Internet of Things – Domande fornite dal Professore

1. Cosa sono le WSN? Fornire un esempio di come vengono inoltrate le informazioni da nodo a nodo;
2. Descrivere la configurazione hardware dei nodi sensori
3. Descrivere i fattori che influenzano la progettazione di una WSN?
4. Parlare delle applicazioni per WSN (*militari, ambientali e sanitarie*)
5. Parlare della comunicazione wireless e delle Underwater WSN e Underground WSN
6. Parlare del routing nelle WSN
7. Descrivere il protocollo flooding
8. Descrivere il protocollo gossiping
9. Descrivere il protocollo SPIN; quale differenza c'è con il protocollo SPIN-2?
10. Descrivere il protocollo directed diffusion; che differenza c'è con il protocollo SPIN?
11. Descrivere il protocollo LEACH
12. Cosa deve implementare il livello di trasporto in una WSN?
13. Com'è progettato il protocollo di livello applicativo?
14. Come sono classificate le query?
15. Cos'è il Sensor Query and Tasking Language (SQTL)?
16. Cos'è il Task Assignment and Data Advertisement Protocol (TADAP)?
17. Cos'è il Network Management Protocol (NMP)?
18. Elencare e descrivere i requisiti nelle WSN
19. Descrivere il protocollo SETA
20. Cosa sono le WMSN? Parlare del problema delle WMSN con la congestione di rete
21. Indicare un protocollo che garantisce la sicurezza nelle WMSN
22. Come viene garantita l'integrità con il protocollo S^2DCC?
23. Descrivere la tecnologia RFID parlando del lettore e dei tipi di tag
24. Descrivere la tecnologia NFC
25. Descrivere il funzionamento, i vantaggi ed i rischi dell'NFC
26. Confrontare l'RFID con il QR Code
27. Introdurre le nanotecnologie, spiegando come comunicano ed i potenziali rischi
28. Descrivere l'architettura, la sicurezza e i nanodispositivi dell'IoT
29. Descrivere l'ICN, le sue caratteristiche ed i suoi vantaggi;
30. Come si è evoluta la rete? (*dalle reti tradizionali a quelle incentrate sull'informazione*)
31. Parlare del paradigma dell'ICN
32. Descrivere un modello ICN astratto (*publisher/subscriber*) elencandone vantaggi e svantaggi
33. Descrivere una possibile implementazione del modello ICN
34. Descrivere il protocollo ZigBee. Quali sono le sue topologie? Dove viene utilizzato? Indicare inoltre i profili
35. Quali sono le componenti di una rete ZigBee?
36. Descrivere lo stack di comunicazione di una rete ZigBee
37. Descrivere il protocollo 6LoWPAN. Quali sono i suoi vantaggi/svantaggi? Quali sono i suoi tipi di architettura?
38. Quali sono le caratteristiche di adattamento di 6LoWPAN? Indicare anche le caratteristiche aggiuntive
39. Cos'è IPv6? Indicare le principali caratteristiche
40. Quali differenze ci sono tra l'indirizzamento IPv4 e l'indirizzamento IPv6?
41. Quali sono le caratteristiche del format di 6LoWPAN?
42. Come avviene la compressione dell'header di 6LoWPAN?
43. Quali sono le caratteristiche dell'indirizzamento IPv6?
44. Perché i protocolli 6LoWPAN dovrebbero evitare la frammentazione?
45. Descrivere l'operazione di autoconfigurazione ed il funzionamento di 6LoWPAN
46. Descrivere il protocollo di rete IPv6 Neighbor Discovery (*descrivere RS, RA, NS, NA*)
47. Descrivere il protocollo di routin 6LoWPAN Neighbor Discovery, quindi, descrivere la Node Confirmation e la Node Registration
48. Descrivere il gruppo IETF ROLL
49. Descrivere il protocollo RPL (*vantaggi, requisiti, caratteristiche, object functions e tipi di messaggi*)
50. Descrivere il protocollo CoAP (*requisiti di progettazione, caratteristiche principali e messaggistica*)
51. Descrivere il protocollo HTTP (*descrivere UDP, TCP e spiegare il funzionamento di HTTP*)
52. Descrivere il protocollo MQTT (*a cosa serve, aspetti tecnici, topics, messaggi e confronto con HTTP*)
53. Descrivere LPWAN (*vantaggi, svantaggi e soluzioni standard o proprietarie*)
54. Descrivere LoRaWAN (*soluzione standard di LPWAN, elencarne le caratteristiche e descriverne la topologia*)
55. Quali sono le classi di LoRaWAN (A, B, C) e quali sono le loro caratteristiche
56. Descrivere NB-IoT (*caratteristiche principali e modalità di deployment*)
57. Descrivere MANET (*caratteristiche, obiettivi e come viene classificato tale protocollo di routing*)
58. Descrivere AODV (*caratteristiche e funzionalità di base*)
59. Cos'è MIP?
60. Descrivere il tunneling di MIP
61. Descrivere il sistema di autenticazione AUPS
62. Cosa si intende per sistema di sincronizzazione?
63. Spiegare l'architettura di enforcement
64. Quali sono le principali vulnerabilità che vengono valutate nell'analisi del rischio?
65. Quali sono i passaggi dell'analisi del rischio?
66. Quali sono i potenziali rischi associati all'attacco ad un singolo NOS nel sistema IoT?
67. Descrivere il ruolo del leader dei NOS nella coordinazione e gestione dei NOS distribuiti nel sistema IoT
68. Come avviene l'aggiunta, l'eliminazione e l'aggiornamento delle politiche nei NOS distribuiti?
69. Quali canali di comunicazione vengono utilizzati per la sincronizzazione dei NOS?
70. Perché l'utilizzo di un singolo NOS rappresenterebbe un problema nel sistema IoT?
71. Qual è la differenza tra una minaccia e un attacco in termini di sicurezza informatica?
72. Quali sono i potenziali rischi associati all'attacco ad un singolo NOS nel sistema IoT?
73. Qual è l'obiettivo dell'analisi del rischio nell'ambito della sicurezza del sistema IoT?
74. Quali sono i passaggi nell'analisi delle dipendenze tra le vulnerabilità nel sistema IoT?

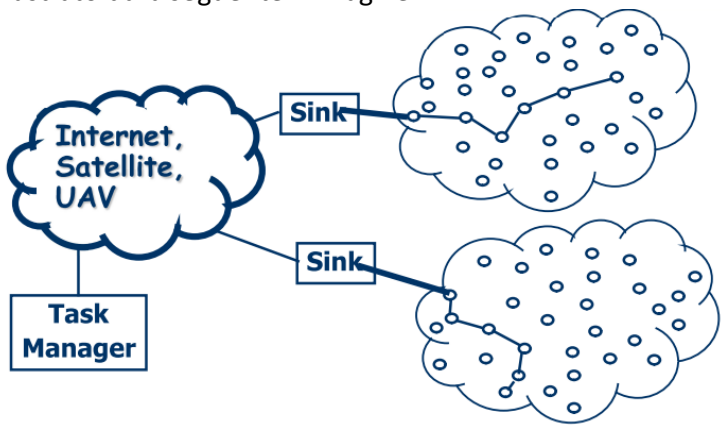
75. Come viene rivalutata l'attaccabilità delle vulnerabilità nel contesto del dominio applicativo?

----------WSN----------

1. **Cosa sono le WSN? Fornire un esempio di come vengono inoltrate le informazioni da nodo a nodo;**

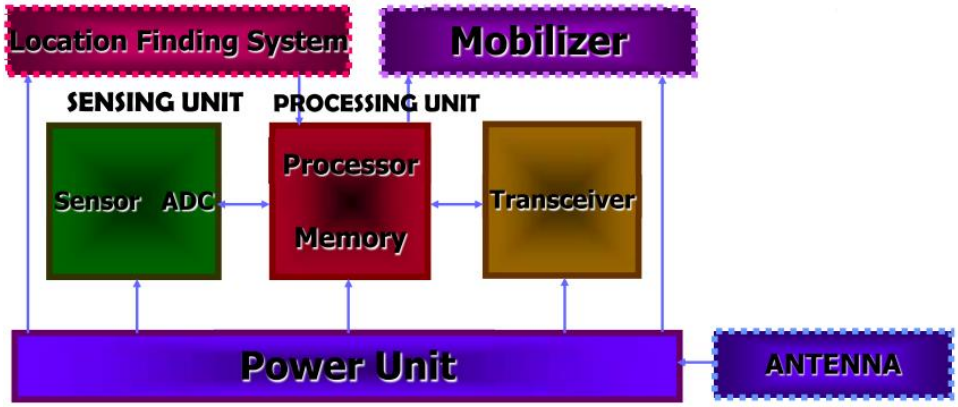
   Le WSN, o **Reti di Sensori Wireless**, sono una tecnologia abilitante dell'IoT. Sono reti molto dense, formate da centinaia di nodi di sensori che comunicano tra di loro tramite comunicazione wireless **multi-hop**. Ogni nodo rileva e trasmette i propri dati (*sensing*) e inoltra i dati provenienti da altri nodi (*forwarding*).

   i dati raccolti dai nodi sensori vengono inviati ad un nodo centrale detto **sink** che li trasmetterà a sua volta attraverso una rete convenzionale. Lo scambio di informazioni tra nodi e sink può essere illustrato dalla seguente immagine:



2. **Descrivere la configurazione hardware dei nodi sensori**

   la configurazione HW di un nodo sensore è composta da diversi componenti e può essere schematizzata dalla seguente immagine:



   Nello specifico:

   a. **POWER UNIT** (o unità di alimentazione): sono delle batterie che alimentano le componenti del sensore; alcuni sensori possono averne 2: una principale ed una di riserva, da utilizzare quando la principale si esaurisce;
   b. **ANTENNA**: è presente in tutti i sensori in quanto, essendo dispositivi wireless, comunicano tramite wireless a radiofrequenza;
   c. **SENSOR ADC** (o sensing unit): rileva la grandezza da monitorare (es. la temperatura); è dotata di un convertitore analogico/digitale che trasforma l'informazione da continua a discreta;

d. **PROCESSOR MEMORY** (o processing unit): è una piccola *CPU on-board* che riceve le informazioni e le inoltra alla sensing unit;
e. **TRANSCEIVER** (o trasmettitore/ricevitore): è un componente principale per le WSN; ha il compito di gestire sia la trasmissione RF che la ricezione RF; è inoltre conforme a qualsiasi standard wireless WSN;
f. **LOCATION FINDING SYSTEM** (o sistema di localizzazione): è un dispositivo presente in alcuni sensori e funge da *GPS on-board* per rilevare la posizione; altri sensori invece localizzano la posizione tramite tecniche di triangolazione;
g. **MOBILIZER** (o sistema di movimentazione): permette ai sensori che lo posseggono di spostarsi in zone di difficile copertura

3. **Descrivere i fattori che influenzano la progettazione di una WSN?**
i principali fattori che influenzano la progettazione di una WSN sono:
   a. **reliability**: calcolata come $R_k(t) = e^{(-\lambda_k t)}$è la capacità di una rete di mantenere le funzionalità senza interruzioni nell'intervallo di tempo (0, t). indichiamo con:
      i. indichiamo con $\lambda_k$il *failure rate* del sensore k, dove con failure rate indichiamo la probabilità del sensore di rompersi nell'intervallo di tempo (0, t).

      $R_k(t)$ è quindi la robustezza del sensore k nel tempo t.
      Più generalmente, la reliability di un broadcast range con N sensori è calcolata dalla formula:

$$R_{(t)} = 1 - \prod_{k=1}^{N}[1 - R_k(t)]$$

   b. **scalabilità**: è la capacità di una rete di mantenere un comportamento che non varia significativamente in base al numero di nodi; viene calcolata dalla formula:

$$\mu(R) = \frac{(N \cdot \pi \cdot R^2)}{A} \; dove:$$

      i. N è il numero di sensori nella regione A;
      ii. R è il range di trasmissione.

      Diremo che la scalabilità è direttamente proporzionale ad N ed R ed inversamente proporzionale a R
   c. **costi di produzione**: i costi di produzione devono essere bassi a causa dell'elevato numero di sensori;
   d. **limitazioni HW**: l'architettura di una WSN ne influenza la progettazione; avendo risorse energetiche limitate infatti, è necessario sviluppare algoritmi e soluzioni che facciano risparmiare più energia possibile durante le operazioni on-board
   e. **topologia**: la disposizione fisica dei nodi all'interno di una rete ne influenza la progettazione; la gestione della topologia di rete si divide in 3 fasi:
      i. **pre-deployment**: consiste nella gestione della disposizione dei nodi: ne abbiamo 2 tipi:
         1. random deployment;
         2. regular deployment;
      ii. **post-deployment**: gestisce cambiamenti topologici che possono essere necessari in seguito a:
         1. cambiamento di posizione;
         2. malfunzionamenti;
         3. energia disponibile;

iii. **re-deployment**: consiste nell'aggiunta di nodi aggiuntivi

f. **ambiente applicativo**: è il contesto in cui la rete di sensori viene utilizzata e può influenzare la scelta del tipo di sensore e dei protocolli di comunicazione da attuare;

g. **mezzo di trasmissione**: influenza la progettazione in quanto influenza il raggio di copertura dei sensori e, quindi, la scalabilità. Il mezzo di trasmissione può esser, ad esempio:
   i. onde a radio-frequenza (es. Wi-Fi a 2,4 GHz);
   ii. onde acustiche

h. **consumo di potenza**: è importante, per aumentare la durata della rete, fare scelte progettuali che riducano il consumo energetico, specialmente nelle fasi di trasmissione e ricezione

4. **Parlare delle applicazioni per WSN** (*militari, ambientali e sanitarie*)
le principali applicazione per WSN sono:
   a. **Applicazioni militari**: possono essere usate per:
      i. Monitoraggio dei campi di battaglia;
      ii. Rilevazione delle forze nemiche;
      iii. Monitoraggio degli armamenti;

      Le WSN in ambito militare dispongono di budget illimitato ed è quindi facile soddisfare i requisiti di privacy e monitoraggio;
   b. **Applicazioni ambientali**: utilizzate, ad esempio, per il monitoraggio degli animali nel loro ambiente naturale, le condizioni del suolo, per il rilevamento di incendi ecc…
   c. **Applicazioni sanitarie**: sono utilizzate per migliorare la qualità della vita dei pazienti e per garantire servizi sanitari più efficienti ed efficaci. Alcune applicazioni sono:
      i. Per la tracciabilità ed il monitoraggio dei medici;
      ii. Per il monitoraggio dei pazienti;
      iii. Come aiuto nella fase di diagnosi tramite il tele-monitoraggio di dati umani fisiologici

      Un classico esempio di WSN in ambito medico è CodeBlue, una piattaforma wireless utilizzata per la gestione dei dispositivi medici indossabili che utilizza come sensore Pluto.

   d. Altri esempi possono essere:
      i. Sviluppo di WSN per case intelligenti;
      ii. WSN per la creazione di musei interattivi;
      iii. Applicazioni in ambito urbano (Smart Roads), che consentono il monitoraggio del traffico, la rilevazione di incidenti ecc…

5. **Parlare della comunicazione wireless e delle Underwater WSN e Underground WSN**
La comunicazione wireless è una modalità di comunicazione senza cavi che utilizza onde elettromagnetiche, solitamente a radiofrequenza. In base alla comunicazione wireless distinguiamo 2 esempi di WSN:
   a. **Underground sensor network**: ovvero reti wireless sotterranee in cui i sensori sono posizionati nel sottosuolo per monitorare la qualità del terreno, per monitorare i terremoti ecc…
   b. **Underwater sensor network**: che utilizzano invece le onde austiche, le quali hanno un bit-rate più basso rispetto alle onde a radiofrequenza. Le underground WSN sono utilizzate, ad esempio, per monitorare la condizione dell'acqua. A differenza delle atre tipologie di WSN, hanno alcune limitazioni; nello specifico:
      i. Banda limitata e canale soggetto a multipath e path loss;

ii. Ritardo di trasmissione che può portare a BER (bit error rate) e perdita temporanea della connessione nelle shadow zones;
iii. Potenza limitata delle batterie
iv. Facili rotture dei sensori

---------- Protocolli di Routing nelle WSN ----------

6. **Parlare del routing nelle WSN**
   i *protocolli di routing* tradizionali non sono adeguati all'uso nelle WSN; i principali motivi di ciò sono:
   a. L'elevato numero di nodi presenti in una WSN;
   b. I frequenti cambiamenti topologici;
   c. La limitata capacità energetica e computazionale dei nodi;
   d. La necessaria integrazione con il compito di acquisizione e trasmissione dati.

   Per questi motivi, sono stati definiti dei protocolli di routing ad-hoc per le WSN che possiamo dividere in 3 categorie:
   a. Protocolli **data centric**: si focalizzano sui dati scambiati tra i nodi (es. flooding, gossiping, SPIN, directed diffusion);
   b. Protocolli **gerarchici**: (es. LEACH);
   c. Protocolli **location based**: si basano sulla posizione fisica dei nodi.

   Il protocollo di routing ideale per una WSN dovrebbe poter:

   a. Selezionare sempre il percorso più corto per la trasmissione;
   b. Evitare che il dato venga inviato più volte ad uno stesso nodo;
   c. Minimizzare il consumo di energia;
   d. Sfruttare una conoscenza globale della topologia di rete.

7. **Descrivere il protocollo flooding**
   in questo protocollo di routing di tipo *data centric* per le WSN, ogni dato ricevuto da un nodo viene inviato in broadcast a tutti i nodi vicini. Il vantaggio di questo protocollo sta nel fatto che, dato che il messaggio percorrerà tutti i possibili percorsi, è garantito che passi anche dal percorso più breve verso la sink. Ha però diversi svantaggi, tra cui:
   a. **Implosion**: in quanto si ha un elevato *overhead* della rete, che può addirittura portare a congestione;
   b. **Data overlap**: ogni nodo può ricevere più volte lo stesso dato e questo porta ad uno spreco di energia;
   c. **Resource blindness**: viene fatto un uso 'cieco' delle risorse disponibili, senza cercare di sfruttarle al meglio; ciò comporta un utilizzo inefficiente dell'energia

8. **Descrivere il protocollo gossiping**
   gossiping è un protocollo di routing di tipo *data centric* per le WSN; prevede che ogni nodo inoltri i dati ricevuti solo ad un suo vicino scelto casualmente (*a differenza, ad esempio, del flooding che li invia in broadcast*). Così facendo si risparmia energia e si evitano *implosion* ed *overlap* ma non è più garantito che i dati arrivino alla sink seguendo il percorso più breve (*si avrà quindi maggior ritardo di trasmissione rispetto al flooding*).

9. **Descrivere il protocollo SPIN; quale differenza c'è con il protocollo SPIN-2?**
   SPIN, acronimo di **Sensor Protocol for Information via Negotiation**, è un protocollo di routing di

tipo *data centric* per le WSN in cui i nodi scambiano informazioni sui dati di cui sono già in possesso e su quelli che desiderano avere, in modo da evitare trasmissioni superflue e diminuire i consumi energetici.
SPIN usa 3 tipi di messaggi, sfruttando il protocollo **3-stage-handshake**:

a. Quando un sensore ha nuovi dati da trasmettere, invia in broadcast un messaggio **ADV** (advertising) per informare gli altri nodi;
b. I nodi interessati, inviano in risposta un pacchetto di **REQ** (request);
c. Infine, il sensore, trasmette un pacchetto di tipo **DATA** ai solo nodi interessati.

Questo metodo evita *implosion* ed *overlap* introducendo però il concetto di *overhead*, dovuto all'invio dei messaggi ADV e REQ, che comporta consumo di potenza.
SPIN-2 è una versione migliorata di SPIN-1 che introduce un **low-energy threshold**: quando l'energia a disposizione del nodo scende sotto una certa soglia, questo si mette in stato **DORMANT** riducendo la propria partecipazione al protocollo per risparmiare energia. È stato analizzato che SPIN-2 garantisce un 10% in più di risparmio energetico rispetto a SPIN-1.

10. **Descrivere il protocollo directed diffusion; che differenza c'è con il protocollo SPIN?**
nel protocollo di routing di tipo *data centric* per le WSN directed diffusion, la sink dichiara in broadcast il proprio interesse a determinati tipi di dato mediante un meccanismo chiamato **interest propagation** e soli i nodi in possesso di tali informazioni rispondo alla chiamata inviando i dati richiesti.
L'identificazione dei dati da diffondere avviene mediante un **naming scheme**: i dati generati dai nodi sono rappresentati infatti da una coppia *attributo-valore* e, per ottenere tali dati, la sink interroga i sensori mediante delle query (che prendono il nome di interest) contenenti una lista di coppie attributo-valore che descrive i criteri di ricerca del dato.
i vantaggi di questo protocollo sono:

a. Non necessita di uno schema di indirizzamento;
b. Ogni nodo può fare aggregazione e caching;
c. Utilizzo efficiente dell'energia;
d. Non è necessario conoscere la topologia globale della rete.

Per quanto riguarda gli svantaggi, invece:

a. L'utilizzo di query non è efficiente per applicazioni che necessitano di un flusso di dati continuo;
b. I naming scheme sono dipendenti dall'applicazione;
c. Overhead causato dal processo di matching tra i dati.

Le principali differenze con SPIN sono:

a. Nell'approccio di routing:
    - SPIN scambia pacchetti di richiesta/risposta per stabilire un percorso di comunicazione;
    - Directed diffusion utilizza un paradigma per cui la sink richiede i dati di interesse e i nodi inviano solo le informazioni richieste.

11. **Descrivere il protocollo LEACH**
LEACH è un protocollo di routing di tipo gerarchico per le WSN. È l'acronimo di **Low Energy Adaptive Clustering Hierarchy** ed è basato sul *clustering* per minimizzare l'utilizzo di energia. Il suo funzionamento si basa sul raggruppamento dei sensori in **cluster**: viene eletto per ogni cluster un cluster head, che fungerà da router per gli altri sensori. Vi sono 2 fasi:

a. **Set-up phase**: ogni nodo ha una probabilità di eleggersi CH. In particolare, sceglierà un numero casuale tra 0 e 1 e, se è minore di una certa soglia, il nodo si elegge cluster head. Ogni CH a questo punto invia in broadcast un messaggio di **advertisement** per informare gli altri nodi della sua natura di CH.
   I sensori sceglieranno a quale CH associarsi in base alla potenza del segnale di advertisement (+ il segnale è forte, - energia sarà necessaria per la comunicazione). Una volta scelto il CH a cui associarsi, inviano una richiesta di associazione, formando un cluster;
b. **Steady phase**: i sensori rilevano i dati e li trasmettono al CH (rispettando, per la trasmissione, gli intervalli di tempo scelti in set-up phase). I CH aggregano i dati ricevuti e li inoltrano alla sink.

Dato che i CH consumano più energia rispetto ai sensori 'normali', LEACH implementa il meccanismo di **clustering dinamico** tramite cui, dopo un certo tempo trascorso in steady phase, si ritorna in set-up phase e si scelgono nuovi CH (escludendo i precedenti) così da equilibrare il consumo di energia su tutti i sensori.
LEACH presenta diversi vantaggi, tra cui:

a. Risparmio energetico rispetto alle comunicazioni dirette;
b. Il clustering dinamico aumenta la vita del sistema;
c. È un protocollo completamente distribuito che non richiede conoscenza globale della rete;
d. Adotta un single-hop routing ovvero, ogni nodo può comunicare direttamente con il CH.

Per quanto riguarda gli svantaggi, invece, LEACH non è applicabile a reti installate in ampie regioni.

---------- Liv. Di Trasporto nelle WSN ----------

12. **Cosa deve implementare il livello di trasporto in una WSN?**
    il livello di trasporto in una WSN deve implementare oltre *all'affidabilità* e al *controllo di congestione* (già necessari per Internet) anche dei requisiti aggiuntivi, tra cui:
    a. **Self-configuration**: il protocollo deve essere adattabile alla topologia dinamica di una WSN;
    b. **Energy awereness**;
    c. **Funzionalità di indirizzamento** e routing limitate.
    Per questi motivi, per le WSN non è adatto il protocollo TCP

13. **Com'è progettato il protocollo di livello applicativo?**
    il protocollo applicativo, in una WSN, è progettato in modo da sfruttare al meglio le risorse della rete. A tale scopo, si utilizza generalmente un modello basato su **query** per ottenere i dati.

14. **Come sono classificate le query?**
    le query possono essere classificate in base a:
    a. All'*intervallo di tempo* su cui vengono raccolti i dati:
        i. **Continuous** queries: che collezionano dati per lunghi intervalli di tempo;
        ii. **Snapshot** queries: che collezionano dati relativi ad un certo istante di tempo;
        iii. **Historical** queries: che collezionano dati riassuntivi del passato.
    b. Al *criterio secondo cui vengono richiesti i dati*:
        i. **Data centric** queries: che ricercano dati che soddisfano determinati criteri;
        ii. Query **geografiche**: che richiedono dati da tutti i sensori situati in una determinata regione geografica;
        iii. **Real-time detection and control** queries: che segnalano la presenza di intrusi

15. **Cos'è il Sensor Query and Tasking Language (SQTL)?**
    SQTL è un linguaggio di scripting utilizzato per interfacciarsi da remoto direttamente con i sensori di una WSN. Fornisce *interfacce e comandi* per accedere all'HW dei sensori, per la **location awareness** (posizione di un nodo, ecc…) e per la comunicazione tra nodi.
    Usando questi comandi, un programmatore può definire degli **event handling block** per 3 diversi tipi di eventi:
    a. Eventi generati quando viene ricevuto un messaggio da un altro nodo (*RECEIVE*);
    b. Eventi sincronizzati periodicamente (*EVERY*);
    c. Eventi causati dallo scadere di un timer (*EXPIRE*)

16. **Cos'è il Task Assignment and Data Advertisement Protocol (TADAP)?**
    TADAP è un protocollo utilizzato per la distribuzione di compiti e dati a livello applicativo in una WSN; funziona in modo simile al protocollo di routing *directed diffusion* e prevede 2 fasi:
    a. **Interest dissemination**: gli utenti inviano i propri interessi ad uno o più sensor nodes;
    b. **Advertisement of available data**: i sensori avvertono che i dati sono disponibili, di conseguenza gli utenti inviano delle queries per i dati di loro interesse.

17. **Cos'è il Network Management Protocol (NMP)?**
    NMP è un protocollo utilizzato dagli amministratori di una rete WSN per interagire con i sensor nodes. Fornisce diverse funzionalità, tra cui:
    a. Accensione/spegnimento dei sensori;
    b. Movimento dei sensori;
    c. Interrogazione della configurazione di rete e dello stato dei sensori;
    d. Riconfigurazione della rete;
    e. Autenticazione e distribuzione delle chiavi di sicurezza;
    f. Sincronizzazione dei sensor nodes;
    g. Scambio di dati utilizzati per triangolare la posizione dei sensori non dotati di GPS.

    In una rete ci possono essere + sensori che fungono da network manager secondo un'architettura che può essere:

    a. Centralizzata;
    b. Distribuita

---------- WSN – Altro ----------

18. **Elencare e descrivere i requisiti nelle WSN**
    i principali requisiti di una WSN sono:
    a. **Integrità**: per garantire l'integrità del dato trasmesso è necessario adottare misure di sicurezza che assicurino che il contenuto del messaggio sia esattamente quello che viene ricevuto dal destinatario. Per fare ciò bisogna:
        i. **criptare i dati**;
        ii. utilizzare tecniche di **hashing** per verificare che i dati non siano stai alterati.
    L'obiettivo della crittografia e dei controlli d'integrità è quello di garantire che solo il destinatario autorizzato possa accedere ai dati e che nessuno possa modificarli senza essere rilevato;
    b. **Confidenzialità**: per garantire questo requisito, è necessario che solo i membri autorizzati possano accedere al contenuto delle informazioni. A questo scopo vengono utilizzate tecniche di *encryption*, che possono essere di 2 tipi:

i. **A chiave simmetrica** (o segreta) in cui si utilizza la stessa chiave per criptare/decriptare i dati;
ii. **A chiave asimmetrica** (o pubblica-privata) in cui si utilizza una chiave pubblica per criptare ed una privata per decriptarli.

c. **Controllo della congestione del traffico**: è importante garantire che la quantità dei dati che viaggiano sulla rete sia tale da evitare rallentamenti. Con il termine *congestione*, si indica lo stato di eccessivo traffico in rete, che può causare appunto rallentamenti o addirittura impedire la corretta trasmissione del dato.
d. **Riservatezza**: è di fondamentale importanza garantire la privacy dei dati sensibili che vengono trasmessi in rete;
e. **Risparmio energetico**: le WSN spesso utilizzano dispositivi a batteria; è quindi importante utilizzare tecniche di risparmio energetico

19. **Descrivere il protocollo SETA**

SETA è un protocollo nato per affrontare contemporaneamente i requisiti delle WSN. Acronimo di **SEcure sharing of TAsks**, SETA garantisce una condivisione sicura dei compiti all'interno di una WSN ed implementa un'architettura ibrida WSM/WMN composta da nodi sensori wireless e *router mesh wireless*, che fungono da capo cluster.
I sensori vengono suddivisi in **cluster**, ciascuno di questi è guidato da un nodo + potente chiamato **mesh router** il quale gestisce la comunicazione tra il cluster e la sink; i cluster head, invece, gestiscono la comunicazione interna con gli altri nodi.
le principali caratteristiche di SETA sono:

a. **Integrità**: utilizza tecniche di crittografia ed hashing per garantire l'integrità dei dati;
b. **Confidenzialità**: permette ai soli membri autorizzati di poter accedere ai dati trasmessi in rete;
c. **Anonimato**: offre un certo grado di anonimato per garantire la privacy dei dati trasmessi;
d. **Risparmio energetico**: utilizza tecniche di risparmio energetico;
e. **Aggregazione dei dati sicura end-to-end**: aggrega i dati in modo sicuro utilizzando uno standard di crittografica omomorfica, ovvero ogni nodo della rete può aggiungere un nuovo dato criptato senza dover decriptare le informazioni precedenti. L'aggregazione dei dati, inoltre, riduce il traffico in rete migliorando l'efficienza energetica dei nodi

inoltre SETA utilizza 3 tipi di protocolli per garantire sicurezza ed affidabilità in rete; abbiamo:

a. Protocolli di **rilevamento**: per rilevare eventuali intrusioni nella rete;
b. Protocolli di **verifica di integrità**: per verificare se i dati trasmessi sulla rete sono stati manipolati;
c. Protocolli di **aggregazione dati**: per aggregare i dati trasmessi in modo sicuro.

20. **Cosa sono le WMSN? Parlare del problema delle WMSN con la congestione di rete**

una WMSN, o **Wireless Multimedia Sensor Network**, è una rete di sensori wireless che consente ai nodi dotati di una piccola videocamera e/o microfono di trasmettere dati multimediali.
Uno dei problemi più frequenti quando si parla di WMSN è il problema della congestione della rete che può avvenire quando si trasmettono grosse quantità di dati multimediali. Questo può causare la perdita di informazioni, è pertanto necessario valutare il carico del canale, il tempo di inter-arrivo dei pacchetti e l'occupazione della banda.
Un altro intervento per ovviare al problema, è l'utilizzo di **codec** per ridurre la risoluzione dell'immagine anche se, in certi casi, può avere un impatto negativo sulla qualità del servizio ed è quindi necessario valutare la qualità del servizio usando misure come il **jitter**, che equivale alla differenza temporale tra l'arrivo di 2 segnali monomediali che compongono un segnale

multimediale.

21. **Indicare un protocollo che garantisce la sicurezza nelle WMSN**
(VEDI 22)

22. **Come viene garantita l'integrità con il protocollo S^2DCC?**
S^2DCC, acronimo di **Secure Selective Dropping Congestion Control** è un protocollo per la trasmissione sicura di messaggi multimediali che garantisce la sicurezza nelle WMSN (SETA è l'analogo delle WSM). In caso di congestione in una rete WMSN, S^2DCC permette di applicare i seguenti meccanismi:
    a. **Network selective data dropping** per ridurre il traffico in rete: si tratta del taglio delle informazioni che non alterano il contenuto informativo base (ad es. la riduzione della qualità di un'immagine);
    b. **Crittografia end-to-end omomorfica** per garantire la sicurezza dei dati trasmessi: i dati vengono criptati dal mittente e rimangono tali durante tutta la trasmissione fino a quando non verranno decriptati dal destinatario finale

    Il sensore che rileva i dati utilizza una chiave per crittografarli ed inviarli al mesh router; quest'ultimo utilizza il campo hash per controllare l'integrità del dato e, in caso di congestione della rete, taglierà i bit non rilevanti. A questo invierà il dato alla sink che, solo alla fine della trasmissione, li decritterà. In questo modo anche se i dati dovessero essere intercettati durante la trasmissione, non sarebbero accessibili in quanto criptati.

---------- RFID ed NFC ----------

23. **Descrivere la tecnologia RFID parlando del lettore e dei tipi di tag**
RFID, acronimo di **Radio Frequency Identification**, è una tecnologia che consente di identificare un oggetto facendo comunicare un tag con un lettore attraverso le onde radio. Il sistema RFID è composto da 2 componenti principali:
    a. Il **lettore**, che possiede:
        i. Una memoria;
        ii. Un'antenna;
        iii. Un'unità di processamento;
        iv. Una batteria;
        v. Altri moduli/interfacce facoltativi;
    b. Il **tag**, che possiede:
        i. Una memoria;
        ii. Un'antenna;
        iii. Un modulo RF;
        iv. Può avere inoltre:
            1. Un'unità di processamento;
            2. Una batteria

    Per quanto riguarda il lettore, esso è formato da una struttura HW ed un SO. Possiede inoltre delle interfacce sia verso l'HW che verso il lato utente, varie librerie ed una serie di applicazioni che consentono di acquisire e di elaborare le informazioni acquisite.
    Per quanto riguarda i tag, invece, essi possono essere collegati a qualsiasi tipo di dispositivo e possono essere classificati in:
    a. Tag **passivi**: funzionano con la potenza irradiata dal reader;

b. Tag **semi-passivi**: hanno una batteria propria, ma non hanno capacità di processamento;
c. Tag **attivi**: posseggono una batteria propria ed un'unità di processamento

In ultimo, per gestire efficacemente gli RFID, è possibile utilizzare un *middleware* che consenta di acquisire grandi quantità di dati dai lettori, filtrarli, immagazzinarli e renderli disponibili all'utilizzo. È anche importante scegliere la giusta banda di frequenza, in base al dominio applicativo; tale banda deve essere tra i 100MHz e 1GHz.

24. **Descrivere la tecnologia NFC**

NFC, acronimo di **Near Field Communication**, è una tecnologia basata su RFID con una portata limitata a circa 10cm che può essere integrata nei dispositivi mobili.
Questa tecnologia è basata sul campo magnetico indotto tra lettori e tag; vi sono infatti NFC che fungono da tag ed NFC che fungono da lettori; lettori e tag sono interscambiabili e servono per trasmettere informazioni.
La tecnologia NFC può essere utilizzata per effettuare pagamenti e trasferire dati tra dispositivi compatibili, ed è ritenuta più sicura rispetto ad altre forme di RFID in quanto la comunicazione è bidirezionale e può essere protetta da controlli di sicurezza; l'unico aspetto negativo rispetto alla tecnologia RFID è il costo più elevato

25. **Descrivere il funzionamento, i vantaggi ed i rischi dell'NFC**

Il funzionamento di NFC può essere suddiviso in 3 operazioni, che coinvolgono 2 dispositivi:

a. Il primo dispositivo emette un campo magnetico che genera un impulso elettrico attraverso un processo di induzione magnetica;
b. Il secondo dispositivo riconosce l'impulso indotto dal primo dispositivo, lo riconosce come valido e offre una connessione;
c. Il primo dispositivo accetta la connessione.

L'utilizzo di NFC ha i seguenti **vantaggi**:

a. Comunicazione bidirezionale dei dati;
b. Livello di sicurezza elevato dovuto ai sistemi di codifica;
c. Elevata velocità di riconoscimento;
d. Riduzione dell'errore di riconoscimento

Ha però anche dei rischi, tra cui:

a. **Privacy**: è infatti possibile che vengano trattenuti dati sensibili durante la trasmissione;
b. **Security**: è importante proteggere i dati per evitare esposizione di informazioni sensibili in caso di smarrimento/furto del dispositivo tuttavia, l'accesso all'NFC, richiede l'autenticazione;
c. **Sentinel hacking**: dovuto al fatto che un hacker potrebbe posizionare dei '*sentinel*' tag per sottrarre informazioni dai dispositivi che passano vicini ad esso

26. **Confrontare l'RFID con il QR Code**

Partendo dal presupposto che RFID e QR sono 2 tecnologie complementari, le principali differenze tra le 2 sono:

a. **RFID**:
    i. Utilizza onde radio per far comunicare un lettore ed un tag;
    ii. Ha maggiore sicurezza rispetto a QR;
    iii. Ha maggiore durata rispetto a QR;

iv. Ha maggiore distanza di lettura rispetto a QR;
v. Le informazioni possono essere aggiornate in tempo reale

b. **QR**:
   i. Utilizza luce ad infrarossi per trasmettere le informazioni;
   ii. Ha una capacità di archiviazione più limitata rispetto ad RFID e può essere solo letto, non scritto;
   iii. Ha un costo minore rispetto ad RFID

---------- Nanotecnologie ed ICN ----------

27. **Introdurre le nanotecnologie, spiegando come comunicano ed i potenziali rischi**

Quando parliamo di nanotecnologie, parliamo di dispositivi di piccolissime dimensioni (da 1 a 100 nm) il cui obiettivo è quello di creare e manipolare atomi e/o molecole. Sono in grado di utilizzare 2 tipi di comunicazione:

a. La **comunicazione molecolare** viene utilizzata all'interno del corpo umano, in particolare nella BAN (Body Area Network); le informazioni vengono codificate nelle molecole e trasmesse tramite la diffusione o il trasporto attivo. Questo tipo di comunicazione è particolarmente efficace negli ambienti fluidi;
b. La **comunicazione elettromagnetica** invece, viene utilizzata per comunicare con il mondo esterno, tra nano-gateway e macro-dispositivi. La frequenza utilizzata è nell'ordine dei THz con lunghezze d'onda molto piccole e può essere calcolata come:

$$\lambda = \frac{c}{f} = \frac{3 \cdot 10^8 \cdot \frac{m}{s}}{10^{12} Hz} = 3 \cdot 10^{-4} m$$

I rischi principali, legati alle nanotecnologie, sono diversi. Tra cui:

a. Difficoltà nel prevederne il comportamento;
b. Possibilità che queste causino problemi alla salute umana e all'ambiente;
c. L'aumento di rischio di tossicità legato alla piccolissima dimensione
d. Incertezza sul comportamento delle nanotecnologie dovuto principalmente al fatto che sono di recente scoperta

28. **Descrivere l'architettura, la sicurezza e i nanodispositivi dell'IoT**

I nanodispositivi sono marcatori costanti che misurano varie grandezze ad esempio, all'interno del corpo umano. Il termine **Internet of Nano Things** (IoNT) indica un sistema di nano-dispositivi in grado di comunicare tra loro.

L'architettura IoNT è composta da 2 strati principali:

a. Il **Service Layer**: definisce i servizi forniti dai nanodispositivi;
b. Il **Context Management Layer**: fornisce informazioni sul contesto in cui si trovano i nanodispositivi.

All'interno del corpo umano, ad esempio, i nanodispositivi sono posizionati in una BAN e raccolgono dati attraverso sensori. All'interno di una BAN sono presenti anche:

a. **Nano-controller**, che si occupano di controllare il flusso dei dati all'interno della BAN;
b. **Nano-gateway/nano-router** che raccolgono i dati dei nanodispositivi e li comunicano all'esterno della BAN tramite una comunicazione elettromagnetica. I macro dispositivi, come smartphone, ecc.. quindi, possono accedere ai dati raccolti tramite i nano-gateway.

Per quanto riguarda la sicurezza dei nanodispositivi, essi sono dotati di crittografia anche se, ultimamente, si sta sperimentando una crittografia basata sull'utilizzo del DNA come mezzo di

encryption.

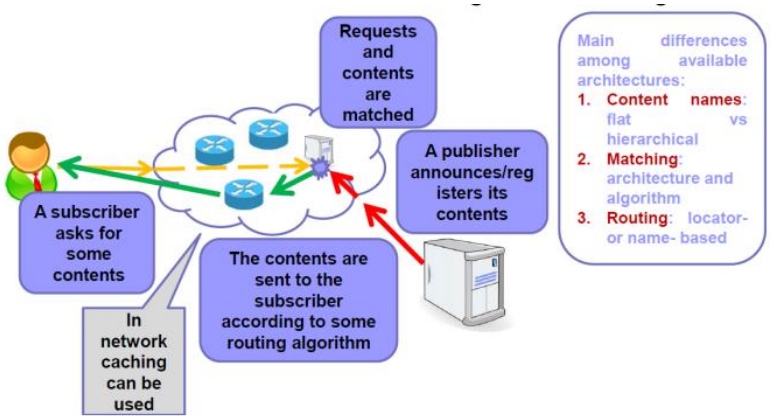
29. **Descrivere l'ICN, le sue caratteristiche ed i suoi vantaggi;**
    ICN, acronimo di **Information Centric Networking**, è un paradigma di networking che, per l'instradamento, si concentra sul contenuto dell'informazione anziché sul 'luogo' di provenienza. L'informazione viene identificata da nomi (*Named Objects Data*) e consente una comunicazione **multi-party**. ICN garantisce:
    a. **Disaccoppiamento nello spazio**: non si associa più il mittente al destinatario;
    b. **Disaccoppiamento nel tempo**: la comunicazione è asincrona, alla risposta non èè associata la domanda e viceversa

    ICN utilizza inoltre il meccanismo di **caching** (l'informazione viene cercata in cache prima di inoltrare la domanda) e si concentra sul **profilo del subscriber** garantendo agli utenti di accedere ai servizi da dispositivi differenti.

30. **Come si è evoluta la rete?** (*dalle reti tradizionali a quelle incentrate sull'informazione*)
    Con l'enorme quantità di dati generata dall'IoT non è più possibile instradare le informazioni utilizzando i protocolli di routing basati sull'identificazione dei nodi di destinazione, come ad esempio gli indirizzi IP. Nella tecnologia IoT infatti è più importante il dato piuttosto che sapere chi siano il mittente/destinatario. Proprio per questo, è nata la tecnologia ICN, che si occupa della gestione di grandi quantità di dati e della loro distribuzione all'interno della rete incentrando il networking sull'informazione, a differenza delle reti 'tradizionali', le cui comunicazioni si basavano sull'host ed erano rivolte ad un end-point.

31. **Parlare del paradigma dell'ICN**
    ICN è un paradigma di networking che si concentra sul contenuto dell'informazione, le informazioni sono identificate da nodi (Named Data Objects o NDOs) e vengono cercate all'interno di una rete distribuita attraverso un meccanismo di caching consentendo di ridurre il traffico in rete e migliorando le prestazioni. ICN supporta inoltre la comunicazione multi-party, in cui i dati possono essere trasmessi contemporaneamente a più destinatari.

32. **Descrivere un modello ICN astratto** (*publisher/subscriber*) **elencandone vantaggi e svantaggi**
    In un classico modello ICN astratto:
    a. Un publisher annuncia che è stato registrato del contenuto;
    b. In un momento diverso (disaccoppiamento nel tempo), un subscriber richiede del contenuto;
    c. Solo a questo punto la domanda e la risposta sono 'matched' in quanto avvengono in modo asincrono;
    d. Il contenuto viene inviato al subscriber mediante un algoritmo di routing.



In un modello del genere il routing del contenuto passa in secondo piano a favore della ricerca di un nodo che fornisca la migliore risposta ed il miglior servizio. I principali vantaggi di questo modello sono:

a. **Native multicast**: uno stesso dato può essere utilizzato in diverse applicazioni e servizi e da diversi utenti
b. **Native multipath routing**: i contenuti possono essere ottenuti da più nodi contemporaneamente;
c. **Supporto della mobilità**: i subscriber sono legati al profilo e non al dispositivo
d. **Content distribution**: tutti i contenuti sono disponibili utilizzando la stessa architettura
e. **Encryption dei contenuti**
f. **Maggiore efficienza della rete** dovuto all'utilizzo dell'in-network caching all'interno di ICN

33. **Descrivere una possibile implementazione del modello ICN**

Una possibile implementazione del modello ICN prevede che i vari dispositivi forniscano i dati e li mandino ad un punto di raccolta chiamato **aggregatore**, che li combina e li manda ad un **Local Service Gateway**; quest'ultimo può inglobare al suo interno un server che:

a. Svolge una serie di funzioni quali: device discovery, naming service, user registration, service discrovery, content delivery ecc…
b. Si occupa di gestire le problematiche legate alla sicurezza;
c. Usa i dati ricevuti per soddisfare i servizi richiesti dagli utenti.

Quando un nuovo dispositivo/sensore/utente deve registrarsi, avvia una secure user registration: tramite questa procedura, manda i suoi dati all'aggregatore, il quale li manda al Local Service Gateway, che effettua la registrazione e genera delle credenziali che manderà al richiedente.

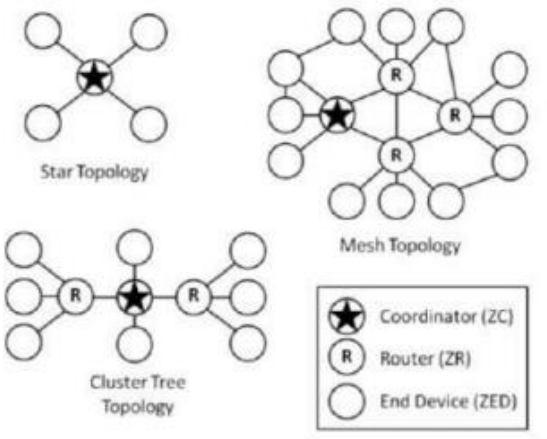
---------- Protocolli e Standard (ZigBee, 6LoWPAN & IPv6) ----------

34. **Descrivere il protocollo ZigBee. Quali sono le sue topologie? Dove viene utilizzato? Indicare inoltre i profili**

ZigBee è un protocollo di comunicazione wireless a basso consumo energetico ed a corto raggio, sviluppato per il monitoraggio dei dispositivi IoT. Supporta diverse topologie di rete ed utilizza lo standard di trasmissione 802.15.4 per la comunicazione dati e, grazie ad esso, ZigBee ha un impatto energetico molto ridotto sui dispositivi, il che lo rende ottimale per applicazioni in cui l'efficienza energetica è cruciale.

Le reti ZigBee supportano le seguenti topologie:

a. **Rete a stella**: è la topologia più semplice; è composta da un solo dispositivo centrale chiamato coordinator che funge da hub mentre tutti gli altri sono connessi direttamente ad esso;
b. **Rete mesh**: è una topologia di rete più complessa e flessibile rispetto alla stella; i dispositivi sono organizzati in nodi interconnessi, chiamati router, che agiscono come ponti per estendere la copertura della rete. I vari router sono collegati al coordinator e possono comunicare tra di loro per instradare pacchetti attraverso la rete;
c. **Rete a cluster tree**: questa topologia organizza i dispositivi in gruppi chiamati cluster; ciascuno di essi è controllato da un router, che sarà l'unico a parlare con il coordinator centrale. Questa topologia di rete è adatta in quei contesti in cui è richiesta un elevato livello di sicurezza.



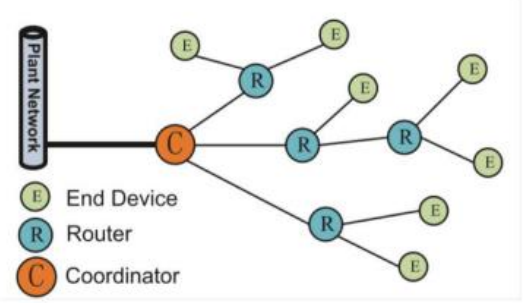
ZigBee è un protocollo che ha diversi utilizzi, principalmente viene utilizzato per applicazioni che richiedono una gestione intelligente dell'energia ed una comunicazione a bassa potenza e a corto raggio, come ad esempio il controllo dell'illuminazione domestica.

35. **Quali sono le componenti di una rete ZigBee?**

Le principali componenti di una rete ZigBee sono:

a. **Coordinator**: è il dispositivo principale, ha il compito di inizializzare la rete ZigBee e consentire ad altri dispositivi di accedere al sistema;
b. **Router**: è responsabile dell'attività di instradamento delle informazioni nella rete. Sono sempre attivi e lavorano per mantenere la connessione tra i vari dispositivi, migliorando la copertura di rete;
c. **End devices**: sono dispositivi a basso consumo energetico che acquisiscono e trasmettono informazioni nella rete.

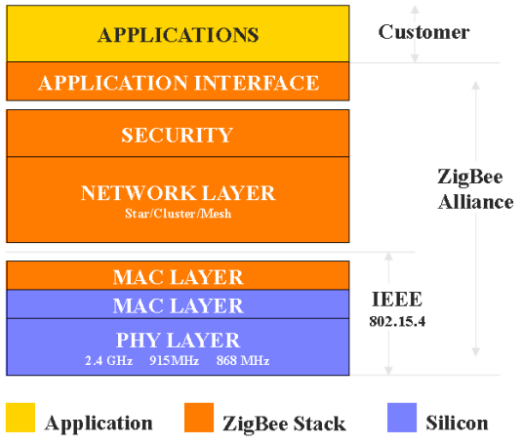
Un esempio di rete che utilizza il protocollo ZigBee (con topologia cluster tree) è la seguente:



36. **Descrivere lo stack di comunicazione di una rete ZigBee**

Lo stack di comunicazione di ZigBee si compone su più livelli e, nello specifico:

a. **Applications layer**: è il livello più alto nello stack e contiene le applicazioni specifiche dell'utente che utilizza la rete ZigBee;
b. **Application interface layer**: offre un'interfaccia tra le applicazioni dell'utente e il livello di sicurezza;
c. **Security layer**: gestisce la sicurezza fornendo crittografia, autenticazione ed altre funzionalità di sicurezza nella rete ZigBee;
d. **Network layer**: questo livello gestisce il routing dei pacchetti all'interno della rete ZigBee;
e. **MAC** (Media Access Control) **layer**: è responsabile del controllo dell'accesso al mezzo di trasmissione ovvero gestisce il modo che utilizzano i nodi di accedere al canale di comunicazione occupandosi di trasferire i pacchetti-dati tra il livello di rete ed il livello fisico
f. **PHY layer**: abbreviazione di PHYsical layer, rappresenta l'interfaccia tra la rete ZigBee ed il mezzo fisico di trasmissione; si occupa della codifica e decodifica dei dati, della modulazione e demodulazione del segnale e del controllo degli errori.



37. **Descrivere il protocollo 6LoWPAN. Quali sono i suoi vantaggi/svantaggi? Quali sono i suoi tipi di architettura?**

6LoWPAN, acronimo di **IPv6 over Low power Wireless Personal Area Network**, è un protocollo di comunicazione wireless che si adatta al protocollo IPv6 per reti a basso consumo energetico ed è stato definito per risolvere i problemi di limitatezza degli indirizzi IPv4 e per fornire una soluzione di comunicazione efficiente a basso consumo energetico per le reti IoT. I principali vantaggi di 6LoWPAN sono:

a. Essendo un protocollo definito da IETF, garantisce l'uso di **standard aperti e affidabili** nel lungo termine;
b. Offre una **curva di apprendimento semplice** grazie alla sua integrazione con IPv6
c. Consente di **integrare le reti wireless in modo trasparente con internet**, offrendo la possibilità di comunicare con qualsiasi dispositivo
d. Garantisce una **facile manutenzione della rete** grazie all'utilizzo di standard aperti e alla possibilità di integrare facilmente nuovi dispositivi nella rete esistente
e. 6LoWPAN consente di **creare reti wireless altamente scalabili** e di connettere un grande numero di dispositivi in modo efficiente, grazie ad IPv6 che offre un ampio spazio di indirizzamento
f. Supporta l'utilizzo di **API socket standard**;
g. È stato progettato per utilizzare il **minimo di codice e memoria possibile**, garantendo una maggiore efficienza e durata della batteria dei dispositivi;

h. **Integrazione diretta end-to-end**: consente una comunicazione diretta end-to-end con internet, offrendo molteplici opzioni di topologia per la creazione della rete.

Per quanto riguarda le architetture di 6LoWPAN invece, sono 3, e nello specifico:

a. **Simple LoWPAN**: ha solo un edge router collegato ad un router che a sua volta è connesso ad internet e che viene fornito all'edge router da un server remoto;
b. **Extended LoWPAN**: vi sono diversi edge router collegati ad una backbone link che estende la copertura della rete. La backbone link è data da un server locale ed è connessa ad un router che è a sua volta connesso ad internet
c. **Ad-hoc LoWPAN**: non ha nessuno edge router e non comunica con l'esterno. In questa architettura non esiste alcun percorso di comunicazione al di fuori della rete 6LoWPAN stessa.

38. **Quali sono le caratteristiche di adattamento di 6LoWPAN? Indicare anche le caratteristiche aggiuntive**

Le principali caratteristiche di adattamento di 6LoWPAN sono:

a. **Compressione efficiente dell'header**: 6LoWPAN utilizza tecniche di compressione per ridurre la dimensione dell'header IPv6 e UDP, permettendo una trasmissione più efficiente dei dati;
b. **Frammentazione**: i pacchetti IPv6 vengono frammentati in pacchetti di dimensione massima di 127 byte per adattarsi alla dimensione massima dei frame 802.15.4.

vi sono inoltre ulteriori caratteristiche di adattamento, tra cui:

a. *Supporto per indirizzamento 802.15.4 sia a 64 bit che a 16 bit;*
b. *Utilizza il protocollo Neighbor Discovery per la configurazione automatica della rete;*
c. *Supporta le trasmissioni unicast, multicast e broadcast;*
d. *Può utilizzare IP per l'instradamento dei pacchetti;*
e. *Può utilizzare reti mesh a livello di link per estendere la copertura di rete.*

39. **Cos'è IPv6? Indicare le principali caratteristiche**

IPv6 è un protocollo per internet, evoluzione del precedente IPv4. Le principali caratteristiche di IPv6 sono:

a. **Redesign completo degli indirizzi IP**: IPv6 utilizza indirizzi a 128 bit, fornendo un numero molto più elevato di indirizzi possibili rispetto ad IPv4;
b. **Indirizzo gerarchico a 128 bit con identificazione di host separato**: IPv6 usa un identificatore di host separato, che semplifica la configurazione di rete e la gestione degli indirizzi
c. IPv6 supporta **l'auto-configurazione**, semplificando la configurazione di rete;
d. IPv6 **semplifica il routing e la gestione degli indirizzi** e quindi, è più efficiente per gestire il traffico di rete

40. **Quali differenze ci sono tra l'indirizzamento IPv4 e l'indirizzamento IPv6?**

le principali differenze che ci sono tra l'indirizzamento IPv4 e l'indirizzamento IPv6 sono:

a. Nell'header IPv6 vi sono delle *classi di traffico con livelli differenti di priorità*, nell'header IPv4 no;
b. La frammentazione è presente per entrambi gli indirizzamenti, *ma la frammentazione nell'indirizzamento di IPv6 non è ottimale per 6LoWPAN in quanto l'obiettivo è quello di ridurre le trasmissioni*;
c. IPv4 utilizza un indirizzo IP a 32 bit, composto da 4 ottetti separati da punti (es. 192.168.0.1). IPv6 invece utilizza un indirizzo IP a 128 bit composto da 8 gruppi di 4 cifre

esadecimali separati da due punti (es. 2001:0db8:85a3:0000:0000:8a2e:0370:7334), che consente un numero di dispositivi connessi virtualmente illimitato;

d. *IPv6 offre un supporto migliore per la sicurezza e l'affidabilità di rete* e ciò comporta un miglioramento generale sulle prestazioni della rete, anche grazie alle classi di traffico e allo scheduling che tiene conto delle caratteristiche del servizio.

41. **Quali sono le caratteristiche del format di 6LoWPAN?**
il format 6LoWPAN è un formato di header di adattamento che consente l'uso di IPv6 su collegamenti wireless a bassa potenza. Le sue principali caratteristiche sono:
    a. **Compressione dell'header IPv6**: che consente di ridurre la dimensione dell'header del pacchetto; in questo modo facilita la trasmissione su collegamenti a banda stretta;
    b. **Compressione dell'header UDP**: che viene utilizzata per identificare le applicazioni all'interno del pacchetto;
    c. **Supporto per le classi di traffico per IPv6**: le quali consentono di definire differenti livelli di priorità per i pacchetti trasmessi sulla rete e permettono un trattamento differenziato dei pacchetti, in base alle esigenze delle diverse applicazioni

42. **Come avviene la compressione dell'header di 6LoWPAN?**
la compressione dell'header IPv6 ed UDP è resa possibile grazie all'uso di algoritmi di compressione specifici, che vengono applicati al pacchetto prima della trasmissione. Vengono applicati inoltre alcuni escamotage per comprimere l'intestazione, tra cui:
    a. Fissare il valore della versione 6;
    b. L'uso di valori comuni per i campi d'intestazione che consentono l'utilizzo di moduli più compatti;
    c. L'assegnamento del valore 0 alla classe di traffico e all'etichetta di flusso;
    d. Il calcolo della lunghezza del payload derivato sempre dall'header L2

43. **Quali sono le caratteristiche dell'indirizzamento IPv6?**
Un indirizzo IPv6 è composto da 128 bit, di cui 64 bit di **prefisso** e 64 bit di **IID** (è un ID di interfaccia). Il prefisso ha una struttura gerarchica, che identifica la rete su cui ci si trova e la sua posizione globale, mentre l'IID identifica l'interfaccia di rete e deve essere unico all'interno di una stessa rete.

44. **Perché i protocolli 6LoWPAN dovrebbero evitare la frammentazione?**
La frammentazione dei pacchetti IPv6 di grandi dimensioni su reti mesh wireless a bassa potenza può comportare prestazioni scadenti. Ciò è dovuto al fatto che la perdita di uno qualsiasi dei frammenti può causare la ritrasmissione dell'intero pacchetto, il che comporta un maggior utilizzo della larghezza di banda e un aumento del ritardo del canale.
Per tutti questi motivi, i protocolli 6LoWPAN dovrebbero evitare la frammentazione.

45. **Descrivere l'operazione di autoconfigurazione ed il funzionamento di 6LoWPAN**
l'auto configurazione è un'operazione importante nelle reti embedded e 6LoWPAN la eredita da IPv6, avendo quindi la capacità di scoprire i nodi vicini ed auto configurarsi. Per far funzionare una rete 6LoWPAN è necessario:
    a. Garantire la connettività a livello di collegamento tra i nodi (**commissioning**);
    b. Configurare gli indirizzi a livello di rete, effettuare il rilevamento dei vicini e le registrazioni (**bootstrapping**);
    c. Applicare un algoritmo di routing che stabilisce i percorsi (**route initialization**);
    d. Effettuare una **manutenzione continua**;

la configurazione iniziale di una rete 6LoWPAN inoltre, richiede la definizione di una serie di parametri, tra cui:

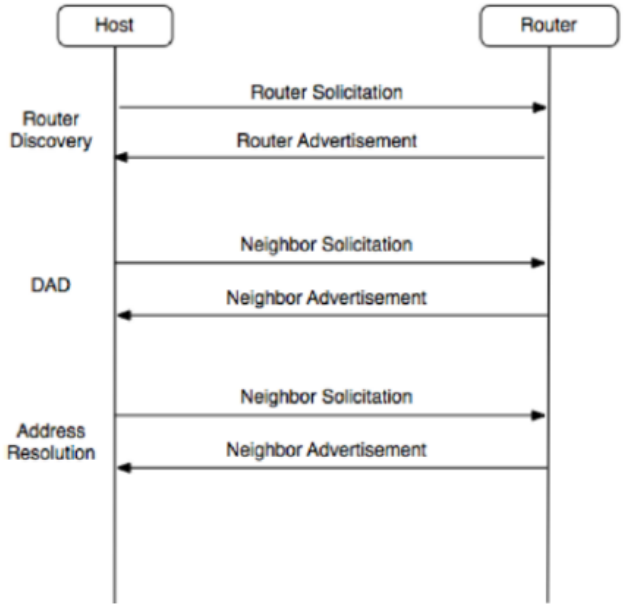
a. Il prefisso dell'indirizzo;
b. L'IID, ovvero l'ID dell'interfaccia;
c. L'indirizzo del gateway;
d. I parametri di sicurezza.

Richiede inoltre una pianificazione attenta dei percorsi di routing per evitare problemi di congestione e perdita di pacchetti.

46. **Descrivere il protocollo di rete IPv6 Neighbor Discovery** (*descrivere RS, RA, NS, NA*)
IPv6 ND è un protocollo di rete, definito nella RFC4861, per la gestione degli indirizzi e, nello specifico, per trovare i dispositivi vicini ed i router su una rete IPv6. il suo funzionamento è dato dall'utilizzo di 4 messaggi:

a. **Neighbor Solicitation** (NS) e **Neighbor Advertisement** (NA) per trovare i vicini;
b. **Router Solicitation** (RS) e **Router Advertisement** (RA) per trovare i router.

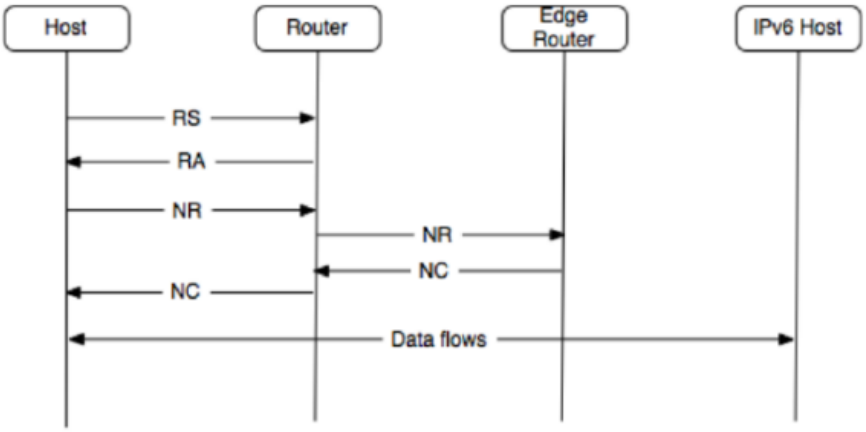
Il funzionamento è il seguente: l'host cerca il router inviando un messaggio di RS e ricevendo un RA (se lo trova); dopodiché cerca i vicini inviando un NS e, se trova dei vicini, riceve un NA. A questo punto IPv6 si occupa della risoluzione degli indirizzi utilizzando il messaggio di NS per richiedere l'utilizzo di un indirizzo e il messaggio di NA per confermare l'utilizzo dell'indirizzo.



47. **Descrivere il protocollo di routing 6LoWPAN Neighbor Discovery, quindi, descrivere la Node Confirmation e la Node Registration**
6LoWPAN ND è un protocollo di routing ad un salto che fornisce un collegamento ed un modello di sottorete appropriati per le reti wireless a bassa potenza riducendo al minimo il traffico di controllo generato dai nodi. Fornisce **Node Registration** (NR) e **Node Confirmation** (NC), **Duplicate Address Detection** (DAD), **recovery** e **supporto per infrastrutture Edge Router estese**. Il suo funzionamento è il seguente:

a. L'host invia un messaggio di RS per identificare un router in modo da poter effettuare la registrazione;
b. Il router risponde con un messaggio di RA;

c. A questo punto, l'host (che corrisponde al nuovo nodo) può inviare al router un messaggio di NR;
d. Tale messaggio si diffonde all'interno della rete fino ad arrivare all'Edge Router che lo intercetta e manda la conferma al nodo tramite un messaggio di NC;
e. A quel punto il nodo (l'host) può trasmettere e comunicare con i dispositivi della rete 6LoWPAN.



---------- Protocolli e Standard (ROLL, RPL, CoAP, MQTT) ----------

48. **Descrivere il gruppo IETF ROLL**
ROLL, acronimo di Routing Over Low power and Lossy networks, è un gruppo di IETF che standardizza i protocolli di routing per le applicazioni embedded, dove per 'applicazioni ambedded' si intendono applicazioni incorporate in dispositivi elettronici con risorse limitate come microcontrollori, sensori ecc…
ROLL sta definendo un protocollo di routing chiamato RPL (Ripple), che utilizza un approccio di routing proattivo di tipo distance vektor, anticipando e tenendo conto dei possibili comportamenti della rete.

49. **Descrivere il protocollo RPL** (*vantaggi, requisiti, caratteristiche, object functions e tipi di messaggi*)
RPL (Ripple) è un protocollo di routing in via di sviluppo definito dal gruppo ROLL. Alcuni degli obiettivi di questo protocollo includono:
a. Il routing di pacchetti unicast/anycast/multicast;
b. L'adattività del routing attraverso diverse metriche;
c. Il routing basato sui vincoli per i percorsi paralleli;
d. La scalabilità.

RPL permette di conoscere la topologia di tutta la rete grazie all'utilizzo di DODAG. DODAG, acronimo di Destination-Oriented Directed Acyclic Graph, è una struttura dati utilizzata dal protocollo per organizzare i nodi in un grafo aciclico diretto consentendo il routing efficiente dei pacchetti nelle reti a basso consumo energetico e a perdita di pacchetti.
L'obiettivo principale di RPL è quindi quello di definire un DODAG, che in funzione delle esigenze di trasmissione, definite come Object Functions, tiene conto di tutte le possibili connessioni tra dispositivi di rete e stabilire un percorso tra mittente e destinatario.
Gli Object Functions si stabiliscono tenendo conto delle metriche e dei constraints che sono, nello specifico:

a. Metriche: sono delle informazioni scalari che riguardano le performance dei link/paths e possono essere classificate:
    i. A livello di link:
        1. La reliability: è la capacita di resistere ai failure e viene espressa ETX e LQL (Expected Transmission Count e Link Quality Level)
    ii. A livello dei nodi:
        1. La potenza residua;
        2. La capacità di memoria;
        3. La CPU;
        4. Ecc…
    iii. A livello di hop:
        1. Il numero di hop tra i nodi
b. Vincoli: ovvero criteri per eliminare determinati percorsi (o cammini) da un DODAG

All'interno del protocollo RPL inoltre, vengono utilizzati 3 tipi di messaggi:

a. DIO (DODAG Information Object): viene utilizzato per costruire il DODAG. Questo messaggio viene inviato periodicamente dai nodi genitori ai loro figli per informarli sulla topologia di rete e sui valori delle metriche e dei vincoli. Il DIO contiene tutte le informazioni necessarie per scambiare metriche ed impostare i vincoli. (sono i messaggi più importanti in quanto contengono l'object function)
b. DAO (Destination Advertisement Object): viene utilizzato per propagare informazioni sulle destinazioni o sui prefissi. Questo messaggio viene inviato dai nodi figli ai loro genitori per annunciare le destinazioni o i prefissi raggiungibili tramite il nodo figlio. (supporta il traffico point-to-point e point-to-multipoint)
c. DIS (DODAG Information Solicitation): viene utilizzato per richiedere il DIO. Questo messaggio viene inviato da un nodo che vuole conoscere la topologia della rete ma non ha ancora ricevuto il DIO dal suo genitore. Il DIS viene inviato tramite broadcast e viene utilizzato per avviare il processo di scoperta della topologia di rete.

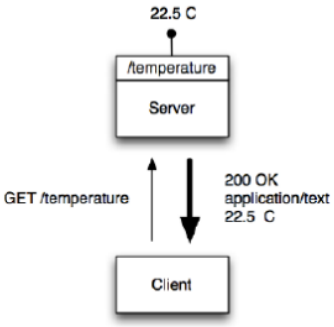
50. **Descrivere il protocollo CoAP** (*requisiti di progettazione, caratteristiche principali e messaggistica*)
CoAP, acronimo di Constrained Application Protocol, è un protocollo utilizzato fornire servizi web-services per constrained wireless network. Una constrained wireless network è una rete wireless con memoria limitata ed a bassa potenza. L'obiettivo del protocollo CoAP è quello di abilitare web services in reti wireless con risorse limitate. Le caratteristiche principali del protocollo CoAP sono:
    a. CoAP è un embedded web transfer protocol;
    b. Utilizza un modello di transazione asincrono poiché comunica con un proxy anziché con un end-point;
    c. Utilizza UDP con supporto multicast e affidabilità;
    d. Identifica le risorse tramite URI;
    e. Utilizza un header di soli 4 byte;
    f. Utilizza un sottoinsieme di MIME types e codici di risposta HTTP;
    g. Dispone di una funzionalità di discovery integrata;
    h. Consente il trasferimento opzionale di osservazione e di blocchi

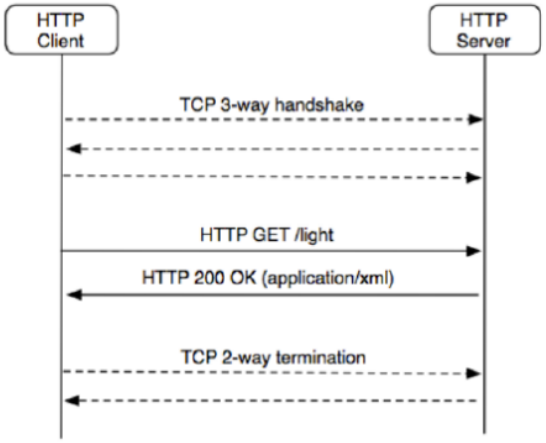
Per quanto riguarda la messaggistica, in CoAP avviene tramite lo scambio di messaggi end-point, ognuno dei quali è composto da un'intestazione di 4 byte contenente un ID del messaggio a 16 bit. Offre uno scambio affidabile di messaggi, con possono essere confermati tramite ACK/message reset ed in caso di mancata ricezione di conferma, viene effettuata una ritrasmissione semplice

stop-and-wait con exponential backoff.

51. **Descrivere il protocollo HTTP** (*descrivere UDP, TCP e spiegare il funzionamento di HTTP*)
HTTP, acronimo di Hypertext Transfer Protocol, è un protocollo utilizzato per trasmettere informazioni usando il meccanismo di Request/Response. L'interazione tra Client e Server è composta da diversi layer protocollari, che includono un Application Layer, un Transport Layer, un IP Layer ed un Network to Access.
per quanto riguarda i protocolli di trasporto, ne esistono di 2 tipi:
    a. TCP: è un protocollo connection-oriented che si basa sulla commutazione di circuito e garantisce robustezza e sicurezza;
    b. UDP: è un protocollo connection-less che si basa sulla commutazione di pacchetto ed è utilizzato per applicazioni real-time.

HTTP, tra i 2 protocolli di trasporto illustrati, sceglie di utilizzare TCP ed il suo funzionamento è il seguente:
    a. Inizialmente deve essere effettuato il set-up per la comunicazione tra client e server: viene effettuato tramite 3-way handshake, attraverso il quale viene creato un socket, ossia un'interfaccia tra il livello di trasporto ed il livello applicativo dello stack protocollare;
    b. Successivamente, il client invia una richiesta di HTTP GET per richiedere informazioni;
    c. Il server risponde con una HTTP RESPONSE, che contiene un tag OK ed un codice (es. 200);
    d. Dopo avere acquisito le informazioni richieste, il client rilascia le risorse e chiude la connessione TCP mediante una TCP 2-way termination





52. **Descrivere il protocollo MQTT** (*a cosa serve, aspetti tecnici, topics, messaggi e confronto con HTTP*)
MQTT, acronimo di Message Queuing Telemetry Transport, è un protocollo di messaggistica leggero sviluppato da IBM nel 1999. Le sue caratteristiche sono:
    a. È progettato per la comunicazione tra dispositivi con risorse energetiche limitate, per lower power and lossy networks e per publisher e subscriber;
    b. È orientato agli eventi e ai messaggi;
    c. Utilizza il protocollo di trasporto TCP e si basa su un broker. Si basa inoltre sul concetto di topic: i messaggi vengono pubblicati su un topic specifico e i client possono sottoscriversi a quel topic così da rimanere aggiornati sui messaggi pubblicati su di esso. Un topic è una stringa di caratteri UTF-8 usata dal broker per filtrare i messaggi di ogni client connesso. Può avere 1 o + livelli (topic levels) e formano una struttura logica ad albero.
    d. È in grado di gestire i messaggi sia in modo affidabile che in modo non affidabile; i messaggi affidabili vengono confermati tramite ACK/messaggi di reset, mentre i messaggi non affidabili possono essere gestiti, ma senza ACK;

e. Prevede una ritrasmissione semplice stop-and-wait con exponential backoff;
f. È agnostico rispetto al contenuto del payload, il che significa che può essere utilizzato con qualsiasi tipo di informazione, dal testo alle immagini;
g. Sono disponibili implementazioni di MQTT per tutte le principali piattaforme di sviluppo IoT.

Tra gli aspetti tecnici, ci sono:

a. La distribuzione dei messaggi uno-a-molti;
b. La decoupling delle informazioni tra le fonti ed i consumatori;
c. L'agnosticità rispetto al contenuto del payload;
d. La costruzione sui protocolli TCP/IP;
e. L'utilizzo di un trasporto a basso overhead

Rispetto ad HTTP, MQTT viene utilizzato per inviare un maggior numero di messaggi e per avere un maggior risparmio energetico ed è inoltre in grado di ridurre il traffico in rete grazie alla struttura leggera e alla possibilità di comunicazione asincrona. MQTT però, a differenza di HTTP, ha un numero maggiore di messaggi inviati/ricevuti persi.

---------- LPWAN, LoRaWAN, NB-IOT, MANET, AODV ----------

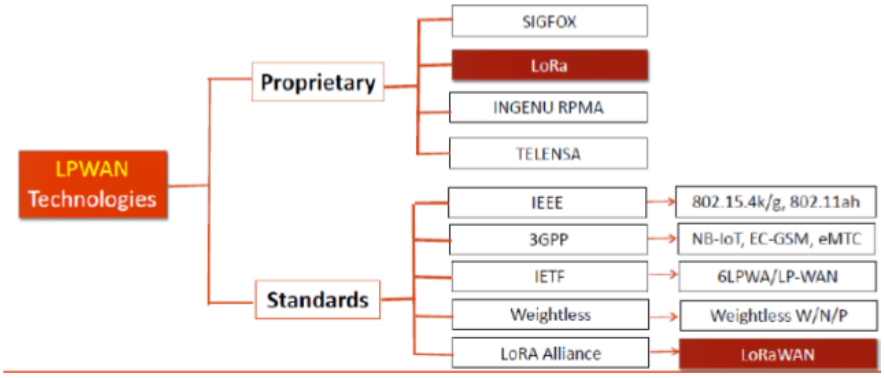
53. **Descrivere LPWAN** (*vantaggi, svantaggi e soluzioni standard o proprietarie*)
LPWAN, acronimo di **Low Power Wide Area Network**, è un protocollo di comunicazione wireless che fornisce connettività a lungo raggio per dispositivi a bassa potenza ed a bassa velocità di trasmissione dati. I principali vantaggi di questo protocollo sono:
    a. **L'ampio raggio di copertura** per la comunicazione wireless, che può arrivare anche a decine di km utilizzando poca potenza per la trasmissione dati;
    b. **Il miglioramento della propagazione del segnale** anche in luoghi difficili da raggiungere;
    c. **Il basso consumo energetico** dovuto principalmente a:
        i. La topologia predominante, la stella, che permette una connessione diretta tra gli end-devices e la base station (al centro della stella), senza aver bisogno di multi-hop;
        ii. L'utilizzo di protocolli MAC ad accesso casuale, come ad esempio, ALOHA, che minimizza l'utilizzo di energia nei dispositivi terminali LPWAN. ALOHA infatti, è un protocollo MAC leggero che consente ai dispositivi di accedere al mezzo trasmissivo in modo casuale, senza sincronizzazione con altri dispositivi;
    d. Il **basso costo**, dovuto principalmente a:
        i. HW semplificato, che riduce il lavoro di processamento di LPWAN;
        ii. Infrastrutture minime; LPWAN infatti utilizza una singola base-station per fornire copertura all'intera rete, riducendo i costi di infrastruttura;
        iii. Uso di bande senza licenza o di proprietà (es. bande industriali, scientifiche, medicali, ecc..), che abbatte i costi di manutenzione e la dipendenza da terze parti.
    e. La **scalabilità**, nello specifico:
        i. LPWAN utilizza tecniche di comunicazione multi-channel e multi-antenna in modo da avere più comunicazioni tra dispositivi LPWAN in parallelo;
        ii. In LPWAN, il data rate viene adattato alle condizioni del traffico del canale di comunicazione (o channel). Con il termine data rate, si intende la quantità di informazione che può essere trasmessa in una certa unità di tempo dai nodi.

iii. Le reti LPWAN sono molto dense, per cui l'allocazione delle risorse è ben coordinata ed ottimizzata.

Per quanto riguarda invece gli svantaggi di LPWAN, sono:

a. **Bassa velocità di trasferimento dei dati**;
b. **Lunghezza limitata del payload**;
c. **Delay elevato**.

La tecnologia LPWAN ha diverse soluzioni, proprietarie e standard. Le soluzioni proprietarie funzionano solo all'interno di altri dispositivi compatibili con la stessa soluzione mentre gli standard, sono regole concordate tra più enti che definiscono le specifiche per poter comunicare ed utilizzare determinate frequenze, in modo che i produttori possano creare dispositivi conformi.



54. **Descrivere LoRaWAN** (*soluzione standard di LPWAN, elencarne le caratteristiche e descriverne la topologia*)

LoRaWAN, è una soluzione standard di LPWAN che definisce tutte le regole per una comunicazione LPWAN tra i dispositivi ed ha le seguenti caratteristiche:

a. **Basso impatto computazionale**;
b. **Grande raggio di trasmissione** (fino a 10km di distanza);
c. **Bassa velocità di trasmissione** (da 250bps fino a 50kbps);
d. **Dimensione massima dei pacchetti** di 255 byte;
e. Una **frequenza** dai 433MHz ai 915MHz;
f. Utilizza **il protocollo ALOHA**, ovvero il protocollo MAC di LPWAN;
g. È una **comunicazione verticale**, perché riesce a lavorare con qualunque tipo di dispositivo.

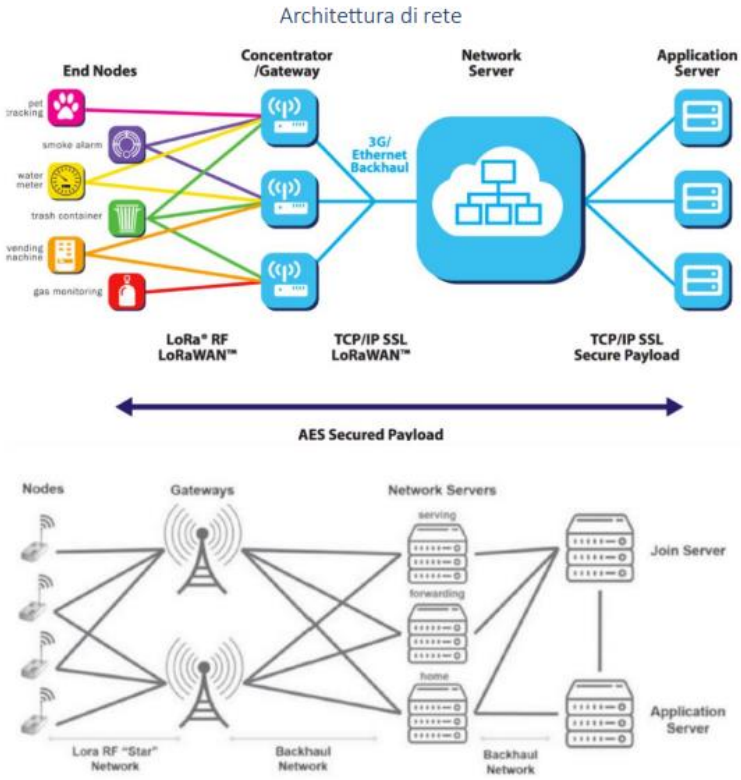
I nodi sensori di LoRaWAN includono 2 livelli:

a. Un livello fisico LoRaWAN MAC che contiene tutte le informazioni necessarie per il valore MAC;
b. Un livello application LoRaWAN per la crittografia delle informazioni.

Inoltre, nella topologia di rete, sono presenti i seguenti dispositivi:

a. I **nodi**;
b. Il **gateway**: acquisisce i dati da client diversi tramite una connessione cablata e li distribuisce ai Network Server tramite una rete backhaul
c. Il **network server**: è il componente back-end che si occupa di compiti complessi come ad esempio, la rilevazione e filtrazione dei duplicati. Implementa inoltre l'adaptive data rate control dei dispositivi LoRaWAN
d. **L'application server**: si occupa di effettuare il data processing in base alle caratteristiche specifiche delle applicazioni;

e. Il **join server**.



1. **Gli end-nodes che comunicano con i gateway.**
2. **I gateway acquisiscono tantissime informazioni da parte dei nodi.**
3. **Ogni gateway manda i dati al Network Server tramite una connessione backhaul.**
4. **Il Network Server cripta e decripta i dati ricevuti dal gateway per mandarli all'Application Server.**
5. **L'Application Server è l'applicazione che usa i dati (fa il data processing).**

55. **Quali sono le classi di LoRaWAN (A, B, C) e quali sono le loro caratteristiche**

All'interno di LoRaWAN e *in particolare, nel livello LoRa MAC*, i dispositivi possono essere classificati secondo 3 classi differenti:

a. Dispositivi di **classe A**: hanno le seguenti caratteristiche:
   i. Effettuano comunicazione bidirezionale;
   ii. Gli end-devices sono alimentati da batterie;
   iii. Gli end-devices inizializzano la comunicazione in uplink;
   iv. Ogni trasmissione in uplink è seguita da 2 brevi periodi di downlink;
   v. Le comunicazioni in downlink dal server dovranno aspettare la prossima schedulazione di uplink quindi, di conseguenza, il server non è sempre in ascolto né può comunicare sempre con il nodo

b. Dispositivi di **classe B**: hanno le seguenti caratteristiche:
   i. La comunicazione con gli end-devices è bidirezionale;
   ii. Gli end-devices sono alimentati a batterie;
   iii. Ogni trasmissione in uplink è seguita di 2 brevi periodi di downlink. Nonostante questo, è possibile aprire degli ulteriori periodi di ricezione nei periodi schedulati;
   iv. Vi è comunicazione sincrona tra server ed end-devices: il server parla con gli end-devices solo quando questi ultimi sono in ascolto;
   v. Possono avere latenza dovuta alla sincronizzazione

c. Dispositivi di **classe C**: hanno le seguenti caratteristiche:

i. La comunicazione con gli end-devices è bidirezionale;
ii. Gli end-devices non hanno energy constraints perché sono collegati ad una backbone;
iii. Il periodo di ricezione degli end-devices è sempre aperto, eccetto durante le trasmissioni;
iv. Il server può inviare dei dati in qualsiasi momento, non vi è latenza;
v. Gli end-devices possono inviare sia messaggi unicast che molticast

56. **Descrivere NB-IoT** (*caratteristiche principali e modalità di deployment*)
NB-IoT è una tecnologia LPWAN progettata per l'IoT mobile, evoluzione della tecnologia LoRaWAN. Sfrutta la copertura globale delle reti mobili per raggiungere dispositivi IoT su scala globale. Le sue principali caratteristiche sono:
    a. **Utilizza frequenze LTE** anziché il set di frequenze libere degli Hertz utilizzate da LoRaWAN;
    b. **Ha bassi data rate e consumi energetici ridotti**;
    c. Offre un **ampio raggio** di copertura;
    d. È **altamente scalabile**;
    e. Offre **bassi costi**;
    f. Ha un **delay elevato** per le comunicazioni rispetto ad altre tecnologie e questo, è dovuto al long range;
    g. Ha un **throughput** limitato a messaggi corti inviati ogni ora/giorno/settimana;
    h. **Richiede 180 KHz di larghezza di banda** di sistema minima sia in downlink che in uplink.

    Per quanto riguarda il deployment di NB-IoT, vi sono 3 diverse modalità:
    a. **Guard-band**: è allocato all'interno dei guard-band delle reti cellulari LTE esistenti;
    b. **Stand-alone**: è allocato in una banda di frequenza separata;
    c. **In-band**: è allocato all'interno della banda di frequenza della rete cellulare esistente

57. **Descrivere MANET** (*caratteristiche, obiettivi e come viene classificato tale protocollo di routing*)
MANET, acronimo di **Mobile Ad-hoc Network**, è un sistema di nodi autonomi che sfruttano una comunicazione wireless; non necessita del supporto di infrastrutture di rete come gateway o Base Stations ed ha una topologia wireless della rete che può cambiare in modo dinamico e imprevedibile a causa dei nodi che possono spostarsi liberamente in base alle esigenze applicative. Ogni nodo è equipaggiato con un'antenna che ha le funzioni di ricezione e trasmissione; inoltre, è presente un trasmettitore wireless ed un ricevitore con un'antenna appropriata.
In MANET, le informazioni vengono trasmesse tramite un approccio **store-and-forward** che utilizza l'instradamento *multi-hop*. Le sue principali caratteristiche sono:
    a. **Topologia dinamica**, dovuta ai nodi in grado di muoversi liberamente;
    b. **Link con capacità variabile** limitata dalla larghezza di banda;
    c. **Limitazioni energetiche** dovute al fatto che alcuni nodi possono essere provvisti di batterie/fonti di energia esauribili;
    d. **Sicurezza fisica limitata** causata principalmente dal fatto che le comunicazioni sono di tipo wireless.

    I principali obiettivi della tecnologia MANET sono:

    a. Garantire la massima affidabilità;
    b. Scegliere un percorso con il minor costo metrico;
    c. Dare ai nodi il miglior tempo di risposta e throughput possibile;
    d. Il calcolo del percorso deve essere distribuito; questo perché il routing centralizzato in una rete dinamica è molto costoso;

e. Il calcolo del percorso non deve comportare la manutenzione dello stato globale;
f. Ogni nodo deve avere un accesso rapido ai percorsi su richiesta;
g. Ogni nodo deve essere preoccupato solo dei percorsi verso la sua destinazione;
h. Le trasmissioni broadcast devono essere evitate in quanto poco affidabili;
i. È desiderabile avere un percorso di backup quando quello primario diventa obsoleto.

per quanto riguarda la classificazione di MANET come protocollo di routing, possiamo dire che è da classificare come protocollo di routing reattivo, ovvero che determina il percorso solo quando ci sono dati da inviare.

58. **Descrivere AODV (*caratteristiche e funzionalità di base*)**

AODV, acronimo di **Ad-hoc On-demand Distance Vector Routing**, è un protocollo di routing reattivo utilizzato in reti ad-hoc wireless in cui sono presenti nodi che possono essere mobili e non vi sono infrastrutture fisse. Utilizza un metodo chiamato **table-driven**, cosicché i nodi mantengano solo le informazioni sulle destinazioni che sono state richieste di recente; questo per risparmiare energia e risorse di memoria. Utilizza come metrica di routing il numero di hop (salti) ed ha le seguenti caratteristiche:

a. È **on-demand**: sceglie il percorso quando esiste il dato da inviare;
b. È **reattivo**: determina il percorso solo quando ci sono i dati da inviare;
c. **Introduce un piccolo ritardo**: perché calcola il percorso al momento (è inutile calcolarlo prima a causa dei nodi che si spostano);
d. Offre una **comunicazione unicast, multicast** e **broadcast**;
e. **È senza loop** in quanto vi sono delle regole di Distance Vector che fanno in modo che un messaggio non possa tornare indietro;
f. C'è **quick aging**;
g. Le rotture dei collegamenti sono facilmente riparabili;
h. Il **routing** è **distribuito hop-by-hop**, in quanto i nodi si scambiano le tabelle di routing;
i. L'approccio è deterministico;
j. È **single path**;
k. È **state-dependent**: dipende tutto dallo stato

Il protocollo AODV inoltre, minimizza il numero di trasmissioni broadcast necessarie creando percorsi on-demand.

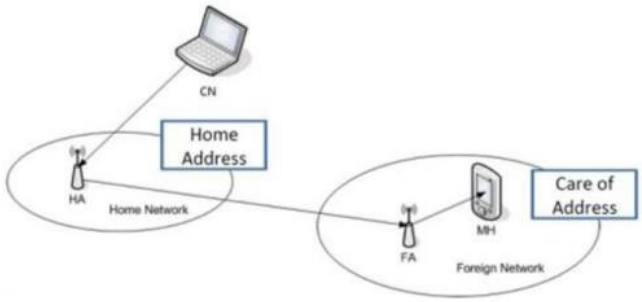
---------- Mobile IP ----------

59. **Cos'è MIP?**

il **Mobile IP** è uno standard IETF progettato per risolvere il problema del Mobile Host: quando un utente si sposta, il suo indirizzo IP deve cambiare e ciò causa l'interruzione delle sessioni di comunicazione esistenti.
Il suo obiettivo principale è quello di garantire la mobilità trasparente per i protocolli di alto livello senza apportare troppi cambiamenti all'infrastruttura internet. La soluzione è il tunneling, che consiste nell'incapsulare un indirizzo IP all'interno di un altro indirizzo IP richiedendo quindi l'utilizzo di 2 indirizzi.
Come già indicato, MIP utilizza 2 indirizzi IP per identificare il Mobile Host:

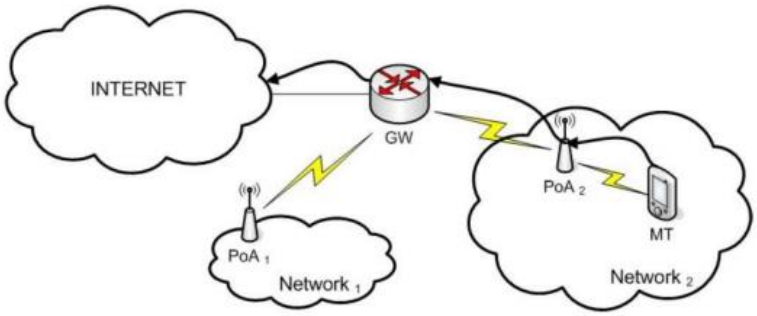
a. **Uno per il routing** (Care of Address): indica la posizione reale del Mobile Host ed è associato alla rete esterna in cui il mobile si sposta;

b. **Uno per la posizione** (Home Address): non cambia mai

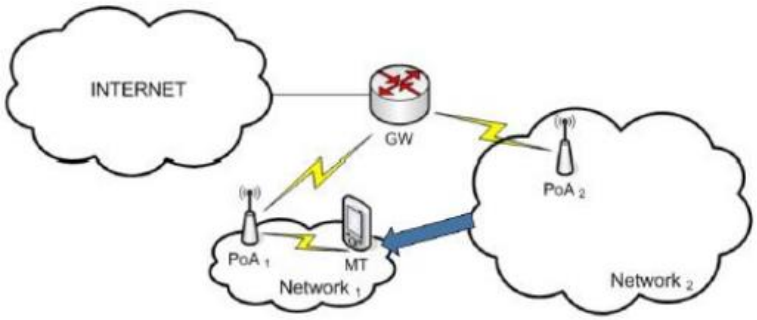


60. **Descrivere il tunneling di MIP**

Quando un dispositivo mobile si connette ad un AP (Access Point), può connettersi ad internet ottenendo un indirizzo IP, ad esempio, tramite DHCP.



Quando il mobile esce dal raggio di copertura di una rete (es. $Network_1$) questo cambia rete (passando alla $Network_2$) e la connessione con internet viene interrotta. È quindi necessario stabilire una nuova connessione con l'AP della nuova rete ed ottenere un nuovo indirizzo IP.



per evitare queste interruzioni, viene utilizzato il tunneling, ovvero un sistema di incapsulamento dei pacchetti IP, che inserisce un pacchetto IP nel payload di un altro pacchetto IP.

---------- Middleware (AWS e IBM Watson) ----------

---------- Middleware (ThingSpeak e NOS) ----------

---------- Middleware (Funzionalità del NOS) ----------

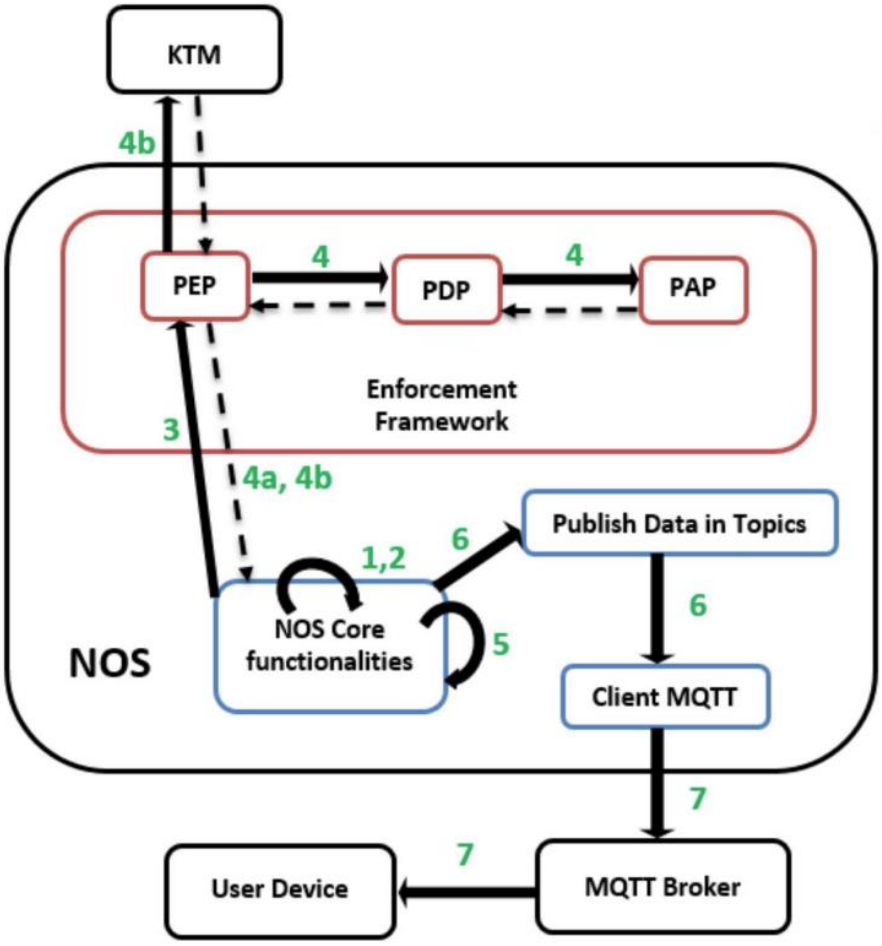
---------- Middleware (NOS e Sticky Policies) ----------

---------- Middleware (NOS) ----------

61. **Descrivere il sistema di autenticazione AUPS**

AUPS è un sistema di autenticazione del broker in un sistema di Publish&Subscribe che utilizza un sistema di gestione delle chiavi ed un framework per l'enforcement per le politiche di sicurezza. L'idea di far autenticare anche il broker, nasce come contromisura per affrontare il problema dello shadow broker ovvero, un broker malevolo che assume l'identità di un broker legittimo. Il suo funzionamento è il seguente:

a. Il NOS riceve una richiesta di pubblicazione di un dato su un topic;
b. Il NOS inoltra questa richiesta al Framework di enforcement;
c. Nel framework di enforcement, la richiesta viene intercettata dal PEP, che la invia al PDP. Quest'ultimo controlla se la richiesta soddisfa le politiche definite dal PAP confrontandola direttamente con il PAP o con la base di dati delle politiche.
d. Se la richiesta è conforme alle politiche, il PDP invia un'autorizzazione al PEP.
e. A questo punto, il dato può essere pubblicato sui topic e successivamente arriva al broker MQTT.
f. Il broker invia il dato al cliente che si è sottoscritto a quel particolare topic.



62. Cosa si intende per sistema di sincronizzazione?
63. **Spiegare l'architettura di enforcement**

Per fare fronte ai tentativi volontari o involontari di violazione delle politiche di privacy e sicurezza, è stato sviluppato un framework di politiche di enforcement.
Nello specifico, per NOS, è stato definito un linguaggio cross-domain nel quale le entità, le interazioni e le regole sono definite nella forma di tag XML.
Queste politiche, specificate con linguaggio JSON supportano meccanismi per

a. Controllare gli accessi sia degli utenti che delle sorgenti dati: questa funzione viene svolta da ABAC (Attribute Based Access Control), un approccio data-centric basato sugli attributi
b. Controllare i dati a disposizione degli utenti

Viene inoltre identificato un set di primitivi in grado di fare l'enforcement di diverse politiche attribute-based, tra cui:

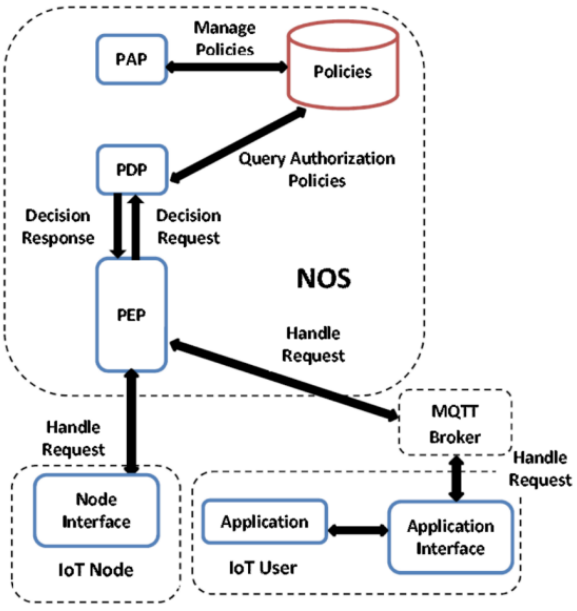
a. Node accesso control;
b. Node data trasmission;
c. Node date processing;
d. User access control;
e. User service request;
f. Service provision.

Per la realizzazione di una politica di enforcement abbiamo bisogno:

a. PEP (Policy Enforcement Point) che intercetta le richieste dai nodi e dagli utenti;
b. PDP (Policy Decision Point) che verifica se le richieste sono conformi alle politiche;
c. PAP (Policy Administration Point) che gestisce le politiche nella base di dati.

Il suo funzionamento è il seguente:

PEP intercetta sia le richieste dei nodi sia quelle dei broker (NOS non usa MQTT). I nodi vogliono fornire dei dati, mentre il broker vuole pubblicare/fornire dati degli utenti della piattaforma IoT. qualunque richiesta che arriva dai nodi viene intercettata dal PEP che le inoltra al PDP. Dopodiché il PDP verifica se la richiesta è conforme alle politiche, facendo delle query su un DB che contiene tali politiche (gestite dal PAP).
Infine, il PDP, invia una risposta al PEP il quale invia al nodo che aveva fatto la richiesta



64. **Quali sono le principali vulnerabilità che vengono valutate nell'analisi del rischio?**

Uno dei concetti fondamentali su cui si basa la sicurezza, è il rischio, che non può essere nullo. Generalmente, qualsiasi cosa criptata, può essere decifrata in un certo periodo di tempo, è quindi importante monitorare costantemente il livello di sicurezza, analizzando i rischi e valutando le potenziali vulnerabilità e, nello specifico:

a. Valutare l'affidabilità della piattaforma IoT, sia nelle componenti statiche che in quelle dinamiche;
b. Trovare le vulnerabilità e le minacce prima che diventino attacchi veri e propri;
c. Svelare le debolezze esistenti.

65. **Quali sono i passaggi dell'analisi del rischio?**
I principali step dell'analisi del rischio sono:
    a. Definizione dei componenti del modello e le loro interazioni usando delle connessioni dirette;
    b. Identificazione delle possibili vulnerabilità per ogni componente;
    c. Per ogni vulnerabilità trovata, l'assegnamento di un punteggio di attaccabilità definendo come 'exploitability' il livello di attaccabilità di una vulnerabilità;
    d. Identificazione delle possibili dipendenze tra le vulnerabilità;
    e. La rivalutazione dei valori di exploitability in base alle dipendenze tra vulnerabilità trovate.

66. Quali sono i potenziali rischi associati all'attacco ad un singolo NOS nel sistema IoT?
67. Descrivere il ruolo del leader dei NOS nella coordinazione e gestione dei NOS distribuiti nel sistema IoT
68. Come avviene l'aggiunta, l'eliminazione e l'aggiornamento delle politiche nei NOS distribuiti?
69. Quali canali di comunicazione vengono utilizzati per la sincronizzazione dei NOS?
70. **Perché l'utilizzo di un singolo NOS rappresenterebbe un problema nel sistema IoT?**
l'utilizzo di un singolo NOS costituisce un fallimento sia dal punto di vista fisico che dal punto di vista logico. Se questa macchina dovesse essere attaccata o si dovesse guastare, l'intero sistema smetterebbe di funzionare. Inoltre, un sistema con un unico NOS permetterebbe ad un hacker di:
    a. Isolare diverse reti IoT e tecnologie;
    b. Avere l'accesso completo a tutti i dati e, quindi, la possibilità di violare l'integrità degli stessi o accedere ad informazioni confidenziali non autorizzate.

71. Qual è la differenza tra una minaccia e un attacco in termini di sicurezza informatica?
72. Quali sono i potenziali rischi associati all'attacco ad un singolo NOS nel sistema IoT?
73. Qual è l'obiettivo dell'analisi del rischio nell'ambito della sicurezza del sistema IoT?
74. Quali sono i passaggi nell'analisi delle dipendenze tra le vulnerabilità nel sistema IoT?
75. Come viene rivalutata l'attaccabilità delle vulnerabilità nel contesto del dominio applicativo?