1. Come funziona il protocollo di accesso alle reti cablate, ad accesso multiplo. CSMA/CD. Come si calcola la P di collisione.

CSMA/CD è un protocollo che permette l'accesso al mezzo ascoltando il mezzo, aspettando un intervallo casuale (mentre si è in ascolto) per diminuire il verificarsi di collisioni e, se è libero, comincia a trasmettere. Il fatto di ascoltare il canale mentre si sta trasmettendo permette il rilevamento delle collisioni, in tal caso la trasmissione viene fermata e si aspetta un intervallo di tempo casuale per fare in modo che il mezzo si svuoti, dopo ricomincia la trasmissione. Il ritardo è dato dal back-off esponenziale: l'intervallo viene deciso casualmente in un intervallo tra 1 e 2^n-1 (dove n è il numero degli host connessi), questo cresce esponenzialmente al susseguirsi di collisioni consecutive, tuttavia per evitare ulteriori ritardi viene segnalato al livello superiori dopo 10 tentativi.

2. Cos'è una socket sicura. Come funziona SSL. Schema con la comunicazione tra i nodi. Che algoritmi vengono usati (algoritmi a chiave simmetrica). Problema propagazione chiave simmetrica. Come fa il server ad essere sicuro di parlare col client e viceversa.

Una socket sicura è una particolare socket (ovvero l'interfaccia a livello trasporto dell'applicazione) in cui i dati vengono criptati prima di essere scritti sopra di esso, per farlo si utilizza SSL, esso cripta i dati prima di una lettura/scrittura dopo che la connessione è stata eseguita (prima però bisogna autenticarsi). Per l'autenticazione SSL utilizza le stringhe casuali, esse non possono essere prese e riutilizzate da terzi per confondere il client/server dato che ne vengono generate di nuove a ogni sessione, vengono utilizzate nel seguente modo: il client che vuole autenticarsi manda al server la stringa e i suoi algoritmi di crittografia, il server risponde con la tecnica da utilizzare, un'altra stringa e il certificato della chiave pubblica. Il client cripta la stringa con la chiave pubblica del server e la spedisce, il server controlla il messaggio ricevuto e fa lo stesso. Se il server si è autenticato ha dimostrato di essere lui è quindi può generare le chiavi simmetrica. Gli algoritmi di crittografia a chiave simmetrica attualmente utilizzati sono DES e AES, il primo utilizza chiavi simmetriche di 56 bit su un testo in chiaro di 64 bit, esso è stato violato in 4 mesi con la forza bruta, tuttavia esistono soluzioni senza backdoor, per risolvere ciò si è passati la 3-DES, una versione dell'algoritmo in cui DES viene applicato 3 volte con 3 chiavi differenti, il secondo permette l'utilizzo di chiavi più lunghe (la più sicura è a 256 bit) e di conseguenza ci vuole più tempo per la codifica del messaggio, tanto che non è stato ancora violato. Per condividere una chiave simmetrica si utilizza il centro di distribuzione delle chiavi, esso permette la generazione di una chiave simmetrica e la sua condivisione: un host chiede al centro una chiave per comunicare con B attraverso un messaggio criptato con la sua chiave privata, il centro genera una chiave e la inserisce in un messaggio insieme a una copia criptata con la chiave pubblica di B (il tutto criptato con la chiave pubblica di A). Ricevuto il messaggio, A lo decripta e manda a B quella criptata, quest'ultimo la decripta e quindi può iniziare la comunicazione.

3. Cos'è il SIP.

Il SIP è un protocollo che permette di raggruppare gli utenti attorno a un'applicazione, ognuno di essi è identificato da un nome e/o da un indirizzo e-mail ed è raggiungibili in qualsiasi punto della rete indipendentemente dal dispositivo che sta utilizzando. SIP supporta i seguenti servizi:

- Attivazione delle chiamate: mette in comunicazione chiamante e chiamato, all'inizio il primo chiama il secondo e, se accetta, vengono mandati dei coded per indicare qual è il migliore per entrambi, dopo averlo scelto si fa partire la chiamata (lo stesso meccanismo viene utilizzato per la terminazione);
- Reperimento del chiamato: si utilizzano reti di supporto in cui vi sono dei register e dei proxy, i primi contengono le informazioni relative agli utenti mentre i secondi fungono da interfaccia dato che gli utenti possono trovarsi in reti private, per prima cosa ci si cerca il proxy, quest'ultimo contatterà il register contenente il chiamato e infine si avvia la comunicazione.

4. Cos'è un protocollo ARP. Come viene usata la tabella ARP. Cosa succede se un nodo sulla rete vuole mandare un pacchetto ARP a un'altra rete. Come viene implementato. Si usa specifico tipo di LAN (si usa solo in quella ethernet). Come si risolve il problema su IPV6 (8 byte per la rete,6 per indirizzo fisico).

ARP è un protocollo che permette di capire a quale indirizzo IP corrisponde un dato indirizzo MAC, per farlo si compila un'apposita tabella, essa viene utilizzata per compilare il campo MAC di destinazione cercando il corrispondente IP del pacchetto. ARP è possibile anche su differenti sottoreti, per farlo l'host esegue un primo ciclo di ARP col router, esso farà da ponte per eseguire un secondo ciclo di ARP in cui si prendono le corrispondenze degli host della sottorete.

5. Meccanismo della firma elettronica. Protocolli wireless: chiave WEP (controllare bene il nome visto che non si è capito); come funziona. Perché n aggiungono 24 bit (perché n cerca di fare in modo di editare chi sono sempre i soliti bit e che vengono riconosciuti). Quale meccanismo più sicuro è stato adottato al posto di questo.

Vi sono due meccanismi di firma elettronica:

- il primo consiste nel criptare il proprio messaggio con la propria chiave privata e spedirlo, il ricevente decripta con la mia chiave pubblica, confermando la mia identità dato che la chiave privata può essere ricevuta solo da me. Questo metodo è tuttavia molto pesante;
- il secondo metodo è l'utilizzo degli hash, essi sono stringhe di lunghezza fissa con date proprietà quale quella in cui, dato un messaggio m, deve essere infattibile trovare un ulteriore messaggio avente lo stesso hash di m. Dopo aver calcolato l'hash del messaggio, si concatena il testo in chiaro e si invia, il ricevente calcola l'hash e lo confronta con quello ricevuto per verificare che il mittente sia chi dice di essere.

WEP utilizza una password comune e una crittografia banale: vengono generate delle chiavi a catena con cui si criptano i pacchetti, se esse vengono registrate, è quindi possibile vedere il contenuto dei pacchetti. Per l'autenticazione vengono utilizzati i number once: viene inviato all'host un Nonce criptato, quest'ultimo lo decripta e lo invia all'access point, quest'ultimo controllerà se il numero ricevuto sia equivalente a quello inviato, verificando l'identità dell'host. Al posto di WEP vi sono due meccanismi migliori:

- 802.11i: vi è un meccanismo di distribuzione delle chiavi e ci si autentica tramite chiave WPA o WPA2 utilizzando un server apposito. Quando un host vuole connettersi, esso chiede al server, quest'ultimo genera una chiave master e la invia

all'access point, esso genera un'ulteriore chiave da inviare all'host il quale la utilizzerà per la comunicazione.
- EAP: vi sono server di autenticazione detti radius aventi un proprio protocollo di autenticazione, essi si appoggiano a TLS per la comunicazione. Dopo aver stabilito una connessione TLS col server, si ha un procedimento analogo al punto precedente, dopodichè si passa a un canale in chiaro dato che a livello wireless la crittografia non è ancora attiva e quindi si attiva.

6. Switch internet: che funzione assolve; usa un meccanismo di auto apprendimento; perché si usa il TTL; è garantito che non ci siano collisioni; nel caso si verifichino collisioni, o trovano il buffer pieno cosa accade; nel caso che sia andato perso un pacchetto di un nodo che accade; vantaggi Switch (si possono usare collegamenti con velocità diverse) e svantaggi (il ritardo dovuto alla bufferizzazione); tecnica dello switch per cercare di risolvere il problema dovuto a questo svantaggio.

Il compito dello switch è quello di recapitare un frame all'host di destinazione, per farlo utilizza una tabella interna in cui si memorizzano indirizzo MAC e la porta a cui è connesso l'host, in ogni riga della tabella vi è anche un campo TTL, esso viene rinnovano ogni volta che un frame va verso quella corrispondenza e, al suo scadere, cancella la riga. La compilazione della tabella avviene tramite un meccanismo di autoapprendimento, essa inizialmente è vuota e, all'arrivo di un frame, controlla se vi sono corrispondenze, nel caso non ci siano il frame viene inviato in broadcast, l'unico a rispondere sarà l'host ricevente, permettendo così di aggiornare la tabella. Lo switch garantisce l'assenza di collisioni sia perchè è full-duplex, sia perchè i pacchetti vengono recapitati solamente al singolo host. In caso di buffer pieno si attiva il controllo di flusso, esso permette di rallentare il traffico per smaltire quello presente, per farlo si utilizza uno dei seguenti meccanismi:

- Si simulano delle collisioni inviando dei segnali di jam agli host con l'obiettivo di interrompere il flusso;
- Si inviano dei frame speciali agli host il cui scopo è rallentare il flusso o addirittura fermarlo per un certo periodo.

In caso di perdita di un frame, esso viene ritrasmesso oppure, per evitare troppi rallentamenti dell'applicazione, si segnala al livello superiore. Al costo di un ritardo maggiore dovuto allo store & forward, gli switch permettono di evitare le collisioni e di utilizzare link anche di velocità differente, per risolvere lo svantaggio si dà priorità ad alcuni frame oppure si utilizza il cut through: nel caso il cui il collegamento sia libero, il frame viene inoltrato senza essere memorizzato.

7. Come vengono implementati i server di servizi streaming. Protocollo RTSP

L'implementazione dei server di streaming può essere effettuata seguendo i seguenti approcci:

- non effettuare streaming: il browser scarica tutto il file e infine lo passa al media player, tuttavia non vi è pipelining e vi sono lunghi ritardi prima di usufruire effettivamente dal servizio.
- Streaming con web server: vi è un web server su cui browser e mediaplayer si appoggiano, il primo prende un metafile contenente delle informazioni da passare al secondo, quest'ultimo invece prende le stream, questo approccio però può portare a

ritardi in quando viene utilizzato HTTP (che si appoggia a TCP) per la comunicazione;
- utilizzo di server separati: viene utilizzato un web server per fornisce il metafile e l'interfaccia comunicando col browser mentre il media player richiede le stream comunicando con un altro server che si appoggia a UDP.

La comunicazione tra client e server avente tramite il protocollo RTSP, esso funziona utilizzando una coppia di porte, una server per inviare i comandi al web server mentre l'altra ha il compito di raccogliere le stream, dal momento che questo protocollo si appoggia a UDP è possibile effettuare il multicast, tuttavia è difficile mantenere la sincronizzazione dato che gli utenti dovrebbero vedere lo stesso film allo stesso tempo, il suo utilizzo è quindi solitamente limitato a eventi in diretta.

9. Differenza tra ethernet wifi e ethernet classico. Quali sono i problemi di uno e dell'altro. Che protocollo di usa per accedere al mezzo (CSMA). Come posso minimizzare le probabilità di collisione. Perché si utilizza il tempo di attesa. Come si calcola.

La differenza principale tra wifi e ethernet è che il primo permette la connessione a Internet senza l'ausilio di cavi mentre il secondo vanta un decadimento minore del segnale. Il wifi tuttavia ha un segnale che degrada molto più velocemente e adatta la comunicazione in base alle condizione della rete (rendendola uguale per tutti), ethernet invece è un servizio senza connessione e inefficiente, infatti non vengono utilizzati degli ACK per verificare che un frame sia stato ricevuto correttamente, tuttavia non ce n'è bisogno perchè errori del genere si verificano raramente. Per minimizzare le probabilità di collisione:

- nel CSMA/CD vengono utilizzati degli intervalli di tempo casuali, essi vengono calcolati col backoff esponenziale, in questo algoritmo si calcola il ritardo prendendo casualmente un numero compreso tra 1 e 2^n-1 (dove n è il numero di collisioni consecutive), il numero di valori possibili aumenta esponenzialmente all'aumentare delle collisioni, quindi c'è il rischio di ottenere un ritardo maggiore. Dopo 10 tentativi viene segnalato l'errore per evitare tempi di attesa troppo lunghi;
- nel CSMA/CA vengono sfruttati gli intervalli di tempo tra un frame e l'altro, l'host ascolta il canale , se è libero, trasmette e attende l'ACK, altrimenti attende un tempo casuale e alla fine riascolta il canale. I tempi di attesa tra un frame e l'altro sono DIFS e SIFS, il primo indica la fine di un frame e l'inizio di quello seguente, il secondo pure ma è più breve perchè deve permette al ricevente l'invio dell'ACK al mittente.

I tempi di attesa vengono utilizzati perchè, dati che sono casuali, vi è poca probabilità che due host scelgano lo stesso intervallo di tempo. Nel caso di CSMA/CD, il tempo di attesa viene calcolato prendendo il numero scelto casualmente nell'intervallo e moltiplicandolo per 512, quest'ultimo è il multiplo di tempo necessario per trasmettere un bit.

14. Protocollo RTP, tipicamente viene usato su UDP. Quali servizi offre RTP rispetto al tempo reale cosa garantisce. TIME STEP. RTCP (da più che altro informazioni statistiche). Tutto quello che mette a disposizione cosa permette di fare (il vantaggio è sicuramente quello di consentire una codifica più semplice).

RTP è un protocollo che permette la veicolazione di dati multimediali utilizzando un'apposita struttura di pacchetto e appoggiandosi a UDP quando la rete lo permette, altrimenti è possibile utilizzare TCP. Questo protocollo non garantisce alcun tipo di qualità del servizio e

fornisce un supporto standardizzato per la trasmissione di questo tipo di dati in modo da offrire interoperabilità tra le componenti, in più possiede le informazioni necessarie da permettere il real-time. RTCP è un protocollo che lavora insieme a RTP e fornisce statistiche relative all'applicazione a livello di rete, con esse è infatti possibile adattare la trasmissione. I pacchetti RTP non devono intasare la rete, per evitare che ciò succeda, esso deve limitare la sua trasmissione al 5% della banda disponibile.