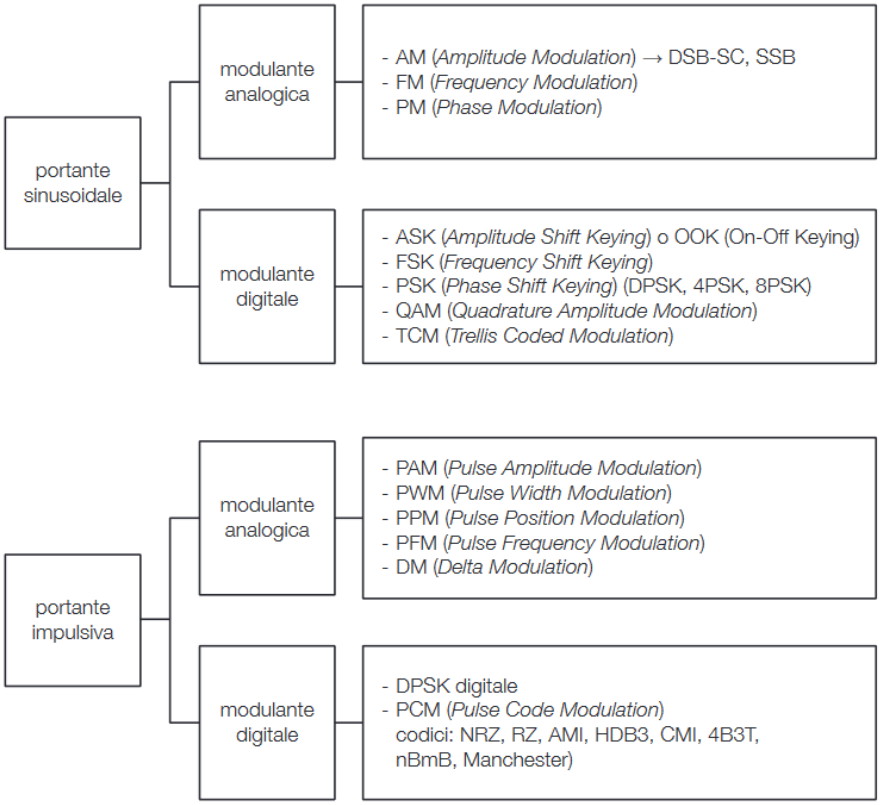


Il **campionamento** consente di trasformare le variazioni nel tempo di una grandezza analogica in una grandezza che varia solo in corrispondenza di determinati istanti di tempo. Il **periodo di campionamento** è il tempo che passa fra l'acquisizione di un campione e l'altro, mentre la **frequenza di campionamento** è il reciproco del *periodo di campionamento*.

La **quantizzazione** consiste nel limitare il numero di valori che la grandezza può assumere. Questa operazione introduce un errore, che sarà tanto più piccolo quanto maggiori saranno i valori usati nella quantizzazione. A differenza del campionamento, la quantizzazione introduce sempre un'approssimazione e dunque un errore sul segnale.

Per terminare il processo di conversione da analogico a digitale, tale intervallo deve essere trasformato in un numero. Il passaggio da intervallo di quantizzazione a valore numerico viene detto **codifica**. Per ragioni pratiche, dovute all'uso di dispositivi elettronici e di calcolatori, la codifica numerica avviene sempre in **codice binario**. In pratica ad ogni intervallo di quantizzazione viene associata una combinazione di cifre binarie in base alla codifica utilizzata.

Le **modulazioni** sono tecniche per la trasmissione dei segnali elettrici (o elettromagnetici mediante antenne) che hanno lo scopo di associare un segnale detto *modulante* ad un altro segnale detto *portante* che ha le caratteristiche adatte ad essere trasmesso in un certo canale trasmissivo; il segnale prodotto è detto *modulato*. La modulazione converte la banda occupata dallo spettro del segnale modulante in una banda, in genere posta a frequenze maggiori, detta *banda traslata*.



Il **multiplexing** è una tecnica che combina più segnali in un unico segnale, adatto per la trasmissione su un canale di comunicazione come un cavo coassiale o una fibra ottica. Il multiplexing è talvolta definito come il muxing. La tecnica di multiplexing divide il canale di comunicazione in diversi **sub-canali logici**, ciascuno dei quali è dedicato a un singolo segnale.

Le componenti di un sistema di comunicazione sono le seguenti:

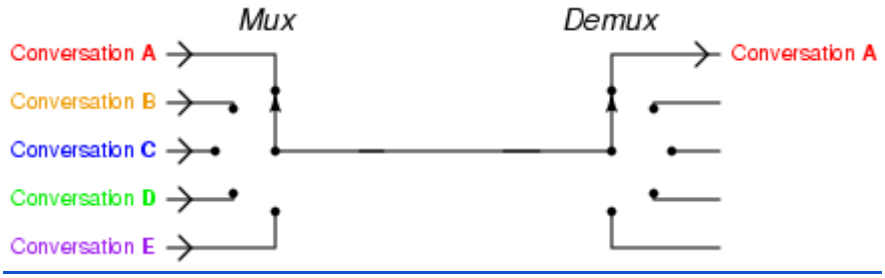
- **Multiplexing analogico**:
    - Multiplexing a divisione di frequenza (**FDM**);
    - Multiplexing a divisione di lunghezza d'onda (**WDM**).
- **Multiplexing digitale**:
    - Multiplexing a divisione temporale (**TDM**):
        - Sincrono;
        - Asincrono.

Quando i segnali devono essere trasmessi abbiamo bisogno di un **canale**, cioè di un mezzo di trasmissione che può essere fisico o logico:

- Un canale è detto **canale logico** se si realizzano più percorsi distinti sullo stesso filo (ad esempio un filo di rame);

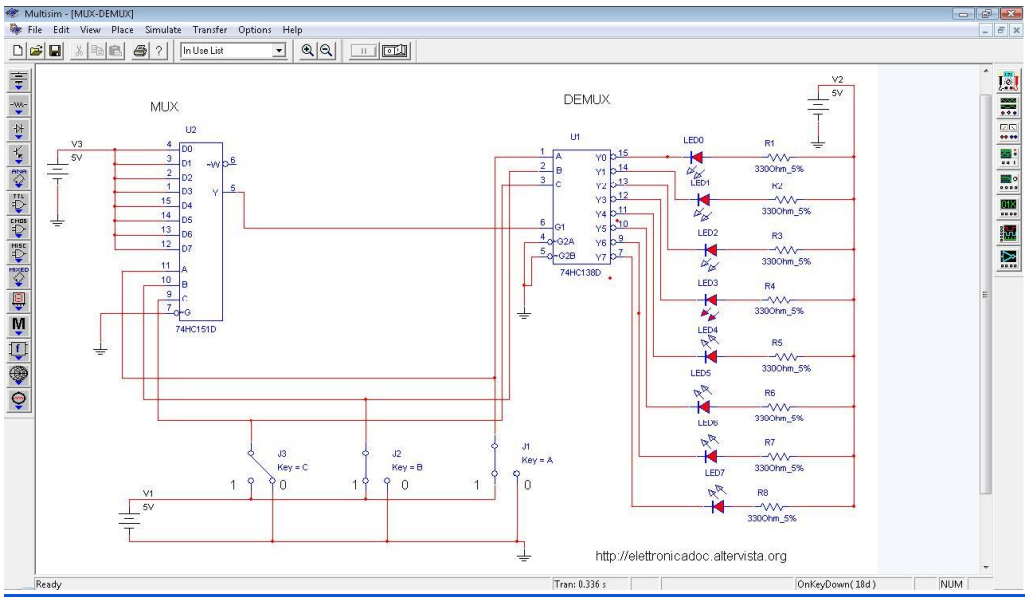
- Un canale è detto **canale fisico** quando per ogni segnale si utilizza un filo diverso.

TDM (Time Division Multiplexing):



La **TDM** rappresenta la multiplazione a divisione di tempo ed è una tecnica di condivisione in un unico **canale logico di comunicazione** secondo la quale un ricetrasmettitore RX ottiene per un determinato tempo l'uso esclusivo del canale. Il tempo di utilizzo del canale è organizzato in **frame tutti della stessa durata**. Il dispositivo di multiplexing (MUX) è dotato di un buffer, in cui prepara il frame prima di inviarlo. Qualora non tutte le linee di input avessero dati da trasmettere, il MUX può comunque trasmettere il frame con bit riempitivi (**padding**) o riempirlo, assegnando più slot a uno stesso mittente. Il dispositivo di demultiplexing (DEMUX) mette su ciascuna linea di output lo slot relativo al destinatario corrispondente.

FDM (Frequency Division Multiplexing):



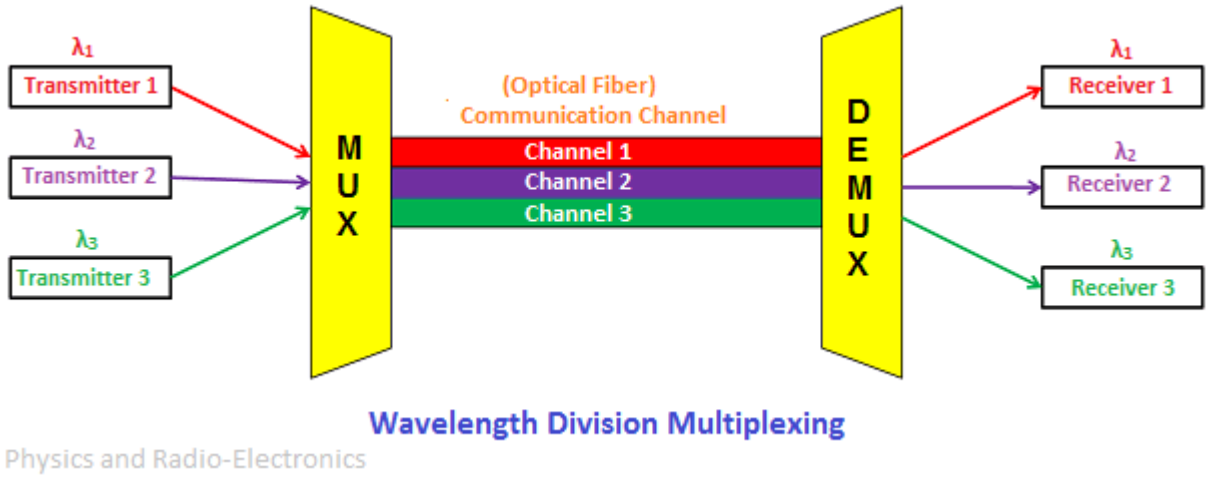
La **FDM** consente di suddividere il canale in sotto canali, uno per ciascun mittente. In pratica, ogni sotto canale lavora a frequenze diverse dagli altri evitando interferenze reciproche. Questa tecnica è utilizzata comunemente nelle trasmissioni televisive, radiofoniche, telefoniche, o dati.

I vantaggi della FDM sono:

1. Trasmettere più segnali contemporaneamente;
2. Nella multiplazione a divisione di frequenza, il processo di demodulazione è semplice.
3. Non ha bisogno di sincronizzazione tra trasmettitore e ricevitore.

Invece, l'unico svantaggio della FDM è che ha bisogno di un canale di comunicazione a larga banda.

WDM (Wavelength Division Multiplexing):



La **WDM** è un sistema di multiplazione utilizzato nei sistemi di comunicazione ottica. È il metodo più importante e più popolare per aumentare la capacità di una **fibra ottica**. Il multiplexing a lunghezza d'onda è una tecnologia in cui più segnali ottici (luce laser) di diverse lunghezze d'onda o colori sono combinati in un unico segnale e vengono trasmessi attraverso il canale di comunicazione. Quindi più segnali vengono trasmessi simultaneamente su un singolo canale di comunicazione. Inoltre, la multiplazione a divisione di lunghezza d'onda è una tecnologia che aumenta la larghezza di banda di un canale di comunicazione (fibra ottica) consentendo simultaneamente molteplici segnali ottici attraverso di essa.

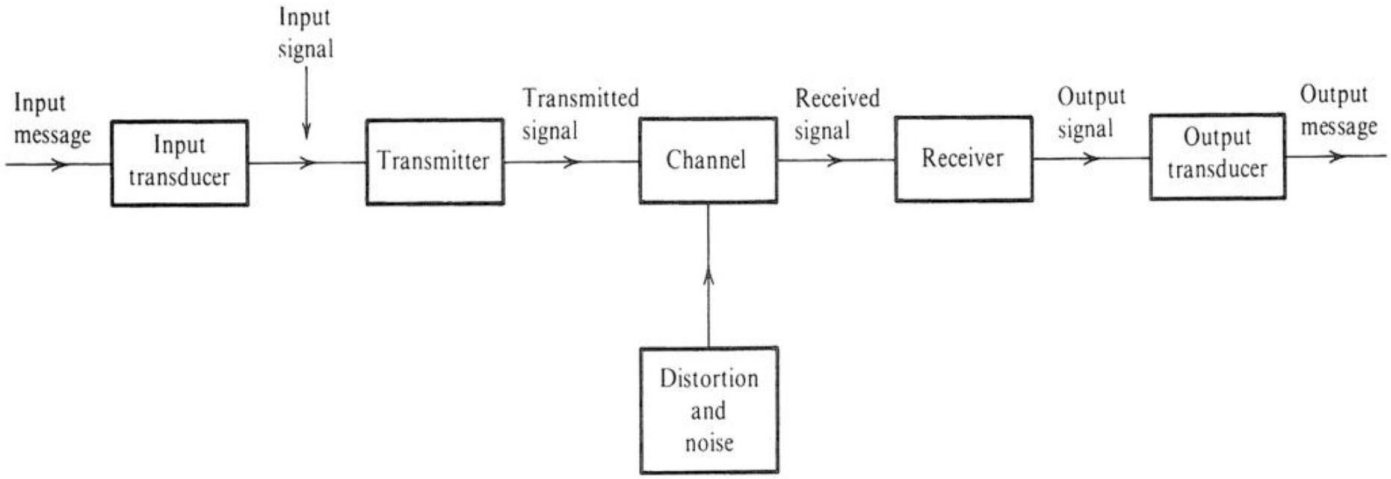
Il vantaggio principale del sistema WDM è che è sufficiente aggiornare il multiplexer e il demultiplexer a ciascuna estremità; non è necessario acquistare più fibre che sono più costose.

Il **Modello ISO/OSI** è uno standard per reti di calcolatori progettato da **OSI** (Open System Interconnection) e promosso da **ISO** (International Organization for Standardization).

Di seguito le descrizioni di ciascun livello:

1. **Fisico**: troviamo tutti i protocolli che regolano la trasmissione dei dati tra due nodi della rete, occupandosi principalmente della forma e tensione del segnale.
2. **Collegamento**: vengono formati tutti i pacchetti che verranno instradati lungo la dorsale di comunicazione. I dati vengono frammentati, impacchettati e modificati in modo da aggiungere un *header* e una *tail*, che hanno la funzione di check (ACK).
3. **Rete**: avviene l'attività di routing e della conversione dei dati nel caso in cui i due nodi siano ospitati da reti con caratteristiche differenti.
4. **Trasporto**: viene determinato tutto ciò che riguarda la connessione tra i due host, stabilendo, mantenendo e terminando la connessione. Inoltre, controllano il sovraccarico dei router di rete.
5. **Sessione**: si occupa di instaurare, mantenere e abbattere connessioni tra applicazioni cooperanti, e consente di effettuare la gestione del dialogo e la sincronizzazione.
6. **Presentazione**: avviene la trasformazione dei dati delle applicazioni in un formato standard, offrendo servizi di comunicazioni comuni come la crittografia.
7. **Applicazione**: i protocolli interagiscono direttamente con i programmi e i software che al loro interno hanno moduli di comunicazione di rete.

Uno schema riassuntivo di un sistema di comunicazione è il seguente:



La **fonte** origina un messaggio, che potrebbe essere una voce, un'immagine televisiva o dati. La fonte viene convertita da un trasduttore in una forma d'onda elettrica a cui si fa riferimento come segnale in banda base o segnale di messaggio.

Il **trasmettitore** modifica il segnale in banda base per rendere efficiente la trasmissione. Il trasmettitore è generalmente costituito da uno o più dei seguenti sottosistemi: un **pre-enfatizzatore**, un **campionatore**, un **quantizzatore**, un **codificatore** e un **modulatore**.

Il **canale** è un mezzo attraverso il quale al trasmettitore viene inviata l'uscita, che potrebbe essere un filo, un cavo coassiale, in fibra ottica o un collegamento radio, ecc. In base al tipo di canale, i moderni sistemi di comunicazione sono divisi in due categorie: **sistemi di comunicazione wireline** e **sistemi di comunicazione wireless**.

Il **ricevitore** elabora il segnale ricevuto dal canale annullando le modifiche al segnale apportate dal trasmettitore e dal canale. Il compito del ricevitore è di estrarre il messaggio distorto, con possibile segnale di rumore. Il ricevente può essere costituito da un **demodulatore**, un **decodificatore**, un **filtro** e un **de-enfatizzatore**.

Le differenze tra una comunicazione cablata e wireless sono le seguenti:

- Le **soluzioni cablate** risultano meno inclini a interruzioni di connessione e sono poco influenzate da fattori locali (muri, pavimenti, armadi, porte). Rispetto al wireless, dunque, l'**affidabilità** è più alta e anche la **velocità di connessione**. Inoltre, il cavo è **sicuro** perché la connessione passa attraverso un mezzo fisico: se qualcuno volesse intercettare i dati, dovrebbe entrare fisicamente nella rete locale. Abbiamo scarsa scalabilità e mobilità.
- Le reti wireless sono, al contrario, facilmente **scalabili** perché richiedono installazioni e **configurazioni semplici e veloci**: l'estensione della rete è possibile perché la struttura in cui è implementata non rappresenta in alcun modo un ostacolo. Senza contare che sono anche molto **più economiche**: non si utilizzano cavi, quindi neanche lavori e manodopera. Di contro, una rete wireless è più soggetta alle interferenze causate dalla vicinanza di dispositivi elettronici e queste **interferenze di segnale** possono influire sulla velocità di trasmissione dati.

Si definisce **sensore** un dispositivo in grado di misurare una grandezza fisica non elettrica (temperatura, luce, forza etc.) convertendola in una grandezza di tipo elettrico (tensione, corrente, resistenza etc.).

Un **attuatore** è un meccanismo attraverso cui un agente agisce su un ambiente; talvolta viene definito come un qualsiasi dispositivo che converte energia da una forma a un'altra, in modo che questa agisca nell'ambiente fisico al posto dell'uomo.

Le differenze tra un sensore e un attuatore sono:

1. Un sensore è un dispositivo che modifica un parametro fisico in un'uscita elettrica, mentre un attuatore è un dispositivo che converte un segnale elettrico in un parametro fisico.
2. Il sensore viene posizionato sulla porta di ingresso, mentre un attuatore viene posizionato sulla porta di uscita.
3. Il sensore genera segnali elettrici, mentre un attuatore produce energia sotto forma di calore o movimento.

L2:

Le trasmissioni e le ricezioni delle informazioni vengono ottenute mediante uno strumento chiamata **antenna**. Un'antenna è un conduttore elettrico o un sistema di conduttori dove:

- Durante la fase di *trasmissione* viene irradiata energia elettromagnetica nello spazio;
- Durante la fase di *ricezione*, viene raccolta energia elettromagnetica dallo spazio.

Nella comunicazione bidirezionale, può essere utilizzata un'unica antenna che svolge il ruolo sia di trasmissione che di ricezione.

Una **radiofrequenza**, nota con la sigla **RF**, indica un segnale elettrico o un'onda elettromagnetica ad alta frequenza che si propaga nello spazio o in un cavo coassiale. Viene spesso utilizzato per specificare circuiti o sistemi elettronici che elaborano e gestiscono segnali elettromagnetici ad alta frequenza.

L'ampiezza rappresenta la massima variazione di una grandezza in un'oscillazione periodica:

$$f(t) = f_{max} \sin(\omega t + \phi) + b$$

La **fase** di una funzione periodica ad un certo istante temporale è la frazione di periodo trascorsa rispetto ad un tempo fissato. Si tratta di un particolare istante durante lo svolgersi di un fenomeno periodico, sia esso un moto o un segnale elettrico, che viene misurato tramite un angolo detto *angolo di fase*.

La **frequenza** del segnale misura il numero di volte che il segnale periodico si ripete in un secondo e si misura in Hertz (Hz).

Le propagazioni delle radiofrequenze possono essere di diverse tipologie, tra cui:

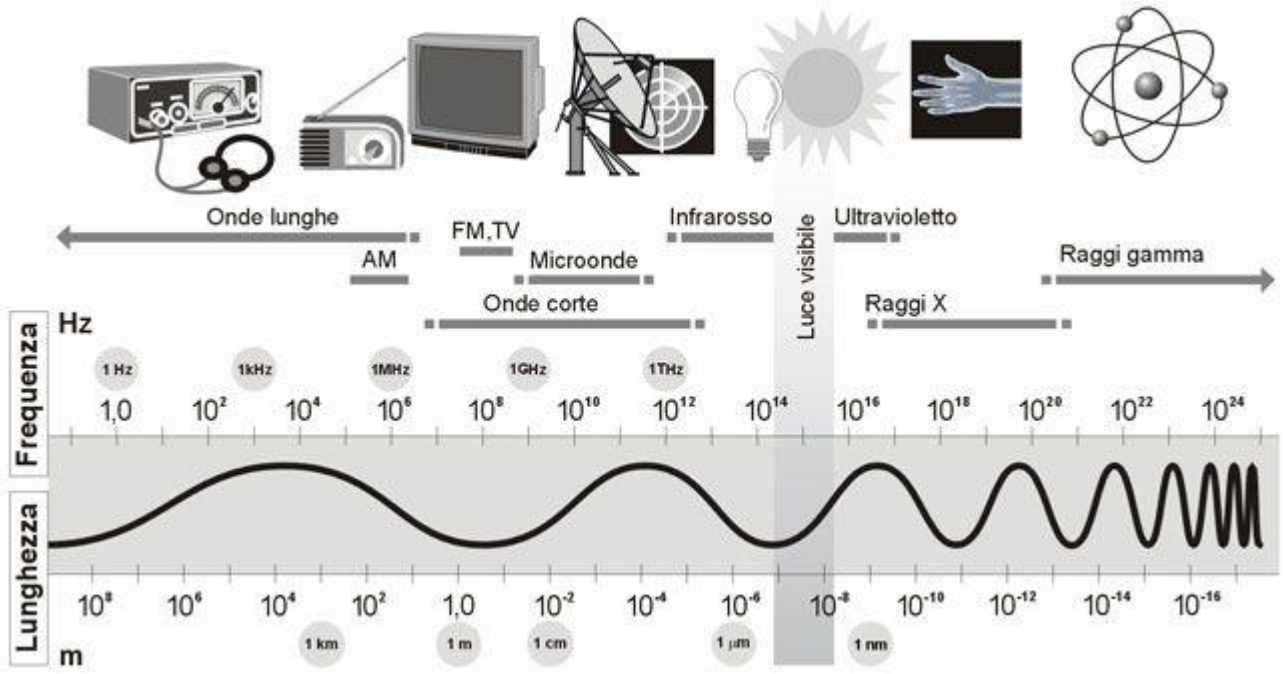
- Onda terrestre o onda di superficie:
    - Si ha quando le antenne Tx e Rx si trovano vicino al suolo, ad altezza relativamente piccola nei confronti della lunghezza d'onda della frequenza

emittente ed entrambe le antenne sono polarizzate verticalmente. Questo tipo di onde si propaga radente al suolo, seguendo la curvatura della superficie terrestre.

- Onda spaziale diretta:
    - Si ha quando le antenne Tx e Rx si trovano ad un'altezza superiore rispetto alla lunghezza d'onda del segnale trasmesso. L'altezza sarà tale che le antenne si potranno considerare a distanza ottica
- Onda spaziale riflessa dalla ionosfera:
    - Si ha quando le onde ionosferiche non raggiungono direttamente l'antenna Rx, ma provengono dall'alto dopo essere state riflesse dalla ionosfera. La riflessione avviene perché queste onde hanno una frequenza inferiore alla *frequenza critica* (30MHz). Quando l'onda elettromagnetica emessa dal Tx penetra in zone successivamente più ionizzate, subisce spostamenti rispetto alla sua traiettoria normale tanto più rilevanti quanto più intensa è la ionizzazione. Quando la deviazione subita dall'onda incidente raggiunge e supera i 90° , essa non può più penetrare nello strato ionizzato e viene da questo totalmente riflessa.
- Onda spaziale riflessa dai satelliti:
    - Si ha quando un segnale viene inviato nello spazio con un angolo incidente molto piccolo ed indirizzato in un punto preciso dello spazio in cui è allocato un satellite geostazionario.

Per prevenire **interferenze** tra utenti diversi, la generazione e la trasmissione di bande di radiofrequenza viene rigorosamente regolata da leggi nazionali, coordinate da un organismo internazionale delle telecomunicazioni (**ITU**).

Una **banda di radiofrequenza** è una piccola sezione contigua delle frequenze dello spettro radio, in cui i canali vengono solitamente utilizzati o messi da parte per l'uso. Per ciascuna di queste bande, l'ITU ha un piano di banda che determina come deve essere utilizzata e condivisa, per evitare interferenze e per impostare il protocollo per la compatibilità di trasmettitori e ricevitori.



La **larghezza di banda** (**bandwidth**) è la quantità massima di dati che è possibile inviare attraverso il percorso di comunicazione entro un secondo. Quando un segnale viene effettivamente trasmesso, possiamo parlare della banda di quel segnale o della larghezza di banda del segnale, ovvero la gamma di frequenze che hanno una potenza di segnale significativa/utile su di esse.

Il **decibel** (**dB**) è l'unità di misura utilizzata per esprimere le differenze tra due o più segnali. Viene espresso tramite la formula:

$$dB = 10\,log_{10}(P1/P2)$$

Il decibel-milliwatt (**dBm**) è un'unità di livello utilizzata per indicare **un rapporto di potenza**, espresso in decibel (dB) con riferimento a un milliwatt (mW):

$$P(dBm) = 10\,log_{10}(P_{mW} / 1mW)$$

Un'**antenna** è un dispositivo in grado di captare o irradiare onde elettromagnetiche da o verso lo spazio: nel primo caso viene detta *ricevente*, nel secondo caso *trasmittente*. Lungo una generica direzione di propagazione, i campi elettromagnetici che compongono la radiazione, cioè quello a grande distanza rispetto alla posizione del radiatore risultano normali sia tra loro, sia alla direzione stessa. Un'antenna che irradia omogeneamente in tutte le direzioni è detta **radiatore isotropico**.

L'intensità di campo delle antenne reali, invece, varia con la direzione ed il comportamento è rappresentato tramite **diagrammi di radiazione**. Questi ultimi sono le curve che si ottengono selezionando il solido di radiazioni con piano opportuni; vengono raffigurati su due sezioni piane perpendicolari fra loro, quella verticale e quella orizzontale. In particolare,

viene raffigurato quello che indica la direzione di massima radiazione, ed è definito **lobo principale**, mentre gli altri sono chiamati **lobi secondari**. Tali lobi secondari, o laterali, limitano la qualità dell'antenna generando eventuale interferenza su altri sistemi di radiocomunicazione o perdita di direttività in sistemi in cui si deve massimizzare la potenza del segnale utile trasmesso o ricevuto in un certa direzione.

Nelle antenne, sia trasmittenti che riceventi, circola corrente elettrica a radiofrequenza che determina perdite per effetto Joule. Si definisce allora rendimento o efficienza, il rapporto fra la potenza irradiata e la potenza ricevuta.

Un'antenna isotropa ha la caratteristica di irradiare in ogni direzione con la stessa intensità ed ha quindi come diagramma di radiazione una sfera che, in una rappresentazione piana, diventa un cerchio.

Il **guadagno G di un'antenna** è definito come il rapporto fra la potenza P_{iso} che dovrebbe essere irradiata dall'antenna isotropa e la potenza P_i irradiata dall'antenna in esame perché si ottenga lo stesso campo ad una certa distanza nella direzione di massima irradiazione:

$$G = P_{iso}/P_i$$

L'**Effective Radiated Power** o **ERP** rappresenta una quantità che indica quanto intenso sia il campo prodotto nella direzione di massima irradiazione:

$$ERP = Pi * G$$

L'onda elettromagnetica può seguire più percorsi dal trasmettitore al ricevitore ad esempio sfruttando, oltre alla linea diretta, la riflessione da parte del terreno o degli edifici specie in un collegamento radiomobile; questa forma di propagazione prende il nome di **multipath**.

Il **multipath fading** è una forma di distorsione di un segnale che giunge a destinazione sotto forma di un certo numero di repliche, sfasate nel tempo, originate dai vari percorsi che il segnale stesso può aver seguito durante la sua propagazione e sommandosi tra loro in ricezione; inoltre, ogni replica avrà compiuto un proprio percorso di una certa lunghezza e caratterizzato da una riflessione su superfici in generale diverse, sarà dunque soggetta ad un'attenuazione in generale diversa da quella subita dalle altre repliche.

Il **modello di riflessione a terra a due raggi** è un modello di propagazione radio multipath che prevede le perdite di percorso tra un'antenna trasmittente e un'antenna ricevente quando sono in linea di vista (**LOS**).

L3:

Arduino è una piattaforma elettronica hardware dotata di un microcontrollore; include un opportuno software di sviluppo, all'interno del quale è possibile scrivere programmi chiamati **sketch** che verranno eseguiti dal microcontrollore.

Una **scheda per microcontrollore** è un sistema su un chip (SoC) che contiene core di elaborazione, RAM ed EPROM per la memorizzazione di programmi personalizzati che vengono eseguiti sul microcontrollore.

Un **microcontrollore** è un chip ottimizzato per controllare i dispositivi elettronici. È memorizzato in un unico circuito integrato dedicato all'esecuzione di un compito particolare e all'esecuzione di un'applicazione specifica. Si tratta di circuiti appositamente progettati per applicazioni embedded ed è ampiamente utilizzato da dispositivi elettronici controllati automaticamente.

L5:

Esistono due importanti modulazioni *analogiche*:

- La modulazione **AM**, una tecnica utilizzata nella comunicazione elettronica che consiste nel variare l'ampiezza dell'onda portante in radiofrequenza; ha una larghezza di banda compresa tra 10 KHz e 8 KHz. Poiché sono frequenze più basse, le cui lunghezze d'onda sono più lunghe, la gamma del segnale è considerevolmente più ampia rispetto a quella della frequenza modulata. La qualità del suono dell'ampiezza modulata (AM) è ben al di sotto di quella della frequenza modulata (FM). Inoltre, poiché sono onde a bassa frequenza, sono più vulnerabili al rumore, poiché si verificano nelle ampiezze delle onde.
- La modulazione **FM**, una tecnica che consente di trasmettere informazioni attraverso un'onda portante, variando la sua frequenza. Il canale di frequenza modulato ha una larghezza di banda di 200 KHz. Tale larghezza consente ai suoni trasmessi (musica e linguaggio) di essere più fedeli e di qualità superiore, e di essere più puliti e chiari rispetto all'ampiezza modulata.

Oltre alle modulazioni analogiche, esistono anche modulazioni digitali come:

- Modulazione **ASK**, che si basa sulla variazione dell'ampiezza del segnale sinusoidale portante con il ritmo del segnale dati modulante. Comunemente il modulatore trasmette la portante senza nessuna variazione quando il segnale dati è a livello alto (bit 1), mentre blocca la portante quando il segnale dati è a livello basso (bit 0).

- Modulazione **FSK**, dove l'ampiezza della portante sinusoidale rimane invece costante. Ciò che viene fatto variare in correlazione al segnale modulante è la frequenza. Questo metodo permette di utilizzare un ricetrasmettitore relativamente semplice da realizzare e assicura un alto livello di immunità ai disturbi, ma non consente velocità di trasmissione molto alte.
- Modulazione **PSK**, dove ampiezza e frequenza della portante sinusoidale rimangono costanti, mentre è la fase che può subire dei cambiamenti. Questo metodo assicura un buon livello di immunità ai disturbi e consente delle velocità di trasmissione elevate, ma richiede un ricetrasmettitore più complesso di quello necessario per il metodo FSK.
- Modulazione **QPSK**, dove vengono utilizzate quattro fasi (0, 90, 180, 270) per codificare 4 livelli logici, ciascuno corrispondente a una coppia di bit.
- Modulazione **QAM**, che corrisponde ad una modulazione combinata di fase e di ampiezza. Viene utilizzata in tutti quei casi in cui la velocità di trasmissione deve essere elevata perché essa permette una codifica multilivello molto spinta.

La **modalità di trasmissione simplex** è il tipo più semplice di modalità di comunicazione unidirezionale, dove il mittente ha solamente la capacità di inviare dati (trasmissioni televisive e radiofoniche).

La **modalità di trasmissione half-duplex** è il tipo di modalità di comunicazione che supporta la comunicazione a due via ma con ritardo. I dati possono viaggiare solo in una direzione alla volta (walkie-talkie).

La **modalità di trasmissione full-duplex** è la modalità di comunicazione più avanzata, dove i dati possono essere inviati e ricevuti da entrambe le direzioni contemporaneamente (chat, videochiamate).

Le tecniche dell'accesso multiplo in un sistema di comunicazione sono:

- **FDMA** (**Frequency Division Multiple Access**), dove a ciascun utente viene assegnata una banda o un canale di frequenza univoco e nessun altro utente può condividere la stessa banda di frequenza.
- **TDMA** (**Time Division Multiple Access**), che divide lo spettro radio in intervalli di tempo e in ogni slot un solo utente può trasmettere o ricevere.
- **SDMA** (**Space Division Multiple Access**), che controlla l'energia irradiata per ogni utente nello spazio.

La **modulazione OFDM** (**Orthogonal Frequency Division Multiplexing**) è una tecnica per trasmettere dati in parallelo utilizzando un certo numero di portanti ortogonali tra loro (tipicamente un numero molto elevato, da qualche centinaio a qualche migliaio). Questa

tecnica consente di suddividere una trasmissione a bit-rate elevato in tanti flussi paralleli ed ortogonali a bit-rate molto più basso. In questo modo è possibile contrastare efficacemente gli effetti deleteri che possono verificarsi su canali affetti da propagazione per cammini multipli.

La **trasformata di Fourier** è un mezzo per mappare un segnale, nel dominio del tempo o dello spazio nel suo spettro nel dominio della frequenza. I domini del tempo e della frequenza sono solo modi alternativi di rappresentare i segnali e la trasformata di Fourier è la relazione matematica tra le due rappresentazioni. Un cambio di segnale in un dominio influenzerebbe anche il segnale nell'altro dominio, ma non necessariamente allo stesso modo. **Discrete Fourier Transform** (DFT) è una trasformata come la trasformata di Fourier utilizzata con i segnali digitalizzati.

Il **throughput** è la frequenza con cui vengono trasmessi i dati. Può anche essere definito come la quantità di dati esportati con successo da un luogo all'altro in un determinato periodo. La velocità effettiva viene misurata in bit al secondo (BPS). Nei termini di oggi questo sarà espresso in megabit al secondo (Mbps), o Gigabit al secondo (Gbps).

<u>L6:</u>

Il **subnetting** è una tecnica che permette di dividere una rete in sottoreti, utilizzando la parte host di un indirizzo IP. Ogni subnet dispone di due soli indirizzi. La **subnet mask** consente di stabilire l'intervallo di indirizzi IP all'interno di una sottorete. La **subnet mask** permette di ricavare la rete cui appartiene un dispositivo partendo dal suo **indirizzo IP**; inoltre, consente di stabilire quali risorse sono da considerarsi locali e quali invece remote. Anche la subnet mask è formata da una sequenza di 32 bit o 4 byte: ciascuno dei quattro gruppi da 8 bit è separato con un punto. Applicando l'operatore logico AND all'indirizzo IP e alla sua subnet mask, è possibile calcolare la rete a cui l'IP appartiene.
ARP (**Address Resolution Protocol**) è un protocollo ausiliario di livello rete, il cui scopo è ottenere l'indirizzo MAC di una stazione di cui è noto l'indirizzo IP. Un pacchetto IP, infatti, può arrivare a destinazione solo se è noto l'indirizzo MAC della stazione destinataria. Per assolvere il suo compito ARP si serve di una tabella (**ARP cache**) in cui sono memorizzate le corrispondenze fra IP e MAC.

La procedura per ottenere l'indirizzo MAC di destinazione, nel caso di due stazioni A e B sulla stessa rete è la seguente:

- La stazione A cerca nella cache l'indirizzo IP di B:
    - Se lo trova, acquisisce l'indirizzo MAC di B e avvia la trasmissione del pacchetto;
    - Se non lo trova, invia una un pacchetto broadcast, contenente i propri indirizzi MAC , IP e l'indirizzo IP di B, in cui richiede l'indirizzo MAC di B;

- La stazione B invia un pacchetto di risposta con il proprio indirizzo MAC;
- La stazione A memorizza nella cache l'IP e il MAC di B e inizia la trasmissione.

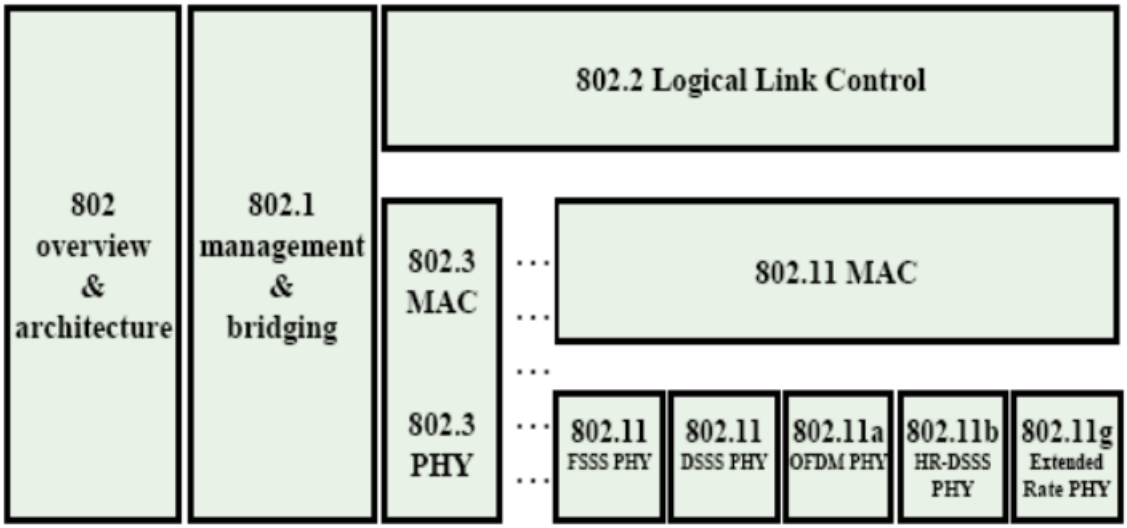
La **cache ARP** può contenere sia voci dinamiche che statiche. Le voci dinamiche vengono aggiunte e rimosse automaticamente, mentre quelle statiche restano nella cache fino a quando il sistema non viene riavviato.

TTL (**time-to-live**) indica per quanto tempo un record rimane memorizzato nella cache di un server DNS, come il tuo ISP.

Un **indirizzo IP** è un indirizzo univoco che identifica un dispositivo su Internet o in una rete locale. IP è acronimo di "**Internet Protocol**", ovvero Protocollo Internet, l'insieme delle regole che disciplinano il formato dei dati scambiati su Internet o sulla rete locale.

Un **indirizzo di trasmissione** (**broadcast**) è un indirizzo IP utilizzato per indirizzare tutti i sistemi su una rete di sottorete specifica anziché i singoli host. In altre parole, l'indirizzo di trasmissione consente di inviare informazioni a tutte le macchine su una determinata sottorete piuttosto che a una macchina specifica. L'indirizzo di trasmissione di qualsiasi indirizzo IP può essere calcolato prendendo il complemento di bit della subnet mask, a volte indicato come maschera inversa e quindi applicandolo con un calcolo OR bit per bit all'indirizzo IP in questione.

Uno **stack di protocolli** è un gruppo di protocolli che vengono eseguiti simultaneamente, e vengono utilizzati per l'implementazione della suite di protocolli di rete. I protocolli in uno stack determinano le regole di interconnettività per un modello di rete a strati come nei modelli OSI o TCP/IP.



Detto anche **indirizzo fisico** (o **indirizzo LAN** o **indirizzo ethernet**), l'**Indirizzo MAC permette a due dispositivi** (che sono fisicamente collegati tra loro) **di scambiare dati**

che (allo stesso tempo) **verranno ignorati da altri dispositivi che condividono la stessa connessione** fisica. In pratica una volta identificato questo codice da 12 cifre, ad esempio sul nostro smartphone, non solo si potrà collegare due dispositivi senza interferenze esterne (da parte di un terzo dispositivo, ad esempio) ma si potrà affidare tutta la banda internet ad un solo dispositivo e si potranno di conseguenza bloccare tutti gli altri dispositivi che si collegano alla rete (magari il Wi-fi di casa), anche se questi ultimi avranno la password della stessa.

Il **Basic Service Set** (**BSS**) è una topologia di rete che consente a tutti i dispositivi wireless di comunicare tra loro attraverso un mezzo comune, come ad esempio un Access Point; contiene un solo AP collegato a tutti i dispositivi wireless all'interno della rete. Ogni BSS viene identificato in modo univoco utilizzando un ID chiamato **BSSID** (**Basic service set identifier**). BSSID è l'indirizzo MAC di AP associato a BSS, e questo indirizzo MAC di AP viene utilizzato per identificare BSS.

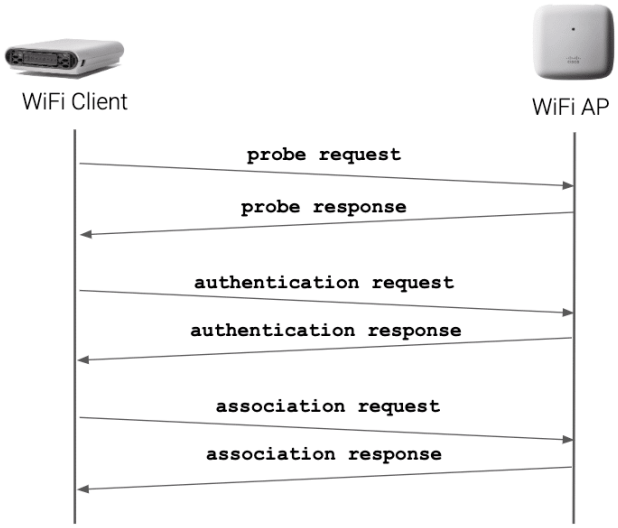
I vantaggi di una BSS sono:

- È una rete a piccola portata, quindi è più sicura;
- Dispositivi e computer comunicano facilmente tra loro senza alcun problema;
- AP gestisce tutte le stazioni all'interno di questa e quindi rende la rete più portatile e gestibile.

I difetti di una BSS sono:

- Contiene un solo AP, quindi non supporta la mobilità;
- Fornisce solo comunicazioni wireless a corto raggio;
- Ogni stazione condivide o comunica attraverso lo stesso mezzo.

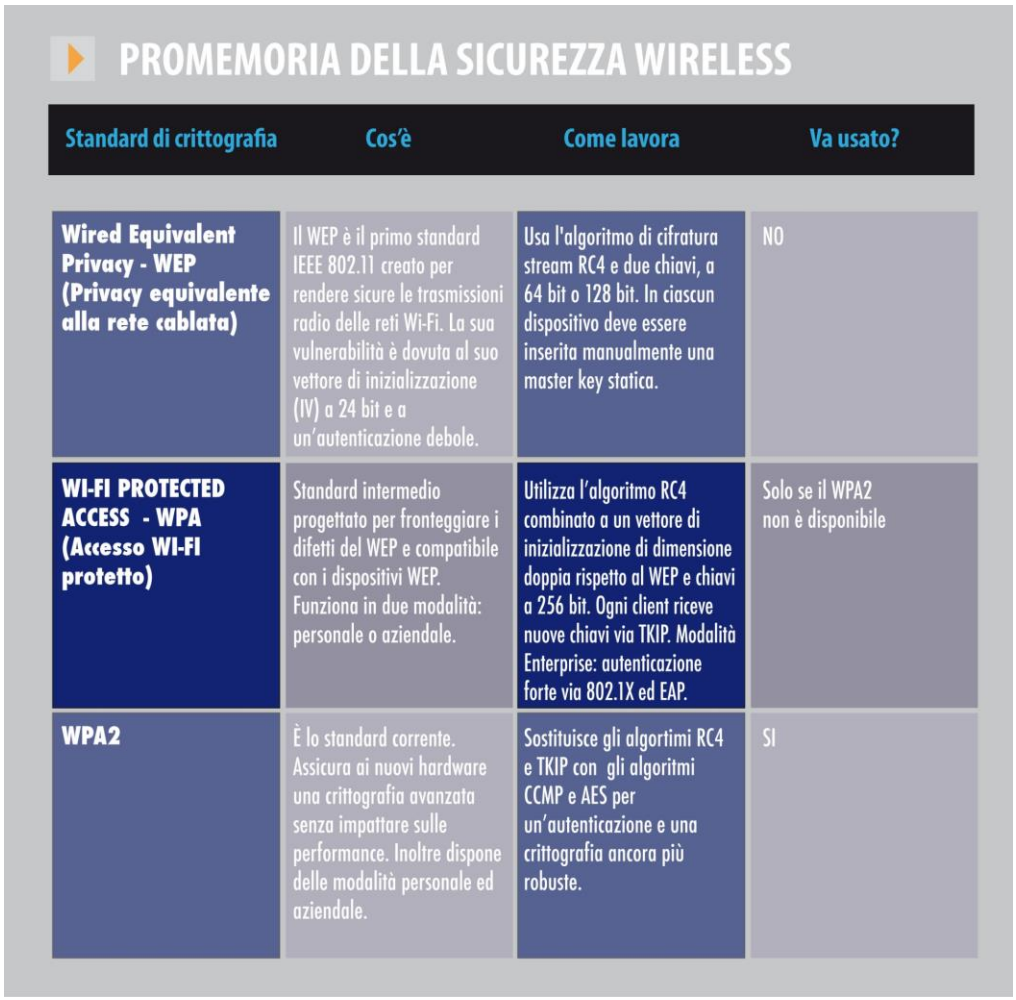
Un **access point**, contraddistinto dall'acronimo **AP** e conosciuto anche come **Access Point wireless**, è un dispositivo hardware di rete che consente ad altri dispositivi Wi-Fi di connettersi a una rete cablata. L'Access Point si collega solitamente a un router (tramite una rete cablata) come dispositivo autonomo, ma può anche essere un componente integrato del router stesso.



La **passive scanning** è un metodo di rilevamento delle vulnerabilità, che si basa su informazioni raccolte dai dati di rete acquisiti da un computer di destinazione senza interazione diretta. Le applicazioni di sniffing dei pacchetti possono essere utilizzate per la passive scanning per rivelare informazioni come il sistema operativo, i protocolli noti in esecuzione su porte non standard e le applicazioni di rete attive con bug noti. Per un intruso, il vantaggio principale della passive scanning è che non lascia una traccia che potrebbe avvisare gli utenti o gli amministratori delle loro attività. Per un amministratore, il vantaggio principale è che non rischia di causare comportamenti indesiderati sul computer di destinazione, come i blocchi. A causa di questi vantaggi, la passive scanning non deve essere limitata a un intervallo di tempo ristretto per ridurre al minimo il rischio o l'interruzione, il che significa che è probabile che restituisca più informazioni.
La passive scanning ha delle limitazioni. Non è completo in dettaglio come la scansione attiva delle vulnerabilità e non è in grado di rilevare alcuna applicazione che non stia attualmente inviando traffico.

La **active scanning** delle informazioni di inventario del sistema e dei dati sulle vulnerabilità è uno strumento potente che può restituire grandi vantaggi. Tuttavia, la scansione attiva sulla rete può anche restituire grandi mal di testa. Può avere un costo politico elevato ed effetti di vasta portata sui tempi di attività e sull'affidabilità del sistema. Se non fatto con attenzione, può essere un modo inefficace e inefficiente per raccogliere informazioni.

In **Open-System Authentication**, il client WLAN non fornisce le proprie credenziali al punto di accesso durante l'autenticazione. Qualsiasi client può eseguire l'autenticazione con l'Access Point e quindi tentare di associarsi. In effetti, non si verifica alcuna autenticazione.



PROMEMORIA DELLA SICUREZZA WIRELESS

Standard di crittografia	Cos'è	Come lavora	Va usato?
Wired Equivalent Privacy - WEP (Privacy equivalente alla rete cablata)	Il WEP è il primo standard IEEE 802.11 creato per rendere sicure le trasmissioni radio delle reti Wi-Fi. La sua vulnerabilità è dovuta al suo vettore di inizializzazione (IV) a 24 bit e a un'autenticazione debole.	Usa l'algoritmo di cifratura stream RC4 e due chiavi, a 64 bit o 128 bit. In ciascun dispositivo deve essere inserita manualmente una master key statica.	NO
WI-FI PROTECTED ACCESS - WPA (Accesso WI-FI protetto)	Standard intermedio progettato per fronteggiare i difetti del WEP e compatibile con i dispositivi WEP. Funziona in due modalità: personale o aziendale.	Utilizza l'algoritmo RC4 combinato a un vettore di inizializzazione di dimensione doppia rispetto al WEP e chiavi a 256 bit. Ogni client riceve nuove chiavi via TKIP. Modalità Enterprise: autenticazione forte via 802.1X ed EAP.	Solo se il WPA2 non è disponibile
WPA2	È lo standard corrente. Assicura ai nuovi hardware una crittografia avanzata senza impattare sulle performance. Inoltre dispone delle modalità personale ed aziendale.	Sostituisce gli algortimi RC4 e TKIP con gli algoritmi CCMP e AES per un'autenticazione e una crittografia ancora più robuste.	SI

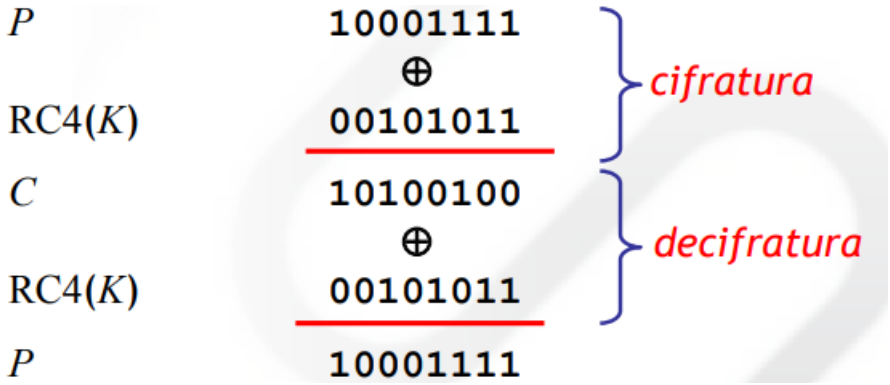
Nella **Shared-Key Authentication**, la chiave WEP viene utilizzata per l'autenticazione in un handshake domanda-risposta in quattro passaggi:

- Il client invia una richiesta di autenticazione all'Access Point;
- L'Access Point risponde con un clear-text challenge;
- Il client crittografa il challenge-text utilizzando la chiave WEP configurata e lo invia in un'altra richiesta di autenticazione;
- Il punto di accesso decripta la risposta. Se questo corrisponde al challenge text, l'Access Point invia una risposta positiva (ACK).

Dopo l'autenticazione e l'associazione, la chiave WEP precondivisa viene utilizzata anche per crittografare i frame di dati utilizzando *RC4* (= un noto cifratore a flusso). A prima vista, potrebbe sembrare che **Shared-Key Authentication** sia più sicura dell' **Open-System Authentication**, poiché quest'ultima non offre alcuna autenticazione reale. Tuttavia, è proprio il contrario. È possibile derivare il **keystream** utilizzato per l'handshake, acquisendo i frame di verifica nella Shared-Key Authentication. Pertanto, i dati possono essere intercettati e decriptati più facilmente con Shared-Key Authentication rispetto all'Open System Authentication. Se la privacy è una preoccupazione primaria, è più consigliabile utilizzare l'autenticazione Open System per l'autenticazione WEP, piuttosto che

l'autenticazione Shared Key; tuttavia, ciò significa anche che qualsiasi client WLAN può connettersi all'AP. (Entrambi i meccanismi di autenticazione sono deboli; La chiave condivisa WEP è decaduta a favore di WPA/WPA2.)

RC4 è una funzione che, a partire da una chiave (lunga da 1 a 256 ottetti), genera una sequenza pseudocasuale (**keystream**) utilizzata per cifrare e decifrare (mediante XOR) un flusso dati.



RTS (**request to send**) corrisponde ad una prenotazione del canale da parte del protocollo, dove il pacchetto RTS viene inviato dal terminale direttamente all'Access Point di destinazione che risponderà in broadcast con un messaggio di **CTS** (**clear to send**). Questa procedura consente di migliorare le prestazioni e risolvere il fastidioso problema del terminale nascosto. Tuttavia, può talvolta creare congestione sulla rete ed è quindi consigliabile il suo utilizzo solo per grosse moli di dati.

Lo standard 802.11 o WIFI prevede la presenza di due modalità per la trasmissione dei dati: **DCF** (Distributed Coordination Function) e **PCF** (Point Coordination Function). La DCF viene utilizzata nelle reti ad-hoc, che ricordiamo sono quelle reti dove ogni client può inviare dati direttamente verso un altro client, mentre la PCF necessita di un Access Point per poter essere implementata.

DCF:

Supponiamo che B abbia necessità di trasmettere ad A. Il terminale B quando trova il canale libero manda un pacchetto **RTS**. A riceve l'RTS, lo interpreta come una richiesta di connessione fatta da B e risponde con un **CTS**. Questo messaggio per B viene interpretato come una conferma di accesso, mentre per gli altri nodi, che hanno visto il CTS, significa che si sta instaurando una comunicazione tra A e B e quindi evitano di trasmettere pacchetti. I terminali che percepiscono i pacchetti RTS e CTS settano un **NAV** (*Network Allocation Vector*), un contatore interno che viene decrementato nel tempo. Il valore al quale viene settato il NAV è quello presente nei pacchetti RTS e CTS e rappresenta sostanzialmente la durata della trasmissione tra il terminale B e il terminale A. Il terminale B, dunque, effettua la trasmissione al terminale A che risponde, se riceve il messaggio in maniera corretta, con

un **ACK** (*Acknowledge*). Questo pacchetto per il terminale B ha valore di corretta ricezione del messaggio, mentre per gli altri nodi della rete indica che il canale è libero ed è terminata la comunicazione tra B ed A. Dato che le trasmissioni radio hanno il difetto di non essere buoni canali di trasmissione, in quanto il rumore ambientale incide fortemente sulla qualità del canale, i messaggi vengono frammentati in **frame** e numerati in maniera progressiva.

PCF:

Questo metodo di trasmissione dati si basa sul **polling**, ovvero sull'interrogazione a turno dei client connessi all'Access Point. Quest'ultimo, dunque, regola l'accesso al mezzo trasmissivo in maniera molto rigida e avremo che un client non può inviare dati se non è stato autorizzato precedentemente dall'Access Point e non può ricevere dati in ingresso se non è stato selezionato direttamente dall'Access Point. Principalmente questo metodo è orientato verso le applicazioni in tempo reale (video, voce, streaming) che necessitano di una gestione dei tempi delle trasmissioni di dati con cadenza regolare. Si tratta, in sostanza, di una modalità con accesso ordinato al canale che viene comandato dall'Access Point.

L8:

Con il metodo **GET** i dati che devono essere inviati al server sono scritti direttamente all'interno dell'URL. Tutte le informazioni fornite dall'utente, quelli che sono definiti parametri URL, sono trasmesse tanto apertamente quanto l'URL stesso. Il vantaggio del metodo di richiesta GET è che i parametri URL possono essere salvati assieme all'indirizzo del sito web. Gli svantaggi principali del metodo di richiesta GET è l'**assenza di protezione dei dati** e la sua **capacità limitata**.

Il metodo **POST** scrive i **parametri URL nella richiesta HTTP** indirizzata al server, celando però alla vista dell'utente. Le richieste POST non prevedono un limite massimo di grandezza. Il metodo POST offre la **discrezione necessaria**. I dati non vengono né salvati nella cache, né compaiono nella cronologia del browser. Anche la **flessibilità** è un punto di forza del POST.

Gli svantaggi del metodo di richiesta POST sono:

- I **dati inseriti nel modulo** vanno nuovamente inseriti e quindi trasmessi un'altra volta.
- I dati trasmessi con il metodo POST **non possono essere salvati come segnalibro insieme all'URL**.

Come regola generale, si può adottare la seguente:

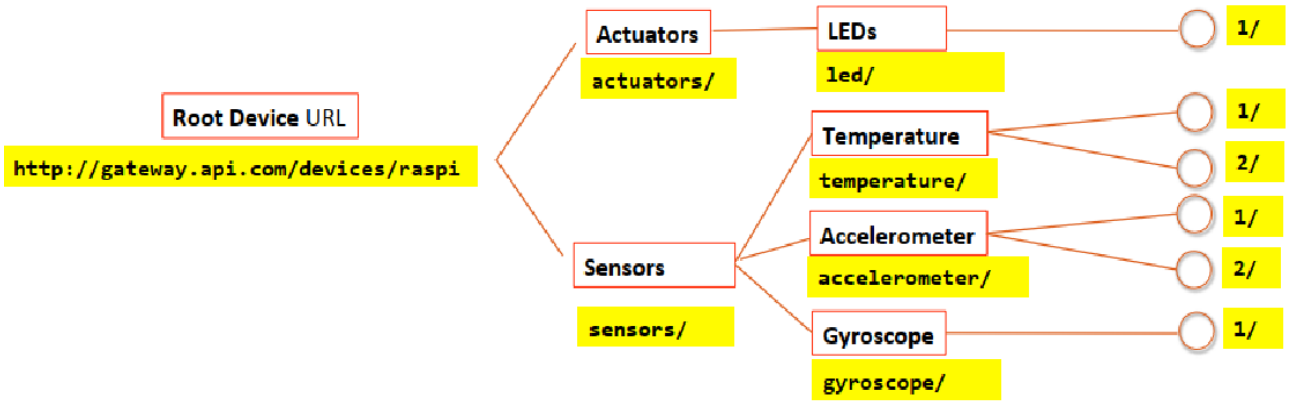
- **GET** per le impostazioni di un sito web (filtri, elenchi, termini di ricerca e così via)
- **POST** per la trasmissione di dati e informazioni relativi all'utente.

L9:

Le **API** sono un insieme di definizioni e protocolli con i quali vengono realizzati e integrati software applicativi. Possono essere considerate come un contratto tra un fornitore di informazioni e l'utente destinatario di tali dati: l'API stabilisce il contenuto richiesto dal consumatore (la chiamata) e il contenuto richiesto dal produttore (la risposta). Se, ad esempio, si desidera interagire con un computer o un sistema per recuperare informazioni o eseguire una funzione, un'API facilita la comunicazione con il sistema che può così comprendere e soddisfare la richiesta.

REST è uno stile architetturale che fornisce degli standard a diversi sistemi informatici sul Web, facilitando la comunicazione tra i sistemi. Affinché un'API sia considerata **RESTful**, deve rispettare i criteri indicati di seguito:

- Un'architettura Client-Server.
- Una comunicazione Client-Server *Stateless*, che quindi non prevede la memorizzazione delle informazioni del client tra le richieste Get; ogni richiesta è distinta e non connessa.
- Dati memorizzabili nella cache che ottimizzano le interazioni Client-Server.
- Un'interfaccia uniforme per i componenti, in modo che le informazioni vengano trasferite in una forma standard.



MQTT è l'acronimo di **Message Queuing Telemetry Transport** e indica un protocollo di trasmissione dati TCP/IP basato su un modello di pubblicazione e sottoscrizione che opera attraverso un apposito *message broker*. In sostanza, i mittenti inviano messaggi relativi ad argomenti specifici, i destinatari si iscrivono ai temi che trovano interessanti e i broker provvedono alla trasmissione dei messaggi tra le due parti. Qualsiasi dispositivo o applicazione può essere un client MQTT che si appoggia a un'apposita libreria MQTT a sua volta connessa in rete a un broker MQTT. I broker MQTT gestiscono la ricezione dei messaggi e il successivo invio ai sottoscrittori e fanno anche un'altra cosa interessante: gestiscono le autorizzazioni. Ciò significa che i mittenti e i destinatari possono accreditarsi

presso il broker così che questi li riconosca nel momento in cui inviano un messaggio o si iscrivono a uno o più argomenti. In questo modo il broker comprende elementi importanti, per esempio sa che un determinato client può ascoltare un argomento, ma non può scrivere nulla in merito allo stesso argomento. Addirittura, il broker potrebbe gestire in autonomia tutti gli argomenti possibili, bloccando la creazione degli stessi ai client, ma si tratta di una configurazione particolare che non rappresenta lo standard.

MQTT è un protocollo di rete leggero e flessibile che garantisce il corretto equilibrio agli sviluppatori IoT:

- La leggerezza del protocollo ne consente l'implementazione sia su dispositivi hardware fortemente vincolati, sia su reti ad elevata latenza o a larghezza di banda limitata in quanto risulta particolarmente resiliente in fase di comunicazione dei dati;
- La flessibilità del protocollo fa sì che possa supportare diversi scenari applicativi per dispositivi e servizi IoT;
- MQTT è un protocollo robusto, con una sua storia e una sua affidabilità. Insomma, non è un azzardo.

Il protocollo MQTT definisce due tipologie di entità nella rete:

- Un message broker:
    - Il message broker è un server che riceve tutti i messaggi da tutti i client per poi indirizzare tali messaggi ai client di destinazione pertinenti.
- Un certo numero di client.

Il client si connette al broker e può effettuare la sottoscrizione a ogni argomento di riferimento dei messaggi del broker. Questa connessione può essere una semplice TCP/IP o una TLS crittografata per i messaggi sensibili; successivamente, il client pubblica messaggi relativi a un argomento inviandoli al broker.

Questo modello di comunicazione si chiama **Publish/subscribe**.

Il cosiddetto **Quality of Service** (**QoS**) è tra le funzionalità più importanti del protocollo MQTT. La *qualità del servizio* a cui si fa riferimento è intesa come il grado di accuratezza nella consegna dei messaggi MQTT **tra i mittenti e il broker e il broker e i sottoscrittori**, ovvero l'accuratezza che definisce la garanzia dell'effettiva, avvenuta consegna di tali messaggi.

Esistono **tre livelli** di servizio **QoS**:

- *Al massimo una volta* (livello 0):
    - Si tratta di un livello concepito per le massime prestazioni col minor sforzo; in questo scenario non c'è alcuna garanzia di consegna

- *Almeno una volta* (livello 1):
    - Il mittente (che sia quello che invia l'iniziale messaggio al broker, o esso sia il broker stesso che gira un messaggio al ricevente finale) mantiene in memoria il messaggio finché non riceve dal destinatario l'ok di avvenuta ricezione
- *Esattamente una volta* (livello 2):
    - Questa è la modalità più lenta ma anche più affidabile. In sostanza il processo prevede un doppio rimbalzo tra mittente e destinatario al fine di confermare al mittente l'effettiva presa in carico del messaggio e quindi l'annullamento di un eventuale rinvio.

L10:

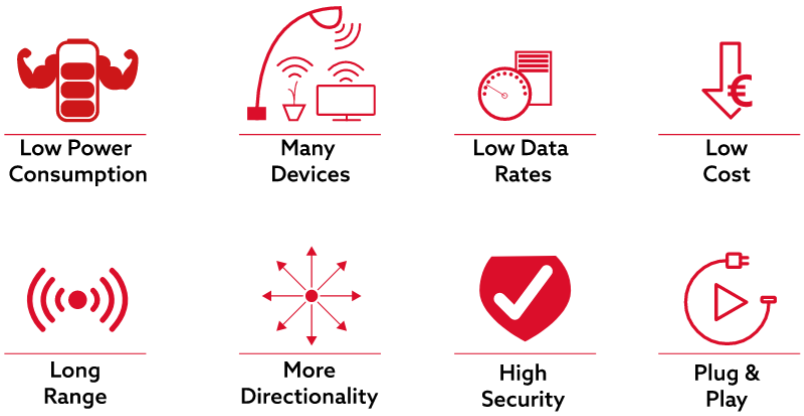
ThingSpeak è un servizio di piattaforma di analisi IoT che raccoglie e archivia i dati dei sensori nel cloud e di sviluppare applicazioni Internet of Things. Funziona con Arduino, Raspberry Pi e MATLAB; inoltre, può essere utilizzato con diversi tipi di linguaggi di programmazione, poiché utilizza un'API REST, HTTP e MQTT.

L11:

Low Power Wide Area Network (**LPWAN**) è una rete per comunicazioni a lungo raggio e a basso bit rate tra "Things". Si differenzia da una WAN classica che ha invece come target comunicazioni tra utenti e aziende con velocità di trasmissione dati e consumi energetici più elevati. Le caratteristiche tecnologiche di una LPWAN sono riassumibili nelle cosiddette "5L":

- Low Power, basso consumo, per consentire lunga durata
- Long Range, lungo raggio da pochi Km a decine di Km;
- Low Traffic, basso traffico, con pacchetti dati di dimensioni ridotte;
- Low Cost, basso costo, per impattare il meno possibile sull'economia dei progetti;
- Low Complexity, bassa complessità, sia di installazione che di utilizzo.

Una tecnologia radio wireless a bassa potenza è il **LoRaWAN**, che consente ai dispositivi alimentati a batteria di connettersi a una rete IoT su un lungo raggio, utilizzando una larghezza di banda ridotta, in una rete regionale, nazionale o globale. Si tratta di uno standard aperto a basso costo. È una rete gratuita che non richiede abbonamenti per il consumo dei dati.



LoRa è il livello fisico o la **modulazione wireless**. Si basa su modulazioni chirp Spread Spectrum, utilizzato nella comunicazione militare e spaziale per decenni a causa delle lunghe distanze di comunicazione che possono essere raggiunte e per la robustezza alle interferenze. **LoRaWAN** è un **protocollo** specifico costruito sulla base della **tecnologia LoRa** sviluppata dalla LoRa Alliance.

L'architettura di rete LoRaWAN è di tipo *star-of-stars* in cui i gateway fungono da bridge trasparenti che inoltrano i messaggi tra i dispositivi finali e un server di rete centrale nel back-end. I gateway sono collegati al server di rete tramite connessioni IP standard, mentre i dispositivi terminali utilizzano la comunicazione wireless a singolo hop su uno o più gateway. La comunicazione *end-point* è generalmente bidirezionale, ma supporta anche operazioni come multicast, consentendo l'aggiornamento del software via etere o altri messaggi di distribuzione di massa per ridurre i tempi di comunicazione. La comunicazione tra dispositivi terminali e gateway viene diffusa tra diversi canali di frequenza e velocità di trasmissione dati.

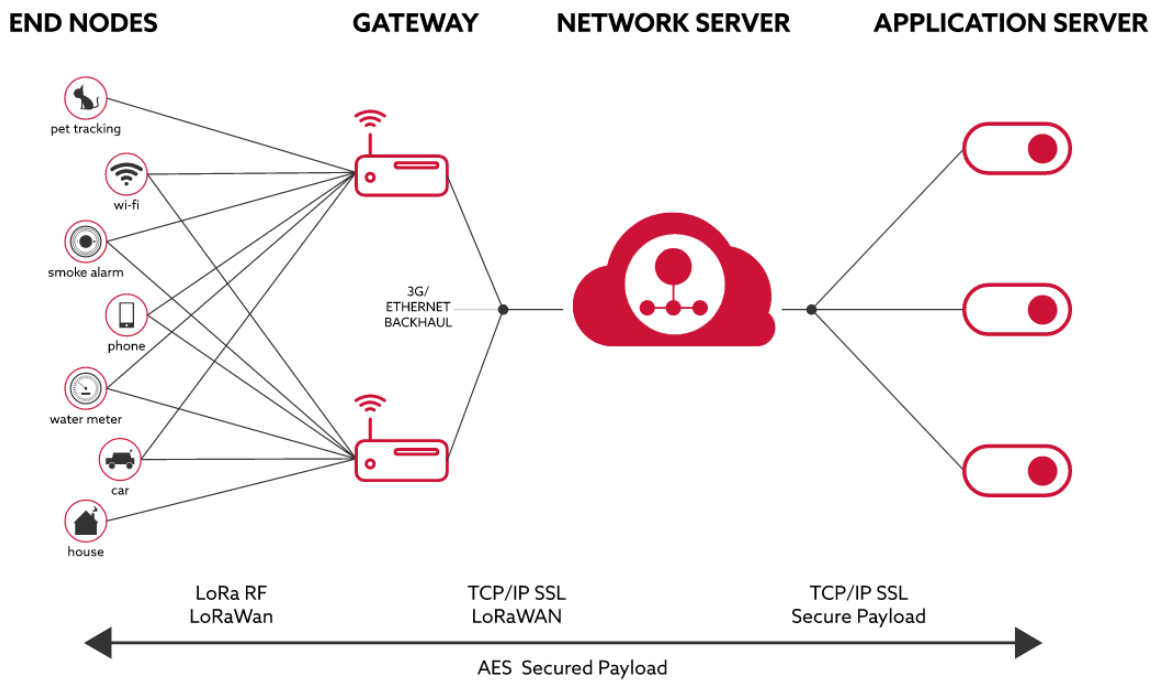
La selezione della velocità dei dati è un compromesso tra intervallo di comunicazione e durata del messaggio. A causa della tecnologia a spettro esteso, le comunicazioni con velocità di trasmissione dati diverse non interferiscono tra loro e creano una serie di canali "virtuali", aumentando la capacità del gateway. Le frequenze di dati LoRaWAN vanno da 0,3 kbps a 50 kbps. Per massimizzare sia la durata della batteria dei dispositivi finali che la capacità complessiva della rete, il server di rete LoRaWAN gestisce la velocità dati e l'uscita RF per ciascun dispositivo finale singolarmente tramite uno schema ADR (Adaptive Data Rate).

La protezione è fornita da diversi livelli di crittografia:

- La chiave di rete unica (EUI64) garantisce la sicurezza a livello di rete.
- La chiave di applicazione unica (EUI64) garantisce la sicurezza end to end a livello di applicazione.
- Chiave specifica del dispositivo (EUI128).

LoRaWAN ha diverse classi di dispositivi end-point:

- **Dispositivi finali bidirezionali** (**Classe A**): i dispositivi di estremità di Classe A consentono comunicazioni bidirezionali in cui ciascuna trasmissione di uplink del dispositivo finale è seguita da due finestre di ricezione short downlink. Lo slot di trasmissione pianificato dal dispositivo terminale si basa sulle proprie esigenze di comunicazione con una piccola variazione basata su una base temporale casuale (tipo di protocollo ALOHA).
- **Dispositivi finali bidirezionali con slot di ricezione programmati** (**Classe B)**: oltre alle finestre di ricezione casuale di Classe A**,** i dispositivi di Classe B aprono finestre di ricezione extra in orari prestabiliti. Il dispositivo terminale riceve un segnale di sincronizzazione sincronizzata dal gateway, per assicurarsi che apra la finestra di ricezione all'ora pianificata. Ciò consente al server di essere a conoscenza di quando il dispositivo terminale è in ascolto.
- **Dispositivi finali bidirezionali con slot di ricezione massimali** (**Classe C**): i dispositivi terminali di Classe C hanno finestre di ricezione quasi continuamente aperte, che si chiudono solo durante la trasmissione.



LoRaWAN security

➔ Before an end-device can communicate on the LoRaWAN, it must be **activated**:

- ⇨ **Device Address (DevAddr)**
  - →Unique (within the network) 32 bit identifier
  - →Shared with Network and Application Server
- ⇨ **Network Security Key (NwkSKey)**
  - →128 bit AES encryption key
  - →Shared between the end device and the network server
  - →Guarantees message integrity on the network infrastructure
- ⇨ **Application Security Key (AppSKey)**
  - →128 bit AES encryption key
  - →Shared between the end device and the application server
  - →Used to encrypt/decrypt the payload
  - →Guarantees confidentiality of the message payload

Ogni dispositivo finale deve essere registrato con una rete prima di inviare e ricevere messaggi. Questa procedura è nota come attivazione. Sono disponibili due metodi di attivazione:

- Over-The-Air-Activation (OTAA):
  - il metodo di attivazione più sicuro e consigliato per i dispositivi finali. I dispositivi eseguono una procedura di unione con la rete, durante la quale viene assegnato un indirizzo di dispositivo dinamico e le chiavi di sicurezza vengono negoziate con il dispositivo.
- Attivazione per personalizzazione (ABP): richiede l'hardcoding dell'indirizzo del dispositivo e delle chiavi di sicurezza nel dispositivo. ABP è meno sicuro di OTAA e presenta anche lo svantaggio che i dispositivi non possono cambiare provider di rete senza cambiare manualmente le chiavi nel dispositivo.

Le variabili che vengono utilizzate sono le seguenti:

- **DevEUI** - Numero a 64 bit - Questo è l'ID univoco del dispositivo finale.
- **AppEUI** - Numero a 64 bit (in v1.1 "AppEUI è rinominato JoinEUI") - Questo è l'ID univoco del server dell'applicazione.

- **AppKey** - Numero a 128 bit - AppKey è la chiave di crittografia tra l'origine del messaggio e la destinazione del messaggio. Questa chiave deve essere univoca per ogni dispositivo.
- Per i dispositivi OTAA, il DevEUI DEVE essere memorizzato nel dispositivo finale prima che venga eseguita la procedura di unione. I dispositivi ABP non necessitano che il DevEUI sia memorizzato nel dispositivo stesso, ma si RACCOMANDA di farlo.
- Il messaggio di richiesta di unione contiene **JoinEUI** e **DevEUI** del dispositivo finale seguiti da un once di due ottetti (DevNonce). DevNonce è un contatore che inizia da 0 quando il dispositivo viene inizialmente acceso e viene incrementato con ogni richiesta di adesione. Un valore DevNonce NON DEVE MAI essere riutilizzato per un dato valore JoinEUI. JoinEUI farà sì che il server di rete elimini le richieste di unione del dispositivo. Per ogni dispositivo finale, la Rete
- **NwkSKey** è una chiave di sessione di rete specifica per il dispositivo finale. Viene utilizzato sia dal server di rete che dall'end-device per calcolare e verificare il MIC (codice di integrità del messaggio) di tutti i messaggi di dati per garantire l'integrità dei dati.
- **AppSKey** è una chiave di sessione dell'applicazione specifica per il dispositivo finale. Viene utilizzato sia dal server delle applicazioni che dal dispositivo finale per crittografare e decrittografare il campo del carico utile dei messaggi di dati specifici dell'applicazione. I payload delle applicazioni sono crittografati end-to-end tra il dispositivo finale e il server delle applicazioni, ma non sono protetti dall'integrità.
- Il **DevAddr** composto da 32 bit identifica il dispositivo finale all'interno della rete corrente.

Esistono due tipi di crittografia di base:

- Asimmetrico, chiamato anche PKI:
    - utilizza una chiave pubblica e una privata.
    - viene utilizzato quando abbiamo due diversi endpoint.
- Simmetrico;
    - utilizza una sola chiave privata.
    - viene utilizzato dove è necessario crittografare i dati molto velocemente e non abbiamo due endpoint.

L'algoritmo hash viene utilizzato per un ambito completamente diverso: serve per controllare l'integrità dei dati e viene considerato come una firma.

Le firme digitali possono essere utilizzate da un Server Directory per mantenere l'integrità dell'informazione. Se alle informazioni vengono applicati crittografia e selezionati dei messaggi durante l'invio, il destinatario può determinare che le informazioni non sono state manomesse durante il transito.

Il rilevamento delle manomissioni e le relative tecniche di autenticazione si basano su una funzione matematica chiamata **hash unidirezionale**, un numero di lunghezza fissa con le seguenti caratteristiche:

- Il valore dell'hash è univoco per i dati hash. Qualsiasi modifica dei dati, anche cancellazione o alterazione di un singolo carattere, restituisce un valore diverso;
- Il contenuto dei dati hash non può, per tutti gli scopi pratici, essere dedotto dall'hash, motivo per cui viene chiamato unidirezionale.