1) Sappiamo che abbiamo N indirizzamenti possibili con N = 2^n, dove n = 32 – k. K rappresenta il numero di bit occupati dal campo rete nella NETMASK. Quindi dovendo indirizzare 256 indirizzi, vorrà dire che avremo 8 bit riservati all'host. La rete è una \24. M = m sarebbe il numero di sottoreti, ma M = 2^m e quindi abbiamo 2^8 sottoreti da utilizzare per coprire 256 indirizzi.

2) PASSAGGIO IPV4-IPV6

Un datagramma IPv4 è un identificatore univoco utile per riconoscere le interfacce di rete nel livello di rete del modello TCP/IP. Il suo header presenta 2 indirizzi IP di sorgente e destinazione, e 3 livelli, tutti formati da 5 byte. Al primo livello c'è la versione (0010) , la lunghezza totale del datagramma e la lunghezza dell'header. Al secondo livello c'è un Identifier(id del pacchetto, associa i frammenti a un pacchetto) e il Fragment Offset(indica la posizione del frammento). Al terzo livello ci sono: protocol, TTL,Header Checksum. Un header IPv6 è invece composto da altri campi: versione, Traffic Class, Flow Label,Payload Length,Next Header e Hop Limit, e non supporta la frammentazione. Ci sono indirizzi IPv6 compatibili con IPv4, cioè indirizzi IPv6 con un prefisso di 96 bit nulli e 32 bit che sono pari a un IPv4. Quindi rappresentabile come 0.0.0.0.0.0.X.Y. Per incorporare un IPv4 in un IPv6 si effettua una mappatura: i primi 80 bit sono nulli, i successivi 16 sono pari a 1, e gli ultimi 32 sono un indirizzo IPv4 classico. Si rappresenta con ::FFFF:X:Y oppure 0000:0000:FFFF:X:Y. Nel tunneling i pacchetti IPv6 sono trasportati come payload in indirizzi IPv4. In questo modo un router IPv4 può trasportare un IPv6 anche non potendolo supportare. I router IPv6 vicini a quelli IPv4 avranno indirizzi compatibili con gli IPv4, viceversa avranno indirizzi IPv6 mappati su IPv4.

3)DIFFERENZA TRA HUB E SWITCH

Dato che l'hub ritrasmette il traffico che ad esso arriva su tutte le porte, ai livelli superiori ci sarà il traffico dei livelli inferiori. Quindi tutta la rete forma un unico DOMINIO DI COLLISIONE, che è l'insieme delle stazioni che possono potenzialmente generare collisioni, perché gli hub non sono in grado di isolare i domini di collisione. Il bridge è un dispositivo in grado di isolare i domini di collisione. Un bridge invece analizza l'indirizzo di destinazione di ogni pacchetto e lo ritrasmette alle opportune porte. Uno switch è un bridge con numerose porte. Con l'uso di uno switch per gestire più hub , che collegano a loro volta gli host, possono creare vari domini di collisione separati. Con l'uso di soli switch non si hanno più collisioni.

5) In uno switch ethernet, in una rete come questa (computer collegati tramite switch ethernet), ci sono possibilità che si generino collisioni?

No, perché appunto uno switch è un tipo di bridge, avente la caratteristica di non creare un dominio di collisione, tramite una tabella di FILTERING che consiste in: Quando riceve un frame, il bridge prende nota di host di provenienza e lo associa alla porta del bridge in cui il frame è arrivato, con la coppia indirizzo MAC sorgente – porta sorgente nella tabella di filtering, assiempe al tempo di arrivo del pacchetto(timestamp). Quando il bridge riceve frame da ogni host la tabella è completa. Lo switch separa i domini di collisione.

6) Cosa si fa per fare in modo che non ci siano collisioni?
Una collisione si verifica quando due o più dispositivi tentano di trasmettere dati contemporaneamente sulla stessa rete. Con gli switch che lavorano in modalità full-duplex, ogni connessione è isolata e non c'è competizione per l'uso del canale. Per questo motivo le collisioni sono quasi del tutto eliminate, ma possono verificarsi in situazioni particolari come, ad esempio, se ci sono errori di configurazione; quindi, se le impostazioni dello switch e del dispositivo non corrispondono, cioè uno lavora in full-duplex e l'altro

in half-duplex. Una delle possibili soluzioni è configurare le porte dello switch e i dispositivi connessi in modalità full-duplex e sostituire eventuali hub con switch.

7) 8) Come è fatta la tabella dello switch? Come fa lo switch a configurare automaticamente i campi della tabella quando è vuoto?
La tabella dello switch è una struttura dati utilizzata dagli switch per instradare i pacchetti ai dispositivi corretti nella rete. Ogni riga della tabella contiene informazioni essenziali per associare un dispositivo alla porta corretta dello switch. La tabella include i campi:
   - Indirizzo MAC: l'indirizzo fisico di un dispositivo nella rete che identifica univocamente ogni dispositivo Ethernet;
   - Porta dello switch: la porta fisica dello switch a cui è connesso il dispositivo con il Mac address corrispondete;
   - VLAN: esso è un campo opzionale, se lo switch supporta VLAN, quest'informazione specifica la VNAL a cui appartiene il dispositivo.
   - Timer di scadenza: un timer che indica per quando tempo l'associazione MAC-Porta rimarrà valida. Se non vengono rilevati pacchetti provenienti da un MAC address per un certo periodo, l'entry viene rimossa.

   Quando uno switch riceve un pacchetto Ethernet, legge l'indirizzo MAC sorgente e lo associa alla porta da cui è arrivato e aggiorna la tabella con quest'informazione. Dopodiché lo switch utilizza la tabella per inoltrare i pacchetti al dispositivo corretto, inoltre, legge l'indirizzo MAC di destinazione e determina la porta corrispondente. Se l'indirizzo non è nella tabella, il pacchetto viene inoltrato a tutte le porte (fenomeno di flooding), tranne a quella di origine. Le associazioni nella tabella hanno una durata limitata, quindi il timer di scadenza consente di liberare spazio nella tabella per nuovi dispositivi.

   Quando lo switch è avviato e ha non informazioni preconfigurate nella sua tabella, costruisce dinamicamente questa tabella utilizzando un processo chiamato apprendimento dinamico dei MAC address, cioè, quando lo switch è appena acceso o ripristinato, la sua tabella è vuota. Quando un frame Ethernet arriva su una porta dello switch, lo switch esamina l'indirizzo MAC sorgente del frame e la porta fisica su cui è stato ricevuto il frame. Lo switch registra nella tabella il MAC address sorgente e associa quell'indirizzo alla porta su cui è stato ricevuto il frame. Quando lo switch riceve un frame con un MAC address destinazione, se il MAC address è nella tabella, inoltra il frame alla porta associata, se il MAC address non è nella tabella, lo switch invia il frame in modalità broadcast a tutte le porte eccetto quella di origine.

9) Perché è importante il tempo di scadenza?
Il tempo di scadenza è un parametro cruciale in molti protocolli di rete e sistemi informatici, in quanto consente di gestire risorse; quindi, se una connessione o un'operazione rimane inattiva indefinitamente, le risorse allocate rimarrebbero occupate inutilmente. Con un timeout, il sistema può chiudere connessioni inattive e mantenere alte prestazioni. Inoltre, consente di gestire errori, quindi se un pacchetto non viene ricevuto entro il tempo previsto, il timeout consente al mittente di rilevare un problema. Noi protocolli con TCP, il timeout è utilizzato per decidere quando ritrasmettere un pacchetto che potrebbe essere stato perso. Infine, consente di avere una protezione contro attacchi, limitando il tempo in cui la connessione inattiva può rimanere aperta.

10) Problema delle oscillazioni utilizzando un protocollo di routing link-state.
Il problema delle oscillazioni in un protocollo di routing link-state si verifica quando le decisioni di routing continuano a cambiare rapidamente, creando instabilità nella rete. Questo può accadere in determinate condizioni, causando problemi come perdita di pacchetti, aumento del ritardo e degrado generale delle prestazioni della rete. Le oscillazioni nei protocolli di routing link-state si verificano quando le metriche o gli stati dei link cambiano frequentemente, portando i router a ricalcolare continuamente i percorsi.

11) Differenza cablaggio orizzontale e cablaggio verticale.

Il cablaggio è il sistema di connessione fisica tra i vari dispositivi di una rete di comunicazione. È attraverso i cavi che i dati viaggiano da un dispositivo all'altro, garantendo che tutto funzioni correttamente. Quando parliamo di cablaggio per le reti, ci riferiamo principalmente a due tipi di cavi:

- Cavi in rame: sono i più comuni, ad esempio il cavo a coppie intrecciate, dove i fili all'interno sono avvolti a spirale per ridurre le interferenze elettromagnetiche . esistono diverse categorie di cavi, che determinano la loro capacità:
  - CAT 5e: supportano una velocità fino a 1 Gbps;
  - CAT 6, CAT 6a, CAT 8: supportano una velocità fino a 10 Gbps.

  I cavi in rame sono perfetti su distanze brevi, mentre su lunghe distanze possono subire interferenze o perdite di segnale.

- Fibra ottica: è la tecnologia di cablaggio più avanzata. Invece di usare segnali elettrici, utilizza impulsi di luce per trasmettere dati attraverso filamenti di vetro o plastica. Questo le da enormi vantaggi, infatti è molto veloce, può coprire lunghe distanze senza perdere qualità e non subisce interferenze elettromagnetiche. Esistono due tipi principali:
  - Fibra monomodale: è usata per coprire distanze molto lunghe, come nelle dorsali internet tra città;
  - Fibra multimodale: è adatta a distanze brevi, come le reti aziendali.

In ambienti più grandi si utilizza un approccio chiamato cablaggio strutturato che prevede due sezioni principali:

- Cablaggio verticale: collega i principali apparati della rete e spesso utilizza fibra ottica per garantire le prestazioni;
- Cablaggio orizzontale: collega i dispositivi degli utenti finali della rete, e si utilizzano i cavi in rame.

12) Quando il cablaggio si fa in rame, qual è la massima distanza tra utente e apparato?

Quando si utilizza un cablaggio in **rame**, la massima distanza tra l'utente e l'apparato di rete dipende dallo standard Ethernet e dalla categoria del cavo:

- Ethernet su cavi UTP/FTP/STP:
  - 100 metri per connessioni Gigabit Ethernet o Fast Ethernet. Questa distanza comprende:
    - 90 metri di cablaggio permanente.
    - 10 metri di patch cable (cavi di collegamento) distribuiti tra entrambe le estremità.
- PoE (Power over Ethernet):
  - Anche con PoE, la distanza massima rimane 100 metri per fornire dati e alimentazione.
- Ethernet 10GBASE-T (10 Gbps):
  - Fino a 100 metri su cavi Cat6a.
  - Fino a 55 metri su cavi Cat6 (con interferenze minime).
- Ethernet su cavi Cat5e:
  - Supporta fino a Gigabit Ethernet su distanze fino a 100 metri.

13) Parliamo di CSMA/CD.

Il CSMA prima di trasmettere, una stazione verifica se il canale è impegnato o meno mettendosi in ascolto. Questa regola però non è sufficiente ad evitare tutte le collisioni. Quando un canale è occupato, una stazione riprova a trasmettere provocando un ritardo. Il ritardo di propagazione fa si che due nodi non possano ascoltare le reciproche trasmissioni

istantaneamente. Dunque, può capitare che un nodo inizia a trasmettere e che un altro nodo verifichi che il canale è libero in un tempo successivo che non è sufficiente per la propagazione della prima trasmissione al secondo nodo. Vedendo il canale libero, il nodo inizia a trasmettere, ma ciò causa una collisione. Il modo per limitare queste collisioni è che una stazione, mentre effettua una trasmissione, sia contemporaneamente in ascolto per rilevare eventuali interferenze. Una collisione è rilevata dalla stazione mittente se riceve un segnale differente da quello inviato. L'ideale è che, quando una stazione rileva una collisione, interrompa immediatamente la trasmissione. Così facendo si ottiene la variante CSMA/CD.

14) Slotted e unslotted Aloha.

Gli schemi ad accesso casuale sono protocolli utilizzati per la gestione dell'accesso al mezzo trasmissivo condiviso da più dispositivi. Un protocollo ad accesso casuale è ciò che specifica come rilevare e risolvere le collisioni. Due di questi protocolli sono:

- Aloha slotted: il tempo è ripartito in slot temporali di uguale durata, e ciascun nodo può inviare dati solo in maniera sincrona all'inizio degli slot. Se un nodo ha dati disponibili li trasmette al primo slot disponibile, e se si verifica una collisione è in grado di saperlo e ritrasmettere i dati negli slot successivi fino a che la trasmissione non va a buon fine. Quando tutti i nodi hanno trasmesso una volta con successo, è terminato un ciclo.
- Aloha unslotted: si utilizza un protocollo privo di sincronizzazione, in cui ogni nodo invia il frame non appena i dati sono disponibili. In questa versione l'efficienza è ancora più bassa, perché non essendoci più slot c'è la possibilità che più frame si sovrappongono, dunque la probabilità di collisione raddoppia.

15) A cosa serve RTP?

RTP è un protocollo sia di trasporto che applicativo. Adotta infatti il modello application level framing, secondo il quale il modo con cui sono fatti i pacchetti è opportuno che sia implementato dalle applicazioni. Si basa sul protocollo UDP, ossia i pacchetti RTP sono incapsulati in pacchetti UDP. RTP supporta due necessità di corretta tempificazione:

- Sincronizzazione inter-media: si devono sincronizzare flussi separati;
- Sincronizzazione intra-media: i dati devono essere prodotti da una corretta tempificazione.

Il protocollo supporta sia la trasmissione unicast che multicast. Nell'header RTP si possono identificare dei campi fondamentali:

- Numero di sequenza: univoco per ogni pacchetto e necessario per identificare perdite di pacchetti.
- Payload type: specifica il tipo di media contenuto e quindi la codifica utilizzata per i dati.
- Timestamp: si riferisce alla tempificazione dei dati trasferiti rispetto ad un clock specifico.
- SSRC: che identifica in maniera univoca la sorgente del flusso.
- Sessione RTP: è un flusso di dati tra più entità, gestita mediante RTP.

16)HTTP e metodi del protocollo, GET condizionale

Il protocollo HTTP è un protocollo della IP suite ideato per la trasmissione di ipertesti, che si basa sul TCP, cioè che presuppone che il protocollo di trasporto sia il TCP. Tra client e server avvengono questi passaggi: il cliente apre un socket (strumento di comunicazione di un SO per agganciare i processi di un end-system all'end point di una connessione UDP o TCP) verso la porta TCP 80 del server(se non diversamente specificato), dopodiché il server accetta la connessione, il client invia una richiesta per uno specifico oggetto(file etc..) identificato da un URL (Uniform Resource Locator, codice che identifica in modo univoco una risorsa del server),

il server risponde e chiude la connessione. A connessione terminata ne client ne server possono avere info relative ai messaggi precedenti, per questo si dice che HTTP è STATELESS (senza stato). Una pagina WEB è un documento di testo scritto in HTML. I metodi del protocollo HTTP sono: GET, HEAD, POST.

GET = si usa per richiedere una risorsa identificata da un URL. Se la risorsa è accessibile (senza autenticazione) il server la invia nel body della risposta. Il GET può essere ASSOLUTO se la richiesta è senza specifiche, CONDIZIONALE se c'è un criterio indicato negli header e PARZIALE se si richiede una sottoparte di una risorsa già memorizzata.

HEAD = si utilizza per richiedere la validità di una risorsa identificata da un URL. Tramite head il client verifica se un URL è valido e accessibile.

POST = si utilizza per trasmettere le info dal client al server senza la creazione di una risorsa.

17) Il Content-Type è un header HTTP che specifica il tipo di contenuto presente nel corpo di una richiesta o risposta HTTP. È una delle informazioni più importanti utilizzate nei protocolli web per permettere al client e al server di capire come devono essere interpretati i dati scambiati. L'header HTTP Content-Type è utilizzato nelle comunicazioni web per indicare il tipo di dati presenti in un corpo della richiesta o risposta HTTP. Questo header aiuta il client o il server a interpretare correttamente il contenuto trasmesso. Il Content-Type specifica:

Formato del contenuto: Identifica il tipo MIME (Multipurpose Internet Mail Extensions) del contenuto, come testo, JSON, immagini, ecc.

Parsing del contenuto: Aiuta il destinatario a interpretare i dati nel formato corretto.

Compatibilità: Permette al server o al client di adattarsi alle esigenze del contenuto (es. un browser per visualizzare immagini o testo).

18) FTP

Il File Transfer Protocol è un protocollo applicativo, con il quale si effettuano 2 tipi di trasferimenti di file, in DOWNLOAD o in UPLOAD, da una macchina remota ad un client e viceversa. Usa il modello client/server e il TCP. Il protocollo lavora usando 2 connessioni parallele, una per i dati e una per le info di controllo. Questa peculiarità lo distingue dall'HTTP. Il canale di controllo di un server FTP corrisponde alla porta 21(in cui si stabilisce una connessione con il client). Il FTP può essere attivo o passivo. Il canale dati ha natura temporanea, e se viene aperto dal server tramite la sua porta 20 si parla di ACTIVE FTP, viceversa, se lo apre il client si parla di PASSIVE FTP. Una volta creato, il canale di controllo è fisso, quindi FTP è STATEFUL, perché FTP mantiene info su connessione, dati di autenticazione o la directory corrente. I suoi comandi sono USER,PASS,LIST,GET filename, PUT filename che rispettivamente inviano e ricevono file dalla macchina remota. Per usare una connessione FTP serve avere un account sulla macchina remota, ma di solito il server non è configurato per accettare connessioni FTP.

19) ARP

L'ARP(Address Resolution Protocol) è un protocollo ausiliare, come il RARP, del livello 3 di rete e svolgono funzioni di supporto alla trasmissione di indirizzi IP in reti locali. Può capitare che sia noto l'IP di destinazione di un dispositivo nella stessa rete, ma non il MAC associato. L'ARP serve a risolvere un indirizzo IP in un MAC address, mentre RARP effettua il procedimento opposto.

Risoluzione IP interno: Quando un host vuole conoscere il MAC associato a un IP, esso invia tramite ARP un messaggio di richiesta, in modo che il dispositivo che conosce l'associazione possa rispondere verso l'host stesso, mentre i restanti ignorano la richiesta. Prima di inviare

un pacchetto verso un dato IP, il mittente verifica a livello di rete se questo IP fa parte della sottorete. Se è così, il mittente usa ARP per ricavare il MAC.

Risoluzione IP esterno: se il destinatario del datagramma è esterno alla rete locale, allora il mittente prima usa ARP per ricavare l'indirizzo MAC dell'interfaccia di gateway del router della propria rete, dopodiché invia il datagramma al gateway usando il MAC ricavato. Se l'IP è esterno, al mittente non serve il MAC associato, ma quello del gateway della propria rete. Il campo Operation Code ha due tipi di messaggi: di richiesta(ARP Request) e di risposta(ARP reply). Il protocollo RARP svolge il ruolo opposto ad ARP, assegnando un IP ad un dato indirizzo MAC. Si presuppone l'esistenza di un server RARP. Questo protocollo è superato da DHCP, perché oltre ad assegnare un IP fornisce anche parametri sulla configurazione.

20) NAT

Il NAT(Network Address Translation) è una tecnica che consente a un dispositivo di rete, un router, di agire come intermediario tra una rete pubblica e una privata. Si mappano un insieme di indirizzi privati, con le relative porte , a un unico indirizzo pubblico. Per mantenere traccia di questo IP si associa un port number. NAT deve modificare in ingresso ogni IP e port number di ogni pacchetto, basandosi sulla NAT Translation Table, per inoltrarlo al lato opposto. Quando un router riceve un pacchetto inviato dalla rete privata, il NAT salva IP e port number provenienti dalla tabella, e vi associa un IP pubblico e il suo port number. Per il processo inverso si crea un problema di TRASVERSAL FORWARDING. Si deve prima inviare un pacchetto dalla rete interna per creare una entry; quindi, che un client esterno possa accedere alla rete dal port number della entry (PORT FORWARDING). Il forwarding statico non è conveniente, perciò si applica il dinamico con dei meccanismi: UPnp(Universal Plug and Play) e IGD(Internet Gateway Device). Essi permettono di effettuare un prestito a tempo di port number dell'IP pubblico.

21) RIP

E' un protocollo applicativo che appartiene alla famiglia degli IGP (Interior Gateway Protocol) ed implementa l'algoritmo distance victor. Si basa sull'invio in broadcast mediante UDP delle tabelle di routing, effettuato ogni 30 secondi, mentre le tabelle sono elaborate a livello applicativo da un app chiamata ROUTED. Oggi si basa su indirizzamenti con netmask /k. RIP non differenzia reti e host singoli, ma suddivide le entità in attive e passive. Le prime possono solo ricevere messaggi(host) e le seconde possono anche spedirli(router). RIP non supporta reti con distanza maggiore da un router di 15 m, quindi è pensata per piccolo raggio.

22-23) ICMP

L'ICMP(Internet Control Message Protocol) è usato per verificare ed interagire con lo stato di una rete. E' un protocollo ausiliario del livello trasporto, e quindi un pacchetto ICMP è sempre incapsulato in un datagramma IP. I messaggi sono individuati da un tipo e un codice. ECHO REQUEST con tipo 8 ed ECHO REPLY con tipo 0 sono importanti. Alla recezione di un messaggio echo request un device risponde sempre con un echo reply. Il tempo che passa tra richiesta e risposta è detto LATENZA. L'invio di echo request si effettua con il comando PING. Il comando TRACEROUTE è usato per scoprire il percorso per arrivare a una destinazione. Si inviano una serie di pacchetti TTL, in modo crescente. Il router, che decrementando il TTL, lo azzera e invia un messaggio TTL Expired. A volte un pacchetto può non giungere a destinazione. Se nessun pacchetto inviato dal traceroute ottiene risposta da un AP, anziché ottenere l'IP esce RICHIESTA SCADUTA. In questo caso il router non è configurato per rispondere a un traceroute.

24) FUNZIONI ASCII CRITTOGRAFICHE

Le funzioni ASCII crittografiche si basano sull'utilizzo dei codici ASCII per trasformare o cifrare un testo. L'obiettivo principale è rendere il contenuto originale non leggibile o sicuro, sfruttando i valori numerici associati ai caratteri. Queste funzioni possono operare applicando trasformazioni dirette, come lo spostamento dei caratteri lungo la tabella ASCII, oppure combinazioni più complesse, come operazioni matematiche sui valori numerici dei caratteri stessi. La crittografia può essere simmetrica, dove la stessa tecnica è usata per cifrare e decifrare, oppure asimmetrica, con processi di trasformazione diversi. Tra le operazioni comuni ci sono la traslazione dei caratteri, che modifica il valore ASCII aggiungendo o sottraendo un numero fisso, o l'utilizzo di operatori logici come XOR per combinare i valori ASCII con una chiave crittografica. Ogni trasformazione deve garantire reversibilità per consentire il ripristino del testo originale. Inoltre, è possibile generare codici univoci dai valori ASCII combinati per verifiche di integrità. L'applicazione di queste funzioni è utile in ambiti dove la sicurezza o l'offuscamento delle informazioni è importante, come nella protezione di dati sensibili, nella verifica di integrità o nell'implementazione di algoritmi personalizzati per la trasmissione sicura dei dati.

25) DOVE SI TROVA IL CAMPO CRC?

Al livello di trasporto è noto che si fa uso di una checksum per il controllo di errori. Al livello data link, invece si fa uso di CRC, codici CICLICI o POLINOMIALI. Si valuta una stringa di bit a partire dai dati, che andrà aggiornata in coda al frame. La stringa R di bit è pari al resto della divisione D traslato di r bit a sinistra ed un polinomio G noto sia a mittente che destinatario. Traslare D di r bit a sinistra corrisponde a valutare D * (2^r). quindi R = resto di D*(2^r) / G. La divisione è effettuata in aritmetica a modulo 2.

26) Funzioni hash.

L'hashing è un processo matematico che trasforma un input di lunghezza variabile in un output di lunghezza fissa, chiamato hash o digest: h=H(m). Questo processo è realizzato da una funzione hash e viene utilizzato in diversi ambiti, dalla sicurezza informatica alla gestione dei dati. Affinché una funzione hash sia crittografica deve soddisfare una proprietà:

- Deve essere computazionalmente impossibile trovare due messaggi x e y diversi, tale che H(x)=H(y); cioè, dal punto di vista computazionale, data la coppia messaggio-hash (m, H(m), creata dal trasmittente, un intruso non può falsificare il contenuto di un messaggio, y, che abbia lo stesso valore hash dell'originale.

27) Checksum sia TCP che IPv4 su cosa è calcolato, qual è l'algoritmo per calcolarlo e a che serve la checksum.

La checksum è un meccanismo di controllo utilizzato nei protocolli di rete, come TCP e IPv4, per rilevare errori nei dati durante la trasmissione.

- Checksum in Ipv4: Verifica l'integrità dell'intestazione IPv4 e serve a rilevare errori causati da corruzione dei dati durante la trasmissione. La checksum IPv4 viene calcolata solo sull'intestazione del pacchetto e non sui dati (payload). Si utilizza un'operazione matematica semplice, basata sulla somma dei valori binari:
  - Dividi l'intestazione in segmenti da 16 bit.
  - Somma tutti i segmenti.
  - Inverti tutti i bit del risultato per ottenere il complemento a uno.
  - Durante la verifica, il destinatario ricalcola la checksum e la confronta con quella ricevuta. Se il risultato è diverso, l'intestazione è considerata corrotta.

- Checksum in TCP: Verifica l'integrità dell'intero segmento TCP, inclusi dati e intestazione e serve per assicurarsi che il segmento non sia stato alterato o corrotto. La checksum TCP viene calcolata su:
    - L'intestazione TCP.
    - I dati (payload).
    - Uno pseudo-intestazione derivata dall'intestazione IPv4 o IPv6, che include:
        - Indirizzo IP sorgente.
        - Indirizzo IP di destinazione.
        - Protocollo (valore 6 per TCP).
        - Lunghezza del segmento TCP.

Calcolo:

- Combina tutti i dati (intestazione TCP, dati, pseudo-intestazione) in segmenti da 16 bit.
- Somma tutti i segmenti usando complemento a uno.
- Inverti i bit del risultato per ottenere la checksum.
- Durante la ricezione, il destinatario esegue lo stesso calcolo e lo confronta con la checksum ricevuta.

28) Come funziona la frammentazione di assemblaggio IPv4.

Quando un datagramma deve attraversare una rete con una MTU (maximum trasmission unit, cioè la dimensione massima del pacchetto che può essere trasmesso) inferiore rispetto alla dimensione del datagramma originale, il datagramma viene suddiviso in frammenti più piccoli per poter essere trasmesso attraverso la rete. Quindi, ogni collegamento di rete ha un valore di MTU che rappresenta la dimensione massima del pacchetto che può essere trasmesso. Se un datagramma supera questa dimensione, il router che lo elabora può frammentarlo in unità più piccole. Il router divide il datagramma originale in frammenti più piccoli, ognuno dai quali può essere trasmesso attraverso il collegamento con l'MTU limitante. Ogni frammento contiene un'intestazione IP che include informazioni per la ricostruzione del datagramma. La ricostruzione avviene solo sul dispositivo di destinazione finale e l'host di destinazione utilizza i campi dell'intestazione per ricostruire il datagramma originale. Durante la frammentazione i flugs devono essere:

- Bit 1: deve essere sempre 0.
- Bit 2 (don't fragment): se è impostato a 1, indica che il pacchetto non deve essere frammentato. Se la frammentazione è necessaria e il bit è 1 allora il pacchetto viene scartato.
- Bit 3 (more fragment): se è impostato a 1, indica che ci sono altri frammenti.

29) CDN

La CDN è un'infrastruttura creata per distribuire efficacemente agli utenti di internet i contenuti dei siti web più popolari. Il suo funzionamento si basa sulla distribuzione dei contenuti in più server che fungono da replica del web server di origine. Questo permette sia di proteggere il web server principale da carico improvviso da parte degli utenti, sia di rendere il sistema più affidabile e robusto ai guasti. Per un buon funzionamento è necessario che anche i server stessi abbiano un buon funzionamento è necessario che anche i server stessi abbiano una buona connettività alla rete. Per ottenere ciò, gli operatori CND stipulano dei contratti con gli internet service provider di medie e grandi dimensioni; questa collaborazione avvantaggia entrambi, perché mentre i CDN garantiscono una buona connettività ai content provider da cui sono usati, gli ISP possono sottrarre il traffico che scorre nei server della CND ai restanti ISP, ed ottenere una buona reputazione nel mercato per aver fornito un servizio di buona qualità. Un CDN può operare in vari modi. Un metodo è quello du fare in modo che

l’HTML richiesto dal browser del client faccia riferimento non al web server, bensì a server più vicini al client e gestiti dal CND.

30) Parla del DNS.

È un sistema di associazione tra indirizzi IP e nomi simbolici. La struttura è di tipo gerarchico, e interessa i domini e i server associati. Partendo dalla cima abbiamo i root DNS server, i TLD server che si occupano dei domini di alto livello, e infine i server autoritativi, cioè i server di competenza. I root DNS server sono 13 server logici in internet. I server autoritativi corrispondono a server di nomi che sono capaci di risolvere tutti i nomi all’interno di un determinato dominio, e ad essi si riferiscono i name server TLD. Poi vi sono i local name server, installati da ciascun operatore di rete nella propria rete, in modo che gli host di ciascuna rete siano configurati con l’indirizzo del DNS server locale. Un local name server non appartiene alla gerarchia di server, ma opera da proxy tra client e gerarchia. Il modo in cui si interfaccia può essere attraverso:

- Query iterative: dove il server chiede l’IP del DNS autoritativo al server radice, ma questo fornisce solo l’IP del TDL server, che a sua volta può fornire l’IP del server autoritativo.
- Query ricorsive: in cui il server chiede al primo server contattato, in genere quello radice, la risoluzione completa, e quest’ultimo effettua ciò chiedendo al TDL una risoluzione completa, che ottiene quindi l’IP del server autoritativo, lo fornisce al server radice, e quest’ultimo lo fornisce al DNS locale.

Un DNS corrisponde ad un enorme database logico, all’interno del quale le informazioni sono contenute sottoforma di record. Ci sono vari tipi di record, i più comuni sono:

- A: associa un nome di dominio a un indirizzo IPv4.
- AAAA: associa un nome di dominio a un indirizzo IPv6.
- CNAME: punta un nome di dominio a un altro nome di dominio.
- MX: identifica i server di posta per un dominio.
- NS indica i server DNS autoritativi per un dominio.

31-32-33) 3-WAY-HANDSHAKE e 4-WAY HANDSHAKE

La connection establishment del TCP si basa su una procedura 3-way-handshake data dall’invio reciproco di vari segmenti di controllo. Il server si mette in ascolto su una data porta(stato LISTEN) mentre il client invia un segmento SYN a questa porta, cioè una richiesta di connessione con un TIMEOUT. Si suppone che il numero di sequenza sia x. Ricevuto il SYN, il server risponde con un segmento di riscontro che avrà stesso flag SYN attivo e valore di riscontro incrementato del numero di sequenza della richiesta, cioè ACK += x. Il numero di sequenza della risposta è slegato da quello di richiesta , può essere un qualsiasi valore y. Quando si vuole terminare la connessione si attua una procedura di 4-way-handshake. Non c’è un end-system preciso, ma si parla di active closer e passive closer. Il primo rappresenta la volontà di chiudere la connessione. L’active closer manda una richiesta con flag FIN attivo. Il passive closer risponde con un segmento che ha flag ACK e FIN attivi. L’active manda un ACK e si pone in TIME_WAIT di durata elevata. Alla ricezione dell’ACK il passive va in stato CLOSED, mentre l’active non può fin quando non termina il TIME_WAIT. Si impedisce la creazione di una nuova connessione tra gli stessi end point, necessario per evitare probabilità che pacchetti persi nella vecchia connessione arrivino nella nuova. Con un elevato TIME_WAIT si pone il pericolo a 0. Se il client non invia l'ACK finale durante l'handshake a 3 fasi nel protocollo TCP, il server rimane in uno stato intermedio chiamato SYN-RECEIVED. Questo stato indica che il server ha ricevuto la richiesta iniziale di connessione (il segmento SYN del client) e ha risposto con il proprio segmento SYN+ACK, ma non ha ancora ricevuto la conferma finale (ACK) da parte del client. Ritardo nelle nuove connessioni: Un server sotto carico può raggiungere il

limite massimo della sua backlog queue, bloccando o rallentando nuove richieste di connessione. Attacchi Denial of Service (DoS): In un attacco SYN Flood, un malintenzionato invia molte richieste SYN senza completare l'handshake. Questo riempie la backlog queue e rende il server incapace di accettare nuove connessioni.

34)DHCP

Il DHCP è un protocollo applicativo basato sul modello client-server, in cui un client che si vuole connettere a una data rete, quindi privo di IP per la rete, interagisce con un server che lo fornisce. Sono forniti campi opzionali, come una netmask, indirizzi di server DNS etc.. L'interazione è di tipo broadcast, perché inizialmente gli IP di client e server non sono noti l'un l'altro. Il client invia un messaggio DHCP discovery, per capire se esiste un server DHCP; il server risponde con DHCP offer, in cui offre un IP, ed eventualmente il client può effettuare una DHCP request in cui lo richiede. Il server risponde con un DHCP ACK.

35)OSPF

E' un protocollo IGP basato sulla tecnica LINK STATE. La versione recente è la 3 che supporta IPv6. Supporta il ROUTING GERARCHICO, dove la rete è partizionata in aree. L'area di backbone si chiama AREA 0. I router si classificano come router interni ad un area, poi i gateway che legano 2 o più aree, e i router di backbone, quelli dentro l'area 0. I nodi in ogni area hanno una determinata topologia, e la conoscenza dei router rimane confinata alla sua area. L'OSPF opera a livello di trasporto, poiché incapsula i messaggi direttamente in datagrammi

36) Distance vector.

Si basa sull'esclusiva comunicazione con i vicini, a cui sono propagate le informazioni note; ogni router mantiene una tabella di tutti gli indirizzamenti noti, inizialmente riferiti solo alle reti a cui è connesso direttamente. Periodicamente, ogni router invia a tutti i vicini, cioè quelli collegati alla stessa rete fisica) un messaggio di aggiornamento contenente tutte le informazioni della propria tabella, cioè un vettore delle distanze. I router che ricevono tale messaggio aggiornano la tabella modificando le informazioni relative a cammini già noti, ed eventualmente aggiungendo cammini nuovi ad eliminando quelli non più disponibili.

37) IGMP.

IGMP è un protocollo che consente di gestire dinamicamente in ambito locale le informazioni di appartenenza degli end-system ai gruppi multicast. Permette quindi:

- Ai router di una rete di sapere quali end-system della propria rete appartengono ad un certo gruppo multicast, e di accettare richieste di unione.
- Agli end-system di conoscere a quali gruppi multicast si possono unire, e di effettuare richieste di unione.

Quando un dispositivo vuole ricevere contenuti multicast, invia un messaggio di adesione al gruppo, chiamati membership report. Il router prende nota di questa richiesta e si assicura che il traffico multicast per quel gruppo venga inoltrato al segmento di rete del dispositivo. Periodicamente i router inviano dei messaggi chiamati membership query per controllare se gli host sono ancora interessati a quel contenuto. Se un dispositivo non risponde, il router presume che non faccia più parte del gruppo e interrompe l'invio del traffico verso quella porzione di rete. Se un dispositivo decide di uscire da un gruppo multicast, può inviare un messaggio esplicito di leave group comunicando al router che non ha bisogno del traffico.

38) Assegnazione indirizzo ipv6.

Esistono varie modalità per attribuire un indirizzo IPv6 ad un'interfaccia host. C'è la possibilità di assegnare in maniera statica da parte dell'amministratore, o in maniera dinamica. I metodi di assegnazione dinamica sono due:

- Generazione automatica: in cui un indirizzo è generato dal sistema operativo e i restanti sono determinati con la comunicazione dei messaggi ICMPv6.
- Generazione da parte di un server DHCPv6: in cui il server conosce gli indirizzi delle macchine, mentre nella generazione automatica gli indirizzi sono ignoti.

39) Distance vector con le soluzioni al problema della slow convergence adottate da RIP.

La slow convergence si verifica quando si ha un cambiamento nella topologia della rete, quindi impiega molto tempo per propagarsi a tutti i nodi. Durante questo processo, le informazioni sbagliate possono essere trasmesse ripetutamente, causando instabilità. In questo caso il RIP adotta due soluzioni:

- Split Horizon: una regola che impedisce a un nodo di pubblicizzare una rotta a un vicino da cui ha appreso quella stessa rotta. Esso previene i loop semplici, poiché un nodo non rinvia informazioni ritondanti nella direzione da cui le ha ricevute.
- Poison Reverse: una variante dello Split Horizon in cui il nodo pubblicizza attivamente al vicino da cui ha appreso una rotta che quella rotta non è più valida, utilizzando una distanza infinita.
- Hold-Down Timers: quando un nodo rileva che una rotta è inaccessibile, ignora gli aggiornamenti di routing che indicano che la rotta è nuovamente accessibile per un certo periodo. Esso riduce la propagazione di informazioni errate durante la convergenza e fornisce il tempo necessario per stabilire la topologia.
- Triggered Updates: un nodo invia immediatamente un aggiornamento di routing quando rileva un cambiamento significativo nella topologia e accelera la propagazione delle informazioni corrette, riducendo il tempo di convergenza.
- Maximum Hop Count: RIP utilizza un limite massimo di hop, solitamente 15; se un percorso richiede più di 15 hop, viene considerato infinito, quindi mitiga il problema del count-to-infinity, limitando la durata dell'inconsistenza della rete.

40) Crittografia a chiave pubblica.

La crittografia a chiave pubblica è un sistema crittografia che utilizza una coppia di chiave per garantire la sicurezza delle comunicazioni:

1. Chiave pubblica: utilizzata per cifrare i messaggi o verificare le firme digitali. Questa chiave è condivisa pubblicamente e può essere conosciuta da chiunque.
2. Chiave privata: visualizzata per decifrare i messaggi o firma digitali. Questa è segreta e deve essere conosciuta solo dal proprietario.

41) RSA

L'RSA è l'algoritmo più diffuso e utilizzato della crittografia a chiave pubblica. Per il suo funzionamento, si scelgono due numeri primi molto grandi p e q e si calcola il loto prodotto n=pq e il prodotto tra i precedenti z=(p-1)(q-1). Poi si sceglie un numero intero 'e' tale che 1<e<z e che non abbia fattori comuni con 'z'. Si sceglie, poi, un numero d tale che la divisione interna 'ed' e 'z' sua 1, quindi che 'ed-1' sia esattamente divisibile per 'z', ovvero 'ed=1'. Così otteniamo la chiave pubblica data dalla coppia (e,n) e la chiave privata dalla coppia (d,n). Supponiamo che il mittente voglia inviare un messaggio 'M' al destinatario. Quindi, trasforma questo messaggio 'M' in un numero intero 'm', tale che 0≤m<n. Calcola il messaggio cifrato 'c' utilizzando la chiave pubblica del destinatario: $c=m^e$. Il destinatario usa la sua chiave privata (d,n) per decifrare il messaggio: $m=c^d$. Il risultato viene convertito nel messaggio originale 'M'.

42) VLAN, come si implementano (disegno), VLAN trunking (quindi il tagging delle frame e la dimensione del vlan_id).

Una VLAN è una tecnologia che permette di segmentare logicamente una rete locale (LAN) in più reti separate a livello di data link, anche se i dispositivi sono fisicamente collegati allo stesso switch. Immaginiamo uno switch gestito con 8 porte, vogliamo dividere i dispositivi connessi in due VLAN, VLAN10 e VLAN20. Assegniamo le porte dello switch alle rispettive VLAN, quindi per VLAN 10 avremo porte 1-4 e per VLAN20 avremo porte 5-8. I dispositivi connessi alle porte 1-4 potranno comunicare solo tra loro, questo vale anche per le porte 5-8, ma non ci sarà comunicazione tra VLAN10 e VLAN20 senza un router o un dispositivo di routing inter-VLAN. Quando le VLAN devono estendersi su più switch o devono essere trasportate verso un router per l'intercomunicazione, è necessario utilizzare un VLAN trunk. Un trunk è una porta dello switch configurata per trasportare il traffico di più VLAN. Questo viene fatto aggiungendo un identificatore di VLAN (VLAN tag) ai frame Ethernet trasmessi sul trunk. Immaginiamo di aere una rete con due switch e un router:

- Switch 1 e switch 2:
  - VLAN10 porte 1-4
  - VLAN 20 porte 5-8
  - Porta 9 configurata come trunk
- Router: connesso al trunk per fornire routing inter-VLAN

[router]

I

(trunk)

I

Switch 1

VLAN10 VLAN20

Porte 1-4 porte 1-5

I

(trunk)

I

Switch 2

VLAN10 VLAN20

Porte 1-4 porte 1-5

Quando un dispositivo nella VLAN10 dello switch 1 vuole comunicare con un dispositivo nella VLAN20 dello switch 2, il frame è taggato con un VLAN ID e inoltra il pacchetto alla VLAN di destinazione tramite il trunk. Un router è necessario per inoltrare il traffico tra VLAN diverse, quindi il traffico passa al router, che decapsula il pacchetto, legge il VLAN ID e lo inoltra alla VLAN corretta.

43) Controllo della congestione in TCP.

Ogni volta che un buffer di un router rilevante nella connessione va in overflow, quindi c'è congestione, gli end-system hanno un ritardo maggiore. Per discutere della congestione serve la teoria delle code, una teoria che modella sistemi in cui ci sono due entità:

- Serventi: svolgono il servizio;
- Clienti: usufruiscono del servizio.

Tra i parametri del modello ci sono il tempo di servizio e il tempo di arrivo dei clienti, entrambi variabili casuali. Ci sono varie tecniche di prelievo di pacchetti della coda. Il più semplice è il modello FIFO, dove è presente un solo serviente, due mittenti e due riceventi. λ_i è tasso medio di arrivo dei byte dei pacchetti, mentre λ_{out} è il tasso medio di uscita dei byte dei pacchetti. Si suppone che il link di trasmissione abbia una capacità totale di R bit al secondo, mentre si suppone che il buffer del servente abbia capacità infinita e quindi non influenza la capacità della rete.

44) Perché si fa la pipeline?

La pipeline è una tecnica utilizzata nelle reti di calcolatori per migliorare l'efficienza e la velocità dell'elaborazione dei dati. La pipeline consente di suddividere un processo complesso in una serie di sotto-processi (o stadi), ognuno dei quali può essere eseguito in parallelo con gli altri. Questo significa che, mentre uno stadio della pipeline sta elaborando un dato, il successivo può iniziare ad elaborare il dato successivo. Ciò riduce i tempi morti e aumenta il throughput, ossia il numero di operazioni eseguite in un dato intervallo di tempo.

45-46) A cosa si riferiscono i numeri di sequenza? Perché non partono da zero?

Quando si stabilisce una connessione in TCP, con i suoi diversi step tra client e server, ci sarà anche una successiva fase di chiusura della connessione stessa. Quando si va ad effettuare la chiusura(4-handshake) sappiamo che il client resta in attesa di chiusura di un certo TIME_WAIT. Un numero di sequenza non è altro che un identificativo di ogni pacchetto, sia di dati sia di riscontro, che viene introdotto per una maggiore efficienza negli algoritmi. Il concetto di TIME_WAIT serve a evitare che i pacchetti andati persi nella connessione possano interferire con la nuova. Perciò è preferibile sia aumentare il TIME_WAIT sia introdurre nei numeri di sequenza delle cifre iniziali casuali, non partendo quindi dallo 0, in modo che i pacchetti della nuova connessione abbiano numeri di sequenza validi.

47) ALGORITMI STOP&WAIT,PIPELINING,SELECTIVE REPEAT, GO BACK N

Stop & wait : Per provvedere alla perdita di pacchetti, si introduce il tempo. Il mittente, una volta inviati i dati, effettua un conto alla rovescia, entro il quale si aspetta dal destinatario un ACK, altrimenti avviene un timeout e il mittente rispedisce gli stessi dati. Il destinatario può accorgersi che i dati sono gli stessi, a partire dal numero di sequenza, e quindi scarta la copia dei dati, ed invia l'ACK. Un timer troppo piccolo rispetto alla latenza di rete può far si che il riscontro ACK ancora non arrivi durante il timeout. Un timer troppo alto invece consente una latenza elevata. E' necessario stabilire un timeout opportuno.

Pipelining: Il mittente invia pacchetti prima di ricevere il riscontro dei precedenti. Maggiore è il gruppo di pacchetti inviati in una singola volta (insieme detto segmento) maggiore è l'utilizzo della linea. E' necessario un buffer del mittente per l'eventuale ritrasmissione di pacchetti senza riscontro. Il RAPPORTO DI UTILIZZO si calcola dividendo il tempo di trasmissione totale alla somma tra tempo di trasmissione del singolo pacchetto e il tempo di riscontro RTT(Round Trip Time), che sarebbe la distanza di tempo tra l'inizio della trasmissione e la ricezione del riscontro. Nel pipelining il tempo di trasmissione totale aumenta di un fattore N, quindi aumenta il rapporto di utilizzo. Il numero di sequenza di un header di un pacchetto assume valori da 0 a N-1, dove N è il numero di pacchetti nel segmento. Il mittente attende i riscontri,

e il segmento successivo sarà inviato dopo aver ottenuto il riscontro precedente. ACK ogni volta con i propri numeri di sequenza saranno inviati dal destinatario.

Go Back-N : Caso di pipelining semplice, dove solo il mittente ha il buffer, il ricevente no; Se si perde il pacchetto i-esimo del segmento,ogni pacchetto arrivato al ricevente che non sia quello, viene scartato e invierà un ACK con il numero di sequenza i-esimo. Il mittente non può rispedirlo perchè un ACK-i comporta l'invio del pacchetto con un nuovo numero di sequenza, non di quello vecchio perso. Si risolve quando scade il timeout per il mittente del pacchetto che doveva ricevere il destinatario. In questo il mittente invia la vecchia sequenza a partire da i, tornando indietro di N pacchetti.

Selective Repeat: Esiste un buffer anche per il ricevente, che contiene i pacchetti fuori ordine. Il mittente distingue i pacchetti non inviati, inviati senza riscontro, inviati con riscontro; ogni pacchetto che ottiene riscontro è rimosso dal buffer e comporta una traslazione della finestra di ricezione. Finchè c'è spazio nei buffer, t(x) e r(x) procedono normalmente. Affinché tutti i pacchetti ricevuti non in ordine e riscontrati siano accettati, quelli precedenti devono essere ricevuti e riscontrati.

In assenza di errori (Pe = 0) entrambi i protocolli usano il canale in modo ottimale e il throughput T_GBN = T_SR = 1 In presenza di errori (Pe > 0):

T_GBN = 1-Pe / (1+ Pe(N-1)) Ritrasmette tutti i pacchetti successivi a uno corrotto, riducendo il throughput. T_SR = 1-Pe Ritrasmette solo i pacchetti persi, mantenendo un throughput maggiore rispetto a Go-Back-N. Selective Repeat è più efficiente in presenza di errori, poiché evita ritrasmissioni ridondanti Il vantaggio cresce con Pe e dimensioni della finestra N.

48) RETI WIRELESS CON CONTROLLO DI COLLISIONI

Queste reti fanno uso di onde elettromagnetiche per trasformare info tra end-system. Le frequenze della WLAN sono dette bande ISM. E' strutturata come un insieme di terminali con supporto radio e che possono essere mobili, in quanto non vincolati da cavi, collegati a elementi centrali detti STAZIONI DI BASE o access point che offrono connettività wireless a un numero definito di terminali che rientrano nel loro raggio di azione, la "cella". In una rete wireless ad hoc non esiste nessun elemento di base, ma è formata solo da terminali, che collaborando effettuano il routing interno alla rete. A differenza delle reti cablate, le WLAN sono soggette a fading(attenuazione) e interferenze, e per via della riflessione si possono propagare in diversi cammini. Si utilizza il protocollo CSMA/CD.