CAPITOLO 2
Serie di Fourier
È una funzione che rappresenta la trasmissione via cavo di informazioni, rappresentando variabili come la tensione e la corrente; è composta da una serie infinita di seni e coseni e può rappresentare un segnale periodico regolare.
La serie di Fourier è soggetta ad attenuazione e distorsione oltre una certa frequenza, quindi il segnale perde uniformità. L'intervallo di frequenze che non subisce una forte attenuazione è chiamato banda passante, è una proprietà fisica di trasmissione e dipende dalla costruzione, spessore e lunghezza del mezzo di trasporto.
Per trasmettere ad alte frequenze è richiesta una potenza maggiore; la potenza richiesta cresce col quadrato della frequenza.
Teorema di Nyquisit: esprime la velocità massima di trasmissione in assenza di rumore:
Poiché i canali di trasmissione non sono perfetti a causa del rumore termico, il teorema di Shannon esprime la velocità massimo di data rate in presenza di rumore:
inoltre per far fronte alla dispersione di segnali si ricorre ai ripetitori.

Bit rate e baud rate
Data rate= quante info trasmettiamo
Bit rate= quanti bit trasmettiamo
Teorema Nyquisit= relazione tra bit rate con banda disponibile
Teorema Shannon= massimo data rate
Bit rate= baud rate

Vari tipi di cavo
Doppino
Formato da cavi in rame intrecciati tra loro in forma elicoidale al fine di limitare l'interferenza reciproca. Maggiore è l'intreccio maggiore è la velocità e minore è l'interferenza; ad un maggiore intreccio corrisponde un costo più alto.
L'applicazione più comune è per il sistema telefonico in quanto cavi in rame possono ricoprire lunghe distanze senza perdere segnale e senza bisogno di ripetitori; inoltre possono trasmettere segnali analogici e digitali. L'ampiezza di banda dipende dal diametro del cavo e dalla distanza percorsa. Questi cavi sono chiamati anche UTP.
I vantaggi sono il basso costo, lunga distanza percorribile, ampiezza di banda considerevole (UTP3= 250MHz, UTP6=600MHz).
Cavo coassiale
Composto da un nucleo di rame coperto da un rivestimento isolante, un tubo cilindrico chiamato calza conduttrice e una copertura in plastica. La sua ampiezza di banda può raggiungere 1 GHz, più elevata del doppino, e può estendersi per distanze più lunghe. Spesso usato per le MAN e le tv via cavo.
Fibra ottica
Sistema di trasmissione formato così: al centro del cavo si trova un nucleo (core) di vetro attraverso il quale si propaga la luce; il nucleo è circondato da un rivestimento in vetro (cladding) che ha un indice di rifrazione più basso, in maniera tale da costringere la luce a rimanere nel nucleo, che a sua volta è rivestito da una sottile fodera di plastica. Le fibre sono solitamente raggruppate in fasci protetti da guaine
Per trasmettere info un rilevatore trasforma il segnale elettrico in impulso luminoso, che attraverso il cavo trovando all'altro capo un ulteriore rilevatore che esegue l'operazione opposta.
Le fibre di vetro sono poco mobili, quindi per connetterle tra loro si possono usare connettori (perdono 10-20% di luce) , allineatori meccanici (10% luce persa), fusione (1% luce persa).
Gli svantaggi della fibra rispetto ai cavi in rame sono la dispersione di segnali, l'alto costo, la necessità ripetitori più complessi; i vantaggi sono la difficile intercettazione, l'alta banda (fino 10 Ghz), la piccola mole dei materiali.

Satelliti
Il satellite è un grande ripetitore di microonde collocato in cielo e che contiene molti transponder, ovvero ricetrasmettitori satellitari. La grandezza dei raggi trasmessi verso terra è detta bent pipe. I satelliti si collocano su 3 fasce di Van Allen, ovvero strati di particelle molto cariche. Più basso è il

satellite, più satelliti servono per garantire la copertura; più alto è il satellite, maggiore sarà la latenza. Il lancio dei satelliti bassi costa meno.
LEO (low earth)= posti nella fascia più bassa, si spostano rapidamente, quindi ne servono molti di questo tipo; per questo motivo hanno anche bisogno di molta energia. Il ritardo nella connessione è di pochi msec, quindi vengono impiegati nelle telecomunicazioni. Sono utilizzati per le telecomunicazioni, fanno parte dei satelliti LEO i satelliti Iridium per le comunicazioni tra satelliti (sempre in ambito di telecomunicazioni), Globalstar per trasmettere a terra, Teledesic per internet con 32 satelliti.
MEO(medium earth)= sono situati nelle fasce intermedie, coprono una distanza più piccola e impiegano 6 ore per compiere un giro completo; questo tipo di satelliti sono i GPS.
GEO= sono i più alti nelle fasce, coprono 1/3 della superficie terrestre, sono posti ad una distanza di 2° quindi ve ne sono 180 in orbita; l'orbita in questione è l'unica a circonferenza e si trova all'altezza dell'equatore. Sono impiegati come satelliti spia o meteo.

Cellulari

1° GENERAZIONE

AMPS
In tutti i sistemi telefonici un'area geografica è divisa in celle, che in AMPS sono ampie 10-20 Km, ognuna delle quali utilizza frequenze non utilizzate dalle celle vicine. Si utilizzano celle relativamente piccole e il riutilizzo delle frequenze di trasmissione delle celle vicine ma non adiacenti. In un'area dove il numero di utenti è cresciuto al punto che il sistema si è sovraccaricato la potenza viene ridotta e le celle sovraccaricate sono divise in celle più piccole, chiamate microcelle, per aumentare il riutilizzo delle frequenze. Al centro di ogni cella si trova una stazione di base, che comunica con tutti i telefoni che si trovano nella cella, composta da un computer e un trasmettitore/ricevitore collegato ad un'antenna. In un piccolo sistema tutte le stazioni sono collegate ad un singolo dispositivo chiamato MTSO (Mobile Telephone switching Office) o MSC (Mobile Switching Center). Gli MTSO comunicano tra di loro mediante una rete di comunicazione a pacchetto. Quando un telefono mobile abbandona fisicamente una cella la stazione di base di quella cella verifica il livello di potenza del segnale ricevuto dalle stazioni che si trovano nelle celle adiacenti e trasferisce la gestione dell'apparecchio alla cella che riceve il segnale più forte, ossia la cella in cui ora si trova il telefono. Il telefono viene informato dell'identità della nuova centrale di controllo e se durante lo spostamento era in corso una chiamata l'apparecchio viene forzato dal MTSO a passare su un nuovo canale (handoff, 300 msec). Nel soft handoff il telefono è acquisito dalla nuova stazione di base prima di interrompere il segnale precedente evitando perdita di continuità (l'apparecchio dev'essere in grado di sintonizzare due frequenze nello stesso momento), nell'hard handoff invece la vecchia stazione di base rilascia il telefono prima che la nuova lo acquisisca.
Il sistema AMPS utilizza 832 canali full duplex ognuno composto da una coppia di canali simplex (832 canali di trasmissione simplex compresi tra 824 e 849 MHz e 832 canali di ricezione simplex compresi tra 869 e 894 MHz). Ognuno di questi canali simplex è ampio 30 kHz, perciò AMPS utilizza FDM per separarli.

2° GENERAZIONE

D-AMPS
È stato progettato per coesistere con AMPS, perciò i telefoni cellulari di prima e seconda generazione possono operare contemporaneamente nella stessa cella. Usa tutte le bande di AMP più 3 aggiuntive per gestire l'aumento di carico: i canali in trasmissione spaziano nell'intervallo 1.850-1.910 MHz e i corrispondenti canali in ricezione occupano l'intervallo 1.930-1.990 MHz, ancora una volta a coppie. In questa banda le onde sono lunghe 16 cm e vengono utilizzati gli stessi canali a 30 kHz. Su un

telefono mobile D-AMPS il segnale vocale raccolto dal microfono viene digitalizzato e compresso da un circuito presente all'interno del telefono chiamato vocoder in maniera tale da ridurre il numero di bit trasmessi attraverso il collegamento. La digitalizzazione e la compressione eseguite nell'apparecchio offrono un enorme miglioramento, talmente elevato che tre utenti DAMPS possono condividere una singola coppia di frequenza usando la tecnica di multiplexing a divisione di tempo. Essendo un sistema digitale si usano tecnologie di compressione del flusso, il maggior problema è che è necessaria una bassa compressione a basso costo.

GSM:
global system for mobile communication; è simile al D-AMP, usa il TDM e FDM.
Rispetto al D-AMP ha i canali da 200 khz con una capienza di 8 utenti; presenta 124 canali simplex ampi 200 khz e supporta 8 connessioni separate, 4 per direzione, inoltre trasmissione e ricezione non avvengono nello stesso momento perchè il sistema non è in grado di gestirlo.
al netto dell'elaborazione dati e della correzione errori rimangono 13 kbs a disposizione per la voce.
Con GSM sono state introdotte le SIM= subscriber identity module che contengono il numero di cellulare, le KI = chiave di identificazione, e le IMSI = international mobile subscriber identity, ovvero l'identificazione della SIM.
L'identificazione avviene così:
- cellulare manda IMSI e ki in broadcast;
- l'operatore lo riceve e manda un numero casuale
- il cellulare lo rimanda firmato con la ki;
- l'operatore controlla la corrispondenza, quinti se corrisponde è tutto ok;

Nel Protocollo GSM ci sono 4 tipi di cellule:
macro: sono sopraelevante rispetto agli edifici e hanno raggio massimo di 35 km;
micro: sono alla stessa altezza degli edifici
pico: sono usate nelle aree particolarmente dense;
umbrella: coprono i vuoti lasciati dalle altre.
Svantaggi: costruito per trasmettere voce, quindi se si volessero trasmettere dati si occuperebbe un intero canale voce anche quando il traffico è poco, inoltre la tariffa corrispondente è a tempo non a traffico/pacchetti.

CDMA:
Permette ad ogni stazione di trasmettere per tutto il tempo attraverso l'intero spettro di frequenza.
Secondo CDMA i segnali sovrapposti si sommano linearmente, quindi ogni coppia può comunicare contemporaneamente grazie al fatto che sfrutta un linguaggio diverso. Per risalire al messaggio originale basta togliere il rumore aggiunto. Questo linguaggio usa uno spazio multidimensionale dove si usano regole di composizione (somma) e proiezione (prodotto scalare) per fare encoding e decoding. Per riuscirci si usano i codici di Walsh, derivati dalle matrici di Hadamard.
Non usando FDM non è necessario separare le celle in frequenza, quindi tutte le celle usano la stessa banda, inoltre sfrutta la caratteristica di intermittenza della voce umana, che in una conversazione occupa il 30/40% del tempo.
Nella pratica ogni tempo di bit è diviso in m intervalli chiamati chip e ad ogni stazione viene assegnata una sequenza di chip univoca.
Per trasmettere un 1 la stazione deve inchiare la sequenza, per trasmettere uno 0 deve farne il complemento. Se si vuole aumentare la quantità di info da inviare si aumenta l'ampiezza di banda di un fattore m.

3° GENERAZIONE

GPRS
Classificato come 2.5G perché consiste in una rete a pacchetti costruita sopra D-AMP e GSM.
GPRS permette di inviare e ricevere pacchetti in una cella IP basata sul sistema vocale; quando attiva infatti alcuni slot temporali sono divisi in canali logici dove ogni canale è usato per scaricare i pacchetti dove è indicato il destinatario.

Per inviare uno o più pacchetti la stazione mobile richiede uno o più slot alla base, quindi la base invia il pacchetto prima tramite internet e poi tramite rete via cavo. Inoltre GPRS supporta i protocolli IP e PPP, quindi è in grado di allocare dinamicamente canali internet e voce.
Vantaggi: con navigazione a pacchetti si spreca poca banda e le tariffe sono a traffico, non a tempo.

Modulazioni FSK, AM, PSK
FSK: si modula la frequenza in maniera proporzionale all'ampiezza che si vuole trasmettere, ovvero si cambia la frequenza in base al simbolo che si vuole trasmettere.
AM: modulazione in ampiezza in maniera proporzionale all'ampiezza da trasmettere; usata principalmente nelle trasmissioni via radio.
PSK: modulazione di fase, cambio fase del segnale a seconda del simbolo
Modulazione delta: variante del DPCM, metodo di codifica che prevede la trasmissione della differenza tra il bit precedente e quello attuale, quindi viene trasmesso +/-1. Le comunicazioni compresse vengono gestite in TDM. È Usata nei sistemi di telecomunicazioni della NATO.

MODEM
Per inviare segnali digitali attraverso una linea telefonica il computer deve convertire i dati in forma analogica per poterle trasmettere attraverso l'ultimo miglio. La conversione è eseguita attraverso un modem. Una volta nella centrale i dati sono riconvertiti in formato digitale prima di essere trasmessi attraverso le linee a lunga distanza.
I problemi principali delle linee di trasmissione sono: 1) attenuazione (dB/Km), ovvero la perdita di energia causata dalla propagazione del segnale verso l'esterno che dipende dalla frequenza del segnale; 2) distorsione, causata dal fatto che ogni componente di Fourier si propaga a velocità differente attraverso il cavo; 3) rumore, energia indesiderata generata da sorgenti esterne al trasmettitore.
Per minimizzare gli effetti che attenuazione, distorsione e rumore hanno sul segnale è meglio che questo non abbia un largo intervallo di frequenze. Le onde quadre utilizzate nei segnali digitali utilizzano un ampio spettro di frequenza e perciò rendono adatta la trasmissione in banda base (DC) solo a velocità basse e distanze brevi. Viene quindi usata la trasmissione AC introducendo un tono continuo, chiamato portante d'onda sinusoidale, la cui ampiezza, frequenza o fase possono essere modulate per trasmettere informazioni. Un apparecchio che accetta un flusso seriale di bit in ingresso e produce una portante modulata attraverso uno o più di questi metodi è chiamato modem, e si trova tra il computer e il sistema telefonico. La banda passante di un mezzo di trasmissione è l'intervallo di frequenze che passa attraverso il mezzo con un'attenuazione minima. Il numero di campioni al secondo è detto baud-rate (baud), durante ogni baud viene prodotto un simbolo quindi baud-rate e frequenza dei simboli si equivalgono. La tecnica di modulazione utilizzata determina il numero di bit per simbolo. Le combinazioni valide di ampiezza e fase sono chiamati diagrammi costellazione, ogni modem ad alta velocità ha un suo schema di costellazione e può comunicare solo con altri modem che adottano lo stesso schema. Tutti i modem moderni permettono di trasmettere contemporaneamente in entrambe le direzioni utilizzando frequenze diverse (full duplex). Una connessione che permette ai dati di scorrere in entrambi i sensi ma solamente un senso alla volta è detta half duplex, mentre quella che permettere di trasmettere i dati in una sola direzione è detta simplex.

Multiplexing: FDM, TDM, CDM, WDM
Si tratta di algoritmi con i quali si condivide il canale
FDM: frequency division multiplexing, divide lo spettro in varie bande di frequenza e ad ogni utente viene assegnata una porzione della banda con uso esclusivo. Nello standard comune si usano 12 canali voce uniti in multiplexing nella banda tra 60-108 KHz, formando un gruppo. Il gruppo a sua volta può essere unito in supergruppo e mastergroup. Usato dal GSM.

TDM: time division multiplexing, l'intera banda viene assegnata a tutti gli utenti a turno per un tempo limitato secondo politica Round Robin. Usato da Bluetooth, GPRS, GSM.
CDM: code division multiplexing: un segnale a banda stretta viene sparso su uno a banda di frequenza più ampia, allora il segnale è più tollerante alle interferenze e più utenti possono condividere la stessa banda; per avere il messaggio originale basta eliminare il rumore aggiunto. Usato da CDMA e reti wireless.
WDM: multiplexing a divisione di lunghezza d'onda; usato per i canali a fibra ottica; 4 fibre sono inserite nello stesso canale e ognuna trasporta energia a diversa lunghezza d'onda. Facendo viaggiare più canali in parallelo su lunghezze d'onda diverse si aumenta l'ampiezza in modo lineare e si amplificano i segnali.

QAM e QAM16
QAM si basa sul principio di combinare la modulazione in ampiezza con quella in frequenza allo scopo di aumentare la banda (ovvero aumentare l'ampiezza), infatti se cambiassimo solo la fase per aumentare l'alfabeto dei simboli, otterremmo un maggior numero di simboli molto simili tra di loro e quindi indistinguibili, aumentando il rischio di errori.
Abbiamo due tipi i QAM: QAM16 usa 16 simboli, quindi 4 ampiezze e 4 fasi, ottenendo bit rate quadruplo rispetto al baud rate; oppure QAM64 che usa 64 simboli e bit rate sestuplo rispetto al baud rate.
Per rappresentare i QAM si usano diagrammi a costellazione che mostrano la combinazione delle varie ampiezze di fase; ogni modem ha il suo schema di costellazione; quello ottimale sarebbe quello circolare come in QAM8, ma nella pratica vengono usati quelli rettangolari perché più facili da generare e codificare.

CAPITOLO 3

STRATO DATA LINK

ALGORITMI SUDDIVISIONE FRAME

Byte Stuffing
Metodo di framing che suddivide il flusso di bit in frame. Per farlo utilizza un byte speciale detto flag byte, che viene posto all'inizio e alla fine di ogni frame; in questo modo se il destinatario perde la sincronizzazione deve cercare solo il flag byte per trovare la fine del frame corrente. Un inconveniente è quando all'interno del flusso di dati compare un flag byte che interferisce con le operazioni di framing. Una soluzione è quella di far inserire dalla sorgente un byte di escape subito prima di ogni occorrenza accidentale; successivamente il destinatario rimuoverà il suddetto byte (destuffing) prima di passarlo allo strato network.
Lo svantaggio di questo metodo è che funziona solo con caratteri di 8 bit e non tutte le codifiche lo supportano. Al contrario il bit stuffing aggira questo problema. È una tecnica usata nel character count.

Bit stuffing
Ha funzionamento simile al byte stuffing, ma i frame sono contrassegnati con un gruppo speciale di bit, ovvero 0111110 (cinque 1), che rappresentano il flag byte. Quando la sorgente incontra cinque 1 consecutivi nei dati inserisce uno 0 nel flusso di uscita; questa operazione è il bit stuffing. Il destinatario, quando riceve i cinque 1 e lo 0 successivo, elimina lo 0 (escaping). Nel caso in cui i dati interferiscano con il flag byte, allora alla sequenza viene aggiunto 10 e dopo l'operazione di destuffing il messaggio torna uguale all'originale. È una tecnica che spreca la banda ma non ha ritardi.

PROTOCOLLI CONTROLLO FLUSSO:

Piggybacking
Tecnica per trasmettere in entrambe le direzioni con full duplex. Per sfruttare maggiormente il canale di comunicazione si sfrutta un messaggio dal destinatario al mittente come mezzo per trasmettere l'ACK in testa al frame. Si usa solo se il destinatario deve inviare qualcosa alla sorgente, altrimenti se la sorgente continua a parlare per troppo tempo si invia l'ACK separato. Ogni partecipante alla comunicazione deve tenere sotto controllo due finestre: quella del frame in uscita e quella in entrata.
Vantaggi: miglior uso della banda e minor numero di frame inviati.

Stop and wait
È un protocollo per il controllo del flusso e si può utilizzare sia per i canali simplex che half duplex. Quando il mittente invia un blocco aspetta che il ricevente invii una conferma ACK; lo svantaggio è l'attesa della risposta, in compenso non c'è bisogno di regolare la velocità. Si possono generare diversi errori: il frame non arriva mai a destinazione, quindi il mittente aspetta all'infinito; risolvibile con un timer, quindi se entro un certo periodo non si riceve l'ACK il mittente reinvia il pacchetto; oppure l'ACK non arriva al mittente, quindi rimanda il pacchetto. In questo caso il destinatario controllerà i pacchetti, ed eliminerà il doppione.
Vantaggi: basta un canale half duplex, svantaggi: si può sprecare il 96% di tempo (banda).

Sliding Window
Utilizza la tecnica del piggybacking e viene utilizzato per il controllo dei flussi dei dati nei casi di full duplex. Ogni frame in uscita contiene un numero di sequenza che va da 0 a un valore massimo che di solito è 2^n -1; se invece è a 1 bit allora il numero di sequenza è 0 e 1.
Ad ogni istante la sorgente tiene traccia dei numeri di sequenza corrispondenti ai frame che è autorizzata a inviare e che quindi sono nella finestra di invio. Ovviamente più è grande la finestra più dati passano. Allo stesso modo la destinazione tiene traccia della finestra di ricezione. Immaginiamo la finestra come un intervallo che ha limite superiore e limite inferiore (es [0-2]). Quando la sorgente invia un frame, aumenta il limite superiore della finestra di 1. Quando arriva l'ACK di quel pacchetto si incrementa il limite inferiore (ovvero la finestra si sposta). Inoltre i frame dentro la finestra devono essere conservati nel buffer per l'eventuale ritrasmissione; se il buffer si riempie la consegna del pacchetto è sospesa.
Quando la destinazione riceve un pacchetto che si aspetta di ricevere, lo accetta e invia l'ACK, spostando la finestra in avanti. Se il pacchetto non è quello che si aspetta, lo scarta.
In caso di traffico sbilanciato ci sono problemi col piggybacking; una soluzione è l'utilizzo di un timer nel receiver, dove alla scadenza del timer manda un pacchetto di ACK senza piggybacking.
Fanno parte di questo tipo di protocollo gli sliding window a 1 bit, il go back n, il selective repeat.
Viene usato da TCP.

Go back n
Algoritmo per il controllo del flusso.
Taglia sliding window del ricevente =1, dell'inviante=n.
Se il tempo di andata e ritorno del segnale è alto, ovvero genera ritardi, si verifica una inefficienza con i protocolli stop and wait perché si attende l'ACK. Una soluzione è usare la tecnica del pipelining, ovvero si invia un certo numero di frame anche senza aver ricevuto l'ACK del primo. Se uno dei frame arriva danneggiato, il destinatario ignora sia quello danneggiato sia i frame successivi. Il mittente quindi non riceverà l'ACK di quei pacchetti e li rispedirà. Se il buffer del mittente si riempie, esso blocca lo strato network fino a quando non crea spazio.
Il difetto di questo approccio è che se il tasso d'errore è alto c'è uno spreco di banda. La soluzione è la gestione di timer multipli, uno per ogni frame inviato e non consegnato.

Selective repeat
Algoritmo per il controllo del flusso.
Taglia sliding window del ricevente=n, dell'inviante=n.
In questo caso si usa il pipelining, ma se un frame arriva danneggiato, il destinatario invia l'ACK di tutti i frame corretti eccetto quello del frame danneggiato, quindi il mittente rispedirà il frame privo di ACK.

Considerazioni: il mittente e il destinatario devono avere un buffer che contenga tutti i frame; vi è un basso spreco di banda che può diminuire ulteriormente se il destinatario inviasse un NACK per ogni frame errato, inoltre è necessaria la gestione di timer multipli, uno per ogni frame inviato e non confermato, mentre il ricevente può usare il piggybacking.

PPP
Point to point protocol, collegamento punto a punto tra router e utente. È un meccaniscmo di framing multiprotocollo adatto alle trasmissioni dati via modem, linee HDCL, SONET e altri strati fisici. Le sue funzioni sono: rilevazione degli errori, supporto per più protocolli, negoziazione IP, autentificazione.
Caratteristiche: metodo di framing che permette di limitare i vari frame in modo non ambiguo e il formato del frame permette la rilevazione degli errori; protocollo di collegamento per gestire connessione, test, negoziazione e gestione pulita di disconnessione; modalità per negoziare opzioni relative allo strato network.
Usa due protocolli: LCP= insieme di comandi per gestione del flusso e della comunicazione, NCP= dialogo con lo strato network. Usa il byte stuffing, non usa né frame numbering, né ACK.
Vantaggi: ha vari parametri settabili, tra cui togliere i byte inutili da ogni frame e settare la dimensione del payload.
Struttura frame:
- FLAG: flag tipico 01111110 (sei volte 1)
- Address: non viene usato, tutto 1
- Control: segnala il tipo di pacchetto che si invia
- Payload: campo dati
- Checksum: usa CRC
- FLAG: altro flag byte tipico

CAPITOLO 4

SOTTOSTRATO MAC

ALGORITMI ASSEGNAZIONE/CONTESA CANALE

ALOHA e ALOHA-Slotted
Algoritmo di assegnazione di un canale ad accesso multiplo dove ognuno trasmette ogni volta che ha bisogno di farlo.
ALOHA puro: non richiede una sincronizzazione temporale globale, quindi le stazioni trasmettono quando vogliono. Prima di trasmettere ascoltano il canale e confrontano ciò che ricevono con ciò che hanno spedito; se anche solo il primo bit di un nuovo frame si sovrappone all'ultimo bit del precedente allora si verifica collisione e le stazioni attendono un periodo di tempo casuale prima di ritrasmettere; questo perché altrimenti una collisione ne creerebbe infinite altre.
Le ritrasmissioni avvengono tramite meccanismo di back off, ovvero la ritrasmissione avviene dopo un periodo di tempo compreso tra 0 e (k-1)T dove T= tempo di trasmissione messaggio e k= collisioni già avvenute.
In generale con ALOHA puro si può usare il 18% del canale. Venne utilizzato quando si passò a internet via cavo e si presentò il problema di allocare un canale condiviso da più utenti.
ALOHA Slotted: il tempo viene suddiviso in intervalli discreti, ognuno corrispondente a un frame, dove i frame hanno dimensione uniforme. Gli utenti si sincronizzeranno in base ad una stazione che segnerà l'inizio e la fine di ogni intervallo come un orologio, e le stazioni trasmetteranno all'inizio di ogni intervallo. In questo modo si dimezzerà il periodo di vulnerabilità affinchè i frame o collidono completamente, o non collidono proprio, e quindi raddoppiando l'efficienza. Al massimo si usa il 37% del canale.

CSMA

Carrier Sense Multiple Access è un protocollo con rilevamento della portante e ne esistono diverse varianti
CSMA 1-persistente quando una stazione è pronta a trasmettere ascolta il canale e, se il canale è occupato, aspetta fino a quando non si libera. In caso di collisione la stazione rimane in attesa di un intervallo casuale prima di ritentare la trasmissione. Il principale problema di questo protocollo è dovuto al ritardo di propagazione, ovvero c'è la possibilità che subito dopo l'inizio di una trasmissione da parte di una stazione un'altra stazione sia pronta ad inviare dati e controlli il canale. Se il segnale della prima stazione non ha ancora raggiunto la seconda quest'ultima potrebbe ritenere il canale libero e iniziare a trasmettere i propri dati causando una collisione.
CSMA non persistente se il canale è occupato la stazione non esegue un controllo continuo per trasmettere subito il proprio frame ma attende un intervallo di tempo casuale prima di ripetere l'algoritmo. Questo meccanismo permette di utilizzare meglio il canale ma allunga i ritardi.
CSMA p-persistente si applica ai canali divisi in intervalli temporali e si basa sul fatto che quando il canale è libero una stazione trasmette subito con una probabilità p e rimanda fino all'intervallo successivo con probabilità q=1-p, il processo si ripete fino a che il frame non è stato trasmesso o un'altra stazione non inizia a trasmettere.
CSMA con rilevamento delle collisioni = CSMA/CD (CSMA/Collision Detection). Se due stazioni iniziano a trasmettere contemporaneamente, entrambe rileveranno la collisione quasi immediatamente. Invece di completare la trasmissione dei rispettivi frame ormai irrimediabilmente danneggiati le stazioni interrompono bruscamente la trasmissione, risparmiando tempo e banda, e attendono un periodo di tempo casuale prima di ritrasmettere i dati.
Vantaggi: migliore a carico basso, ma a carico alto ha troppi conflitti.

Collision Free Binary Countdown
Protocollo per la contesa del canale in caso di molte stazioni. Ogni stazione ha un proprio indirizzo univoco; se desiderare utilizzare il canale deve comunicare in broadcast il proprio indirizzo MAC sottoforma di stringa binaria partendo dal bit più significativo. Nel canale si fanno degli OR degli indirizzi di tutte le stazioni che vogliono trasmettere. Per stabilire chi vuole trasmettere si inizia a guardare la stringa con più bit significativi, e vince la stazione indirizzo più alto, la quale trasmetterà, e dopo inizierà un nuovo turno. Per evitare che la stazione continui a trasmettere, ad ogni round si riassegna una priorità casuale, ma si possono generare collisioni, oppure si assegna un priorità 0 e 1 se la stazione ha già trasmesso, oppure si ricorre al protocollo ALOHA. Con questo metodo l'efficienza può arrivare anche al 100%.
Vantaggi: migliore a carico alto, ma a basso ha spreco di banda.

Basic Bitmap
Fa parte di quei protocolli che risolvono la contesa per il canale senza generare collisioni. Date N stazioni, ogni periodo di contesa viene diviso in N intervalli (uno per stazione); ogni stazione trasmette con un bit la proprio volontà di trasmettere oppure no, in modo tale che durante il suo intervallo nessun altro trasmetta. Una volta trascorsi gli N intervalli ogni stazione sa esattamente quando deve trasmettere, quindi non ci sarà mai collisione.
Il problema è quando ci sono tante stazioni e il tempo di contesa è lungo. Efficienza: d/(d+1) dove d è la taglia del frame.

PROTOCOLLI SENZA COLLISIONE

Adaptive tree walk
Le stazioni vengono viste come foglie di un albero binario; ad ogni slot di trasmissione, tutte quelle che devono trasmettere, trasmettono. Se si verifica una collisione vengono creati due slot uno per il sottoalbero destro e uno per quello sinistro; se si verifica una nuova collisione allora si creano due ulteriori slot, ripetendo lo stesso procedimento finchè tutte non riescono a trasmettere.

Nel primo intervallo di contesa che segue una trasmissione senza collisioni, l'intervallo 0, tutte le stazioni possono tentare di acquisire il controllo del canale. In caso di collisione durante l'algoritmo analizza l'intera struttura ad albero partendo dal basso per individuare tutte le stazioni pronte. Ogni

intervallo di bit è associato a qualche particolare nodo dell'albero e, in caso di collisioni, la ricerca continua in modo ricorsivo con i figli posti a sinistra del nodo. Se un intervallo di bit è libero oppure se una sola stazione trasmette durante quel periodo la ricerca del suo nodo può interrompersi perché tutte le stazioni pronte sono state individuate.

Stazione esposta e stazione nascosta; MACA
Ogni apparato trasmittente è caratterizzato da una portata, dipendente dalla potenza trasmissiva impiegata, che è la distanza massima alla quale il segnale emesso può essere rilevato. Tutte le apparecchiature entro la portata di un apparato ricevono il segnale trasmesso da tale apparato, mentre quelle al di fuori di tale portata non lo ricevono.
Problema della Stazione nascosta:
Supponiamo ora che la stazione A voglia trasmettere a B. Se C controlla la presenza di portante sul mezzo di trasmissione (CSMA!), non potrà rilevare A, perché si trova al di fuori della sua portata; di conseguenza C pensa erroneamente di poter trasmettere a B. Se inizia a trasmettere, C interferisce con B distruggendo il frame inviato da A. Il problema di una stazione che non è in grado di rilevare i potenziali concorrenti sul mezzo di trasmissione a causa della distanza eccessiva è chiamato problema della stazione nascosta.
Problema della Stazione esposta:
Consideriamo ora la situazione inversa: B trasmette ad A. Se C controlla la presenza di portante sul mezzo di trasmissione, rileva una trasmissione in atto ed erroneamente pensa di non poter inviare dati a D; in realtà la trasmissione causerebbe una cattiva ricezione solo nella zona compresa tra B e C, che non ospita nessuno dei ricevitori designati. La situazione genera quello che è chiamato problema della stazione esposta.
Una semplice soluzione è data dal protocollo MACA (Multiple Access with Collision Avoidance). Questo protocollo, sfrutta l'idea che chi deve trasmettere renda il suo spazio locale "conosciuto" anche agli altri, tramite frame RTS (request to send) e CTS (clear to send) di 30 byte. In caso di collisione un trasmettitore che non ha avuto successo, ovvero che non riceve il CTS nel tempo previsto, aspetta per un intervallo di tempo casuale prima di ripetere l'operazione.
Nel MACAW (MACA for Wireless) sono stati risolti alcuni problemi, come il fatto che in assenza di ACK nello strato data link i frame perduti non sono trasmessi fino a che lo strato di trasporto non rileva la loro assenza, introducendo un ACK dopo ogni frame dati trasmesso con successo e introducendo la capacità di rilevamento della portante in modo da impedire alle stazioni di trasmettere un frame RTS quando una stazione nelle vicinanze ne sta inviando un altro alla stessa destinazione. Inoltre è stato deciso di eseguire il controllo di backoff separatamente per ogni flusso dati invece che per ogni stazione ed è stato aggiunto un meccanismo che consente alle stazioni di scambiare informazioni sulla congestione.

Binary exponential backoff
È un algoritmo che gestisce l'attesa casuale dopo una collisione. Il tempo di attesa viene scelto dinamicamente e casualmente: dopo una collisione il tempo è diviso in intervalli la cui lunghezza è uguale al tempo di percorrenza andata e ritorno sul mezzo di trasmissione; il tempo di attesa prima delle prossima ritrasmissione dipende da quante collisioni sono già avvenute. Il limite è fino a 10 collisioni, altrimenti si rinuncia. La crescita esponenziale dell'intervallo garantisce un buon adattamento in caso di molte stazioni perché se il tempo fosse piccolo avremmo molte collisioni, mentre se fosse ampio avremmo un tempo di attesa elevato.
È un protocollo usato da MACAW.

Codifica Manchester
Determina senza ambiguità il punto iniziale finale e centrale di ogni bit senza impulsi esterni. La codifica divide il periodo in due porzioni: l'1 binario è inviato scegliendo il livello di tensione alto durante il primo intervallo e un livello basso durante il secondo, mentre lo schema contrario è utilizzato per trasmettere lo 0 binario. Questa tecnica aiuta la sincronizzazione trasmettitore/ricevitore, lo svantaggio è che occupa il doppio della banda della codifica elementare, perché gli impulsi sono larghi la metà
Variante: codifica Manchester differenziale, meno soggetta a rumori; si basa sul cambio di transizione tra intervalli, ovvero se c'è uno 0 avviene un cambio di transizione altrimenti no.
Tutti i sistemi Ethernet usano la codifica Manchester.

Bluetooth
Progetto volto alla realizzazione di standard wireless che permette il collegamento tra dispositivi di calcolo, accessori e comunicazioni mediante wireless a basso costo, bassa potenza e portanza ridotta (massimo 10 metri).
L'unità di base è il piconet, composto da un noto master e diversi nodi slave (7) situati in un raggio di 10 metri; più piconet possono connettersi formando uno scatternet.
La comunicazione avviene partendo dal nodo master mentre i nodi slave possono solo rispondere al master, inoltre esso decide quale slave deve rispondere, tramite TDM.
Per comunicare il nodo master definisce gli intervalli di trasmissione ed il metodo TDM, il master trasmette negli intervalli pari mentre gli slave rispondono negli intervalli dispari. I frame possono occupare 1,3,5 intervalli di tempo; ogni frame è trasmesso attraverso un canale logico chiamato link, che stabilisce la connessione tramite master e slave. Tra questi link ricordiamo ACL usato per i dati a commutazione di pacchetto, dove i dati sono trasmessi senza garanzia di arrivo, e SCO usato per i dati in tempo reale. I frame inviati attraverso questi canali non vengono mai ritrasmessi bensì avviene la correzione degli errori.

Ethernet, frame e tipologie
IEEE 802.3
È lo standard delle reti locali metropolitane. In base al cablaggio esistono diversi tipo di ethernet:
- 10Base5: (thick Ethernet) cavo coassiale grosso, connessioni effettuate con spine a vampiro 10 Mbps, trasmissione in banda base. supporta segmenti lunghi fino a 500 m. Ai cavi è fissato saldamente un tranceiver utile per rilevare le collisioni e per mantenere un stabile contatto con il nucleo del cavo. Un cavo tranceiver collega il trasmettitore all'interfaccia installata nel pc ed `e costituito di 5 doppini. 1 per i dati in ingresso e 1 per quelli in uscita, 2 per il controllo IN/OUT e 1 per l'alimentazione.
- 10Base2: (thin Ethernet) cavo coassiale più sottili. I connettori BNC standard, che formano giunzioni a T, sono più affidabili e facili da utilizzare. più economico e semplice da installare, ogni segmento lungo al massimo 185 m, supporta non più di 30 macchine. Per trovare guasti in questi mezzi è usata la tecnica TDR (Time Domain Reflectory) che sostanzialmente misura il ritardo dell'eco dell'impulso immesso nel cavo.
- 10Base-T: ogni stazione `e collegata direttamente a più hub con doppini telefonici.
- 10Base-F: usa fibre ottiche. E' un alternativa costosa ma buona per l'immunità alle interferenze consentendo di collegare edifici/hub molto distanti

Fast Ethernet IEEE 802.3u
Nata per la necessità di velocizzare le reti è basata sullo standard 802.3 preesistente ottimizzata, mantenendo la retro-compatibilità.
- 100Base-T4: utilizza una velocità di segnale di 25 MHz con cavo di categoria 3. 4 doppini per raggiungere la banda necessaria. Uno dei 4 doppini trasmette sempre all'hub e no riceve e gli altri sono commutabili. Si abbandona la codifica Manchester. Grazie a 3 doppini dedicati alla trasmissione si invia un segnale ternario a ogni ciclo di clock avendo valori tra 0 e 2. In questo modo si inviano 4bit di informazione a ogni ciclo arrivando a 100Mbps con canale inverso a 33Mbps (schema 8B/6T). Poco elegante ma funzionante con i cavi esistenti. Lunghezza fino a 100 m.
- 100Base-TX: utilizza una velocità di segnale di 125 MHz con cavo di categoria 5. Per raggiungere la banda necessaria è richiesto l'uso di soli 2 doppini, uno verso e uno dall'hub. Anche qui `e abbandonata la codifica binaria e si utilizza uno schema chiamato 4B/5B: ogni 5 cicli di clock si hanno 32 combinazioni, le prime sedici trasmettono i 4 gruppi di bit e i rimanenti per funzioni di controllo. Lunghezza fino a 100 m.
- 100Base-FX: utilizza fibre ottiche multimodali raggiungendo in full duplex una velocità di 100 Mbps. Lunghezza fino a 2 Km.

Gigabit Ethernet 802.3z
L'idea principale è di rendere Ethernet 10 volte più veloce mantenendo la retro-compatibilità. Tutte le configurazioni Gigabit sono punto-punto, supportando 2 modalità: full duplex se collegati a switch (che offre anche un buffer di memorizzazione) e half duplex se collegati ad hub. In full duplex non esistono più le collisioni così si abbandona l'uso del CSMA/CD, in half duplex invece viene utilizzato. Siccome per raggiungere velocità elevate si doveva pero` ridurre la distanza notevolmente (distanza massima 25 m!!) furono introdotte alcune funzionalità chiamate carrier extension e frame bursting.

Carrier extensio: Essenzialmente dice all'hardware di aggiungere byte al pacchetto fino a raggiungere i 512 byte. Questo aumenta l'efficienza di circa il 9%. Siccome è tutto sull'hardware non c'è bisogno di modifica al software esistente.
Frame bursting: Concatena più frame in in una singola trasmissione riempendoli per raggiungere i 512 byte se necessario. Se i dati sono minori di 512 byte vengono aggiunti per riempire direttamente dall'hw. Se molti frame sono in attesa questo schema è più efficiente del precedente. Queste 2 funzionalità estendono la rete per un raggio di circa 200 m.

CAPITOLO 5

STRATO NETWORK

ALGORITMI DI ROUTING

Flooding

Algoritmo di routing statico che consiste nell'inviare ogni pacchetto su tutte le linee eccetto quella da cui è arrivato. Ha come svantaggio il generare un numero infinito di pacchetti. Ci sono delle tecniche per limitare il traffico generato:

- Inserire in ogni pacchetto un contatore che viene decrementato ad ogni hop; quando il contatore arriva a 0 il pacchetto viene scartato; si mette come valore iniziale il valore della subnet;
- Inserire la coppia source ID- sequence number in ogni pacchetto, così ogni router esamina tali info e ne tiene traccia; quando vede per la seconda volta la stessa coppia scarta il pacchetto;
- Selective flooding: i pacchetti vengono duplicati solo sulle linee che vanno nella giusta direzione

Il flooding non è utilizzabile come algoritmo di routing, però è utile in campo militare, è utile per l'aggiornamento contemporaneo di info distribuite, è utile come strumento di paragone per altri algoritmi in quanto trova sempre il cammino minimo.

Distance vector routing

È un algoritmo di routing dinamico che tiene conto del carico della rete. Ogni router ha una tabella di routing che contiene info su quanto veloce è la connessione ad un altro router e qual è la via migliore per raggiungerlo. Ogni router chiede ai suoi vicini la loro tabella ad intervalli regolari; usa poi le loro tabelle ed il tempo che c'è voluto per ottenerle per costruire la propria tabella selezionando i percorsi migliori.
Vantaggi: veloce a recepire info.
Svantaggi: non tiene conto della capcità della banda, ha il problema del conteggio all'infinito ed è soggetto al seesaw.
Per conteggio all'infinito si intende che quando una stazione C vuole trasmettere ad A perché è in linea, se il pacchetto arriva a B e A esce dalla rete, B non ha il collegamento diretto con A, quindi in base alla tabella di C sa che quel router può arrivare ad A, e così B e C si passano il pacchetto all'infinito. Di fatto i router non conoscono la topologia della rete.
Il seesaw vuol dire altalena, avviene quando, date due linee una occupata e una libera, tutti gli host vanno verso la linee libera per spedire; questa si occupa, e l'altra si libera, quindi gli host si spostano sull'altra linea.

Reverse path Forwarding

Algoritmo di routing usato per trasmettere in modalità broadcast. Quando il router riceve un pacchetto broadcast verifica se è giunto attraverso la linea normalmente utilizzata per inviare pacchetti. Se affermativo c'è la probabilità che il pacchetto abbia seguito il percorso migliore e quindi essendo il primo verrà inoltrato sulle altre linee, altrimenti potrebbe trattarsi di un doppione e quindi verrebbe scartato.
Vantaggio: si tratta di un sistema efficiente e facile da implementare, non richiede una lista di destinazioni o una mappa di bit per ogni pacchetto broadcast e non necessita di un meccanismo speciale per l'interruzione del processo.

Link state routing

Algoritmo di routing dinamico basato sullo stato dei collegamenti; è un'alternativa al distance vector routing: mentre il primo si occupa della velocità di connessione tra un router e l'altro, questo algoritmo

si occupa di conoscere la topologia della rete. Se la rete è troppo grande viene divisa in zone e il router ha come obiettivo conoscere la sua zona.
Ogni router tiene sotto controllo lo stato dei collegamenti tra sé e i nuovi vicini immediati misurando il ritardo su ogni linea e distribuisce queste info a tutti gli altri router. Come fa:

- Quando un router si avvia invia un pacchetto HELLO su tutte le linee in uscita; in risposta riceve dai suoi vicini i loro indirizzi;
- Invia pacchetti ECHO per misurare i tempi di arrivo della risposta, allo scopo di calcolare il ritardo sulla linea;
- Si costruisce un pacchetto composto da una tabella dove memorizza il mittente, il numero di sequenza del pacchetto, l'età del pacchetto, la lista dei vicini, i relativi ritardi. Questo pacchetto viene modificato e inviato a intervalli regolari o quando accade una modifica alla topologia della rete.
- Per la distribuzione dei pacchetti si usa il flooding. Tutti i pacchetti sono confermati; per evitare pacchetti vaganti l'età dei suddetti viene decrementata ogni secondo.
- Combinando le informazioni pervenute dagli altri router si costruisce il grafo della subnet.

È un algoritmo poco aperto ai cambiamenti improvvisi. Problema: più è grande la rete più saranno grandi le tabelle di routing e maggiore sarà il tempo di refresh.

ALGORITMI CONTROLLO CONGESTIONE

Choke Bucket

È un algoritmo per il controllo della congestione. Se un router si accorge che c'è congestione può inviare un pacchetto choke packet a chi sta inviando dati per dirgli di rallentare. Quando la sorgente riceve il pacchetto dimezza il flusso di dati e ignora i successivi choke per un tempo prefissato, in quanto tipicamente ne arrivano molti in sequenza. Trascorso il tempo prefissato, l'host si rimette in attesa di altri choke packet. Se ne arrivano altri riduce ancora il flusso, altrimenti lo incrementa poco per volta per evitare la congestione.
Problema: se la rete è grande la richiesta può metterci troppo ad arrivare; la soluzione è il token hop-by-hop.

Token hop-by-hop

Algoritmo per il controllo della congestione; se la rete è grande non appena un router invia un choke packet ogni router lungo la strada rallenta subito il ritmo. Questa tecnica è ottima per il router che richiede sollievo ma richiede un buffer più grande per i router lungo il percorso.

Load shedding

Quando nessuno dei precedenti metodi riesce ad eliminare la congestione i router gettano via il carico, ovvero in caso di sovraccarico alcuni pacchetti vengono eliminati secondo due possibili tecniche.
Wine: vino, il vecchio è migliore del nuovo, es trasmissione file;
milk: latte, il nuovo è migliore del vecchio, es pacchetto multimediale.
Un'alternativa è la cooperazione tra trasmettitori: le applicazioni devono contrassegnare il pacchetto secondo loro più importante; se lo fanno i router scartano quelli con importanza minore.

RED

Random early detection. Fa parte degli algoritmi per il controllo della congestione. Consiste nello scartare i pacchetti prima che il buffer sia completamente esaurito. Per stabilire quando è il momento di scartare i pacchetti i router mantengono una soglia nel buffer oltre la quale i pacchetti vengono scartati. Non avviseranno la sorgente, bensì quest'ultima, non ricevendo ACK, li ritrasmetterà, rallentando il flusso.
Nelle reti wireless la maggior parte delle perdite è causata dal rumore presente nel collegamento aereo, quindi questo approccio non può essere utilizzato.

Store and forward
Nella commutazione di pacchetto store and forward un host con un pacchetto da trasmettere invia i dati ai router più vicini attraverso la sua stessa LAN o attraverso un collegamento punto-punto con l'operatore di telecomunicazioni. Qui il pacchetto viene memorizzato fino a quando non è interamente arrivato per verificare il checksum, quindi viene inoltrato al router successivo fino all'host di destinazione.

Quality of service.
In una rete orientata alla connessione tutti i pacchetti che appartengono ad un flusso seguono lo stesso percorso, mentre nelle reti senza connessione possono prendere percorsi differenti.
Le esigenze di ogni flusso possono essere caratterizzate da quattro parametri: affidabilità, ritardo, jitter, banda.
Affidabilità: nel trasferimento dei file nessun bit può essere emesso in modo scorretto; questo obiettivo è raggiunto creando il checksum di ogni pacchetto e verificandolo alla destinazione. Il pacchetto in transito che arriva danneggiato non riceve ACK e sarà di conseguenza ritrasmesso. Audio e video possono tollerare errori quindi nessun checksum viene elaborato.
Ritardo: se tutti i pacchetti subiscono un ritardo uniforme di pochi secondi non accade nulla di male, mentre applicazioni in tempo reale hanno requisiti severi.
Jitter: Un jitter è la variazione nel tempo di arrivo di un pacchetto. Il jitter può essere delimitato calcolando il tempo di transito atteso per ogni salto lungo il percorso. Quando il pacchetto raggiunge il router questo controlla di quanto il pacchetto è in anticipo o in ritardo rispetto alla sua programmazione e questa informazione viene memorizzata nel pacchetto e aggiornata ad ogni salto. Se è in anticipo il pacchetto è trattenuto quanto basta per rientrare nella pianificazione, mentre se è in ritardo il router tenta di trasmetterlo il prima possibile. In alcune applicazioni, come quelle basate sui video on demand, il jitter può essere eliminato memorizzando i dati in un buffer del computer ricevente mentre in altre, come quelle che richiedono interazione in tempo reale, il ritardo inerente alla memorizzazione non è accettabile.
Banda: la posta elettronica non richiede molta banda, i video si.
Tecniche per ottenere una buona Qos: sovradimensionamento, uso del buffer, traffic shaping, choke packet, token hop by hop, load shedding, leaky bucket.
Sovradimensionamento: fornire tanta capacità al router in termini di spazio buffer e banda, per far transitare facilmente i pacchetti. È una soluzione costosa
Utilizzo del buffer: elimina lo jitter, utile soprattutto in caso di audio e video on demand.
Traffic shaping: un output non uniforme è frequente quando il server deve gestire più flussi contemporaneamente. Rendendo uniforme le transazioni del server la qualità del servizio migliorerebbe. Per fare questo quando una connessione viene impostata l'utente e la sottorete si mettono d'accordo su un particolare modello di traffico (service level agreement) e fintanto che il cliente si attiene alla sua parte dell'accordo e invia solo i pacchetti secondo il contratto concordato, l'operatore di telecomunicazioni promette di consegnare i dati in modo tempestivo. Il traffic shaping riduce la congestione regolando la velocità media di trasmissione e aiuta così l'operatore a tener fede alle sue promesse. La supervisione del flusso di traffico è chiamata traffic policing.

Leaky bucket
È una tecnica per migliorare le QoS attraverso il controllo della congestione. Analogia del secchio riempito da rubinetto aperto e con foro sul fondo che fa scorrere l'acqua a ritmo costante; se viene immessa troppa acqua questa esce dal secchio.
Ogni host si interfaccia alla rete con un leaky bucket, ovvero un bucket sottoforma di coda. Quando arriva un pacchetto a coda piene viene subito scartato. L'host trasmette un pacchetto ad ogni ciclo di clock, e ogni pacchetto ha dimensione costante. Il ciclo di clock trasforma un flusso irregolare in flusso regolare. Quando si usano pacchetti a dimensione variabile è meglio consentire un numero fisso di byte per ogni ciclo di clock invece che limitarsi ad un unico pacchetto.
Vantaggio: data rate sempre costante, quando il traffico è sostenuto si aumenta il data rate, non segue la variabilità del traffico, è facile da implementare.

Token Bucket
Tecnica per migliorare le QoS attraverso il controllo della congestione; è un secchio a gettoni (token). Il leaky bucket contiene dei token generati da un clock; perché un pacchetto possa essere trasmesso deve prendere e distruggere un token. Se i token finiscono i pacchetti devono attendere la nuova

generazione. Si accumula credito trasmissivo con un certo data rate fino al massimo consentito nei momenti in cui non si trasmette nulla. Quando c'è da trasmettere invece si usa tutto il credito disponibile.
I token si creano ogni msec fino a che il loro numero non arriva a un certo tot prefissato che corrisponde all'aver riempito il secchio di token.
Il leaky bucket non permette agli host inattivi di risparmiare permessi in modo da inviare grandi raffiche di dati, il token bucket consente di risparmiare fino a riempire la dimensione massima del secchio; inoltre con i leaky bucket i pacchetti non vengono mai scartati perché il secchio contiene token e non pacchetti.

PROTOCOLLO IP
Regge tutto internet in quanto è pensato per la comunicazione tra reti: lo strato trasporto prende i flussi di dati e li divide in datagrammi, ognuno di questi è trasmesso attraverso internet e può essere frammentato in unità più piccole.
Datagramma/header:
- version: indica la versione del protocollo (IPv4, IPv6)
- IHL: lunghezza intestazione, parola da 32 bit, max 60 byte
- Type of service: tipo di servizio usato (Qos)
- Total lenght: tiene conto di tutto il contenuto del datagramma
- Identification: indica il datagramma di appartenenza del flusso
- DF/MF: don't fragments/more fragments
- Time to live: limite di vita del pacchetto
- Protocol: quale processo di trasporto attende quei dati
- Header checksum: verifica l'header
- Source address: indirizzo sorgente (32 bit)
- Destination address: indirizzo destinatario (32 bit)
- Option: campi opzionali

L'indirizzo IP si riferisce ad una scheda di rete, ogni host e router hanno un indirizzo IP che codifica il suo indirizzo di rete e il suo numero di host. Questa combinazione è unica e, per evitare conflitti, i numeri di rete sono gestiti da un ente no profit chiamato ICANN. Gli indirizzi sono lunghi 32 bit, l'indirizzamento avviene per classi di tipo A-B-C…..-E.
IPv6 è una nuova versione di IP, successore di IPv4, ha lo scopo di aumentare il numero degli indirizzi ormai quasi esauriti, ottenere maggiore efficienza nei router con tavole più piccole e routing più veloce, supporta meglio il traffico real time, offre maggiore sicurezza ai dati riservati. Le principali differenze sono gli indirizzi che sono di 16 byte anziché 4, l'header ha 7 campi contro 13 di IPv4, e IPv6 non ha il campo checksum, ha funzioni di autentificazione basate sulla crittografia, gestisce la qualità del servizio offerto tramite campo flow label che consente di istruire delle pseudo connessioni.

Header di IPv6:
- Version
- Traffic class
- Flow label
- Payload lenght
- Next header
- Hop limit
- Source address
- Destination address

CIDR
Classes interdomain routing. È un metodo di assegnazione degli indirizzi che non rispetta i limiti delle classi, ma che permette di assegnare indirizzi IP rimanenti in blocchi di dimensione variabili.
Quando una rete diventa troppo vasta, l'assegnazione di indirizzi IP tra sottoreti è complicata, quindi si ricorre ad una subnet masck di 32 bit che identifica il punto di demarcazione tra l'indirizzo della rete e quello dell'host. Gli indirizzi rimanenti vengono assegnati in base alle necessità, senza tenere conto delle classi, ma è un problema quando si vuole inoltrare. La soluzione è una voce aggregata di tipo /N dove N sta per il numero di bit della rete.
Quando arriva un pacchetto indirizzato ad una rete divisa in sottoreti il CIDR prende il pacchetto e lo mette in AND con la mask delle sottoreti; si assegna il pacchetto alla rete che coincide con più bit. Se

un router non ha linee di output specifiche e separate verso una zona può utilizzare voci aggregate per diminuire la dimensione della tabella di routing.

NAT
Network address translation, è una soluzione che si è dovuta adottare fino al completo utilizzo di IPv6 per risolvere il problema dell'esaurimento di indirizzi IP.
Consiste nel simulare una rete in un unico indirizzo IP, es nel caso delle aziende, per cui una azienda ha un solo indirizzo IP per il traffico internet. Dentro un'azienda ogni macchina ha un unico indirizzo espresso nella forma 10.x.y.z, ma quando un pacchetto lascia l'azienda passa attraverso un dispositivo NAT che converte l'indirizzo IP interno nel vero indirizzo IP assegnato all'azienda..
Solitamente questo dispositivo è abbinato ad un firewall e a volte è integrato nei router.
Il problema di questo protocollo è quando si riceve la risposta, in quando l'indirizzo è un generico aziendale. La soluzione viene dal fatto che quasi tutti i pacchetti IP trasportano anche carichi TCP/UDP, i quali riportano la porta sorgente e destinazione del pacchetto. Quando il mittente riceve risposta dal destinatario, si risale proprio alla porta sorgente.

ARP
Address resolution protocol; serve per conoscere l'indirizzo Ethernet di un host, dato il suo indirizzo IP.
Quando un host vuole sapere a che altro host corrisponde un dato indirizzo IP, lo chiede in broadcast a tutte le stazioni e risponderà solo quella con l'indirizzo corrispondente, inserendo nella risposta il suo indirizzo data link (ethernet).
Alcune migliorie sono che quando si riceve la risposta l'host mantenga in memoria l'indirizzo nel caso debba ricontattare lo stesso computer, oppure l'host mittente può includere nella domanda la propria associazione IP-ethernet nel pacchetto ARP, che viene poi inserito nella cache del destinatario; oppure ancora si potrebbe fare in modo che ogni computer/host invii in broadcast la propria associazione durante l'accensione.
Tecnica proxy ARP: i router vengono configurati per rispondere alle richieste ARP dalla rete dell'host sorgente, così tutto il traffico diretto verso quella rete passa per il router che ha mappato IP e indirizzo Ethernet.

DHCP
Dynamic host configuration protocol. Permette l'assegnazione manuale o automatica degli indirizzi IP. Si basa sull'utilizzo di un server speciale, DHCP server, che assegna gli indirizzi agli host che ne richiedono uno, anche nei casi in cui questo server non si trovi sulla stessa LAN del richiedente. Poiché il server DHCP potrebbe non essere raggiunto dalle trasmissioni broadcast è necessario installare per ogni LAN un agente di inoltro chiamato DHCP relay agent.
Per conoscere un proprio indirizzo IP una macchina appena accesa invia in modalità broadcast un pacchetto chiamato DHCP discover; l'agente di inoltre presente su quella LAN intercetta il pacchetto e lo invia in modalità unicast al server DHCP.
Problema: se un host abbandona la rete e non restituisce l'indirizzo, questo andrà perso, quindi dopo un po' ci sarebbero molti indirizzi inutilizzati e non più disponibili. Per impedire ciò si può assegnare gli indirizzi in leasing, ovvero per un certo tot di tempo. Poco prima dello scadere di questo leasing l'host chiede il rinnovo dell'indirizzo; se non lo rinnova non può riutilizzare quell'indirizzo una volta scaduto.

CAPITOLO 6

STRATO TRASPORTO

UDP

È un protocollo di trasporto senza connessione, in particolare permette di inviare datagrammi IP incapsulati senza dover stabilire una connessione. Essenzialmente UDP equivale ad IP con l'aggiunta di un'intestazione di 8 byte per lo strato trasporto. L'UDP aggiunge la porta di chi manda e la porta di chi riceve e fa il controllo tramite checksum.
L'intestazione UDP è formata da:
- Source port, 2 byte;
- Destination port; 2 byte;
- UDP lenght, 8 byte, che include intestazione e dati;
- UDP checksum, 8 byte, è facoltativo e contiene 0 se non elaborato;

Un'applicazione che fa uso dell'UDP è il DNS e il NAT.

TCP
Trasmission control protocol, è un proto collo orientato alla connessione. È stato progettato per garantire solide prestazioni anche in presenza di molti errori di vario genere. Accetta dai processi locali il flusso di dati degli utenti e li suddivide in pezzi di dimensione non superiore ai 64 kb per poi inviarli in un datagramma IP autonomo.
Sia il ricevete sia il mittente devono creare dei socket (punti finali) i quali possiedono un indirizzo IP (una porta); un singolo socket supporta più connessioni contemporaneamente. Per ottenere un servizio TCP si deve stabilire esplicitamente una connessione tra un socket sulla macchina d'invio e uno sulla macchina ricevente.
Le entità TCP si scambiano dati sottoforma di segmenti, dove ogni segmento consiste in un'intestazione di 20 byte seguita dai dati; ogni segmento può essere al massimo di 65 mila e rotti byte, inoltre la rete ha un MTU= maximun transfer unit e ogni segmento deve essere contenuto in questo. Il protocollo di base usato lo sliding window.
Caratteristiche del TCP: tutte le connessioni sono di tipo full duplex punto-punto, non supportano il broadcasting o il multicasting. Una connessione TCP è un flusso di byte e non di messaggi, quindi i confini dei messaggi non vengono conservati. Di conseguenza alcune problematiche sono che i segmenti possono arrivare in ordine sbagliato in quando durante il transito alcuni segmenti possono essere ritardati così tanto che il mittente va in timeout ed è costretto a ripetere la trasmissione.
Intestazione TCP:
- Source port
- Destination port
- Sequence number
- Numero di ACK
- TCP header lenght: quante parole di 32 bit sono contenute nell'intestazione
- URG: flag impostato a 1 quando si usa l'urgent pointer
- ACK: flag impostato a 1 se l'ACK numer è valido; 0 se non contiene ACK
- PSH: flag impostato a 1 se c'è la presenza di dati push
- RST: flag impostato a 1 se si vuole resettare la connessione a causa di errori
- SYN: flag usato per stabilire la connessione
- FIN: flag usato per rilasciare la connessione
- Windows size: indica le dimensioni della finestra
- Checksum: contiene la somma di controllo dell'intestazione, dati e pseudo intestazione dati
- Urgent pointer: indica l'inizio di dati urgenti
- Options: aggiunge info extra
- Dati: dati veri e propri

DNS
Poiché su internet ogni risorsa è contrassegnata con un indirizzo IP numerico, si è creato un metodo che associasse questo indirizzo IP a un nome logico, ovvero una stringa di caratteri. Il DNS si occupa di accoppiare indirizzi e nomi ricorrendo ad uno schema gerarchico di denominazione chiamato dominio, un database distribuito che implementasse lo schema e un protocollo per il mantenimento e la distribuzione delle info sulle corrispondenze. I domini hanno caratteristiche gerarchiche, gli indirizzi sono di tipo Nome.com; vi sono domini di primo livello che coprono molti host, oppure quelli di secondo livello. Per ottenerli è necessario contattare un registrator il quale controlla la disponibilità di quel nome nel dominio di primo livello; per ottenerlo si paga una tariffa annuale. Se si vuole creare un nuovo dominio è necessaria l'autorizzazione del dominio in cui sarà incluso.

A ogni dominio può essere associato un insieme di resource records; per un semplice host il recordi di risorse è l'indirizzo IP, quindi il DNS associa il nome dei domini ai record. Un record delle risorse è una quintupla di tipo NomeDominio TempoDiVita Classe Tipo Valore.
Quando un'applicazione deve collegarsi ad una risorsa di cui non conosce il nome logico invia una richiesta al DNS server locale; se conosce la risposta la invia altrimenti chiede al DNS server di livello superiore, è un'interrogazione ricorsiva. Quando l'applicazione riceve la risposta crea una connessione TCP con la destinazione usando l'indirizzo IP ricevuto. Il dominio ha la responsabilità di fornire il DNS rispondendo alle interrogazioni riguardanti tutti gli host contenuti nel dominio stesso.

CAPITOLO 7

SICUREZZA

One time pad
è un algoritmo crittograficamente sicuro Si usa una chiave lunga quanto il messaggio da inviare e si fa lo XOR (addizione modulare) col messaggio. Questo serve ad unire il "caos" della chiave all' "ordine" del messaggio
problemi:

- Poco Pratico: "one-time", si pu`o usare una volta solo, e la stessa password non pu`o essere usata per mandare messaggi pi`u lunghi, altrimenti si torna ad usare uno dei metodi attaccabili (non c'`e abbastanza "caos" da "distrubuire" sul testo).
- La sequenza deve essere scelta bene (deve essere caotica), non vi deve essere ordine (neanche battere a caso sulla tastiera non`e completamente casuale, dato che l'uomo tende a creare dei pattern e ripetizioni ricorrenti dopo un po')

CIFRARI

Cifrario a sostituzione
È uno dei cifrari più semplici, attribuito a Cesare.
Si basa sul principio di sostituzione di lettere con altre, spostando l'alfabeto di un numero K di caratteri, dove K diventa la chiave. Questi cifrari conservano l'ordine dei simboli di testo in chiaro, limitandosi a mascherare la loro apparenza. Un miglioramento potrebbe essere far si che ognuno dei simboli dell'alfabeto corrisponda ad altre lettere, ottenendo quindi una sostituzione monoalfabetica. Per risolvere l'enigma, ovvero decriptare, si usa un approccio statistico chiamato frequency analysis che si basa sul fatto che le singole lettere in ogni lingua hanno una certa frequenza. Un altro approccio è quello di provare con una parola che ha una buona possibilità di essere presente in quel contesto, quindi ricavare tutte le altre.

Cifrario a trasposizione
Vengono riordinate le lettere, ma non vengono mascherate. Lo scopo della chiave è quello di riordinare le colonne. Per forzare un cifrario di questo tipo il criptoanalista per prima cosa deve sapere che si tratta di un cifrario a trasposizione. Il passo successivo consiste nel fare ipotesi sul numero di colonne, mentre il passo conclusivo consiste nel trovare l'ordine delle colonne.

Cipher block
È un algoritmo a chiave simmetrica, prende n bit dal testo in chiaro e li trasforma usando una chiave a n bit; agiscono su blocchi di bit, sono composti da P-box (box di permutazione), e S-box (box di sostituzione); collegando questi due dispositivi a cascata di ottiene il cifrario prodotto. Possono essere realizzati via software o via hardware; un esempio di cifrario a blocchi è il DES.

Cipher block chaining
È un modo per evitare che vengano invertite parti di testo anche senza decifrare. Si basa sull'idea che ogni blocco abbia un legame con il successivo in modo che un loro spostamento faccia perdere significato a tutto. Il metodo in questione parte da un primo blocco, fa uno XOR con un blocco casuale detto IV (inizialization vector= vettore inizializzazione) che è trasmesso assieme al testo cifrato, e poi ogni blocco di testo successivo viene messo in XOR col precedente.
Svantaggio: per decifrare è necessario avere tutto il blocco di 64 bit già scaricato, e poi si può procedere.

Stream cipher
Algoritmo di cifratura simmetrica; cifra un IV con una chiave crittografica per ottenere un blocco in uscita; il blocco viene cifrato per ottenere un secondo blocco in uscita, e si procede così con il terzo ecc, ma in questo caso si riutilizza il vettore.
La sequenza di blocchi in uscita è chiamata keystream e viene usata come blocco monouso= one time pad e applicata in XOR sul testo in chiaro per ottenere quello cifrato. Il keystream è indipendente dai dati e può essere calcolato in anticipo perché immune da errori di trasmissione.
Una cosa essenziale nella modalità stream cipher è non usare mai la stessa coppia di chiave-IV perché espone il testo cifrato ad attacchi di tipo keystream riutilizzato.
Pro: si può precalcolare l'encrypting usando la chiave, rendendo la decodifica parallelizzabile; contro: per parallelizzare la decodifica devo precalcolare l'encrypting, e quel processo non è parallelizzabile.
Brevemente: si cifra il IV con chiave crittografica, e poi si usa il risultato per cifrare il testo facendo uno XOR; il risultato viene ulteriormente cifrato e così via.

ECB
Electronic Code Book. Questo metodo consiste nel prendere il testo in chiaro e suddividerlo in blocchi di 8 byte (64 bit) che vengono poi cifrati uno dopo l'altro usando la stessa chiave. L'ultimo pezzo di testo in chiaro, se necessario, viene riempito fino a fargli raggiungere la lunghezza di 64 bit. Per evitare attacchi i blocchi cifrati possono essere collegati in diverse maniere.

ALGORITMI A CHIAVE SIMMETRICA

DES e Tripli-DES
Il DES è un algoritmo a chiave simmetrica e cifrario a blocchi. Il testo in chiaro viene cifrato in blocchi da 64 bit che generano 64 bit di test cifrato. L'algoritmo funziona con una chiave da 56 bit e ha 19 stadi distinti. Nel 1° e 19° stadio si effettua una trasposizione dei 64 bit del testo in chiaro, nel 18° stadio (penultimo) si scambiano i 32 bit a destra con i 32 bit a sinistra, mentre i 16 bit in mezzo sono parametrizzati con la funzione della chiave. Ogni stadio intermedio prende due ingressi da 32 bit e produce due uscite da 64; l'output di sinistra è una copia di quello di destra, mentre quello di destra è un XOR bit per bit dell'output di sinistra con una funzione dell'input di destra e della chiave per questo stadio. Per rendere più sicuro DES si usa la tecnica dello sbiancamento, ovvero si cifra il testo in chiaro preliminarmente tramite due XOR tra blocchi di 64 bit del testo in chiaro con 2 chiavi a 64 bit.
Il triplo DES è diviso in 3 stadi:
- DES in criptazione con chiave K1 (112 bit)
- DES in decriptazione con chiave K2 (112 bit)
- Criptazione con K1

Per una questione di retrocompatibilità con DES, si usano due chiavi uguali

AES
AES (Advanced Encryption Standard) Nel gennaio 1997 NIST (National Institute of Standards and Tecnology) invitò i ricercatori di tutto il mondo ad inviare proposte per un nuovo standard che avrebbe preso il nome di AES. Le regole del concorso erano: 1) l'algoritmo doveva essere un cifrario simmetrico a blocchi, 2) la struttura doveva essere interamente pubblica, 3) doveva supportare chiavi di lunghezza di 128, 192 e 256 bit, 4) dovevano essere possibili implementazioni software e hardware

e 5) l'algoritmo doveva essere pubblico o rilasciato senza vincoli di alcun tipo. Nel novembre 2001 Rijndael divenne uno standard del governo degli Stati Uniti.

Blowfish
Un altro block Cipher inventato nel 1993 da Bruce Schneier. è open source ed ha avuto (ed ha ancora) successo. `E considerato sicuro (non è ancora stato craccato) Usa blocchi da 64 bit e chiavi che vanno da 32 a 448 bits, però è più lento di AES

ALGORITMI A CHIAVE PUBBLICA

Si basano su questi presupposti: sorgente e destinatario hanno 2 chiavi diverse (K, J) e usano rispettivamente E e D per criptare e decrittare. Vengono resi pubblici K,EK eEJ, mentre sono segreti DK,DJ. Gli algoritmi devono soddisfare queste proprietà:
- D(E(P)) = P
- Deve essere difficile ricavare D da E
- E non può essere forzato con un attacco di tipo 'testo in chiaro a scelta'.

RSA
Richiede chiavi di almeno 1024 bit, per questo è abbastanza lento e rappresenta il suo maggior svantaggio. L'algoritmo funziona così:
1. Si scelgono 2 numeri primi molto grandi p e q (almeno 1024 bit)
2. Si calcoli n = pq e z = (p-1)(q-1)
3. Scegliamo un numero coprimo con z, detto d
4. Troviamo e tale che ed = 1 mod z

Dividiamo in blocchi il testo in chiaro in modo che ogni messaggio P sia tale che $0 \leq P < n$. Per farlo basta raggruppare il testo in chiaro in blocchi di k bit con k tale che sia il massimo intero per cui vale $2k < n$. Ora per cifrare il messaggio P calcoliamo C = Pe(modn) mentre per decifrare c si calcola P = Cd(modn). Questo vale perch´e P = (xemodn)dmodn = Pedmodn.

PROTOCOLLI DI AUTENTIFICAZIONE

Reflection Attack
Un attacco per riflessione funziona cos`ı: indichiamo con T l'impostore. T finge di essere A e invia un numero casuale RT a B che risponde con il suo numero casuale RB e cripta RT con la chiave comune. Ora T dovrebbe rispondere con criptando il numero casuale ma non conosce la chiave. Per riuscire a ricavarla T puo` riaprire una nuova sessione e mandare come numero casuale RB che B gli ritorna criptato. Ora T ha quello che voleva e puo` completare la prima sessione. Questo attacco riesce a sorprendere anche l'autenticazione a 2 vie non ridotta: se A vuole dialogare con B invia la propria identita` e T la intercetta. T fingendo di essere B apre una nuova sessione mandando la sua identita` e A risponde con il suo numero casuale RA. Ora T pu`o continuare la sessione 1 inviando l'RA appena ricevuto al quale A risponde con KAB(RA) proprio quello che serve a T per continuare la sessione 2. Ora T pu`o abbandonare la sessione 1 e dialogare come se fosse B nella 2 oppure puo` ripetere il procedimento appena descritto e avere cos`ı 2 sessioni autenticate.

Replay Attack
E' una forma di attacco di rete che consiste nell'impossessarsi di una credenziale di autenticazione comunicata da un host ad un altro, e riproporla successivamente simulando l'identita` dell'emittente. In genere l'azione viene compiuta da un attaccante che s'interpone tra i due lati comunicanti. A differenza dell'attacco di tipo man in the middle che opera sempre in tempo reale, il replay attack puo` operare anche in modo asincrono quando la comunicazione originale `e terminata. Si verifica un replay-attack quando Mallory intercetta la comunicazione tra Alice, che si sta autenticando con Bob, e si spaccia, agli occhi di Bob, per Alice. Quando Bob chiede a Mallory (convinto di parlare con Alice)

una chiave d'autenticazione, Mallory pronta invia quella di Alice, instaurando cos`ı la comunicazione. Gli attacchi di tipo replay si evitano con l'uso di token di sessione generati pseudocasualmente: Bob invia ad Alice uno di questi token usa e getta, che Alice utilizza per criptare la propria chiave da inviare a Bob. Bob effettua lo stesso calcolo e controlla che il suo risultato corrisponda con quello di Alice. Un'altra contromisura `e quella di utilizzare una marca temporale e di far s`ı che questa sia inserita nel corpo del messaggio criptato.

Man in the middle attack

E' un attacco nel quale l'attaccante `e in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento sia stato compromesso. L'attaccante deve essere in grado di osservare e intercettare il transito dei messaggi tra le due vittime. Supponiamo che Alice voglia comunicare con Bob, e che Giacomo voglia spiare la conversazione, e se possibile consegnare a Bob dei falsi messaggi. Per iniziare, Alice deve chiedere a Bob la sua chiave pubblica. Se Bob invia la sua chiave pubblica ad Alice, ma Giacomo `e in grado di intercettarla, pu`o iniziare un attacco Man in the middle. Giacomo puo` semplicemente inviare ad Alice una chiave pubblica della quale possiede la corrispondente chiave privata. Alice poi, credendo che questa sia la chiave pubblica di Bob, cifra i suoi messaggi con la chiave di Giacomo ed invia i suoi messaggi cifrati a Bob. Giacomo quindi li intercetta, li decifra, ne tiene una copia per s`e, e li re-cifra (dopo averli alterati se lo desidera) usando la chiave pubblica che Bob aveva originariamente inviato ad Alice. Quando Bob ricevera` il messaggio cifrato, credera` che questo provenga direttamente da Alice. Un simile attacco `e possibile, in teoria, verso qualsiasi messaggio inviato usando tecnologia a chiave pubblica, compresi pacchetti di dati trasportati su reti di computer.