Domande e risposte di Reti e Sicurezza

Autore: Federico Z.
Editore Latex: Riccardo A.

18 febbraio 2018

Premesse

Date le 65 domande che generalmente girano per l'esame di reti, mi sono permesso di reinterpretarle in maniera personale rispetto a quelle già presenti online, dando possibili risposte prendendo informazioni dal libro "Computer Networks 4th Edition" di Andrew S. Tanenbaum, unite a ricerche sul web e conoscenze personali. NON assicuro la correttezza delle risposte che NON vogliono neppure essere un riassunto al libro, vogliono servire come spunto e ripasso in preparazione dell'esame. Scià belli.
Federico Z.

Indice

1 Cosa si intende per serie di Fourier?

Un segnale che ha una durata finita può essere gestito immaginando semplicemente che esso ripeta infinite volte l'intero schema (intervallo T e 2T è identico all'intervallo 0 a T).

È possibile quindi rappresentare i segnali tramite funzioni, le quali permettono un'analisi e una modellazione più efficace. La Serie di Fourier non è altro che la scomposizione di un segnale in componenti sinusoidali (possibilmente infiniti).

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n sen(2\pi nft) + \sum_{n=1}^{\infty} b_n cos(2\pi nft)$$

$f = 1/T$ rappresenta la frequenza fondamentale, a_n b_n sono rispettivamente le ampiezze seno e coseno dell'n-esima armonica e c rappresenta una costante.

Su questo teorema si basano le reti e il passaggio dei dati tramite i mezzi di trasmissione; purtroppo nella pratica i mezzi di trasmissione attenuano in modo non uniforme i componenti della serie di Fourier, generando così una distorsione. Per ovviare a questa distorsione, le ampiezze fino ad una certa frequenza vengono trasmesse senza modifiche, da quella frequenza in poi vengono attenuate.

L'intervallo di frequenze trasmesse senza una forte attenuazione è chiamato Banda Passante. Generalmente nella realtà viene indicata la banda passante compresa tra 0 e la frequenza dove la potenza è attenuata del 50%.

2 Bitrate e Baudrate

Il **Bitrate** è la quantità di informazioni digitali che è trasferita o registrata nell'unita di tempo. Stiamo parlando quindi di velocità di trasmissione, espressa in bit/s. La velocità di trasmissione è anche detta Banda e dipende dal tipo di mezzo trasmissivo utilizzato e dalle sue condizioni fisiche al momento dell'uso.

Il **Baudrate** invece rappresenta il numero di simboli che viene trasmesso in un secondo. Non va confusa con il sopracitato bitrate in quanto misurano unità differenti; infatti ad un simbolo corrisponde un numero di bit differente in base alle tecniche di modulazione utilizzate.

3 Descrivere i vari tipi di cavo e confrontarli

I principali tipi di cavo utilizzato nelle telecomunicazioni sono: il doppino, il cavo coassiale e la fibra ottica.

Il doppino:
-Cos'è: è un cavo composto da due conduttori di rame isolati, spessi circa 1mm e avvolti uno intorno all'altro in una forma elicoidale. L'intreccio è utile per annullare i campi elettromagnetici generati dai due conduttori, i quali si annullano a vicenda. Esistono diverse varietà di doppini, i più importanti per le telecomunicazioni sono gli UTP3 e UTP5 (UTP= Unshielded Twisted Pair, doppini non schermati). Le differenze tra i doppini di categoria 3 e categoria 5 sta nel numero di spire per centimetro: minor numero di spire per cm negli UTP3 e maggiore negli UTP5. Un maggior numero di spire permette di migliorare la qualità del segnale trasmesso su lunghe distanze, a scapito però della quantità di materiale necessario. Esistono anche categorie superiori, i quali gestiscono segnali con banda più ampia.
-Applicazione: Il sistema di applicazione più diffuso per il doppino è il sistema telefonico. I doppini si possono utilizzare per trasmettere segnali analogici e digitali, l'ampiezza di banda dipende dal diametro del cavo e dalla distanza percorsa. Sono molto utilizzati grazie al basso costo e al discreto livello di prestazioni.

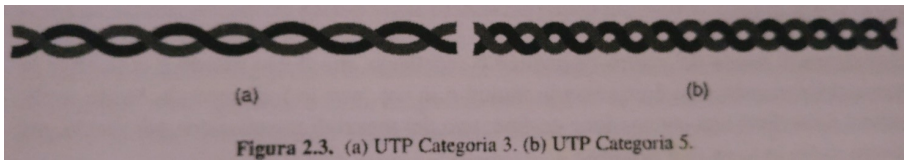


Figura 2.3. (a) UTP Categoria 3. (b) UTP Categoria 5.

Il cavo coassiale:
-Cos'è: è un cavo 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. La costruzione e la schermatura del cavo coassiale forniscono ampiezza di banda ed eccellente immunità al rumore. Ne esistono di due tipi, a 50Ω per le trasmissioni digitali e a 75Ω per quelle analogiche; non c'è una motivazione tecnica per questa distinzione.
-Applicazione: Il cavo coassiale è molto utilizzato per le reti metropolitane e le televisioni via cavo; la banda disponibile dipende dalla qualità, dalla lunghezza del cavo e dal rapporto segnale-rumore del segnale dati. Per molti ambiti il cavo coassiale è stato sostituito dalla fibra ottica per i tratti più lunghi.

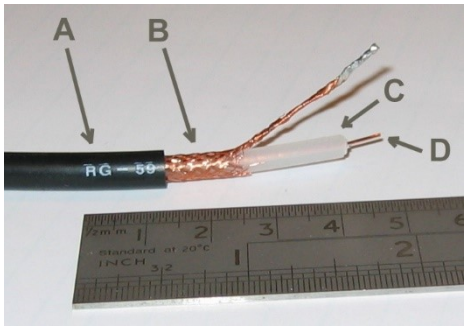
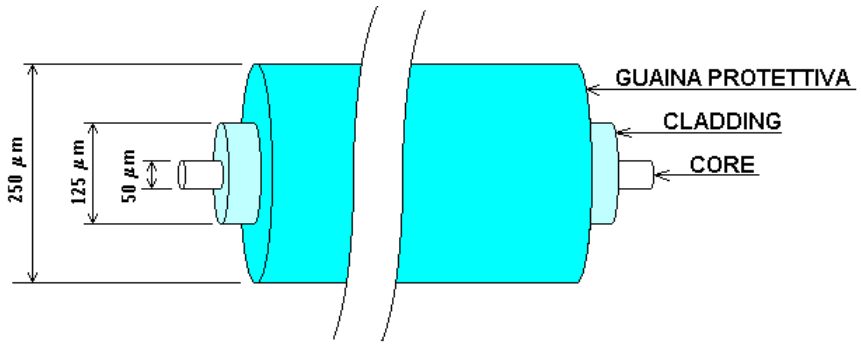


Figura 1: D: nucleo, C: rivestimento isolante, B: conduttore cilindrico, A: guaina protettiva

Fibra ottica:
-Cos'è: Un sistema di trasmissione ottico è formato da: sorgente luminosa, mezzo di trasmissione e rilevatore. I cavi in fibra ottica sono il mezzo di trasmissione di questo sistema, che si basa su segnali luminosi invece che elettrici. La fibra ottica è formata da un nucleo (core) di vetro, attraverso il quale si propaga la luce, ha uno spessore di 50 micron per le fibre multimodali mentre dagli 8 ai 10 micron per quelle monomodali.

Il nucleo è avvolto da un rivestimento di vetro (cladding) che ha un indice di rifrazione più basso; ciò costringe la luce a rimanere nel nucleo. L'ultimo strato è formato da plastica e serve a proteggere il rivestimento. Generalmente le fibre sono raggruppate in fasci, protetti da un'ulteriore guaina più esterna.



Esistono due tipi di fibra, la monomodale e la multimodale. La monomodale è più costosa e utilizzata soprattutto per le lunghe distanze, in cui la luce può propagarsi solo in linea retta senza rimbalzare. Nella multi-

modale invece può contenere più raggi che rimbalzano ad angoli diversi, in questo caso si dice che ogni raggio ha una modalità diversa, da qui il nome multimodale.

Le fibre si possono collegare in diversi modi:

- Tramite connettori in apposite prese, perdono il 10-20% di luce ma semplificano la riconfigurazione dei sistemi.
- Attaccate meccanicamente, tramite una manichetta speciale viene pinzato, viene poi allineato in modo da massimizzare il segnale, perdita del 10%
- Fusione delle due parti, genera una piccola attenuazione.

-Applicazione: La fibra è molto utilizzata nelle LAN e nei sistemi di trasmissioni a lunga distanza e apporta diversi vantaggi rispetto al cavo in rame:

- Maggiore ampiezza di banda.
- I ripetitori possono essere installati ogni 50km rispetto ai 5km dei cavi in rame, con un evidente risparmio.
- Non è influenzata da sorgenti elettriche, dai campi elettromagnetici e dalle interruzioni della linea elettrica, la fibra è adatta anche agli ambienti più inospitali.
- La fibra è sottile e leggera, occupando meno spazio permette alle aziende telefoniche di svuotare i condotti ormai saturi di cavi.
- Le fibre non perdono la luce ed è difficile intercettare i dati, questo le rendono molto più sicure rispetto ai cavi in rame.

Presenta tuttavia degli svantaggi, che nonostante tutto non limitano troppo questa tecnologia, che rappresenta il futuro per le telecomunicazioni. Tra gli svantaggi troviamo:

- Tecnologia meno nota, richiede conoscenze che non tutti gli ingegneri possiedono.
- Si può danneggiare se la si piega troppo.
- La trasmissione è unidirezionale, di conseguenza, per avere una comunicazione bidirezionale è richiesta una doppia fibra o due bande di frequenza in una sola.
- Le interfacce per la fibra ottica costano di più di quelle elettriche.

4 Caratteristiche e confronto tra i vari tipi di satellite: GEO, MEO e LEO

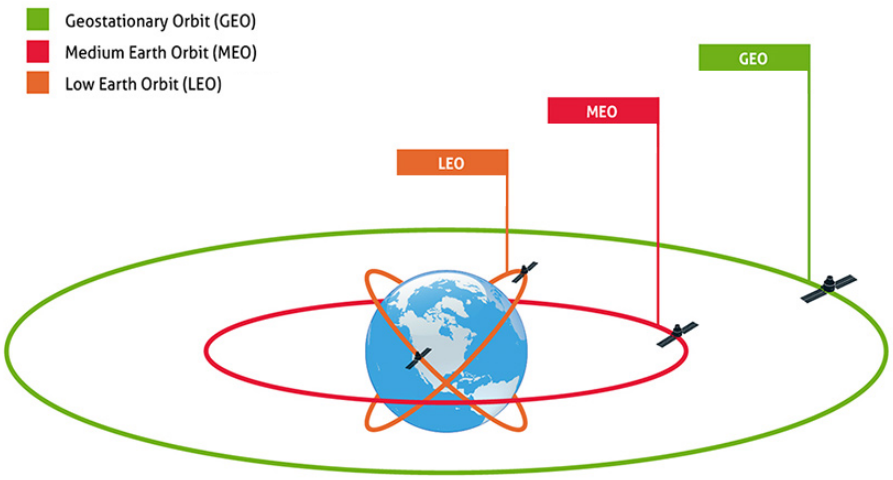
Un satellite di comunicazioni può essere immaginato come un grande ripetitore di microonde posto nel cielo. Questo dispositivo contiene diversi transponder, ossia ricetrasmettitori satellitari, i quali ascoltano una parte dello spettro, amplificano il segnale e lo ritrasmettono su altre frequenze per evitare interferenze.

La collocazione dei satelliti è importante, e determinata da alcuni fattori:

- Il periodo orbitale: più alto è il satellite, più lungo è il periodo.
- Le fasce di Van Allen distruggerebbero velocemente un satellite che le attraversasse.

Esistono quindi 3 zone in cui i satelliti possono essere collocati

- LEO: sotto la fascia di Van Allen inferiore
- MEO: tra la fascia VA inferiore e quella superiore
- GEO: molto al di sopra della fascia VA superiore



GEO GEO (Geostationary Earth Orbit), sono collocati nella fascia più alta, disposti con un intervallo di 2° nel piano equatoriale, così da evitare interferenze, di conseguenza c'è posto per "solo" 180 satelliti di questo tipo, la loro dimensione è importante e la gestione dell'allocazione degli slot orbitali è motivo di disputa tra paesi, stazioni televisive e militari.

MEO Tra le due fasce di Van Allen troviamo i satelliti MEO (Medium Earth Orbit), questi satelliti si spostano lentamente lungo la longitudine, impiegando 6 ore per compiere un giro attorno al pianeta, attualmente non sono utilizzati per le telecomunicazioni. Rispetto al GEO, il MEO permette un ritardo di propagazione inferiore, tuttavia si perde la comodità del "punto fisso" garantito dal GEO, questo perché il MEO si sposta più velocemente.

LEO I LEO (Low Earth Orbit) sono i più bassi tra i tre tipi; si spostano molto velocemente, di conseguenza un sistema completo richiede l'utilizzo di molti satelliti di questo tipo. D'altra parte, le stazioni terrestri non hanno bisogno di molta energia per la comunicazione e i ritardi sono di pochi millisecondi. Questo tipo di satellite tratta prevalentemente trasmissione voce e servizi internet/GPS.

Una menzione particolare va fatta alla differenza tra satelliti e fibra: quale preferire?
Non esiste una risposta ben definita, la fibra grazie alla sua comodità sembrava avesse preso dominio nel mercato, tuttavia i satelliti avevano applicazione in campo in cui la fibra non poteva arrivare:

- La fibra non è attualmente disponibile a una gran parte dell'utenza, mentre per i satelliti, l'utente basta che innalzi un'antenna sul tetto di casa per ottenere una maggiore ampiezza di banda.
- Comunicazione mobile, la fibra ottica non è di nessuna utilità per questa categoria, mentre i collegamenti satellitari potenzialmente ce l'hanno.
- Comunicazione broadcast, un messaggio inviato da un satellite può essere ricevuto contemporaneamente da migliaia di stazioni terrestri.
- Comunicazione in luoghi con terreni inospitali o scarsamente dotati di infrastrutture.

Il sistema di comunicazione principale del futuro sarà quello terrestre basato su fibre ottiche, combinato con la rete radio cellulare, tuttavia per alcune applicazioni specifiche i satelliti sono migliori.

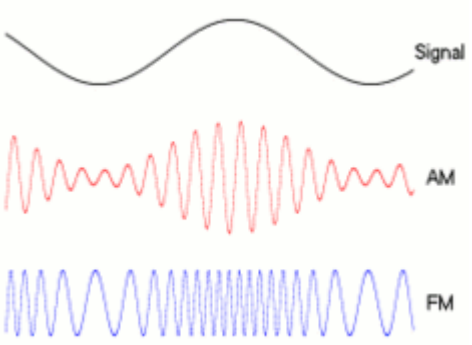
5 Cos'è la modulazione in frequenza?

Durante l'invio di informazioni, il segnale può subire attenuazione, distorsione o venir disturbata dal rumore; questo porta ad evitare l'uso di un

largo intervallo di frequenze, ma sfortunatamente le onde quadre utilizzate nei segnali digitali utilizzano un ampio spettro di frequenza, e perciò sono soggette ad una forte attenuazione e alla distorsione.

Questi effetti rendono adatta la trasmissione in banda base (DC) solo a velocità basse e distanze brevi.

Per aggirare questi problemi viene usata la trasmissione AC, un tono continuo (portante d'onda sinusoidale) nell'intervallo compreso tra 1000 e 2000Hz, il quale permette la modulazione della sua ampiezza (AM), frequenza (FM) o fase.



La modulazione in frequenza non è altro che una tecnica di trasmissione utilizzata per trasmettere informazioni usando la variazione di frequenza dell'onda portante. Rispetto alla modulazione in ampiezza ha il vantaggio di essere molto meno sensibile ai disturbi e permette una trasmissione di miglior qualità. Ha inoltre un'efficienza energetica molto maggiore dato che la potenza del segnale modulato FM è esclusivamente quello della portante.

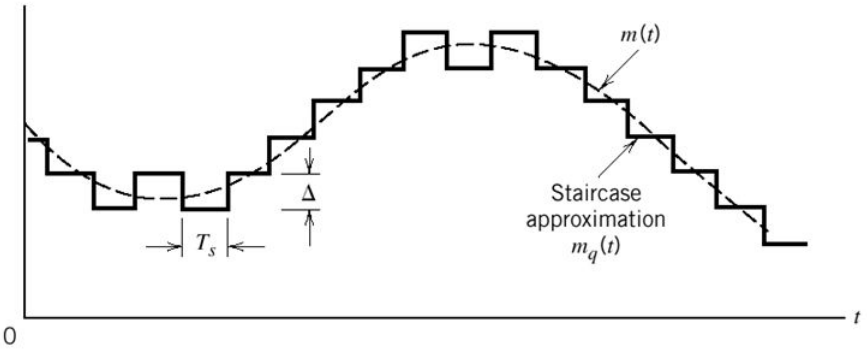
Il difetto principale è la necessità di circuiti più complessi, sia per la generazione del segnale sia per la ricezione. L'attuale tecnologia ha permesso di superare queste problematiche, rendendo la modulazione in frequenza molto più usata rispetto a quella in ampiezza, soprattutto in ambito di broadcasting commerciale.

6 Cos'è la modulazione delta (delta modulation)?

La delta modulation è un metodo di digitalizzazione e compressione di un segnale analogico. Si basa sul fatto che il segnale cambia in modo relativamente lento rispetto alla frequenza di campionamento, ciò rende gran parte dell'informazione ridondante.

Questo metodo prevede che ogni valore campionato differisca dal precedente di +1 o -1, sotto queste condizioni è possibile trasmettere un singolo bit che dice se il nuovo campione è maggiore o minore del precedente.

Un problema si ha se il segnale cambia troppo rapidamente, in quel caso si perdono informazioni.



7 Descrivere in dettaglio il GSM (Global System for Mobile connection)

Esistono tre generazioni distinte di telefoni cellulari ognuna caratterizzata da una diversa tecnologia:

- Voce analogica
- Voce digitale
- Voce e dati digitali (Internet, posta elettronica ecc.)

Il GSM tratta dei telefoni della seconda generazione: voce digitale. La sua struttura è formata da 4 tipi di celle: macro, micro, pico e umbrella. Le prime sono le più grandi, sono sopraelevate rispetto gli edifici e hanno un raggio massimo di 35 km. Le micro sono più piccole, coprono un'altezza pari agli edifici. Le pico sono molto piccole, usate in aree molto dense, tipicamente indoor. Umbrella è una piccola estensione, usata per coprire i buchi tra le varie celle sopracitate.

Sfrutta il multiplexing a divisione di frequenza, con ogni apparecchio che trasmette su una frequenza e riceve su una frequenza più alta. Una singola coppia di frequenza è divisa in slot temporali e condivisa tra più utenti attraverso un meccanismo di multiplexing a divisione di tempo.

Questi fattori lo rendono molto simile al D-AMPS, tecnologia molto utilizzata in America, che condivide la stessa generazione di telefoni. Tuttavia, GSM sono molto più ampi di quelli AMPS e contengo un numero poco più alto di utenti, perciò la velocità dati per utente di GSM è superiore a quella di D-AMPS.

Un sistema GSM ha 124 coppie di canali simplex e supporta otto connessioni separate mediante multiplexing a divisione di tempo. A ogni stazione attiva è assegnato uno slot temporale su una coppia di canali.

Trasmissione e ricezione non avvengono nello stesso intervallo temporale perché GSM non è in grado di trasmettere e ricevere contemporaneamente.

Il GSM introduce anche l'utilizzo della SIM card, in cui vengono memorizzati i dati descrittivi dell'abbonato e ha la funzione principale di fornire autenticazione ed autorizzazione all'utilizzo della rete.

8 Si descriva la tecnica CDMA (Code Division Multiple Access), possibilmente con esempio

Esistono tre generazioni distinte di telefoni cellulari ognuna caratterizzata da una diversa tecnologia:

- Voce analogica
- Voce digitale
- Voce e dati digitali (Internet, posta elettronica ecc.)

Il CDMA tratta dei telefoni della seconda generazione: voce digitale. D-AMPS e GSM sono sistemi che utilizzano FDM e TDM per dividere lo spettro in canali e i canali in slot temporali. CDMA invece di dividere l'intero intervallo di frequenze assegnate in poche centinaia di canali a banda stretta, permette ad ogni stazione di trasmettere per tutto il tempo attraverso l'intero spettro di frequenza. Trasmissioni multiple simultanee sono separate usando la teoria della codifica. La capacità del CDMA è di riuscire a estrarre il segnale desiderato scartando tutto il resto.

In CDMA, ogni tempo bit è suddiviso in m intervalli chiamati chip. In genere ci sono 64 o 128 chip per ogni bit. Ad ogni stazione è assegnato un codice di m-bit univoco chiamato sequenza di chip. Per trasmettere un bit 1, una stazione invia la sua sequenza di chip; per trasmettere un bit 0 la stazione invia il complemento a uno della propria sequenza di chip. Ogni stazione adotta una sequenza di chip univoca.

CDMA rispetto a GSM e D-AMPS opera in una banda di 1,25MHz, permettendo agli utenti di avere un'ampiezza di banda considerevole. Una sequenza di chip e il suo contrario sono a due a due ortogonali (il prodotto interno normalizzato è 0). Per generare queste sequenze di frammento ortogonali si utilizza un metodo noto come codici Walsh. Se la sequenza di chip ricevuta è S e il ricevitore sta cercando di ascoltare una stazione la cui sequenza di chip è C, il prodotto interno normalizzato da calcolare è S*C; facendo i calcoli si possono eliminare i termini superflui grazie all'ortogonalità dei valori, estraendo correttamente il valore trasmesso da C. Ad esempio, A e C trasmettono 1, B trasmette 0. Il ricevitore vede la somma S=A+!B+C e calcola:

$$S * C = (A+!B + C) * C = A * C + B * C + C * C = 0 + 0 + 1 = 1$$

I primi due termini spariscono perché le sequenze di chip sono state scelte per essere ortogonali.

9 Il GPRS: Cos'è? Pregi e difetti

Esistono tre generazioni distinte di telefoni cellulari ognuna caratterizzata da una diversa tecnologia:

- Voce analogica
- Voce digitale
- Voce e dati digitali (Internet, posta elettronica ecc.)

GPRS è un'evoluzione tra la seconda e la terza generazione di telefoni cellulari. È una rete a pacchetti costruita sopra D-AMPS e GSM. Questa permette alle stazioni mobili di inviare e ricevere pacchetti IP in una cella basata su un sistema vocale.

Quando GPRS è operativo vengono riservate alcuni slot temporali posti su alcune frequenze, per il traffico di pacchetti. Gli slot disponibili sono divisi in canali logici, la stazione base determina l'associazione tra i canali logici e time slot. Un canale logico è usato per scaricare i pacchetti dalla stazione base nella stazione mobile e ogni pacchetto indica il destinatario.

Per inviare un pacchetto IP, una stazione mobile chiede uno o più slot inviando una richiesta alla stazione base. Se la richiesta arriva senza problemi, la stazione comunica all'apparecchio mobile la frequenza e gli slot che

dovrà utilizzare per trasmettere il pacchetto. Una volta arrivato alla stazione base, il pacchetto è trasferito su Internet attraverso una connessione via cavo.

I vantaggi rispetto ai suoi predecessori stanno nel fatto che lo spreco di banda inesistente e viene utilizzata una tariffa a traffico e non a tempo. GPRS aggiunge il supporto a PPP e IP.

10 Handoff cos'è e vari tipi

Nell'ambito della telefonia mobile, con "Handoff" si intende la procedura per la quale un terminale cambia il canale (frequenza e slot di tempo) che sta utilizzando durante una comunicazione.

Un'area geografica è divisa in celle, al centro di ogni cella si trova una stazione base che comunica con tutti i telefoni che si trovano nella cella.

Quando un telefono mobile abbandona fisicamente una cella perché si accorge che il segnale si sta affievolendo, la stazione base di quella cella verifica il livello di potenza del segnale ricevuto dalle stazioni 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 della nuova centrale di controllo e viene forzato al cambiamento, questo è l'handoff.

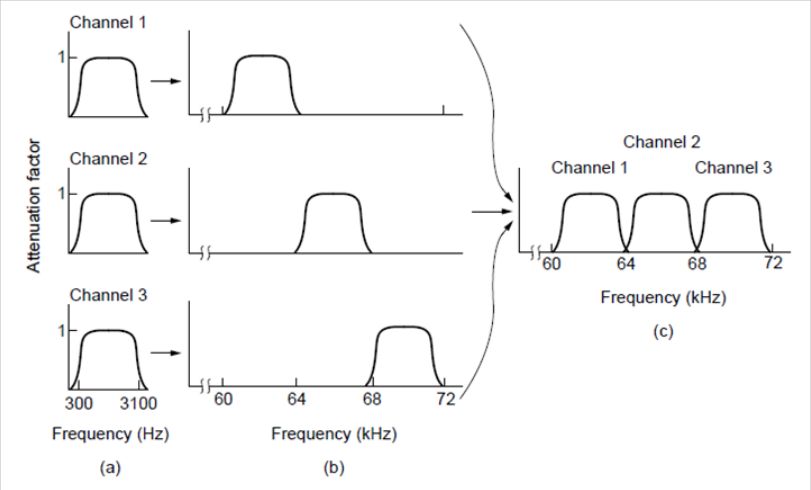
Esistono due tipi di handoff: il soft e l'hard handoff. Nel soft handoff il telefono è acquisito dalla nuova stazione di base prima di interrompere il segnale precedente, il vantaggio sta nel fatto che non vi è nessuna perdita di continuità, tuttavia il telefono deve riuscire a gestire più frequenze nello stesso momento (né i telefoni di prima generazione ne seconda sono in grado).

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 (ad esempio se non è disponibile nessuna frequenza) il segnale viene interrotto bruscamente, con il risultato di terminazione brusca di una possibile chiamata.

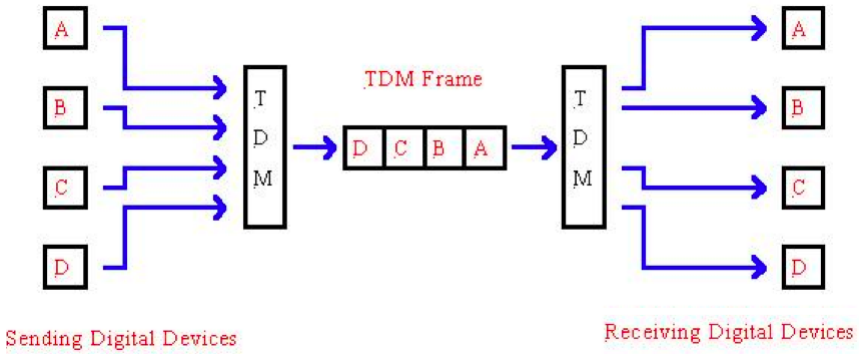
11 FDM, TDM, CDM: Algoritmi per la selezione della banda

FDM (Frequency Division Multiplexing) è una tecnica di condivisione delle risorse trasmissive di un canale di comunicazione. L'intero canale trasmissivo disponibile è diviso in sotto canali, ognuno costituito da una banda di frequenza e separato da un altro grazie ad un piccolo intervallo

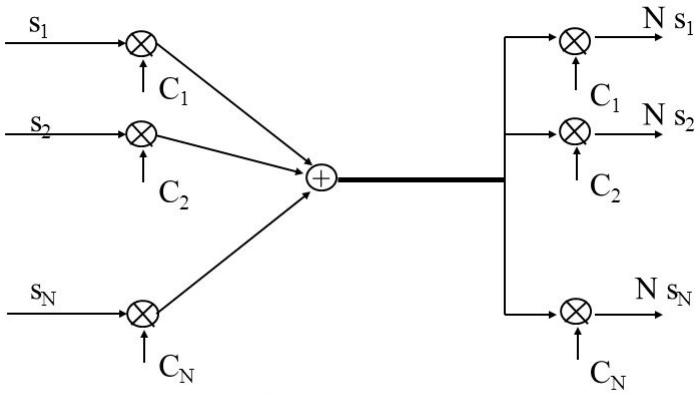
di guardia. Questo permette la condivisione dello stesso canale da parte di dispositivi che utilizzano diverse regioni di frequenze e utenti che possono cosi comunicare contemporaneamente senza interferirsi tra loro. Questa tecnica è comunemente utilizzata nelle trasmissioni televisive, radiofoniche, telefoniche o di dati. Anche le reti cellulari utilizzano in parte questo tipo di multiplazione per suddividere e assegnare l'intera capacità trasmissiva o banda radio disponibile alle varie celle di copertura servite da stazioni radio base.



TDM (Time Division Multiplexing) è una tecnica di condivisione di un canale di comunicazione secondo la quale ogni dispositivo ricetrasmittente ottiene a turno l'uso esclusivo dello stesso per un breve lasso di tempo. Il tempo di utilizzo del canale è diviso in frame tutti della stessa durata, questi frame sono ulteriormente divisi in slot. Confrontato all'FDM il TDM risulta essere più efficiente in quanto elimina la necessità degli intervalli di guardia o separazione tra le varie bande di frequenza. Necessita tuttavia di un circuito di sincronizzazione temporale in ricezione per l'estrazione del time-slot di competenza.



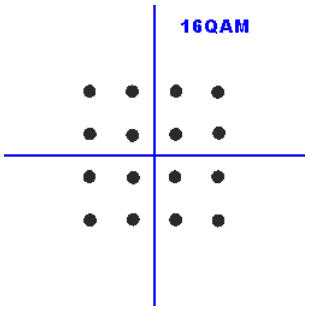
CDM (Code Division Multiplexing) o conosciuta anche come CDMA è il protocollo di accesso multiplo a canale condiviso. Offre una maggiore velocità di trasmissione di dati rispetto a TDM e FDM. Questa tecnica è realizzata moltiplicando in trasmissione l'informazione generata per un'opportuna parola detta chip; la sequenza in uscita dal moltiplicatore sarà successivamente modulata e infine trasmessa sul canale. In ricezione il segnale ricevuto sarà costituito dalla somma vettoriale di tutti i segnali trasmessi dalle singole stazioni. Grazie all'ortogonalità dei chip delle sorgenti, l'estrazione dell'informazione associata a ciascuna sorgente potrà essere fatta moltiplicando il segnale ricevuto con il particolare codice associato alla determinata sorgente che si vuole estrarre. La miglior efficienza rispetto alle precedenti forme di multiplazione è dovuta al fatto che ciascun canale utilizza l'intera banda di frequenza assegnata al servizio per tutto il tempo che desidera, e la non-interferenza è assicurata grazie all'uso di codici ortogonali.



$$\left(\sum_{i=0}^{N-1} s_i C_i\right) \cdot C_k = N \cdot s_k$$

12 QAM e QAM16

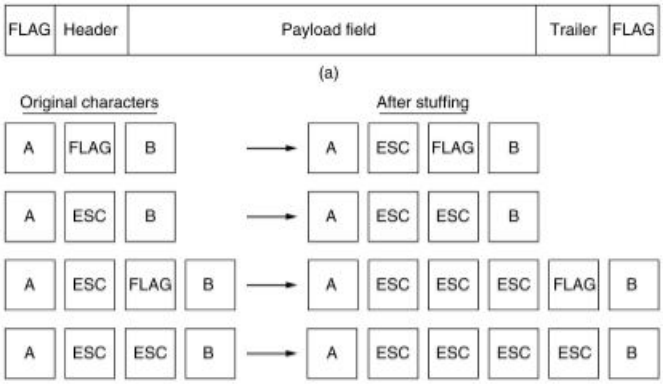
QAM è un sistema di modulazione numerica di ampiezza in quadratura, sia digitale che analogica. Le portanti sono sinusoidi. Il termine quadratura indica che differiscono di 90°. Il segnale in ingresso viene suddiviso e modulato per l'ampiezza. Nel caso di segnali digitali si sommano i segnali modulati e si ottiene una forma d'onda che risulta una combinazione della modulazione di fase e quella d'ampiezza. Ciascun tipo di modulazione QAM è caratterizzato da un diagramma (costellazione) su cui sono rappresentati tutti gli stati della portante. La QAM, rispetto alla PSK (Phase shift keying), migliora l'immunità al rumore. QAM16 non è altro che un tipo di costellazione del QAM, utilizzando quattro ampiezze e quattro fasi, per un totale di 16 diverse combinazioni. Ogni modem ad alta velocità ha un suo schema di costellazione e può comunicare solo con altri modem che adottano lo stesso schema (anche se generalmente un modem riesce a emulare anche quelli più lenti).



13 Cos'è il byte stuffing?

Lo strato data link deve servire lo stato network, per farlo necessita di usare a sua volta le informazioni fornite dallo strato fisico il cui scopo è quello di prendere un flusso di bit e cercare di portarli a destinazione. Non esiste nessuna garanzia per la correttezza dei dati, i bit potrebbero essere maggiori, minori, modificati ecc. Uno dei compiti dello strato data link è quello di rilevare ed eventualmente correggere questi errori. Il modo per rinvenire questi errori è quello di suddividere il flusso dei bit in frame, per poi controllarli, uno dei metodi di framing è quello di utilizzare un flag byte con il byte stuffing. Il byte stuffing prevede l'uso di un flag per delimitare l'inizio e la fine dei frame. In questo modo quando il destinatario perde la sincronizzazione può cercare il flag byte per trovare la fine del frame

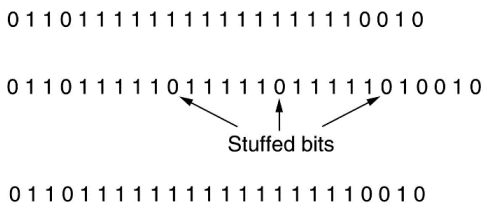
corrente. Due flag byte consecutivi indicano la fine di un frame e l'inizio del successivo. Per far si che un flag byte sia contenuto internamente ai dati, bisogna utilizzare un byte di escape (ESC) prima di ogni occorrenza "accidentale" del byte flag nei dati. Successivamente lo strato data link della destinazione provvederà a rimuovere i byte di escape prima di passare i dati allo strato network, se anche un carattere ESC si trova dentro i dati, va preceduto da un ulteriore carattere ESC. Questo metodo di framing presenta notevoli svantaggi, in primis quello di essere legato all'uso di caratteri da 8 bit, non tutte le codifiche dei caratteri li usano. Un altro problema deriva dalla quantità di caratteri superflui da inserire per effettuare lo stuffing, per questo si è sentita la necessità di sviluppare una nuova tecnica di framing che consente di gestire caratteri di lunghezza arbitraria (bit stuffing). Il byte stuffing è usato in PPP (Point-to-Point Protocol).



14 Cos'è il bit stuffing?

Lo strato data link deve servire lo stato network, per farlo necessita di usare a sua volta le informazioni fornite dallo strato fisico il cui scopo è quello di prendere un flusso di bit e cercare di portarli a destinazione. Non esiste nessuna garanzia per la correttezza dei dati, i bit potrebbero essere maggiori, minori, modificati ecc. Uno dei compiti dello strato data link è quello di rilevare ed eventualmente correggere questi errori. Per risolvere i problemi e le limitazioni provocate dal byte stuffing, viene sviluppata una nuova tecnica di framing , che prende il nome di bit stuffing, questa nuova tecnica permette di creare data frame che contengono sia un numero arbitrario di frame, sia codifiche di carattere con un numero arbitrario di bit. Ogni frame comincia e finisce con un gruppo speciale di bit "0111110" (flag byte). Ogni volta

che lo strato data link della sorgente incontra cinque “1” consecutivi nei dati inserisce automaticamente un bit con valore 0 nel flusso in uscita. La destinazione quindi quando riceve cinque bit consecutivi con valore 1 seguiti da uno 0, automaticamente elimina lo 0. Con il bit stuffing il confine fra i due frame viene riconosciuto in modo inequivocabile tramite l’uso della sequenza flag.



15 Numero di bit necessari per riconoscimento (correzione) degli errori di trasmissione?

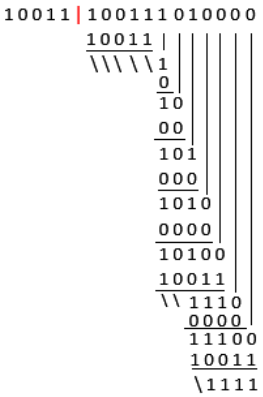
I dati trasmessi nei collegamenti locali sono spesso soggetti ad errori, per la loro gestione sono state sviluppate due strategie di base: la prima si basa su una codifica a correzione d’errore mentre la seconda è una codifica a rilevazione d’errore. La prima introduce una ridondanza (in ciascun blocco trasmesso) tale da riuscire a ricostruire il messaggio in caso di anomalie. La seconda invece introduce ridondanza sufficiente solo a capire che c’è stato un errore, ma non di correggerlo. Un frame generalmente consiste di m bit di dati e r bit ridondanti per i controlli, la somma n=m+r è la lunghezza totale del frame chiamata codeword di n bit. Date due codeword, per capire quanti bit corrispondenti sono differenti bisogna effettuare l’OR esclusivo e contare il numero di bit a “1” nel risultato, questo numero è chiamato distanza di Hamming. Detto questo, per trovare d errori è necessaria una codifica con distanza d+1, quando la destinazione vede una codeword non valida riesce a determinare che c’è stato un errore, ma non a correggerlo. Per correggere d errori è necessaria una codifica con distanza 2d+1, in tal modo codeword legali sono distanziate in modo tale che anche con d cambiamenti la codeword originale è sempre più vicina di ogni altra, può quindi essere determinata univocamente. Un semplice esempio di codifica a rilevazione d’errore si può realizzare aggiungendo un bit di parità ai dati, calcolato in modo che il numero di “1” nella codeword sia sempre pari (o dispari). Entrambe le codifiche trovano uso in diversi ambienti: Nelle reti wireless, in cui è presente molto rumore, conviene utilizzare una codifica a correzione d’errore,

cosi da ricostruire il messaggio in caso di errori, invece di farselo rispedire rischiandone di ulteriori. Sui canali affidabili invece è più economico usare codifiche a rilevazione, ed eventualmente farsi ritrasmettere il blocco. Questo perché, anche come visto dalla formula, per correggere gli errori abbiamo bisogno di molti più bit rispetto ad accorgersene solamente.

16 Si descriva cos'è il CRC (Cycle Redundancy check). Si calcoli inoltre il CRC di 10011101 usando il polinomio generatore di $x^4 + x + 1$

Il CRC o Cycle Redundancy Check, è un metodo per il calcolo di somme di controllo, serve a individuare errori casuali nella trasmissione di dati (causati da interferenze, rumori di linea o distorsione). Non è utile invece nel caso di tentativi intenzionali di manomissione. Il CRC tratta le sequenze di bit come dei polinomi a coefficienti che possono assumere solo valori "0" o "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. Questo polinomio è detto di grado k-1 e il coefficiente più alto è quello più a sinistra del polinomio (es 110001 ha 6 bit, quindi rappresenta un polinomio di 5° grado con coefficienti 1,1,0,0,0 e 1: $x^5 + x^4 + x^0$.

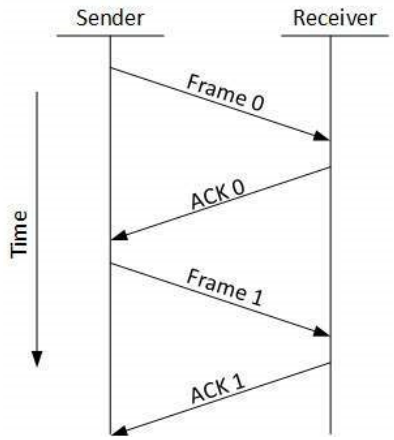
Quando si utilizza una codifica di questo tipo, sorgente e destinazione devono mettersi d'accordo in anticipo su un polinomio generatore G(x). Che deve avere i bit di ordine più alto e più basso a "1". Per poter calcolare il checksum di un frame di m bit, quest'ultimo dev'essere più lungo del polinomio 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). Quando la destinazione riceve il frame con il checksum e prova a dividerlo per G(x). Se c'è un resto vuol dire che c'è stato un errore di trasmissione. Ora proviamo con l'esempio di un frame 10011101 con polinomio generatore $x^4 + x + 1$: Frame: 1 0 0 1 1 1 0 1 Generatore G(x): 1 0 0 1 1 Il grado di G(x) è 4, aggiungo 4 "0" al frame (ottenendo un nuovo frame M(x)) in modo da poter dividere le due parti ottenendo il resto da sottrarre al M(x). M(x)= 1 0 0 1 1 1 0 1 0 0 0 0 Effettuo la divisione:



1 1 1 1 è il resto di conseguenza, il frame trasmesso è 1 0 0 1 1 1 0 1 1 1 1 1.

17 Descrivere il protocollo stop-and-wait, pregi e difetti

Durante la ricezione dei dati, il frame viene controllato, e a seconda se è integro o meno, si segue uno dei tre diversi protocolli più comuni: Stop-and-wait è il più semplice tra questi. Un mittente manda solo un frame alla volta, il destinatario, dopo aver ricevuto il frame corretto, invia un ACK (Acknowledge) al mittente, che a sua volta provvede a spedire il secondo frame e cosi via. Se l'ACK non raggiunge il mittente, questo provvederà a inviare nuovamente lo stesso frame dopo aver atteso un certo tempo (timeout). Altri problemi sorgono quando l'ACK arriva danneggiato, in quel caso il mittente invia nuovamente il frame, con il risultato che il destinatario si trova due frame uguali, senza sapere se è un duplicato o se effettivamente il pacchetto successivo ha gli stessi dati, per questo è stato implementato un numero di sequenza per i frame, e il destinatario invia l'ACK inerente a quel frame. Anche in questo caso sorgono problemi di dissincronia, in cui, sbagliando i numeri dei frame si rischia di perderne molteplici. Concludendo lo stop-and-wait è parecchio inefficiente rispetto agli altri protocolli di "comunicazione di richiesta di ripetizione automatica", specialmente a causa del tempo che intercorre tra l'invio dei vari pacchetti e contando anche il fatto che essendoci gli ACK il tempo di comunicazione aumenta considerevolmente, limitando la capacità del canale di comunicazione.



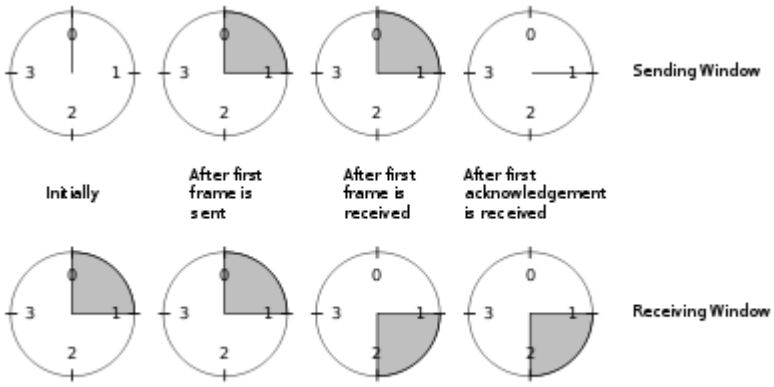
18 Cos'è il piggybacking?

Molti protocolli di comunicazione necessitano di inviare l'ACK come segnale di avvenuta ricezione del frame. Fatto per ogni singolo frame, questo invio rischia di intasare inutilmente il canale di comunicazione, allungando i tempi e incorrendo in molteplici errori. La tecnica del piggybacking permette di aggiungere l'ACK al frame di dati in uscita, utilizzando il campo ack nell'intestazione di questo. In questo modo l'acknowledgement si procura un passaggio gratis insieme al successivo frame dati trasmesso. Questo avviene quando arriva un frame di dati, la destinazione non invia subito un frame di controllo separato, ma aspetta che lo strato network gli passi il successivo pacchetto. Un problema può sorgere in caso di attesa molto lunga del pacchetto, poiché si rischia di far scattare il timer del mittente che re-invia il frame nell'attesa dell'ACK, in questo caso si decide un timeout in modo tale da fare piggybacking nel caso in cui il pacchetto da inviare è pronto in tempi celeri, altrimenti si invia l'ACK in modo indipendente. Il vantaggio principale sta nel miglior uso della banda disponibile, inoltre un minor numero di frame inviati significa anche un minor numero di interrupt "frame in arrivo", con conseguente minor necessità di buffer.

19 Si descriva la tecnica dello Sliding window

Sliding window è una classe di protocolli di controllo di flusso di dati, usato in particolare dal TCP. Una sliding window è formata da una finestra di invio e da una finestra di ricezione. La prima indica i frame che è autorizzata ad inviare, la seconda invece corrisponde all'insieme dei frame che può

accettare. La finestra di invio contiene i frame da spedire, o spediti ma in attesa di ack, lo scopo è quello di mantenere nel buffer più frame, in modo da ritrasmetterli in caso di problemi. Se questo buffer è pieno, il livello data link costringe il livello network a sospendere la consegna di pacchetti. Quando si ottiene un ack il frame corrispondente esce dalla finestra lasciando posto ad altri. Analogamente, il destinatario mantiene una finestra corrispondente agli indici dei frame che possono essere accettati, se arriva un frame il cui indice è fuori dalla finestra questo viene scartato (senza invio dell'ack). Se l'indice è dentro la finestra, il frame viene accettato, viene spedito l'ack e si sposta in avanti la finestra. Le finestre di mittente e destinatario non devono avere necessariamente uguali dimensioni.



A sliding window with a 2-bit sequence, of size 1

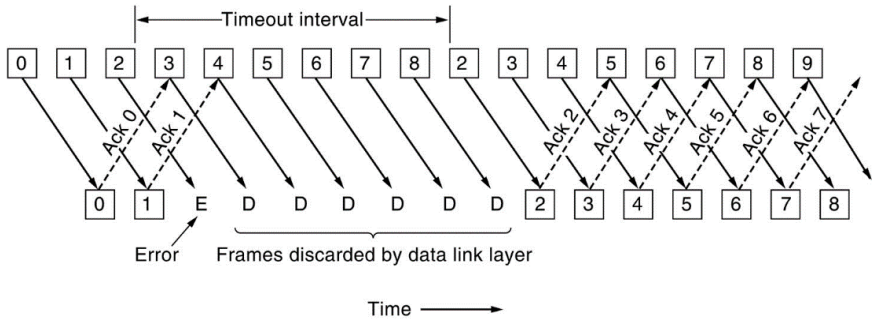
Si noti che nel caso in cui abbiamo una finestra di dimensione massima uguale a 1 ci troviamo nel caso stop-and-wait, ovvero, dopo aver inviato un frame si attende l'ack corrispondente prima di inviarne ulteriori. In questo caso si mantiene l'ordine, con finestre più larghe questo non è più vero.

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

Il problema di ricezione dell'ack per ogni frame inviato, limitava di molto l'utilizzo della banda e rallentava le comunicazioni, per ovviare a questo problema viene usata la tecnica di pipelining. Si decide quindi di inviare più frame prima di ricevere i vari ack aumentando di parecchio l'utilizzo della linea. Tuttavia, sorge un problema, cosa succede nel caso in cui si

perdano dei frames? Per il ripristino degli errori in presenza di pipelining sono disponibili due approcci base.

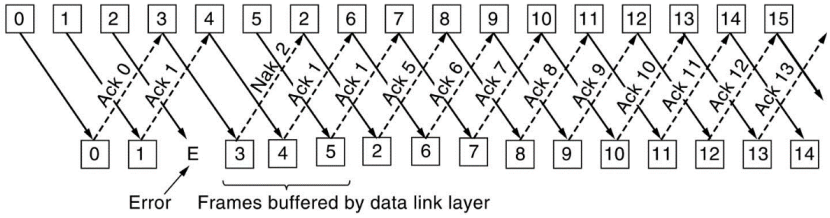
Tra questi go back n. Go back n è un'istanza specifica del protocollo "Automatic Repeat-reQuest" (modalità di trasmissione di pacchetti di dati) nel quale il processo mittente continua a mandare un numero di frame specificato nella window size anche senza aver ricevuto nessun ACK. La strategia corrisponde ad una finestra in ricezione di dimensione 1, rilevato l'errore si rifiuta di accettare qualunque frame eccetto il successivo che deve inviare allo strato network. Per questo il mittente scaduto il timeout riprende a spedire i frames che non hanno ricevuto l'ack. Questa tecnica può essere ottimizzata dall'uso del piggybacking, che consiste nello scrivere l'ack di un pacchetto nell'intestazione del pacchetto di informazione successivo, evitando latenze di trasmissione dovute alla trasmissione del solo ack. Go back n è uno dei metodi più efficienti per effettuare una connessione in quanto spedisce più pacchetti senza attendere ack, migliorando l'uso della banda, tuttavia può far perdere molta banda se la frequenza degli errori è molto alta. Go back-n e il selective repeat hanno diverse conseguenze in termini di uso di banda e di spazio di buffer nello strato data link, si può utilizzare un approccio oppure un altro in base a quale risorsa è più scarsa.



21 Si descriva cos'è la tecnica del selective repeat

Il problema di ricezione dell'ack per ogni frame inviato, limitava di molto l'utilizzo della banda e rallentava le comunicazioni, per ovviare a questo problema viene usata la tecnica di pipelining. Si decide quindi di inviare più frame prima di ricevere i vari ack aumentando di parecchio l'utilizzo della linea. Tuttavia, sorge un problema, cosa succede nel caso in cui si perdano dei frames? Per il ripristino degli errori in presenza di pipelining sono disponibili due approcci base.

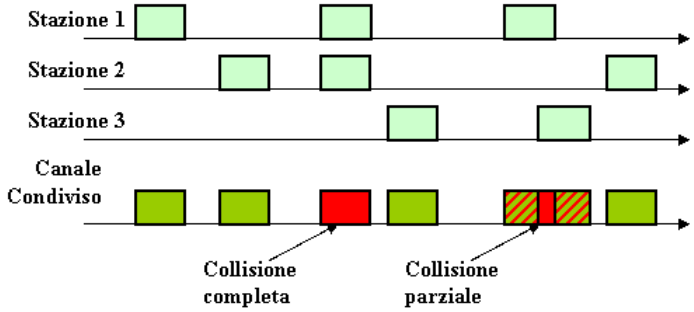
Tra questi troviamo il selective repeat, usando questo metodo quando viene ricevuto un frame in errore viene scartato, mentre i frame buoni ricevuti successivamente vengono salvati in un buffer, quando la sorgente va in timeout, solo il frame più vecchio senza ack viene ritrasmesso. Se quel frame arriva correttamente, la destinazione può passare in sequenza allo strato network tutti i frame presenti nel buffer. La ripetizione selettiva può inviare dei NACK (Not acknowledgement) quando trova un errore, cosi da stimolare la ritrasmissione prima dello scadere del timer. La ripetizione selettiva corrisponde ad avere una finestra di ricezione maggiore di 1. Go back-n e il selective repeat hanno diverse conseguenze in termini di uso di banda e di spazio di buffer nello strato data link, si può utilizzare un approccio oppure un altro in base a quale risorsa è più scarsa.

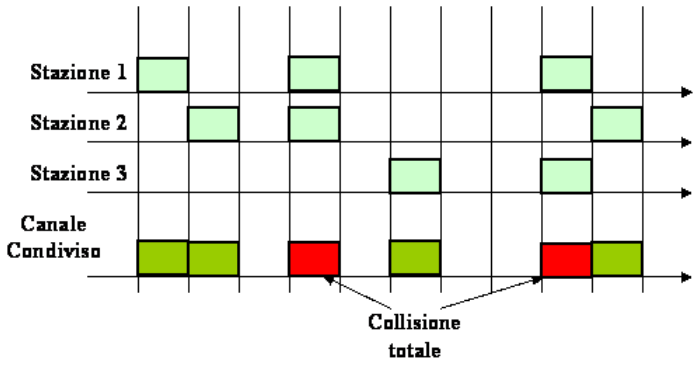


22 Descrivere la differenza tra ALOHA e ALOHA-SLOTTED

ALOHA è un protocollo di rette per garantire le funzionalità di accesso multiplo al mezzo di trasmissione dati condiviso tra più utenti. Esistono due tipi di reti: quelle che utilizzano le connessioni punto-punto e quelle che usa canali broadcast, questo protocollo viene utilizzato per le seconde. Inventato negli anni '70 nelle Hawaii, l'idea di fondo è di consentire agli utenti di trasmettere ogni volta che hanno dati da inviare. Questo naturalmente genera collisioni, tuttavia poiché i canali broadcast danno la possibilità di verificare se il frame trasmesso è stato ricevuto correttamente o no, la stazione trasmittente ascolta il canale e determina il successo o insuccesso della trasmissione. Le stazioni attendono un tempo variabile prima di provare a ritrasmettere un frame non andato a buon fine. Il successo dell'ALOHA puro è di circa 18%. Il protocollo Slotted ALOHA aggiunge al protocollo sopracitato la divisione del tempo in intervalli discreti, chiamati slot. Ogni stazione viene vincolata a cominciare la propria trasmissione solo all'inizio

di uno slot temporale, se una stazione è pronta ad un certo istante, dovrà necessariamente attendere l'inizio dello slot successivo. Lo svantaggio di questo protocollo è la necessità di un meccanismo di sincronizzazione che indichi alle varie stazioni quando possono cominciare la trasmissione. Questa divisione in slot migliora il grado di successo del doppio rispetto all'ALOHA puro, circa 36%. Questi risultati non dovrebbero sorprendere, in quanto con stazioni che trasmettono a piacimento è molto facile incorrere in collisioni. Subito dopo l'invenzione, questi protocolli caddero in disuso, fino a quando non si presentò il problema di allocare un canale condiviso da più utenti in competizione, di conseguenza slotted ALOHA tornò ad essere utilizzato.





23 Si illustri il CSMA (Carrier Sense Multiple Access), indicandone pregi e difetti

I protocolli ALOHA e le sue varianti permettevano di inviare dati ogniqualvolta si voleva, limitando però le percentuali di successo. Per migliorare i

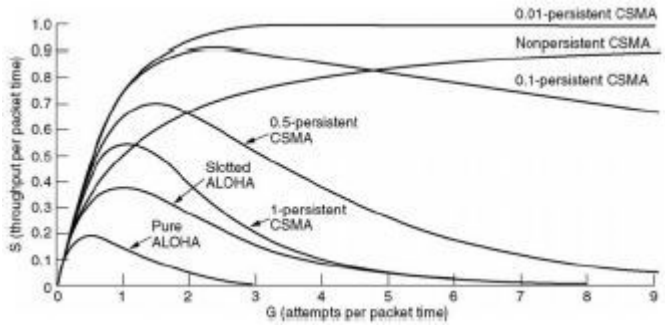
risultati di accesso multiplo ad un mezzo di trasmissione condiviso, vengono implementati protocolli in cui le stazioni rimangono in ascolto di una portante e si comportano di conseguenza, questi protocolli sono chiamati protocolli con rilevamento della portante. Il CSMA è una tecnica di trasmissione dati che si basa su questi principi. Ogni dispositivo prima di avviare la trasmissione dei dati deve verificare se sul canale, altri nodi stanno trasmettendo, rilevando la portante. Se il canale è libero iniziano a trasmettere, altrimenti attendono un tempo arbitrario prima di riprovare. Esistono diverse versioni di CSMA:

- CSMA 1-persistente: è il primo tra i protocolli CSMA, ha la particolarità di inviare con probabilità 1 sul canale in caso di nessun rilevamento. Questo migliora sicuramente ALOHA puro, tuttavia l'ingordigia di inviare non appena si libera il canale non rende immuni dalle collisioni, che potrebbero accadere in caso di stazioni che controllano nello stesso momento un canale vuoto e inviano contemporaneamente.

- CSMA non persistente: seconda variante del CSMA. Prima di trasmettere ogni stazione controlla il canale. Se lo trova libero inizia ad inviare i dati, ma se il canale è occupato la stazione non esegue un controllo continuo per trasmettere subito il proprio frame; invece attende per un intervallo casuale prima di ripetere l'algoritmo. Questo meccanismo permette di utilizzare meglio il canale ma allunga i ritardi.

- CSMA p-persistente: questa variante si applica su canali divisi in intervalli temporali. Quando è pronta a trasmettere, ogni stazione controlla il canale. Se lo trova libero, trasmette subito con una probabilità p, e rimanda fino all'intervallo successivo con probabilità q=1-p. Se anche quell'intervallo risulta libero la stazione trasmette oppure rimanda un'altra volta. Il processo si ripete finché il frame non è stato trasmesso.

Queste varianti migliorano enormemente il tasso di successo rispetto ad ALOHA e ALOHA-slotted. Un ulteriore miglioramento si ottiene consentendo ad ogni stazione di annullare la propria trasmissione in caso di collisione. Se due stazioni iniziano a trasmettere contemporaneamente, invece di completare la trasmissione dei relativi frame, ormai danneggiati, terminano bruscamente la trasmissione. La terminazione rapida dei frame danneggiati risparmia tempo e banda, questa variante è chiamata CSMA/CD ed è ampiamente utilizzata nelle LAN Ethernet.



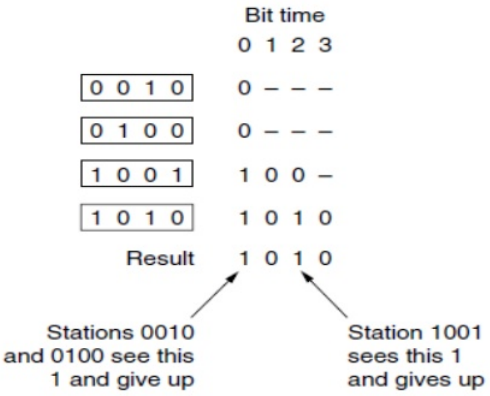
24 Basic Bitmap

Nella gestione di accesso multiplo ad un mezzo di trasmissione condiviso, esistono diversi protocolli che gestiscono l'accesso gestendo le collisioni e garantendo l'accesso (ALOHA, slotted ALOHA, CSMA), tuttavia le collisioni sono sfavorevoli alle prestazioni del sistema, specialmente quando il cavo è lungo e i frame corti. Esistono però protocolli che garantiscono la gestione degli accessi senza collisione, uno tra questi è il basic Bitmap (metodo a mappa di bit elementare). In questo protocollo ogni periodo di contesa è composto esattamente da N intervalli (N=# stazioni). Ogni stazione è numerata, e se ha un frame da inviare deve inviare un "1" nell'intervallo corrispondente al suo numero. A nessun'altra stazione è concesso di trasmettere durante questo intervallo. Cosi facendo ogni stazione si "prenota" l'intervallo di trasmissione. Una volta trascorsi gli N intervalli, ogni stazione sa quali sono le stazioni che vogliono trasmettere, di conseguenza non ci sarà mai alcuna collisione. Questo è anche chiamato protocollo a prenotazione. Questo protocollo non è ben bilanciato, da priorità alle stazioni con un numero basso, se una stazione "i" e una "j" vogliono trasmettere e i<j allora i si aggiudica la posizione. Contemporaneamente però le stazioni numerate con numeri bassi dovranno attendere di più rispetto a quelle con numeri più alti. Il basic bitmap ha bisogno di 1 bit di controllo a stazione, perciò non si adatta molto bene alle reti composte da migliaia di stazioni.

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

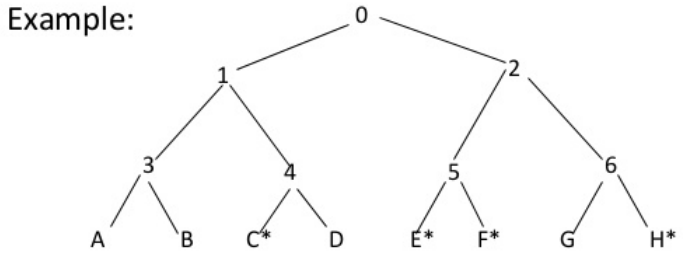
I dati vengono trasportati tramite un impulso elettrico. Ci possono essere molti dispositivi collegati allo stesso cavo con il rischio di collisioni e danneg-

giamento dei dati. Per evitare la collisione una stazione deve controllare se ci sono altre stazioni collegate allo stesso mezzo, esistono diversi protocolli che effettuano questo controllo evitando le collisioni. Il basic bitmap è uno di questi, tuttavia risulta elementare e su reti composte da molte stazioni risulta poco utilizzabile. Il collision free binary countdown o conteggio binario migliora il basic bitmap, utilizzando un sistema di assegnazione della linea in base ad una stringa binaria. Una stazione che desidera utilizzare il canale deve comunicare a tutti il proprio indirizzo sotto forma di stringa binaria, hanno tutti la stessa lunghezza. I conflitti si evitano grazie ad una regola di arbitraggio: la stazione rinuncia ad inviare non appena si accorge che un'altra stazione con un "1" in una posizione di bit di ordine elevato che nel proprio indirizzo vale "0". Esempio: 0010, 0100, 1001, 1010, queste stazioni vogliono inviare, vengono inviati i primi bit: 0 (0010), 0 (0100), 1 (1001), 1 (1010), le stazioni con "0" più a sinistra capiscono che ci sono stazioni con numero più grande che stanno concorrendo e si fanno da parte, le altre due continuano: 0 (1001), 0 (1010); sono uguali quindi continuano, il terzo bit è "1" quindi la stazione 1001 si arrende, vince 1010 che può trasmettere. L'efficienza è pari a $(d/d * log_2 N)$ (con d numero di bit) ma può raggiungere anche il 100% se l'indirizzo del mittente costituisce l'intestazione del frame. Si possono notare uno sbilanciamento notevole in quanto le stazioni con numero maggiore risultano avere sempre la precedenza, questo può essere ovviato facendo ruotare i valori delle stazioni ad ogni step, cosi quando una stazione riesce ad inviare viene spostata alla fine della coda, cosi da permettere in egual modo a tutte le stazioni la possibilità di inviare. Questo algoritmo è semplice, elegante ed efficiente, tuttavia attualmente non è utilizzato.



26 Spiegare cos'è l'adaptive tree walk protocol?

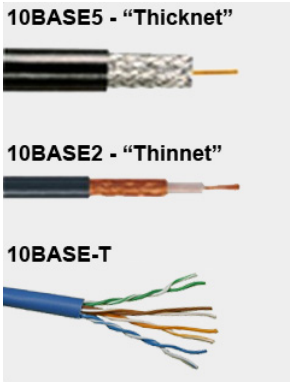
Per gestire la contesa di accesso ad un canale condiviso esistono protocolli con controllo della portante, con metodo della contesa tipo il CSMA o il metodo senza collisioni. Nelle situazioni di carico leggero la contesa è preferibile per il suo basso ritardo, tuttavia a carichi elevati diventa sempre più inefficiente. Il contrario avviene con i protocolli senza collisioni, a basso carico hanno un ritardo elevato ma al crescere del carico l'efficienza migliora. Adaptive tree walk protocol è un protocollo a contesa limitata che migliora ulteriormente le prestazioni dei protocolli sopracitati. Si può immaginare questo metodo come un albero binario, in cui le stazioni sono le foglie e sono divise nei vari rami. Inizialmente si prova a inviare ad altezza 0 se non vi è collisione si procede all'invio, in caso contrario ci si sposta sul sottoalbero sinistro e si ritenta, se il conflitto non c'è più si fa inviare la stazione che lo desidera (se non c'è conflitto vuol dire che nel sottoalbero sinistro c'è solo una stazione che vuole inviare). Dopo aver inviato si torna al nodo padre e si analizza il sottoalbero destro, ripetendo i test e scendendo nei sottoalberi in caso di conflitto.



Slot 0: C*, E*, F*, H* (all nodes under node 0 can try), conflict
slot 1: C* (all nodes under node 1 can try), C sends
slot 2: E*, F*, H*(all nodes under node 2 can try), conflict
slot 3: E*, F* (all nodes under node 5 can try), conflict
slot 4: E* (all nodes under E can try), E sends
slot 5: F* (all nodes under F can try), F sends
slot 6: H* (all nodes under node 6 can try), H sends.

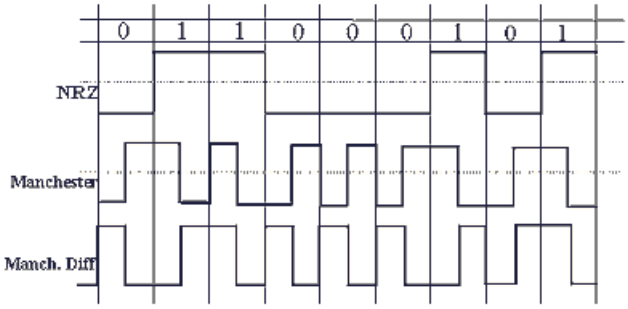
27 Ethernet e i vari tipi di cavo

Ethernet è il sistema LAN più diffuso al mondo, è economico e facile da usare e la diffusione delle componenti hardware ne ha facilitato l'adozione, è adeguata all'utilizzo con TCP/IP. Nasce con l'intento di ottenere una trasmissione affidabile su cavo coassiale in condizioni di traffico contenuto, ma in grado di tollerare possibili picchi di carico. Per regolamentare l'accesso al mezzo trasmissivo era stato adottato un protocollo di accesso multiplo del tipo CSMA/CD. Il nome Ethernet si riferisce al cavo (definito "etere"), andiamo quindi ad elencare le tipologie di cavi utilizzati in questo standard. Generalmente vengono utilizzati 4 tipi di cavo, il più vecchio è il modello 10base5 chiamato anche thick Ethernet, questo cavo assomiglia ad un tubo giallo con segni a intervalli di 2,5m che indicano la posizione delle spine. Le connessioni sono generalmente realizzate mediante spine a vampiro (spilli spinti nel nucleo centrale del cavo coassiale). La notazione 10Base5 indica che opera a 10Mbps, utilizza un sistema di segnali a banda base e può supportare segmenti lunghi fino a 500m. Questo cavo è ormai obsoleto. Il secondo cavo in ordine di tempo è stato il cavo 10base2 o thin Ethernet, più facile da piegare rispetto al precedente e le connessioni sono realizzate usando connettori BNC (giunzioni a "T" più affidabili e facili da usare rispetto alle spine a vampiro.). Il thin Ethernet è più economico e semplice da installare, però può essere lungo al massimo 185 metri e può supportare non più di 30 macchine. Per trovare guasti in questi mezzi è usata la tecnica TDR (Time Domain Rectory) che sostanzialmente misura il ritardo dell'eco dell'impulso immesso nel cavo. La tecnica TDR per la ricerca di guasti è difficile e onerosa da utilizzare, ci si è spostati quindi sulla terza tipologia di cablaggio 10Base-T, ormai diventata uno standard grazie alla facilità di gestione e all'uso di cablaggi preesistenti. Questo sistema di cablaggio utilizza hub di controllo tramite doppini telefonici, che sono largamente usati e semplici da gestire, ogni macchina si interfaccia con l'hub tramite cavo dedicato; rendendo cosi semplice aggiungere o rimuovere una stazione e individuare le interruzioni. Il suo svantaggio è rappresentato dalla lunghezza massima dei cavi che partono dall'hub: 100 metri. Esiste una versione più veloce del 10Base-T chiamata 100Base-T. Il quarto tipo di cavi per Ethernet si chiama 10Base-F e utilizza le fibre ottiche. È un'alternativa costosa a causa del prezzo dei connettori e dei terminatori, ma offre un'eccellente immunità alle interferenze e consente di collegare edifici o hub molto lontani. 10Base-F nonostante il costo consente inoltre una buona sicurezza in quanto i dati trasmessi sulla fibra sono difficili da intercettare.



28 Codifica Manchester

Nel sistema Ethernet la codifica binaria del segnale è “0” viene indicato con 0 volt mentre “1” utilizzando 5 volt, questo fa sorgere numerosi problemi, in quanto altre stazioni potrebbero interpretare erroneamente il segnale (a causa degli 0 volt, una stazione potrebbe confondere l’assenza del segnale con uno “0”). Si può passare a +1 volt per “1” e -1 volt per “0”, ma rimane il problema dei ricevitori che possono campionare il segnale in maniera diversa. Per risolvere questo problema sono state inventate due tecniche codifica Manchester e codifica Manchester differenziale. Queste codifiche sono dette auto-sincronizzanti in quanto non necessitano di un segnale di sincronia esterno. Queste codifiche suddividono ogni bit codificato in due, nella codifica Manchester lo “0” viene rappresentato da un segnale Basso-Alto, mentre l’”1” viene rappresentato da un segnale Alto-Basso. (esistono due convenzioni opposte riguardo la rappresentazione dei segnali “1” e “0”). Cosi facendo anche in caso di dissincronia, i dati in questo formato permettono un flusso auto-sincronizzante. La codifica Manchester differenziale invece differisce da quella originale nella rappresentazione dei bit: questa infatti si basa sulla verifica di transizioni all’inizio di un intervallo. La presenza di una di queste infatti (che siano alto-basso o basso-alto) identifica un valore, la mancanza di transizione invece indica il valore opposto. Per convenzione il bit 1 viene rappresentato dalla mancanza di transizione all’inizio del suo intervallo, mentre lo 0 è indicato con un cambiamento di segnale nello stesso periodo. Tutti i sistemi Ethernet adottano la codifica Manchester perché è più semplice, mentre la Manchester differenziale è utilizzata da altre LAN.

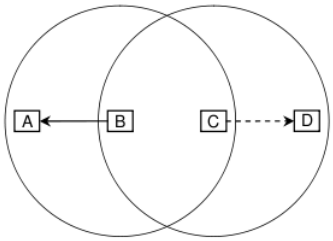


29 Cos'è il binary exponential backoff?

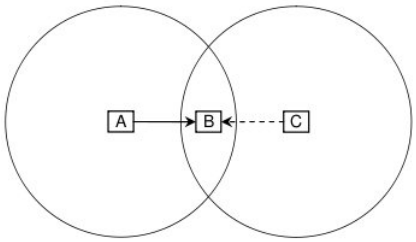
Nel protocollo di accesso multiplo CSMA/CD viene utilizzato l'algoritmo di backoff esponenziale, il quale serve a decidere il tempo di entrata di una stazione nel canale dopo aver riscontrato una collisione. La caratteristica principale del CSMA/CD (algoritmo che controlla il canale prima di trasmettere ed evita le collisioni analizzando la portante) è che una volta rilevata una collisione, si attende un intervallo prima di ritrasmettere, questo intervallo viene calcolato ogni volta tramite l'algoritmo di backoff esponenziale. Dopo una collisione il tempo viene diviso in intervalli discreti, la cui lunghezza è uguale al tempo di propagazione di andata e ritorno del caso peggiore sul mezzo di trasmissione. Dopo la prima collisione, ogni stazione aspetta 0 o 1 intervalli temporali prima di ritentare. Se due stazioni collidono e ognuna sceglie lo stesso numero casuale, la collisione si ripeterà. Dopo la seconda collisione ogni stazione sceglie 0, 1, 2 o 3 a caso e rimane in attesa per quel numero di intervalli temporali. In generale quindi, dopo i collisioni, viene scelto un numero casuale compreso tra 0 e 2i-1 e si salta quel numero di intervalli. Il limite di collisioni è 16, dopodiché il chip di controllo getta la spugna e manda un errore. Questo algoritmo è stato scelto perché si adatta dinamicamente al numero di stazioni che tentano di trasmettere. Poiché l'intervallo di scelta casuale cresce esponenzialmente con il numero di collisioni avvenute l'algoritmo assicura un basso ritardo quando poche stazioni collidono e garantisce un intervallo di tempo ragionevole quando la collisione coinvolge molte stazioni.

30 Stazione nascosta e stazione esposta: cosa sono e cosa fanno?

Al crescere del numero di computer e dispositivi mobili aumenta anche la domanda di collegare tali apparecchi al mondo esterno. Nascono così le LAN wireless, le quali permettono la connessione dei dispositivi senza bisogno di cavi. Tuttavia, questo porta a dei problemi di conflitto in caso di scambio di dati. Utilizzando banalmente il sistema CSMA per evitare le collisioni, porterebbe ad ascoltare le altre trasmissioni, e trasmettere in caso di nessun'altra connessione attiva. Questo però può portare a due diversi problemi: problema della stazione nascosta e stazione esposta. La stazione nascosta non è altro che una stazione che vuole inviare, non riesce a ricevere i segnali dei concorrenti a causa della sua distanza eccessiva. Supponiamo di avere A, B e C. A vuole inviare a B, prima di farlo ascolta se ci sono altre connessioni, non ne sente e procede all'invio. Tuttavia, C, è troppo distante perché A lo senta, ma abbastanza vicino a B per inviargli dati, cosi lo fa e va in conflitto con l'invio di A.



Il problema della stazione esposta invece è l'inverso, B trasmette ad A, C vuole inviare a D e controlla la presenza di portante sul mezzo di trasmissione e rileva B che sta inviando, cosi attende per evitare conflitti, tuttavia B non intralcerebbe la trasmissione di C, ma questo non lo può sapere, di conseguenza si genera uno stallo inutile. Questo è il problema della stazione esposta.



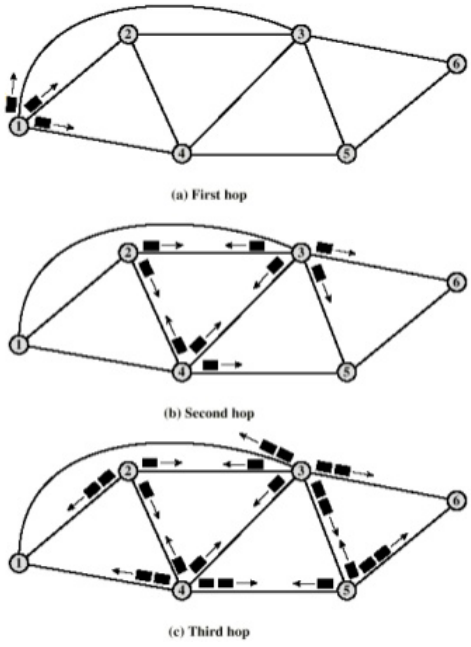
31 Bluetooth

Bluetooth è uno standard wireless che permette il collegamento di dispositivi di calcolo, di comunicazione e accessori vari mediante un sistema radio wireless a basso costo, bassa potenza e portata ridotta. L'unità di base di un sistema Bluetooth è la piconet, composta da un nodo master e da diversi (non più di 7) nodi slave, situati nel raggio di 10 metri. Più piconet possono trovarsi nella stessa stanza e possono essere collegate tramite un nodo ponte, un insieme di piconet è chiamato scatternet. Tutto si basa sulla comunicazione tra nodo master e nodo slave, il master controlla il clock e decide quale dispositivo può comunicare in ogni intervallo temporale. I tipi di collegamenti si suddividono in due tipi principali: orientati alla connessione o senza connessione. Il primo richiede di stabilire una connessione tra i dispositivi prima di inviare i dati, mentre in quello senza connessione il trasmettitore può in qualsiasi momento iniziare a inviare i propri pacchetti purché conosca l'indirizzo del destinatario. Bluetooth definisce inoltre due tipi di collegamenti a supporto delle applicazioni voce e trasferimento dati: un servizio asincrono senza connessione (ACL) ed un servizio sincrono orientato alla connessione(SCO). ACL supporta il traffico dati e si basa su un servizio di tipo best-effort (ovvero un servizio che non da alcuna garanzia dell'effettiva consegna dei dati né tantomeno livelli di qualità o priorità garantiti.). Supporta connessioni a commutazione di pacchetto, connessioni punto-multipunto (multicast) e connessioni simmetriche o asimmetriche. SCO invece è un collegamento che supporta connessioni con un traffico di tipo real-time e multimediali, prevede connessioni a commutazione di circuito, connessioni punto-punto e connessioni simmetriche. Bluetooth ha protocolli raggruppati in strati, che non seguono ne modello OSI né TCP/IP.

32 Si descriva l'algoritmo statico Flooding

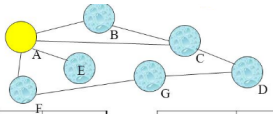
La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. Lo strato network sfrutta particolari algoritmi detti algoritmi di routing per instradare correttamente i pacchetti nei vari percorsi. Esistono diversi modi di instradare i pacchetti in quanto ci sono molti fattori da tenere in considerazione, però possiamo suddividerli in due grandi tipi: algoritmi non adattivi e algoritmi adattivi. Gli algoritmi non adattivi basano le loro decisioni su misure e stime del traffico e della topologia corrente, viene calcolato il percorso all'avvio della rete, in modalità fuori linea e viene scaricato nei router, questa proce-

dura si chiama anche routing statico. Gli algoritmi adattivi invece cambiano le loro decisioni secondo le modifiche apportate alla topologia e al traffico. L'algoritmo di Flooding è un algoritmo statico, in cui ogni pacchetto in arrivo è inviato a tutte le linee tranne quella da cui proviene. I vantaggi che porta si possono elencare in due punti, semplicità di attuazione e assicurazione di ricezione del pacchetto alla stazione desiderata (molteplici volte). Tuttavia, gli svantaggi sono evidenti, la banda è sprecata, i pacchetti vengono duplicati aumentando la complessità perché vengano scartati, e in caso di cicli i pacchetti potrebbero circolare nella rete all'infinito. Per questo vanno prese delle precauzioni, una variante un po' più pratica è chiamata flooding selettivo. In questo algoritmo i router non trasmettono ogni pacchetto verso tutte le linee, ma solo attraverso quelle che vanno approssimativamente nella direzione corretta. Nella maggior parte delle applicazioni questo algoritmo non è molto utilizzato, salvo casi particolari (i militari lo utilizzano, in quanto un gran numero di router potrebbero saltare in aria, aver questo metodo di trasmissione di pacchetti accerta la ricezione dei dati). Questo algoritmo viene utilizzato anche come metrica di confronto per altri algoritmi di routing, in quanto sceglie sempre il percorso più breve (scegliendoli tutti LOL), di conseguenza nessun algoritmo può produrre un ritardo più breve (ignorando il tempo di elaborazione dati generato dal processo di flooding).



33 Descrivere il distance vector routing

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. Per fare questo vengono utilizzati diversi algoritmi che si possono raggruppare in due grandi gruppo: algoritmi adattivi e non adattivi. Gli algoritmi non adattivi sono anche detti statici, in quanto basano i loro calcoli sulla rete "a freddo" senza tener conto del carico istantaneo o dei problemi di linea, un esempio è l'algoritmo di Flooding. Generalmente le moderne reti di computer utilizzano algoritmi adattivi, o dinamici se vogliamo. Tra i più popolari ci sono il distance vector routing e il linkstate routing. Gli algoritmi di routing basati sul vettore delle distanze (distance vector routing) operano facendo in modo che ogni router conservi una tabella (vettore) che definisce la miglior distanza conosciuta per ogni destinazione e la linea che lo conduce ad essa. Queste tabelle vengono aggiornate scambiando informazioni con i router vicini. Questo algoritmo è basato sull'algoritmo di Bellman-Ford (che calcola i cammini minimi su un grafo (RO insegna)). Ogni router misura la "distanza" (secondo una metrica che può includere vari fattori) che lo separa dai nodi adiacenti ricevendo i dati dai router vicini. A partire da tali dati, utilizzando l'algoritmo di Bellman-Ford, il router costruisce una tabella che associa ad ogni destinazione conosciuta la stima della distanza che lo separa dalla destinazione e il primo passo del percorso calcolato. Questo aggiornamento viene fatto periodicamente e dopo sufficienti scambi ciascun router avrà una riga per ogni altro nodo nella rete. Purtroppo, usando questo algoritmo c'è la possibilità che si creino cicli, e, nel caso in cui un collegamento si interrompe, si può avere una situazione di "count-to-infinity". Viene sostituito dal linkstate routing, in quanto l'algoritmo basato sul vettore delle distanze molte volte impiegava troppo tempo a raggiungere la convergenza, e non teneva conto della banda della linea quando sceglieva i percorsi.



Destination	Cost	NextHop
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	F
G	∞	-

Initial routing table at A

Destination	Cost	NextHop
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Final routing table at A

34 Descrivere Linkstate routing

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. Per fare questo vengono utilizzati diversi algoritmi che si possono raggruppare in due grandi gruppo: algoritmi adattivi e non adattivi. Gli algoritmi non adattivi sono anche detti statici, in quanto basano i loro calcoli sulla rete "a freddo" senza tener conto del carico istantaneo o dei problemi di linea, un esempio è l'algoritmo di Flooding. Generalmente le moderne reti di computer utilizzano algoritmi adattivi, o dinamici se vogliamo. Tra i più popolari ci sono il distance vector routing e il linkstate routing. Gli algoritmi di routing basati sullo stato dei collegamenti (linkstate routing) è il sostituto del distance vector routing. L'idea di questo algoritmo si basa su 5 punti:

- Scoprire i propri vicini e i relativi indirizzi di rete.
- Misurare il ritardo o il costo di ogni vicino.
- Costruire un pacchetto che contiene tutte le informazioni raccolte.
- Inviare questo pacchetto a tutti gli altri router
- Elaborare il percorso più breve verso gli altri router.

Un router, prima di tutto, cerca di scoprire chi sono i suoi vicini, lo fa inviando uno speciale pacchetto "HELLO" su ogni linea punto-punto; il router all'altro capo risponde fornendo la propria identità (si noti che i nomi devono essere globalmente unici, in quanto si necessità una non ambiguità durante lo scambio di pacchetti). Il passo successivo è la misurazione del costo della linea, avviene tramite l'invio di uno speciale pacchetto "ECHO" al quale l'altra parte deve rispondere immediatamente, in base al tempo di andata/ritorno si può ottenere una stima ragionevole del ritardo. Dopo aver raccolto le informazioni necessarie per lo scambio, ogni router deve costruire un pacchetto contenente tutti i dati. Il pacchetto inizia con l'identità del trasmittente, un numero di sequenza, l'età (contatore che viene decrementato ogni secondo, al raggiungere dello 0 le informazioni provenienti da quel router vengono scartate) e una lista dei vicini. Per ogni vicino è riportato il ritardo misurato. I pacchetti vengono creati periodicamente, oppure in caso di avvenimenti speciali: interruzione della linea o modifica/spegnimento/accensione di un vicino. La parte più delicata dell'algoritmo è la distribuzione affidabile dei pacchetti che contengono la descrizione dello stato dei collegamenti. Durante la distribuzione e l'installazione, i router che ricevono i primi pacchetti cambieranno i loro percorsi, rischiando di

creare inconsistenza, cicli, computer irraggiungibili e cosi via. L'idea fondamentale è quella di utilizzare l'algoritmo di flooding (inviare ogni pacchetto ad ogni linea in uscita (tranne da dov'è arrivato)) un computer che riceve un pacchetto con le informazioni sullo stato della connessione:

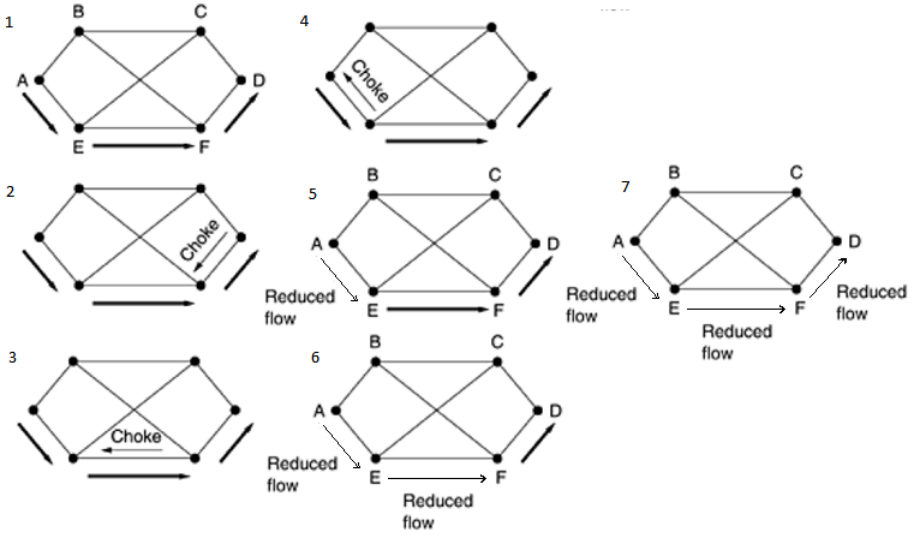
- Se è duplicato il pacchetto viene scartato
- Se è nuovo il pacchetto viene inoltrato a tutte le linee tranne a quella di ricezione (flooding)
- Se il numero di sequenza è inferiore al numero più alto visto in quel momento, il pacchetto viene scartato in quanto obsoleto (il router ha informazioni più recenti).

Esistono diversi miglioramenti per questo metodo di distribuzione di pacchetti, ma sarebbe troppo lunga da elencare. Dopo aver accumulato una serie completa di pacchetti sullo stato della connessione, il router può costruire l'intero grafo della sottorete, lo fa utilizzando localmente l'algoritmo di Dijkstra (algoritmo per la costruzione di grafi, simile a quello di Bellman-Ford, non può essere però utilizzato in caso di cammini negativi (RO insegna pt.2)). Questo algoritmo è molto utilizzato nelle reti reali in quanto può gestire reti composte da molti nodi, converge rapidamente al cammino minimo, difficilmente genera cicli ed è facile da comprendere in quanto ogni nodo ha la mappa completa della rete. Il principale svantaggio è la complessità di realizzazione, anche dovuta alla notevole capacità di memoria ed elaborazione richiesti dai router.

35 Choke packet

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. La decisione del miglior percorso viene effettuato dagli algoritmi di routing (flooding, linkstate o distance vector). Purtroppo, per molteplici motivi, le reti potrebbero congestionarsi, più computer vogliono inviare pacchetti alla stessa destinazione che, non riuscendo ad elaborarli tutti ne perde, questo causa la ritrasmissione che causa ulteriori ingorghi. Questo problema è la congestione ed è un punto critico che va regolamentato. Il choke packet è uno speciale pacchetto utilizzato per il controllo di flusso in una rete. Un router che rileva una congestione, invia all'host originale del pacchetto che un choke packet per avvertirlo di diminuire il flusso. Quando l'host sorgente riceve il pacchetto speciale diminuisce il flusso (tipicamente lo dimezza) e ignora i successivi

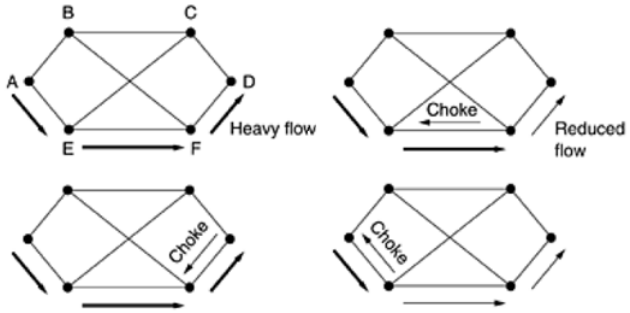
choke packet (generalmente ne arrivano in rapida successione), passato un tempo prefissato l'host si rimette all'ascolto, se arrivano altri choke packet in quel frangente diminuisce ulteriormente il flusso, altrimenti riprende gradualmente la velocità normale. Un problema di questa tecnica è la lentezza di reazione, perché l'host che produce i pacchetti ci mette un certo tempo a ricevere il choke packet e prendere provvedimenti, un miglioramento è dato da hop-by-hop choke packet che diminuisce il flusso per ogni router sul percorso in modo immediato.



36 Choke packet hop-by-hop

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. La decisione del miglior percorso viene effettuato dagli algoritmi di routing (flooding, linkstate o distance vector). Purtroppo, per molteplici motivi, le reti potrebbero congestionarsi, più computer vogliono inviare pacchetti alla stessa destinazione che, non riuscendo ad elaborarli tutti ne perde, questo causa la ritrasmissione che causa ulteriori ingorghi. Questo problema è la congestione ed è un punto critico che va regolamentato. Il hop-by-hop choke packet è un miglioramento della sua versione precedente (choke packet). Choke packet aveva il problema di aver un tempo di reazione a prendere provvedimenti troppo lento, il che causava una grossa perdita di dati prima di risolvere il problema Hop-by-hop choke packet risolve questo problema limitando tutte

le stazioni che attraversa in maniera immediata, senza dover attendere di arrivare all'host sorgente. Questa tecnica rende più veloce il sollievo del router destinatario, ma richiede spazio di buffer nei router "in mezzo" (tra mittente e destinatario).



37 Load shedding

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. La decisione del miglior percorso viene effettuato dagli algoritmi di routing (flooding, linkstate o distance vector). Purtroppo, per molteplici motivi, le reti potrebbero congestionarsi, più computer vogliono inviare pacchetti alla stessa destinazione che, non riuscendo ad elaborarli tutti ne perde, questo causa la ritrasmissione che causa ulteriori ingorghi. Questo problema è la congestione ed è un punto critico che va regolamentato. Quando gli algoritmi di choke packet (puro e hop-by-hop) non bastano per gestire la congestione, i router possono utilizzare la tecnica load shedding che, molto banalmente elimina dei pacchetti casuali in caso di sovraffollamento. Lo scartare pacchetti casuali non è sempre la scelta migliore, per migliorare l'algoritmo infatti la scelta può basarsi sull'applicazione in esecuzione, esistono due criteri generali per identificare queste scelte, wine e milk. Wine da più importanza ai pacchetti vecchi, scarta di conseguenza quelli nuovi (vecchio è meglio del nuovo), milk invece al contrario da importanza maggiore ai pacchetti nuovi (nuovo è migliore del vecchio). Questa tecnica permette numerose applicazioni e metodi per implementarla (oltre a wine e milk) questo permette di tenere sotto controllo possibili momenti di congestione.

38 Red (Random Early Detection)

Nello strato network esistono numerosi algoritmi di instradamento per portare un pacchetto da una destinazione ad un mittente (flooding, distance vector, linkstate), quando questa linea si congestiona esistono algoritmi che permettono di gestire la congestione e risolvere il problema (choke packet e load shedding). Risulta tuttavia più semplice gestire la congestione appena viene rilevata, non cercare di porvi rimedio dopo averle dato il tempo di bloccare tutta la linea. Questa osservazione conduce all'idea di scartare i pacchetti prima che il buffer sia completamente pieno, da qui nasce un celebre algoritmo usato per mettere in pratica questo schema: RED (Random Early Detection). Red in pratica fa in modo che i router scartino i pacchetti prima che la situazione diventi senza speranza (early). 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 su una linea supera una soglia di guardia allora quella determinata linea è considerata congestionata e prende le dovute azioni di correzione. Il massimo che può fare purtroppo è scegliere un pacchetto a caso dalla coda che ha attivato "l'azione difensiva". Per segnalare il rischio di congestione il router potrebbe inviare un choke packet per chiedere la diminuzione di flusso, tuttavia questo congestionerebbe ulteriormente le linee. La strategia migliore è scartare banalmente il pacchetto e attendere che la sorgente lo re-invii a causa del mancato acknowledgement. Questa ultima strategia funziona solo quando le sorgenti rispondono ai pacchetti perduti rallentando il flusso. Nelle reti wireless, dove la maggior parte dei pacchetti persi è a causa del rumore, questo non avviene, è infatti impossibile usarla in quei casi.

39 Reverse Path Forwarding

I router spesso necessitano di inviare messaggi a molti o a tutti gli altri host. Questi tipi di trasmissioni sono dette trasmissioni broadcast. L'algoritmo di routing più quotato per questo genere di trasmissioni è sicuramente quello di flooding, in quanto invia i pacchetti a tutte le stazioni vicine (tranne quella da cui ha ricevuto il pacchetto). Un problema di questa tecnica è sicuramente lo spreco di banda e la creazione di troppi pacchetti. Per ovviare a questo problema sono stati creati numerosi algoritmi che cercano di migliorare questo sistema di broadcasting. Con il Reverse path forwarding il router che riceve un pacchetto controlla se gli è giunto da una linea che normalmente è utilizzata per inviare i pacchetti alla sorgente (ovvero che

sia la linea con cammino minimo da lui alla sorgente). In caso affermativo, c'è una forte probabilità che il pacchetto broadcast abbia seguito il percorso migliore dalla sorgente fino a lui, di conseguenza lo copia e lo inoltra a tutte le linee (tranne quella da cui l'ha ricevuto). Se invece il pacchetto broadcast è giunto attraverso una linea diversa dalla preferita per raggiungere la sorgente, il pacchetto viene scartato in quanto è probabile si tratti di un duplicato. Questo algoritmo previene il problema dell'IP spoofing (falsificazione dell'indirizzo del mittente). La sua implementazione è efficiente e non richiede di conoscere la mappa della sottorete, liste di destinazione o mappe di bit per ogni pacchetto broadcast, il che lo rende anche di facile implementazione.

40 Quality of Service (QoS)

Un flusso di pacchetti da una sorgente a una destinazione è chiamato, appunto, flusso. Ogni flusso viene regolamentato per il percorso da effettuare e quando effettuarlo, i metodi di gestione della congestione e così via. Ogni flusso ha le sue esigenze, in base all'applicazione che sta servendo, possiamo quindi caratterizzare queste esigenze in 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.

- Affidabilità: nessun bit può essere trasmesso in modo scorretto. Questo obiettivo viene di solito raggiunto creando il checksum di ogni pacchetto e verificandolo alla destinazione. Questo parametro è ricercato da applicazioni tipo la posta elettronica o trasferimento di file, che necessitano di un'alta affidabilità, applicazioni come audio o video possono tollerare errori, perciò non viene elaborato o verificato nessun checksum.

- Ritardo: il ritardo dei pacchetti in applicazioni come la posta elettronica o il trasferimento file non è molto sentito, è importante invece in applicazioni come telefonate o videoconferenze.

- Jitter: Il Jitter non è altro che la variazione del segnale in modo casuale. Questo può portare ad una ricezione di dati in intervalli irregolari, applicazioni come può essere la posta elettronica o il trasferimento file non sono molto soggette a questo problema. Lo sono invece per applicazioni di login remoto o di streaming video, a causa della variazione casuale della trasmissione, il risultato è terribile.

- Banda: ogni applicazione differisce per l'esigenza di banda, posta elettronica e accesso remoto non ne richiede molta, il video in tutte le sue forme invece sì.

Nessuna tecnica è in grado di fornire QoS efficiente e sicura in modo ottimo.

Application Type	Throughput Demand	Latency Tolerance	Jitter Tolerance	Loss Tolerance	Application Type	Throughput Demand	Latency Tolerance	Jitter Tolerance	Loss Tolerance
Email	Low	High	High	High	Video on demand (e.g. YouTube / NetFlix)	High	Medium	Medium	Low
Web browsing	Low	High	High	High					
File transfer (FTP)	Low - High	High	High	High	Voice over IP / WiFi	Low	Low	Low	Low
Chat (IM)	Low	Medium	Medium	Medium	Videoconferencing (e.g. Skype, FaceTime)	Medium - High	Low	Low	Low
Video streaming (e.g. surveillance)	Medium - High	Medium	Medium	Medium					

41 Leaky bucket, pregi e difetti

Quando ci si scambia pacchetti nella rete, serve un modo per controllare il flusso; per delimitare banda e velocità di trasmissione si può utilizzare l'algoritmo leaky bucket, un sistema di accodamento a singolo server con tempo di servizio costante.

Questo algoritmo si basa sull'idea del "secchio che perde" attraverso il quale qualsiasi quantità d'acqua contenuta fluirà all'esterno sempre con la stessa velocità, se l'acqua viene aggiunta troppo velocemente questa supererà in volume la capacità del secchio e straborderà.

Allo stesso modo il leaky bucket è formato da una coda finita. Al suo arrivo, se c'è spazio il pacchetto viene aggiunto alla coda, altrimenti viene scartato. Ad ogni ciclo di clock viene trasmesso un pacchetto (se la coda non è vuota).

Così facendo si gestiscono burst di dati che altrimenti congestionerebbero la rete; un contro però può essere che, siccome trasmette pacchetti solo ad intervalli prefissati, ci saranno parecchi casi in cui il volume del traffico sarà molto basso e ampie porzioni di risorse di rete non verranno utilizzate.

42 Descrivere il token bucket, pregi e difetti

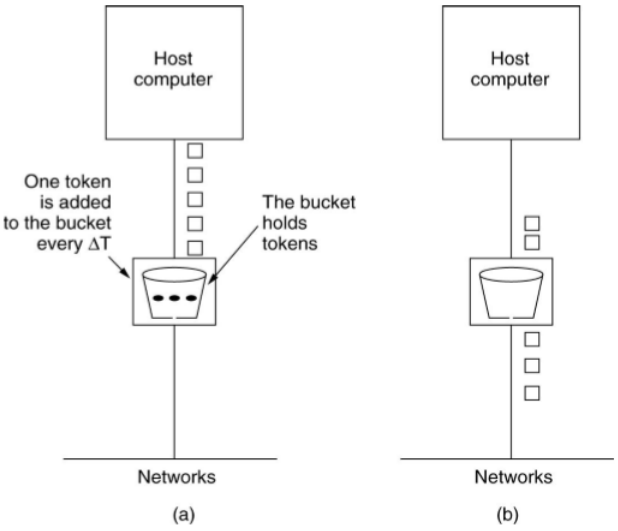
Per gestire il flusso di pacchetti su una rete è necessario utilizzare algoritmi che permettano un controllo della congestione e che sfruttino al meglio le risorse di rete. L'algoritmo leaky bucket (secchio che perde) gestiva le congestioni, ma purtroppo imponeva un modello di output troppo rigido, che non seguiva la variabilità del traffico.

Per molte applicazioni è meglio permettere all'output di accelerare un po' quando ci sono burst di dati, perciò serve un algoritmo più flessibile e che non perda mai dati.

L'algoritmo token bucket riprende l'idea del leaky bucket, ma aggiunge dei token, generati da un clock. Un pacchetto per passare deve distruggere un token, se non c'è attende finché non viene generato dal clock. A differenza del leaky bucket, il token bucket non scarta i pacchetti quando il secchio è pieno.

Se non arrivano pacchetti da inviare, il token bucket accumula i token fino ad un massimo di n. Così facendo si prepara a gestire dei possibili burst di massimo n pacchetti (pari al numero di token), bruciando i token in rapida successione e dando una risposta più veloce a picchi improvvisi.

Per implementare questo algoritmo è necessaria solo una variabile che tenga conto del numero di token, e li diminuisca quando un pacchetto viene inviato.



43 Descrivere l'ARP

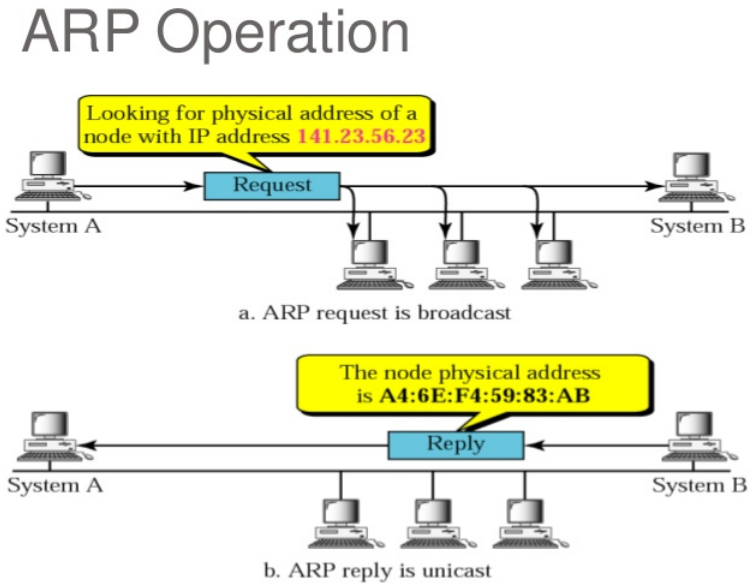
Ogni macchina di Internet ha uno o più indirizzi IP, tuttavia questi non possono essere utilizzati per inviare pacchetti, in quanto l'hardware che opera sullo strato data link non comprende gli indirizzi Internet. Bisogna trovare un modo per associare l'indirizzo Ethernet a 48 bit (indirizzo MAC) con l'indirizzo IP associato.

ARP è un protocollo che permette di associare ad un indirizzo IP all'indirizzo Ethernet in una sottorete (o anche tra più sottoreti utilizzando Arp-proxy). Viene trasmesso un pacchetto broadcast a tutte le stazioni nella sottorete che chiede chi è il proprietario di un determinato indirizzo IP. Le stazioni controllano il proprio indirizzo IP e solo il proprietario di tale indirizzo risponde inviando il proprio indirizzo Ethernet. In questo modo la stazione che cercava un determinato indirizzo riesce a collegare l'IP con il MAC.

A questo punto, il software IP costruisce un frame Ethernet indirizzato al destinatario appena scoperto e inserisce il pacchetto IP nel campo carico utile, dopodiché scarica tutto sulla Ethernet. La scheda Ethernet del destinatario rileva il frame, si accorge di essere la stazione designata della comunicazione, preleva i dati ed estrae il pacchetto IP dal carico utile per passarlo al software IP, il quale verifica la correttezza dell'indirizzo ed elabora i dati. Per migliorare le prestazioni, dopo aver associato degli indirizzi,

questi vengono memorizzati nella cache, cosi, in caso di nuove trasmissioni verso la stessa stazione, si ha già l'indirizzo pronto.

Questo protocollo viene usato tutte le volte che un host collegato ad una LAN deve inviare un messaggio ad un host nella stessa LAN di cui conosce esclusivamente l'indirizzo di rete (IP). Inoltre, non prevede metodi per autenticare le risposte ricevute, il che lo rende molto vulnerabile a possibili attacchi.



44 Si descriva DHCP e il suo funzionamento

Con ARP è possibile associare (in una sottorete) l'indirizzo MAC di una macchina conoscendo il suo indirizzo IP. A volte è necessario risolvere il problema inverso: dato un indirizzo Ethernet, qual è il corrispondente indirizzo IP?

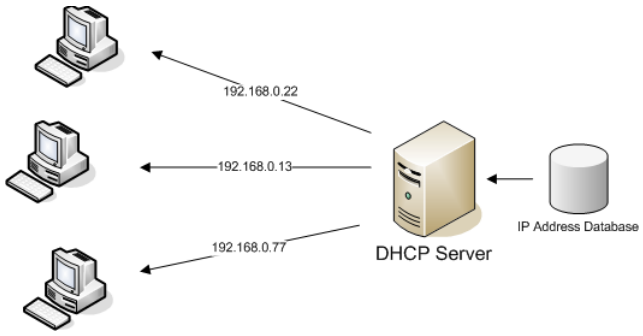
È stato creato una possibile soluzione RARP che permette di risolvere il problema, tuttavia necessita di installare su ogni router dei server RARP. Per aggirare questo problema si è passati ad un protocollo alternativo BOOTP, che a differenza di RARP utilizza messaggi UDP inoltrati attraverso i router. Purtroppo, questo protocollo necessita una configurazione manuale delle tabelle che associano indirizzi IP e agli indirizzi Ethernet (non è possibile utilizzare BOOTP fino a quando l'amministratore non assegna alla macchi-

na un indirizzo IP e non inserisce manualmente l'associazione del tipo nelle tabelle di configurazione di BOOTP).

Per risolvere questo problema BOOTP viene esteso e chiamato in modo diverso DHCP (Dynamic Host Configuration Protocol), che permette un'assegnazione manuale o automatica degli indirizzi IP. Questo protocollo ha ampiamente sostituito RARP e BOOTP. DHCP si basa sull'idea di un server speciale che assegna gli indirizzi IP agli host che ne richiedono uno. Questo server non deve trovarsi sulla stessa LAN, questo comporta che potrebbe non essere raggiunto dalle trasmissioni broadcast, perciò è necessario installare in ogni LAN un agente di inoltro DHCP.

Una macchina appena accesa invia in modalità broadcast un pacchetto DHCP DISCOVER, questo pacchetto viene intercettato dall'agente di inoltro presente nella LAN che provvede ad inoltrarlo al server DHCP che assegna un indirizzo IP alla macchina tramite un pacchetto DHCPOFFER, questa risponde con un pacchetto DHCPREQUEST che viene accettata dal server tramite ACK. Questo avviene nel caso di un singolo server DHCP, potrebbero essercene multipli, in questo caso l'host che necessita di un indirizzo IP valuta le varie proposte, ed invia un pacchetto DHCPREQUEST indicando il server selezionato. L'indirizzo assegnato proviene da una pool di indirizzi IP comuni, un problema causato da questo potrebbe essere la durata di allocazione: se un host abbandona la rete senza restituire l'indirizzo IP questo viene perso per sempre.

Per evitare questa eventualità, gli indirizzi IP sono assegnati secondo una tecnica chiamata di leasing, ovvero a scadenza di tempo. Prima che questo scada l'host deve fare richiesta di rinnovo dell'indirizzo, se non riesce a farla o se viene rifiutata, l'host non può più utilizzare quell'indirizzo IP. DHCP base non include nessun meccanismo di autenticazione, per questo motivo è vulnerabile a vari attacchi.



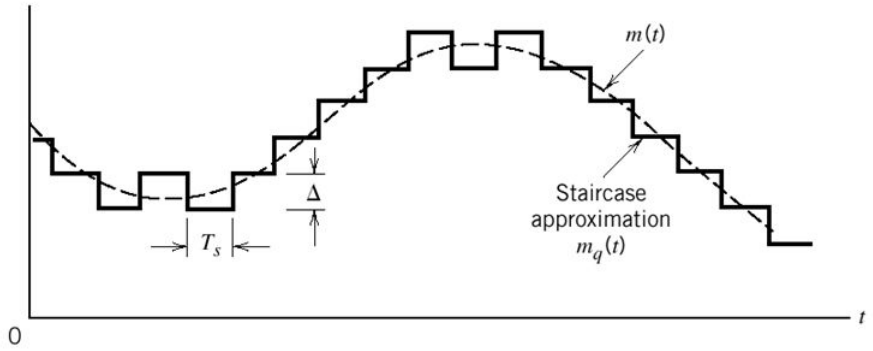
45 IPV6

Un indirizzo IP, è un'etichetta numerica che identifica univocamente un dispositivo (host) collegato ad una rete informatica che utilizza l'internet Protocol come protocollo di rete.

IPv4 (Internet Protocol version 4) è attualmente il protocollo più usato a livello di rete, la sua tecnologia però supporta al massimo 2^32 indirizzi univoci. Inizialmente poteva andare bene, ma con la crescita esponenziale della rete questi iniziano a scarseggiare. Esistono protocolli tipo CIDR e NAT che permettono di sfruttare gli indirizzi IP restanti in modo variabile, cosi da resistere ancora un po', tuttavia IPv4 ha i giorni contati.

IPv6 è un upgrade dell'IPv4 e conta di risolvere i problemi di numero, in quanto riuscirebbe a gestire 2^128 indirizzi diversi. IPv6 oltre a colmare il problema della quantità di indirizzi migliora e semplifica l'intestazione, infatti prevede solo 8 campi rispetto ai 13 dell IPv4. Questo consente al router di elaborare i pacchetti più velocemente. Sempre riguardo l'elaborazione dei pacchetti, IPv6 migliora il supporto per le opzioni, rendendo campi che prima erano obbligatori, opzionali. Un altro grande passo avanti riguarda la sicurezza.

IPv6 e IPv4 non sono compatibili tra loro, è facile trasformare un indirizzo di versione 4 a uno di versione 6, tuttavia la rete ormai è basata sull'IPv4 e il passaggio alla versione successiva è lenta e impegnativa, si stanno facendo passi avanti, però rimane la necessità di mantenere entrambi i protocolli almeno per decenni prima di passare alla nuova versione.



46 Elencare e descrivere brevemente i secondi (primi) 32b dell'header IPv4 (IPv6)

(sinceramente sta domanda non la capisco... faccio entrambe le versioni, poi nella risposta va scelta quella che viene richiesta. inizio con un'intro comune, poi un'intro per IPv4 e una IPv6 (da scegliere), successivamente descrivo in blocco i primi 32b dell'IPv4, seguiti dai secondi 32, poi faccio lo stesso per IPv6, Enjoy).

Un indirizzo IP, è un'etichetta numerica che identifica univocamente un dispositivo (host) collegato ad una rete informatica che utilizza l'internet Protocol come protocollo di rete.
IPv4 è il protocollo più usato e la sua tecnologia può supportare al massimo 2^32 indirizzi univoci, numero che sta iniziando a diventare stretto. Un datagramma IP di questa versione è costituito da una parte di intestazione e una parte di testo, L'intestazione è di 20B fissi e una parte opzionale di lunghezza variabile, consiste in 13 campi.
IPv6 è l'evoluzione dell'IPv4 e conta di risolvere molti dei suoi problemi, può supportare al massimo 2^128 indirizzi univoci. Un datagramma IP di questa versione è costituito da una parte di intestazione e una parte di carico utile. L'header è costituito dai primi 40 byte e contiene 8 campi, il carico utile invece va da un minimo di 1280 byte e arriva fino a 65535 byte (in modalità standard).

I primi 32b dell'IPv4 sono cosi formati:

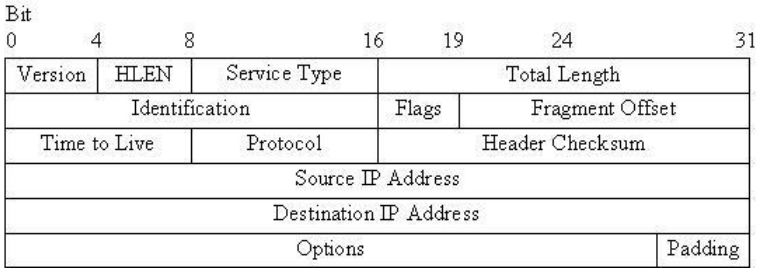
- Version [4 bit]: indica la versione del pacchetto IP; per IPv4, ha valore 4 (simpy).
- Internet Header Lenght (IHL) [4bit]: indica la lunghezza (in word da 32 bit) dell'header del pacchetto IP; tale lunghezza può variare da 5 word (20 byte) a 15 word (60 byte) a seconda della presenza e della lunghezza del campo facoltativo.
- Type of Service (TOS) [8 bit]: Nelle specifiche iniziali, questo campo avrebbe dovuto specificare il modo e la precedenza con cui l'host ricevente doveva trattare il datagramma; Ad esempio, un host poteva scegliere una bassa latenza, mentre un altro preferire un'alta affidabilità. Nella pratica questo uso del campo TOS non ha preso piede.
- Total Length [16 bit]: Indica la dimensione (in byte) dell'intero pacchetto, comprendendo header e dati.

I secondi 32b dell'IPv4 sono cosi formati:

- Identification[16 bit]: Inizialmente sarebbe dovuto essere utilizzato per identificare in modo univoco i vari frammenti in cui può essere spezzato un pacchetto IP. Sperimentazioni successive però hanno suggerito di utilizzarlo per aggiungere la funzionalità di tracciamento dei pacchetti. Serve per determinare quale datagramma appartiene al frammento appena arrivato (tutti i frammenti di un datagramma hanno lo stesso campo identification).

- Flags [3 bit]: Bit utilizzati per il controllo del protocollo e della frammentazione dei datagrammi. Il primo è Reserved sempre settato a "0" (bit inutilizzato in poche parole), successivamente troviamo DF (Don't Fragment) se settato a "1" indica che il pacchetto non deve essere frammentato, se non è possibile inviarlo senza frammentazione, il pacchetto viene scartato. L'ultimo bit di flag è MF (More Fragments) se settato a "0" indica che il pacchetto è l'ultimo frammento (o il solo frammento del pacchetto originario), perciò tutti gli altri frammenti dello stesso pacchetto avranno MF settato a "1".

- Fragment Offset [13 bit]: Indica l'offset (misurato in blocchi di 8 byte) di un particolare frammento relativamente all'inizio del pacchetto IP originale: il primo frammento ha offset 0, i successivi avranno valore multiplo di 8byte e indica la posizione del frammento nel datagramma. Il valore massimo è pari a 65536 byte.



I primi 32b dell'IPv6 sono cosi formati:

- Version [4 bit]: Indica la versione del datagramma IP: per IPv6, ha valore 6 (lel).

- Traffic Class [8 bit]: Permette di gestire le code di priorità, assegnando ad ogni pacchetto una classe di priorità rispetto ad altri pacchetti

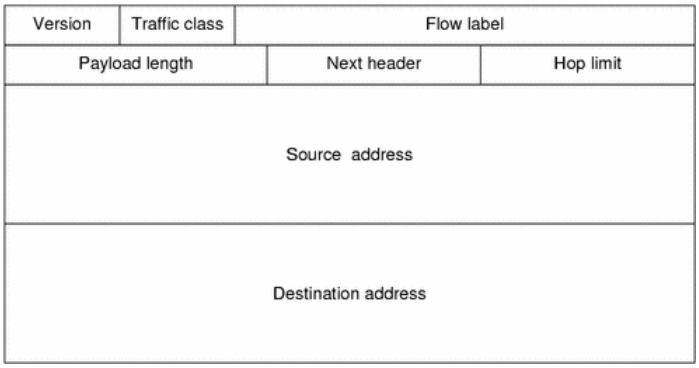
provenienti dalla stessa sorgente. Viene usata anche per controllare la congestione.

- Flow Label [20 bit]: Campo ancora in fase sperimentale, usato dal mittente per etichettare una sequenza di pacchetti come se fossero nello stesso flusso. Supporta la gestione del QoS (Quality of Service) consentendo ad esempio di specificare quali etichette abbiano via libera rispetto ad altre. I pacchetti con flow label diverso da "0" avranno trattamenti speciali dai router. I secondi 32b dell'IPv6 sono cosi formati:

- Payload Length [16 bit]: è la dimensione del payload (carico utile), ovvero il numero di byte di tutto il contenuto presente dopo l'header.

- Next Header [8 bit]: Indica quale tipo di processo di trasporto è in attesa di quei dati (UDP, TCP o altri). Simile al campo protocol dell'IPv4 con cui condivide i valori.

- Hop Limit [8 bit]: Indica il tempo di vita del pacchetto, il suo valore viene decrementato di 1 ogni volta che il pacchetto passa da un router, quando arriva a 0 viene scartato. Simile al campo Time to live presente nell'IPv4.



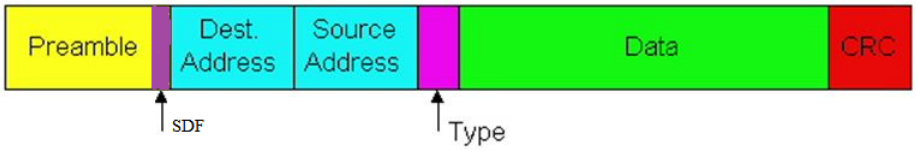
NOTA: Ripeto che questa domanda alla fine contiene 4(?) domande possibili, bisogna utilizzare i pezzi che vengono richiesti al momento, letta tutta d'un fiato non ha senso, è divisa e si dovrebbe capire il suo contenuto, se non lo capite cambiate esame :P.

47 Frame Ethernet

Un frame Ethernet è l'unità trasportata nel livello Data Link. Esistono diverse versioni di questo frame; ora analizziamo la versione IEEE 802.3.

Un frame Ethernet ha una grandezza compresa tra 64 e 1518 byte, ed è formato da:

- Preambolo [7 byte]: contenente "10101010" e serve per sincronizzare il clock del ricevitore con quello del trasmettitore.
- SFD [1 byte]: Start of the Frame, "10101011" indica al destinatario che dal prossimo byte comincerà il frame vero e proprio.
- MAC address di destinazione [6 byte]: Indica l'indirizzo di destinazione, il bit di ordine più elevato vale "0" per gli indirizzi ordinari e "1" per quelli di gruppo. Con gruppo si intende una trasmissione multicast, che differisce dalla broadcast, più rozza ma che non richiede alcuna gestione. Per una trasmissione broadcast basta mettere tutti i bit a "1".
- MAC address sorgente [6 byte]: indica l'indirizzo sorgente del frame.
- Type [2 byte]: Indica al ricevitore cosa deve fare del frame. Sullo stesso computer si possono usare più protocolli dello stato network contemporaneamente, questo campo indica il processo a cui passare il frame.
- Dati [da 46 a 1500 byte]: Questo campo contiene i dati veri e propri, non può essere nullo in quanto Ethernet richiede frame lunghi almeno 64 byte (dal destination address al checksum inclusi). Perciò se la parte occupata dai dati è lunga meno di 46 byte il campo successivo viene utilizzato per riempire il frame.
- Pad [0-46 byte]: Come descritto sopra, se il frame dati è inferiore a 46 byte, questo campo provvede a riempire i byte mancanti, cosi che vengano accettati dal protocollo Ethernet.
- Checksum [4 byte]: Contiene codice CRC per il rilevamento degli errori (senza correzione).



48 Si descriva l'header UDP

Lo stato di trasporto è il cuore dell'intera gerarchia dei protocolli. Il suo compito è fornire il trasporto dei dati, affidabile ed efficiente in termini di costi, dal computer di origine a quello di destinazione, indipendentemente dalla rete o dalle reti fisiche effettivamente utilizzate. Nello strato di trasporto ci sono due protocolli principali, che si distinguono dal fatto che uno è orientato alla connessione l'altro è senza connessione (TCP e UDP).
Senza connessione: lo scambio di dati a pacchetto tra mittente e destinatario non richiede l'operazione preliminare di creazione di un circuito su cui instradare l'intero flusso.

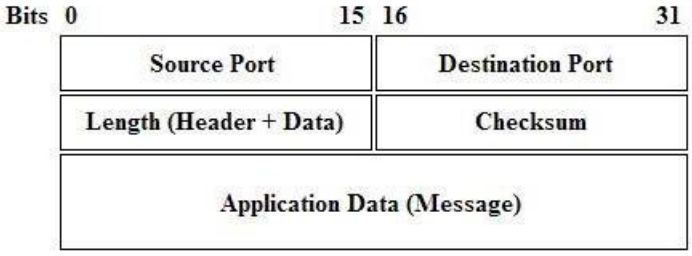
UDP (User Datagram Protocol) è un protocollo dello stato di trasporto senza connessione. Non gestisce il riordinamento dei pacchetti né la ritrasmissione di quelli persi, il che lo rendono di minor affidabilità rispetto al TCP. In compenso è molto rapido ed efficiente per applicazioni leggere o time sensitive (audio video real-time). UDP fornisce servizi basilari: Multiplazione delle connessioni tramite assegnazione delle porte e verifica degli errori mediante una checksum inserita in un campo dell'header.

L'header dell'UDP è cosi formato:

- Source port [16 bit]: identifica il numero di porta sull'host del mittente del datagramma;
- Destination port [16 bit]: identifica il numero di porta sull'host del destinatario del datagramma;
- Length [16 bit]: contiene la lunghezza totale (in byte) del datagramma UDP (header+dati);
- Checksum [16 bit]: contiene il codice di controllo del datagramma, l'algoritmo di calcolo è definito nell'RFC del protocollo (documento con informazioni e specifiche del protocollo).

Infine sono presenti i dati del messaggio. UDP viene utilizzato dalle applicazioni di rete che sono elastiche riguardo alla perdita dei dati e strettamente

dipendenti dal tempo, si usa inoltre per comunicazioni in broadcast (tutti i terminali in una rete) e multicast (tutti i terminali iscritti ad un servizio).



49 Descrivere l'header TCP/IP e commentarlo

Lo stato di trasporto è il cuore dell'intera gerarchia dei protocolli. Il suo compito è fornire il trasporto dei dati, affidabile ed efficiente in termini di costi, dal computer di origine a quello di destinazione, indipendentemente dalla rete o dalle reti fisiche effettivamente utilizzate. Nello strato di trasporto ci sono due protocolli principali, che si distinguono dal fatto che uno è orientato alla connessione l'altro è senza connessione (TCP e UDP).
Orientato alla connessione: I dispositivi utilizzano un protocollo di comunicazione per stabilire una connessione end-to-end tra gli agenti della comunicazione prima della trasmissione di qualsiasi tipo di dato.

TCP (Transmission Control Protocol) è il protocollo orientato alla connessione dello strato di trasporto. Si occupa di controllo della trasmissione, di rendere affidabile la comunicazione di dati in rete tra mittente e destinatario.

Contrariamente a UDP, TCP riesce a garantire la consegna dei dati, utilizzando meccanismi di acknowledgment e di ritrasmissione su timeout, al costo però di un maggior overhead (viene usata più banda di quello che servirebbe per i dati) della rete. TCP inoltre possiede funzionalità di controllo di flusso e controllo della congestione (attraverso la sliding window). TCP è solitamente usato in combinazione con il protocollo di livello di rete IP. Erroneamente TCP/IP sono considerati un unico protocollo.

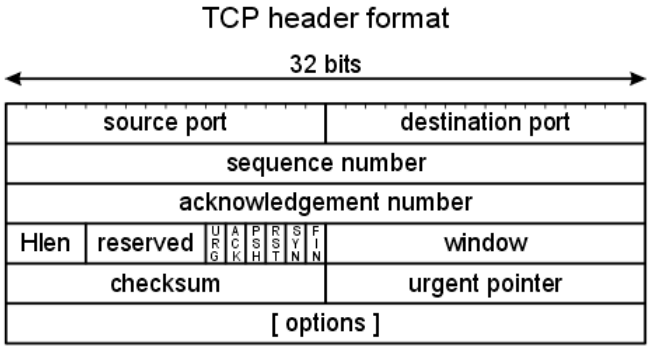
L'header del TCP è formato nel seguente modo:

- Source port [16 bit]: Identifica il numero di porta sull'host mittente associato alla connessione TCP.
- Destination port [16 bit]: Identifica il numero di porta sull'host destinatario.

- Sequence number [32 bit]: Indica lo scostamento (in byte) dell'inizio del segmento TCP interno al flusso completo, a partire dall'ISN (initial sequnce number), negoziato all'apertura della connessione.
- Acknowledgment number [32 bit]: Ha senso solo se il flag ACK è impostato a "1", e conferma la ricezione di una parte del flusso di dati nella direzione opposta, indicando il valore del prossimo Sequence number che l'host mittente del segmento TCP si aspetta di ricevere.
- Data offset [4 bit]: Indica la lunghezza (in word da 32 bit) dell'header del segmento TCP; può variare in base alla presenza e alla lunghezza del campo facoltativo Options.
- Reserved [4 bit] Bit non utilizzati. Predisposti per sviluppi future dell'applicazione.
- Flags [8 bit]: Bit utilizzati per il controllo del protocollo:
  - CWR (Congestion Window Reduced): Se impostato a "1" indica che l'host sorgente ha ricevuto un segmento TCP con flag ECE (prossimo) impostato a "1". QUESTA è NUOVA, NON CREDO SERVA
  - ECN (Explicit Congestion Notification): se impostato a "1" indica che l'host supporta L'ECN durante il 3-way handshake. QUESTA è NUOVA, NON CREDO SERVA
  - URG: Se impostato a "1" indica che nel flusso sono presenti dati URGENTI alla posizione (offset) indicata nel campo Urgent pointer.
  - ACK: Se impostato a "1" indica che il campo Acknowledgment number è valido;
  - PSH: Se impostato a "1" indica che i dati in arrivo devono essere passati subito ai livelli superiori senza che vengano bufferizzati.
  - RST: Se impostato a "1" indica che la connessione non è valida; usato in caso di errore grave; Utilizzato per la reimpostazione della connessione diventata incongruente.
  - SYN: Indica che l'host mittente del segmento vuole stabilire una connessione e specifica nel campo Sequence number il valore dell'ISN; utilizzato per stabilire le connessioni. Chi invia il SYN deve attendere dall'host remoto un SYN/ACK.

  - FIN: Se impostato a “1” indica che l’host mittente del segmento vuole chiudere la connessione TCP aperta con l’host destinatario, chi invia FIN non può più inviare dati, mentre il destinatario ha ancora la linea aperta, dovrà inviare un ACK per chiuderla definitivamente.

- Window size [16 bit]: Indica la dimensione della finestra di ricezione dell’host mittente, cioè il numero di byte che il mittente è in grado di accettare a partire da quello specificato nell’ Acknowledgment number.
- Checksum [16 bit]: Campo di controllo utilizzato per la verifica della validità del segmento. L’algoritmo di checksum somma semplicemente i complementi a uno delle parole di 16 bit e quindi calcola il complemento a uno della somma. Quando il ricevente esegue il calcolo sull’intero segmento (compreso il checksum) il risultato dovrebbe essere 0.
- Urgent pointer [16 bit]: Puntatore a dato urgente, ha senso solo se il flag URG è impostato a “1”, indica lo scostamento in byte a partire dal Sequence number del byte di dati urgenti all’interno del flusso.
- Options: opzioni facoltative per usi del protocollo avanzati.
- Data: Rappresenta il carico utile (payload) da trasmettere.



50 Cos’è il DNS?

Protocollo dello strato applicativo, **DNS** (Domain Name System) è un sistema per la risoluzione di nomi degli host in indirizzi IP. L’essenza del DNS

è l'invenzione di uno schema di denominazione gerarchico basato su dominio, e di un sistema di database distribuito per l'implementazione di questo schema di denominazione.

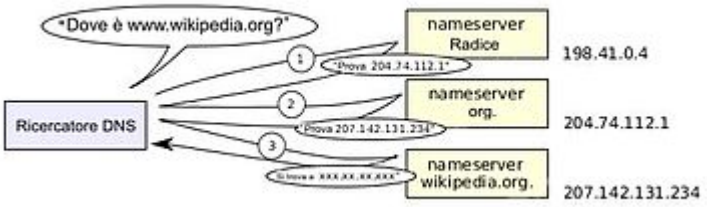
Per associare un nome ad un indirizzo IP, un programma applicativo chiama una procedura di libreria chiamata risolutore, passando il nome come parametro. Il risolutore invia un pacchetto UDP ad un server DNS locale, che quindi cerca il nome e restituisci l'indirizzo IP al risolutore, che a sua volta lo restituisce al chiamante. Ora il programma, conoscendo l'indirizzo IP, può stabilire una connessione TCP con la destinazione oppure inviarle i pacchetti UDP.

Questa tecnica è utile in quanto l'ampia diffusione di internet anche per utenti non tecnici non è pratica a memorizzare indirizzi IP numerici, per questo modificandoli in nomi testuali sono più semplici da memorizzare e utilizzare.

È possibile inoltre attribuire più nomi allo stesso indirizzo IP (o viceversa) per rappresentare diversi servizi o funzioni forniti da uno stesso host. Una stringa come www.ciaofede.it indica un host a cui ti sei connesso e a sua volta può essere scomposto in tre segmenti distinti:

- It denota il dominio di primo livello;
- Ciaofede è un dominio di secondo livello, cioè il nome che caratterizza questo sito web (insieme a .it).
- www è il dominio di terzo livello ed identifica un particolare host all'interno del dominio ciaofede.it.

Così facendo grazie al DNS è possibile visitare quell'host remoto senza dover scrivere l'indirizzo IP del server, ma scrivendo l'indirizzo testuale e facile da ricordare.



51 Cos'è un cifrario a sostituzione? E a trasposizione?

Le reti inizialmente venivano utilizzate da ricercatori universitari per scambiarsi e-mail, e dalle aziende per condividere le stampanti, di conseguenza la sicurezza aveva un ruolo marginale.

Oggi le reti sono utilizzate da milioni di persone per fare acquisti, lavorare con la banca o per documenti importanti. Questo fa diventare la sicurezza qualcosa di fondamentale e ricercato in quanto sempre più persone malintenzionate cercano di rubare dati sensibili. La crittografia serve a rendere un messaggio non comprensibile/leggibile a persone non autorizzate a leggerlo.

Per cifrare un messaggio ci sono diverse tecniche, una di queste è il **cifrario a sostituzione** (per cifrario s'intende una trasformazione carattere per carattere, senza considerare la struttura linguistica del messaggio). Uno dei cifrari più antichi che si conoscono è il cifrario di Cesare.

Il sistema generale sta nel sostituire appunto un carattere/coppie di lettere/sillabe/ecc con altre. Un altro tipo di cifrario è il **cifrario a trasposizione** che riordina le lettere senza mascherarle come fa il cifrario a sostituzione.

Un esempio è la trasposizione colonnare che funziona come segue: tramite una parola chiave si numerano le colonne, il testo in chiaro va disposto di seguito sulle colonne. Successivamente si ordinano le colonne in base alla parola chiave, ad ogni lettera viene dato un valore dipendente dal valore della lettera nell'alfabeto, successivamente si riscrive per colonne il testo cifrato.

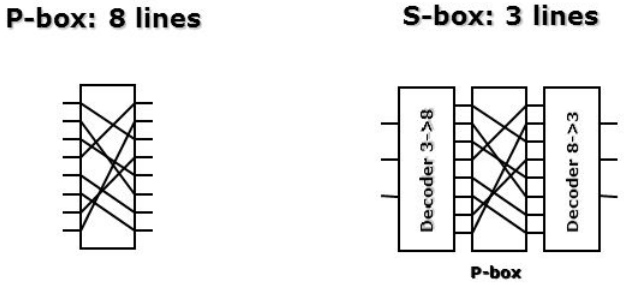
Le differenze sostanziali tra i due è che nel cifrario a sostituzione l'ordine rimane invariato ma le lettere vengono mascherate, in quello a trasposizione le lettere non vengono mascherate e il testo viene mescolato (secondo opportuni criteri).

52 Si descriva il block cipher

Block cipher è un algoritmo a chiave simmetrica (tecnica di cifratura in cui la chiave è la stessa sia per la crittazione sia per la decrittazione) operante su un gruppo di bit di lunghezza finita organizzati in un blocco. Questo tipo di algoritmi sono composti da due parti, una che cifra (E) e un'altra che decifra (E_1). Dati n bit in entrata in blocco, l'algoritmo cifra n bit in blocco. Per eseguire la crittazione e la decrittazione è possibile implemen-

tarli tramite semplici circuiti elettrici, come ad esempio la P-box (scatola di permutazione) o la S-box (scatole di sostituzione).

La P-box permette di trasporre 8 bit, se un input è lineare 01234567, l'output è 24506713, ovviamente la P-box lavora alla velocità della luce, in quanto non sono necessari calcoli, però è necessario conoscere la chiave di cifratura (ossia come sono disposti i collegamenti interni della P-box). la S-box invece è un altro tipo di circuito che sostituisce il numero di bit del messaggio, mescolandoli. Se il messaggio in entrata ha m bit, l'output è da n. Ad esempio si ha un input di 8 bit, l'output sarà da 3 bit permutati dagli 8, servirà poi una S-box per decifrare il messaggio e tornare agli 8 bit originali. Singolarmente questi metodi di cifratura non sono molto affidabili, la S-box infatti è molto vulnerabile agli attacchi basati sul tempo. La vera forza di queste tecniche sta nella loro combinazioni, combinando S-box e P-box infatti è possibile creare un output estremamente complicato da decrittare senza l'opportuna chiave.



53 Si descriva l'algoritmo DES e triplo DES

DES (Data Encryption Standard) è un algoritmo di cifratura scelto come standard, prima dal governo degli Stati Uniti e successivamente è diventato di utilizzo internazionale.

Si basa su un algoritmo a chiave simmetrica (Usa la stessa chiave per la crittografia e per la decrittazione) con chiave a 64bit (solo 56 utili, gli altri 8 sono di controllo). DES è un perfetto esempio di cifrario a blocchi, è un algoritmo che prende in ingresso una stringa di lunghezza fissa di testo in chiaro e, con una serie di operazioni complesse, da in output una stringa di testo della stessa lunghezza.

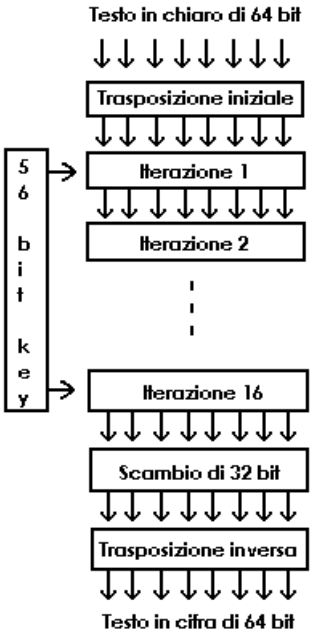
DES è formato da 19 stadi distinti:

- il primo traspone semplicemente i 64 bit di testo in chiaro, l'ultimo fa il contrario.
- Il penultimo stadio scambia i 32 bit più a sinistra con i 32 più a destra.
- Gli altri 16 stadi sono funzionalmente identici, ma sono parametrizzati da funzioni diverse della chiave.

A causa della dimensione ridotta della chiave (64 bit sono facili da forzare) DES non è molto sicuro. Per migliorare la complessità dell'algoritmo viene implementato un nuovo metodo chiamato triplo DES. Nel triplo DES vengono utilizzate due chiavi e tre stadi. Nel primo stadio il testo viene cifrato con il sopracitato DES usando la chiave K_1, nel secondo stadio DES viene usato in modalità di decifrazione usando la chiave K_2. Infine, un'ultima cifratura viene fatta con K_1. È un metodo Encrypt Decrypt Encrypt (EDE). Il metodo EDE è stato scelto in quanto risulta compatibile con i computer che usano la cifratura singola, semplicemente impostando $K_1 = K_2$.

Usando questi metodi crittografici un problema è il fatto che se si prende un testo in chiaro e si cifra, il testo cifrato sarà sempre uguale, anche se si prova 100 volte.

AES (Advanced Encryption Standard) sostituisce triplo DES (quindi anche DES).

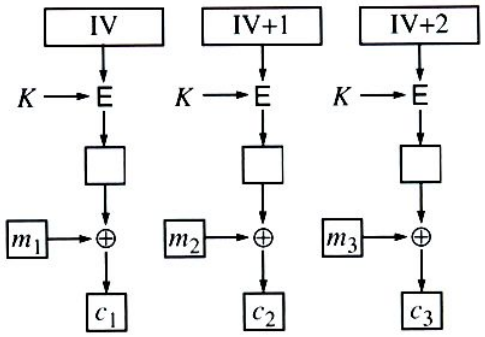


54 Counter Mode Cipher

La maggior parte delle tecniche di cifratura hanno il problema di rendere impossibile l'accesso casuale ai dati. Questo è un problema quando ad esempio si va accede ad un file su disco in ordine non sequenziale (random), se il file è cifrato con il cipher block chaining (tecnica che cifra i blocchi basandosi sui blocchi precedenti) allora bisogna prima decifrare tutti i blocchi precedenti, questo può diventare inutilmente oneroso.

Per questo motivo è stata creata la modalità contatore. In questo caso il testo in chiaro non viene cifrato direttamente; si cifra invece un vettore d'inizializzazione (IV) con una costante (K), successivamente il risultato viene messo in XOR con il testo in chiaro. Si incrementa di 1 il vettore d'inizializzazione ad ogni blocco, diventa facile riuscire a decifrare un blocco in qualunque posizione esso si trovi, senza decifrare prima i suoi predecessori.

Questa tecnica ha una debolezza abbastanza notevole, se si utilizza la stessa chiave e lo stesso IV per due messaggi diversi, se un malintenzionato riesce a reperire i due testi cifrati, facendo un semplice XOR fra i due riesce a sopprimere tutta la protezione crittografica. Nonostante ciò, questa tecnica è sicuramente utile.



55 Cipher block chaining

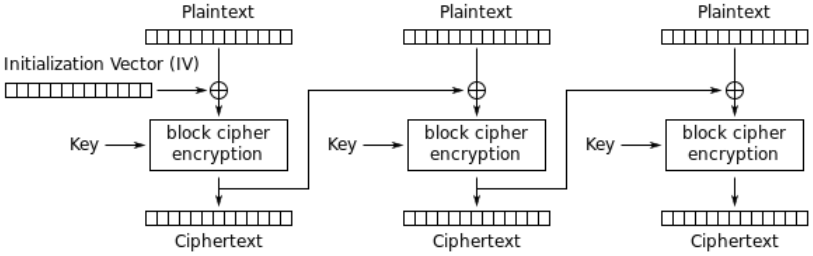
DES, triplo DES e AES, utilizzano un cifrario a sostituzione monoalfabetica che usa caratteri lunghi. Usando sempre la stessa chiave, ottenendo sempre blocchi di testo cifrato uguali (per testo in chiaro uguale), risulta semplice (con un po' di forza bruta) compromettere la sicurezza dei blocchi cifrati con queste tecniche.

Un modo per evitare questo problema è collegare tutti i blocchi cifrati in modo diverso, questa tecnica è chiamata Cipher block chaining. In questo

metodo, ogni blocco di testo in chiaro 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. Per il primo blocco di questa catena lo XOR viene calcolato con un blocco di dati casuali (vettore di inizializzazione IV), che è trasmesso (in chiaro) insieme al testo cifrato.

Questo metodo rende la criptoanalisi più difficile, con un grande incremento di sicurezza. Un problema è il fatto di rendere impossibile la decrittazione di un blocco in maniera casuale senza prima aver decrittato tutti i blocchi precedenti. Problema risolto dal counter mode cipher.

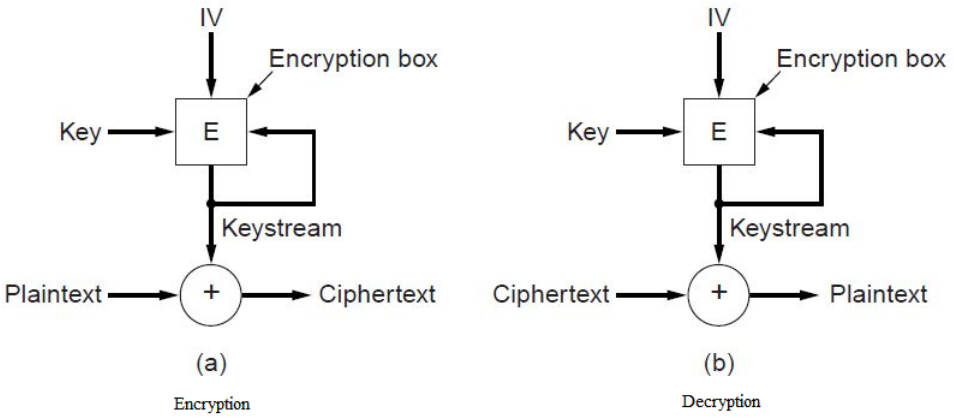


56 Stream cipher

Una variante dei cifrari a blocchi è stream cipher (cifrario di flusso). Questa tecnica sfrutta un vettore di inizializzazione (IV) e una chiave, cifrate insieme generano un keystream che è indipendente dal testo in chiaro, successivamente si può cifrare nuovamente il keystream con la chiave, un numero arbitrario di volte per ottenere keystream differenti, con la quale poi verrà cifrato il testo in XOR. Per la decrittazione viene eseguita generando lo stesso keystream dal lato del ricevente.

Questa tecnica permette un'alta elasticità agli errori, in quanto la keystream non dipende dai dati e su di essa si basa la cifratura di ogni blocco, di conseguenza un errore nel testo in chiaro vale come un errore nel testo cifrato (problema che riguardava il cipher block chaining).

Tuttavia, per utilizzare al meglio questa tecnica, IV e chiave non devono mai essere riutilizzati, altrimenti si genererebbe più volte lo stesso keystream, stessa cosa vale per la cifratura, non va mai utilizzato lo stesso keystream per cifrare un testo, altrimenti si viene esposti al problema del tipo keystream riutilizzato.



57 RSA

Un grosso problema del sistema crittografico è sempre stata la distribuzione delle chiavi. È sempre stato assunto che le chiavi di cifratura e decifrazione fossero le stesse (o derivabili l'una dall'altra), e la chiave doveva essere distribuita a tutti gli utenti del sistema. Qualora un intruso riusciva a rubare una chiave, tutto il sistema andava a rotoli.

Una variante per le chiavi simmetriche (stessa chiave per decifrare e cifrare) è stato dato dalle chiavi asimmetriche (o chiavi pubbliche/private). Questo sistema richiede che ogni utente sia in possesso di due chiavi, una pubblica per la cifratura e una privata per la decifratura, quella pubblica può essere condivisa al mondo, mentre quella privata dev'essere in possesso solo del proprietario. Cosi facendo chiunque può scrivere un messaggio cifrato a chi vuole, basta cifrarlo con la chiave pubblica della persona interessata, la persona interessata poi usera la sua chiave privata per decifrarlo.

RSA è un algoritmo di crittografia che cerca di trovare un modo per generare queste chiavi, in modo da renderle impossibili da dedurre tramite calcoli. È considerato un algoritmo molto robusto, il suo maggior svantaggio è che richiede chiavi di almeno 1024 bit per poter offrire una buona sicurezza (contro i 128 bit degli algoritmi a chiave simmetrica) il che lo rende abbastanza lento. Si basa su alcuni principi di teoria dei numeri che si possono riassumere in quattro punti:

- Si scelgono due numeri primi, p e q (tipicamente di 1024 bit)
- Si calcola n=p*q e z=(p-1)*(q-1).

- Si sceglie un numero primo relativamente a z, detto d.
- Si trova e tale che e*d=1 mod z.

Si divide il testo in chiaro, P, in modo che $0 \leq P < n$. Per cifrare il messaggio P, calcoliamo $C=P^e$ (mod n). Per decifrare C calcoliamo $P=C^d$. Questo si può fare perché le funzioni di cifratura e decifrazione sono una l'inverso dell'altra. La chiave pubblica quindi consiste nella coppia (e,n) mentre quella privata consiste in (d, n).

La sicurezza del metodo è basata sulla difficoltà di scomporre in fattori i numeri molto grandi. Grazie a questo metodo si può fare il passaggio di dati con persone sconosciute, come nell'esempio di prima.

58 Si descriva la tecnica di attacco "Birthday attack"

L'autenticità di molti documenti legali, finanziari ecc. è basata sulla presenza o assenza di una firma autografa autorizzata. Per questo esistono le firme digitali. Grazie a queste si può verificare l'autenticità di un documento. Queste firme si basano su protocolli crittografici comunemente utilizzati.

Per generare una firma digitale vengono utilizzate delle funzioni di hash, tra queste la funzione MD (message digest) che ha 4 importanti proprietà:

- È facile calcolare MD(P) (P messaggio).
- Da MD(P) è praticamente impossibile trovare P.
- Dato P, nessuno è in grado di trovare P' tale che MD(P')=MD(P). (non è possibile trovare un testo la cui cifratura è uguale alla cifratura di un altro testo.
- Se l'input cambia anche solo di 1 bit, l'output diventa completamente diverso.

Grazie a queste proprietà la firma diventa estremamente sicura e può far da garante per documenti importanti.

Il birthday attack è un esempio per dimostrare che, per forzare una MD di m bit, bastano solamente $2^{m/2}$ operazioni. L'idea per quest'attacco viene da una tecnica che i professori di matematica usano spesso nei corsi di matematica: "Quanti studenti ci devono essere in una classe perché la probabilità che due persone abbiano lo stesso compleanno superi il 50%?" (23). Con 23 persone possiamo formare (23*22)/2=253 coppie differenti, ognuna

ha probabilità 1/365 di essere quella buona, di conseguenza la percentuale di possibilità supera facilmente il 50%.

Generalizzando questa idea: Se c'è una funzione fra input e output con n valori di input e k possibili valori di output, ci sono n(n-1)/2 coppie di input. Se n(n-1)/2>k la possibilità di avere una coppia con lo stesso output è decisamente alta: Per avere due output uguali basta avere $n>\sqrt{k}$. Tutto questo significa che un MD di 64 bit, può essere forzato, con buona probabilità, generando 232 messaggi e cercandone due con lo stesso MD.

59 Sicurezza in 802.11

Lo standard 802.11 (standard di trasmissione per le reti WLAN (Wireless LAN)) prescrive un protocollo per lo strato data link, questo protocollo è chiamato WEP (Wired Equivalent Privacy) il cui scopo è portare sulla LAN wireless la stessa sicurezza di quella cablata.

WEP utilizza uno stream cipher (cifratura di flusso a chiave simmetrica) basato sull'algoritmo RC4 per cifrare i dati e CRC-32 (controllo a ridondanza ciclica) per verificare l'integrità. Nel WEP, RC4 è utilizzato per generare un keystream che viene applicato in XOR al testo in chiaro per produrre il testo cifrato. La keystream è generata partendo da un vettore di inizializzazione (IV), vettore che deve essere cambiato ad ogni invio per mantenere alta la sicurezza. Il suo funzionamento è il seguente:

- Viene calcolato il checksum del payload utilizzando il CRC-32.
- Il checksum viene aggiunto al payload per formare il testo in chiaro.
- Al testo in chiaro (payload+checksum) viene applicato in XOR una parte del keystream pari alla sua lunghezza. Il risultato è il testo cifrato.
- L'IV utilizzato per inizializzare il keystream RC4 viene inviato insieme al testo cifrato. Quando il destinatario riceve il pacchetto:
- Estrae il payload cifrato.
- Genera il keystream a partire dalla chiave segreta condivisa e l'IV ricevuto.
- Calcola lo XOR fra il testo cifrato e il keystream ottenendo il testo in chiaro

- Verifica il checksum per vedere se ci sono state manomissioni.

Purtroppo, questo sistema non è molto affidabile, in quanto l'IV facilmente si ripete, generando il pericolo del riutilizzo del keystream e rendendo tutte le transazioni a rischio di letture indesiderate. WEP è stato già sostituito da nuovi sistemi più sicuri.

60 Si descriva la sicurezza di Bluetooth

Rispetto a 802.11, Bluetooth ha un raggio d'azione considerevolmente minore, tuttavia necessita di un buon grado di sicurezza. La sicurezza in Bluetooth è divisa in 3 modalità diverse, che vanno da nessuna sicurezza a una completa sicurezza dei dati e controllo dell'integrità. Generalmente la sicurezza bluetooth è tenuta disabilitata.

La sicurezza Bluetooth inizia quando un nuovo dispositivo slave chiede un canale al master. Questo controllo viene effettuato tramite passkey, generalmente salvate in entrambi i dispositivi e scambiate al momento del collegamento. Altre volte è una chiave interna ad un dispositivo che va poi inserita all'interno di un altro sotto forma di numero decimale. Quando si stabilisce un canale, master e slave controllano se l'altro conosce la passkey, in caso affermativo negoziano se il canale dev'essere cifrato e/o se bisogna effettuare il controllo di integrità. La cifratura usa uno stream cipher (cifratura a flusso a chiave simmetrica) e per il controllo d'integrità usa Safer+ (altro cifrario a blocco con chiave simmetrica).

Un altro problema di bluetooth è che autentica solo i dispositivi, e non gli utenti, quindi il furto di un dispositivo bluetooth lascia l'accesso a tutti i dati del proprietario precedente. Bluetooth implementa però la sicurezza anche in strati superiori al data link, tipo con password o PIN per completare la transazione.

61 La tecnica di attacco reflection attack

Il reflection attack è una tipologia di attacco informatico che sfrutta delle falle nei protocolli di autenticazione (servono per autenticare l'identità in caso di scambio di messaggi) cercando di simulare diverse entità.

In questa tipologia di attacco sono necessari due interlocutori, A e B, e dev'essere aprire più conversazioni contemporaneamente con la vittima (B). C , il nostro malintenzionato, seguendo alcune procedure e scambi multipli riesce a simulare l'identità di A, imbrogliando B, e potenzialmente aver accesso a tutte le conoscenze private di A che conosce B. (immaginando che B

sia una banca, C che finge di essere A, ha libero accesso ai suoi soldi, non è proprio una cosa carina).

Questo attacco porta a generare 4 regole per la buona riuscita di un protocollo di autenticazione:

- Fare in modo che chi inizia l'autenticazione provi la sua identità prima che lo faccia chi risponde.
- Far si che entrambi gli interlocutori utilizzino chiavi differenti per provare la propria identità.
- Far si che gli interlocutori usino (per le richieste) numeri presi da insiemi diversi.
- Rendere il protocollo resistente a attacchi che coinvolgono una seconda sessione parallela.

Se anche una sola di queste regole viene meno, il protocollo può essere forzato.

62 Replay attack

Il replay attack è una tipologia di attacco informatico che sfrutta le falle nei protocolli di autenticazione (servono per autenticare l'identità in caso di scambio di messaggi), cercando di simulare diverse identità e potenzialmente rubare dati.

Simile all'attacco Man-in-the-middle il replay attack consiste nell'impossessarsi di una credenziale di autenticazione comunicata da un host ad un altro, e riproporla successivamente simulando l'identità dell'emittente. La differenza con il Man-in-the-middle sta nell'asincronia dell'operazione: mentre in MITM le operazioni avvengono in tempo reale, nel replay attack l'azione fraudolenta può essere eseguita anche a distanza di giorni.

Un esempio si ha quando A invia una richiesta di bonifico alla propria banca (B), C intercetta i messaggi e li salva. Dopo un certo tempo C rispedisce gli stessi messaggi a B. B, credendo di parlare con A, esegue le istruzioni.

Esistono diversi metodi per impedire questo tipo di attacchi, uno è inserire un timestamp ai messaggi, cosi da evitare una ritrasmissione futura (vulnerabile, in quanto qualsiasi finestra temporale si metta per la validità dei messaggi, C può sempre sfruttarla). Un secondo metodo è inserire dei nonce (numero casuale che ha un utilizzo unico) nei messaggi, così da scartare messaggi con lo stesso nonce (il problema qui sta nel fatto che i nonce

vanno ricordati PER SEMPRE, nel caso di perdita si diventa vulnerabili ad attacchi).

63 Algoritmo Diffie-hellman

Chiamato anche scambio di chiavi Diffie-Hellman, è un protocollo crittografico che consente a due entità di stabilire una chiave condivisa e segreta, utilizzando un canale di comunicazione pubblico (a rischio di attacchi), senza che le due parti si siano scambiate informazioni o si siano incontrate in precedenza.

"A" e "B" devono mettersi d'accordo su due numeri grandi, n e g, in cui n e (n-1)/2 sono primi. Questi numeri possono essere pubblici, possono essere scelti entrambi da A o da B e poi riferiti all'altro in caso di necessità. "A" e "B" ora scelgono due numeri grandi e li tengono segreti , x e y per comodità. A questo punto "A" inizia la conversazione inviando a "B" un messaggio contenente (n, g, g^x mod n). "B" risponde inviando a sua volta un messaggio contenente g^y mod n. "A" prende il numero ricevuto da "B" e lo eleva alla x, mod n = $(g^y mod n)^x$ mod n. "B" fa una cosa simile per ottenere $(g^x mod n)^y$ mod n. A questo punto grazie alle regole dell'aritmetica entrambe le espressioni valgono g^{xy} mod n. "A" e "B" utilizzano questa come chiave segreta condivisa. Un possibile intruso non riuscirebbe a carpirla nemmeno se avesse ascoltato i messaggi in quanto non conosce le chiavi segrete di A e B.

Il problema dell'algoritmo sta nel fatto che "B" non può effettivamente sapere che è "A" a inviare la tripla iniziale, a causa di ciò, l'algoritmo diventa facilmente vittima del man-in-the-middle, una persona C se si mette tra i due e ascolta le conversazioni può simulare di essere sia A che B.

64 Attacco Man in the middle

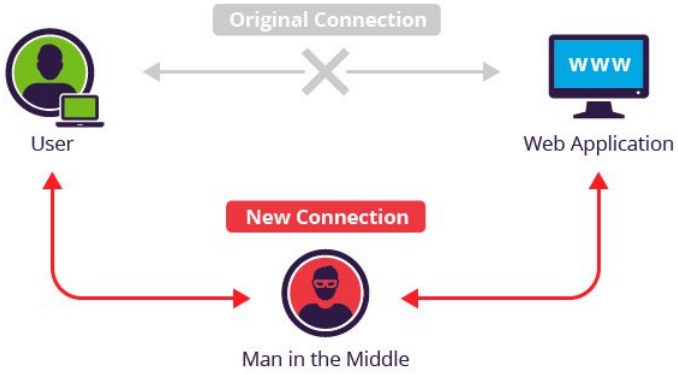
L'attacco Man-in-the-middle, letterlamente l'attacco dell'uomo in mezzo, è un attacco crittografico nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere i messaggi tra due interlocutori senza che nessuno dei due sospetti qualcosa.

L'attaccante dev'essere in grado di frapporsi tra le due parti e intercettare i messaggi, cosi facendo può simulare la risposta per entrambi. Potenzialmente questo attacco è fattibile verso qualsiasi conversazione che utilizza chiave pubblica.

Un esempio del suo funzionamento è il seguente:

- A e B vogliono comunicare.
- A chiede a B la propria chiave pubblica, B la invia
- La chiave di B viene intercettata da C, da qui inizia l'attacco.
- C invia ad A una propria chiave pubblica, di cui conosce la chiave privata per decrittare, A riceve la chiave pubblica pensando sia di B.
- A cifra i messaggi con la chiave di C (pensando sia di B) e invia i messaggi a B.
- C intercetta i messaggi, li decifra, tiene una copia per se e li ricifra (modificati se lo desidera) usando la chiave pubblica che B aveva inizialmente inviato ad A.
- Quando B riceverà il messaggio questo crederà provenga da A.

Una delle possibili difese da questo tipo di attacco è quella di creare un canale di comunicazione secondario, aggiuntivo e sicuro tra i due interlocutori.



65 DNS spoofing

DNS spoofing è una tipologia di attacco crittografico, fa parte di una categoria più vasta denominata man-in-the-middle. Gli attacchi di questo tipo consistono nel deviare i pacchetti di una comunicazione tra due host verso un attaccante. Questo attaccante finge di essere il mittente o il destinatario reale e può leggere, inserire o modificare i dati presenti nella conversazione.

Il protocollo DNS invece ha il compito di trasformare un indirizzo letterale (ad esempio www.fedesimpy.it) in indirizzo numerico o IP (202.159.222.222). Il DNS Spoofing si svolge quindi nel modo seguente:

- La vittima fa una DNS Query
- L'attaccante la intercetta e risponde con una risposta falsa, diversa da quella che sarebbe stata fornita dal DNS.

Lo scopo dello spoofing è modificare la corrispondenza tra indirizzo IP e nome del sito contenuti nelle risposte.

Una possibile soluzione per rendersi conto di essere sotto attacco è di individuare possibili risposte multiple. Ci sono altri protocolli utilizzabili per evitare questo tipo di manomissione.