

1 - Virtual Lan

Una VLAN è una rete LAN realizzata logicamente, isolata quindi virtualmente ma non fisicamente, da altre LAN Virtuali.

L'argomento delle VLAN si colloca **al livello di collegamento** dello stack TCP/IP

Definizione

La tecnologia della Virtual LAN permette di segmentare il dominio di broadcast di una LAN, suddividendola in più Lan Virtuali, isolate tra loro, ma che condividono la stessa infrastruttura fisica.

Una Virtual LAN, quindi, consente di:

- Separare host appartenenti allo stesso dominio di broadcast;
- Connettere host separati fisicamente, alla stessa rete logica virtuale

Vantaggi

- **Risparmio** - Si realizzano LAN Virtuali sulle stesse strutture fisiche, con notevole risparmio di tempo e denaro
- **Prestazioni** - I frame non vengono propagati verso destinazioni non necessarie, grazie al confinamento del traffico broadcast alla singola VLAN
- **Sicurezza** – Gli host possono vedere solo il traffico della loro VLAN
- **Flessibilità**
 - **Spostamento fisico di host:** l'host rimane collegato alla stessa VLAN senza riconfigurare gli switch
 - **Spostamento fisico di un utente nell'infrastruttura di rete:** l'utente può rimanere assegnato ad una VLAN, dopo una riconfigurazione degli apparati

Realizzazione

Due modi:

- **Port Based (Private VLAN):** lo switch assegna una VLAN a delle porte;
- **Tagged (802.1Q):** lo switch associa un indirizzo IP/MAC ad una VLAN;

Per gestire più VLAN, lo switch deve essere in grado di svolgere funzioni di:

- **Ingress:** capire la VLAN di provenienza del frame;
- **Forwarding:** capire la porta di destinazione del frame, in base alla VLAN di destinazione;
- **Egress:** trasmettere il frame in modo che la sua appartenenza alla VLAN venga correttamente interpretata da eventuali altri switch

Associazione

Due modi:

- **Statico:** Assegnazione su base porta
- **Dinamico:** Assegnazione su base MAC address

VLAN Trunking (Tagged), 802.1Q

Questo protocollo(VTP) permette di far condividere una VLAN su più switch.

Per fare questo, vengono aggiunti 4 byte (TAG) al frame Ethernet:

- TPID (Tag Protocol Identifier): contiene il tag EtherType che identifica il frame come 802.1Q;
- TCI (Tag Control Information):
 - PCP (Priority Code Point): priorità del frame (0-7);
 - DEI (Drop Eligible Indicator): designa il frame come scartabile in caso di congestione;
 - VID (VLAN Identifier): campo hex che identifica la VLAN di appartenenza del frame.

2 – Broadcast e Multicast

Le reti “**broadcast**” consistono in un unico canale di comunicazione che è condiviso da tutti gli elaboratori.

I pacchetti inviati da un elaboratore sono ricevuti da tutti gli altri elaboratori; un indirizzo all’interno specifica il destinatario.

Le reti broadcast, consentono anche di inviare un pacchetto a tutti gli elaboratori, in questo caso parliamo di **broadcasting**.

Si parla invece di **multicasting** quando vogliamo inviare un pacchetto soltanto ad un sottoinsieme degli elaboratori, in questo caso solo gli elaboratori del suddetto sottoinsieme prendono in considerazione il pacchetto, che viene ignorato dagli altri.

In ciascun pacchetto è presente un bit che indica che si tratta di una trasmissione in multicasting, mentre i rimanenti bit contengono l’indirizzo del gruppo destinatario ed i dati.

3 – Cos’è la metrica?

La **metrica** interviene nella caratterizzazione di un percorso per l’instradamento di pacchetti tra due nodi; serve per selezionare il percorso “migliore” e definisce quindi l’algoritmo di instradamento (Hop Count, Load, Delay, Bandwith, etc.)

4 – Cos’è un Trunk e cosa fa, cos’è il tagging?

Un **trunk** è un collegamento in grado di trasportare il traffico VLAN multiple.

Il **tagging** è una logica sviluppata per la comunicazione inter-switch in ambienti multi VLAN, nell’header di ciascuna trama è trasportato il VLAN-ID (**opera al layer 2**)

(fanno la stessa cosa)- le info tag viaggiano solo su collegamenti trunk

5 – Come si costruisce una Tabella di Routing?

Una tabella di instradamento (Routing Table) raccoglie le informazioni necessarie per individuare il percorso ottimale verso tutte le possibili reti, è composta dai seguenti campi:

- **Indirizzo IP di destinazione:** È il campo più importante contenuto nella Routing Table, quando un router riceve un pacchetto dati attraverso la sua porta di IN, controlla nella propria tabella di routing se esiste una entry per tale destinazione, ed in caso affermativo inoltra il flusso dati nella corrispondente porta di OUT.
- **Metrica:** Definisce l’algoritmo di instradamento (Hop Count, Load, Delay, Bandwith, ecc.)
- **Indirizzo del router di Next Hop:** È l’indirizzo del router successivo per raggiungere la rete di destinazione
- **Interface:** Interfaccia del router attraverso cui deve essere instradato il pacchetto verso il next hop
- **Timer:** Scandisce temporalmente ogni quanto tempo inviare gli updates ad i router vicini

6 – Protocolli a finestra scorrevole

I protocolli a finestra scorrevole (sliding window) permettono di inviare più di un frame prima di fermarsi per attendere il riscontro poiché in ricezione possono arrivare più frame consecutivi, i frame devono essere numerati per garantire in ricezione che non si siano persi frame: saranno dedicati n bit di controllo per la numerazione.

In ricezione non è necessario riscontrare tutti i frame: il ricevente può attendere di ricevere un certo numero di frame prima di inviare un solo riscontro cumulativo.

Per non avere sovrapposizione dei numeri identificativi tra i frame in attesa di riscontro, questi non dovranno essere in numero maggiore di 2^n (quindi saranno numerati da 0 a 2^n-1), quindi si avrà sempre $W \leq 2^n$; in funzione del protocollo usato si potranno avere restrizioni maggiori come per il **selective reject** che avrà la finestra $W \leq 2^{(n-1)}$ (quindi la metà dello spazio di indirizzamento dei frame)

7 - Differenze tra switch e switch Layer 3

Uno switch è un dispositivo di rete che agisce istradando i frame ricevuti e dirigendoli verso il dispositivo corretto.

Quindi uno switch opera tra dispositivi della stessa rete; mentre uno Switch Layer 3 svolge la stessa funzione, operando su più reti.

8 – Com'è fatta e su cosa si basa la fibra ottica?

La fibra ottica consiste in un cavo composto da un'anima trasparente di silicio avvolto in un rivestimento di vetro, la parte in vetro viene poi ricoperta da una guaina nera, si basa sulla rifrazione, può essere monomodale e multimodale, la migliore tra le due è la monomodale perché è diretta.

9 – Perché preferiamo la fibra ottica al rame?

La fibra ottica è da preferire al rame, poiché è immune dai disturbi elettrici/radio/climatici, ha un'ampia capacità di banda e un'elevata velocità di trasmissione.

10- Shannon e Nyquist (teorema del campionamento)

Nyquist dimostrò che un segnale a larghezza di banda B può essere ricostruito perfettamente campionando lo stesso al doppio della larghezza di banda, quindi a partire da $2B$ campioni del segnale stesso.

Shannon estese il lavoro di Nyquist a canali soggetti a rumore termico, secondo la dimostrazione di Shannon sarebbe possibile aumentare il tasso di trasferimento dei dati, aumentando il livello del segnale, tuttavia l'aumento del segnale comporta effetti collaterali (non linearità) che accrescono gli errori di ricezione.

11- Differenza tra link state e distance vector (routing dinamico).

In una logica link state gli aggiornamenti sono propagati uno ad uno a tutti i nodi nel dominio di routing. I protocolli distance vector sono invece più leggeri: ogni router misura la distanza che lo separa dai nodi adiacenti ricevendo i dati dai router vicini.

12- Capacità del mezzo trasmissivo (collegata a Shannon e Nyquist)

Con l'ausilio del teorema del campionamento, se utilizziamo un numero V di livelli trasmissivi equiprobabili, dato che la quantità di informazione associata è esprimibile come $Q = \log_2 V$, allora la massima quantità di informazione trasmessa in un canale non rumoroso è di $2BQ$. (primo teorema di Nyquist)

La massima informazione trasmessa in un canale con rumore termico è invece di $B_{\log_2}(1+S/N)$.

13- A livello data link, come viene gestita la collisione e la contesa?

La collisione viene gestita tramite 3 protocolli con cui i nodi regolano le loro trasmissioni e sono **Protocolli a suddivisione del canale** (slot di tempo, frequenza, codice) **protocolli ad accesso casuale** (slotted aloha, aloha puro, CSMA-CSMA/CD) e **Collision free** (token ring)

La contesa consiste nella trasmissione dei dati da parte di ciascuna sorgente, indipendentemente dalle altre. Essa viene gestita utilizzando il protocollo CSMA - CSMA/CD o protocolli collision-free (es. Token Ring).

(CSMA/CD = Carrier Sense Multiple Access Collision Detection)

14-Differenza tra Switch (livello data link) e ripetitore (livello fisico)

Il ripetitore opera al livello fisico, e permette la ritrasmissione del segnale in modo bidirezionale; lo Switch invece, opera a livello data link e permette di connettere più LAN.

15- Come fa lo switch ad imparare le informazioni di chi sta da una parte e di chi sta dall'altra?

Lo switch, riesce ad imparare le informazioni del mittente e del destinatario attraverso l'uso dell'indirizzo MAC, selezione i frame ricevuti e li dirige verso il dispositivo corretto, leggendo il MAC di destinazione.

L'instradamento avviene per mezzo di una corrispondenza univoca porta-indirizzo.

16- Con lo switch, come si gestiscono i loop nella broadcast storm? C'è un protocollo che usiamo? (spanning-tree protocol)

Sì, utilizziamo il protocollo spanning-tree che mantiene inattive alcune interfacce in modo da garantire che la rete rimanga connessa ma priva di loop.

17- Che differenza c'è, a livello di rete, tra l'attività di forwarding (hardware) e routing(instradamento)?

L'inoltro o forwarding è il processo che, in base all'indirizzo fisico di destinazione, sceglie la linea di uscita in funzione di dati noti (tabelle, stato delle linee, etc.).

L'instradamento invece, è il processo di creazione ed aggiornamento della tabella (detta di routing), che associa alla destinazione la linea d'uscita da utilizzare; questa operazione viene eseguita in base ad algoritmi detti algoritmi di routing.

18- Come funziona il bit stuffing?

Il bit stuffing è una tecnica che consiste nell'aggiungere dei bit a zero ad un flusso di dati numerici.

Tali bit aggiunti non trasportano informazione, ma vengono utilizzati per prevenire che i dati siano interpretati come dati di controllo. Nel framing ad esempio, per evitare che il flag byte possa trovarsi all'interno dei dati del pacchetto, viene inserito un bit 0 dopo ogni gruppo di 5 bit a 1; il bit inserito viene eliminato in ricezione.

19- Cos'è e come funziona lo spanning-tree protocol

L'STP è un protocollo "loop free" utilizzato per realizzare reti con percorsi ridondanti utilizzando tecnologie di livello datalink.

Nell'STP viene localizzato il "root bridge" (nodo debole), successivamente vengono localizzati i loop che vengono poi risolti bloccando le porte.

20-Cos'è la tabella di routing e come funziona?

La tavola di routing contiene tutte le informazioni necessarie per indicare il percorso ottimale verso le possibili reti. La tavola deve contenere l'indirizzo IP di destinazione, l'indirizzo dei router adiacenti ed i possibili percorsi.

21-Chi è che immette i dati nella tavola di routing?

Ci sono due possibili casi, nel caso statico li immette l'amministratore di rete; nel dinamico invece vengono aggiunti attraverso i protocolli di routing.

22-Cos'è il DNS? Qual è la query ricorsiva ed iterativa? Quali sono i vari servizi del DNS

Il DNS (Domain Name System) è un database distribuito(ogni sito mantiene il suo database relativo agli host locali eseguendo su una macchina il **server DNS** che può essere interrogato da altri sistemi su internet) che permette di convertire i nomi simbolici degli host negli indirizzi IP numerici. Il resolver è la procedura che effettua la conversione.

Le caratteristiche principali sono:

- Database distribuito
- Basato sul modello client/server
- 3 componenti principali
 - **Resolver**
 - **Spazio dei nomi**
 - **Name server**
- Accesso veloce ai dati

Nella query iterativa la negoziazione con i vari name server autoritativi per le zone interessate è gestita direttamente dal resolver.

Nella query ricorsiva il resolver propaga la richiesta al name server di livello superiore che gestisce la stessa negoziando con gli altri name server nella gerarchia (la risposta viene propagata all'indietro)

Oltre alla traduzione il DNS fa anche da host aliasing (semplifica il nome degli host complicati e lunghi), Mail serve aliasing e distribuzione del carico tra server replicanti di un web server affollato

23- Distance vector (problemi di hop count infinito, split horizon, hold down timer)

L'instradamento distance vector, noto anche come routing di Bellman-Ford perché basato sull'omonimo algoritmo, è un tipo di algoritmo di routing dinamico, che tiene conto del carico istantaneo della rete.

I router che utilizzano questo protocollo, prelevano informazioni dai router (nodi) adiacenti.

Il routing basato su distance vector è soggetto a diversi problemi, ovvero, problema del conteggio infinito, non tiene conto della capacità delle linee e converge in tempi molto lunghi.

Parziali soluzioni:

- 1- **Split horizon:** Un router, quando inoltra la propria tabella di routing ad un router vicino, omette i percorsi che ha appreso da quel vicino
- 2- **Route poisoning:** dove tutti i router settano la distanza di ogni router che passa dallo stato di down ad infinito così da boicottare quella strada.

24-Differenza UDP livello trasporto con livello network(rete)

UDP definisce un protocollo senza connessione che permette di inviare datagram IP senza stabilire una connessione. UDP maneggia i dati in un unico segmento, mentre IP eventualmente lo spezzetta e poi UDP lo riceve nuovamente come un unico segmento

25-Il trunk nel livello trasporto riguardante le VLAN TCP.

(LA RISPOSTA È NELLA DOMANDA 1)

26- La modulazione (ampiezza, fase e frequenza)

La modulazione è un processo con il quale il segnale da trasmettere (segnale modulante) viene utilizzato per modificare nel tempo le caratteristiche di un segnale ausiliario sinusoidale (portante).

Il segnale modulante viene utilizzato per modulare le caratteristiche della portante:

- **ampiezza**: il segnale viene utilizzato per modificare il valore della ampiezza della portante (modulazione di ampiezza)
- **frequenza**: il segnale modulante modifica istante per istante la frequenza della portante (modulazione di frequenza)
- **fase**: il segnale modulante cambia la fase della portante (modulazione di fase)

27-L'indirizzo MAC ha validità universale?

No, non è possibile trovare 2 MAC address uguali su due differenti segmenti di rete.

28- Cos'è il BGP (Border Gateway Protocol)?

Il BGP è un gateway protocol per lo scambio di informazioni di instradamento tra sistemi autonomi, che tiene aggiornate le tabelle di routing.

29- Differenze tra TCP e UDP.

TCP definisce un protocollo di trasporto orientato alla connessione, mentre UDP definisce un protocollo senza connessione. TCP è affidabile a differenza di UDP.

Inoltre, UDP si occupa di un datagram per volta senza suddividerli, mentre TCP suddivide i datagram.

30- Porte TCP

Le porte TCP attive definiscono i servizi disponibili.

Per connettersi a un servizio specifico si deve conoscere il relativo numero di porta.

Le porte sono suddivise in tre gruppi:

- Well-Known-Ports: Queste porte vengono assegnate univocamente dall'IANA.
- Registered Ports: L'uso di queste porte viene registrato a beneficio degli utenti della rete, ma non esistono vincoli restrittivi.
- Dynamic / Private Ports: Non viene applicato nessun controllo all'uso di queste porte.

31- ?

32- Reti wireless

Le reti wireless sono reti che offrono mobilità senza perdita della connessione; hanno costi ridotti, e sono estendibili senza necessità di cablaggio.

33-Multiplazione e demultiplazione

La multiplazione permette di spedire più comunicazione all'interno dello stesso mezzo trasmissivo, 1 canale fisico, **n** canali logici, si aggregano i dati dei canali logici e alla ricezione il **demultiplexer** li ridivide fra i vari canali logici, ci sono varie tecniche di multiplazione e sono

- A divisione di tempo(TDM)
- A divisione di spazio(SDM)
- A divisione di frequenza(FDM e WDM)
- Per codifica(CDM)

34-Protocollo di routing interno ed esterno (igp ed egp)

Un protocollo di routing, è un protocollo di rete relativo allo strato network che permette ai router di scambiarsi informazioni tra loro al fine di costruire delle tabelle di routing permettendo così il corretto instradamento dei pacchetti.

Il collegamento di più reti sotto un unico dominio amministrativo prende il nome di **AUTONOMOUS SYSTEM(AS)**. I router che instradano messaggi all'interno dello stesso AS e non hanno diretta connessione con altre reti(network) esterne, sono chiamati **Interior router** e scambiano info di instradamento tramite un **igp** (Interior gateway protocol)- es di protocolli igp – RIP(basato su distance vector, utilizzato per le aree piccole),OSPF(tipo link state, protocollo più diffuso in rete)

Mentre i router che instradano i messaggi tra AS diversi sono detti **Exterior Router**, scambiano info di instradamento utilizzando un protocollo **egp** (Exterior Gateway Protocol)

Mentre i router che fungono da “ponte di collegamento” tra AS diversi si chiamano **Border Router**

35-Differenza tra IPv4 ed IPv6

La differenza più evidente, è la differenza nei formati:

IPv4 utilizza un indirizzo a **32 bit**

IPv6 utilizza un indirizzo **128 bit**

Ciò significa che IPv6 offre un numero di indirizzi 1.028 volte maggiore di IPv4, il che risolve essenzialmente il problema dell'“esaurimento degli indirizzi” (almeno per il prossimo futuro).

Un indirizzo IPv4 può essere mappato in un indirizzo IPv6 e consiste di 80 bit posti a 0 seguiti da 16 bit a 1, seguiti da un indirizzo IPv4 a 32 bit.

Un'altra opzione è il **tunneling** che consente di incapsulare pacchetti IPv6 in IPv4

36-Come funziona la posta elettronica(SMTP)

Consta di 3 componenti principali: **agente utente, server di posta e simple mail transfer protocol(SMTP-protocollo che definisce la sequenza di comandi inviati in ASCII necessaria per il trasferimento dei messaggi)**

L'agente utente è detto anche “mail reader” e utilizza programmi per leggere e gestire la posta

Il server di posta include la **casella di posta** (mailbox) e contiene i messaggi in arrivo per l'utente e usa il **protocollo smtp** tra server di posta per inviare messaggi di posta elettronica

37-Fibra monomodale e multimodale

All'interno di una fibra la luce può propagarsi in accordo a diversi modi (fasci di fotoni) simultanei o non simultanei in dipendenza dal tipo di fibra utilizzata:

-fibre ottiche multimodali: vi è la propagazione secondo diversi modi e percorsi simultanei

-**step-index** (ad indice di variazione a gradino/scatto)

-**graded-index**(o a indice di variazione graduale)

-Fibre ottiche monomodali: vi è la propagazione in un unico modo

-La fibra si comporta come una guida d'onda

-Maggiori distanze coperte

-Nessuna dispersione modale

38-Vlan trunk

Il Vlan Trunking Protocol (VTP) è un sistema/protocollo che diffonde le info di configurazione delle VLAN information e garantisce la consistenza delle configurazioni delle VLAN all'interno di un singolo dominio amministrativo, il VTP manda gli annunci solo sulle trunk ports, i router bloccano la propagazione degli annunci VTP.

Ci sono 3 modalità operative:

- **Server mode:** possibile creare e rimuovere VLANs
- **Client mode:** non può modificare configurazioni VLANs
- **Transparent:** possibile creare/rimuovere VLANs localmente, ignora e fa passare annunci VTP

Gli annunci sono inviati come trame multicast:

- Periodicamente
- Su base richiesta
- In presenza di modifiche

(risolve in parte il problema dell'interscalabilità tra le VLAN)

39-Rilevamento errore a livello datalink

Per la rilevazione di errori, nell'header di ogni trama il livello 2 inserisce un campo denominato **checksum** che è il risultato di un calcolo fatto utilizzando il bit della trama, la **destinazione** ripete il calcolo e confronta il risultato con il checksum, se coincide la trama è corretta.

Altri controlli:

- Bit di parità/parità bidimensionale
- Campi di Galois
- CRC (cyclic Redundance Checksum)
- Codifica polinomiale che il sender e il receiver si accordano sull'utilizzo di un polinomio generatore di grado r in modo che il polinomio associato ai bit del frame trasmesso sia divisibile per quest'ultimo

40-IP forwarding (instradamento)

La funzione principale dello strato di rete è l'instradamento (routing), questo è il processo che permette al router di scegliere (tramite un algoritmo come: distance vector o link state) la linea di uscita verso cui instradare i dati.

Concettualmente si possono distinguere due operazioni:

- **Inoltro**(forwarding): il processo che, in base all'indirizzo di destinazione o al circuito virtuale, sceglie la linea di uscita in funzione ai dati noti (tabelle stato delle linee ecc)
- **Instradamento:** il processo di creazione ed aggiornamento della tabella che associa alla destinazione la linea di uscita da utilizzare; questa operazione viene eseguita in base ad algoritmi detti: algoritmi di routing

41-Routing table

Per poter instradare in modo corretto i vari pacchetti che girano nella rete un router ha bisogno di avere alcune info fondamentali come:

- Indirizzo ip dell'host di destinazione
- Indirizzo dei router ad esso adiacenti da cui poter ricavare le info delle varie reti e sottoreti remote raggiungibili
- I possibili percorsi alternativi (per raggiungere la meta)
- Il miglior percorso verso ciascuna delle reti remote non direttamente connesse ad esso

Una tabella di instradamento (routing table) raccoglie le info necessarie per individuare il percorso ottimale verso tutte le possibili reti

42-Cos'è il collo di transito

????

43-Problemi che causano il distance vector, ci sono altre tecniche per ovviare a questi problemi?

Il Distance vector è un algoritmo adattivo sviluppato attorno al 1960, l'idea è quella di partire dal nodo sorgente e cominciare a guardare i nodi adiacenti assegnando loro il valore del costo per raggiungerli iterando il ragionamento per ciascuno dei nodi raggiunti, se il grafo ha $|V|$ nodi, dopo $|V|-1$ iterazioni tutti i nodi avranno assegnato il costo minimo per essere raggiunti dal nodo sorgente. E' un algoritmo di facile implementazione ma è sconsigliato per le reti di vaste dimensioni poiché lento a convergere in quanto converge alla velocità degli elementi più lenti, in dettaglio questo tipo di algoritmi funziona mantenendo una tabella contenente la più piccola distanza conosciuta per ogni destinazione e quale canale utilizzare per raggiungerla, queste tabelle sono aggiornate scambiando info con i propri vicini. La problematica di questo algoritmo è che si possono creare loop in quanto ogni router memorizza solo il primo passo dei percorsi che ha nella tabella, questo implica se per esempio A pubblica un percorso verso C, i vicini di A non possono sapere se sono stati inclusi da A nel percorso calcolato quindi implica sia la formazione di cicli e quando si interrompe si può avere un collegamento **count-to-infinity** (non si può arrivare ad un router nonostante un router diverso dice che si può arrivare) si possono usare due soluzioni per evitare i loop e il count-to-infinity:

- 3- **Split horizon:** Un router, quando inoltra la propria tabella di routing ad un router vicino, omette i percorsi che ha appreso da quel vicino
- 4- **Route poisoning:** dove tutti i router settano la distanza di ogni router che passa dallo stato di down ad infinito così da boicottare quella strada.

44-Cos'è il grafo di rete?

Il concetto è quello di costruire un grafo della rete, dove ogni nodo del grafo rappresenta un router ed ogni arco del grafo rappresenta una linea di comunicazione (chiamata **canale**). Per scegliere un percorso tra due router, l'algoritmo cerca nel grafo il cammino più breve tra di essi

45-Come si costruisce la tavola di routing a partire dal grafo di rete? Con quali informazioni vengono propagate?

46-Esempi di protocolli di rete

DNS (Domain Name System) è la Risoluzione dei nomi degli host

SMTP(Simple Mail Transfer Protocol)

http(HyperText Transfer Protocol)

47-backward e forward

48-piggy backing

Per motivi di efficienza si usa la tecnica del piggybacking, una tecnica nel quale, per evitare di dover costruire e trasmettere un frame ACK si dedica un campo dell'header di un frame di dati per trasportare l'ACK della trasmissione in senso inverso, quindi quando si deve trasmettere un **ACK**, si aspetta di dover trasmettere un frame dati che possa trasportare l'info di ACK

49-A livello di trasporto cosa serve per il sequence number?

(forse) il sistema di enumerazione e di riscontro dei dati inviati, TCP numera ogni byte trasmesso, per cui ogni byte ha un numero di sequenza, nell'header del segmento TCP è trasportato il numero di sequenza del primo byte nel segmento stesso, il ricevitore deve riscontrare i dati ricevuti inviando il numero di sequenza dell'ultimo byte ricevuto correttamente ed in sequenza +1 (next expected byte)

50-3 way handshaking

E' un metodo utilizzato in una rete TCP/IP per creare una connessione tra un host/client locale ed un server, si tratta di un metodo a 3 fasi che richiede sia al client che al server di scambiare i pacchetti SYN e ACK prima dell'inizio della comunicazione dei dati

- Un client invia un pacchetto dati SYN su una rete IP a un server sulla stessa rete o a una rete esterna. L'obiettivo di questo pacchetto è di chiedere se il server è disponibile per nuove connessioni.
- Il server di destinazione deve disporre di porte aperte in grado di accettare e avviare nuove connessioni. Quando il server riceve il pacchetto SYN dal nodo client, risponde e restituisce una ricevuta di conferma, il pacchetto ACK o SYN/ACK.
- Il client riceve il SYN/ACK dal server e risponde con un pacchetto ACK.
- Al termine di questo processo, viene creata la connessione e l'host e il server sono in grado di comunicare.

Quando si vuole chiudere la connessione

- 1- Il client invia un segmento di controllo FIN al server
- 2- Il server riceve il segmento FIN e risponde con un ACK. Chiude la connessione ed invia un FIN
- 3- Il client riceve FIN e risponde con un ACK (inizia l'attesa temporizzata) risponde con un ACK ai FIN che riceve (se l'ACK di un messaggio FIN si perde dopo un'attesa temporizzata si chiude comunque la connessione)
- 4- Il server riceve un ACK. La connessione viene chiusa

51-Differenza tra ripetitore- switch e router

Un ripetitore opera al livello fisico amplificando e ritrasmettendo il segnale in modo bidirezionale, ha più porte (>2) ed è spesso definito **hub**, uno **Switch** permette di interconnettere più LAN mantenendo la suddivisione a livello data link, si possono collegare LAN operanti con protocolli diversi e si creano domini di collisione separati diminuendo il carico di ciascuna sottorete. **Router** invece è considerata come una stazione intermedia che opera al livello 3 e inoltra i pacchetti attraverso sottoreti diverse permettendo l'interoperabilità a livello di indirizzamento.

52-Differenza tra FDM, WDM e TDM

Sono tutte tecniche di moltiplicazione, la TDM è una tecnica a divisione di tempo (ogni intervallo temporale si chiama **slot**) che utilizza una stessa connessione per più trasmissioni distinte, richiede la tramatura dei flussi e l'uso di multiplexer e demultiplexer, è meno efficiente ma ottimizza l'uso dei mezzi trasmissivi.

Mentre la FDM utilizza la trasmissione in banda passante, dividendo lo spettro in bande di frequenza separate, una per canale e nessuna coppia di canali può condividere la stessa porzione di spettro, per ovviare a fenomeni di interferenza si lascia uno spazio (bande di separazione o di guardia). La differenza tra FDM e WDM è che gli **FDM** sono modulati su frequenze diverse mentre per **WDM** sono modulati su diverse lunghezze d'onda.

53-Differenze tra TDM sincrono e statistico

Deterministico: Ogni canale di comunicazione è identificato dalla sua posizione in termini di slot temporali all'interno della trama. Questa correlazione fissa fra il canale di comunicazione e il relativo timeslot è il principale svantaggio del TDM deterministico: se il canale non è usato comunque occupa il timeslot inviando un pattern idle

Statistico: non esiste correlazione fra canale di comunicazione e relativo timeslot. La capacità del mezzo è distribuita statisticamente fra gli utenti che ne concorrono all'uso. E' necessario uno schema separato di

tramatura ed indirizzamento per garantire le associazioni dinamiche: se un canale non è usato gli altri possono disporre della sua capacità trasmissiva.

54-Quale tecnica TDM è più adatta per la trasmissione dati su una rete di computer?

55-Identificazione MAC

Indirizzo mac è l'analogo al numero di codice fiscale di una persona, ha una struttura orizzontale e non varia a seconda del luogo in cui la persona si trasferisce (indirizzo a 48 bit per la maggior parte delle LAN)

(se inteso come sottolivello MAC) è specifico di ogni LAN e risolve il problema della condivisione del mezzo trasmissivo, esistono vari tipi di MAC basati su principi diversi quali, la contesa, il token, la prenotazione round robin.

Il MAC è indispensabile in quanto a livello 2 (data link) le LAN implementano sempre una sottorete trasmissiva di tipo **broadcast** in cui ogni sistema riceve i frame inviati dagli altri

56-Differenza tra switch layer 2 e layer 3

Lo switch tradizionale opera al livello Data link (layer 2) mentre lo switch che opera al livello rete (layer 3) integra funzioni di livello 3

57-Rete gerarchica(ospf)

OSPF (open short path first) è stato sviluppato nel 1988 ed è oggi il più diffuso protocollo IGP utilizzato in internet, è un algoritmo capace di reagire dinamicamente e rapidamente ad eventi che modificano la topologia della rete. Supporto per il tunneling e supporto per sistemi gerarchici (routing gerarchico anche all'interno dello stesso AS)

58-Fisicamente, di che ha bisogno il pc per la trasmissione dei dati?(ha bisogno di un'antenna che serve per la ricezione e trasmissione)

59-Link state

È una classificazione dei protocolli di routing introdotti nel 79 e si basa sull'invio di pacchetti contenenti le info di costo e di ritardo relativi a ciascun link ai nodi adiacenti, ogni nodo utilizza queste informazioni per calcolare il costo minimo verso tutti i nodi a lui noti, mentre l'aggiornamento è propagato uno ad uno a tutti i nodi nel dominio di routing attraverso il flooding(ogni pacchetto è inviato su ogni linea in uscita eccetto quella da cui è arrivata)

60-Multiplazione statistica

(già risposta domanda 53)

61-Dopo quante ritrasmissione si arresta la trasmissione di un frame?

16

62-Come funziona, nel TCP, il controllo della congestione?

Il sender percepisce la congestione con la perdita di pacchetti e di conseguenza un evento di perdita si può esprimere con **timeout e ricezione di 3 ACK duplicati**.

L'algoritmo ha 3 componenti principali:

- **Incremento additivo e decremento moltiplicativo**

Decremento riduce a metà **CongWin** (finestra di congestione) dopo un evento di perdita mentre aumenta lentamente il **congrwin** nell'incremento additivo

- **Partenza lenta**

Si inizia una connessione con **CingWin** impostato a 1ms e se va bene il sender aumenta il ritmo esponenzialmente

- **Reazione ad eventi di timeout**

3 ACK duplicati o timeout, il sender entra nella fase di partenza lenta, il sender aumenta il valore in modo esponenziale finché **congWin** raggiunge una soglia

63-Indirizzi di rete

64-Diafonia

La diafonia è un fenomeno di accoppiamento elettrico tra mezzi trasmissivi vicini non isolati adeguatamente, il segnale trasmesso su un cavo genera per induttanza un segnale corrispondente nel cavo vicino che si sovrappone al segnale trasmesso in quest'ultimo

65-Differenza tra bridge locale e remoto

66-Principali applicazioni delle reti locali wireless

Una WLAN è un sistema di comunicazione dati molto flessibile e può essere utilizzato come estensione o anche alternativa alle normali LAN su cavo, usata principalmente su pc portatili offre mobilità senza perdita di connessione ed ha come vantaggi la **semplicità di installazione, la flessibilità di installazione i costi e la scalabilità**

67-Tecniche per fronteggiare l'esaurimento degli indirizzi IP

Per risolvere il problema della carenza degli indirizzi IP è stata sviluppata una tecnica chiamata subnetting, un'organizzazione può usare i bit rimasti per indirizzare gli host per creare altre reti interne alla principale, per identificare quali bit definiscono la rete e quali l'host si utilizza una maschera di sottorete.

68-Cos'è e come si misura il NEXT, quali mezzi trasmissivi riguarda?

69-Si può utilizzare una LAN broadcast utilizzando mezzi trasmissivi punto-punto?

70-Significato del protocollo ARP e funzionamento

È un protocollo per la risoluzione degli indirizzi ed è composto da una tabella che contiene la corrispondenza tra indirizzi IP e MAC, ogni nodo IP (host, router) nella LAN ha una tabella ARP

71-Nei doppini si usa una tecnica di trasmissione bilanciata o sbilanciata

72-Diff tra una rete a commutazione di circuito e commutazione di pacchetto

Una rete a commutazione di **pacchetto** è un metodo di comunicazione che suddivide un messaggio in parti più piccole (pacchetti) prima di inoltrarle al destinatario dove ogni pacchetto segue un proprio percorso per arrivare al destinatario che dovrà riassemblare il messaggio (ottimizza l'impiego della rete). Mentre nella rete a commutazione di **circuito**, il canale viene assegnato esclusivamente alle due stazioni, fino al termine della comunicazione (più flessibile)

73-Differenza tra un servizio di file transfer (esempio: FTP di TCP/IP) ed un servizio di file system distribuito?

74-Cos'è l'SNMP? A che livello di ISO/OSI si colloca?

È un protocollo di rete e si occupa della gestione di apparati di rete, nel livello applicazione

75-Qual è quel protocollo che, nella rete internet, è utilizzato da qualunque applicazione debba trasmettere una qualsiasi informazione? Che tipo di servizio fornisce?

76-Elencare e spiegare il significato dei parametri necessari per la configurazione di un calcolatore collegato a una rete TCP/IP

77-Descrivere il funzionamento dell'applicazione traceroute, per quale motivo la rotta fornita da questa applicazione potrebbe essere inconsistente?

78-descrivere il funzionamento dell'applicazione ping

Viene usata per misurare il tempo (espresso in millisecondi) di un pacchetto ICMP per arrivare a destinazione e tornare all'origine

79-Che cos'è la rotta di default? Come si rappresenta?

Il default gateway è presente nell'ultima riga della tabella di instradamento ed è rappresentato con tutti zero sia nel campo prefisso di destinazione che nel campo subnet mask, **router verso cui è inviato il traffico diretto ad una destinazione non presente nella tabella di routing**, la route di default specifica l'instradamento di tutti i pacchetti per i quali la tabella di instradamento non fornisce una route esplicita

80-Descrivere il problema dell'instradamento

81-TCP implementa un ARQ di tipo go-back-n o ritrasmissione selettiva?

(Sliding windows)Go-back-n con timeout (dopo di che vi è la ritrasmissione dei dati), questa opzione permette di utilizzare il selective reject. Il go-back-n utilizza una finestra di dimensione N contenente un numero di pacchetti non ancora riscontrati, se un pacchetto con num di seq. N è ricevuto correttamente ed è in ordine, il receiver invia un ACK cumulativo per il pacchetto n ed invia i dati allo strato superiore

82-Che cos'è un VCI?

83-Descrivere il funzionamento di un codice CRC

Basato sul concetto di codice ciclico, in cui permutando ciclicamente gli elementi di una qualsiasi combinazione, si ottengono sempre combinazioni dello stesso codice

84-Illustrare le funzionalità fornite dai sottostati MAC e LLC dello standard IEEE 802

Il sottolivello LLC è comune a tutte le LAN, mentre il MAC è peculiare di ciascuna LAN, così come il livello fisico al quale è strettamente associato. Il sottolivello LLC è l'interfaccia unificata verso il livello Network ed è descritto nello standard IEEE 802.2 mentre i vari MAC sono descritti negli standard specifici di ogni rete locale

85-Protocollo TCP

IP è il protocollo di rete della suite TCP/IP

86-In un protocollo di routing di tipo distance vector: cosa contengono i messaggi inviati dai router?

Informazioni di routing

87-Che cos'è una porta effimera?

88-CSMA/CA 1 persistente, non persistente e p-persistente

1-persistente: perché quando trova il canale occupato resta in ascolto continuamente, ed appena il canale si libera trasmette con probabilità 1(sempre)

Non Persistente: si differenzia perché una stazione quando vuole trasmettere e trova il canale occupato non trasmette subito ma attende un tempo casuale e prova a ritrasmettere

P-persistente: In p-persistente il tempo è diviso in slot e quando una stazione vuole trasmettere e trova il canale occupato ascolta continuamente e quando lo trova libero trasmette con probabilità p, oppure attende uno slot successivo per trasmettere con probabilità (1-p) o ancora attende lo slot successivo e trasmette sempre con probabilità 1-p

89-CSMA/CD

Il protocollo opera in 3 diverse fasi:

- 1- **Carrier sense:** ogni stazione che deve trasmettere ascolta il bus e decide di trasmettere solo se questo è libero
- 2- **Multiple access:** nonostante la prima fase è possibile che due stazioni trasmettono contemporaneamente
- 3- **Collision detection:** se si verifica la sovrapposizione di due trasmissioni si ha una collisione, per rilevarla ogni stazione, mentre trasmette un pacchetto, ascolta i segnali sul mezzo trasmissivo, confrontandoli con quelli da lei generati, (si usa il jamming per eliminare la trasmissione)

Nb il tempo di propagazione dev'essere $2T_{ao}$

90-Time To Live

Numero massimo di hop rimanenti, dopo il pacchetto viene eliminato, è un contatore che viene decrementato via via che il pacchetto viaggia in rete

91-Cos'è un DS(distribution system)

È uno strato residente in ciascun AP è viene usato come dorsale di una WLAN in modo da far comunicare 2 AP differenti

92- FHSS vs DSSS

Il direct sequence ha la codifica ridondante grazie all'utilizzo di chip, dove ogni bit viene codificato ed è più immune ai rumori mentre nella frequency hopping è più sicura in quanto sono disponibili 79 diversi canali e dove dopo ogni comunicazione si salta in una frequenza diversa

93-Protocollo di accesso al mezzo per le WLAN

Il protocollo di accesso al mezzo per le wlan è il CSMA/CA con collision avoidance (evita collisioni ma non le rileva in quanto per farlo il canale deve sia trasmettere che ricevere), la stazione ascolta (un tempo DIFS) se il canale è libero e trasmette altrimenti aspetta un tempo casuale, quando il receiver riceve aspetta anche lui un tempo (SIFS) e invia un riscontro al server, non elimina del tutto le collisioni. **(back-off esponenziale con numero random)**

94-Stazione nascosta

La stazione nascosta nella WLAN è quando ci sono 3 stazione A,B,C dove B vede C e A ma A e C non si vedono e cercano di comunicare entrambi con B, questo dà vita ad una collisione, se invece è B a trasmettere ad A, C non trasmette perché trova B occupata

95-In cosa consiste il protocollo CSMA/CA

La stazione che vuole trasmettere A invia un frame chiamato RTS (request to send) al ricevente che se è libero risponde con un altro frame CTS (clear to send) ad B , (anche eventuali stazioni nascoste vedono questo frame e non trasmettono) ed inizia la comunicazione tra A e B.

96-I compiti dello strato di rete

Evitare sovraccarichi, scegliere la strada migliore per far recapitare i dati, reagire a modifiche di topologie e risolvere problemi connessi al transito attraverso reti differenti

97-Differenza tra instradamento connected oriented e connectionless

Il servizio senza connessione richiede che i pacchetti siano instradati indipendentemente l'uno dall'altro, ogni pacchetto quindi deve contenere l'indirizzo di destinazione mentre con l'instradamento connection oriented l'idea di base è di associare ad una connessione un circuito virtuale nella sottorete e tutti i pacchetti appartenenti alla stessa connessione seguiranno la stessa strada l'instradamento dei pacchetti sarà fatto in base alla sua appartenenza ad una connessione e non alla sua destinazione

98-longest prefix match

Un indirizzo di destinazione può corrispondere a più di una voce della tabella di inoltro del router, la scelta viene sempre fatta verso la rete (adatta) che ha la maschera più lunga (matching), numero maggiore di bit in comune

99-II CIDR

È il meccanismo di base per la scalabilità di internet, gli indirizzi vengono allocati e distribuiti in blocchi contigui, aggregando si riesce a contenere la dimensione delle routing tables

100-In che modo un host ottiene un indirizzo da una rete?

Tramite il DHCP, ottiene un indirizzo dinamicamente dal server di rete, in modo "plug and play"

101-Cos'è l'ICMP

Protocollo utilizzato per monitorare il funzionamento del livello di rete, ed ha lo scopo di notificare allo strato di rete i problemi nella comunicazione a livello3

102-Cos'è e cosa fa il NAT

Il router traduce gli indirizzi interni in esterni, mappando indirizzi e porte nella NAT table

103-Come fa un host che deve inviare un pacchetto dati a sapere che un altro host appartiene alla stessa rete?

Analizzando il suo indirizzo e facendo l'AND logico e tramite la tabella ARP fa l'associazione, questo protocollo non fa altro che inviare in modo broadcast una ARP request su tutta la rete, solo chi ha quell'indirizzo IP con quel numero di MAC processa questo pacchetto e risponde con un pacchetto ARP response. Per migliorare le prestazioni un host può avere un'ARP cache in memoria (con tempo di scadenza)

104-Quando usare il route statiche

La route statica prevede il percorso statico e viene inserito dall'amministratore di rete quando la linea è ancora offline ed è utile nelle route ad un'unica connessione o per le route con un percorso ben definito.

105-Routing dinamico

Il **routing dinamico** si basa in tempo reale e si cambia percorso in base a congestione di rete ecc, ci sono dei protocolli utilizzati da router per costruire le tabelle che contengono le info di instradamento dei pacchetti, per costruire la tabella un router dovrà scambiare dei pacchetti informativi con i routers ad esso collegati

106-Flooding

Ogni pacchetto viene inoltrato su ogni linea eccetto quella da cui proviene, algoritmi di flooding usati come benchmark perché utilizzano sempre la strada più corta, ma molto inefficienti in quanto ogni pacchetto va a finire su tutte le linee della rete provocando inefficienza

107-Aggiornamento distance vector-link state

Distance vector gli aggiornamenti presenti sono inviati solo ai vicini direttamente connessi mentre l'aggiornamento nell'algoritmo link state si basa sulla propagazione degli aggiornamenti uno ad uno

108-Routing loops

Ogni nodo conserva la distanza fra se stesso e ogni possibile rete di destinazione ma una convergenza troppo lenta può portare a informazioni inconsistenti, soluzione **split horizon** (non si prende info sull'interfaccia circa lo stato di una route sulla stessa interfaccia da cui le stesse sono state acquisite)

109-Hold-down timers

Per evitare fluttuazioni alla ricezione di un annuncio il router setta un time di hold-down e accetta la modifica solo allo scadere dello stesso

110-Algoritmi di routing link state

Nel 79 al posto degli distance vector, si basa sull'invio di pacchetti contenenti le info di costo e di ritardo relativi a ciascun link ai nodi adiacenti, ogni router deve avere in memoria la mappa di tutta la rete e cooperare per crearla, mantenendola aggiornata, i router apprendono i primi n nodi vicini, associando ad ognuno di essi il costo della linea, l'info è propagata ai router della rete con un mex definito **link state packet** e la propagazione avviene con algoritmo di tipo flood, quando un nodo ha ricevuto le info dagli altri e costruisce il grafo di rete si usa Dijkstra per trovare i cammini minimi

111-Routing gerarchico

A causa della crescita esponenziale di internet, le tabelle di routing diventano sempre più grandi, quindi si divide il gruppo di router in regioni, ogni router conosce i dettagli della propria regione e come comunicare con le altre, ma non conosce la loro struttura interna.

112-I sistemi autonomi

Ogni organizzazione è composta da un insieme di router e LAN sotto una singola amministrazione, un algoritmo di routing è prescelto per aggiornare automaticamente le tabelle di instradamento che devono avere un'entry per ogni possibile destinazione (sia per le destinazioni locali che per quelle globali). Un AS definisce in maniera coerente le politiche di instradamento all'interno della sua organizzazione, quando due AS si uniscono per formare una inter-rete, occorre stabilire tra loro punti di collegamento o di **peering**

113-Relazione tra peering

I provider di transito garantiscono il passaggio del traffico fra i rispettivi customers, le info possono essere scambiate tra due AS solo se una sessione di peering è attiva (connessione TCP tra i due AS)

114-CIDR

115-Annunci BGP

BGP permette ad un AS di offrire connettività ad un altro AS tramite annunci (tecnica che permette di “richiedere” traffico). Gli annunci sono accettati solo se alcune condizioni sono verificate come una lista di prefissi validi ecc

116-Attributi BGP

In ingresso utilizzati per il filtraggio delle routes mentre in uscita per influenzare la selezione dei percorsi verso l'esterno

117-Med/metrica

Adotta la route associata più piccola, di default è 0 ed è usato sugli annunci in uscita per condizionare il comportamento del traffico in ingresso

118-Local preference

Attributo associabile agli annunci in ingresso, è utile per gestire le politiche di scelta sul traffico in uscita, di default 100

119-Stub network

Un router alla rete è scelto come gateway di default ed è connesso ad un singolo router dell'isp con una o più connessioni (instradamento statico senza bisogno di bgp)

120-Multi-homed stub networks

Due collegamenti allo stesso isp o isp differenti, per evitare single point of failure o per la divisione del carico, un pacchetto diretto ad internet può viaggiare su uno dei due link o su entrambi

121-Funzione del livello di trasporto

Fornisce una comunicazione logica tra due applicazioni che girano su due host differenti mascherando il fatto che tra due host esista una rete di qualsiasi tipo e topologia. Per assolvere alle sue funzioni lo strato del trasporto (**comunicazione logica tra processi di applicazioni che girano su host**) utilizza i servizi dello strato di rete (**comunicazione logica tra host**). Nel lato invio scinde i messaggi in segmenti e nel lato ricezione li riassembla

122-Protocolli servizio trasporto

Affidabile (TCP-connection oriented) e inaffidabile (UDP-connectionless)

123-Numero di porta

Il numero di porta (formato da un numero di 16 bit che va da 1 a 65535) del destinatario definisce il processo applicativo, indirizzo IP (host) + numero di porta (processo) formano la **socket**

124-socket

Una porta attraverso la quale i dati passano dalla rete al processo e viceversa

125- demultiplexing TCP vs UDP

Il demultiplexing, tecnica per demultiplare i dati alle applicazioni corrette può essere: **tcp** (orientato alla connessione) è dato grazie a 4 parametri che sono: - numero porta di destinazione/invio -indirizzo IP invio/destinazione, mentre l'**udp** (senza connessione) si identifica tramite il numero di porta di destinazione e IP di destinazione

126-TCP: funzionamento del controllo di flusso

Il receiver comunica lo spazio disponibile includendo il valore di **RcvWindows** (finestra di ricezione) nei segmenti, così il sender limita i dati non riscontrati a **RcWindows** in modo che il buffer di ricezione non vada in overflow (pacchetti smarriti o scartati, lunghi ritardi)

127-Segmento UDP

Il segmento UDP è costituito da un header di lunghezza fissata (8 byte) più il campo dati, che deve avere dimensione massima tale da stare dentro il campo dati di IP, poiché il pacchetto può essere lungo 65535 byte, utilizzato per le trasmissioni **broadcast o multicast**

128-Livello Sessione

Consente di stabilire una sessione tra applicazioni (scambio di info temporaneo tra due o più dispositivi), controllo del dialogo, gestione dei token e sincronizzazione, esempio di livello sessione: **Chiamata via internet basata sul protocollo SIP**

Esempio livello applicazione: Sessioni HTTP che consentono di associare informazioni a singoli visitatori

Esempio livello trasporto: Una sessione TCP

129-Livello presentazione

Si occupa di trasformare i dati forniti dal livello di applicazione in un formato standard e offrire servizi di comunicazione comuni quali: la crittografia o la compressione

130-Livello Applicazione

La sua funzione è quella di interfacciare e fornire i servizi per i processi delle applicazioni, interagendo con uno dei protocolli di livello trasporto per ricevere dati o inviarli nella forma richiesta

Un protocollo a livello applicazione definisce:

- 1- Tipi di messaggi scambiati
- 2- La sintassi dei vari tipi di messaggi
- 3- La semantica dei campi
- 4- Le regole per determinare quando e come un processo invia e risponde ai mex

Servizio di TCP:

- **orientato alla connessione:** è richiesto un setup fra i processi client e server
- **trasporto affidabile** fra i processi d'invio e di ricezione
- **controllo di flusso:** il mittente non vuole sovraccaricare il destinatario
- **controllo della congestione:** "strozza" il processo d'invio quando la rete è sovraccaricata
- **non offre:** temporizzazione, ampiezza di banda minima

Servizio di UDP:

- trasferimento dati inaffidabile fra i processi d'invio e di ricezione
- non offre: setup della connessione, affidabilità, controllo di flusso, controllo della congestione, temporizzazione né ampiezza di banda minima

131-

132-Protocolli di accesso alla posta

Si preoccupa di come ottenere i messaggi dal server

- POP: Post Office Protocol
- IMAP: Internet mail access protocol
- http: Hotmail, yahoo ecc

NB: Tutti i client inviano la posta al relay agent che la invia al destinatario, gli indirizzi sono risolti dal DNS che individua il server a cui inviare il messaggio

133-II WEB

Collezione di documenti ipertestuali distribuita su server collegati alla rete Internet, la maggior parte dei documenti è in formato HTML, grafo in cui i nodi sono singoli documenti collegati fra di loro da puntatori

134-WWW

Protocollo http che permette una lettura ipertestuale, non sequenziale dei documenti

135-URL

Sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in internet

136-http

Protocollo di comunicazione fra client e server, utilizzato per trasferire ogni tipo di risorsa (file) su WWW

137-proxy http

Agisce da intermediario fra client e server, riceve la richiesta del client e la propaga al server, vengono usati su LAN per caching o accesso ad internet tramite firewall

138-Lunghezza del frame

Un frame valido deve essere lungo almeno 64 byte, Se si tolgono i 6+6 riservati agli indirizzi, i 2 per il campo length e i 4 del checksum, il campo dati(max 1500 byte) deve avere almeno 46 byte (eventuale padding)