*Esame 19/01/2021*

1. Come è strutturata la tabella di routing? Che regola deve rispettare? ***(Regola prefisso più lungo)***
   **Ci troviamo a livello di rete. La tabella di routing o di inoltro è un database memorizzato in ciascuna porta di ingresso che elenca le rotte di destinazione, è organizzata secondo una struttura ad albero. L'algoritmo di instradamento determina i valori inseriti in questa tabella. Durante l'instradamento è necessario rispettare la regola a prefisso più lungo. Questa regola è utilizzata per evitare errori di instradamento in quanto il prefisso più corto potrebbe creare una corrispondenza errata.**
2. Qual è una regola presente nella tabella di routing? Come viene scritta la regola di default gateway?
   **Nel caso in cui nello scorrere la tabella non viene trovata alcuna corrispondenza il pacchetto sarà inoltrato all'ultimo indirizzo disponibile, il default gateway 0.0.0.0. Questo invierà il pacchetto in un'altra sottorete che si occuperà del successivo inoltro.**
3. Cos'è il meccanismo di natting e a cosa serve?
   **Quando un dispositivo connesso deve comunicare verso l'esterno è necessario "nattare" la comunicazione. Il router abilitato al NAT nasconde i dettagli della rete domestica al mondo esterno. Con questo meccanismo non è necessario allocare un intervallo di indirizzi da un Internet Service Provider perché un unico indirizzo IP è sufficiente per tutte le macchine di una rete locale. Quando un router NAT riceve il datagramma genera un nuovo numero di porta d'origine con il proprio indirizzo IP e sostituisce il numero di porta originale iniziale con il nuovo numero.**
   **Il meccanismo avviene in 4 fasi: l'host invia il datagramma, il router NAT cambia l'indirizzo di origine del datagramma e aggiorna la tabella, la risposta arriva all'indirizzo di destinazione e infine il router NAT cambia l'indirizzo di destinazione del datagramma all'inverso.**
   **Il protocollo NAT può supportare più di 60.000 (16 bit) connessioni simultanee con un suo IP sul lato WAN. Il NAT viola l'argomento punto-punto perchè non permette agli host di comunicare direttamente.**
4. Come si capisce che nell'IPv4 sono 4 miliardi di indirizzi? **($2^{32} = 2^{10} * 2^{10} * 2^{10} * 2^2 = 1024 * 1024 * 1024 * 4$)**
5. Cosa sono le sottoreti?
   **E' detta sottorete una rete isolata i cui punti terminali sono collegati all'interfaccia di un host o di un router.**
   **L'assegnazione degli indirizzi può avvenire con CIDR (Classless InterDomain Routing) o Classful Addressing. CIDR è la strategia di assegnazione degli indirizzi, la struttura dell'indirizzo IP è divisa in due parti e mantiene la forma decimale puntata a.b.c.d/x dove x indica il numero di bit nella prima parte dell'indirizzo. Prima del CIDR le parti di rete di un indirizzo dovevano essere lunghe 8/16/24 bit e le relative sottoreti venivano dette classe A/B/C. La classe A era composta dalla sottoclasse 8 bit con un massimo di 24 bit computer interni, la classe B dalla sottoclasse di 16 bit e da 16 bit (65.635) computer, e la classe C dalla sottoclasse di 24 bit e 8 bit (256) di computer interni.**
   **La sottorete permette di snellire la tabella di routing ed evitare di inserire i singoli host diminuendo esponenzialmente la dimensione della tabella.**
   **Non è possibile memorizzare tutte le sottoreti, quindi si memorizzano solo alcune regole e si lascia al Default Router il compito di risolvere le rimanenti.**
6. Cos'è il DHCP? ***(Protocollo di assegnazione indirizzo IP in modo automatico)***
   **Il DHCP è il Dynamic Host Configuration Protocol permette a un host di ottenere un indirizzo IP in modo automatico, questo consente di rinnovare la proprietà dell'indirizzo in uso, riutilizzare gli indirizzi e supporta gli utenti mobili che vogliono unirsi alla rete.**
   **Il procedimento avviene in 4 fasi:**
      **l'host invia un messaggio di broadcast "DHCP discover"**
      **il server DHCP risponde con un "DHCP offer"**
      **l'host richiede l'indirizzo IP "DHCP request"**
      **il server DHCP invia l'indirizzo "DHCP ack"**
   a. Come viene effettuata questa richiesta? **(broadcast 255.255.255.255)**
   b. Le offerte dei server hanno un tempo di durata? **(mezz'ora / un'ora / due ore - 3600 secondi)**
7. Cosa sono RTS e CTS? Dove vengono utilizzati? **(livello di datalink)**

**Ci troviamo a livello di data link, RTS (Request To Send) e CTS (Clear To Send).**
**L'idea iniziale è quella di consentire al mittente di "prenotare" il canale in modo da evitare le collisioni anche durante l'invio di lunghi pacchetti di dati.**
**Il mittente inizia a trasmettere un pacchetto RTS all'Access Point usando CSMA, l'AP risponde diffondendo in broadcast il pacchetto CTS in risposta all'RTS.**
**Il pacchetto CTS è ricevuto da tutti i nodi e solo il mittente invierà il pacchetto, le altre stazioni rimanderanno eventuali trasmissioni**

8. Come si chiama il protocollo usato (per l'accesso) in ethernet? ***(CSMA/CSMA-CD, aloha, aloha slotted)***
   **I principali protocolli di accesso sono divisi in 3 categorie principali:**
   - **suddivisione del canale**
     - **TDM (tempo)**
     - **FDM (frequenza)**
   - **suddivisione casuale**
     - **ALOHA**
     - **SLOTTED ALOHA**
     - **CSMA**
     - **CSMA/CD**
   - **a rotazione**
     - **Bluetooth**
     - **Token Ring**
9. Come si chiama il protocollo usato nelle reti wireless? ***(CSMA-CA)***
   **Il protocollo utilizzato nelle reti wireless è il CSMA-CA. Questo protocollo evita di trasmettere mentre decrementa il contatore.**
   **Il mittente se percepisce il canale inattivo trasmette l'intero pacchetto, se percepisce il canale occupato sceglie un valore di ritardo casuale, decrementa questo valore quando il canale sarà percepito come inattivo, quanto il contatore arriva a zero trasmette l'intero pacchetto e se non riceve ACK scegli un nuovo valore di ritardo casuale superiore a quello scelto in precedenza.**
   **Il destinatario invia un ACK alla ricezione del pacchetto.**
10. Come funziona il livello di trasporto? Come funziona e quali sono i meccanismi di base offerti da questo livello, a cosa servono? **(multiplexing, demultiplexing, UDT, TCP)**
    **Il livello di trasporto si occupa di interfacciare trasporto e applicazioni. Questo avviene attraverso una "socket", è un'interfaccia di programmazione ma anche l'insieme di porte e indirizzi IP necessari al trasporto per gestire le connessioni.**
    **Lo stato di trasporto si occupa di fornire un servizio di trasferimento dati dal nodo sorgente al nodo destinazione, generalmente viene richiesto che il trasporto sia affidabile ed efficiente.**
    **Internet offre due tipi di trasporto:**
    - **TCP, affidabile, orientato alla connessione e dotato di controllo di congestione e di flusso**
    - **UDP, non affidabile e senza connessione**
      - **essendo senza connessione il ritardo sarà minimo, i pacchetti sono inviati costantemente alla massima velocità non essendo presente alcun controllo di flusso o di congestione.**

    **Il livello di trasporto si occupa anche del multiplexing e demultiplexing: il mittente (multiplexing) raccoglierà da tutte le socket con l'aggiunta dell'header e invierà i dati tramite lo strato di rete, il destinatario smisterà i pacchetti alla socket corretta.**
    **Ogni strato dello stack riceve e invia dati agli strati adiacenti. Il pacchetto che a livello di applicazione conterrà solo il messaggio, scendendo nello stack protocollare ogni livello aggiungerà un header che avrà senso solo per lo strato adiacente del destinatario. Questo avviene per tutti i livelli dello stack e l'header prenderà un nome diverso a seconda del livello in cui ci troviamo (a livello di trasporto sarà segmento, a livello di rete datagramma e a livello di data link frame).**
    **La socket TCP è identificata da quattro valori:**
    - **indirizzo IP mittente**
    - **porta mittente**
    - **indirizzo IP destinatario**

**porta destinatario**

**il nodo ricevente usa questi valori per smistare il segmento nella socket corretta.**

11. Quali sono i meccanismi che vengono utilizzati per controllare la trasmissione? Cos'è il controllo di flusso e il controllo di congestione? Dove avvengono e come funzionano

    **Nel corso degli anni sono state effettuate alcune modifiche al TCP, queste modifiche si sono concentrate sul controllo di flusso e di congestione.**

    **Il controllo di flusso garantisce un equilibrio fra la velocità di spedizione del trasmittente e quella di svuotamento del buffer dell'applicazione del ricevente. Lo spazio libero sarà dato da RcvWindow=RcvBuffer - [LastByteRcvd - LastByteRead]**

    **LastByteRcvd - LastByteRead deve essere minore o uguale del RcvBuffer e l'host B comunica ad A quanto spazio ha a disposizione nel proprio buffer.**

    **LastByteSent-LastByteAcked deve essere minore o uguale alla RcvWindow in modo da garantire che l'host A non mandi in overflow il buffer dell'host B.**

    **Per quanto riguarda il controllo di congestione esistono due approcci diversi: il controllo end-end utilizzato nel TCP dove non viene rilevata alcuna informazione dalla rete e la congestione è riconosciuta attraverso la perdita di segmenti e l'aumento del ritardo, o a livello di rete dove i router forniscono informazioni ai sistemi finali e vengono utilizzati uno o più bit per indicare la congestione.**

    **In questo caso occorre regolare l'invio anche per non congestionare la rete e in particolare i buffer dei router. La velocità di invio sarà minore tra quella consentita dall'applicazione e quella consentita dalla rete. Per trovare il rate corretto si procede per tentativi partendo dal basso.**

    a. Cos'è il meccanismo di slow start?

       **Il meccanismo di slow start è usato nel controllo di congestione. Consiste nel far crescere esponenzialmente la CWND (congestion window) all'inizio della connessione fino al primo evento di perdita del segmento, a ogni RTT (Round Trip Time) la CWND raddoppia, in pratica aumenta di 1 MSS per ogni ACK ricevuto. Parte molto lentamente ma la crescita è rapida.**

       **Gli eventi che segnalano la congestione sono timeout e ACK duplicati. TCP diminuisce CWND in caso di questi eventi dividendola a metà o riducendola a 1MSS ripartendo dallo slow start.**

       **Il TCP Tahoe introduce alcune tecniche per un funzionamento migliore:**

       - **slow start per controllare la congestione**
       - **una soglia oltre la quale la crescita avviene linearmente (additive increase), questa soglia viene dimezzata a ogni evento di perdita (multiplicative decrease).**
       - **fast retransmission per mantenere la velocità di trasmissione anche in caso di 3 ack duplicati che se arrivano prima dello scadere del timeout vengono ritrasmessi subito.**

       **I 3 ACK duplicati indicano una rete solo parzialmente congestionata, il timeout indica una congestione grave.**

       **Il TCP Reno introduce fast recovery per un recupero più veloce dopo una congestione: in caso di ACK duplicati non si riparte dallo slow start ma dalla fase di congestion avoidance. La soglia diviene la metà del minore tra la CWND e la Receive Window Size remota, il segmento mancante viene ritrasmesso, la CWND diviene uguale alla soglia + 3 segmenti, in caso di altri duplicati si ritrasmette immediatamente e si aumenta la CWND di un segmento, al primo ACK di dati nuovi si pone la CWND = ssthresh (soglia) e si continua in congestion avoidance.**

       **Il TCP New Reno introduce l'header prediction per migliorare la trasmissione in caso di funzionamento normale. Migliora fast retransmit/recovery in presenza di acknowledgement parziali.**

12. Qual'è l'efficienza dei protocolli aloha?

    **Nel caso dello slotted aloha l'efficienza nel caso migliore è il 37% degli slot compie un lavoro utile, nell'aloha puro è del 18%.**

13. Cos'è e come funziona il protocollo HTTP?

    **L'HyperText Transfer Protocol è un protocollo del livello applicativo generico, senza stato, orientato agli oggetti, utilizzato come name servers.**

**Il client inizia una connessione con TCP verso il server alla porta 80, il server accetta la connessione. Attraverso questo protocollo il client invia i comandi in chiaro. Non viene mantenuto lo stato delle richieste precedenti.**
**Le connessioni HTTP posso essere non persistenti quando viene trasferito un solo oggetto per ogni connessione TCP o persistenti quando più di un oggetto può essere inviato all'interno della stessa connessione.**
**Nell'HTTP non persistente il client inizia la connessione TCP al server HTTP sulla porta 80, il server HTTP nel nodo la accetta rispondendo al client, il client manda un messaggio di richiesta contenente l'URL, il server HTTP riceve la richiesta la richiesta, forma il messaggio di risposta e lo invia. Il server chiude la connessione e il client riceve il messaggio di risposta contenente l'HTML. Questo viene ripetuto per ogni richiesta. Queste connessioni presentano alcuni difetti, per ciascun oggetto deve essere stabilita e mantenuta una nuova connessione e ciascun oggetto subisce due RTT, uno per stabilire la connessione e l'altro per richiedere e ricevere l'oggetto.**
**L'HTTP persistente risolve questi problemi. Il server lascia aperta la connessione TCP dopo aver spedito la risposta, le richieste successive fra gli stessi client e server possono essere inviate sulla stessa connessione.**

14. Quali sono gli algoritmi di routing?

***Gli algoritmi di instradamento o routing sono divisi a seconda che siano intradominio o interdominio. Tra gli algoritmi intradominio troviamo il vettore delle distanze (RIP - Routing Information Protocol) e stato dei collegamenti (OSPF - Open Shortest Path First). Tra gli algoritmi interdominio troviamo il vettore dei cammini (BGP - Border Gateway Protocol).***
***Gli algoritmi di instradamento vengono classificati in:***
***globale (link state algorithm - LS che riceve in ingresso tutti i collegamenti tra i nodi e i loro costi)***
***decentralizzato (distance vector algorithm - DV in cui ogni nodo elabora un vettore di stima dei costi verso tutti gli altri nodi della rete e il cammino a costo minimo deve essere calcolato in modo distribuito e iterativo)***
***singolo in cui è supportato solo un percorso per la stessa destinazione***
***multiplo in cui sono supportati più percorsi per la stessa destinazione***
***statico i cui i cammini cambiano raramente***
***dinamico in cui gli instradamenti sono determinati dal volume di traffico e dalle topologia della rete***
***RIP, OSPF e BGP sono insensibili al carico.***

a. protocolli intradominio e interdominio

**I protocolli intradominio sono RIP e OSPF.**
**RIP è un protocollo a vettore distanza, il costo viene calcolato in base agli hop (max 15) e il costo finale è dato dal numero di sottoreti attraversate, inclusa quella di destinazione. In questo protocollo i router adiacenti si scambiano aggiornamenti di instradamento ogni 30 secondi utilizzando un annuncio RIP e in caso non venga aggiornata entro 3 minuti la distanza viene fissata a infinito e l'entry verrà rimossa dalle tabelle.**
**I processi RIP possono anche ricevere messaggi di richiesta. Queste richieste vengono normalmente inviate allo scopo di ottenere dai suoi vicini il valore iniziale delle tabelle di routing.**
**Un processo chiamato routed esegue RIP, ossia mantiene le informazioni di instradamento e scambia messaggi con i processi routed nei router vicini e, poiché RIP viene implementato come un processo a livello di applicazione può inviare e ricevere messaggi su una socket standard e utilizzare un protocollo di trasporto standard.**
**OSPF è un protocollo a stato di collegamento: utilizza il flooding di informazioni di stato del collegamento e l'algoritmo di Dijkstra per la determinazione del percorso a costo minimo. Ogni volta che si verifica un cambiamento nello stato di un collegamento il router manda informazioni di instradamento a tutti gli altri router utilizzando il flooding.**
**Questo protocollo offre diversi vantaggi non presenti in RIP: una maggiore sicurezza in quanto gli scambi tra router sono autenticati, quando più percorsi hanno lo stesso costo**

**OSPF consente di usarli senza sceglierne uno, è presente un supporto per l'instradamento unicast e multicast.**
**OSPF è strutturato gerarchicamente secondo due livelli: area locale e dorsale. I router di confine appartengono sia a un'area generica sia dorsale, i router di dorsale si occupano di instradare all'interno della dorsale ma non sono router di confine e i router di confine scambiano informazioni con i router di altri sistemi autonomi.**

15. Sono un amministratore di rete, devo gestire una sottorete, a livello di un dominio ho a disposizione sia OSPF che RIP, li posso utilizzare indistintamente, contemporaneamente, l'uno o l'altro? Posso configurare alcuni router alcuni utilizzando RIP altri OSPF? **(no, o uno o l'altro, hanno funzionamenti diversi)**
16. Differenza tra TCP e UDP? Quando si usa l'uno e quando si usa l'altro? **(livello di trasporto)**
    **Ci troviamo a livello di trasporto. Il TCP è un protocollo orientato alla connessione e affidabile dotato di controllo di flusso e di congestione, UDP è un protocollo senza connessione e non affidabile.**
    **TCP (Transmission Control Protocol) è un servizio affidabile, orientato alla connessione, end to end che trasporta uno stream di byte ed è in grado di riordinare i dati nei segmenti ricevuti ed eliminarne i duplicati. TCP effettua una trasmissione che è sempre full duplex, ovvero il flusso dati è bidirezionale sulla stessa connessione. I dati sono spezzati in segmenti che hanno come MSS (Maximum Segment Size) un valore deciso all'inizio della connessione. Lo scambio di informazioni è basato su ACK, spediti in leggero ritardo in modo da poter essere cumulativi ed evitare che il buffer ricevente si esaurisca.**
    **L'UDP (Unreliable Data Protocol) definisce un trasporto semplice in cui ogni operazione di invio da parte dell'applicazione produce esattamente un datagramma. La consegna non è garantita e quindi neanche gli altri parametri di qualità. Il ritardo è minimo e, non essendo dotato di controlli, i pacchetti possono essere inviati costantemente alla stessa velocità. UDP viene utilizzato in applicazioni in cui è necessario avere una velocità quasi istantanea, è necessario mantenere una frequenza di emissione dei segmenti a una velocità costante preferendo avere perdite. UDP non è un protocollo fair.**
    a. All'apertura di una socket TCP quanti parametri servono? **(4)** E nell'UDP? **(2)**
    **Per l'apertura di una socket TCP sono necessari 4 parametri:**
    - **indirizzo IP mittente**
    - **porta mittente**
    - **indirizzo IP destinatario**
    - **porta destinatario**

    **Mentre nell'UDP sono necessari solo 2:**
    - **IP**
    - **porta di destinazione**

17. Dove si usa lo slow start e perchè?
    **Lo slow start si usa nel controllo di congestione**
18. Cos'è l'handshake a 3 vie?
    **L'handshake a 3 vie viene utilizzato per l'apertura di una connessione TCP in cui nella prima fase un nodo manda un segmento contenente il flag SYN, un proprio numero di sequenza iniziale e le opzioni per MSS e timestamp. In questa prima fase non è presente alcun dato.**
    **Nella seconda fase il ricevente risponde al SYN con un segmento SYN e ACK pari al numero di SEQ del segmento SYN ricevuto +1, viene creato lo stato nel nodo, il ricevente sceglie il proprio numero di sequenza iniziale e invia la sua scelta di opzioni.**
    **Nella terza e ultima fase il primo nodo risponde con segmento con solo flag ACK ed eventuali primi dati.**
19. A cosa serve la maschera di sottorete? E come avviene il suo uso all'interno delle tabelle di routing?
    **La maschera di sottorete è un parametro di configurazione che definisce la dimensione della sottorete a cui appartiene un host al fine di ridurre il traffico di rete e facilitare la ricerca e il raggiungimento di un determinato host con relativo indirizzo IP.**
    **All'interno delle tabelle di routing, con l'indirizzamento CIDR (Classless Interdomain Routing), deve essere contenuta una colonna con la dimensione della maschera.**

**Il router utilizza la prima riga della tabella per fare l'end bit a bit con l'indirizzo di destinazione e viene confrontato con l'indirizzo di rete della prima riga, se non c'è corrispondenza continua fino ad arrivare al default router con indirizzo 0.0.0.0.**

20. Cos'è il protocollo ARP?

    **ARP è il protocollo per la risoluzione di indirizzi. Ogni nodo IP (host, router) nella LAN ha una tabella ARP. Questa tabella contiene la corrispondenza tra indirizzi IP e MAC.**
    **Poniamo per esempio che A voglia inviare un datagramma a B e l'indirizzo MAC di B non è nella tabella ARP di A. A trasmetterà in un pacchetto broadcast il messaggio di richiesta ARP contenente l'IP di B e tutte le macchine della LAN riceveranno questa richiesta.**
    **B riceve il pacchetto ARP e risponde ad A comunicando il proprio MAC address.**
    **Il messaggio di richiesta ARP è inviato in un pacchetto broadcast mentre il messaggio di risposta ARP è inviato in un pacchetto standard.**
    **ARP è "plug-and-play": la tabella ARP di un nodo si costituisce automaticamente e non deve essere configurata dall'amministratore di sistema.**

    a. una volta utilizzato questo protocollo, l'informazione che è stata risolta dove viene conservata?
       **L'informazione viene conservata all'interno del nodo che ha richiesto**

*Esame 21/01/2021*

1. Come si chiama la notazione degli indirizzi IP?
   **Notazione decimale puntata**
2. Cos'è la maschera di sottorete?
   **La maschera di sottorete, nell'ambito di una rete TCP/IP, è un parametro di configurazione che definisce la dimensione (intesa come intervallo di indirizzi) della sottorete IP a cui appartiene un host, al fine di ridurre il traffico di rete e facilitare la ricerca e il raggiungimento di un determinato host con relativo indirizzo IP.**
   a. E come è organizzata?
      **E' organizzata attraverso CIDR (Classless Interdomain Routing), una strategia di assegnazione degli indirizzi. La struttura dell'indirizzo è diviso in 2 parti e mantiene la forma decimale puntata a.b.c.d/x dove x è il numero di bit nella prima parte dell'indirizzo.**
   b. Come viene utilizzata all'interno dei router la maschera di sottorete?
      **Con l'indirizzamento CIDR nella tabella di routing deve essere contenuta anche una colonna con la dimensione della maschera. Questo è necessario per la corrispondenza con la maschera più lunga.**
   c. Come sfrutta questa informazione il router? **(come instrada? tramite algoritmo di instradamento)**
      **Il router instrada attraverso algoritmi di instradamento che identificano percorsi ottimali attraverso i router della rete.**
      **Un protocollo di routing è un insieme di regole e procedure che permette ai router di una rete di scambiarsi informazioni sui cambiamenti e condividere informazioni sui loro vicini.**
      **L'obiettivo è quello di ottimizzare il percorso in modo che il costo dato dalla somma dei costi dei passaggi attraverso le singole reti sia il più basso possibile.**
      **Il RIP (Routing Information Protocol) assume un costo unitario uguale per tutte le reti.**
      **L'OSPF (Open Shortest Path First) permette all'amministratore della rete di assegnare un costo in funzione del tipo di servizio richiesto.**
      **Il BGP (Border Gateway Protocol) utilizza criteri di tipo amministrativo, un ISP (Internet Service Provider) decide di non voler instradare pacchetti attraverso un ISP concorrente.**
   d. Come capisce il router dove instradare il pacchetto? Come usa la tabella? Che operazione fa?
      **Prende l'indirizzo di destinazione, parte dal primo indirizzo nella tabella di routing e fa l'and bit a bit con ciò che c'è scritto, se ciò che trova è la stessa sottorete capisce che ha trovato dove deve andare, scorre la tabella di routing e trova la porta di uscita. Se non c'è matching passa alla successiva, se non dovesse trovarla in tutta la tabella instraderà verso il default router.**
   e. Come fa a capire che deve andare verso il default router?
      **Non trova alcuna corrispondenza nella sottorete e cerca esternamente.**
   f. Quando si ferma? Cos'è che gli fa capire di andare verso il default router?
      **Si ferma dopo aver controllato tutti gli indirizzi nella tabella e l'unico modo per instradare è quello del default router.**
   g. C'è una riga precisa inserita nella tabella di routing per fare questo, quale?
      **Si, alla fine della tabella c'è una riga dedicata al default router 0.0.0.0, è fatta così perchè facendo l'and bit a bit viene certamente soddisfatta. Deve essere sempre presente nella tabella di routing.**
3. Quanti sono i bit che abbiamo a disposizione per fare un indirizzo IP?
   **Abbiamo a disposizione 32 bit che ci forniscono circa 4 miliardi di indirizzi con l'IPv4, con l'IPv6 abbiamo 128 bit suddiviso in 8 gruppi di 4 cifre esadecimali divisi da 2 punti (3ffe:0000:0000:2f3b:02aa:00ff:fe28:0001)**
4. Come si calcola questo 4 miliardi?
   **$2^{32} = 2^{10} * 2^{10} * 2^{10} * 2^{2} = 1024 * 1024 * 1024 * 4$**
5. TCP e UDP, a che livello siamo? cosa sono? a cosa servono?
   **TCP e UDP sono protocolli presenti a livello di Trasporto. Il Transmission Control Protocol (TCP) è un protocollo che si occupa di controllo della trasmissione ovvero rendere affidabile la comunicazione dati in rete tra mittente e destinatario.**
   **TCP è un protocollo orientato alla connessione, ovvero prima di poter trasmettere dati deve stabilire la comunicazione, negoziando una connessione tra mittente e destinatario, che rimane attiva anche in assenza di scambio di dati e viene esplicitamente chiusa quando non più**

**necessaria. Esso quindi possiede le funzionalità per creare, mantenere e chiudere una connessione.**
**TCP è un protocollo affidabile: garantisce la consegna dei segmenti a destinazione attraverso il meccanismo degli acknowledgements.**
**Il servizio offerto da TCP è il trasporto di un flusso di byte bidirezionale tra due applicazioni in esecuzione su host differenti. Il protocollo permette alle due applicazioni di trasmettere contemporaneamente nelle due direzioni, quindi il servizio può essere considerato "Full-duplex" anche se non tutti i protocolli applicativi basati su TCP utilizzano questa possibilità.**
**Il flusso di byte prodotto dall'applicazione (o applicativo, o protocollo applicativo) sull'host mittente, viene preso in carico da TCP per la trasmissione, viene quindi frazionato in blocchi, detti segmenti, e consegnato al TCP sull'host destinatario che lo passerà all'applicativo indicato dal numero di porta del destinatario nell'header del segmento (es.: applicativo HTTP, porta 80).**
**TCP garantisce che i dati trasmessi, se giungono a destinazione, lo facciano in ordine e una volta sola ("at most once"). Più formalmente, il protocollo fornisce ai livelli superiori un servizio equivalente ad una connessione fisica diretta che trasporta un flusso di byte. Questo è realizzato attraverso vari meccanismi di acknowledgment e di ritrasmissione su timeout.**
**TCP offre funzionalità di controllo di errore sui pacchetti pervenuti grazie al campo checksum contenuto nella sua PDU.**
**TCP possiede funzionalità di controllo di flusso tra terminali in comunicazione e controllo della congestione sulla connessione, attraverso il meccanismo della finestra scorrevole. Questo permette di ottimizzare l'utilizzo dei buffer di ricezione/invio sui due end devices (controllo di flusso) e di diminuire il numero di segmenti inviati in caso di congestione della rete.**
**TCP fornisce un servizio di multiplazione delle connessioni su un host, attraverso il meccanismo dei numeri di porta del mittente.**
**Lo User Datagram Protocol (UDP), è un protocollo di tipo connectionless, inoltre non gestisce il riordinamento dei pacchetti né la ritrasmissione di quelli persi, ed è perciò generalmente considerato di minore affidabilità.**
**L'UDP fornisce soltanto i servizi basilari del livello di trasporto, ovvero:**
- **multiplazione delle connessioni, ottenuta attraverso il meccanismo di assegnazione delle porte;**
- **verifica degli errori (integrità dei dati) mediante una checksum, inserita in un campo dell'intestazione (header) del pacchetto, mentre TCP garantisce anche il trasferimento affidabile dei dati, il controllo di flusso e il controllo della congestione.**

a. Quando si deve aprire la connessione qual è il meccanismo che viene usato?
**L'apertura di una connessione TCP è detta Three Way Handshake, un nodo manda un segmento contenente SYN e numero di sequenza, il ricevente replica al SYN con SYN e ACK, viene creato lo stato del nodo e il ricevente sceglie il proprio numero di sequenza iniziale e invia la sua scelta di opzioni, il nodo risponde con ACK e dati iniziali.**

b. Socket UDP e TCP?
**Una socket è analoga a una porta, un processo che vuole inviare un messaggio lo fa uscire dalla propria "porta" (socket). Il processo stesso presuppone l'esistenza di un'infrastruttura esterna che trasporterà il messaggio attraverso la rete fino alla "porta" del processo di destinazione.**
**La socket UDP è identificata da IP e porta di destinazione. La socket TCP da indirizzo IP mittente, porta mittente, indirizzo IP destinatario e porta destinatario.**

c. Che cos'è il meccanismo di slow start e dove viene utilizzato?
**Il meccanismo di slow start viene utilizzato nel controllo di congestione. Consiste nel far crescere esponenzialmente la congestion window all'inizio della connessione fino al primo evento di perdita di segmento: la congestion window raddoppia a ogni RTT, la congestion windows aumenta di 1MSS per ogni ACK ricevuto.**

i. Quali sono gli elementi che interrompono la crescita lineare?
**ACK duplicati e il timeout.**

6. Cos'è il DHCP?
**Il DHCP (Dynamic Host Configuration Protocol) permette a un host di ottenere un indirizzo IP in modo automatico consentendo il riuso degli indirizzi e il supporto agli utenti mobili che si vogliono unire alla rete.**

a. Come evolve il protocollo?
   **Il protocollo evolve in 4 fasi: il client invia un pacchetto con indirizzo IP sorgente 0.0.0.0, non ha un indirizzo IP e utilizza questo speciale per identificarsi, e come indirizzo di destinazione il broadcast 255.255.255 ed emetterà un transaction ID. Il server prepara la risposta**
b. Per quanto tempo è valida l'assegnazione dell'IP?
   **Generalmente mezz'ora/un'ora.**

7. Cos'è il Natting? **(classificazione reti pubbliche e privato)**
   a. Esempio di indirizzo di tipo privato? **(la classica 192.168.0.0 fino a 192.168.255.254/16, abbiamo anche /12 e /8)**
   b. Cosa fa il NAT?
   **Il router abilitato al NAT nasconde i dettagli della rete domestica al mondo esterno. Consente l'utilizzo di un unico indirizzo IP per tutte le macchine di una rete locale. Consente di cmbiare gli indirizzi delle macchine di una rete privata senza doverlo comunicare all'internet globale, è possibile cambiare ISP senza modificare gli indirizzi delle macchine della rete privata.**
   c. Che principio di base utilizza?
   **Quando un router NAT riceve un datagramma, genera per esso un nuovo numero di porta di origine, sostituisce l'indirizzo IP di origine con il proprio indirizzo IP sul lato WAN e sostituisce il numero di porta origine iniziale con il nuovo numero.**
   **Il protocollo NAT può supportare più di 60.000 connessioni simultanee con un solo IP sul lato WAN (campo numero di porta è lungo 16 bit)**
8. Cos'è il protocollo ARP? **(associa a un indirizzo IP al relativo indirizzo MAC)**
   **Il protocollo ARP è il protocollo per la risoluzione degli indirizzi. Ogni nodo IP nella LAN ha una tabella ARP, questa tabella contiene la corrispondenza tra indirizzi IP e indirizzi MAC.**
   a. Come viene utilizzato?
   **Il protocollo, nella caso della stessa sottorete:**
   **A vuole inviare un datagramma a B ma l'indirizzo MAC di B non è nella tabella ARP di A.**
   **A trasmette in un pacchetto broadcast il messaggio di richiesta ARP contenente l'indirizzo IP di B (tutte le macchine della LAN riceveranno una richiesta di ARP)**
   **B riceve il pacchetto ARP e risponde ad A comunicando il proprio indirizzo MAC.**
   **Il messaggio di richiesta viene inviato in broadcast a tutte le macchine della LAN ma il pacchetto di risposta viene inviato in un pacchetto standard.**
   b. Come funziona?
9. Cosa sono request to send RTS e clear to send CTS?
   **RTS (request to send) e CTS (clear to send) sono i pacchetti di prenotazioni utilizzati nel CSMA/CA.**
   **Questi pacchetti vengono utilizzati per evitare le collissioni consentendo al mittente di "prenotare" il canale.**
   **Il mittente comincia a trasmettere un piccolo pacchetto RTS all'AP utilizzando CSMA, potrebbero anche in questo caso verificarsi delle collisioni ma sono di pacchetti molto piccoli.**
   **AP risponde diffondendo in broadcast il pacchetto CTS in risposta all'RTS ricevuto.**
   **Il pacchetto CTS è ricevuto da tutti i nodi.**
   a. Cosa stiamo cercando di fare? **(risolvere il problema del terminale nascosto)**
   **Attraverso questi pacchetti cerchiamo di risolvere il problema del terminale nascosto:**
   **A e B possono comunicare, B e C possono comunicare, A e C non possono comunicare ma possono causare interferenza presso la destinazione B.**
10. Cos'è il controllo di flusso e di congestione?
    **Il controllo di flusso garantisce che vi sia un equilibrio fra la velocità di spedizione del trasmittente e quella di svuotamento del buffer da parte dell'applicazione del ricevente. Questo controllo permette di mantenere al mittente una variabile chiamata finestra di ricezione che fornisce al mittente un'indicazione sullo spazio libero disponibile nel buffer del destinatario.**
    **Il controllo di congestione permette, attraverso la perdita di pacchetti, di far scattare dei meccanismi per diminuire la velocità di trasmissione prima dell'esaurimento dei buffer. Vi sono due approcci differenti al controllo di congestione: il controllo end to end, utilizzato nel TCP, in cui non viene rilevata alcuna informazione della rete.**
11. Come avviene la chiusura di una connessione TCP? **(four way handshake)**

**La chiusura avviene attraverso la four way handshake, in cui il primo nodo invia un segmento con FIN e riceve un segmento con l'ACK del FIN. Il secondo nodo invia un segmento con FIN e riceve un ACK. Solo dopo chiude la connessione.**

12. Come avviene l'apertura di una connessione TCP? **(three way handshake)**

    **L'apertura della connessione avviene attraverso la three way handshake in cui un nodo manda un segmento contenente:**
    **– il flag SYN (apertura attiva)**
    **– un proprio numero di sequenza iniziale**
    **– nessun dato**
    **– opzioni per MSS, Window scale, timestamp**
    **Il ricevente replica sl SYN con un segmento con SYN e ACK (pari al numero di SEQ del segmento SYN ricevuto + 1):**
    **– viene creato lo stato nel nodo, es.: allocazione strutture dati (apertura passiva)**
    **– il ricevente sceglie il proprio numero di sequenza iniziale**
    **– invia la sua scelta di opzioni**
    **Il primo nodo risponde con segmento con solo flag ACK (sempre pari a SEQ precedente + 1) ed eventuali primi dati**

    a. Come vengono utilizzati i bit FIN, SYN? Con che criteri?

       **I bit FIN e SYN sono dei FLAGS contenuti nell'header. Sono singoli bit con valore on pari a 1 e off pari a 0 e forniscono informazioni di validità di altri campi dell'header o segnalano eventi.**
       **SYN è la richiesta di sincronizzazione dei numeri di sequenza per iniziare una connessione, FIN è la richiesta di chiusura della connessione ma esistono anche altri flags come URG che indica la presenza di dati urgenti, PSH che dice al ricevente che deva passare l'informazione allo stato superiore il prima possibile.**

13. Cos'è il protocollo RARP? **(reverse address resolution protocol, l'opposto dell'arp)**

    **Il RARP è il protocollo inverso dell'ARP ed è usato per risalire all'indirizzo IP conoscendo l'indirizzo fisico.**

14. Cos'è il protocollo aloha?

    **Il protocollo aloha è un protocollo ad accesso casuale. Esistono due tipi di protocollo aloha, lo slotted aloha e aloha puro.**
    **Lo slotted aloha il tempo è suddiviso in slot e ogni slot equivale al tempo di trasmissione di un pacchetto. I nodi iniziano la trasmissione dei pacchetti solo all'inizio degli slot, i nodi sono sincronizzati, se in uno slot due o più pacchetti collidono i nodi coinvolti rilevano l'evento prima del termine dello slot.**
    **Quando a un nodo arriva un nuovo pacchetto da spedire il nodo attende fino all'inizio dello slot successivo. Se non si verifica una collisione il nodo può trasmettere un nuovo pacchetto nello slot successivo, se si verifica una collisione il nodo la rileva prima della fine dello slot e ristrasmette con probabilità p il suo pacchetto durante gli slot successivi.**
    **I vantaggi di questo protocollo è che consente a un singolo nodo di trasmettere continuamente alla massima velocità, è decentralizzato quindi ciascun nodo decide indipendentemente quando ritrasmettere ed è semplice. Tra gli svantaggi abbiamo che una certa frazione di slot presenterà collisioni e di conseguenza verranno sprecati slot e un'altra frazione rimane inattiva.**
    **Per quanto riguarda aloha puro è molto più semplice: quando arriva il primo pacchetto lo trasmette immediatamente e integralmente nel canale broadcast. Questo metodo presenta elevate probabilità di collisione.**

    a. Perché è stato inventato? Cosa si cercava di risolvere?

       **Il protocollo ad accesso casuale definisce come rilevare un'eventuale collisione e come ristrasmettere ad avvenuta collisione.**

    b. A che livello siamo? **(di data link)**
    c. Qual è l'efficienza?

       **L'efficienza per lo slotted aloha è del 37%, dell'aloha puro il 18%.**

15. Come vengono catalogati gli algoritmi di routing/instradamento?

    **Gli algoritmi di routing vengono catalogati in intradominio e interdominio.**
    **Tra gli algoritmi intradominio troviamo il vettore delle distanze (RIP - routing information protocol - che assume un costo unitario uguale per tutte le reti) e stato dei collegamenti (OSPF - open**

**shortest path first - che permette all'amministratore della rete di assegnare un costo in funzione del tipo di servizio richiesto, mentre tra quelli interdominio troviamo il vettore dei cammini (BGP - border gateway protocol - che utilizza criteri di tipo amministrativo, per esempio un ISP decide di non voler instradare i propri pacchetti attraverso un ISP concorrente.)**

**Gli algoritmi sono inoltre classificati in:**

**globale o decentralizzato:**
- **globale (link state algorithm):**
  **l'algoritmo riceve in ingresso tutti i collegamenti tra i nodi e i loro costi**
- **decentralizzato (distance-vector algorithm):**
  **ogni nodo elabora un vettore di stima dei costi (distanze) verso tutti gli altri nodi nella rete, il cammino a costo minimo viene calcolato in modo distribuito e iterativo.**

**statico o dinamico:**
- **statico:**
  **i cammini cambiano raramente**
- **dinamico:**
  **gli instradamenti sono determinati al variare di volume di traffico e topologia della rete**

**percorso singolo o multiplo:**
- **singolo:**
  **è supportato solo un percorso per una stessa destinazione**
- **multiplo**
  **sono supportati più percorsi**

**metrica:**
- **hops:**
  **link attraversati durante il cammino**
- **costo:**
  **somma dei costi di tutte le linee attraversate**

a. Dove vengono utilizzati? Che problema di instradamento risolvono? **(intradominio e interdominio)**

16. Cos'è il CSMA? A cosa serve?

**Il CSMA (carrier sense multiple access) è un protocollo ad accesso casuale, si pone in ascolto prima di trasmettere. Se rileva che il canale è libero trasmette l'intero pacchetto, se il canale sta già trasmettendo il nodo aspetta un altro intervallo di tempo.**
**Questo non significa che non potrebbero avvenire collisioni, il ritardo di propagazione fa si che due nodi non rilevino la reciproca trasmissione e non appena il un nodo rileva una collisione cessa immediatamente di trasmettere.**

a. Quali sono le varianti del CSMA?
   **Le varianti sono CSMA/CD (collision detection) e CSMA/CA (collision avoidance)**
b. Perchè sono stati inventati?

17. Cosa significa multiplexing e demultiplexing? Dove viene utilizzato e perché? **(livello di trasporto)**

**Viene utilizzato nel livello di trasporto. Alla ricezione avviene demultiplexing, i pacchetti vengono smistati alla socket corretta usando l'header del trasporto. Nel mittente avviene il multiplexing che consiste nella raccolta da tutte le socket con l'aggiunta dell'header inviando i dati tramite lo strato di rete.**

18. Quant'è il numero massimo di porte che posso avere? **(1024 riservate, $2^{16}$ combinazioni 65.536)**
19. Cos'è il DHCP?

**Il DHCP (Dynaic Host Configuration Protocol) permette a un host di ottenere un indirizzo IP in modo dinamico dal server di rete. Questo permette di rinnovare le proprietà dell'indirizzo in uso, il riutilizzo degli indirizzi e supporta anche gli utenti mobili che si vogliono unire alla rete.**
**L'host invia un messaggio broadcast "DHCP discover", il server DHCP risponde con "DHCP offer", l'host richiede l'indirizzo IP "DHCP request", il server DHCP invia l'indirizzo "DHCP ack"**

20. Cos'è la maschera di sottorete?

    **La maschera di sottorete è un parametro di configurazione che definisce la dimensione (l'intervallo di indirizzi) della sottorete IP a cui appartiene un host.**

    a. Perché è così importante? **(perchè raggruppando questi indirizzi sotto il concetto di sottorete quando devo mettere delle entry nelle tabelle di routing mi limito a citare la sottorete senza scrivere singolarmente gli indirizzi)**

21. Cosa si intende per additive increase e multiplicative decrease?

    **Additive Increase del TCP è l'aumento della congestion window di un 1MSS ogni RTT in assenza di perdite. Per Multiplicative Decrease invece è dividere la congestion window a metà in caso di evento che segnali perdita.**

    a. Qual è l'evento che interrompe questo aumento lineare? **(timeout, 3 ack ripetuti da parte del mittente)**
    b. E' più grave il timeout o gli ack ripetuti? **(timeout)**
    c. Cosa succede se scatta il timeout? **(si ricomincia da 1 MSS)**
    d. Cosa succede se scattano i 3 ack? **(si riparte dalla soglia, si entra in congestion avoidance)**

22. Come vengono catalogati e che caratteristiche hanno gli algoritmi di routing?

    **Gli algoritmi sono classificati in:**

    **globale o decentralizzato:**
    **globale (link state algorithm):**
    **l'algoritmo riceve in ingresso tutti i collegamenti tra i nodi e i loro costi**
    **decentralizzato (distance-vector algorithm):**
    **ogni nodo elabora un vettore di stima dei costi (distanze) verso tutti gli altri nodi nella rete, il cammino a costo minimo viene calcolato in modo distribuito e iterativo.**

    **statico o dinamico:**
    **statico:**
    **i cammini cambiano raramente**
    **dinamico:**
    **gli instradamenti sono determinati al variare di volume di traffico e topologia della rete**

    **percorso singolo o multiplo:**
    **singolo:**
    **è supportato solo un percorso per una stessa destinazione**
    **multiplo**
    **sono supportati più percorsi**

    **metrica:**
    **hops:**
    **link attraversati durante il cammino**
    **costo:**
    **somma dei costi di tutte le linee attraversate**

    **L'algoritmo di instradamento a stato del collegamento (LS) è un algoritmo globale in cui ogni nodo costruisce una propria conoscenza dell'intera rete. Ogni nodo ha una conoscenza diretta dello stato dei collegamenti di cui fa parte e mettendo insieme le conoscenze parziali di tutti i nodi è possibile avere una conoscenza globale della rete.**

    1. **le informazioni sullo stato di ogni collegamento da parte di ogni nodo vengono create**
    2. **vengono disseminate tramite pacchetti LSP verso ogni altro nodo (flooding)**
    3. **viene calcolato l'albero dei cammini minimi (algoritmo di dijkstra)**
    4. **e vengono costruite le tabelle di routing**

    **L'algoritmo di instradamento con vettore distanza è basato sullo scambio di informazioni tra nodi direttamente collegati. E' un algoritmo distribuito, ciascun nodo riceve parte dell'informazione da uno dei vicini direttamente connessi, è iterativo, il processo si ripete fino a quando non avviene più lo scambio di informazioni tra i vicini, è asincrono, ogni nodo opera in modo indipendente dagli altri.**

**Confrontando LS e DV:**

**Complessità dei messaggi:**

**LS: con n nodi, E collegamenti, implica l'invio di O(nE) messaggi**

**DV: richiede scambi tra nodi adiacenti**

**Velocità di convergenza:**

**LS: l'algoritmo è $O(n^2)$ è richiede O(nE) messaggi, è possibile che ci siano oscillazioni di velocità**

**DV: può convergere lentamente**

**Robustezza:**

**LS: un router può comunicare via broadcast un costo sbagliato per uno dei suoi collegamenti connessi, i nodi si occupano di calcolare soltanto le proprie tabelle**

**DV: un nodo può comunicare cammini a costo minimo errati a tutte le destinazioni, la tabella di ciascun nodo può essere usata dagli altri, un calcolo errato si può diffondere nell'intera rete**

a. Quali sono i criteri secondo quali funzionano intradomain e interdomain? **(aspetti di prestazione e aspetti amministrative)**

23. Quali sono i protocolli dell'email? **(POP3 e IMAP)**

**I protocolli per l'email sono POP3 e IMAP.**

**POP3 permette il collegamento con TCP alla porta 110 del server che contiene la posta dopo una fase di autenticazione attraverso username e password. Permette di scaricare i messaggi nuovi dal server ed è efficiente solo se si ricevono pochi messaggi e si usa lo stesso dispositivo per leggerli.**

**IMAP utilizza la porta 143, la posta, a differenza di POP3, è raccolta nel server e può essere letta sia online che offline. E' il protocollo usato negli ultimi anni, permette la sincronizzazione su diversi dispositivi.**

*Esame 04/02/2021*

1. Cosa sono e a cosa servono i socket?
   **Una socket è sia un'interfaccia di programmazione (tra applicazione e trasporto) sia un insieme di porte e indirizzi IP necessari al trasporto per gestire le connessioni.**
   **Una socket è analoga a una porta, permette a un processo che vuole inviare un messaggio di farlo uscire attraverso la propria "porta". Il processo presuppone l'esistenza di un'infrastruttura esterna che trasporterà il messaggio attraverso la rete fino alla porta del processo di destinazione.**
2. Cosa sono TCP e UDP?
   **Sono dei protocolli di trasporto. TCP è affidabile, orientato alla connessione con controllo di flusso e di congestione. UDP non è affidabile e senza connessione.**
   a. Cosa significa non orientato alla connessione?
      **Non orientato alla connessione significa che non è necessario che venga stabilita una connessione, che venga creato un "canale ideale" prima dell'invio. Ogni pacchetto contiene nell'header nel quale l'indirizzo di destinazione è sufficiente per permettere la spedizione indipendente del pacchetto.**
   b. Cosa significa orientato alla connessione?
      **Prima di far transitare la voce o i pacchetti viene creato un canale tra le due entità accertandosi il corretto recapito dei dati.**
   c. Quali sono le caratteristiche del TCP? Cosa fa che non fa l'UDP?
      **Il TCP è un protocollo orientato alla connessione. Ha un controllo di flusso e di congestione che l'UDP non implementa per inviare i pacchetti alla massima velocità**
   d. Quali meccanismi prevede il TCP per poter garantire che non venga perso nulla e che tutto venga consegnato? **(controllo di flusso e di congestione)**
   e. Come avvengono il controllo di flusso e di congestione?
      **Il controllo di flusso garantisce un equilibrio tra la velocità di spedizione del trasmittente e quella di svuotamento del buffer da parte del ricevente.**
      **Il controllo di congestione viene rilevata attraverso la pedita di segmenti e l'aumento di ritardo.**
3. A che serve il meccanismo di NAT?
   **Serve a mascherare l'indirizzo IP della rete domestica al mondo esterno.**
4. Cosa sono le sottoreti e perché sono state pensate? Che problema risolviamo?
   **La sottorete è una rete isolata i cui punti terminali sono collegati all'interfaccia di un host o di un router. L'assegnazione degli indirizzi avviene attraverso CIDR (classless interdomain routing) e struttura l'indirizzo IP in due parti. Prima del CIDR il metodo di assegnazione era definito Classfull e le relative sottoreti erano definite A, B, C ma lo spreco di indirizzi era notevole.**
   **Le sottoreti risolvono il poblema delle tabelle di routing. Permettono l'inserimento di una singola sottorete invece che di singoli host.**
   a. Dove vengono sfruttate?
   b. Come si usano?
5. Come fa il router a capire dove indirizzare il pacchetto? Dato l'indirizzo di destinazione cosa fa il router?
   **(prende la prima riga della tabella, vedo la maschera di sottorete, faccio l'end bit a bit con l'indirizzo di destinazione del pacchetto e se c'è trovo la stessa maschera di sottorete e lo inserisco nella porta di uscita, se non trovo corrispondenza alla fine viene inviato nell'ultima riga particolare con tutti 0 e il pacchetto viene inviato al gateway di uscita)**
6. Cos'è e a cosa serve il DNS?
   **Il domain name system è utilizzato per associare un nome a ogni indirizzo IP in modo che l'identificazione di un sito web fosse più semplice.**
   **Oltre al servizio di traduzione il DNS offre servizi di:**
   **host aliasing in cui associa un host name canonico a più sinonimi**
   **mail server aliasing che permette di avere più sinonimi a un indirizzo email canonico**
   **distribuzione locale che associa un host name canonico a più indirizzi IP che permettono di distribuire il traffico su più server web replicati se ben "ruotati".**
   **Il sistema DNS si compone di 3 parti principali:**
   **lo schema gerarchico per la nominazione**
   **database distribuito**
   **protocollo (per il mantenimento e la distribuzione delle informazioni sulle corrispondenza)**

**L'utilizzo di un database centralizzato avrebbe portato a diversi svantaggi. Basti pensare al volume di traffico. Per ovviare a questo problema ogni server è responsabile di una parte del database, e si utilizza la ridondanza e il caching.**
**Il nome si legge da destra a sinistra: nodo.sottodominio.dominio.country.**

7. Quali sono i principi di base e lo schema che va utilizzato per l'accesso al WiFi?
   a. Qual è il protocollo per l'accesso al mezzo?
8. Cos'è il CSMA e quali sono le sue varianti?
   **CSMA è un protocollo ad accesso casuale (carrier sense multiple access) e si pone in ascolto prima di trasmettere. Se rileva che il canale è libero trasmette il pacchetto, se il canale sta già trasmettendo il nodo aspetta un altro intervallo di tempo.**
   **Le sue varianti sono CSMA/CD (collision detection) che rileva la collissione e annulla la trasmissione non appena si rende conto che c'è un'altra in corso. Questa rilevazione è semplice nelle LAN cablate ma complessa nelle LAN wireless. Questa variante è utilizzata in Ethernet.**
   **L'altra variante è CSMA/CA (collision avoidance), utilizzata nelle reti wireless 802.11, la stazione evita di trasmettere mentre decrementa il contatore (valore casuale). Le possibilità che ci sia una collisione sono basse.**
   a. Cos'è lo slow start?
      **E' il meccanismo presente nel TCP che fa crescere esponenzialmente la congestion window all'inizio della connessione fino al primo evento di perdita. A ogni RTT la CWND raddoppia.**
      **L'inizio è lento ma la crescita è rapidissima.**
      **Viene usato per controllare la congestione.**
9. Cos'è ethernet?
   **Ethernet (802.3) è stata la prima LAN ad alta velocità con vasta diffusione, è progettata con topologia a stella dove al centro è collegato uno switch, ciascun nodo esegue un protocollo ethernet separato e non entra in collisione con gli altri.**
   **Utilizza il protocollo CSMA/CD, una stazione inizia a trasmettere appena percepisce che il canale è libero e in presenza di collisione interrompe subito l'invio.**
10. Come viene implementato il tempo di attesa casuale?
11. Cos'è l'RTS e il CTS?
    **RTS (request to send) e CTS (clear to send) sono pacchetti di prenotazione utilizzati nel CSMA/CA. Questi pacchetti consentono al mittente di prenotare il canale in modo da evitare collisioni anche in casi di invii di lunghi pacchetti di dati.**
    **Il mittente inizia a trasmettere un piccolo pacchetto RTS all'AP, l'AP risponde diffondendo in broadcast il pacchetto CTS in risposta all'RTS. Il pacchetto CTS è ricevuto da tutti i nodi, il mittente invierà il pacchetto e le altre stazioni rimanderanno eventuali trasmissioni.**
12. Qual è la sigla del protocollo ethernet?
    **IEEE 802.3**
13. Quali sono i protocolli a livello di datalink?
14. Quali sono i protocolli di accesso al mezzo?
    Il protocollo MAC controlla l'accesso al mezzo. CSMA?? Aloha??
15. Quali sono i protocolli a rotazione?
    **I protocolli MAC a rotazione sfruttano le migliori caratteristiche dei protocolli a suddivisione del canale (condividono il canale equamente ed efficientemente con carichi elevati ma poco efficiente con carichi non elevati) e i protocolli MAC ad accesso casuale (efficienti con carichi non elevati, un singolo nodo può utilizzare interamente il canale ma con carichi elevati le collisioni sono frequenti).**
    **I protocolli a rotazione possono essere:**
    **protocollo polling in cui un nodo principale sonda a turno gli altri, elimina le collisioni, slot vuoti, se il nodo principale si guasta l'intero canale rimane inattivo**
    **protocollo token-passing in cui un messaggio di controllo circola fra i nodi seguendo un ordine prefissato, il messaggio di controllo è detto token, è un sistema decentralizzato e molto efficiente ma il guasto di un nodo potrebbe mettere fuori uso il canale**
16. Apertura e chiusura delle connessione TCP?
    **L'apertura di una connessione TCP avviene attraverso la three way handshake:**
    **1. un nodo manda un segmento contenente**
    **– il flag SYN (apertura attiva)**

**– un proprio numero di sequenza iniziale**
**– nessun dato**
**– opzioni per MSS, Window scale, timestamp**
**2. il ricevente replica al SYN con un segmento con SYN ed ACK (pari al numero di SEQ del segmento SYN ricevuto + 1):**
**– viene creato lo stato nel nodo, es.: allocazione strutture dati (apertura passiva)**
**– il ricevente sceglie il proprio numero di sequenza iniziale**
**– invia la sua scelta di opzioni**
**3. Il primo nodo risponde con segmento con solo flag ACK (sempre pari a SEQ precedente + 1) ed eventuali primi dati**
**La chiusura avviene con la stretta di mano a quattro fasi:**
**Il primo nodo:**
**1: invia un segmento con FIN**
**2: riceve un segmento con l'ACK del FIN**
**Quindi, il secondo nodo:**
**3: invia un segmento con FIN**
**4: riceve ACK e chiude la connessione**

17. Cos'è la regola a prefisso più lungo?
    **E' la regola di corrispondenza utilizzata nelle tabelle di inoltro. All'interno della tabella di inoltro, il router individua il prefisso memorizzato che costituisce la parte iniziale dell'(intero) indirizzo contenuto nel datagramma e che, tra tutti i prefissi memorizzati che costituiscono la parte iniziale dell'indirizzo in oggetto, è quello più lungo;**
    **Il router inoltra il datagramma verso la porta di uscita corrispondente al prefisso più lungo individuato precedentemente.**
    a. Perché questa regola?
       **Per evitare corrispondenze errate a causa di un indirizzo parzialmente uguale**
18. Nell'header del TCP c'è un capo che si chiama Time to Live, a cosa serve?
    **E' un meccanismo che determina il tempo di vita di un dato (nelle cache).**
    a. Cosa succede quando il contatore arriva a 0?
19. Cos'è la checksum?
    **La checksum ha il compito di scoprire errori nei bit del segmento trasmesso ed è calcolato in modo tale che, se si deve cambiare anche una sola coppia di byte, basterà sottrarre il vecchio valore e sommare il nuovo senza ricalcolarla completamente. Nell'IPv6 non è presente.**
    a. Perchè è stata eliminata dall'IPv6?
    Un router IPv6 non ha bisogno di ricalcolare la checksum per sapere se il pacchetto è corrotto. La logica dietro questa scelta è che il secondo livello e il quarto dello stack protocollare sono già dotati di checksum.
20. In una socket TCP quali sono i parametri necessari?
21. Perchè ho bisogno di questi?
22. Cosa sono SYN ACK e dove vengono utilizzate?
    **Sono utilizzate nell'header del TCP e sono dei flags a cui vengono assegnati dei valori compresi tra 0 e 1, dove 0 è off e 1 è on e forniscono informazioni o segnalano eventi.**
23. Cosa sono indirizzi pubblici e indirizzi privati? Come si differenziano?
    **IP pubblico – si tratta dell'indirizzo IP con cui un dispositivo viene identificato su Internet, ossia quello tramite cui esso può essere raggiunto da qualsiasi altro nodo di Internet.**
    **IP privato locale – è l'indirizzo IP attraverso il quale un dispositivo viene riconosciuto all'interno di una rete locale.**
    **Una classica rete domestica, l'indirizzo IP privato è quello che il router assegna a tutti i dispositivi connessi alla rete da esso generato. Tali dispositivi comunicano con l'esterno utilizzando un solo IP pubblico, in genere associato al router: la condivisione dell'IP pubblico è possibile poiché le comunicazioni interne vengono correttamente gestite dal router stesso, che sa esattamente a quale dispositivo "dirottare" i pacchetti ricevuti. Questo meccanismo prende il nome di NAT.**
    a. Un esempio di indirizzo privato
       **192.168.1.7**
    b. Come sono costituiti gli indirizzi?
    c. Fino a che numero arrivano? **(255.255.255)**

d. L’indirizzo può essere presente più volte nelle sottoreti?
e. Come faccio a far dialogare un dispositivo che ha assegnato un indirizzo privato a un server con un indirizzo pubblico?

1. Cos'è CIDR?
   **Classless InterDomain Routing, è la strategia di assegnazione degli indirizzi. L'indirizzo IP è diviso in due parti e mantiene la forma decimale puntata del tipo a.b.c.d/x, dove x è il numero di bit della prima parte dell'indirizzo.**
2. Come vengono gestite le sottoreti?
   **Una sottorete è una rete isolata i cui punti terminali sono collegati a all'interfaccia di un host o router. Nella tabella di routing sono utilizzate per diminuire le dimensioni della tabella stessa.**
3. Come viene utilizzata la tabella di inoltro?
   **La tabella di routing viene utilizzata per l'instradamento dei pacchetti.**
   a. Che operazioni faccio?
   b. Come vengono scritte le entry all'interno della tabella di routing?
      **Secondo la regola a prefisso più lungo**
   c. Perchè sono così?
      **Per evitare errori nell'inoltro a causa del prefisso parzialmente uguale**
   d. Qual è l'ultima entry presente nella tabella di routing?
      **L'ultima entry è il default**
   e. Come viene scritta? **(0.0.0.0/0)**
4. Cos'è il mobile IP?
   **Mobile IP è un protocollo di comunicazione standard IETF ( Internet Engineering Task Force ) progettato per consentire agli utenti con dispositivi mobili di spostarsi da una rete all'altra mantenendo un indirizzo IP permanente.**
5. Cos'è il DNS?
   a. A che livello siamo?
   b. Come viene implementato? **(ci sono due modi: iterativa e ricorsiva)**
      **Nell'interrogazione iterativa:**
      **1.Il client chiede al Local NS l'indirizzo del dominio;**
      **2.Il Local NS interroga il Root NS, per l'indirizzo del NS autoritativo per il TLD del dominio;**
      **3.Il Local NS interroga il TLD NS, per l'indirizzo del NS autoritativo per il dominio richiesto;**
      **4.Il Local NS interroga il NS autoritativo per il dominio, per l'indirizzo della risorsa richiesta;**
      **5.Il Local NS restituisce l'indirizzo al client, che raggiunge la destinazione**
      **E' il Local NS che si occupa di interrogare iterativamente, tutti i NS che saranno coinvolti. Dopo ogni singola interrogazione, sempre il Local NS interroga il NS successivo, fino all'autoritativo.**

      **Nell'interrogazione iterativa:**
      **1.Il client chiede al Local NS l'indirizzo del dominio;**
      **2.Il Local NS delega la richiesta al Root NS;**
      **3.Il Root NS delega la richiesta al TLD NS;**
      **4.Il TLD NS interroga il NS autoritativo per il dominio;**
      **5.Il NS autoritativo rimanda il record al TLD NS. Il record viene passato tra tutti i NS coinvolti, fino al Local NS;**
      **6.Il Local NS restituisce l'indirizzo al client, che raggiunge la destinazione.**
      **I NS sono interrogati ricorsivamente. Ogni NS coinvolto, interroga il successivo, che interrogherà quello successivo ancora.**
6. Come identifico la sottorete? **(maschera di sottorete)**
7. Che cos'è l'IMAP?
   a. Quali sono i vantaggi?
   b. Qual'è l'altro protocollo? **(POP3)**
8. Cos'è 802.3? **(standard delle connessioni ethernet)**
   a. Come funziona ethernet?
      **Ethernet usa un solo cavo per collegare decine di stazioni di lavoro, ciascuna delle quali riceve contemporaneamente tutto quel che passa sulla rete, mentre solo una stazione alla volta ha la facoltà di trasmettere. Ogni stazione è indipendente e non esiste una singola entità che funzioni da arbitro.**

9. Quante porte ha uno switch?
10. Com'è organizzato un router al suo interno?
    a. Com'è strutturato al suo interno? Che architettura ha?
    b. Porte? Memoria?
11. Cos'è il protocollo aloha? Che caratteristiche ha?
    **Sviluppato negli anni settanta originariamente per collegamenti radio, dell'università delle Hawaii per poter collegare in un network le varie facoltà "sparpagliate" per le isole, questo protocollo deve garantire la correttezza e l'efficienza delle trasmissioni che, avvenendo appunto su reti condivise da molte postazioni, vanno incontro a numerose collisioni.**
    **E' un protocollo ad accesso casuale, è può essere puro o slotted.**
    **L'aloha puro è molto semplice, quando arriva il primo pacchetto lo trasmette immediatamente nel canale broadcast e le probabilità di collisione sono elevate.**
    **Nell'aloha slotted quando un nodo arriva un nuovo pacchetto da spedire attende l'inizio dello slot successivo, se non si verifica collisione il nodo può trasmettere un nuovo pacchetto nello slot successivo, se si verifica una collisione il nodo la rileva prima della fine dello slot e ritrasmette con probabilità p il suo pacchetto durante gli slot successivi.**
    a. Meglio aloha puro o slotted?
       **L'aloha puro ha un'efficienza del 18%, lo slotted del 37%**
12. Quali protocolli MAC (accesso al mezzo) esistono? **(il più comune è ethernet)**
    **Protocolli MAC a suddivisione del canale che condividono il canale equamente ed efficientemente con carichi elevati ma sono inefficienti con carichi leggeri.**
    **Protocolli MAC ad accesso casuale efficienti con carichi leggeri ma problematici con i carichi elevati a causa dell'eccessive collisioni.**
    a. Oltre ethernet quali altri esistono? **(token ring e token pass)**
13. Cos'è la checksum?
    a. Come funziona?
    b. Dove viene inserito questo valore?
    c. Come si implementa a livello di trasporto?
14. Cos'è TTL? **(è un contatore, sono il numero di salti che può fare il pacchetto)**
15. Quanto sono grandi gli indirizzi IPv6?
    **Il formato generale degli indirizzi IPv6 è composto da 8 campi e ogni campo rappresente 16bit. IPv6 consente fino a $2^{128}$ indirizzi possibile e utilizza la notazione esadecimale a due punti.**
    a. Cosa è cambiato rispetto all'IPv4?
       **La checksum è stata rimossa, le opzioni non fanno più parte dell'intestazione, l'intestazione è 40 byte e a lunghezza fissa e non è consentita la frammentazione**.
    b. Da cosa sono sostituiti i 20 byte?
16. Come funziona l'ARP?
    a. Esempi di ARP?
17. Cos'è e come funziona il RARP?
18. L'indirizzo MAC da quanti bit è costituito?
    **E' costruito da 48 bit**
    a. Come viene scritto?
    b. Esempi di MAC?
       **00-08-74-4C-7F-1D**
    c. Come viene fatta la codifica?
       **Bit 1 (ricevente): il primo bit dell'indirizzo MAC indica se si tratta di un indirizzo singolo o di gruppo. Questo bit è chiamato I/G (abbreviazione di individual/group). Se I/G = 0, si tratta di un indirizzo Unicast per una singola scheda di rete. Gli indirizzi Multicast sono identificati da I/G = 1 e sono indirizzati a più destinatari.**
       **Bit 2 (validità): il secondo bit dell'indirizzo MAC indica se si tratta di un indirizzo con validità globale (universal) o se l'indirizzo è stato assegnato localmente (local). Il bit è chiamato U/L. Se U/L = =, l'indirizzo è considerato come Universally Administered Address (UAA) valido in tutto il mondo. Gli indirizzi che sono solo localmente unici sono denominati Locally Administered Address (LAA) e contrassegnati con U/L = 1.**

**Bit 3–24 (identificazione del produttore): i bit dal 3 al 24 codificano un identificatore (Organizationally Unique Identifier, OUI) assegnato da IEEE in modo esclusivo ai produttori di hardware. L'assegnazione di OUI è pubblica e può essere determinata tramite database. L'OUI dell'indirizzo di esempio (AC-16-ID) è stato assegnato dall'IEEE al produttore di dispositivi statunitense Hewlett Packard.**

**Bit 25–48 (Network Adapter Identifier): i bit dal 25 al 48 forniscono ai produttori di dispositivi con 24 bit l'assegnazione di un'unica identificazione hardware (Organizationally Unique Address, OUA). Così si possono assegnare 224 (= 16.777.216) OUA univoche per ogni OUI.**

19. Cos'è un bridge? A che livello operiamo?
    a. Cos'è un bridge autoapprendente? **(apprendono la topologia della rete e memorizzano il MAC [...])**
20. Quali sono i meccanismi di controllo congestione?
    **Vi sono due approcci diversi al controllo della congestione: il controllo end-to-end utilizzato nel TCP in cui non viene ricavata alcuna informazione dalla rete e la congestione è rilevata attraverso la perdita di segmenti e l'aumento del ritardo.**
    **Il secondo approccio è il controllo a livello di rete dove i router forniscono informazioni ai sistemi finali e vengono utilizzati bit per indicare la congestione.**
    **Nel TCP viene utilizzato lo slow start che fa crescere la congestion window all'inizio della congestione fino al primo evento di perdita del segmento. A ogni RTT la CWND raddoppia, l'inizio è lento ma la crescita è rapida.**
21. Cosa sono gli switch di livello 2 (data link)?
    **E' un dispositivo del livello di data link che filtra e inoltra i pacchetti Ethernet, esamina l'indirizzo di destinazione e lo invia all'interfaccia corrispondente all asua destinazione. Quando un pacchetto è stato inoltrato nel segmento usa CSMA/CD per accedere al segmento. Gli host non hanno idea della presenza di questi switch e gli switch non hanno bisogno di essere configurati, autoapprendono.**
22. Cosa sono gli switch autoapprendenti? **(plug-and-play)**
23. Tree?
24. Cos'è 255.255.255.0? Cosa significa?
    **E' l'indirizzo di destinazione del broadcast.**
25. Quali sono i protocolli di accesso al mezzo? **(802.3(?))**
26. Cos'è il mobile IP?
27. Come funziona?
28. Quali sono gli elementi di base di questo protocollo?
29. Come faccio a comunicare con un utente che si sposta?
30. Quali sono le differenze tra IPv4 e IPv6?
31. Estensioni? **(stiamo parlando dell'header, sono porte fondamentali, nell'IPv4 20 byte, nell'IPv6 sono agganciate come carico dati?)**
32. Dove si trova il bit di FIN?
33. Cos'è il BGP? **(border gateway protocol)**
    **E' uno dei protocolli di routing. Si occupa dei criteri di tipo amministrativo, per esempio se un ISP decide di non voler instradare i pacchetti attraverso un ISP concorrente.**
34. Quali sono i due algoritmi di routing utilizzati all'interno di un autonomous system? **(RIP, OSP)**