RETI: tutte le 65 domande in un unico testo con risposte!

INTRODUZIONE

Dato che ormai le precedenti “risposte” non erano più sufficienti a coprire la lista delle domande mi son permesso di aggiornare la lista.

Per rispondere alle domande, ho utilizzato gli appunti fatti da Mirko Polato e Fava (che ringrazio), “Reti di Calcolatori” di Andrew A. Tanenbaum, Wikipedia e materiale vario tratto da Google.

Facilmente ci saranno errori, perché l’ho scritto velocemente, ma nel complesso dovrebbero esserci quasi tutte le domande fatte fino ad ora (tranne il WEP di 802.11 e Bluetooth).

Se trovate errori o volete aggiungere delle domande con relativa risposta, modificate pure il documento e riuppatelo.

Fede

Update 20/3/14

In data odierna ho incluso le domande che mancavano, ovvero wep e bluetooth, inoltre ho sistemato le domande per capitolo del libro, in modo da rendere la consultazione più semplice e rapida.

Ho anche corretto alcuni errori della versione precedente degli altri ragazzi che ringrazio! Ho inserito un indice all’inizio, in cui potete trovare le info e tutte le domande presenti nel documento. Come sempre, in presenza di altri errori o altro, correggete e riuppate!

Enjoy it! By SCAP

Update 1/7/14

Aggiungo il testo e le domande del terzo appello, alcune non sono risposte, attenzione!

Domande del terzo appello:
1) QoS
2)Slotted Aloha
3)ECB
4)CIDR

Enjoy it! By SCAP

INDICE GENERALE DOMANDE DEL TESTO

CAPITOLO 2 del testo “Reti di Calcolatori” di Andrew A.Tanenbaum

1. Cosa si intende per serie di Fourier.
2. Bitrate e baudrate
3. Descrivere i vari tipi di cavo e confrontarli
4. Caratteristiche e confronto fra i vari tipi di satellite, GEO, MEO, LEO
5. Che cos'è la modulazione in frequenza?
6. Che cos'è la modulazione delta(delta modulation)?
7. Descrivere in dettaglio il GSM(Global System for Mobile connection)
8. Si descriva la tecnica CDMA(Code Division Multiple Access), possibilmente con esempio
9. Il GPRS: cos'è, difetti e pregi.
10. Handoff
11. FDM, TDM, CDM: algortmi per la selezione della banda
12. QAM e QAM16

CAPITOLO 3

13. Che cos'è il byte stuffing
14. Descrivere il Bit stuffing
15. Numero di bit necessari per riconoscimento(correzione) degli errori di trasmissione
16. Si descriva cos'è il CRC. Si calcoli inoltre il CRC di 10011101 usando il polinomio generatore di x^4+x+1.
17. Descrivere Il protocollo stop and wait, pregi e difetti

18. Cos'è il piggybacking

19. Si descriva la tecnica del Sliding window

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

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

CAPITOLO 4

22. descrivere la differenza fra ALOHA e ALOHA-SLOTTED

23. Si illustri CSMA, indicandone pregi e difetti.

24. basic bitmap

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

26. spiegare che cos'è l'adaptive tree walk protocol.

27. ethernet

28. Codifica Manchester

29. Cos'e' il binary exponential backoff?

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

31. Bluetooth

CAPITOLO 5

32. Si descriva l'algoritmo statico Flooding

33. Descrivere il distance vector routing

34. Linkstate routing

35. choke bucket

36. Token hop-by-hop

37. Load shedding

38. 4red

39. Reverse Path Forwarding

40. Quality of Service

41. Leaky Bucket, pregi e difetti

42. Descrivere il token bucket, pregi e difetti

43. descrivere l'ARP

44. Si descriva DHCP.

45. IPV6

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

CAPITOLO 6

47. Frame ethernet

48. Si descriva l'header UDP.

49. descrivere l'header del TCP/IP e commentarlo;

50. DNS

CAPITOLO 7

51. Cos'è un cifrario a sostituzione e

52. Si descriva l'algoritmo DES e triplo DES

53. Si descriva il cipher block

54. Counter mode cipher

55. Cipher block chaining

56. Stream cipher

57. RSA

58. Si descriva la tecnica di attacco "birthday attack"

59. Sicurezza in 802.11

60. Si descriva la sicurezza del bluetooth

61. La tecnica di attacco reflection attack

62. Il replay attack

63. L’algoritmo Diffie-hellman

64. Man in the middle

65. DNS spoofing

1. Cosa si intende per serie di Fourier

CAPITOLO 2

le informazioni possono essere trasmesse via cavo variando alcune proprietà fisiche, come la tensione e corrente. Fourier condusse alcuni studi ed arrivò alla conclusione che le informazioni trasmesse via cavo potevano essere rappresentata da una funzione f(t). Questa funzione è composta da una serie infinita di somme di seni e coseni, ed è in grado di rappresentare un segnale periodico e regolare. La trasmissione però non è mai perfetta e c'è per forza attenuazione di linea. L'intervallo di frequenze trasmesse senza forte attenuazione è detto banda passante.

Anche in un ipotetico canale perfetto, ovvero senza attenuazioni, la velocità di trasmissione non può essere troppo elevata; la massima velocità è data dall'equazione di Nyquist/Shannon:

Vmax= log2 V bit/sec

2. Bitrate e baudrate

Bitrate: Velocità di trasmissione si indica in bit/s. Il teorema di Nyquist mette in relazione il bitrate con la banda disponibile:

2HLog2V

Con H banda disponibile e V livelli di segnale (simboli) usati

S/N = segnale/rumore SNR = 10Log10(S/N) Massimo bitrate = 2Log2(1+(S/N))

Baudrate: Simboli al secondo un simbolo può valere più bit.

3. Descrivere i vari tipi di cavo e confrontarli

principalmente esistono 3 tipi di cavo, il classico doppino, il cavo coassiale e la fibra.

Il doppino è composto da due conduttori di rame isolati, attorcigliati tra loro in modo elicoidale(DNA style), per evitare interferenze fra di loro. Il doppino è molto utile per la linea telefonica dato che può percorrere molti km senza che il segnale si indebolisca, ovvero senza bisogno di una amplificazione.

Il cavo coassiale è più grosso e può estendersi per distanze maggiori rispetto il doppino. La distanza maggiore è frutto di unamaggior schermatura a cui è sottoposto il nucleo in rame del cavo che lo rende immune dal rumore. Esistono due cavi coassiali, uno da 50 Ohm per le trasmissioni digitali e uno da 75 Ohm per quelle analogiche.

La fibra ottica è formata da 3 parti: sorgente luminosa, mezzo di trasmissione e rilevatore di luce. La sorgente di luce è rappresentata da LED oppure laser, anche se il secondo, oltre ad essere meno diffuso è anche più costoso. Il mezzo trasmissivo è la fibra, composta un nucleo di vetro di pochi micron, avvolta in una guaina di vetro rivestita a sua volta da una guaina di plastica. La luce che attraversa la fibra è riflessa al suo interno, da un'estremità all'altra del cavo. Nonostante si

trasmetta alla velocità della luce, quest'ultima viene stroncata dalla velocità di decodifica inferiore che avviene alle estremità. La fibra può contenere più raggi che si differenziano per l'angolo di riflessione. Questo tipo di fibra è detto multimodale. Se la trasmissione all'interno della fibra è unica, si ha una trasmissione in linea retta, detta monomodale.

Lo svantaggio della fibra rispetto al doppino e cavo coassiale è il costo maggiore e la difficoltà nell'unire vari pezzi di cavo, mentre per gli altri due tipi basta attorcigliare il nucleo di rame. Il vantaggio della fibra è la manutenzione, essendo vetro è pari a zero. Altro vantaggio è l'unione di più canali, che avviene tramite prismi.

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

Un satellite è un grande ripetitore di microonde posizionato in cielo. Ci sono tre tipi di satelliti che si differenziano per la loro distanza dalla superficie terrestre.

I satelliti più lontani sono detti geostazionari e sono posti in successione su un'orbita circolare al livello dell'equatore, ad una distanza minima di 2 gradi uno dall'altro(ps: immaginare tanti cerchi concentrici che hanno come primo cerchio il nostro equatore e tutti gli altri più grandi, i satelliti sono su uno di questi). Questi satelliti sono molto lontani dalla terra e per questo hanno un tempo medio di ritardo della trasmissione di 300 millisecondi, ma con uno di essi possiamo coprire quasi

un terzo della superficie terrestre. I satelliti LEO distano circa 500 km dalla terra, hanno un tempo di

latenza inferiore rispetto ai GEO, come il consumo energetico. Essendo vicini, per coprire tutta la terra, sono necessari molti satelliti. Si muovono velocemente. I satelliti MEO, sono posti a un'orbita intermedia tra i LEO e GEO, hanno una velocità relativamente bassa, in quanto sono posti a 18 mila km dalla terra e il loro tempo di rivoluzione è di 6 ore.

5. Che cos'è la modulazione in frequenza (FM)? E in ampiezza(AM)?

Per riuscire a inviare dati in forma digitale è necessario un ampio spettro di frequenza, questo rende adatta la trasmissione in banda base solo a basse velocità e a distanze brevi. Nella

modulazione a frequenza vengono utilizzate 2 o più frequenze.

- Pro

o Molto meno sensibile ai disturbi rispetto all'AM

o Permette una trasmissione di miglior qualità

o Efficienza energetica molto maggiore, cioè il segnale di informazione non richiede

potenza aggiuntiva per essere trasmesso.

- Contro

o Necessità di circuiti molto più complessi

o Occupa più banda

Modulazione in ampiezza (AM): due diverse ampiezze sono usate per rappresentare 0 e 1.

- Pro

o Semplice da mettere in pratica

- Contro

o Molto sensibile a disturbi

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

Questa tecnica è una differente tecnica di multiplexing(più conversazioni nello stesso mezzo fisico)

a divisione di tempo. Ogni valore campionato differisce dal precedente di 1+ o -1 sotto le condizioni che può essere trasmesso un singolo bit che dice se il nuovo campione è maggiore o minore del precedente.

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

il GSM è una tecnologia simile al D-AMPS, appartenente alla seconda generazione di cellullari con qualche modifica. La prima sostanziale è il numero di canali, infatti il GSM ha 124 coppie di canali simplex ampi 200KH e supporta fino ad 8 connessioni contemporanee grazie al multiplexing a divisione di tempo. La trasmissione e ricezione non avvengono nello stesso intervallo, poichè il sistema non è in grado di gestirlo. Il GSM è il protocollo che ha introdotto le SIM, le quali contengono IMSI e la chiave crittografia KI, diversa per ogni SIM. Il cellulare manda IMSI e KI in broadcast. L'operatore riceve entrambi e invia un numero casuale, che viene analizzato e rimandato con la firma del KI all'operatore.

La struttura a cella GSM

Nel protocollo GSM ci sono 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 si 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.

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

CDMA permette la trasmissione per tutto il tempo attraverso l'intero spettro. Queste trasmissioni multiple e simultanee vengono separate tramite tecnica di codifica. L'idea è che i segnali si sommino linearmente, ma ogni coppia lo fa in lingua diversa. Per risalire a ciò che viene detto, basta togliere il rumore aggiunto dalle altre conversazioni utilizzando le matrici di Walsh. Vediamo un esempio.

Creando una matrice di Hadamard 4x4 posso gestire 4 lingue, invertendo ogni riga ottengo altre 4 parole, in modo da avere una coppia di parole per ogni lingua. Ognuno usa una parola, si sommano le coordinate di ogni parola ottenendo un unico vettore risultante che moltiplicato per una parola di una determinata lingua, fornisce un numero:

o Zero: se il dispositivo non ha trasmesso

o Positivo: c'è una parola in quella lingua e la parola è la parola positiva

o Negativo: c'è una parola in quella lingua e la parola è la parola negativa

ES: Si costruisca una base trasmissiva (chip codes) per 18 stazioni in CDMA (volendo, usando le matrici di Hadamard)

Basta fare la matrice di hadamard 32x32 e prendere solo 18 righe Il chip codes è una riga della matrice (di Hadamard) che viene assegnata alla singola stazione che trasmette quello per mandare un 1 o il complemento a 1 (riga * -1) per mandare uno 0 Ogni riga definisce una "lingua" diversa che è linearmente indipendente dalle altre (alias riga S*T = S*(-1*T)= 0 se S != T)

9. Il GPRS: cos'è, difetti e pregi.

Il GPRS è un'evoluzione del GMS che permette la gestione del traffico a pacchetti. Al contrario del GSM non serve un servizio dedicato ma vi è un canale condiviso. Lo spreco di banda è inesistente e si utilizza una tariffa a traffico e non a tempo, come avviene per il GSM. IL GPRS aggiunge il supporto a PPP e IP. essendo una naturale evoluzione del GSM, ci furono differenti classi di cellulare, a seconda del supporto alla prima o seconda tecnologia.

Nei cellulari in classe C, l'utente deve selezionare quale comunicazione utilizzare, se GSM oppure GPRS. La classe B, permette di utilizzare entrambe le reti, ma se si sta scaricando un pacchetto e si riceve una chiamata, il download viene sospeso. Prima della classe A, esiste una pseudo classe A, in cui si possono usare contemporaneamente utilizzando una solo frequenza. La Classe A, permette di utilizzare sia una che l'altra, contemporaneamente, è come avere due cellulari indipendenti.

La sicurezza è analoga al GSM, con l’aggiunta di una seconda chiave Kc(cipher key). Questa è

generata ogni volta dalla Ki e da un numero casuale ogni volta che l’utente di autentica.

10. Ha ndo ff: ch e co s'è e i vari tipi

Nelle connessioni mobili, ogni telefono è connesso alla rete ad una sola cella finché non si sposta. Quando ci si sposta, si deve cambiare la cella precedente con una più vicina, anche per evitare problemi dati dalla distanza. La disconnessione da una cella, può avvenire con due modalità.

Hard handoff: quando il segnale è troppo debole, lo switching office chiede alle celle vicine quanta

potenza ricevono dal cellulare. Queste gli rispondono e il cellulare viene riassegnato alla cella con più potenza. Quindi il cellulare viene mollato e poi riagganciato, in qualche caso è presente del lag che fa cadere la linea.

Soft handoff: Introdotto da GSM (MAHO) per ovviare al problema del lag, quando il cellulare ha poco segnale dalla cella, prima di lasciarla, si aggancia ad una nuova e poi abbandona la vecchia. Occorre che il cellulare gestisca due frequenze, cosa che 1G e 2G non supportavano.

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

FDM: sfrutta la trasmissione in banda passante per condividere un canale, divide lo spettro in bande di frequenza di cui ogni utente ha uso esclusivo per inviare il proprio segnale.

TDM: gli utenti fanno a turni secondo una politica round-robin e ognuno di loro, periodicamente

prende possesso della banda completa per un tempo limitato.

CDM: comunicazione a spettro distribuito in cui un segnale a banda stretta viene sparso su una banda di frequenza più ampia. Ciò rende il segnale più tollerante alle interferenze e permette a più segnali di utenti diversi di condividere la stessa banda di frequenza, chiamato anche CDMA.

12. QAM e QAM16

QAM: Più immune al rumore si ottiene tramite i diagrammi a costellazione, quelli circolari sono quelli ideali ma sono più difficili sia da ottenere che da decodificare.

QAM 16: Quando si voleva spingere sull'acceleratore, nella trasmissione di dati via cavo, si è pensato che il miglior approccio da utilizzare era combinare due tipi di modulazione assieme, l'ampiezza e la fase.

Da questa idea nasce il QAM-16. Grazie ad esso possiamo utilizzare un alfabeto più ampio e spedire un simbolo su 16 ogni unità di tempo con bitrate quadruplo.

13. Che cos'è il byte stuffing

CAPITOLO 3 del testo

Il byte stuffing è usato in PPP (Point-to-Point Protocol) ed è un metodo usato per capire dove inizia e quando finisce un frame. Il byte stuffing inserisce prima e dopo ogni frame un byte, chiamato flag byte. Quindi in caso di perdita di dati, basterà cercare l'ultimo flag byte caricato. Un possibile inconveniente è che dentro i dati ci sia un flag byte. In questo caso, basta che la sorgente inserisca un byte di Escape subito prima di ogni occorrenza e la destinazione provvederà a toglierli.

14. Descrivere il Bit stuffing

È analogo al byte stuffing, solo che è fatto a livello di bit, così viene aggirato il problema del byte stuffing e quindi si può scegliere la dimensione della flag. Ogni frame inizia e finisce con 01111110 (protocollo X.25). Ogni volta che lo strato datalink della sorgente incontra 5, uni di fila inseriscono uno zero. Il destinatario ogni volta che incontra 5 uni, elimina lo zero successivo. Questo metodo è usato anche per fare budino.

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

Per trovare tot errori è necessaria una codifica con distanza tot+1 mentre per correggere tot errori, è necessaria una codifica con distanza 2tot+1. Per distanza di Hamming s’intende il peso minimo ottenibile con la somma minima dei valori di una riga di matrice.

NB: Controllo del flusso: esistono due tecniche per la gestione del flusso: tramite feedback e tramite limitazione della velocità

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 cyclic redundancy check è un metodo per il calcolo di checksum. Il nome deriva dal fatto che i dati d'uscita sono ottenuti elaborando i dati di ingresso i quali vengono fatti scorrere ciclicamente in

una rete logica. Il controllo CRC è molto diffuso perché la sua implementazione binaria è semplice da realizzare, richiede conoscenze matematiche modeste per la stima degli errori e si presta bene a rilevare errori di trasmissione su linee affette da elevato rumore di fondo.

Dati due polinomi P e G (generatore) dobbiamo aggiungere alla destra di P tanti zeri quanto è il grado massimo di G e otteniamo il polinomio F. Poi si dive il polinomio ottenuto per G, si ottiene un resto che va sommato al polinomio F, infine si raggruppano i bit in gruppetti di 4 e si codifica in esadecimale.

Esempio: P=10011101 e G= x^4+x+, quindi abbiamo G=10011

F= P=100111010000 e il resto è 1111.

Il polinomio finale è 1001 1101 1111 in esadecimale è 9DF

17. Descrivere Il protocollo stop and wait, pregi e difetti

Il protocollo S&W è un protocollo molto semplice per il controllo del flusso e si può utilizzare in canali simplex o half-duplex. Quando il mittente invia un blocco aspetta che il ricevente invii una conferma, un ACK (acknowledge). Lo svantaggio principale è l'attesa, ma in compenso non c'è bisogno di regolare la velocità.

Possono sorgere due errori: il frame non arriva mai a destinazione e il mittente aspetta e rinvia all'infinito: c'è bisogno di un tempo limite di rinvio. L'altro problema riguarda l'ACK: potrebbe non arrivare al mittente, il quale rinvia il pacchetto e al destinatario arriva più volte, ma per fortuna viene scartato, grazie al numero di messaggio.

18. Co s’è il pig g yb acking

La tecnica consiste nello sfruttare un messaggio del destinatario al mittente come passaggio per l’ACK, in modo da non perdere tempo e sfruttare al meglio il canale di comunicazione(un messaggio in meno da inviare). Il campo ACK è posto all’inizio del frame. Il problema principale è quando fare

piggybacking: in attesa molto lunga può essere vana, poiché il mittente rinvia il frame. Quindi se il pacchetto arriva per il mittente è caricato e inviato in tempo breve si fa piggybacking, altrimenti

s'invia l'ACK separatamente.

19. Si descriva la tecnica dello Sliding window

È un protocollo per il controllo di flusso. Utilizza la tecnica del piggybacking. Invia pacchetti e aspetta messaggio di conferma ACK. Sorge il problema di quando fare il piggybacking, un'attesa troppo lunga può rendere vano il tutto perché il mittente fa un rinvio del frame. Quindi se il pacchetto arriva velocemente viene fatto piggybacking sennò viene inviato separatamente. L'essenza del protocollo è che ogni partecipante alla comunicazione deve tener sotto controllo 2 finestre, quella dei frame in entrata e quella dei frame in uscita. Ogni frame in usciata contiene un numero di sequenza e il destinatario deve tener traccia di questi per la ricezione mentre il mittente per l'invio.

Con lo sliding window a 1 bit, viene utilizzato il metodo stop and wait. Quando il mittente invia un

frame resta nella finestra finché non viene ricevuto l'ACK corrispondente prima di aggiornare la finestra. I frame inviati sono numerati con 1 o 0. Quando il destinatario riceve il frame, controlla che il numero sia uguale a quello che aspettava, se s'invia l'ACK. Se l'ACK contiene il numero che la sorgente si aspettava allora continua a inviare, altrimenti re invia quello segnato nel buffer. Si può

utilizzare anche il pipelining, inviando più frame contemporaneamente prima di entrare in attesa. Il destinatario aggiorna la finestra non appena riceve il frame e invia l'ACK. Esistono 2 approccio: go back n e selective repeat.

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

Questo protocollo è utilizzato con living window di ampiezza 1 in ricezione e maggiore di uno in invio. I pacchetti arrivano uno per volta e su di essi viene fatto un checksum, se si trovano errori vengono segnalati alla sorgente indicando il numero del pacchetto danneggiato. Per questo motivo la finestra deve essere capiente. Se la finestra sorgente si riempie prima che il timer di arrivo scatti, la pipeline viene svuotata. La destinazione intanto scarta i pacchetti successivi a quello in errore. Questo approccio è efficacie contro la prevenzione di errori, ma occupa molta banda se la frequenza di errori è alta.

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

La tecnica del selective repeat è una tecnica che si usa con il protocollo sliding window. In questo caso il buffer della destinazione deve essere più capiente. Infatti in caso di errori, viene inviato alla

sorgente un NACK, indicandone il pacchetto. Finché il pacchetto contenente l'errore non arriva al destinatario, i pacchetti successivi vengono mantenuti nel buffer. Una volta arrivato tutto, il messaggio viene passato allo strato network. Inoltre la sorgente dispone di un timer per cui, se il pacchetto è errato e non arrivasse un NACK il pacchetto sarebbe rinviato comunque.

CAPITOLO 4

22. descrivere la differenza fra ALOHA e ALOHA-SLOTTED

L'aloha è un metodo inventato alle isole Hawaii per le comunicazioni fra le varie isole. L'Aloha puro è una tecnica dove ognuno trasmette ogniqualvolta ha bisogno di farlo. Una volta inviato il frame la sorgente si mette in ascolto attendendo un feedback, ovvero capire se quel frame è arrivato a destinazione, altrimenti dopo un periodo casuale lo ritrasmette. Questo però crea un alto numero

di collisioni. L'Aloha slotted risolve parzialmente il problema delle collisioni. Questo metodo

prevede che il tempo venga diviso in intervalli discreti che rappresentano uno slot. Gli utenti quindi devono concordarsi sui limiti degli intervalli in modo da sincronizzarsi. Così facendo il periodo di vulnerabilità è dimezzato, poiché i frame collido completamente oppure no. Rispetto all'Aloha

puro, la percentuale di successo nella trasmissione è del 36%,cioè il doppio.

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

Il CSMA è una tecnica di trasmissione dati che si basa sull'accesso multiplo tramite rilevamento della portante. Ogni dispositivo prima di avviare la trasmissione dei dati deve verificare se sul canale, altri nodi stiano trasmettendo, rilevando la portante. Se il canale è libero, inizia a trasmettere, altrimenti aspetta un tempo arbitrario prima di riprovare a trasmettere. La tecnica ha tre varianti:

- CSMA 1-persistente: si controlla continuamente se il canale è libero, appena è libero si trasmette. In caso di collisioni si attende un intervallo casuale prima di ritrasmettere. Le stazioni trasmettono con probabilità 1, non appena il canale si libera. Le migliori prestazioni si ottengono in condizioni di basso carico, il messaggio verrà trasmesso nel più breve tempo possibile. Viceversa, in condizioni di saturazione, cresce la probabilità che siano più stazioni in attesa di trasmissione con conseguente aumento delle collisioni.

- CSMA 0-persistente(non persistente): è detto non-persistente, perché si controlla una sola volta se il canale è libero. Se è occupato si attente un intervallo casuale prima di controllare di nuovo.

- CSMA p-persistente: viene utilizzato nei canali divisi in intervalli di tempo. Una volta controllato il canale se:

  - se è libero, si trasmette con probabilità p o si rimanda fino all'intervallo successivo

con probabilità 1-p.

 ad ogni intervallo si itera l'operazione descritta sopra finché il canale è libero o tutto il frame è stato trasmesso

 se ad un certo intervallo il canale è occupato si attende un intervallo di tempo casuale eri ricomincia dal primo punto.

24. basic bitmap

La basic bitmap è un protocollo a mappa di bit. In tale protocollo ogni periodo di contesa è diviso in N intervalli. Se la stazione 0 deve inviare un frame, trasmette un bit 1 durante l'intervallo 0, ovvero il suo intervallo di comunicazione e all'interno del quale, può trasmettere solo lei. In generale la stazione i-esima invia un 1 nell'intervallo i-esimo quando ha un frame accodato da inviare, incurante del fatto che altre stazioni voglio trasmettere. Una volta finiti gli N intervalli, il ciclo ricomincia. Nonostante questa tecnica eviti collisioni, i tempi di invio del frame in una rete con molte stazioni può essere molto ampio.

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

Il protocollo precedente è poco adatto a reti con molte stazioni. Un'alternativa è il protocollo

collision free binary countdown. Quando una stazione vuole trasmettere invia il proprio indirizzo sotto forma di stringa binaria, un bit alla volta partendo dal bit più significativo. Questi bit vengono uniti in OR, quindi dopo ogni serie di bit si ha un risultato che ha la funzione di fermare la contesa di tutte le stazioni aventi il bit in quella posizione minore (passano al round successivo quelle con uno, quelle con 0 vengono eliminate). Alla fine il vincitore coinciderà con la stazione con l'indirizzo più alto. L'efficienza del canale è pari a d/(d*log2 N) ma può raggiungere anche il 100%. Funziona bene ad alto carico.

26. spi eg a re ch e co s'è l'ad ap tive t ree walk protocol

Questo protocollo si basa su un'idea tanto semplice quanto particolare. Pensiamo alle stazioni

come foglie di un albero binario. Ora al primo livello di contesa dopo una trasmissione, all'istante 0, tutti i nodi cercano di trasmettere. Se uno ci riesce va tutto bene, altrimenti se c'è una collisione all'instante 1 provano a trasmettere solo quelle stazioni sotto il nodo due(figlio a sinistra del nodo padre). Se una di queste riesce a trasmettere tutto bene, all'istante 3 tocca a trasmettere alle stazioni del nodo 3(figlio destro del nodo padre), altrimenti si continua a scendere verso sinistra.

27. Ethernet e i vari tipi di cavo

Ethernet è lo standard delle reti locali metropolitane, In base al cablaggio esistono diversi tipi di

Ethernet:

- 10Base5: (thick Ethernet) cavo coassiale molto grosso, con connessioni generalmente effettuate con spine a vampiro. Il 10 indica che opera a 10 Mbps, la parola 'Base' indica che la trasmissione in banda base.

Può supportare segmenti lunghi fino a 500 m (il numero 5 indica). Ai cavi è fissato saldamente un tranceiver utile per rilevare le collisioni e per mantenere uno stabile contatto con il nucleo del cavo.

Un cavo tranceiver collega il trasmettitore all'interfaccia installata nel pc ed è 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 sottile del precedente. I connettori sono BNC standard, che formano giunzioni a T, sono più affidabili e facili da utilizzare. Molto più economico e semplice da installare, ma ogni segmento può essere lungo al massimo 185 m 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.

- 10Base-T: ogni stazione è 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.

28. Codifica Manchester

Questo tipo di codifica nasce dalla necessità di dover determinare senza ambiguità il punto iniziale, finale e centrale di ogni bit senza impulsi esterni. Questa decodifica divide il periodo di bit in 2 intervalli uguali. Se si deve inviare 1 si tiene un livello di tensione alto nel primo intervallo e basso nel secondo, mentre viceversa se si invia uno 0 (lo standard direbbe esattamente il contrario!!). Questa tecnica aiuta non poco la sincronizzazione di trasmettitore e ricevitore.

Esiste inoltre una variante di questa codifica detta differenziale che si basa sul cambio di

transizione tra intervalli. Se `è uno 0 avviene un cambio di transizione altrimenti no. Questo metodo `e piùimmune al rumore anche se piùcomplesso.

29. Cos'e' il binary exponential backoff?

Algoritmo che descrive come viene scelto (dinamicamente) il tempo di attesa casuale dopo una collisione. Dopo una collisione il tempo viene discretizzato in intervalli di lunghezza pari al massimo tempo di propagazione sul mezzo di trasmissione. Ogni stazione può decidere se ritrasmettere sull'intervallo 0 o 1. Questo fa diminuire bruscamente la probabilità di collisione aumentando a

ogni iterazione il tempo di attesa.

Questo può essere ovviato se si tronca l'algoritmo a una decina di iterazioni cosicché la probabilità di collisione è trascurabile e il ritardo accettabile.

- Si calcola il tempo di propagazione in andata e ritorno nel caso peggiore (2t)
- Si divide il tempo in intervalli di durata p
- Alla collisione iesima (con 1=< i =<16) si sceglie un numero a caso N compreso tra 0 e 2i-1 e

si attendono N*P intervalli prima di ritentare

- Alla 16 collisione si getta la spugna e si segnala un errore

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

Problema stazione che non è in grado di rilevare i potenziali concorrenti per il mezzo trasmissivo a causa della distanza.

A invia un frame a B. Anche C deve inviare un frame a B, controlla se ci sono trasmissioni in corso, ma essendo che A e C sono troppo distanti non vedrà A e trasmetterà il frame a B. La trasmissione interferisce su B e distruggerà entrambi i frame.

Quando B trasmette ad A, nello stesso momento in cui C vuole trasmettere a D. C controlla il canale, sente che c'è una trasmissione è conclude che non può trasmettere a D. Ma questa trasmissione potrebbe creare una cattiva ricezione solo tra B e C e non tra C e D perciò c'è uno spreco di banda.

Risoluzione: MACA: trasmittente incita il ricevente a trasmettere un piccolo frame, in modo che le stazioni vicine rilevando questa trasmissione, evitano di inviare dati durante la trasmissione.

31. Bluetooth

L'unità base del sistema Bluetooth è il piconet, composto da un nodo master e un numero minore

o uguale a sette di nodi slave, situati entro un raggio di circa 10 metri. Il cuore del piconet è il nodo master, il quale controlla il clock e decide chi può comunicare a ogni intervallo. La comunicazione avviene sempre passando attraverso il nodo master. I nodi slave non possono scambiarsi dati

direttamente. La banda è divisa in 79 canali da 1MHZ. La modulazione è FSK con un bit per Hz, per una velocità di circa 1 Mbps. La struttura del frame inizia con un codice di accesso che identifica il nodo master di riferimenti. Segue l'intestazione di 54 bit che contengono i campi del sottostrato MAC, quindi type, checksum, il campo indirizzo del destinatario ecc. il campo dati può arrivare a

2744bit.

CAPITOLO 5

NB: closed loop/ dynamic: algoritmo che tiene d'occhio la congestione e interviene quando opportuno. Open loop/static: tutte le decisioni prese all'inizio in modo che la congestione non si verifichi, ma poi non compie correzioni se accade la congestione.

32. Si descriva l'algoritmo statico Flooding(open loop)

Il flooding è un algoritmo statico in cui ogni pacchetto che arriva a una stazione viene rimandato in tutte le direzioni, esclusa quella da cui è arrivato. È un metodo potente ma a rischio congestione.

Si può migliorare utilizzando un metodo di hop counting, che semplicemente conta le stazioni finora percorse e la trasmissione rimandata si ferma fino ad un hop max. Una variante della tecnica è il flooding selettivo, cioè ogni router ritrasmette solo verso le stazioni che approssimativamente vanno nella direzione giusta.

33. Descrivere il distance vector routing (DVR)(closed loop)

Algoritmo dinamico che tiene conto del carico istantaneo della rete. Ogni router possiede una mappa di tutte le distanze e le connessioni con ogni altro router. Per trovare la via migliore, ogni router chiede la mappa ai router vicini e grazie a quest'ultima e al tempo di risposta costruisce la propria. Ogni voce in questa tabella contiene la linea di trasmissione preferita e la stima del tempo

o la distanza associata a quella destinazione. Unità di misura utilizzare sono il numero di hop, la lunghezza nella coda e il ritardo, che si calcola con l'invio di un pacchetto ECHO. Ogni tot millisecondi, ogni router invia ai propri vicini i ritardi segnati sulla propria tabella, cosi da tenere la rete sempre aggiornata. Si possono avere problemi nell'aggiornamento della mappa quando un nodo della rete sparisce, oppure quando un router diventa lento si ha una congestione della rete .

34. Linkstate routing

Questo algoritmo è basato sullo stato dei collegamenti e può essere riassunto in 5 punti:

1. Scoprire i propri vicini e il loro indirizzo di rete
2. Misurare il ritardo dai vicini
3. Costruire un pacchetto con le informazioni raccolte
4. Inviare pacchetti agli altri router
5. Elaborare il percorso più breve dai router.

Inizialmente, avviene il passaggio di pacchetti HELLO che indica al vicino di inviare il proprio indirizzo di rete dicendogli anche la propria identità. Successivamente ogni router deve capire il ritardo da ogni vicino, grazie a un pacchetto ECHO che indica al ricevente di rispondere immediatamente per capire il ritardo dalla sorgente. Poi vengono costruiti i pacchetti con le informazioni sullo stato dei collegamenti e inviati in broadcast utilizzando il flooding. Questa costruzione è molto semplice: il pacchetto inizia con la propria identità seguita da un numero di sequenza, dall'età e da una lista di vicini con affiancato il ritardo rilevato. Se il numero del pacchetto ricevuto rispetto al precedente è più recente viene memorizzato e inoltrato alle altre stazione, se è meno recente viene ritrasmesso alla sorgente, se invece è lo stesso viene scartato.

35. Choke packet

In questo approccio di tipo cloosed loop, è previsto che un router tenga d'occhio il grado di utilizzo delle sue linee in uscita. In router misura, per ciascuna linea, l'utilizzo istantaneo e la storia

passata. Quando una delle linee in uscita, si avvicina a una soglia di congestione prestabilita, il

router esamina i pacchetti in ingresso per vedere se sono destinati alla linea intasata. In caso affermativo, invia all'host un choke packet per avvertirlo di diminuire il flusso. Quando il mittente(l'host) riceve il choke packet diminuisce il flusso, ignorando i successivi choke packet per un tempo prefissato, dato che ne arriveranno molti in sequenza. Dopo l'intervallo di tempo. L'host ristabilisce gradualmente la velocità.

36. Choke packet hop-by-hop

È analogo al precedente, ma cerca di risolvere il problema principale, cioè la lentezza di reazione. L'host che produce i pacchetti ci mette un certo tempo a ricevere i choke packet e di conseguenza a diminuire il flusso. Per migliorare la situazione e provare ad arginare il problema, si può costringere ogni router sul percorso del pacchetto, a rallentare subito il ritmo. Questa tecnica

rende più veloce il sollievo del router destinatario ma richiede spazio di buffer nei router sul percorso dal mittente al destinatario.

37. Load shedding

Questo metodo è davvero banale: quando un router è troppo carico, scarta alcuni pacchetti, ma lo fa con un minimo di criterio. Infatti se sta trasmettendo semplici file, il pacchetto in attesa da più tempo ha la precedenza, quindi i nuovi pacchetti sono i primi ad essere scartati. Per migliorare l'algoritmo sono assegnate delle priorità ai vari pacchetti.

Variante milk and wine: se sta trasmettendo semplici file, il pacchetto in attesa da più tempo ha la precedenza, quindi i nuovi pacchetti sono i primi ad essere scartati(wine). Se la trasmissione è ad esempio di carattere multimediale, avviene il contrario(milk).

38. Red (random early detection)

L'idea alla base di questo algoritmo è simile a quella del Load shedding con la sola differenza che

al posto di aspettare che la congestione fermi tutto, lo scarto dei pacchetti viene fatto prima che il buffer sia pieno. Si avvia lo scarto anticipato quando le code delle linee superano una certa soglia prestabilita. La sorgente non viene avvisata della cancellazione del pacchetto per evitare traffico inutile. La sorgente, non vedendo l'ACK, si comporta di conseguenza

39. Reverse Path Forwarding

Una tecnica usata con lo scopo di assicurare un cammino di pacchetti Multicast privi di loop e per prevenire l'IP spoofing. Funziona come il flooding solo che vengono considerati solo i pacchetti che arrivano dal cammino migliore. Se arriva da una linea non considerata migliore, il pacchetto è visto come duplicato, quindi scartato.

40. Quality of Service(da ampliare)

I quattro parametri della QoS sono: affidabilità, ritardo, Jitter (variazione statistica nel ritardo di ricezione dei pacchetti trasmessi) e banda.

Controllo dello Jitter: la variazione di tempo con cui arrivano i pacchetti è detta jitter. In trasmissioni audio/video un jitter elevato causa una qualità variabile del media.

Quando un pacchetto arriva al router viene controllato il suo anticipo/ritardo e viene inserita questa info nel pacchetto stesso. Se il pacchetto è in anticipo viene trattenuto per il tempo necessario, se in ritardo viene ritrasmesso il prima possibile.

41. Leaky Bucket, pregi e difetti

L'idea che sta alla base è questa: si pensi a un secchio con dell'acqua avente un piccolo foro. Per quanta acqua ci sia dentro la velocità di fuori uscita dal foro è costante. Ecco, ogni host si interfaccia alla rete con un leaky bucket, ovvero un buffer sotto forma di coda. Quando arriva un pacchetto a coda piena viene subito scartato. L'host trasmette un pacchetto ogni ciclo di clock.

Questi comportamenti possono essere gestiti sia dall'OS che a livello HW. Questo algoritmo viene applicato così come appena descritto quando i pacchetto hanno dimensione costante. In caso contrario viene gestito un contatore inizializzato a n ad ogni ciclo di clock. Se si trasmette un pacchetto di dimensioni inferiore si ha l'opportunità di trasmetterne altri restando però all'interno della dimensione n.

42. Descrivere il token bucket, pregi e difetti

Versione dinamica del leaky bucket. 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. Se un host resta molto inattivo il numero di token posseduto non è infinito ma limitato a un certo n.

Token bucket consente un certo controllo del traffico dati pur imponendo un limite al tasso medio di trasmissione dei dati.

43. descrivere l'ARP(Address Resolution Protocol)

ARP si occupa dell'associazione tra indirizzi IP e indirizzi MAC. Idea: quando un host vuole sapere a che host corrisponde un certo indirizzo IP non fa altro che chiederlo in broadcast e ovviamente risponde solo la macchina che ha quell'indirizzo. Host1 prepara il pacchetto e inserisce l'indirizzo destinazione. Host 2 riceve il frame e vede è indirizzato a lui, lancia interrupt e lo manda allo strato superiore. ARC memorizza in cache l'indirizzo della sorgente.

44. Si descriva DHCP e il suo funzionamento

Usa UDP. Il DHCP è il protocollo che permette l'assegnazione manuale o automatica dell'indirizzo IP. L'idea di base è semplice, esiste un server speciale che assegnali gli indirizzi alle macchine che lo richiedono, Questo server può non trovarsi sulla stessa LAN del richiedente. È buona norma che in ogni sottorete ci sia un agente di inoltro DHCP. Quando una macchina vuole il proprio indirizzo manda un pacchetto DHCP Discover che viene catturato dal DHCP relay e viene girato al server. Come funziona?

- Il client invia un pacchetto DHCPDISCOVER in broadcast, con indirizzo IP sorgente messo

convenzionalmente a 0.0.0.0, e destinazione 255.255.255.255 (indirizzo di broadcast).

- Il pacchetto viene ricevuto da tutti i server DHCP presenti, i quali possono rispondere (o meno) ciascuno con un pacchetto di DHCPOFFER in cui propongono un indirizzo IP e gli altri parametri di configurazione. Questo pacchetto di ritorno è indirizzato direttamente all'indirizzo di livello datalink del client (che non ha ancora un indirizzo IP) in unicast

Se nel dominio di broadcast ci sono anche uno o più DHCP relay, questi inoltrano il pacchetto al loro server di riferimento.

- Il client aspetta per un certo tempo di ricevere una o più offerte, dopodiché ne seleziona una, ed invia un pacchetto DHCPREQUEST in broadcast, indicando all'interno del pacchetto, con il campo "server identifier", quale server ha selezionato. Anche questo pacchetto raggiunge tutti i server DHCP presenti sulla rete (direttamente o tramite un relay).

- Il server che è stato selezionato conferma l'assegnazione dell'indirizzo con un pacchetto di DHCPACK (in unicast all'indirizzo di livello datalink del client, possibilmente attraverso un relay); gli altri server vengono automaticamente informati che la loro offerta non è stata scelta dal client, e che sulla sottorete è presente un altro server DHCP.

- A questo punto, il client è autorizzato ad usare l'indirizzo ricevuto per un tempo limitato,

detto tempo di lease. Prima della scadenza, dovrà tentare di rinnovarlo inviando un nuovo pacchetto DHCPREQUEST al server, che gli risponderà con un DHCPACK se vuole prolungare l'assegnazione dell'indirizzo. Questi sono normali pacchetti IP unicast scambiati tra due calcolatori che hanno indirizzi validi. Se il client non riesce a rinnovare l'indirizzo, tornerà allo stato iniziale cercando di farsene attribuire un altro.

45. IPV6(da sistemare)

Riserva 128 bit per ipv6 Version, Differentiated services, flow label; payload length, next header, hop limit; source address; destination address.

- Version:4 Bit, determina la versione di IP che si sta usando.
- Traffic Class: 8 Bit, usato per distinguere le classi di servizio permette di gestire le code by priority assegnando ad ogni pacchetto una classe di priorità rispetto ad altri pacchetti provenienti dalla stessa sorgente. Viene usata nel controllo della congestione.
- Flow label: 20 Bit, consente una sorgente e a una destinazione di marcare un gruppo di pacchetti che, avendo gli stessi requisiti, devono essere trattati allo stesso modo.
- Payload lenght: 16 Bit, indica il numero di byte che segue l'intestazione di 40 byte.
- Next header: 8 Bit, Indica quale tipo di intestazione segue l'header. Molto simile al campo protocol dell'header IPv4, del quale usa gli stessi valori.
- Hop limit: 8 Bit, utilizzato per impedire ai pacchetti di vivere per sempre, come il TTL.

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

o 32 Bit per: indirizzo version, type of service, total length; Identification, Flags, Fragment offset; time to live, protocol, header checksum; source address; destination address; options, data.

o Version: 4 Bit, determina la versione del pacchetto IP

o IHL: 4 Bit, indica la lunghezza dell'intestazione espresso in word di 32 bit dato che non è costante.

o Differentiated services: 8 Bit, classe di servizio di appartenenza del pacchetto.

o Total lenght: 16 Bit, indica la dimensione (in byte) dell'intero pacchetto, comprendendo header e dati.

o Identification: 16 Bit, serve all'host di destinazione per determinare a quale datagramma appartiene il frammento appena arrivato.

o Flags: 3 Bit, 2 campi lunghi 1 bit per la frammentazione:

o DF: Don’t fragment, rappresenta un ordine che impone ai router di non dividere in frammenti il datagramma. Originariamente venne pensato per host non in grado di rimettere insieme i pezzi. MF: More fragment: tutti i frammenti a parte l’ultimo hanno questo bit impostato a 1, fondamentale per sapere quando sono arrivati tutti i frammenti di un datagramma.

o Fragment offset: 13 Bit, indica la posizione del frammento nel datagramma corrente. Tutti i frammenti tranne l’ultimo di un datagramma devono essere multipli di 8 byte, che è la dimensione del frammento elementare.

o Time to live: 8 Bit, contatore per limitare la vita di un pacchetto.

o Protocol: 8 Bit, indica quale processo di trasporto è in attesa di quei dati (TCP, UDP).

o Header checksum: 16 Bit È un campo usato per il controllo degli errori dell'header. Somma tutti i gruppi di 16 bit appena arrivano usando l’aritmetica in complemento a uno e poi si prende il complemento a uno del risultato. Aiuta a rilevare errori durante il percorso del pacchetto.

CAPITOLO 6

47. Frame ethernet

Questo è il frame ovvero il pacchetto dati ricevuto dallo strato di datalink nella pila di protocolli. Gli elementi sono:

Preamble: 7 byte: questi primi byte hanno valore 10101010 e servono a "svegliare" gli adattatori del ricevente e a sincronizzare gli oscillatori con quelli del mittente.

Start Frame Delimiter (SFD): 1 byte, questo byte ha valore 10101011 e la serie dei due bit a

1 indica al destinatario che sta arrivando del contenuto importante; è protetto mediante la violazione del codice Manchester; svolge la stessa funzione del campo flag della

trama HDLC;

Destination MAC address: 6 byte: questo campo contiene l'indirizzo LAN dell'adattatore di destinazione; se l'indirizzo non corrisponde, il livello fisico del protocollo lo scarta e non lo invia agli strati successivi;

Source MAC address 6 byte;

EtherType: 2 byte: questo campo indica il tipo di protocollo del livello di rete in uso durante la trasmissione, oppure la lunghezza del campo dati;

Payload: da 46 a 1500 byte: contiene i dati reali, che possono essere di lunghezza variabile in base al MTU se i dati superano la capacità massima, vengono suddivisi in più pacchetti, mentre se i dati non raggiungono la lunghezza minima di 46 byte, viene aggiunto del padding della lunghezza opportuna;

Frame Check Sequence (FCS), CRC di 4 byte: permette di rilevare se sono presenti errori di trasmissione; il ricevente calcola il CRC e lo confronta con quello ricevuto in questo campo.

48. Si descriva l'header UDP.

E' un protocollo di trasporto connectionless. Trasmette segmenti costituiti da un intestazione di 8 byte seguita dal carico utile. L'intestazione UDP è formata da 2 byte di Source port seguiti da altri 2 di Destination port che indicano le porte a cui sono associati i processi di destinazione. Poi c'è il campo UDP lenght che include l'intestazione e i dati. Infine c'è il Checksum che è facoltativo è settato a 0 se non utilizzato. L'UDP predilige la velocità al controllo. Questo protocollo è utilizzato dal DNS.

49. descrivere l'header del TCP/IP e commentarlo;

TCP è stato progettato per riuscire a garantire solide prestazioni anche in presenza di molti errori di vario genere. Un entità TCP accetta dai processi locali il cui uso di dati degli utenti e li suddivide in pezzi di dimensione non superiore ai 64 KB e li invia in un datagramma IP autonomo. E' un protocollo orientato alla connessione.

Sia il ricevente che il mittente devono creare dei socket i quali possiedono un indirizzo (porta). Source port, destination port; sequence number; acknowlegement number; tcp header length, CWR ECE (congestion), URG (urgente), ACK (indica che aknowledgement è valido) PSH (dati PUSH) RST (reimpostare connessione) SYN (stabilire connessione) FIN (finire connessione), windows size;

checksum, urgent pointer; options; dati (facoltativo).

50. Ch e co s'è il DNS

Il DNS è il sistema dei nomi di dominio. Concettualmente internet è divisa in 200 domini di primo livello. Ogni dominio è diviso in sotto domini e così via. I domini di primo livello sono di due tipi: generici (.com, .net, ecc) e per nazione(.it, .uk ecc). per ottenere un indirizzo si contatta un register per il dominio di primo livello corrispondente, controllata la disponibilità si paga una

tariffa(tipicamente) annuale e il gioco è fatto. I nomi possono avere fino a 63 caratteri e il percorso completo non può superare i 255 caratteri.

CAPITOLO 7

51. Co s'è un ci fra rio a so stituz io n e e a t ra sp o si zi on e

Un cifrario a sostituzione si basa sul principio della sostituzione di lettere con altre, oppure più semplicemente di shiftare l'alfabeto di un numero K di caratteri. Nonostante la semplicità, provare tutte le possibili combinazioni è proibitivo. I cifrari a trasposizione mascherano il testo in chiaro senza modificarlo. Si basa su due principi: il primo riguarda la scrittura in righe di N caratteri del messaggio, una sotto l'altra, in modo da creare colonne di M caratteri. Poi una chiave ha lo scopo di dare un ordine a come vengono prese tali colonne di caratteri per formare la parola criptata.

52. Si descriva il block cipher

I Block cipher sono algoritmi a chiave simmetrica, in altre parole per decifrare e cifrare si usa la stessa chiave. I cifrari a blocco prendono n bit dal testo in chiaro e li trasformano utilizzando una chiave a n bit. Questi algoritmi spesso utilizzano una trasposizione e una sostituzione per cifrare. Per permutare si usa una cosiddetta P-box che prende in input n bit e li permuta, senza violare il principio di Kerckhoff(cioè, si sa che è una permutazione, ma non quale sia). Per la sostituzione si usa una S-box che compie la sostituzione.

53. Si d escri va l'al go ritmo DES e t rip lo DES

E' uno dei primi block cipher:

Ogni block cipher è costituito da due elementi che possono essere composto come mattoncini lego:
P-Box: permutation box: fanno una permutazione, prende dei dati in input e fa una permutazione.

S-Box: Substitution box: sostituisce certi bit con altri.

DES composto da 64 bits, chiave da 56 bits e 19 passaggi.

Creato dall'IBM, inizialmente usava chiavi da 128 bits, ridotta però a 56 bits.

Più tardi si sono resi conto che la chiave era troppo piccola allora si passo al triplo DES. Il triple DES usa tre volte DES in sequenza, con due chiavi da 112 bits. Cripta prima con la prima chiave, poi decripta con la seconda e poi cripta di nuovo con la prima.

Se si usano due chiavi uguali si ritorna ad avere DES.

54. Counter Mode Cipher

Questa modalità permette l'accesso casuale a dati criptati, quello che gli altri metodi non permettono. Con questo metodo il testo in chiaro non viene cifrato direttamente ma viene cifrato un IV con chiave crittografica.

Questo blocco cifrato viene messo in XOR con il testo in chiaro. A ogni blocco dell'IV viene incrementato di 1. Questo sistema però è esposto ad attacchi di tipo keystream riutilizzati.

55. Cipher block chaining

Questa modalità di cifratura si basa sull'idea che ogni blocco ha un legame con il successivo, in modo che un loro spostamento fa perdere il significato di tutto. Questo metodo in particolare prende ogni blocco del testo e lo mette in XOR con il precedente. Per il primo blocco, lo XOR viene fatto con un blocco casuale detto IV(initialization Vector) che è trasmesso insieme al testo cifrato.

56. Stream cipher

Questo è un metodo per evitare che parti del testo vengano invertite, anche senza decifrare. Ci sono vari metodi, dei quali il cipher block chaining e il cipher feedback che però dipendono dai blocchi precedenti, facendo così perdere tempo durante il decripting. Per ovviare al problema appena descritto viene utilizzato un metodo di cifratura diverso: lo stream cipher. Questa funzione non fa altro che criptare un IV con una chiave crittografica ottenendo un blocco di uscita, R, il quale viene cifrato per ottenere il successivo blocco di uscita e così via. La sequenza di blocchi cifrati in uscita è chiamata keystream. L'IV viene utilizzato solo per la prima iterazione, poi sono i keystream a essere decifrati. L'uso di diversi keystream evita gli attacchi di tipo keystream riutilizzato.

57. RSA

Facendo un esempio pratico, se Alice vuole spedire un messaggio a Bob e non vuole che altri all'infuori di Bob possano leggerlo, Alice cercherà sull'elenco la chiave pubblica di Bob e con quella potrà cifrare il messaggio. Essendo Bob l'unico a possedere la chiave inversa, sarà anche l'unico a poter decifrare il messaggio, che rimarrà così segreto per tutti gli altri, compresa Alice, che non disponendo della chiave inversa non sarà in grado di decifrare il messaggio da lei stessa creato. Ovviamente il successo di questo sistema si basa sull'assoluta necessità che Bob sia l'unico ad essere in possesso della chiave inversa. In caso contrario, avendo entrambe le chiavi, chiunque potrebbe decifrare agevolmente il messaggio.

Con questo metodo di cifratura è possibile anche garantire la provenienza di un messaggio. Riprendiamo l'esempio precedente: Alice questa volta, prima di cifrare il messaggio usando la chiave pubblica di Bob, lo cifrerà usando la propria chiave inversa e solo in un secondo momento lo ri-crittograferà utilizzando la chiave pubblica di Bob. Quando Bob riceverà il messaggio e lo decifrerà usando la propria chiave inversa, otterrà ancora un messaggio crittografato. Quel dato messaggio necessiterà poi della chiave pubblica di Alice per essere decifrato, garantendo in questo

modo che il messaggio è stato spedito solo e soltanto da Alice, unica a possedere la chiave inversa con la quale era stato crittografato il messaggio.

Più semplicemente, utilizzando questo metodo di cifratura, Alice può mandare messaggi a tutti,

garantendo la provenienza. Infatti crittografando il messaggio con la propria chiave inversa, chiunque sarà in grado di leggere il messaggio, decrittandolo con la sua chiave pubblica, assicurandosi in tal modo che il mittente sia proprio Alice.

Per semplificare il funzionamento immaginiamo che A debba spedire un messaggio segreto a B. Occorrono i seguenti passaggi:

o B sceglie due numeri primi molto grandi (per esempio di 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).

o B invia il numero che ha ottenuto ad A. Chiunque può vedere questo numero.

o A usa questo numero per cifrare il messaggio.

o A manda il messaggio cifrato a B, chiunque può vederlo, ma non decifrarlo.

o B riceve il messaggio e utilizzando i due fattori primi che solo lui conosceva lo decifra.

A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro

comunicazioni impiegherebbe troppo tempo per scoprire i due fattori primi, con cui si può decifrare il messaggio.

In realtà questo sistema non è così semplice, come si può notare dai calcoli descritti nel paragrafo successivo, e per trasmettere grandi quantità di dati occorre tanto tempo per la decifratura, quindi A e B si scambieranno con questo sistema una chiave segreta (che non occupa molto spazio), che poi useranno per comunicare tra loro usando un sistema a crittografia simmetrica, più semplice e veloce.

58. Si descriva la tecnica di attacco "birthday attack"

Data una funzione f, lo scopo dell'attacco è quello di trovare 2 numeri a e b tali che f(a) = f(b), si valuta la funzione f per input diversi.

Questo attacco riduce il numero di operazioni medie per forzare un MD a m bit da 2m a 2m/2. 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 queste coppie sono > k la possibilità di avere una coppia con lo stesso output è molto buona. Quindi approssimativamente basta avere un n > della radice di k. Quindi con

64 bit si ha una buona probabilità generando 232 messaggi di trovarne 2 con lo stesso MD.

59. Sicurezza in 802.11

Il protocollo di sicurezza prescritto dallo standard 802.11 è il WEP. Quando la sicurezza viene attivata ogni stazione deve stabilire una chiave segreta con la base, il modo in cui questo avviene non è specificato. Un'altra possibilità è che la stazione base generi numeri casuali e li invii con una trasmissione wireless cifrata usando la chiave pubblica del ricevente. La cifratura WEP usa uno stream cipher basato sull'algoritmo RC4 che genera un keystream che viene messo in XOR con il testo in chiaro per produrre il cifrato. Lo standard WEP raccomanda che l'IV, utilizzato per

inizializzare il keystream) sia cambiato ad ogni invio, anche se questo non evita gli attacchi(ad

esempio birthday attack). Oltre a questa debolezza, c'è anche la vulnerabilità dell'algoritmo RC4.

60. Si descriva la sicurezza del Bluetooth

La sicurezza del Bluetooth consiste nella comunicazione tra master e slave. Si suppone che i due dispositivi si siano scambiati le chiavi. Questa chiave è detta passkey. Per stabilire una connessione si controlla che l'altro conosce la passkey. In caso affermativo viene scelta una chiave di sessione casuale a 120bit. La cifratura usa uno stream cipher detto E0 e il controllo di integrità usa SAFER+.

61. La tecnica di attacco reflection attack

reflection attack è un tipo di attacco informatico in cui un attaccante, invece di colpire direttamente la vittima, dirige il suo traffico verso un host intermedio (testa di ponte o reflector) e poi questo lo dirige verso la vittima.

In genere per ottenere questo effetto nelle reti IP si usa l'IP spoofing. L'attaccante genera un

pacchetto con l'indirizzo sorgente della vittima e l'indirizzo di destinazione del refletctor. Il reflector risponde con un pacchetto che però, a causa dello spoofing, avrà come indirizzo quello della

vittima. La vittima quindi riceverà pacchetti provenienti dal reflector e non riuscirà a risalire

all'attaccante vero.

Se l'attaccante è in grado di far sì che i sistemi intermedi mandino dei pacchetti di risposta più grossi dei pacchetti iniziali si è in presenza di un attacco di amplificazione.

62. Il replay attack

Nell'ambito della sicurezza informatica il replay-attack è una forma di attacco di rete che consiste nell'impossessarsi di una credenziale di autenticazione comunicata da un host ad un altro, e riproporla successivamente simulando l'identità dell'emittente. In genere l'azione viene compiuta da un attaccante che s'interpone tra i due lati comunicanti. Questo attacco permette operazioni fraudolente come falsa autenticazione e/o transazioni duplicate, senza dover necessariamente decrittare la password, ma soltanto ritrasmettendola in un tempo successivo[1].

A differenza dell'attacco di tipo man in the middle che opera sempre in tempo reale, il replay attack può operare anche in modo asincrono quando la comunicazione originale è terminata. Per

esempio, 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 prontamente invia quella di Alice, instaurando così la comunicazione.

63. L' al go ri tmo Diffie-hellman

Lo scambio di chiavi Diffie-Hellman (Diffie-Hellman key exchange) è un protocollo crittografico che consente a due entità di stabilire una chiave condivisa e segreta utilizzando un canale di comunicazione insicuro (pubblico) senza la necessità che le due parti si siano scambiate

informazioni o si siano incontrate in precedenza. La chiave ottenuta mediante questo protocollo può essere successivamente impiegata per cifrare le comunicazioni successive tramite uno schema di crittografia simmetrica.

Sebbene l'algoritmo in sé sia anonimo (cioè non autenticato) è alla base di numerosi protocolli

autenticati ed è usato anche in alcune modalità di funzionamento del protocollo TLS.
Nell'implementazione originale (e più semplice) del protocollo si considera inizialmente un numero g, generatore del gruppo moltiplicativo degli interi modulo p, dove p è un numero primo. Uno dei due interlocutori, ad esempio Alice, sceglie un numero casuale a e calcola il valore A = ga mod p (dove mod indica l'operazione modulo, ovvero il resto della divisione intera) e lo invia attraverso il canale pubblico a Bob (l'altro interlocutore), assieme ai valori g e p. Bob da parte sua sceglie un numero casuale b, calcola B = gb mod p e lo invia ad Alice. A questo punto Alice calcola KA = Ba mod p, mentre Bob calcola KB = Ab mod p.

I valori calcolati sono gli stessi, in quanto Ba = gba e Ab = gab.

A questo punto i due interlocutori sono entrambi in possesso della chiave segreta e possono cominciare ad usarla per cifrare le comunicazioni successive.

Un attaccante può benissimo ascoltare tutto lo scambio, ma per calcolare i valori a e b avrebbe bisogno di risolvere l'operazione del logaritmo discreto, che è computazionalmente onerosa e richiede parecchio tempo, in quanto sub-esponenziale (sicuramente molto più del tempo di conversazione tra i 2 interlocutori).

64. Attacco Man in the middle

In crittografia, l'attacco dell'uomo in mezzo, meglio conosciuto come man in the middle attack, MITM o MIM è un tipo di attacco nel quale l'attaccante è 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 che li unisce reciprocamente sia stato effettivamente compromesso da una terza parte, ovvero appunto un attaccante. L'attaccante deve essere in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due vittime. Supponiamo che Alice voglia comunicare con Bob e che Mallory 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 Mallory è in grado di intercettarla, può iniziare un attacco Man in the middle. Mallory può 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 Mallory ed invia i suoi messaggi cifrati a Bob. Mallory quindi li intercetta, li decifra, ne tiene una copia per sé, e li re-cifra (dopo averli alterati se lo desidera) usando la chiave pubblica che Bob aveva originariamente inviato ad Alice. Quando Bob riceverà il messaggio cifrato, crederà che questo provenga direttamente da Alice. Un simile attacco è possibile, in teoria, verso qualsiasi messaggio inviato usando tecnologia a chiave pubblica, compresi pacchetti di dati trasportati su reti di computer.

65. DNS spoofing

E’ un tipo di attacco Man in the middle. Il DNS spoofing si svolge nel modo seguente: la vittima fa una DNS query, che viene catturata dall'attaccante, che la corrompe e manda alla vittima una risposta diversa da quella che sarebbe stata fornita dal DNS. Tale attacco può esser effettuato in varie modalità:

- Simulazione delle risposte del DNS
- Cache poisoning
- Manomissione fisica del DNS

L'obiettivo dello spoofing è modificare la corrispondenza tra indirizzo IP e nome del sito contenuti nelle risposte. Vedi DNSSEC.