1. Cosa si intende per serie di Fourier

Le informazioni possono essere trasmesse via cavo variando alcune proprietà fisiche, come la tensione e corrente. Fourier condusse alcuni studi ed arrivò alla conclusione che le informazioni trasmesse via cavo potevano essere rappresentata da una funzione f(t). Questa funzione è composta da una serie infinita di somme di seni e coseni, ed è in grado di rappresentare un segnale periodico e regolare. La trasmissione però non è mai perfetta e c'è per forza attenuazione di linea. L'intervallo di frequenze trasmesse senza forte attenuazione è detto banda passante.
Anche in un ipotetico canale perfetto, ovvero senza attenuazioni, la velocità di trasmissione non può essere troppo elevata; se si trasmette un segnale arbitrario attraverso un filtro passa basso la cui ampiezza di banda è pari a B, lo si deve campionare a 2B campioni al secondo. Se il segnale è composto da V livelli discreti, il massimo tasso trasmissivo è dato da $2B \log_2 V$ bit/s. Per esempio un canale a 3 kHz senza rumore non è in grado di trasmettere segnali binari a velocità maggiore di 6000bps.

2. Bitrate e Baudrate

Bitrate: velocità massima di trasmissione in un canale. Se si trasmette un segnale arbitrario attraverso un filtro passa basso la cui ampiezza di banda è pari a B, il segnale filtrato può essere ricostruito completamente prendendo solo 2B (esatti) al secondo. Campionare la linea più velocemente di 2B volte al secondo non ha senso. Se il segnale è composto da V livelli discreti, il massimo tasso trasmissivo è di $2B \log_2 V$ bit/s. V sta anche ad indicare il numero di simboli usati.
S/N = segnale/rumore SNR = $10 \log_{10}$ (S/N) Massimo bitrate = $B \log_2 (1+(S/N))$
Baudrate: Simboli al secondo. Un simbolo può valere più bit. In un mezzo trasmissivo che utilizza il byte stuffing, il baud rate può ad esempio calcolare quanti byte (e quindi non bit) vengono trasmessi al secondo.

3. Descrivere i vari tipi di cavo e confrontarli

Doppino: Un doppino (twisted pair) è composto da due conduttori di rame isolati, spessi circa 1mm, avvolti intorno l'uno all'altro in forma elicoidale (DNA); l'intreccio è usato perché i campi elettromagnetici generati dai due conduttori si annullano a vicenda, perciò il cavo irradia meno. Un segnale è generalmente costituito da una differenza di potenziale tra i due cavi della coppia. L'applicazione più comune per il doppino è il sistema telefonico. I doppini possono raggiungere una lunghezza di alcuni chilometri senza bisogno di amplificazione, ma per distanze maggiori il segnale si attenua troppo ed è necessario fare uso di ripetitori. I doppini si possono usare per trasmettere segnali analogici e digitali. Esistono diverse varietà di doppini, quella più comune e posata nella maggior parte degli edifici a uso ufficio prende il nome di categoria 5, o cat5. Un doppino di cat5 consiste di due cavi elettricamente isolati e intrecciati tra loro. Quattro di queste coppie sono raccolte all'interno di una guaina di plastica che le protegge e le mantiene unite. Cat5 ha rimpiazzato cat3 con un cavo quasi identico facente uso dello stesso connettore, ma con un numero di intrecci più elevato per ogni metro. Il maggior numero di intrecci permette di diminuire il crosstalk (fenomeno in cui un segnale trasmesso tramite un circuito ha un effetto indesiderato su un altro circuito) e ottenere una migliore qualità del segnale sulle lunghe distanze. Si arriva fino a cat7, fino a cat6 i cablaggi sono identificati come UTP (unshielded twisted pair), in quanto consistono solamente di cavi e isolanti. I cavi cat7 possiedono una schermatura su ogni singolo doppino come pure attorno all'intero cavo.
Cavo coassiale: essendo più schermato rispetto al doppino, può estendersi per distanze più lunghe e consente velocità più elevate. Esistono due tipi di cavi coassiali, uno a 50 Ohm, usato per le trasmissioni digitali, l'altro a 75Ohm usato per le trasmissioni analogiche e la TV via cavo. Un cavo coassiale è composto da un nucleo conduttore coperto da un rivestimento isolante, a sua volta circondato da un conduttore cilindrico solitamente realizzato con una calza di conduttori sottili, che infine è avvolto da una guaina protettiva di plastica. Questa realizzazione fornisce ampiezza di banda ed eccellente immunità al rumore. I cavi moderni hanno un'ampiezza di banda fino a qualche Ghz.
Linee elettriche: l'idea di usare linee elettriche per la trasmissione dati non è recente; sono state già usate per molti anni dalle compagnie elettriche per comunicazioni a basso tasso di invio o bit rate. E' una soluzione semplice, ma presenta una difficoltà: un circuito elettrico è stato progettato per distribuire segnale elettrico, cosa molto diversa rispetto ai dati, per cui ha delle pessime prestazioni. Il

segnale elettrico viene inviato a 50-60Hz e il mezzo trasmissivo attenua le frequenze più alte richieste dalle trasmissioni dati. E' possibile inviare almeno 100Mbps facendo uso del circuito elettrico di un'abitazione se si adottano tecniche che possano resistere a frequenze disturbate e sequenze di errori.
Fibre ottiche: ad oggi, il limite pratico per la trasmissione dei segnali, pari a circa 100Gbps, deriva alla nostra incapacità di convertire più velocemente i segnali da elettrici a ottici. I cavi in fibra ottica sono simili ai cavi coassiali, ma non sono avvolti dalla calza conduttrice. Al centro si trova un nucleo (core) di vetro, attraverso il quale si propaga la luce; ha un diametro che va dagli 8 ai 50 micron, dipendente dal fatto di essere una fibra monomodale o multimodale. Il nucleo è circondato da un rivestimento di vetro (cladding) che ha un indice di rifrazione più basso, lo strato successivo è una settile fodera di plastica che protegge il rivestimento. Per generare il segnale normalmente si impiegano due tipi di sorgenti luminose: i LED e i laser a semiconduttore. La luce si propaga all'interno del core. La fibra può contenere molti raggi che rimbalzano ad angoli diversi (fibra multimodale), oppure un unico raggio che si propaga in linea retta (per via dello spessore della fibra, monomodale). Le fibre si possono collegare in tre diversi modi, primo, con dei connettori inseriti in apposite prese, che perdono il 10-20% della luce; secondo, possono essere attaccate meccanicamente, un'estremità di un cavo viene appoggiata all'estremità dell'altro e il segmento viene pinzato (causa una perdita del 10%); terzo, due pezzi di fibra possono essere fusi per formare una connessione solida, si genera una piccola attenuazione del segnare. La fibra offre molti vantaggi tra cui la maggiore ampiezza di banda, non è influenzata dalle sorgenti elettriche, è sottile e leggera, non hanno perdita di luce, ed è difficile intercettare i dati trasportati, la comunicazione bidirezionale richiede due fibre o due bande di frequenza su una singola fibra. L'unico svantaggio vero della fibra ottica è che è molto costosa rispetto a qualsiasi altro tipo di cavo.

4. Caratteristiche e confronto fra i vari tipi di satellite, GEO, MEO, LEO

Nella sua forma più semplice, un satellite di comunicazione può essere immaginato come un grande ripetitore di microonde collocato nel cielo. Questo dispositivo contiene diversi transponder, ossia ricetrasmettitori satellitari. Ognuno ascolta una parte dello spettro, amplifica il segnale in ingresso e lo ritrasmette su un'altra frequenza per evitare interferenze con in segnale in arrivo. Esistono vari tipi di satelliti e si differenziano per la distanza dalla Terra della loro orbita. Gravità solare, lunare e planetaria tendono ad allontanarli dagli slot e dagli orientamenti assegnati, ma l'effetto è contrastato dai motori a razzo installati, alimentati da pannelli solari.
GEO: satelliti geostazionari. Posti a 35800km di distanza, con le tecnologie attuali vengono disposti nel piano equatoriale a intervalli maggiori di 2 gradi. Coprono una grande area, pari a 1/3 della superficie terreste, ma si è deciso di ridurre questa area per poter piazzare più satelliti senza provocare interferenze. I GEO sono collegati alla Terra tramite VSAT, delle piccole stazioni con un'antenna da circa 1m, essendo piccole non possono comunicare tra loro, si è dovuto quindi ideare stazioni particolari più potenti per permettere la connessione terrestre. Il costo della trasmissione satellitare non dipende dalla distanza ma è costante. GEO hanno una reattività quasi istantanea e un ottimo tasso di errore.
MEO: ad altitudini molto più basse, comprese tra le due fasce di Van Alien. Impiegano circa 6 ore per compiere un giro completo intorno al pianeta, di conseguenza devono essere seguiti mentre si spostano in cielo. Poiché sono più bassi de GEO, coprono un'area più piccola e sono raggiungibili per mezzo di trasmettitori meno potenti. Sono utilizzati per i sistemi di navigazione più che per le telecomunicazioni. I circa 30 satelliti GPS che orbitano a 20200km di altezza sono di tipo MEO
LEO: low earth orbit. Si spostano velocemente, quindi un sistema completo impiega un alto numero di satelliti di questo tipo. Hanno un costo di lancio relativamente basso, e il ritardo delle comunicazioni è di pochi millisecondi. I più piccoli possono avere una forma cubica da soli 10cm di lato.
Al momento per le telecomunicazioni sembra che fibre ottiche combinate con la rete radio cellulare siano il sistema migliore, ma per alcune applicazioni specializzate i satelliti sono migliori. Se i satelliti riuscissero ad abbattere i costi di dispiegamento, oppure se i satelliti su orbite basse avranno successo, la fibra potrebbe rischiare di perdere il dominio dei mercati.

5. Che cos'è la modulazione in frequenza?

Per permettere a molti segnali di condividere uno stesso canale trasmissivo sono nate le tecniche multiplexing. FDM (Frequency Division Multiplexing) sfrutta la trasmissione in banda passante

per condividere un canale: divide lo spettro in bande di frequenza di cui ogni utente ha uso esclusivo per inviare i propri segnali. Solitamente si ha un eccesso di allocazione per ogni canale, che prende il nome di banda di guardia (guard band) e permette di tenere i canali ben separati tra loro. Per prima cosa i canali vocali sono traslati verso l'alto in frequenza ognuno di un valore differente; successivamente possono essere combinati, in quanto nessuno di loro occupa la stessa porzione di spettro. Un forte picco ai bordi di un canale sarà trattato come rumore nel canale adiacente. Quando vengono inviati dati digitali è possibile dividere lo spettro in maniera efficiente senza usare le bande di guardia, OFDM (Orthogonal Frequency Division Multiplexing) divide la banda del canale in molto sottoportanti che inviano dati in maniera indipendente; queste sottoportanti sono stipate una a ridosso all'altra nel dominio delle frequenze. Di solito un flusso di informazioni digitali d alta velocità è diviso in molti altri più lenti che sono trasmessi in parallelo sulle sottoportanti. Se una di queste è troppo disturbata la si esclude in favore di altre che vengono ricevute meglio.

6. Cos'è la modulazione nel tempo?

Un'alternativa a FDM è la TDM (Time Division Multiplexing), in questo caso gli utenti fanno i turni secondo una politica round robin e ognuno di loro, periodicamente, prende possesso della banda completa per un tempo limitato. Per poter funzionare, i flussi devono essere sincronizzati nel tempo; piccoli intervalli (tempi di guardia), analoghi alle bande di guardia nella FDM, possono essere aggiunti per permettere minimi aggiustamenti. TDM viene spesso usato come parte delle reti telefoniche e cellulari.

7. Che cos'è la modulazione delta (delta modulation)?

La modulazione delta è una tecnica di conversione analogico-digitale e digitale-analogico per la trasmissione di informazioni vocali dove la qualità non è di primaria importanza. Nella modulazione delta, i dati trasmessi sono ridotti a un flusso di dati di 1 bit. Le sue caratteristiche principali sono: in segnale analogico viene approssimato con una serie di segmenti, ogni segmento del segnale approssimato viene confrontato con l'onda analogica del segnale originale per determinare l'aumento o la diminuzione di ampiezza relativa, il processo decisionale per stabilire lo stato di bit successivi è determinato da questo confronto, viene inviato solo il cambiamento delle informazioni, ovvero viene inviato solamente un aumento o una diminuzione dell'ampiezza del segnale dal campione precedente; una non variazione provoca che in segnale modulato rimanga 0.

8. Rete telefonica pubblica commutata

PSTN (Public Switched Telephone network) aveva come obiettivo trasmettere la voce umana in una forma più o meno comprensibile. Il fattore limitante ai fini della rete risulta essere ciò che commercialmente viene definito "ultimo miglio", cioè il tratto di cavo/doppino tramite cui il cliente si connette, e non le linee principali (trunk) o gli apparati all'interno della rete telefonica. La rete telefonica è così composta: da ogni telefono partono due cavi di rame che si collegano direttamente alla centrale più vicina dell'azienda telefonica; di solito la centrale si trova a una distanza compresa tra 1 e 10km, è più vicina nelle città, mentre più lontana nelle aree rurali. Le connessioni tramite doppino tra ogni telefono e le centrali sono chiamate commercialmente local lopp, ultimo miglio e collegamento locale. Ogni centrale locale ha diverse linee in uscita che conducono a uno o più centri di commutazione attigui chiamati centrali interurbane. Queste linee sono chiamate linee di connessione interurbana. Le centrali interurbane comunicano tra loro attraverso speciali linee a larga banda, intertoll trunk o interoffice trunk. Per le telecomunicazioni viene usata una moltitudine di mezzi trasmissivi, diversamente dagli edifici moderni, dove il cablaggio è normalmente in cat5, l'ultimo miglio a uso domestico consiste tipicamente id un doppino cat3 e le fibre stanno cominciando solo ora ad apparire. Tutte le linee e i commutatori sono diventati digitali e l'ultimo miglio rappresenta l'ultimo tassello di tecnologia analogica del sistema.

9. Descrivere in dettaglio il GSM (Global System for Mobile connections)

GSM (Global System for Mobile connection) è uno standard europeo per il 2G nato negli anni 80. Il terminale mobile è ora diviso in un dispositivo e un chip rimovibile chiamato SIM (Subscriber

Identity Module) card. La SIM può essere rimossa e inserita in un dispositivo diverso per farlo diventare, dal punto di vista della rete, il vostro telefono mobile (la SIM è personale, ad una SIM è associato un utente). Il telefono parla con la stazione base cellulare usando un collegamento wireless che prende il nome di air interface. Le stazioni base cellulare sono collegate a un BSC (Base Station Controller) che gestisce le risorse radio delle celle e handoff dei dispositivi. Il BSC è a sua volta collegato ad un MSC che instrada le chiamate e si connette alla rete telefonica fissa, PSTN. MSC ha bisogno di sapere dove trovare i dispositivi mobili, per cui mantiene un database dei telefoni associati con le celle che gestisce. GSM usa una gamma di frequenze allocate a livello globale, incluse 900, 1800 e 1900MHz. E' un sistema cellulare duplex a divisione di frequenza, ogni coppia di frequenze viene divisa con TDM in intervalli di tempo per cui non può essere condivisa da più terminali. Ad ogni stazione attiva è assegnato uno slot temporale su una coppia di canali. Trasmissione e ricezione non avvengono nello stesso intervallo temporale perché le radio GSM non sono in grado di trasmettere e ricevere contemporaneamente. La velocità complessiva di ogni canale è di 270833 bps, condivisa da otto utenti. GSM utilizza MAHO (Mobile Assisted Hand Off), ovvero aiuta a gestire l'handoff dei dispositivi.

10. Di descriva la tecnica CDMA (Code Division Multiple Access), possibilmente con esempio

Anche chiamato CDM (Code division multiplexing), si tratta di una forma di comunicazione a spettro distribuito in cui un segnale a banda stretta viene sparso su una banda di frequenza più ampia. Ciò rende il segnale più tollerante alle interferenze e permette a più segnali di utenti diversi di condividere la stessa banda di frequenza, è usato principalmente per il secondo scopo. Infatti CDMA permette a ogni stazione di trasmettere su tutto lo spettro di frequenza in ogni momento. Le trasmissioni simultanee vengono separate usando la teoria dei codici. Il punto centrale di CDMA è essere in grado di estrarre il segnale e rifiutare tutto il resto come rumore casuale. In CDMA il tempo di trasmissione di ogni bit è suddiviso in m intervalli più brevi chiamati chip. Di solito ci sono da 64 a 128 chip per bit. A ogni stazione viene assegnato un codice univoco di m bit chiamato chip sequence. Per trasmettere un bit con valore 1 una stazione invia la sua sequenza di chip, mentre per trasmettere uno 0 ne invia la sua negazione, nessun'altra sequenza è ammessa. Con CDMA ogni stazione occupa l'intera banda disponibile. Durante il tempo di trasmissione di ogni bit una stazione può trasmettere un 1, uno 0 o rimanere in silenzio e non trasmettere nulla. Quando due stazioni trasmettono contemporaneamente le loro sequenze bipolari si sommano linearmente. Per recuperare la sequenza di bit generata da una certa stazione il ricevente deve conoscere in anticipo la sequenza di chip di quella stazione. Il recupero si effettua calcolando il prodotto interno normalizzato tra la sequenza di chip ricevuta e la sequenza della stazione i cui bit vogliamo recuperare. CDMA sincrono differisce da CDMA asincrono.

11. Il GPRS: cos'è, pregi e difetti

GRPS (General Packet Radio Service) è una delle tecnologie di telefonia mobile cellulare, viene convenzionalmente definita di generazione 2.5, ovvero una via di mezzo tra GSM e UMTS. E' stato il primo sistema cellulare progettato specificatamente per realizzare un trasferimento dati a commutazione di pacchetto e a media velocità su rete cellulare per agganciarsi alla rete internet, usando canali TDMA della rete GSM. Per traffico vocale e altri servizi GPRS conserva la classica commutazione di circuito propria del GSM. Il GPRS espande le funzionalità dei servizi di scambio dati basati su GSM. Le tariffe sono solitamente calcolate in base al consumo, e non più in base al tempo di connessione come nelle reti commutate (questo perché in GPRS l'intera larghezza di banda disponibile è occupata anche quando nessun dato è in corso di trasferimento). La velocità limite è di 171Kbit/s, ma un valore realistico si aggira sui 30-70Kbit/s. La banda è frazionata in base al numero di utenti collegati per cella, quindi se ci sono più utenti connessi, la velocità diminuisce.

12. Hand off

Quando un telefono mobile abbandona fisicamente una cella, poiché si accorge che il segnale dell'apparecchio si sta affievolendo, la stazione base di quella cella verifica il livello di potenza del segnale ricevuto dalle stazioni che si trovano nelle celle adiacenti. A questo punto la stazione trasferisce la gestione dell'apparecchio alla cella che riceve il segnale più forte, ossia alla cella in cui ora si trova il telefono. Il telefono viene informato dell'identità della nuova cella centrale di controllo e, se

durante lo spostamento era in corso una chiamata, l'apparecchio viene forzato a passare su un nuovo canale (perché quello vecchio non è utilizzato nelle celle adiacenti). Questo processo chiamato handoff richiede circa 300 mse. L'assegnazione del canale è eseguita dal MTSO, il centro nevralgico del sistema, mentre le stazioni base sono semplici ripetitori radio. Esistono due tipi di handoff: nel **soft handoff** il telefono è acquisito dalla nuova stazione di base prima di interrompere il segnale precedente; in questo modo non c'è alcuna perdita di continuità ma il telefono deve essere in grado di sintonizzare due frequenze nello stesso momento (quella vecchia e quella nuova). Né i telefono di prima generazione né quelli di seconda erano in grado di farlo. Nel caso di **hard handoff**, la vecchia stazione di base rilascia il telefono prima che la nuova lo acquisisca. Se la nuova non è in grado di prendere il controllo del dispositivo (per esempio perché non è disponibile alcuna frequenza), la chiamata viene interrotta bruscamente. Gli utenti tendono a notare questo evento, che però è inevitabile con l'architettura corrente.

13. Terza generazione (3G): voce digitale e dati

La terza generazione per la telefonia mobile è tutta centrata su voce digitale e dati. Questa tecnologia ha un unico obiettivo: fornire abbastanza banda wireless per appagare le attese degli utenti futuri. UMT (Universal Mobile Telecommunication) è il nome europeo per WCDMA (Wireband CDMA), ovvero la tecnologia 3G. E' compatibile con GSM. La potenza del segnale che raggiunge la stazione base dipende non solo dall'energia usata dai trasmittenti, ma anche dalla loro distanza. Un altro miglioramento rispetto a CDMA è quello di permettere a utenti diversi di mandare dati a velocità distinte. Ha 3 vantaggi cruciali: per prima cosa è in grado di aumentare la capacità trasmissiva sfruttando i brevi periodi in cui i trasmettitori sono silenziosi, ogni cella usa le stesse frequenze, non è necessario usare FDM per separare le trasmissioni di utenti diversi, è quindi più facile per una stazione base usare delle antenne direzionali invece di una sola omnidirezionale; terzo, utilizza il soft hand-off. Anche se le reti 3G non sono ancora state completamente installate, già si sta lavorando alla tecnologia 4G, chiamata LTE.

14. FDM, TDM, CDM: algoritmi per la selezione della banda

Le aziende telefoniche hanno sviluppato elaborati schemi per convogliare molte conversazioni lungo un singolo collegamento fisico. Questi schemi di multiplexing possono essere divisi in due categorie di base: FDM, e TDM. In FDM lo spettro di frequenza è diviso in bande di frequenza e ogni utente ha il possesso esclusivo di parte della banda. Gli schemi FDM utilizzati in tutto il mondo sono parzialmente standardizzati. La frequenza viene suddivisa in gruppi, super gruppi e master gruppi. In TDM, gli utenti si danno il cambio (in una sorta di girotondo), acquisendo periodicamente il possesso di tutta la banda per un tempo brevissimo. TDM può essere gestita completamente da dispositivi elettronici digitali, ma può essere utilizzato solo per i dati digitali. CDM o CDMA (Code Division Multiple Access), permette a ogni stazione di trasmettere per tutto il tempo attraverso l'intero spettro di frequenza. Trasmissioni multiple simultanee sono separate usando la teoria della codifica. CDM presume che segnali sovrapposti si sommino linearmente.

15. QAM e QAM16

Le comunicazioni possono avvenire anche in trasmissione in banda passante, in quanto una banda di frequenza arbitraria è usata per far passare il segnale. Il valore assoluto della frequenza non influenza la capacità di trasferimento de dati, questo significa che possiamo prendere un segnale in banda base che occupa da 0 a B Hz e traslarlo fino a occupare una banda passante da S a S+B Hz senza cambiare il quantitativo di informazioni che può trasmettere. La modulazione digitale è ottenuta sulla trasmissione in banda passante modulando un segnale portante che risiede in banda passante. Possiamo modulare ampiezza, frequenza o fase del segnale. Solo una tra frequenza e fase può essere modulata ogni volta perché esse sono correlate, ma ampiezza e fase possono essere modulate in maniera combinata. Questo tipo di modulazione prende il nome di QAM (Quadrature Amplitude Modulation), in quanto la rappresentazione è un diagramma a costellazione (costellation diagram). In base alla densità della costellazione, esistono varie modalità di QAM, tipo QAM16 o QAM64. QAM-16 utilizza 16 combinazioni di ampiezza e fase, così si possono trasmettere 4 bit per simbolo. Viene utilizzata un'associazione chiamata Gray code, che consiste nell'associare bit ai simboli in maniera

tale che simboli adiacenti differiscano di solo un bit. Un simbolo rappresenta una “stella” nella costellazione descritta prima.

16. Che cos’è il byte stuffing?

Utilizzando la tecnica del framing, ovvero della divisione in frame dei dati da mandare, la destinazione deve essere in grado di identificare l’inizio e la fine di un frame. Il byte stuffing è una delle 4 tecniche usate per facilitare una destinazione in questo compito (le altre 3 sono: conteggio dei byte, bit stuffing e violazione della codifica del livello fisico). Il byte stuffing aggira il problema di una nuova sincronizzazione, necessaria a seguito di un errore, inserendo byte speciali all’inizio e al termine di ogni frame. La maggior parte de protocolli usa lo steso byte, chiamato flag byte. Due flag byte consecutivi indicano la fine di un frame e l’inizio del successivo. Può capitare che il valore corrispondente al flag byte compaia naturalmente all’interno dei dati; un modo per sviare questo problema è l’inserimento di un byte di escape (ESC) da inserire prima di ogni occorrenza del flagbyte nei dati, paradossalmente, il byte ESC deve essere preceduto da se stesso se presente nei dati. La destinazione, ogni qualvolta troverà un carattere di escape, lo rimuoverà, ottenendo così i dati originali. E’ usato in PPP.

17. Che cos’è il bit stuffing?

Un altro metodo per sviare al problema della sincronizzazione durante il framing è il bit stuffing. Il bit stuffing è stato sviluppato per HDLC. Ogni frame inizia e finisce con una speciale sequenza di bit: 01111110, corrispondente a un flag byte. Il livello data link di chi trasmette, ogni volta che incontra cinque bit a 1 consecutivi nei dati, automaticamente inserisce un bit a 0 nel flusso di bit in uscita, analogamente, la destinazione, ogni 5 bit a 1, toglie uno 0, in modo da ottenere i dati nella loro forma originale. USB utilizza il bit stuffing, con questa tecnica il confine tra due frame viene riconosciuto in modo inequivocabile tramite l’uso della sequenza nel flag byte, visto che questa può essere presente solo al confine tra i frame e mai al loro interno.

18. Numero di bit necessari per riconoscimento (e correzione) degli errori di trasmissione

In una trasmissione dati, si possono verificare degli errori, esistono varie tecniche per il riconoscimento e la correzione degli errori. Molti metodi implicano l’aggiunta di bit nella word inviata. Questi bit aggiunti, hanno dei valori particolari, in base alla tecnica di rilevamento o correzione utilizzata. Vi sono tecniche che utilizzano svariati bit di rilevazione e correzione, ma il numero minimo per rilevare errori in parole di n bit è n+1. Nella maggior parte dei protocolli è sufficiente rilevare l’errore, successivamente, rilevato un errore, si richiede la ritrasmissione del frame errato. Ma alcuni protocolli sono anche in grado di correggere degli eventuali errori: in una word sempre di n bit, il numero minimo di bit da spedire per poter rilevare e correggere gli errori presenti risulta essere 2n+1. In una connessione veloce, la correzione risulta superflua, in quanto si impiega di meno a ritrasmettere il frame rispetto a calcolare quali bit sono stati comunicati in modo erroneo e correggerli. Il numero di bit corrispondenti diversi in due sequenze di bit è detto distanza di Hamming, codici di correzione e rilevamento di errori si basano su questo. La distanza di Hamming che si riesce a rilevare con n+1 bit è n, e a correggere servono 2n+1 bit per n bit.

19. Si descriva cos’è il CRC. Si calcoli inoltre il CRC di 10011101 usando il polinomio generatore di x^4 +x +1

CRC (Cyclic Redundant Check) è un protocollo a rilevamento di errore noto anche come codifica polinomiale. Si basa sul fatto di trattare le sequenze di bit come dei polinomi a coefficienti che possono assumere solo valori 0 e 1. Un frame di k bit è visto come una lista di coefficienti per un polinomio con k termini che variano da x^k-1 a x^0. Quando si utilizza CRC, sorgente e destinazione devono mettersi d’accordo in anticipo su un polinomio generatore G(x). Questo polinomio deve avere i bit di ordine più basso e più alto pari a 1 (ad esempio 10011 dato dal problema, ma 10110 non va bene). Per poter calcolare il checksum di un frame di m bit corrispondente al polinomio M(x), il frame deve essere più lungo del polinomio generatore. L’idea è quella di aggiungere un checksum alla fine del frame, in modo che il polinomio rappresentato dal frame con checksum sia divisibile per G(x). Se c’è un resto vuol dire che c’è stato un errore di trasmissione. Il modo di operare comprende solo 3 passi:

- Sia r il grado di G(x), si aggiungono r bit con valore zero dopo la parte di ordine più basso del frame, così che venga a contenere m + r bit
- Si divide la sequenza di bit così ottenuta per la sequenza corrispondente a G(x), usando la divisione modulo 2
- Si sottrae il resto (che contiene sempre al massimo r bit) dalla sequenza calcolata prima usando la sottrazione in modulo 2. Il risultato è il frame con checksum pronto per la trasmissione.

10011101 è il nostro M(x), mentre 10011 è G(x). Aggiungiamo quindi 4 zeri a M(x), ottenendo diciamo F(x) = 100111010000. Ora dividiamo F(x) per G(x). Otteniamo un resto di massimo r bit, che andranno aggiunti a M(x) per poi essere trasmessi. In questo caso i 4 bit ottenuti sono 1101, che vanno aggiunti a M(x), per ottenere 100111011101, questo è il campo trasmesso.

20. Descrivere il protocollo stop and wait, pregi e difetti

E' un protocollo semplice per un canale soggetto a rumore. I frame possono essere danneggiati o addirittura persi completamente. Supponiamo che se un frame è danneggiato durante la trasmissione, l'hardware della destinazione riesca ad accorgersene calcolando il checksum. L'idea è che quando la sorgente invia un frame, la destinazione risponda con un ack solo quando il frame sia stato ricevuto correttamente. Se arriva un frame danneggiato, allora la destinazione semplicemente lo scarta. Dopo un po' di tempo il timer della sorgente scatta e il frame viene inviato di nuovo. Il problema sorge quando l'ack viene perso. La sorgente ritrasmette il frame, e la destinazione riceve due volte lo stesso frame, ma non sa che è lo stesso. Un modo per risolvere questo problema sta nell'inserire un ID nel frame, in modo che la destinazione possa controllarlo. Un numero di sequenza con un solo bit (0 o 1) è quindi sufficiente. Quando arriva un frame con il numero di sequenza corretto, viene accettato, passato al livello di rete e quindi inviato l'ack. 0 e 1 si devono alternare, infatti vengono incrementati in aritmetica modulo 2. Un altro improvement può essere l'aggiunta alla destinazione della possibilità di invio di frame NAK (not ACK), in modo da velocizzare la ritrasmissione dei frame danneggiati o persi.

21. Che cos'è il piggybacking?

Il piggybacking è un protocollo per la trasmissione degli ACK utile quanto pericoloso. E' utilizzato quando sorgente e destinazione comunicano entrambe, ovvero, non è solo la sorgente a trasmettere frame, ma anche la destinazione, che chiameremo per comodità A e B. Quando A invia un frame a B, se il frame arriva correttamente, B deve inviare un ACK ad A. Con il piggybacking B non invia immediatamente l'ACK ad A, ma aspetta di dover trasmettere lei stessa un frame ad A, e inserisce l'ACK in questo frame. Il problema principale sta nel tempo. Se B non ha frame da inviare ad A, non invia l'ACK ed A rinvia il frame (inutilmente) a B. A questo si può ovviare imponendo un timer su B, in modo che essa se non ha un frame da inviare ad A, scaduto questo timer (che è più piccolo del timer di timeout di A per ritrasmettere il frame) invia l'ACK ad A senza piggybacking.

22. Si descriva la tecnica del sliding window

L'essenza dei protocolli a finestra scorrevole è che, a ogni istante, la sorgente tiene traccia di un insieme di numeri di sequenza corrispondenti ai frame che è autorizzata a inviare. Si dice che questi frame si trovano nella finestra di invio (che è un buffer). In modo analogo la destinazione tiene traccia della finestra di ricezione. Le finestra di invio e ricezione non devono necessariamente avere gli stessi limiti inferiori o superiori e neppure la stessa dimensione. In alcuni protocolli tali finestre hanno dimensioni variabili nel tempo. Fissare le finestre a grandezza 1 significa trasformare il protocollo in uno stop and wait. Sliding window funziona così: la sorgente ha un buffer con i frame da inviare, li invia, e attende un ack dalla destinazione, quando riceve un ack, sposta la finestra di 1, e invia il nuovo frame. La destinazione, ha un buffer in cui è pronta a mettere i frame, una volta ricevuti i frame, manda l'ack e trasla subito la finestra di 1. Se la stazione riceve frame fuori dalla finestra, vengono scartati. Questo protocollo può usare pipelining, ovvero tiene più frame in viaggio contemporaneamente.

23. Si descriva l'idea dei protocolli "go back N", indicandone pregi e difetti

E' uno dei modi per risolvere il problema dovuto al pipelining, ovvero: che cosa succede quando un frame nel mezzo di una sequenza viene danneggiato o perso. Una gran quantità di frame arriverà alla destinazione prima che la sorgente riesca a sapere che qualcosa è andato storto. La destinazione deve semplicemente scartare tutti i frame successivi all'errore senza mandare ack per questi frame scartati. Equivale ad avere una finestra di ricezione di dimensione 1 e una finestra di invio più grande.

24. Si descriva cos'è la tecnica del selective repeat

E' il secondo dei modi per risolvere il problema dovuto al pipelining, ovvero: che cosa succede quando un frame nel mezzo di una sequenza viene danneggiato o perso. Una gran quantità di frame arriverà alla destinazione prima che la sorgente riesca a sapere che qualcosa è andato storto. Un frame in errore viene scartato, mentre i frame corretti, ricevuti successivamente, vengono messi nel buffer e vengono inviati i rispettivi ack. Quando la sorgente va in timeout, solo il frame più vecchio senza ack viene ritrasmesso. Una volta ricevuto anche il frame mancato, la destinazione passa al livello superiore tutti i frame ricevuti. Corrisponde ad avere una finestra di ricezione di grandezza maggiore di 1. Questa tecnica è spesso associata all'utilizzo dei NAK (not ACK) che stimolano la ritrasmissione prima che il timer della sorgente vada in timeout, risparmiando così tempo.

25. Descrivere la differenza tra ALOHA e slottet-ALOHA

ALOHA e slotted-ALOHA sono due protocolli a contesa, ovvero il canale non è riservato prima di ogni trasmissione. Ogni terminale utilizza la stessa frequenza di upstream per spedire i frame al computer centrale: metodo semplice ed elegante per risolvere il problema dell'allocazione del canale. L'idea alla base di ALOHA è semplice: consentire agli utenti di trasmettere ogni volta che hanno dati da inviare, ovviamente ci potranno essere collisioni che danneggeranno i frame inviati, e chi trasmette deve sapere se è successo. In ALOHA, dopo che una stazione ha inviato il suo frame, il computer centrale rispedisce tale frame in broadcast a tutte le stazioni. Se si presenta una collisione, la stazione rimane in attesa per un intervallo casuale prima di ripetere la trasmissione. Il tempo di attesa deve essere casuale, altrimenti le stesse stazioni ritrasmetteranno nello stesso istante provocando così una nuova collisione. Con ALOHA si può sperare di utilizzare al massimo il 18% del canale.
Con slotted-ALOHA il tempo è diviso in slot, ognuno corrispondente ad un frame. Questo approccio richiede che gli utenti concordino sui limiti degli intervalli; la necessaria sincronizzazione si può soddisfare con una speciale stazione che emetta un segnale all'inizio di ogni intervallo. Un computer non può più inviare dati quando vuole, ma deve aspettare l'inizio di uno slot per farlo; questo implica che due frame inviati sul canale, o collidono completamente, o non collidono, questo raddoppia la potenza del protocollo a un 37% rispetto al 18% di ALOHA puro in cui i frame potevano collidere anche per un singolo bit o per metà.

26. Si illustri CSMA, indicandone pregi e difetti

CSMA (Carrier Sense Multiple Access) – è un protocollo con rilevamento della portante. Ne esistono 3 varianti:
CSMA 1-persistente: quando una stazione ha dei dati da trasmettere, prima di tutto ascolta il canale per scoprire se qualcun altro in quel momento sta trasmettendo. Se il canale è libero la stazione trasmette i propri dati, altrimenti la stazione aspetta finché non si libera il canale per poi trasmettere un frame. Se avviene una collisione la stazione attende un tempo casuale e ricomincia da capo. 1-persistente perché la probabilità di trasmissione a canale libero è 1.
CSMA non persistente: prima di trasmettere, ogni stazione controlla il canale, se nessun altro sta trasmettendo inizia ad inviare dati, ma se il canale è occupato la stazione non esegue un controllo continuo per impossessarsene subito alla fine della trasmissione, ma attende invece per un intervallo di tempo casuale prima di ripetere il controllo.
CSMA p-persistente: si applica a canali divisi in intervalli temporali e funziona così: quando è pronta a trasmettere, ogni stazione controlla il canale. Se lo trova libero, trasmette subito con una probabilità p e rimanda la trasmissione all'intervallo successivo con probabilità q = 1 – p. Se anche quell'intervallo

risultasse libero, la stazione trasmetterebbe oppure rimanderebbe un'altra volta. Il processo si ripete fino a quando il frame non è stato trasmesso o un'altra stazione ha iniziato a trasmettere. Se la stazione inizialmente trova il canale occupato, attende l'intervallo successivo per effettuare il controllo.
CSMA/CD: CSMA with Collision Detection. Uguale a CSMA, solo che l'hardware della stazione, deve ascoltare il canale durante la trasmissione. Se il segnale letto è diverso da quella inviato, sa che sta avvenendo una collisione. Questo implica che il segnale letto non debba essere molto piccolo rispetto a quello inviato (difficile in wireless), e la modulazione deve essere scelta in maniera tale da permettere la determinazione delle collisioni. Nel caso di rilevamento di una collisione, la stazione interrompe immediatamente la trasmissione, senza continuare ad inviare il frame inutilmente (la stazione tronca la trasmissione brutalmente).

27. Basic bitmap

E' un protocollo senza collisione, tra i protocolli a prenotazione, poiché riserva la proprietà del canale in anticipo e previene ogni collisione. Ogni periodo di contesa è composta da N slot, dove N sono le stazioni presenti nella rete. Se la stazione 0 ha un frame da inviare, trasmette un bit 1 durante l'intervallo 0. A nessun'altra stazione è concesso di trasmettere durante questo slot. Indipendentemente da quella che sta facendo la stazione 0, la stazione 1 ha la possibilità di trasmettere un 1 durante lo slot 1, ma solo se ha un frame in coda. In generale, la stazione j può annunciare il possesso di un frame da inviare inserendo un bit 1 nello slot j. Una volta trascorsi tutti gli N intervalli, ogni stazione sa quali sono le stazioni che intendono trasmettere; e a questo punto le stazioni iniziano a trasmettere in ordine numerico. Poiché tutti sono d'accorso su chi sarà il successivo, non ci sarà mai alcuna collisione. Dopo che l'ultima stazione che aveva effettuato la prenotazione ha mandato il proprio frame, ha inizio un altro periodo di contesa di N bit. Se una stazione diventa pronta a spedire un frame quando ormai il suo intervallo è scaduto, deve rimanere in silenzio finché tutte le altre non abbiano trasmesso, e la mappa di bit ricominci da capo.

28. Spiegare in cosa consiste il protocollo collision free binary countdown, pregi e difetti

Il protocollo collision free binary countdown è un protocollo a contesa, ovvero usato per assegnare a priori un canale ad una determinata stazione (che appunto se lo contende prima dello slot di trasmissione con le altre). In questo protocollo ogni stazione ha un indirizzo espresso in binario. Se questa stazione è intenzionata a comunicare, invia in broadcast il proprio indirizzo binario. Se è l'unica ad inviarlo, il canale è suo. Se non è l'unica stazione, i vari indirizzi della varie stazioni che vogliono comunicare vengono combinati mediante l'operatore booleano OR. Si presuppone che i ritardi di trasmissione siano trascurabili, in modo che tutte le stazioni possano vedere istantaneamente i bit dichiarati. Per evitare dei conflitti si deve applicare una regola di arbitraggio: una stazione rinuncia al canale non appena si accorge che una stazione con un indirizzo più alto del suo vuole anch'essa trasmettere. Se le due stazioni 1010 e 0111 vogliono trasmettere, 1010 trasmette, 0111 si accorge che c'è l'altra stazione, che ha un bit più significativo di lei impostato ad uno, e rinuncia al canale. Una volta assegnato ad una stazione il canale, essa può trasmettere un frame, a fine frame, riparte la contesa. Per evitare che una stazione con un numero alto ottenga sempre il canale, gli indirizzi possono essere intercambiati tra stazioni.

29. Spiegare cos'è l'adaptive tree walk protocol

E' un protocollo per evitare collisioni di pacchetti in una rete. Le stazioni vengono pensate come foglie di una struttura ad albero binario. Si lascia libero il canale in modo che ogni stazione possa comunicare, se una ci riesce, bene, non succede nulla, se invece si verifica una collisione, nell'intervallo successivo possono comunicare (provare ad inviare pacchetti) solamente le stazioni sotto al nodo sinistro del nodo padre, se una di queste riesce ad acquisire il controllo de canale, l'intervallo successivo è riservato alle stazioni che si trovano sotto l'albero destro del canale. Se invece c'è subito un'altra collisione, nell'intervallo successivo, di nuovo tocca alle stazioni sotto al nodo figlio sinistro. E avanti così, è un algoritmo ricorsivo, finché una o tutte le stazioni che dovevano trasmettere non ci riescono.

30. Ethernet

Esistono due tipi di Ethernet: ethernet classica, che risolve il problema dell'accesso multiplo; e ethernet commutata (switched ethernet) in cui dispostivi chiamati commutatori (switch) sono usati per connettere diversi computer.

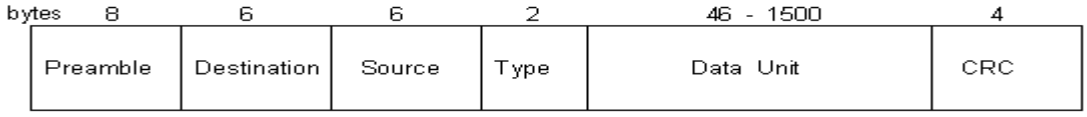
Ethernet classica è la forma originale e permette dei tassi di trasmissione dati tra i 3 e i 10Mbps. Ethernet thick (ovvero spessa): 10base5 -> utilizza un cavo coassiale molto grosso, connessioni generalmente effettuate con spine a vampiro. 10 indica la velocità di 10Mbps, base indica che la trasmissione avviene in banda base, 5 indica che i segmenti possono essere lunghi fino a 500 metri. Ethernet thin (ovvero sottile): 10base2 -> utilizza un cavo coassiale più sottile del precedente, era più flessibile ed utilizzava collettori standard BNC, era più economica e più facile da installare, ma poteva estendersi per soli 185 metri (invece dei 500 della thick), e ogni segmento supportava solo 30 macchina, invece della 100.

10base-T: ogni stazione è collegata direttamente a più hub con doppini telefonici

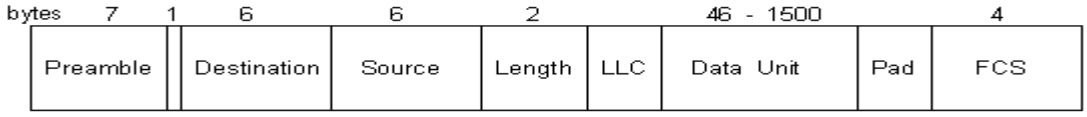
10base-F: utilizza fibre ottiche, è un'alternativa costosa ma buona per l'immunità alle interferenze, che consente di collegare edifici/hub molto distanti.

Per costruire reti più grandi, più cavi possono essere connessi attraverso repeater (dispositivo di livello fisico che riceve, amplifica e ritrasmette il segnale).

Ethernet commutata raggiunge velocità di 100, 1000 e 100000Mbps, in varianti chiamate fast, giga e 10-giga ethernet.



DIX Ethernet Packet



IEEE 802.3 Frame

31. Codifica di manchester

Nelle telecomunicazioni la codifica di manchester è una forma di comunicazione dati nella quale ogni punto viene segnalato da una transizione. La codifica manchester è considerata una codifica auto-sincronizzante (non necessita di un segnale di sincronia esterno), il che significa che permette un'accurata sincronizzazione del flusso dati. Ogni bit viene trasmesso in un intervallo di bit predefinito. In questa codifica i segnali dei dati e del clock sono combinati per formare un flusso di dati auto-sincronizzante. Ogni bit codificato contiene una transizione a metà del periodo di bit, la direzione della transizione determina se il bit è uno 0 o un 1: la prima metà del periodo è il valore vero del bit, e la seconda metà è il complemento del valore del bit. Ovvero uno 0 è tradotto in una transizione dal basso verso l'alto, mentre uno 1 è tradotto con una transizione dall'alto al basso. Esiste una derivazione di tale tecnica, chiamata codifica di manchester differenziale. Si differenzia nella rappresentazione dei bit: quest'ultima è basata sulla verifica di transizione all'inizio di un intervallo. La presenza di una di queste, sia esso di tipo alto-basso o basso-alto, indica un valore (tipicamente lo 0), mentre l'assenza di una transizione indica un 1.

32. Cos'è il binary exponential backoff?

Questo algoritmo, chiamato backoff esponenziale binario, è stato scelto per adattarsi dinamicamente al numero di stazioni che tentano di trasmettere. E' usato un CDMA/CD-1. Se c'è una collisione, le stazioni interrompono la trasmissione con un breve messaggio caotico per poi ritrasmettere dopo un periodo di tempo casuale. Dopo la prima collisione, ogni stazione aspetta casualmente 0 o 1 slot prima di ritentare. Dopo la seconda collisione, ogni stazione sceglie 0, 1, 2 o 3 a caso e rimane in

attesa quel numero di slot. Se avviene una terza collisione la volta successiva il numero di intervalli di attesa è scelto a casa tra 0 e 2^3 -1. In generale, dopo i collisioni, viene scelto un numero casuale compreso tra 0 e 2^i -1 e si salta quel numero di slot; dopo dieci collisioni il tetto massimo di scelta rimane bloccato a 1023 slot, questo per evitare una crescita infinita nell'attesa della ritrasmissione.

33. Stazione nascosta e stazione esposta: cosa sono e come si comportano

Il problema di una stazione che non è in grado di rilevare i potenziali concorrenti per il mezzo di trasmissione a causa della distanza eccessiva è chiamato problema del terminale nascosto (hiddent terminal problem). Se A vuole trasferire a B, ma non riesce a vedere C, che anche vuole trasferire a B, può succedere che entrambe, non vedendo l'altra stazione che sta trasmettendo, inizino a trasmettere a B, il risultato è che B riceve due segnali sovrapposti, con la conseguente perdita di entrambi. Un altro problema sta nella stazione esposta, è un po' il problema inverso. In questo caso B trasmette ad A nello stesso momento in cui C vuole trasmettere a D. Se C controlla il canale, vedendo B, sentirà una trasmissione ed erroneamente concluderà di non poter trasmettere a D. Se C trasmettesse, questa trasmissione potrebbe causare un problema solo nella zona tra B e C, dove nessuno dei destinatari è posizionato. Si crea così un ritardo inutile ed evitabile.

34. Bluetooth

Bluetooth fu reso pubblico nel luglio del 1999. Ogni tipo di apparecchiatura elettronica utilizza Bluetooth. I protocolli bluetooth permettono a questi apparecchi di individuarsi a vicenda e connettersi, un'azione chiamata pairing (associazione), per poi trasferire dati in sicurezza. L'unità base di un sistema bluetooth è la piconet, comporta da un nodo master e da fino a sette nodi slave attivi situati entro un raggio di 10 metri. Più piconet possono trovarsi nella stessa stanza, e possono essere collegate attraverso un bridge. Un insieme di piconet interconnesse è chiamato scatternet. Una piconet può contenere fino a 255 nodi sospesi (parked): dispositivi a cui il nodo master ha imposto di attivare uno stato di basso consumo. Quando si trova in uno stato di basso consumo, un dispositivo può solo rispondere a una richiesta di attivazione o a un segnale di beacon trasmesso dal nodo master. Il cuore di ogni piconet è costituito da un sistema TDM centralizzato: il nodo master controlla il clock e decide quale dispositivo possa comunicare in ogni intervallo temporale. Tutta la comunicazione avviene tra il nodo master e un nodo slave, non è ammessa alcuna comunicazione diretta tra nodi slave. Il livello più basso di bluetooth è quella della trasmissione radio, il livello link control (o baseband) è per certi versi analogo al sottolivello MAC, ma include anche elementi del livello fisico. Seguono due protocolli che utilizzano il protocollo link control. Bluetooth definisce diversi formati di frame. Uno de più comuni è così formato:

- Codice di accesso: identifica il nodo master
- Intestazione: contiene: addr (identifica il destinatario), type (identifica il tipo di frame, il tipo di correzione degli errori e il numero di intervalli occupati dal frame), flow (bit attivato da un nodo slave quando non può ricevere altri dati), ACK, Checksum
- Dati: opzionale, dimensione da 0 a 2744 bit.

35. Si descriva l'algoritmo statico flooding

Una semplice tecnica locale (letteralmente, inondazione), in cui ogni pacchetto in arrivo è inviato a tutte le linee in uscita tranne quella da cui proviene. Questo meccanismo genera un elevato numero di pacchetti duplicati; teoricamente il numero di questi pacchetti è infinito, a meno che non si prendano dei provvedimenti. Una possibile tecnica è utilizzare un contatore di salti inserito nell'intestazione di ogni pacchetto e decrementare il suo valore ad ogni salto, in modo da scartare il pacchetto quando il contatore raggiunge lo 0 (idealmente questo contatore dovrebbe essere uguale alla distanza sorgente-destinazione). Una tecnica migliore consiste nel tener traccia dei pacchetti già trasmessi, in modo da evitare una seconda trasmissione, questo è possibile inserendo un numero di sequenza in ogni pacchetto. Il flooding non è un metodo pratico per inviare pacchetti, ma ha alcune importanti applicazioni. In primo luogo garantisce che un pacchetto venga consegnato a tutti i nodi della rete, è infatti efficiente per informazioni indirizzate a tutti (broadcast). E' un metodo totalmente robusto, anche

se un gran numero di router saltasse, il flooding troverebbe un percorso, se esiste, per portare il messaggio a destinazione. Esso richiede poco in termini di configurazione, ogni router deve solamente conoscere i suoi vicini.

36. Descrivere il distance vetor routing

Il distance vector routing (o routing basato sul vettore delle distanze) è un algoritmo dinamico. Questo algoritmo opera in modo che ogni router conservi una tabella (ossia un vettore) che definisce la migliore distanza conosciuta per ogni destinazione e il collegamento che conduce a tale destinazione. Queste tabelle sono aggiornate scambiando informazioni con i router vicini. In questa tabella, ogni router forma una voce, formata da due campi, che sono: la linea di trasmissione preferita da utilizzare per quella destinazione e una stima del tempo o della distanza associata a quella destinazione. Il distance vector routing è utile, è una tecnica semplice con cui i router possono collettivamente calcolare i cammini minimi, ma ha un serio difetto pratico: può raggiungere l'obiettivo lentamente. Reagisce bene alle buone notizie (trovato un cammino più corto per arrivare all'host 4), ma troppo lentamente a quelle cattive (no, questa strada è peggiore di quella che già conosco per l'host 4). Esiste un altro problema, quando il router X dice a Y di avere un percorso che punta a Z, Y non ha modo di sapere se fa parte di quel percorso.

37. Linkstate routing

Il linkstate routing è un routing basato sullo stato dei collegamenti. L'idea alla base di questo algoritmo è semplice, e può così essere riassunta: ogni router deve: scoprire i propri vicini e i relativi indirizzi di rete, misurare la distanza o la metrica di costo di ogni vicino, costruire un pacchetto contenente tutte le informazioni raccolte, inviare tale pacchetto a tutti gli altri router e ricevere da loro i pacchetti, elaborare il percorso più breve verso tutti gli altri router. Ogni router, quando viene acceso, manda uno speciale pacchetto HELLO, per scoprire chi sono i propri vicini, i router all'altro capo della linea devono rispondere fornendo il proprio nome, che deve essere UNICO all'interno della rete. Per calcolare i cammini minimo, l'algoritmo di linkstate routing richiede che ogni collegamento abbia una metrica di costo o distanza (se la rete è particolarmente estesa, il ritardo dei collegamenti può essere incluso nella funzione di costo). Una volta rilevate le distanze, ogni router costruisce un pacchetto contenente queste informazioni, che poi invia ad ogni suo vicino, che, presi i dati dei vicini, aggiornano il proprio pacchetto. Calcolare le distanze è facile. OSPF è un algoritmo di link state routing. Questo protocollo richiede più memoria e tempo di calcolo rispetto al distance vector routing; per reti grandi questo può diventare un problema

38. Choke packet

Il modo più diretto per notificare una congestione a una sorgente è comunicarglielo direttamente. Il router seleziona un pacchetto congestionato e invia all'host sorgente un choke packet (letteralmente, pacchetto di strozzamento). Il pacchetto originale viene etichettato in modo da impedire la generazione di altri choke packet lungo il percorso e poi è inoltrato nel solito modo. Quando riceve il choke packet, l'host sorgente deve ridurre il traffico inviato alla destinazione specificata, per esempio del 50%. E' facile che più choke packet vengano inviati alla stessa sorgente o destinazione. L'host dovrebbe ignorare questi choke packet aggiuntivi per l'intervallo di tempo necessario affinché la sua riduzione di traffico abbia effetto. Dopo tale termine ulteriori choke packet indicano che la rete è ancora congestionata. Il feedback implicito di questo protocollo può aiutare a prevenire la congestione, ma non ferma alcuna sorgente.

39. Choke packet hop by hop

Ad alte velocità o a lunghe distanze, molti nuovi pacchetti possono essere trasmessi dopo la segnalazione di una congestione a causa della lenta diffusione del segnale. In un approccio alternativo, il choke packet ha effetto su tutti i salti (hop) attraversati. In questo caso, partendo dal router 1 per arrivare al router 4, il choke packet arriva al router 2, che diminuisce il flusso diretto al router 1, dedicando però più buffer al flusso che riceve da 3, che riceve da 4 (che continua ad inviare dati a piena velocità finché il choke packet non arriva anche a lui). Tuttavia, 1 riceve un sollievo immediato.

Questo schema, che considera la sequenza di hop attraversati, ha l'effetto di alleviare rapidamente la congestione nel punto in cui si forma, al prezzo di un incremento dell'utilizzo dei buffer di trasmissione nella parte di percorso dalla congestione alla sorgente. In questo modo la congestione può essere stroncata sul nascere senza alcuna perdita di pacchetto.

40. Load shedding

Il load shedding (eliminazione del carico) è l'ultima risorsa dei router per rimuovere la congestione, viene infatti messo in atto dai router quando altri protocolli non riescono ad evitare la congestione. La questione chiave è come scegliere i pacchetti da scartare, e ovviamente non c'è un modo "migliore", ma dipende dalle applicazioni in esecuzione. Per il trasferimento dei file, un pacchetto vecchio è più prezioso di uno nuovo, al contrario, nel caso dei dati multimediali un pacchetto nuovo è più importante di un pacchetto vecchio. La prima delle due politiche (il vecchio è migliore del nuovo) è chiamata WINE, mentre la seconda (il nuovo è migliore del vecchio) è chiamata MILK. Per implementare un criterio di eliminazione intelligente, le applicazioni devono contrassegnare i loro pacchetti con classi di priorità, in modo da indicare la loro importanza. I ruoter possono scartare i pacchetti da classe più bassa.

41. RED

RED (Random Early Detenction) – per evitare una congestione, conviene scartare i pacchetti prima che un eccesso di questi ultimi provochi una congestione. RED è un metodo che viene messo in atto dai router per scartare questi pacchetti. Per stabilire quando è il momento giusto per iniziare a scartare i pacchetti, i router mantengono una media mobile delle lunghezze delle code. Quando la lunghezza media della coda su una linea supera una soglia di guardia, la linea è considerata congestionata e una piccola frazione di pacchetti viene scartata in modo casuale. I router RED permettono di migliorare le prestazioni della rete, ma per funzionare correttamente richiedono una fase di inizializzazione. Per esempio il numero ideale di pacchetti da scartare dipende dal numero di sorgenti a cui notificare la congestione. RED viene usato quando gli host non possono ricevere segnali espliciti.

42. Reverse Path Forwarding RPF

Il reverse path forwarding è un'idea semplice una volta capita. Quando riceve un pacchetto broadcast, il router verifica se il pacchetto è giunto attraverso la linea che normalmente è utilizzata per inviare i pacchetti alla sorgente della trasmissione broadcast. In caso affermativo, c'è una forte probabilità che il pacchetto broadcast stesso abbia seguito il percorso migliore dal router, e che perciò sia la prima copia arrivata al router. In questo caso, il router inoltra le copie del pacchetto attraverso tutte le linee esclusa quella di input. Se al contrario il pacchetto broadcast è giunto attraverso una linea diversa da quella che viene preferita per raggiungere la sorgente, il pacchetto è scartato in quando è probabile che si tratti di un duplicato. Funziona in modo similare al flooding, inoltre non è necessario alcun meccanismo speciale d'interruzione del processo.

43. Quality Of Service

Una soluzione semplice per fornire una buona qualità del servizio è quella di costruire una rete con capacità sufficiente per qualsiasi traffico venga immesso. Il nome di tale soluzione è overprovisioning (fornitura in eccesso). La rete risultante sarebbe in grado di supportare il traffico delle applicazioni, senza perdite significative e, ipotizzando un algoritmo di routing decente, di consegnare i pacchetti con una bassa latenza; tali prestazioni sarebbero ottimali. Il problema di questa soluzione sono i costi. Con i meccanismi di qualità del servizio la rete può onorare le garanzie di prestazione fatte anche quando vi sono picchi di traffico, a costo di abbassare il livello di alcune richieste. Per garantire la qualità del servizio devono essere affrontate le seguenti quattro questioni: 1. Di che cosa le applicazioni hanno bisogno dalla rete; 2. Come regolare il traffico che entra in rete; 3. Come prenotare le risorse dei router per garantire le prestazioni; 4. Capire se la rete può tranquillamente accettare più traffico. Nella pratica le soluzioni di qualità del servizio combinano molte tecniche. Le esigenze di ogni flusso possono essere caratterizzate da quattro parametri primari: affidabilità, ritardo, jitter e banda.

Insieme questi parametri determinano la QoS (Quality of Service), ossia la qualità del servizio richiesta dal flusso. Per poter ospitare una varietà di applicazioni, le reti supportano differenti categorie di QoS.

44. Leacky bucket, pregi e difetti

Si immagini un secchio con un piccolo buco sul fondo. Qualunque sia la velocità d'ingresso dell'acqua nel secchio, l'efflusso avrà una velocità costante quando ci sarà acqua nel secchio, e avrà una velocità pari a 0 quando il secchio sarà vuoto. Inoltre, una volta che il secchio è pieno, l'acqua aggiuntiva versata nel contenitore traboccherà e andrà perduta. Ogni host è collegato alla rete da un'interfaccia che contiene un leacky bucket (letteralmente, secchio bucato). Per immettere un pacchetto nella rete deve essere possibile mettere ancora acqua nel secchio. Se il pacchetto arriva quando il secchio è pieno deve essere accodato finché abbastanza acqua non sia uscita o scartata. Questo algoritmo limita il tasso di trasmissione a lungo termine di un flusso, ma permette a brevi picchi con una lunghezza massima regolata di passare inalterati senza subire ritardi aggiuntivi. Grandi picchi vengono smussati da un traffic shaper.

45. Descrivere il token bucket, pregi e difetti

Immaginate l'interfaccia di rete come un secchio che si riempie. Il rubinetto lavora a tasso R e il secchio ha una capacità B. Per inviare un pacchetto dobbiamo essere in grado di togliere l'acqua, o i token, come i contenuti sono comunemente chiamati, dal secchio. Non più di un numero fisso di token, B, può accumularsi nel secchio, e, se il secchio è vuoto, dobbiamo aspettare che più token arrivino prima di poter inviare un altro pacchetto. Questo algoritmo limita il tasso di trasmissione a lungo termine di un flusso, ma permette a brevi picchi con una lunghezza massima regolata di passare inalterati senza subire ritardi aggiuntivi. Grandi picchi vengono smussati da un traffic shaper.

46. Descrivere ARP

ARP (Address Resolution Protocol) – quasi tutte le macchine di internet lo utilizzano. Un host effettua una domanda in broadcast, chiedendo chi sia il proprietario di un determinato indirizzo IP, tutta la rete ascolta, ma solo la macchina che ha quell'indirizzo risponde, inviando il proprio indirizzo Ethernet. In questo modo chi aveva fatto la domanda scopre l'assegnazione IP-Ethernet. Una volta utilizzato questo protocollo, il computer memorizza in una cache il risultato, caso mai dovesse essere necessario ricontattare lo stesso computer. Queste informazioni scadono in pochi minuti, per permettere cambiamenti nelle associazioni

47. Di descriva DHCP

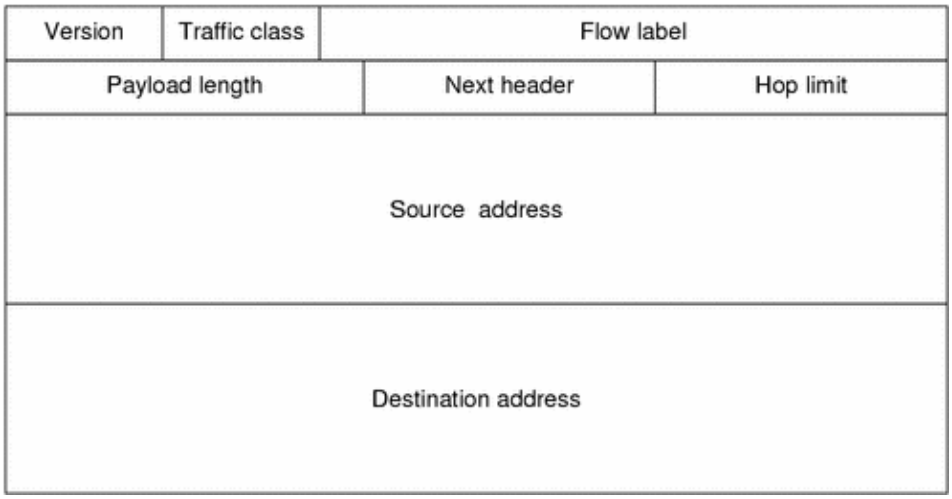
DHCP (Dynamic Host Configuration Protocol) – con esso ogni rete deve avere un server DHCP responsabile della configurazione. Quando viene avviato, un computer non possiede un indirizzo IP, esso invia una richiesta broadcast tramite un pacchetto DHCP DISCOVER per ottenere un indirizzo IP. Il pacchetto deve raggiungere il server DHCP. Il server invia un pacchetto di offerta all'host, utilizzando il suo indirizzo ethernet. DHCP utilizza una tecnica chiamata LEASING. Consiste nel rilasciato, dopo un quanto di tempo, dell'indirizzo IP dall'host. Poco prima della scadenza del leasing, l'host deve richiedere al server DHCP il rinnovo dell'indirizzo IP, se non riesce a fare la richiesta, o il server la rifiuta, l'host non può più utilizzare l'indirizzo IP che gli era stato assegnato. DHCP ha quasi completamente sostituito i protocolli precedenti che avevano funzionalità più limitate.

48. Ipv6

IPv6 utilizza 128bit invece dei 32 di IPv4. Si è dimostrato un protocollo difficile da implementare, e non interagisce con IPv4. Chiamato SIPP (Simple Internet Protocol Plus). Aveva i seguenti obiettivi: supportare miliardi di host, ridurre la dimensione delle tabelle di routing, semplificare i protocolli, fornire un grado di sicurezza maggiore, prestare più attenzione al tipo di servizio, aiutare il multicasting, permettere ad un host di spostarsi senza cambiare il suo indirizzo, permettere al protocollo di evolversi in fururo, permettere al protocollo vecchio e nuovo di coesistere per anni. Li ha mantenuti tutti. La sua

intestazione contiene solo sette campi. Migliorano perciò throughput e ritardo. L'intestazione presenta i seguenti campi:

- Version: è sempre 6
- Differentiated services: è usato per distinguere le classi di servizio dei pacchetti con differenti richieste di consegna in tempo reale
- Flow label: consente a una sorgente e a una destinazione di marcare un gruppo di pacchetti che, avendo gli stessi requisiti, devono essere trattati allo stesso modo.
- Payload length: indica il numero di byte che segue l'intestazione di 40 byte
- Next header: indica quale delle sei intestazioni estese, se presente, segue l'intestazione corrente
- Hop limit: come time to live, utilizzato per impedire ai pacchetti di vivedere per sempre.
- Source address, destination address: indicano gli indirizzi di sorgente e destinazione.



49. Elencare e descrivere brevemente l'header ipv4

Un datagramma IPv4 è costituito da una parte di intestazione e da un corpo, il payload. L'intestazione ha una parte fissa di 20byte e una parte opzionale di lunghezza variabile. I campi sono i seguenti:

- Version: contiene la versione del protocollo, in questo caso 4
- IHL: indica la lunghezza dell'intestazione espressa in parole di 32 bit
- Differentiated services: è usato per distinguere diverse classi di servizio
- Total length: tiene conto del contenuto del datagramma, intestazione e dati
- Identification: serve all'host di destinazione per determinare a quale programma appartiene il frammento appena arrivato
- DF: don't fragment
- MF: more fragment, indica che ci sono altri frammenti
- Fragment offset: indica la posizione del frammento nel datagramma corrente
- Time to live: contatore utilizzato per limitare la vita di un pacchetto
- Protocol: indica quale processo di trasporto è in attesa di quei dati
- Header checksum: somma tutti i gruppi di 16 bit appena arrivano usando l'aritmetica in complemento a uno e poi prende il complemento a uno del risultato
- Source e Destination address: indicano gli indirizzi IP delle interfacce di rete di partenza e arrivo
- Option: sono di lunghezza variabile, è riempito con multipli di quattro byte.

50. Frame ethernet

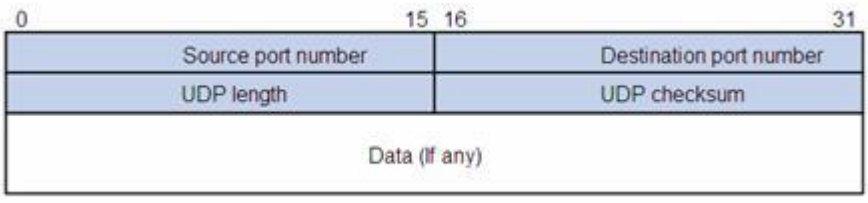
Il frame ethernet è composto dai seguenti campi

- Preamble: questi primi byte hanno valore 1010101010… e servono a svegliare gli adattori del ricevente e a sincronizzare gli oscillatori con quelli del mittente
- Start of frame delimiter (SFD): 1byte, ha valore 10101011, la serie di due bit a 1 indica al destinatario che sta arrivando del contenuto importante, è protetto mediante la violazione del codice Manchester; svolge la stessa funzione del campo flag della trama DHLC
- Destination address: MAC address, questo campo contiene l'indirizzo LAN dell'adattatore di destinazione, se l'indirizzo non trova corrispondenza, il livello fisico del protocollo lo scarta e non lo invia agli strati successivi
- Source address: MAC address, questo campo contiene l'indirizzo LAN del mittente
- Type: questo campo indica il tipo di protocollo del livello di rete in uso durante la trasmissione, oppure la lunghezza del campo dati
- Payload (data): da 46 a 1500 byte, contiene i dati reali, che possono essere di lunghezza variabile in base al MTU. Se i dati superano la capacità massima, vengono suddivisi in più pacchetti, mentre se i dati non raggiungono la lunghezza minima di 46 byte, viene aggiunto del padding di lunghezza opportuna
- Frame check sequence (FCS): CRC di 4 byte, permette di rilevare se sono presenti errori di trasmissione, il ricevente calcola il CRC e lo condronta con quello ricevuto in questo campo

51. Di descriva l'header UDP

La suite di protocolli di Internet supporta un protocollo di transporto non orientato alla connessione chiamato UDP (User Datagram Protocol), esso offre alle applicazioni un modo per inviare datagrammi senza dover stabilire una connessione. UDP trasmette segmenti costituiti da un'intestazione di 8 byte seguita dal payload. L'intestazione è formata dai seguenti campi:

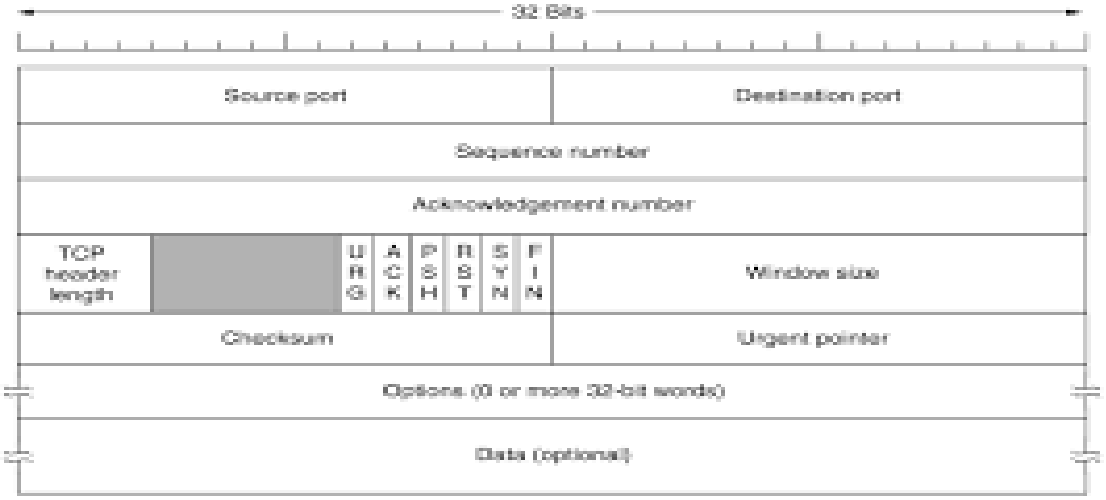
- Source port e destination port: servono per identificare gli endpoint all'interno dei computer di sorgente e destinazione
- UDP length include l'intestazione di 8 byte e tutti i dati, minimo 8 byte e massimo 65515 byte
- Checksum: è opzionale, verifica la somma dell'intestazione



52. Descrivere l'header TCP e commentarlo

TCP (Transmission Control Protocol) – è stato progettato per fornire un flusso di byte affidabile end-to-end su una internetwork inaffidabile. E' stato progettato per adattarsi dinamicamente alle proprietà della internetwork e per continuare a offrire solide prestazioni in presenza di molti tipi di errore. Il servizio TCP è ottenuto con la creazione di punti terminali di un sistema di comunicazione da parte del mittente e ricevente, chiamati socket. Ogni socket possiede un numero composto dall'indirizzo IP dell'host e da un numero di 16bit locale all'host, chiamata porta. Una socket può essere usata per più connessioni contemporaneamente. Le connessioni sono identificate dalla coppia delle socket. Le entità TCP di invio e ricezione scambiano i dati sotto forma di segmenti, un segmento TCP consiste di un'intestazione fissa di 20byte più una parte facoltativa seguita da zero o più byte di dati. L'intestazione TCP è composta dai campi:

- Source port e destination port: identificano gli estremi locali della connessione.
- Sequence number e acknoledgement number: svolgono le loro solite funzioni
- Header lenght: indica quanti gruppi di 32 bit sono contenuti nell'intestazione
- 4 bit inutilizzati
- 8 flag di un bit: CWR (riduzione della finestra di congestione), ECE, URG (impostato a 1 quando si usa urgent pointer), ACK, PSH (segnala la presenza di dati push), RST (reimposta connessione), SYN (richiede connessione), FIN (rilascia connessione)
- Window size: indica la grandezza della finestra
- Checksum: effettua un controllo dell'intestazione
- Options: fornisce un modo per aggiungere funzionalità aggiuntive
- Dati: è facoltativo



53. DNS

Il DNS (Domain Name System) è un meccanismo per convertire i nomi in indirizzi di rete. Utilizza uno schema di denominazione gerarchico basato su domini e di un database distribuito per l'implementazione di questo schema di denominazione. E' principalmente usato per associare nomi di host a indirizzi IP, ma può essere utilizzato anche per altri scopi. Esso invoca una procedura di libreria chiamata resolver, passato il nome come parametro. Il resolver invia un pacchetto UDP contenente la richiesta a un server DNS locale, che cerca il nome e restituisce l'indirizzo IP al DNS locale che a sua volta lo restituisce al resolver. Equipaggiato dell'indirizzo IP, il programma può quindi stabilire una connessione TCP con la destinazione oppure inviarle pacchetti UDP. Lo spazio dei nomi è gestito da un'associazione no profit ICANN (Internet Corporation for Assigned Names and Numbers). Internet al momento è divisa in oltre 250 domini di primo livello (.com, .edu, .mil, ecc). I domini di primo livello sono di due tipi: generici e per nazioni. A ogni dominio, che sia rappresentato da un singolo host

o sia un dominio di primo livello, può essere associato un insieme di resource record (record di risorse) che formano il database DNS. Vi sono varie tecniche di interrogazione del database DNS.

54. Cos'è un cifrario a sostituzione e a trasposizione

Cifrario a sostituzione – in un cifrario a sostituzione, ogni lettera o gruppo di lettere viene rimpiazzato da un0altra lettera o gruppo di lettere per mascherare il messaggio. Uno dei cifrari più antichi che si conoscano è il cifrario di Cesare, che consiste nello spostare l'alfabeto del testo cifrato di k lettere. K è considerata la chiave del metodo general. Il sistema generale per la sostituzione simbolo a simbolo viene chiamato sostituzione monoalfabetica, dove la chiave è la stringa di lettere che corrisponde all'intero alfabeto. Per ogni testo esistono circa 26! Chiavi possibili. Resta comunque facile da cifrare, gli attacchi bruti ormai sono superati, esistono algoritmi più efficienti.

Cifrario a trasposizione – i cifrari a sostituzione conservano l'ordine dei simboli del testo in chiaro, limitandosi a mascherare la loro apparenza. I cifrari a trasposizione, al contrario, riordinano le lettere ma non le mascherano. Si mette il testo in forma matriciale, e si numerano (utilizzando una parola senza ripetizione di lettere) le colonne. Il testo cifrato viene letto per colonna, cominciando con quella che ha la lettere chiave più bassa. Alcuni cifrari a trasposizione prendono un blocco di lunghezza fissa in input e producono in output un altro blocco di lunghezza fissa.

55. Si descriva l'algoritmo DES e triplo DES

DES (Data Encryption Standard) è ormai uno standard obsoleto. Il testo in chiaro viene cifrato in blocchi di 64 bit, che generano 64 bit di testo cifrato. L'algoritmo è parametrizzato da una chiave a 56 bit e ha 19 stadi distinti, il primo stadio è indipendente dalla chiave e consiste nella trasposizione dei 64bit del testo in chiaro. L'ultimo stadio è esattamente l'inverso del primo. Il penultimo stadio consiste nello scambiare i 32 bit di sinistra con i 32 di destra. I rimanenti 16 stadi sono funzionalmente identici, ma sono parametrizzati da diverse funzioni della chiave. L'algoritmo è simmetrico, ovvero con la stessa chiave si effettua sia cifratura che decifratura. Una tecnica che viene talvolta utilizzata per rafforzare DES si chiama sbiancamento. Consiste nell'operare lo XOR di una chiave casuale a 64 bit su ogni blocco di dati del testo in chiaro, usare il risultato come input per DES e infine eseguire lo XOR di una seconda chiave a 64bit; il risultato finale è il testo cifrato da trasmettere.

Triple DES – Vengono usate due chiavi e tre stadi. Nel primo stadio, il testo in chiaro viene cifrato con DES nel modo solito usando la chiave k1. Nel secondo stadio, DES viene usato in modalità di decifrazione usando la chiave k2. Infine un'altra cifratura viene fatta con la chiave k1. La sequenza cifra, decifra, cifra è stata scelta per compatibilità all'indietro con i sistemi DES a chiave singola.

56. Counter mode cipher (RIMOSSO)

Counter mode permette un accesso casuale ai dati. Il testo in chiaro non viene cifrato direttamente; si cifra invece un vettore di inizializzazione (IV) con una costante e il risultato è messo in XOR con il testo in chiaro. Incrementando di 1 il vettore di inizializzazione a ogni blocco diventa facile riuscire a decifrare un blocco in qualunque posizione si trovi, senza dover decifrare prima tutti i predecessori. Ha una debolezza: è esposto ad attacchi di tipo keystream riutilizzato. La coppia chiave-IV vanno scelti indipendentemente e in modo casuale, anche se la chiave viene usata due volte, se l'IV è differente, il testo rimane al sicuro.

57. Cipher block chaining (RIMOSSO)

Si suddivide il testo in blocchi, ogni blocco è messo in XOR con il precedente blocco cifrato prima di eseguire la cifratura vera e propria. Così facendo a blocchi di testo in chiaro uguali non corrispondono più blocchi di testo cifrato identici e la cifratura non è più costituita da un cifrario a sostituzione monoalfabetica. Per il primo blocco lo XOR viene calcolato con un blocco di dati casuali, detto IN (initialization vector), trasmesso in chiaro insieme al testo cifrato. Notiamo che la cifratura del blocco i è una funzione di tutto il testo in chiaro a partire dal blocco 0 fino a i-1, quindi lo stesso testo in chiaro

dà origine a diversi testi cifrati a seconda della sua posizione. Questa tecnica non produce lo stesso testo cifrato a partire da blocchi di testo in chiaro uguali, complicando quindi ulteriormente la criptoanalisi.

58. Stream cipher

Il cosiddetto cifrario a flusso. Questa modalità funziona cifrando un vettore di inizializzazione con una chiave crittografica per ottenere un blocco in uscita. Quest'ultimo viene cifrato per produrre un secondo blocco in uscita, quindi si procede con il terzo, ecc. La sequenza di blocchi cifrati in uscita, chiamata keystream, viene utilizzata come un blocco monouso e applicata con uno XOR al testo in chiaro per ottenere il testo cifrato. IV (initialization vector) è utilizzato solamente nel primo passo, nei passi successivi l'output è cifrato. Il keystream è indipendente dai dati, così che può essere calcolato in anticipo, se necessario, ed è anche immune da errori di trasmissione. La decifrazione viene eseguita generando lo stesso keystream dal lato del ricevente. E' essenziale che non venga mai riutilizzata la coppia chiave-IV perché questo vorrebbe dire generare più volte lo stesso keystream. Questo implicherebbe esporre il testo cifrato ad attacchi di tipo keystream riutilizzato.

59. RSA

E' considerato un algoritmo molto robusto. Una gran parte delle applicazioni pratiche nel campo della sicurezza si basa su RSA. L'unico difetto di RSA è che richiede chiavi di 1024 bit per poter offrire una buona sicurezza, il che lo rende abbastanza lento. RSA si basa su alcuni principi di teoria dei numeri. Faremo riepilogo sull'uso di questo metodo:

- Scegliamo due numeri primi, p e q
- Calcoliamo n = p * q e z = (p – l) * (q – l)
- Scegliamo un numero relativamente primo rispetto a z, detto d
- Troviamo e tale che e*d = 1 mod z

La sicurezza del metodo è basata sulla difficoltà di scomporre in fattori primi i numeri molto grandi. Notiamo che RSA, per come l'abbiamo descritto, è simile a un algoritmo simmetrico in modalità ECB, cioè blocchi di input uguali originano lo stesso blocco di output: anche in questo caso occorre qualche forma di concatenamento. RSA è troppo lento per poterlo usare nella cifratura di grandi volumi di dati, mentre è spesso impiegato per la distribuzione delle chiavi.

60. Si descriva la tecnica di attacco birthday attack (RIMOSSO)

Si può pensare che ci voglia un numero di operazioni dell'ordine di 2^m per forzare un message digest di m bit. In realtà, spesso possono bastare 2^(m/2) operazioni, usando l'attacco del compleanno. L'idea per questo attacco viene da una tecnica che i professori di matematica usano spesso nei corsi di probabilità. La domanda è: quanti studenti ci devono essere in una classe perché la probabilità che due persone abbiano il compleanno lo stesso giorno superi ½? Se c'è una funzione fra input e output con n valori di input e k possibili valori di output, ci sono n(n-l)/2 coppie di input. Se n(n-l)/2 > k, la possibilità di avere almeno una coppia con lo stesso output è decisamente buona. Quindi, approssimativamente, per avere due output uguali basta avere n> √k. Questo risultato significa che un message digest di 64bit può essere forzato, con una buona probailità, generando 2^32 messaggi e cercandone due con lo stesso message digest.

61. Sicurezza in 802.11

Molti dei problemi di sicurezza delle reti wireless sono causati dal fatto che i produttori delle stazioni di trasmissione wireless (gli access point) vogliono semplificare l'uso di questi prodotti agli utenti finali. 802.11 in parte usa WPA2 (WiFi Protected Access 2). WEP era la vecchia generazione di protocolli di sicurezza di 802.11. Il WEP cifrava i dati per ottenere riservatezza tramite XOR con l'output di un cifrario a flusso. Utilizzava CRC a 32 bit. WPA2 è usato in due scenari comuni: un ambito aziendale e un ambiente domestico. Il traffico viene cifrato da delle chiavi calcolate come parte di un

handshake di autenticazione. L'handshake ha luogo appena dopo che il client si associa con una rete wireless e si autentica con un server di autenticazione. Viene generate una chiave master, che non viene però usata direttamente per cifrare i pacchetti. E' una pratica crittografica standard ottenere una chiave di sessione per ogni periodo di utilizzo. 802.11 utilizza il protocollo CCMP, che utilizza la cifratura AES con una chiave e una dimensione di blocco a 128 bit. La chiave arriva dalla chiave di sessione. I messaggi sono cifrati con AES in modalità counter.

62. Sicurezza in bluetooth

Bluetooth ha quattro modalità di sicurezza, che vanno dal nulla alla cifratura completa dei dati e il controllo dell'integralità. Bluetooth presente soluzioni di sicurezza su più livelli. A livello fisico, il salto di frequenza fornisce un margine di sicurezza minimo. Utilizza delle chiavi detta passkey. Per stabilire un canale, master e slave effettuano il controllo per vedere se l'altro conosce la passkey. Scelgono quindi una chiave di sessione a 128 bit, di cui alcuni bit possono essere resi pubblici. La cifratura in bluetooth usa uno stream cipher detto E0, il controllo di integrità usa SAFER+. Entrambi sono cifrati a blocco tradizionali con chiave simmetrica. Bluetooth autentica solo i dispositivi e non gli utenti, quindi il furto di un dispositivo può dare al ladro accesso ai dati finanziari, o comunque riservati dell'utente. Bluetooth implementa la sicurezza anche nei livelli superiori, quindi nel caso in cui ci sia una violazione a livello data link, rimane ancora un po' di sicurezza, specialmente per le applicazioni che richiedono l'inserimento manuale dalla tastiera di un PIN per poter completare la transizione.

63. Reflection attack

Il reflection attack è un tipo di attacco infromatica in cui un attaccante, invece di colpire direttamente la vittima, dirige il suo traffico verso un host intermedio (testa di ponte o reflector) e poi questo lo dirige verso la vittima. In genere per ottenere questo effetto nelle reti IP si usa l'IP spoofing. L'attaccante genere un pacchetto con l'indirizzo sorgente della vittima e l'indirizzo di destinazione del reflector. Il reflector risponde con un pacchetto che però, a causo dello spoofing, avrà come indirizzo quello della vittima. La vittima quindi riceverà pacchetti proveniente dal reflector e non riuscirà a risalire all'attaccante vero. Se l'attaccante è in grado di far sì che i sistemi intermedi mandino dei pacchetti di risposta più grossi dei pacchetti iniziali si è in presenza di un attacco di amplificazione. La vittima può difendersi con un firewall che sia stateful, che sia cioè in grado di scartare i pacchetti TCP fuori sequenza.

64. Replay attack

Nell'ambito della sicurezza informatica il replay-attack è una forma di attacco di rete che consiste nell'impossessarsi di una credenziale di autenticazione comunicata da un host ad un altro, e riproporla successivamente simulando l'identità dell'emittente. In genere l'azione viene compiuta da un attaccante che s'interpone tra i due lati comunicanti. Questo attacco permette operazioni fraudolente come falsa autenticazione e/o transazioni duplicate, senza dover necessariamente decrittare la password, ma soltanto ritrasmettendola in un tempo successivo. A differenza dell'attacco man in the middle che opera sempre in tempo reale, il replay attack può operare anche in modo asincrono quando la comunicazione originale è terminata. Gli attacchi di tipo replay si evitano con l'uso di token di sessione generati pseudocasualmente. Un'altra contromisura è quella di utilizzare una marca temporale e di far sì che questa sia inserita nel corpo del messaggio criptato.

65. Algoritmo diffie-hellman

Partendo a priori, quando due stazioni A e B non hanno ancora una chiave per comunicare segretamente tra loro, come fanno queste due ad impostare questa chiave senza che nessun altro la senta? Il protocollo che permette a due stazioni di scambiarsi una chiave segreta è chiamato scambio di chiave di Diffie-Hellman. Questo protocollo richiede come prima azione che A e B si mettano d'accordo su due numeri grandi, n e g, dove n è un numero primo, (n-1)/2 è pure primo, e g soddisfa certe condizioni particolari. Questi numeri possono essere pubblici, quindi uno dei due può scegliere la coppia di numeri e poi semplicemente la comunica all'altro. A questo punto la stazione A sceglie un numero grande, di 512 bit, x e lo tiene segreto, B fa lo stesso con y. A inizia il protocollo di scambio

della chiave inviando a B un messaggio contenente *n, g, g^x mod n*. B risponde inviando ad A *g^y mod n*. A prende il numero inviato da B e calcola *(g^y mod n)^x mod n*. B esegue un calcolo simile per ottenere *(g^x mod n)^y mod n*. Per le regole dell'aritmentica modulare le espressioni equivalgono. Il gioco è fatto, A e B hanno una chiave segreta uguale.

66. Man in the middle

L'attacco man in the middle si basa sul presupposto che l'attaccante sia in grado di intercettare la conversazione che sta avvenendo tra i due malcapitati, che riesca a catturare i messaggi, modificarli se necessario e rispedirli. L'attaccante intercetta il primo messaggio, diciamo da A verso B, e lo modifica, mandandolo modificato a B, attende una risposta, la intercetta, e la modifica, mandandola ad A, A e B non hanno idea di cosa stia succedendo, e pensano rispettivamente di parlare con l'altro. L'attacco man in the middle consiste proprio in questo. Vari algoritmi di riconoscimento rendono vano questo attacco, a meno che non inizi a priori, quando inizia la conversazione, ovvero quando vengono scambiati tra A e B i primi dati, per stabilire una connessione.

67. DNS spoofing

Il DNS spoofing è un tipo di attacco man in the middle. Quindi l'attaccante deve essere in grado di intercettare la conversazione. Questo attacco compromette il sistema DNS o forse solo la sua cache nell'ISP della vittima. Consiste nel modificare l'indirizzo IP del destinatario della richiesta della vittima con uno a piacere (magari il proprio). E' sufficiente penetrare nel server DNS e cambiare un record, compito molto semplice. Una cache che contiene un indirizzo IP intenzionalmente falsificato è detta poisoned cache (cache avvelenata). Questo attacco può essere sventato con l'uso nei server DNS di ID casuali nelle loro query. Essendo questi ID di soli 16bit, risulta facile per un computer scandirli tutti e quindi replicarli con un falso.

68. NAT

Gli indirizzi IP sono scarsi. Un approccio è quello di assegnare gli indirizzi IP ai computer in modo dinamico al momento della connessione e recuperarli al termine della sessione per essere assegnati ad altri computer che si connettono. Ma la soluzione adottata è un'altra, ed è chiamata NAT (Network Address Translation). L'idea di base di NAT è assegnare a ogni azienda o casa un singolo indirizzo IP per il traffico di internet. Dentro la rete del cliente, ogni computer riceve un indirizzo IP unico, utilizzato per instradare il traffico interno alla rete locale. Quando un pacchetto sta per lasciare la rete locale per dirigersi verso l'ISP viene eseguita una traduzione di indirizzo dall'unico indirizzo IP interno a quello pubblico condiviso. L'unica regola è che nessun pacchetto contenente questi indirizzi possa apparire su internet. La parte che effettua la conversione è chiamata apparato NAT, ed è spesso abbinato ad un firewall ed inserito all'interno di un singolo apparecchio che protegge la rete locale. L'unico problema è: quando da internet arriva un pacchetto, l'apparecchio NAT come riconosce la stazione locale a cui indirizzarlo? L'utilizzo del campo source port permette di risolvere il problema dell'associazione. NAT viola il modello gerarchico di IP, che afferma che ogni indirizzo IP identifica in modo univoco a livello mondiale una singola macchina.

69. 802.11

Le LAN wireless possono anche essere usate per permettere a due o più computer vicini di comunicare tra loro senza usare internet. Il principale standard per le LAN wireless è 802.11. Le reti 802.11 possono essere utilizzate in due modalità: quella più comune è connettere dei client, come portatili e smart phone, a un'altra rete, come una intranet o Internet. Nella modalità con infrastruttura, ogni client è associato ad un AP (Access Point) connesso a sua volta all'altra rete. L'altra modalità è una rete ad hoc. Questa modalità consiste in una collezione di computer associati tra loro che possono spedirsi direttamente i frame. Dal momento che l'accesso a Internet è la killer application per le reti wireless, le reti ad hoc non sono molto popolari.
Lo stack di protocolli è lo stesso per client e AP: il livello fisico corrisponde abbastanza bene al livello fisico OSI. In 802.11 il sottolivello MAC determina com'è allocato il canale, cioè a chi tocca trasmettere.

LLC (Logical Link Control) ha il compito di nascondere la differenza tra i differenti 802 e renderli indistinguibili a livello di rete.
Vi sono varie versioni di 802.11, ognuna retrocompatibile, e sono 802.11b/a/g/n. L'ultima versione, 802.11n, utilizza fino a quattro antenne per trasmettere fino a quattro flussi d'informazione contemporaneamente. I segnali di questi flussi interferiscono col ricevitore, ma possono essere separati utilizzando le tecniche di comunicazione MIMO (Multiple Input Multiple Output). L'utilizzo di più antenne dà una grande spinta alla velocità oppure migliora raggio di copertura e affidabilità.
Le interfacce radio sono quasi sempre half duplex, il che vuol dire che non possono trasmettere e controllare picchi di rumore nello stesso istante su una solo frequenza. Il segnale ricevuto può facilmente essere un milione di volte più debole di quello trasmesso, quindi non può essere sentito in contemporanea. 802.11 prova ad evitare le collisioni con CDMA/CA (CDMA with Collision Avoidance). 802.11 offre vari servizi: il servizio di associazione, usato dalle stazioni mobili per connettersi agli AP, la stazione invia una richiesta per associarsi con l'AP e questo ha la facoltà di accettare o rifiutare la richiesta; le riassociazioni, che permettono a una stazione di cambiare il suo AP preferenziale, utile alle stazioni che si spostano da un AP all'altro nella stessa LAN; e il servizio di autenticazione, gestito in modi diversi a seconda dello schema di sicurezza scelto. Con WPA2 l'AP può parlare con un server di autenticazione che ha un database di utenti e password per determinare se la stazione abbia il permesso di accesso alla rete; servizio di distribuzione determina come instradare i frame che raggiungono l'AP; servizio di integrazione gestisce ogni traduzione necessaria a un frame per essere spedito all'esterno della LAN o per farlo arrivare dall'esterno della LAN; servizio di spedizione usato per la trasmissione dei dati; servizio di privacy.

70. OSPF

Tutte le reti devono usare lo stesso protocollo di routing interdominio o exterior gateway protocol. OSPF (Open Shortest Path First) è un protocollo di routing intradominio di tipo link state. Questo protocollo si impone di rispettare i seguenti requisiti: essere open; supportare diverse metriche di distanza; essere un algoritmo dinamico, in grado di modificarsi rapidamente e automaticamente; supportare il routing basato sul tipo di servizio; eseguire il bilanciamento del carico; supportare sistemi gerarchici; e implementare un po' di sicurezza per impedire agli studenti in caccia di facile divertimento di imbrogliare i router inviando loro false informazioni di routing. OSPF supporta sia collegamenti punto a punto che reti broadcast. Questo protocollo calcola il percorso più breve in base al peso degli archi che collegano i router.

71. Handshake a 3 vie

Questo è un protocollo per l'impostazione di una connessione e richiede la verifica reciproca da parte de peer che l'attuale richiesta di connessione non sia un duplicato. L'host1 sceglie un numero di sequenza, x, e invia un segmento CONNECTION REQUEST contenente x all'host2, che risponde con un segmento ACK per confermare x e annunciare il suo numero di sequenza iniziale, y. Per finire, l'host1 conferma la scelta del numero di sequenza iniziale dell'host2 con il primo segmento di dati inviati. Se vi è presenza di segmenti di controllo duplicati: un CONNECTION REQUEST arriva all'host2 senza che l'host1 lo sappia, l'host2 risponde con un ACK, chiedendo in definitiva una conferma del fatto che l'host1 stia tentando di creare una nuova connessione. Quando l'host1 rifiuta il tentativo dell'host2 di stabilire una connessione, l'host2 comprende di essere stato ingannato da un duplicato in ritardo e abbandona la connessione. La disconnessione funziona in modo analogo, dopo aver inviato la richiesta, l'host1 attende un ACK, appena lo riceve rilascia la connessione e manda un ACK all'host2 che rilascia la connessione. Entrambi usano un timer per rilasciare la connessione in qualsiasi caso, anche di perdita di ACK.

72. Due principi crittografici fondamentali

Due principi fondamentali sono alla base dello studio dei diversi sistemi crittografici: la ridondanza e l'attualità.
Il primo principio afferma che tutti i messaggi cifrati devono contenere una qualche forma di ridondanza, cioè d'informazione non necessaria alla comprensione del messaggio. In altre parole, il destinatario, dopo aver decifrato il messaggio, deve essere in grado di stabilirne la validità con un semplice

esame del contenuto o con un breve calcolo. Questo tipo di ridondanza è necessario per prevenire gli attacchi degli intrusi attivi. Il rovescio della medaglia è che la ridondanza semplifica agli intrusi passivi la decifrazione del messaggio.
Il secondo principio crittografico afferma che è necessario avere la possibilità di verificare che ogni messaggio ricevuto sia attuale, cioè trasmesso di recente. Questo serve per evitare che intrusi attivi possano inviare messaggi vecchi spacciandoli per nuovi. Una possibilità consiste nell'includere un timestamp (data e ora) valido, per esempio, solamente per 10 secondi.

73. Message digest

Spesso ai metodi di firma si rivolge una critica: nel loro funzionamento riuniscono due funzioni distinte: l'autenticazione e la segretezza. In molti casi è necessaria l'autenticazione, ma non la segretezza; inoltre è più facile ottenere le licenze per l'esportazione della tecnologia se un sistema fornisce solo autenticazione e non segretezza. Una soluzione è il message digest (riassunto del messaggio), una funzione hash MD, che consiste nel costruire una stringa di lunghezza fissa, dato un qualsiasi input a lunghezza variabile. Questa tecnica ha quattro proprietà importanti: dato P, è facile calcolare MD(P); dato MD(P), è praticamente imposibile trovare P; dato P, nessuno è in grado di trovare P', trale che MD(P') = MD(P); se l'input cambia anche di 1 bit, l'output diventa completamente diverso.