F.A.Q. Esame orale di “Reti di Calcolatori” prof. Esposito

1)Parlare del Three-Way-Handshake:
È un fondamentale processo di inizializzazione delle connessioni TCP usato nei protocolli di comunicazione su internet.
Questo procedimento coinvolge l’invio di tre messaggi coordinati tra il mittente e il destinatario per stabilire una connessione affidabile e bidirezionale. I tre messaggi sono SYN (syncronize) SYN-ACK e ACK.
Durante il T.W.H. il mittente invia un pacchetto di richiesta di connessione (SYN); il destinatario risponde con un pacchetto di conferma della richiesta(SYN-ACK); infine il mittente conferma la ricezione del pacchetto di conferma (ACK).
Questa procedura garantisce che entrambi i nodi siano pronti per scambiare dati in modo sincronizzato

perché si usa questo e non uno più semplice?

Non per la sicurezza ma per evitare che possibili messaggi multipli causino l’instauramento di una connessione anche se il client non l’ha richiesta oppure che si vada a perdere un messaggio del server o che il client pensa di avere la connessione invece non c’è.

2)Come funziona il controllo di flusso in TCP?
Il livello di trasporto implementa il controllo del flusso per evitare che un mittente trasmetta dati più velocemente di quanto il destinatario sia in grado di elaborare.
Entrambi gli host della connessione TCP riservano un buffer di ricezione, nei quali vanno collocati i dati correttamente ricevuti.
L’applicazione leggerà poi quei dati direttamente dal buffer, ma non necessariamente nel preciso momento in cui verranno allocati nel buffer . Ma se l’applicazione che sta leggendo i dati è lenta, il tender potrebbe sovraccaricare l’applicazione che perderà i nuovi dati. Il controllo del flusso si basa su due componenti:
-Finestra di ricezione, il destinatario comunica al mittente quanta capacità di ricezione ha disponibile, che viene espressa in quantità di dati. Il mittente quindi regola il flusso di dati in base a questa finestra.
-Finestra di congestione, che evita l’intasamento della rete imponendo un limite alla quantità di traffico che un host può inviare. Il mittente monitora costantemente le condizioni della rete e la finestra di congestione è regolata automaticamente

3)Parla di HTTP
Hypertext Transfer Protocol è il protocollo di comunicazione usato per il trasferimento di documenti ipertestuali come pagine web, su Internet. Le richieste di HTTP vengono effettuate dai browser web ai server web per recuperare contenuti web.

4) Protocollo ALOHA
Fa parte dei protocolli ad accesso casuale dove un nodo trasmette sempre alla velocità massima consentita dal canale (K b/s).
nell’ALOHA puro ogni dispositivo ha la possibilità di trasmettere in qualsiasi momento senza una sincronizzazione con gli altri dispositivi sulla rete. Quando un dispositivo ha un pacchetto di dati da inviare, lo trasmette immediatamente sulla rete.
Se la trasmissione di un pacchetto si sovrappone a quella di un altro dispositivo sulla stessa frequenza, si verifica una collisione tra i pacchetti e entrambi i dispositivi riceveranno un segnale di errore. In tal caso i dispositivi riproveranno a trasmettere il pacchetto in un momento successivo in modo casuale.

Nello Slotted ALOHA, il canale viene diviso in intervalli di tempo, chiamati slot, di lunghezza fissa. Ogni dispositivo ha la possibilità di inviare un pacchetto dati in uno dei qualsiasi degli slot disponibili, ma può farlo solo all'inizio di un determinato slot.
Se un dispositivo trasmette in uno slot, gli altri dispositivi devono attendere quello successivo per evitare collisioni tra pacchetti. Slotted ha il vantaggio di ridurre le collisioni ma richiede un sincronismo tra i dispositivi per coordinare l'invio dei pacchetti quindi non è adatto a reti ad alta densità di traffico o con dispositivi a basso costo e bassa potenza.

5)Cos'è il NAT?
Network Address Translation è un meccanismo che permette di mappare un indirizzo IP in un altro indirizzo IP. Le reti locali hanno diversi indirizzi IP privati che riguardano precisi dispositivi connessi ala rete. Attraverso il NAT questi indirizzi vengono tradotti in un indirizzo IP pubblico quando le richieste in uscita vengono inviate ad Internet. Il processo inverso si verifica nel caso i dati siano in entrata.

6) Algoritmo di Routing Distance Vector
Uno degli algoritmi di routing basati sul percorso più breve è OSPF (Open Shortest Path First di Dijkstra): tale algoritmo mantiene in una tabella la più piccola distanza conosciuta per ogni destinazione e quale canale utilizzare per raggiungerla. Tali tabelle vengono aggiornate scambiando informazioni con i router vicini. Questo è un algoritmo greedy.
L'algoritmo di Dijkstra utilizza il protocollo distance vector: l'idea è quella di partire dal nodo sorgente e di guardare i nodi adiacenti assegnando loro il valore del costo per raggiungerli.

7) Cos'è il routing link state?
È un algoritmo di routing che nasce con l'intenzione di sostituire il Distance Vector e si basa sull'invio di pacchetti detti Link State Packet (LSP), contenenti le informazioni di costo e di ritardo di ogni link uscente dal nodo in cui si opera. La propagazione avviene tramite flooding (simile al broadcast), ogni nodo poi usa queste informazioni per calcolare il costo minimo verso gli altri nodi. Si costruisce quindi un grafo di rete e si usa Dijkstra per trovare il cammino minimo. Quindi a differenza del Distance Vector avremo una visione totale della rete e non parziale. Però gli algoritmi LSP non possono gestire qualsiasi rete, quindi per reti di grandi dimensioni si fa il routing in modo gerarchico suddividendo la rete in aree.

8)Parlare del DNS e delle due modalità di query.
Domain Name System è un database distribuito (decentralizzato) che svolge un ruolo cruciale nella conversione dei nomi di dominio in indirizzi IP e viceversa, facilitando così la comunicazione tra computer e server all'interno della rete.
Il DNS opera come una "rubrica telefonica" globale per Internet. Ogni dispositivo connesso ad Internet ha un indirizzo IP unico, che è una serie numerica difficile da ricordare, il DNS quindi risolve questo problema permettendo agli utenti di usare nomi di dominio significativi tipo "example.com" anziché dover inserire gli indirizzi IP numerici corrispondenti. Il DNS distribuisce anche il carico di richieste.
Server DNS Locale: è il primo server DNS a cui un dispositivo si rivolge quando cerca di tradurre un nome di un dominio in un indirizzo IP. Esso è configurato nella rete locale ISP o sul dispositivo dell'host richiedente.
Se la richiesta non può essere soddisfatta dal DNS locale, verrà inoltrata al server DNS superiore attraverso una struttura gerarchica.

Quando un utente digita l'indirizzo, il sistema DNS avvia una serie di query(ricorsiva) che inizia dai root server e scende lungo la gerarchia fino ad arrivare il server DNS autoritativo appropriato per il dominio cercato, il quale poi restituisce l'indirizzo IP associato.
Nelle query iterative la negoziazione con i vari name server autoritativi per le zone interessate è gestita interamente dal resolver. Quando un DNS impara la mappatura, la mette nella cache.

9) Protocollo ARP
Nel livello di rete il problema principale è quello di trovare l'indirizzo MAC corretto a cui inviare il pacchetto contando che l'host conosce solo l'indirizzo IP del destinatario.
Quindi si ci appoggia ad un protocollo chiamato ARP (Address Resolution Protocol).

Poniamo di avere un host con indirizzo IP A1 e con indirizzo MAC MA1 il quale deve inviare un pacchetto IP ad un host con indirizzo IP A2 sulla stessa rete. ARP si procura le informazioni necessarie nel seguente modo:
-Viene costruito un pacchetto data-link (chiamato ARP Request) contenente A1,MA1,A2 e MA2, quest'ultimo contrassegnato da una serie di 0;
-Tale pacchetto viene inviato in broadcast sulla rete locale;
-Tutti ricevono tale pacchetto ARP, ma solo l'host con MAC MA2 lo processerà;
-L'host di destinazione creerà un pacchetto data-link (chiamato ARP Response) nella quale inserirà il campo mancante. Tale pacchetto verrà trasmesso in maniera diretta e non in broadcast;
-Viene quindi acquisito il MAC MA2 rilegato all'indirizzo IP A2.
Esiste anche l'ARP reverse che serve a trovare l'indirizzo IP associato ad un indirizzo MAC.

10)Cosa dicevano Shannon e Nyquist?
Entrambi hanno enunciato teoremi che esprimono la massima velocità di trasmissione per ogni tipo di canale.
Nyquist permette di stabilire la massima quantità di informazione trasmessa (bit rate) in un canale non rumoroso.
"Dato un segnale con banda limitata B, si può ricostruire il segnale se la frequenza di campionamento è maggiore o uguale a 2B"(generalmente deve essere leggermente maggiore a 2B.
Invece il teorema di Shannon permette di stabilirlo in un canale rumoroso:
"La frequenza di campionamento deve essere almeno il doppio della frequenza massima presente nel segnale di ingresso, cioè la frequenza più elevata tra le sue componenti armoniche"

11) Parla della posta elettronica
La posta elettronica fa riferimento al protocollo SMTP (Simple Mail Transfer Protocol) che fa parte dei protocolli applicativi del livello di applicazione. Si usa per invia e recapitare email tramite TCP.
In particolare definisce la sequenza di comandi (inviati in ASCII) necessaria per il trasferimento dei messaggi. Usa un insieme minimale di comandi (helo,mail-from,rcpt-to,data,quit).
Possono essere usati anche latri protocolli oltre SMTP per inviare e ricevere la posta: IMAP e POP3.
La modalità POP3 consente di scaricare tutti i messaggi della posta in arrivo dal server direttamente sul pc o sul dispositivo che stai utilizzando. Eventuali messaggi di posta inviata, Cestino, Bozze o altri non verranno salvati. Se selezioni l'opzione "mantiene

messaggi sul server per n giorni" potrai ritrovare esclusivamente i messaggi della cartella "posta in arrivo" sulla webmail. Se non selezioni l'opzione di mantenere i messaggi sul server, i messaggi resteranno esclusivamente sul suo dispositivo e saranno cancellati dalla webmail.
Nella modalità IMAP viene lasciata tutta la posta sul server così da poter essere consultata anche da webmail e su più dispositivi, incluse le sottocartelle. Se elimini un messaggio dalla webmail, esso sparirà anche da tutti i dispositivi configurati con IMAP e viceversa. Se anche un solo dispositivo fosse configurato in modalità POP3, questo dispositivo scaricherebbe rutti i messaggi eliminandoli dalla webmail e da tutti i dispositivi configurati con IMAP.

LIVELLO FISICO

- codifiche RZ/NRZ/AMI/MANCHESTER/...
- Tecniche di modulazione ASK/FSK/PSK/...
- multiplazione
- doppino/fibra/ecc...

DATA-LINK [PACCHETTI]

- framing (header/Trailer con CRC e altro)
- RDT
- protocolli TDMA/ALOHA/CSMA
- switch/bridge/eThernet
- spanning Tree/ADSL/ATM
- SONET

NETWORKING (RETE) [datagrammi]

- iP
- submitting
- routing/Atonomous System
- ARP/Distance Vector/Routing Link State/R.I.P.
- Split Horizon/Poisoning

TRASPORTO

- TCP / UDP / Three-Way-Handshake
- socket

APPLICAZIONE

- posta elettronica
- DNS / SMTP
- HTTP / Browser

———————————DOMANDE GENERICHE PER LIVELLI———————————
-LIVELLO FISICO

1)Cos'è il doppino?
È composto da due fili di rame attorcigliati tra loro ricoperti da una guaina isolante(binatura).

2)Il cavo coassiale
È un cavo ormai sostituito da doppino e fibra ottica e viene usato solo nelle reti WAN. È un filo di rame rigido circondato da una garza metallica.

3)Fibra Ottica
È un cavo composto da un'anima trasparente in silicio puro(core), avvolta in un rivestimento in silicio con indice di rifrazione diverso(cladding).
La propagazione al suo interno può avvenire in due modi:
MONOMODALE: il nucleo permette il passaggio di poche lunghezze d'onda. Questo fa comportare la fibra come una semplice guida d'onda.
MULTIMODALE: il nucleo è abbastanza ampio da permettere diversi angoli di rimbalzo della luce trasmessa. Può essere step-index se la variazione dell'indice di rifrazione tra core e cladding è brusca e causa molta dispersione modale, per questo motivo non vengono più usate; oppure graded-index se la variazione continua degli indici di rifrazione rallenta i raggi più centrali.

4)Trasmissione power-line?
È una tecnologia che usa la rete di alimentazione elettrica come mezzo di trasmissione sovrapponendosi, usa una frequenza più elevata.

5)Quali sono le trasmissioni wireless?
RADIODIFFUSIONE: viene usato per il broadcasting, il segnale segue le curvatura terrestre fino ai MHz, dai MHz ai GHz viene assorbito dalla superficie terrestre ma viene riflesso bene dalla ionosfera
VIA PONTE RADIO: per le frequenze tra 1-40GHz e instaura una comunicazione ottica rettilinea punto-a-punto. Se si usano più stazioni si possono coprire grandi distanze.
SATELLITE: usa la tecnologia FDM(ossia la divisione in sottocanali) e usa bande 1-10GHz

6)DTE,DSE
Il DTE è un qualsiasi calcolatore connesso alla rete, il DSE è un nodo di commutazione intermedio della rete, che commuta il traffico tra due DTE

7)Cos'è un segnale?
È una variazione di grandezza fisica che trasporta informazioni e possono essere di vario tipo(acustico, elettrico, luminoso,…) e si dividono in ANALOGICO (quando varia nel tempo e può assumere tutti i valori tra il max e il min) e DIGITALE (può assumere solo due valori).
Un segnale di periodo T può essere sviluppato in serie di Fourier come una somma di infinite sinusoidi di ampiezza variabile.
La rappresentazione di dati numerici con segnali numerici è normalmente fatta tramite sequenze di impulsi discreti di tensione di una certa durata temporale. Il dato binario è codificato in modo da dar corrispondere al valore di un bit, un determinato livello del segnale.

8)Cosa dicevano Shannon e Nyquist?
Entrambi hanno enunciato teoremi che esprimono la massima velocità di trasmissione per ogni tipo di canale.
Nyquist permette di stabilire la massima quantità di informazione trasmessa (bit rate) in un canale non rumoroso.
"Dato un segnale con banda limitata B, si può ricostruire il segnale se la frequenza di campionamento è maggiore o uguale a 2B"(generalmente deve essere leggermente maggiore a 2B.
Invece il teorema di Shannon permette di stabilirlo in un canale rumoroso:
"La frequenza di campionamento deve essere almeno il doppio della frequenza massima presente nel segnale di ingresso, cioè la frequenza più elevata tra le sue componenti armoniche"

9)Cos'è il rumore?
È una forma di energia indesiderata che si somma al segnale utile degradandone il contenuto informativo, ed impedendo così, di rilevare in ricezione tutto l'insieme delle informazioni trasmesse e può essere di varie tipologie:
Bianco, intermodulazione, modo comune, quantizzazione, termico.
C[bit/s]=Blog2 (1+S/N)
C=capacità del canale, S=potenzasegnale, N= potenza rumore
Aumentare il segnale porta solamente ad un aumento degli errori e non ad una riduzione del rumore.

10)Codifiche:
RZ: lunghezza T per ogni bit, segnale nullo per 0, T/2 per 1.
NRZ: uguale alla RZ, il bit 1 rimane alto.
AMI: usa tre livello, il livello 0 per il bit 0. Il livello +V/-V per il bit 1.
PSEUDOTERNARIA: uguale alla AMI ma con 0 ed 1 invertiti.
MANCHESTER: due livelli di tensione, -V per mezzo periodo per il bit 1, +V per mezzo periodo per il bit 0.
MANCHESTER DIFFERENZIALE: usa lo stesso tipo, ma rappresenta 1 come variazione rispetto alla codifica del bit precedente.

11)La modulazione
È un processo con il quale il segnale da trasmettere(segnale modulante) viene usato per modificare nel tempo le caratteristiche di un segnale ausiliario(portante). Ciò permette di trasmettere più comunicazioni differenti e contemporaneamente sullo stesso mezzo.
Il segnale si può modulare in ampiezza(ASK-amplitude key shifting), per cambio fase(PSK-Phase key shifting) e in altri modi.

-DATA LINK

1)Cos'è il framing?

Detto anche incapsulamento, è una tecnica usata per dividere il pacchetto in unità più piccole chiamate frame, a ciascuna ne aggiunge un header e trailer che me garantisce una consegna affidabile.

L'header viene aggiunto all'inizio del frame e contiene indirizzo di destinazione, lunghezza del frame e altre informazioni di controllo.

Il trailer viene aggiunto alla fine e contiene informazioni sul controllo degli errori dei dati come il checksum o il CRC.

Un frame può essere individuato in 3 modi: conteggio caratteri(l'intestazione indica il numero dei caratteri nel pacchetto); indicatori di inizio e fine (sequenza di 0 111 111 0); con una violazione di codifica.

2)Checksum e CRC

Il checksum viene calcolato sommando tutti i byte trasmessi e viene aggiunto nell'header di ogni frame, a destinazione di ripete il calcolo e si confronta.

Il Cyclic Redundancy Check invece, considera i dati da trasmettere come un polinomio e viene usato un algoritmo basato sulla divisione polinomiale per generare un valore di controllo (CRC code) che viene aggiunto al trailer; in ricezione viene ricalcolato il CRC e si fa la verifica.

3) RDT e pipeline

Reliable Data Transfer, è un insieme di tecniche per il controllo trasmissivo:

1.0 - senza controllo, viene usata se il canale di comunicazione è perfetto

2.0/2.1 - viene inviato un ACK(acknowledgment) o un NAK (negative ack), è detto anche di stop-and-wait in quanto bisogna aspettare una risposta, c'è da considerare però che il feedback può arrivare corrotto, quindi va aggiunto un checksum, che produrrebbe pacchetti duplicati, quindi va aggiunto anche un numero di sequenza.

3.0 - detta sliding window, si inviano più pacchetti e aspetta un periodo di tempo, entro il quale se non riceve una risposta, rinvia i pacchetti, viene introdotto un timer.

Per usare la sliding window vengono introdotti due protocolli:

GO-BACK-N: il mittente invia pacchetti numerati e se non riceve un ack dopo un periodo di tempo, rinvia i pacchetti a partire dall'ultimo per il quale non ha ricevuto l'ack, non viene usato un buffer.

SELECTIVE REJECT: il mittente rinvia solo i pacchetti per il quale non ha ricevuto un ack.

4)Quali sono i protocolli che evitano collisioni?

Sono detti ad accesso multiplo, essi regolano anche la velocità con cui i dispositivi possono comunicare:

Se solo un nodo deve comunicare, velocità K b/s

Se N nodi devono comunicare, K/N b/s ciascuno

Questi protocolli si dividono in 3 categorie:

—a suddivisione del canale

TDMA: time division multiple access

FDMA: frequency division multiple access

—ad accesso casuale

ALOHA PURO: ogni dispositivo ha la possibilità di trasmettere in qualsiasi momento senza una sincronizzazione con gli altri dispositivi sulla rete. Quando un dispositivo ha un pacchetto di dati da inviare, lo trasmette immediatamente sulla rete.

Se la trasmissione di un pacchetto si sovrappone a quella di un altro dispositivo sulla stessa frequenza, si verifica una collisione tra i pacchetti e entrambi i dispositivi

riceveranno un segnale di errore. In tal caso i dispositivi riproveranno a trasmettere il pacchetto in un momento successivo in modo casuale.
SLOTTED ALOHA: il canale viene diviso in intervalli di tempo, chiamati slot, di lunghezza fissa. Ogni dispositivo ha la possibilità di inviare un pacchetto dati in uno dei qualsiasi degli slot disponibili, ma può farlo solo all'inizio di un determinato slot.
Se un dispositivo trasmette in uno slot, gli altri dispositivi devono attendere quello successivo per evitare collisioni tra pacchetti. Slotted ha il vantaggio di ridurre le collisioni ma richiede un sincronismo tra i dispositivi per coordinare l'invio dei pacchetti quindi non è adatto a reti ad alta densità di traffico o con dispositivi a basso costo e bassa potenza.
CSMA (Carrier Sense Multiple Access, ogni dispositivo controlla il canale di comunicazione prima di trasmettere i dati, se il canale è occupato attende prima di trasmettere i dati (carrier sense). Può succedere però un ritardo di propagazione, che porta un altro nodo a trasmettere, creando così conflitti.
CSMA PERSISTENTE: Un nodo ascolta continuamente il canale attendendo che si liberi, se è occupato attende un tempo casuale restando ad ascoltare e riprova.
CSMA NON PERSISTENTE: Il canale non resta sempre in ascolto quando trova occupato ma ritenta dopo un tempo casuale, però può crescere il tempo di attesa se ci sono tante connessioni.
CSMA P-PERSISTENTE: Ascolta continuamente il canale e se è libero trasmette con probabilità P
CSMA/CD: Collision Detection, ogni nodo ascolta continuamente il canale e trasmette se è libero, se di verifica una collisione i nodi bloccano la trasmissione e il nodo mittente trasmette Jamming (interferenze) per comunicare a tutti della collisione.
—a rotazione
MAPPA BIT ELEMENTARE: Questa mappa permette ad ogni nodo, durante il periodo di contesa, di comunicare se serve trasmettere o no(bit 1 se deve).Dopo la contesa, i nodi che hanno inviato 1 potranno trasmettere uno alla volta. L'efficienza è bassa, poiché tanti nodi potrebbero sovraccaricare la stazione di controllo.
TOKEN RING: Utilizza un insieme di collegamenti punto a punto, associati in successione tipo anello. Sull'anello circola un piccolo frame, detto token(una sequenza di bit che circola quando i nodi sono inattivi), a cui autorizzerà la trasmissione al nodo che ne è in possesso.

5)Ethernet
È una tecnologia della rete LAN che consente a dispositivi di comunicare tra loro all'interno di una rete locale, utilizza il protocollo CSMA/CD con un bus condiviso.
I PACCHETTI ETHERNET:
-L'header contiene un preambolo per la sincronizzazione, l'indirizzo MAC di destinazione e quello del mittente e il protocollo
-Il payload, contiene i dati
-Ed è presente un CRC

6)Bridge
È un dispositivo che collega due o più segmenti di rete consentendo ai dati di passare da un segmento all'altro. Quando un pacchetto arriva ad un bridge ne verifica il Mac di destinazione e sceglie se inoltrarlo al segmento di rete successivo(backward Learning).
È in grado di isolare il traffico, quando un bridge unisce, forma una rete LAN più grande con lo stesso dominio di collisione.Conserva in modo promiscuo il traffico LAN e crea una MAC Address Table che associa ogni indirizzo Mac alla porta.

7)Switch
È un dispositivo che collega due o più segmenti di rete e funziona simile al bridge, però è in grado di indirizzare il traffico di rete in modo più efficiente.
Inoltre tiene costantemente separate le reti che unisce, che quindi avranno domini di collisione separati. Quando arriva un pacchetto controlla il MAC e sceglie a quale porta inoltrarlo tramite la MAC Address Table(backward Learning).
Uno switch è composto da: Memoria condivisa, dove vengono memorizzati i pacchetti, Fabric, recapita da input ad output, Porte ,Bus interno ad alta velocità con TDMA.

8)Come avviene il Backward Learning?
Al boot, le tabelle sono vuote. Viene usato l'indirizzo di provenienza per definire la posizione del mittente. Se un pacchetto ha una destinazione sconosciuta viene inoltrato a tutte le porte tranne quella di provenienza.

9)Cosa sono gli switching loop e come possono avvenire?
Quando si connettono due o più switch possono creare 3 possibili switching loop, che si possono prevenire usando lo Spanning Tree Protocol. A partire dal protocollo IPv4 è possibile individuare due pacchetti che vanno in loop attraverso il TTL (time to live):
- REPLICAZIONE DELLA TRAMA
- INSTABILITÀ MAC ADDRESS TABLE
- BROADCAST STORM

10)Parla dello Spanning Tree Protocol
È un protocollo che costruisce una topologia locale di una rete Ethernet senza loop, usando una struttura ad albero. Rimane in ascolto facendo il backward learning e individua le interfacce(bridge o loop). Bisogna trovare il nodo radice.
La porte potranno essere in 3 modalità:
BLOCKED
ROOT,è per indicare che è quella più vicina alla radice.
DESIGNATED dove può passare il traffico normalmente.

11)Cos'è la VLAN?
Virtual Local Area Network, permette di dividere una rete basata su switch in più parti, quindi permette di segmentare il dominio di broadcast. Ciascuna VLAN è identificata da un numero VID(VLAN ID). Esistono inoltre porte chiamate *trunks* che trasportano il traffico tra multiple VLAN. È indicata principalmente per le aziende per separare il traffico.
Si può configurare in port-based o MAC-based.

12)Parla dell'architettura delle WLAN e delle WLAN IEEE 802.11
Wireless Local Area Network, è una rete locale in cui i nodi comunicano tra loro attraverso il canale radio dove risulta difficoltoso l'uso di cavi. Con uso di bande a 2.4 e 5GHz
Ha dei vantaggi: mobilità, velocità, costi, scalabilità.
La WLAN IEEE 802.11 è una architettura costituita da diverse componenti e servizi che interagiscono tra loro. La componente base è la stazione (una qualsiasi unità che ha il protocollo 802.11). Un insieme di stazioni costituisce un Basic Service Set (BSS). Abbiamo due tipologie:
- AD HOC NETWORK: è la tipologia più semplice, dove le stazioni comunicano in modalità Peer-to-Peer, se situata nel raggio di copertura, senza relay.
- INFRASTRUCTURE MODE: è una BBS con un componente chiamato access point che fornisce la funzione di relay ,la comunicazione tra stazioni avviene solo tramite access point

13)ADSL
Asymmetric Digital Subscriber Line, è lo standard per fornire all'abbonamento un accesso digitale tramite un modem collegato al doppino telefonico, si applica un passa basso a 4KHz.
Lo spettro disponibile viene suddiviso in 256 canali da 4 KHz (fino a 60 Kbps ciascuno):
Il canale 0 viene riservato per la telefonia
I successivi 4 canali non vengono utilizzati per evitare problemi di interferenza tra la trasmissione dati e quella telefonica
I restanti canali vengono destinati al traffico dati. Alcuni per il traffico uscente (upstream), altri per il traffico entrante (downstream)

14)Le reti ATM (Asyncrhonous Transfer Mode)
È un modo di trasferimento packet-oriented basato sulla multiplazione sincrona a divisione di tempo di celle di lunghezza fissa. Le celle vengono trasferite attraverso la rete in modo trasparente. Non viene effettuato il controllo di errore all'interno della rete.
Ha una architettura di rete diversa da quella ISO-OSI e TCP/IP, usa infatti una rete a più livelli e piani ortogonali tra loro, usa sempre una connessione punto-a-punto.

15) SONET(Synchronous Optical NETwork)
È una tecnologia usata per trasmissioni a lunga distanza su fibre ottiche dagli operatori telefonici. È basato sulla sincronizzazione precisa del tempo tra i nodi di rete, usa la Optical Carrier. Ha la caratteristica di rilevare e ripristinare automaticamente le interruzioni nella rete, creando percorsi alternativi. Ogni frame in SONET è di 810byte.

-LIVELLO DI RETE
È il terzo strato del modello ISO-OSI e si occupa dell' instradamento dei pacchetti tra due dispositivi separati da N nodi intermedi. Cerca di far apparire la trasmissione come punto-a-punto, mascherando l'infrastruttura della rete.
Ha due funzioni principali: instradamento, detto anche routing, consiste nel determinare il percorso ottimale che avviene attraverso algoritmi di instradamento, gestisce le congestioni e crea/aggiorna la tabella di routing. Inoltro(forwarding), inoltra i pacchetti lungo il percorso. Questo livello opera su datagrammi che contengono indirizzo di origine/ destinazione e i dati. Il livello di rete è implementato in protocolli IP.

1)Quali sono le caratteristiche di un algoritmo di routing?
È un processo mediante il quale i pacchetti dati vengono instradati da una sorgente ad una destinazione attraverso una rete di computer o dispositivi . In altre parole determina il percorso ottimale che un pacchetto deve fare per raggiungere la destinazione.
Vengono inviati da un router/gateway lungo una serie di hop (salti). Ogni router prende decisioni sul percorso da far seguire in base alla tabella di routing. Durante il routing viene estratto il campo di destinazione, si cerca la destinazione nella Routing Table , si trova il prossimo hop e viene spedito. Deve avere inoltre le seguenti caratteristiche:
– correttezza
– semplicità: meno soggetto ad errori in implementazione o in esecuzione
– robustezza: l'algoritmo deve poter fare fronte alle modifiche di topologia
– stabilità: convergenza verso l'equilibrio
– imparzialità: servire qualunque tragitto possibile senza penalizzare nessuno
– ottimizzazione: efficienza globale

1.1)Parla della routing table
Raccoglie le informazioni necessarie per individuare il percorso ottimale verso tutte le possibili reti ed è formata da:
-indirizzo IP destinazione (se presente già lo inoltra nella corrispondente porta out)
-metrica
-indirizzo router next hop
-interfaccia
Può essere STATICO se vengono configurate manualmente.
DINAMICO se vengono aggiornate automaticamente in base alle informazioni ricevute.

2) Parla del subnetting
È la divisione della singola rete in sottoreti in cui i dispositivi avranno l'indirizzo di rete identico. Viene fatto uso della network mask (o subnet mask) permettere di dividere la parte del prefisso da quella del suffisso.

3)IPv4
L'Internet Protocol è un protocollo di comunicazione a livello di rete che ha la funzione di recapitare datagrammi dalla sorgente alla destinazione. È a 32 bit, rappresentati in 4 numeri decimali che hanno valore 0-255 [XX.XX.XX.XX]
Ogni IP ha una parte che specifica la rete e una parte che identifica l'host. E sono divisi in classi in base al valore del primo campo:
-CLASSE A: [0-127], 1 prefisso, 3 suffisso, comincia con 0
-CLASSE B: [128-191], 2 prefisso, 2 suffisso, comincia con 10
-CLASSE C: [192-223], 3 prefisso, 1 suffisso, inizia con 110
-CLASSE D: [224-239], indirizzi per il multicasting, inizia con 1110
-CLASSE E: [240-255], indirizzi sperimentali, inizia con 1111

In particolar modo, ogni pacchetto IP ha una lunghezza di 20 byte, più una parte opzionale fino a 40 byte:
Tutti bit a 0 nel campo host, indica la rete specificata
Tutti bit a 0 campo rete, indica questa rete
Tutti 0 in host e rete, indica questo host di questa rete
Tutti 1 in host e rete, è l'indirizzo broadcast della rete locale
Tutti 1 nell' host, indica broadcast nella rete specificata
Gli indirizzi vengono assegnati falla ICANN, però non abbiamo sufficienti indirizzi per soddisfare la domanda, quindi si usa il subnetting. In particolare il CIDR (classless interdomain routing) permette la suddivisione dell'indirizzo IP in prefisso e suffisso senza la divisione in classi.

4)Parla di IPv6
È un modello ampliato dell'IPv4 sviluppato negli anni 90, che porta i vantaggi dell'indirizzamento illimitato, il supporto i pacchetti grandi e riduzione di tempi di elaborazione del router.
Usa un formato a 128bit(16byte) ed è diviso in 8 parti separati da ":" compiti da 4 cifre esadecimali (0-9,A-F). Il pacchetto contiene un header di 40byte e un campo dati, non è presente il checksum per motivi di efficienza.
Una macchina con IPv6 può spedire , instradare e ricevere datagrammi IPv4, ma non viceversa. Possiamo però usare indirizzi v4 compatibili con v6 oppure una DNS.

5)Come avviene il forwarding?
Avviene quando un dispositivo di rete riceve un pacchetto e determina l'interfaccia di uscita. Prende la decisione di inoltro basandosi sull' header del pacchetto.
Per quanto riguarda IPv6 abbiamo un instradamento DIRETTO se non coinvolge nessun router intermedio, INDIRETTO se vengono coinvolti, se però il destinatario si trova nella stessa sottorete si usa la procedura ARP.

6) Protocollo ARP
Nel livello di rete il problema principale è quello di trovare l'indirizzo MAC corretto a cui inviare il pacchetto contando che l'host conosce solo l'indirizzo IP del destinatario.
Quindi si ci appoggia ad un protocollo chiamato ARP (Address Resolution Protocol).
Poniamo di avere un host con indirizzo IP A1 e con indirizzo MAC MA1 il quale deve inviare un pacchetto IP ad un host con indirizzo IP A2 sulla stessa rete. ARP si procura le informazioni necessarie nel seguente modo:
-Viene costruito un pacchetto data-link (chiamato ARP Request) contenente A1,MA1,A2 e MA2, quest'ultimo contrassegnato da una serie di 0;
-Tale pacchetto viene inviato in broadcast sulla rete locale;
-Tutti ricevono tale pacchetto ARP, ma solo l'host con MAC MA2 lo processerà;
-L'host di destinazione creerà un pacchetto data-link (chiamato ARP Response) nella quale inserirà il campo mancante. Tale pacchetto verrà trasmesso in maniera diretta e non in broadcast;
-Viene quindi acquisito il MAC MA2 rilegato all'indirizzo IP A2.
Esiste anche l'ARP Reverse che serve a trovare l'indirizzo IP associato ad un indirizzo MAC.

7)Definisci un router
Un router può interconnettere reti che usano diverse tecnologie, inclusi mezzi fisici diversi.
Un router monta un sistema operativo chiamato "CISCO IOS" ed è caratterizzato da:

porte di ingresso e uscita, un blocco di commutazione, un processore che esegue protocolli di routing e varie memorie.

8)AS- Atonomous System
È il collegamento di più reti sotto lo stesso dominio, se il router instrada messaggi nello stesso AS si chiama interior router, invece se usano AS diversi verrà detto exterior router. I router invece che fungono da ponte di collegamento tra diversi AS sono detti border router.

9)Peering
È la connessione tra due AS appartenenti a provider distinti. L'instradamento avviene sempre allo stesso modo, solo che esiste un unico algoritmo di instradamento e bisogna aggiornare manualmente le tabelle di routing aggiungendo percorsi statici.

10)Parla degli algoritmi di routing
OSPF (Open Shortest Path First di Dijkstra): tale algoritmo mantiene in una tabella la più piccola distanza conosciuta per ogni destinazione e quale canale utilizzare per raggiungerla. Tali tabelle vengono aggiornate scambiando informazioni con i router vicini. Questo è un algoritmo greedy.
L'algoritmo di Dijkstra utilizza il protocollo distance vector: l'idea è quella di partire dal nodo sorgente e di guardare i nodi adiacenti assegnando loro il valore del costo per raggiungerli.
FLOODING: è un protocollo di instradamento usato dal router che inoltra un pacchetto in ingresso su tutte le linee, ad eccezione di quella da dove proviene e viene usato per trovare il percorso migliore. Questo algoritmo genera tanti pacchetti duplicati, quindi si associa ad un contatore. È molto inefficiente, siccome manda ogni pacchetto su ogni rete. Però è vantaggioso in quanto non dobbiamo conoscere la topologia della rete a priori.
ROUTING LINK STATE: è un algoritmo di routing che nasce con l'intenzione di sostituire il Distance Vector e si basa sull'invio di pacchetti detti Link State Packet (LSP), contenenti le informazioni di costo e di ritardo di ogni link uscente dal nodo in cui si opera. La propagazione avviene tramite flooding (simile al broadcast), ogni nodo poi usa queste informazioni per calcolare il costo minimo verso gli altri nodi. Si costruisce quindi un grafo di rete e si usa Dijkstra per trovare il cammino minimo. Quindi a differenza del Distance Vector avremo una visione totale della rete e non parziale. Però gli algoritmi LSP non possono gestire qualsiasi rete, quindi per reti di grandi dimensioni si fa il routing in modo gerarchico suddividendo la rete in aree.

-LIVELLO DI TRASPORTO
È il quarto strarrò del modello ISO-OSI e ha lo scopo di fornire al livello superiore un trasferimento end-to-end nascondendo le complessità della rete.
Il livello di trasporto offre due protocolli: TCP e UDP.

1)Protocollo TCP
Transmission Control Protocol è usato per effettuare una connessione Connection Oriented e full-duplex rendendolo affidabile, stabilisce una connessione prima di scambiare i dati (handshake). Suddivide i dati in pacchetti più piccoli per gestire meglio il flusso dei dati, usa la sliding window di tipo Go-Back-N. Adotta inoltre una finestra di congestione dinamica che impone un limite alla quantità di traffico che un host può inviare.
Three-Way-Handshake: questo procedimento coinvolge l'invio di tre messaggi coordinati tra il mittente e il destinatario per stabilire una connessione affidabile e bidirezionale. I tre messaggi sono SYN (syncronize) SYN-ACK e ACK.
Durante il T.W.H. il mittente invia un pacchetto di richiesta di connessione (SYN); il destinatario risponde con un pacchetto di conferma della richiesta(SYN-ACK); infine il mittente conferma la ricezione del pacchetto di conferma (ACK).
Questa procedura garantisce che entrambi i nodi siano pronti per scambiare dati in modo sincronizzato
Abbiamo anche un Four-Way-Handshake. Questo processo è un processo di interruzione della connessione dopo un TWH, in particolar modo assicura che entrambi i nodi hanno avuto l'opportunità di consegnare tutti i dati. Il mittente(client) invia un pacchetto FIN(finish) al server destinatario, il server risponde con un ACK, nel frattempo solo il server destinatario può continuare ad inviare dati se necessario. Successivamente quando il server finisce, invia anch'esso un pacchetto FIN e il mittente invia un ACK si avvenuta ricezione.

2)Protocollo UDP
User Datagram Protocol è un protocollo connectionless poco affidabile ma più veloce.
Prima dell'invio dei dati non c'è alcun tentativo di stabilire una connessione (senza handshake), cerca inoltre di inviare i dati in un unico pacchetto.
Però ha dei vantaggi: può usare la trasmissione broadcast o multicast ed è più leggero ed efficiente.

3)Porte e Socket
Una porta è un numero di 16 bit che identifica un canale virtuale all'interno di un computer che usufruisce dei servizi TCP disponibili.
Un Socket è l'estremità della connessione di una rete che fa interfacciare un processo nel sistema operativo alla connessione. È capace di effettuare una comunicazione bidirezionale.
SOCKET TCP:
Indirizzo IP origine e destinazione
Numeri di porta di origine e destinazione
SOCKET UDP:
Indirizzo IP destinazione
Numero di porta di destinazione

-LIVELLO DI APPLICAZIONE
È il quinto ed ultimo strato del Modello ISO-OSI ed è responsabile dell'interazione diretta con le applicazioni software e gli utenti finali. Questo strato fornisce servizi di rete specifici alle applicazioni e facilita la comunicazione tra i programmi e la rete sottostante.
Infatti, uno dei principali ruoli del livello applicazione è quello di servire da interfaccia utente, offrendo un mezzo attraverso cui gli utenti finali o le applicazioni possono accedere ai servizi, avviare, gestire e terminare le comunicazioni di rete.

1) Servizio SMTP
(Simple Mail Transfer Protocol) si tratta di un protocollo di comunicazione utilizzato per inviare e recapitare messaggi di posta elettronica attraverso Internet.
Nell'SMTP ci sono due componenti principali, oltre il protocollo stesso:
Agente Utente (mail reader), un programma per leggere e gestire la posta;
Mail Server, contiene una casella di posta per ogni utente con i messaggi in arrivo ed una coda di messaggi da trasmettere.
Per inviare un messaggio (che corrisponde al trasporto di un file) in modo affidabile, SMTP utilizza TCP, il quale effettua l'handshaking per aprire la connessione, trasferisce il messaggio e chiude la connessione.

2)HTTP
L' HTTP (HyperText Transfer Protocol) è un Protocollo usato come principale sistema per la trasmissione d'informazioni (pagine o elementi di pagina) dal Server al Client attraverso il Web.
Gestisce sia le richieste (URL) inviate al server che le risposte inviate al client (pagine) ed utilizza il TCP per far comunicare il client al server e viceversa.
MIME (Multipurpose Internet Mail Extensions), è uno standard utilizzato per consentire la trasmissione di dati non solo in formato testuale, ma anche in formato multimediale, come immagini, audio, video e altri tipi di dati binari.
In HTTP, MIME è utilizzato per consentire ai server Web di inviare risorse diverse dal semplice testo HTML ai browser dei client.
Quando un server Web invia una risorsa a un client tramite HTTP, solitamente include un'intestazione Content-Type che specifica il tipo di dati contenuto nella risorsa. Ad esempio, il server può specificare che il contenuto è un documento HTML, un'immagine JPEG, un file audio MP3, ecc.
I MIME types sono rappresentati da una stringa del tipo tipo/sottotipo (esempio: text/html per HTML o image/jpeg per JPEG). Queste informazioni sono utilizzate dal browser per interpretare correttamente il contenuto ricevuto e renderlo in modo appropriato.

3)DNS
Il Domain Name System (DNS) è un Database Distribuito (decentralizzato) che svolge un ruolo cruciale nella conversione dei nomi di dominio in indirizzi IP e viceversa, facilitando così la comunicazione tra computer e server all'interno della rete.
Il DNS opera come una sorta di "rubrica telefonica" globale per Internet. Ogni dispositivo connesso a Internet ha un indirizzo IP unico, che è una serie numerica difficile da ricordare. Il DNS risolve questo problema consentendo agli utenti di utilizzare nomi di dominio significativi, come example.com, anziché dover inserire gli indirizzi IP numerici corrispondenti, che sarebbero molto più difficili da memorizzare.
Il DNS può anche svolgere il compito della distribuzione del carico tra server replicati di un web server affollato e permettono di creare indirizzi IPv6 partendo da un IPv4: il kernel capisce che si tratta di un indirizzo speciale ed usa la comunicazione IPv4.

4)Gerarchia DNS

Il sistema del DNS funziona attraverso una struttura gerarchica di server.
Quando un utente digita un nome di dominio nel proprio browser o esegue qualsiasi altra operazione basata su DNS, il sistema DNS avvia una serie di query che inizia dai root server e scende lungo la gerarchia fino a raggiungere il server DNS autoritativo appropriato per il dominio cercato. Questo server quindi restituisce l'indirizzo IP associato al nome di dominio richiesto, consentendo al dispositivo di stabilire una connessione con il server desiderato.
- Server DNS Locale è il primo server DNS a cui un dispositivo si rivolge quando cerca di tradurre un nome di dominio in un indirizzo IP. Se la richiesta non può essere soddisfatta dal server DNS locale, verrà inoltrata al server DNS superiore (Root).
Il server DNS locale è configurato nella rete locale (Internet Service Provider) o sul dispositivo dell'host richiedente ed è responsabile di gestire le richieste DNS localmente.
Non fa parte ufficialmente della gerarchia DNS.
- Root Server sono i server di base nella gerarchia del DNS che contengono informazioni sui server DNS dei domini di primo livello (TLD) e forniscono le fondamenta per la risoluzione dei nomi di dominio su Internet.
I server TLD (Top-Level Domain) sono server specializzati che gestiscono e forniscono informazioni sui domini di primo livello, come .com, .org e .net, nella gerarchia del DNS.
- Authoritative Server i server DNS responsabili di specifici domini di secondo livello.
I server DNS autoritativi come quelli di google.com o facebook.com sono responsabili di memorizzare e gestire gli indirizzi IP associati ai nomi di dominio all'interno del loro dominio specifico, come mail.google.com o maps.google.com.

5)Tipi di Query

Nel sistema DNS, ci sono principalmente due tipi di query che vengono utilizzati per ottenere informazioni sui nomi di dominio e tradurli in indirizzi IP o viceversa.
Query Ricorsiva
In una query ricorsiva, un client DNS, come un computer o un router, fa una richiesta a un server DNS. Quest'ultimo comunica con altri server DNS per cercare l'indirizzo IP e restituirlo al client.
Se il Server DNS Locale non ha l'indirizzo IP, verrà inoltrata la richiesta al Root Server per poi scendere fino ad arrivare all'Authoritative Server appropriato per il dominio cercato.
Questo significa che solo il server DNS interrogherà altri server DNS (in una struttura gerarchica), se necessario, fino a quando non otterrà una risposta definitiva o un errore.
Questo tipo di query è comunemente utilizzato dai client per ottenere informazioni sui nomi di dominio e richiede una risposta completa.
Query Iterativa
In una query iterativa, un server DNS fornisce una risposta basata sulle informazioni disponibili, ma non esegue tutte le operazioni per risolvere completamente la richiesta.
Se il server DNS consultato possiede le informazioni necessarie per risolvere la richiesta, restituirà una risposta diretta. Tuttavia, se non ha le informazioni, fornirà una lista di server DNS o indirizzi IP a cui il client può rivolgersi successivamente per ulteriori dettagli.
Il client DNS è quindi responsabile di contattare i vari server DNS fino a quando non ottiene una risposta completa o raggiunge un server DNS che può risolvere la richiesta.