

Domande e risposte di Reti e Sicurezza

Autore: Federico Z.

Editore Latex: Riccardo A.

16 luglio 2018

Premesse

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

Link alla repository GitHub: <https://github.com/FedeBrichi/Reti>

Indice

1	Cosa si intende per serie di Fourier?	17
1.1	Cos'è?	17
1.2	Pregi	17
1.3	Difetti	17
1.4	Ambiti d'uso	17
2	Bitrate e Baudrate	18
2.1	Cosa sono?	18
2.2	Pregi	18
2.3	Difetti	18
2.4	Ambiti d'uso	18
3	Descrivere i vari tipi di cavo e confrontarli	18
3.1	Il doppino, cos'è?	18
3.1.1	Pregi	19
3.1.2	Difetti	19
3.1.3	Ambiti d'uso	19
3.2	Il cavo coassiale, cos'è?	19
3.2.1	Pregi	20
3.2.2	Difetti	20
3.2.3	Ambiti d'uso	20
3.3	Fibra ottica, cos'è?	20
3.3.1	Pregi	21
3.3.2	Difetti	22
3.3.3	Ambiti d'uso	22
4	Caratteristiche e confronto tra i vari tipi di satellite: GEO, MEO e LEO	22
4.1	Cosa sono?	23
4.2	Pregi	24
4.3	Difetti	24
4.4	Ambiti d'uso	24
5	Cos'è la modulazione di frequenza?	24
5.1	Cos'è?	25
5.2	Pregi	25
5.3	Difetti	25
5.4	Ambiti d'uso	25

6	Cos'è la modulazione delta (delta modulation)?	26
6.1	Cos'è?	26
6.2	Pregi	26
6.3	Difetti	26
6.4	Ambiti d'uso	26
7	Descrivere in dettaglio il GSM (Global System for Mobile connection)	27
7.1	Cos'è?	27
7.2	Pregi	28
7.3	Difetti	28
7.4	Ambiti d'uso	28
8	Si descriva la tecnica CDMA (Code Division Multiple Access), possibilmente con esempio	28
8.1	Cos'è?	28
8.2	Pregi	29
8.3	Difetti	29
8.4	Ambiti d'uso	29
9	Il GPRS: Cos'è? Pregi e difetti	29
9.1	Cos'è?	30
9.2	Pregi	30
9.3	Difetti	30
9.4	Ambiti d'uso	30
10	Handoff cos'è e vari tipi	30
10.1	Pregi	31
10.2	Difetti	31
10.3	Ambiti d'uso	31
11	FDM, TDM, CDM: algoritmi per la selezione della banda	32
11.1	FDM (Frequency Division Multiplexing) cos'è?	32
11.1.1	Pregi	32
11.1.2	Difetti	32
11.1.3	Ambiti d'uso	32
11.2	TDM (Time Division Multiplexing) cos'è?	33
11.2.1	Pregi	33
11.2.2	Difetti	33
11.2.3	Ambiti d'uso	33

11.3	CDM (Code Division Multiplexing) cos'è?	33
11.3.1	Pregi	34
11.3.2	Difetti	34
11.3.3	Ambiti d'uso	35
12	QAM e QAM16	35
12.1	QAM16, cos'è?	35
12.2	Pregi	35
12.3	Difetti	36
12.4	Ambiti d'uso	36
13	byte stuffing?	36
13.1	Cos'è?	36
13.2	Pregi	37
13.3	Difetti	37
13.4	Ambiti d'uso	37
14	bit stuffing?	37
14.1	Cos'è?	38
14.2	Pregi	38
14.3	Difetti	38
14.4	Ambiti d'uso	38
15	Numero di bit necessari per riconoscimento (correzione) degli errori di trasmissione?	39
15.1	Bit necessari per rilevare un errore	39
15.2	Bit necessari per rilevare e correggere un errore	39
15.3	Pregi	39
15.4	Difetti	40
15.5	Ambiti d'uso	40
16	Si descriva cos'è il CRC (Cycle Redundancy check). Si calcoli inoltre il CRC di 10011101 usando il polinomio generatore di $x^4 + x + 1$	40
16.1	Cos'è?	40
16.2	Esempio	41
16.3	Pregi	41
16.4	Difetti	41
16.5	Ambiti d'uso	41

17	Descrivere il protocollo stop-and-wait, pregi e difetti	42
17.1	Cos'è?	42
17.2	Pregi	43
17.3	Difetti	43
17.4	Ambiti d'uso	43
18	Cos'è il piggybacking?	43
18.1	Cos'è?	43
18.2	Pregi	44
18.3	Difetti	44
18.4	Ambiti d'uso	44
19	Si descriva la tecnica dello Sliding window	44
19.1	Cos'è?	44
19.2	Pregi	45
19.3	Difetti	45
19.4	Ambiti d'uso	45
20	Si descriva l'idea dei protocolli "go back N", indicandone pregi e difetti	45
20.1	Cos'è?	46
20.2	Pregi	46
20.3	Difetti	47
20.4	Ambiti d'uso	47
21	Si descriva cos'è la tecnica del selective repeat	47
21.1	Cos'è?	47
21.2	Pregi	48
21.3	Difetti	48
21.4	Ambiti d'uso	48
22	Descrivere la differenza tra ALOHA e ALOHA-SLOTTED	48
22.1	Cos'è ALOHA?	48
22.1.1	Pregi	49
22.1.2	Difetti	49
22.1.3	Ambiti d'uso	49
22.2	Cos'è ALOHA Slotted?	49
22.2.1	Pregi	49
22.2.2	Difetti	50
22.2.3	Ambiti d'uso	50

23 Si illustri il CSMA (Carrier Sense Multiple Access), indicandone pregi e difetti	50
23.1 Cos'è?	51
23.2 Pregi	52
23.3 Difetti	52
23.4 Ambiti d'uso	52
24 Basic Bitmap	52
24.1 Cos'è?	52
24.2 Pregi	53
24.3 Difetti	53
24.4 Ambiti d'uso	53
25 Spiegare in cosa consiste il protocollo collision free binary countdown, pregi e difetti	53
25.1 Cos'è?	54
25.2 Pregi	54
25.3 Difetti	54
25.4 Ambiti d'uso	55
26 Spiegare cos'è l'adaptive tree walk protocol?	55
26.1 Cos'è?	55
26.2 Pregi	56
26.3 Difetti	56
26.4 Ambiti d'uso	56
27 Ethernet e i vari tipi di cavo	56
27.1 Cos'è?	56
27.2 10base5	57
27.3 10base2	57
27.4 10base-T	57
27.5 10base-F	58
27.6 Pregi	58
27.7 Difetti	58
27.8 Ambiti d'uso	58
28 Codifica Manchester	59
28.1 Codifica Manchester cos'è?	59
28.2 Codifica Manchester differenziale cos'è?	59
28.3 Pregi	60

28.4 Difetti	60
28.5 Ambiti d'uso	60
29 Cos'è il binary exponential backoff?	60
29.1 Cos'è?	60
29.2 Pregi	61
29.3 Difetti	61
29.4 Ambiti d'uso	61
30 Stazione nascosta e stazione esposta: cosa sono e cosa fanno?	61
30.1 Stazione nascosta, cos'è?	62
30.2 Stazione esposta, cos'è?	62
31 Bluetooth	62
31.1 Cos'è?	62
32 Si descriva l'algoritmo statico Flooding	63
32.1 Cos'è?	64
32.2 Pregi	64
32.3 Difetti	65
32.4 Ambiti d'uso	65
33 Descrivere il distance vector routing	65
33.1 Cos'è?	65
33.2 Pregi	66
33.3 Difetti	66
33.4 Ambiti d'uso	66
34 Descrivere Linkstate routing	66
34.1 Cos'è?	67
34.2 Pregi	68
34.3 Difetti	68
34.4 Ambiti d'uso	68
35 Choke packet	68
35.1 Cos'è?	69
35.2 Pregi	69
35.3 Difetti	70
35.4 Ambiti d'uso	70

36 Choke packet hop-by-hop	70
36.1 Cos'è?	70
36.2 Pregi	71
36.3 Difetti	71
36.4 Ambiti d'uso	71
37 Load shedding	71
37.1 Cos'è?	71
37.2 Pregi	72
37.3 Difetti	72
37.4 Ambiti d'uso	72
38 Red (Random Early Detection)	72
38.1 Cos'è?	72
38.2 Pregi	73
38.3 Difetti	73
38.4 Ambiti d'uso	73
39 Reverse Path Forwarding	73
39.1 Cos'è?	73
39.2 Pregi	74
39.3 Difetti	74
39.4 Ambiti d'uso	74
40 Quality of Service (QoS)	74
40.1 Cos'è?	74
41 Leaky bucket, pregi e difetti	75
41.1 Cos'è?	75
41.2 Pregi	76
41.3 Difetti	76
41.4 Ambiti d'uso	76
42 Descrivere il token bucket, pregi e difetti	76
42.1 Cos'è?	77
42.2 Pregi	77
42.3 Difetti	78
42.4 Ambiti d'uso	78

43	Descrivere l'ARP	78
43.1	Cos'è?	78
43.2	Pregi	79
43.3	Difetti	79
43.4	Ambiti d'uso	79
44	Si descriva DHCP e il suo funzionamento	79
44.1	Cos'è?	80
44.2	Pregi	81
44.3	Difetti	81
44.4	Ambiti d'uso	81
45	IPV6	81
45.1	Pregi	82
45.2	Difetti	82
45.3	Ambiti d'uso	82
46	Elencare e descrivere brevemente i secondi (primi) 32b dell'header IPv4 (IPv6)	83
46.1	IPv4	83
46.2	IPv6	83
46.3	IPv4, primi 32bit	83
46.4	IPv4, secondi 32bit	84
46.5	IPv6, primi 32bit	85
46.6	IPv6, secondi 32bit	85
47	Frame Ethernet	86
47.1	Cos'è?	86
48	Si descriva l'header UDP	87
48.1	Cos'è UDP?	87
48.2	Header UDP	88
48.3	Pregi	88
48.4	Difetti	88
48.5	Ambiti d'uso	88
49	Descrivere l'header TCP/IP e commentarlo	89
49.1	Cos'è TCP?	89
49.2	Header TCP	89
49.3	Pregi	91
49.4	Difetti	92

49.5	Ambiti d'uso	92
50	Cos'è il DNS?	92
50.1	Cos'è?	92
50.2	Pregi	93
50.3	Difetti	93
50.4	Ambiti d'uso	93
51	Cos'è un cifrario a sostituzione? E a trasposizione?	93
51.1	Cos'è il cifrario a sostituzione	94
51.2	Cos'è il cifrario a trasposizione	94
51.3	Differenze tra i due	94
52	Si descriva il block cipher	94
52.1	Cos'è	94
52.2	P-box	95
52.3	S-box	95
52.4	Pregi	95
52.5	Difetti	95
52.6	Ambiti d'uso	95
53	Si descriva l'algoritmo DES e triplo DES	96
53.1	Cos'è DES?	96
53.2	Cos'è Triplo-DES?	96
53.3	Pregi	97
53.4	Difetti	97
53.5	Ambiti d'uso	97
54	Counter Mode Cipher	98
54.1	Causa della creazione	98
54.2	Cos'è?	98
54.3	Pregi	98
54.4	Difetti	98
54.5	Ambiti d'uso	99
55	Cipher block chaining	99
55.1	Cos'è?	99
55.2	Pregi	100
55.3	Difetti	100
55.4	Ambiti d'uso	100

56 Stream cipher	100
56.1 Cos'è?	100
56.2 Pregi	101
56.3 Difetti	101
56.4 Ambiti d'uso	101
57 RSA	101
57.1 Causa della creazione	101
57.2 Cos'è?	102
57.3 Pregi	102
57.4 Difetti	102
57.5 Ambiti d'uso	102
58 Si descriva la tecnica di attacco “Birthday attack”	103
58.1 Firme digitali	103
58.2 Cos'è il birthday attack	103
59 Sicurezza in 802.11	104
59.1 Cos'è?	104
59.2 Come funziona	104
59.3 Pregi	105
59.4 Difetti	105
59.5 Ambiti d'uso	105
60 Si descriva la sicurezza di Bluetooth	105
60.1 Livelli di sicurezza	105
60.2 Pregi	106
60.3 Difetti	106
60.4 Ambiti d'uso	106
61 La tecnica di attacco reflection attack	106
61.1 Cos'è?	106
61.2 Regole per evitarlo	106
62 Replay attack	107
62.1 Cos'è?	107
62.2 Metodi per evitarlo	107

63	Algoritmo Diffie-hellman	108
63.1	Cos'è?	108
63.2	Pregi	108
63.3	Difetti	108
63.4	Ambiti d'uso	108
64	Attacco Man in the middle	109
64.1	Cos'è?	109
64.2	Come evitarlo	109
65	DNS spoofing	110
65.1	Cos'è?	110
65.2	Possibile soluzione	110
A	Capitolo 1 - Introduzione	112
A.1	Tipi di collegamento	112
A.2	Classificazione delle reti	112
A.3	Architettura delle reti	112
A.3.1	Progettare una rete	113
A.3.2	Tipi di servizi offerti da un livello	113
A.4	Modelli di reti	114
B	Capitolo 2 - Strato fisico	115
B.1	Serie di Fourier e Banda passante	115
B.2	Mezzi di trasmissione guidati	115
B.2.1	Mezzi magnetici	115
B.2.2	Il doppino	116
B.2.3	Il cavo coassiale	116
B.2.4	Fibra ottica	117
B.3	Mezzi wireless	118
B.3.1	Spettro elettromagnetico	118
B.3.2	Trasmissioni radio	118
B.3.3	Trasmissioni a microonde	119
B.3.4	Infrarossi	119
B.3.5	Trasmissioni a onde luminose	119
B.4	Satelliti	120
B.5	Rete telefonica pubblica commutata	120
B.5.1	Collegamenti locali	120
B.6	Linee e multiplexing	122
B.6.1	Multiplexing a divisione di frequenza	122

B.6.2	Multiplexing a divisione di lunghezza d'onda	122
B.6.3	Multiplexing a divisione di tempo	123
B.7	Commutazione (<i>Switching</i>)	123
B.7.1	Commutazione di circuito	123
B.7.2	Commutazione di messaggio	123
B.7.3	Commutazione di pacchetto	123
B.8	Sistema telefonico mobile	124
B.8.1	Prima generazione - voce analogica	124
B.8.2	Seconda generazione - voce digitale	125
B.8.3	Terza generazione - voce e dati digitali	126
C	Capitolo 3 - Strato data link	127
C.1	Progetto dello strato data link	127
C.1.1	Servizi forniti allo strato network	127
C.1.2	Suddivisione in frame	128
C.1.3	Controllo errori	129
C.1.4	Controllo di flusso	129
C.2	Rilevazione e correzione errori	129
C.2.1	Codici per la correzione degli errori	129
C.2.2	Codifiche a rilevazione d'errore	130
C.3	Protocolli data link elementari	131
C.3.1	Simplex senza restrizioni	131
C.3.2	Simplex stop-and-wait	131
C.3.3	Simplex per canali rumorosi	132
C.4	Protocolli sliding window	132
C.4.1	Sliding window a 1 bit	133
C.4.2	Go back N e Ripetizione selettiva	133
C.5	Esempi di protocolli	134
C.5.1	HDLC - High-level Data Link Control	134
C.5.2	PPP - protocollo punto a punto	135
D	Capitolo 4 - Sottostrato MAC	136
D.1	Il problema dell'assegnazione del canale	136
D.1.1	Assegnazione statica	136
D.1.2	Assegnazione dinamica	136
D.2	Protocolli ad accesso multiplo	137
D.2.1	Aloha	137
D.2.2	Protocolli ad accesso multiplo con rilevamento della portante	138
D.2.3	Protocolli senza collisione	138

D.2.4	Protocolli a contesa limitata	139
D.2.5	Protocolli LAN Wireless	140
D.3	Ethernet	141
D.3.1	Cablaggio Ethernet	141
D.3.2	La codifica Manchester	142
D.3.3	Il protocollo del sottostrato MAC Ethernet	142
D.3.4	Algoritmo di backoff esponenziale binario	143
D.3.5	Prestazioni di Ethernet	144
D.3.6	Ethernet commutata	144
D.3.7	Fast Ethernet	144
D.3.8	Gigabit Ethernet	145
D.3.9	Retrospectiva su Ethernet	146
D.4	LAN Wireless	146
D.4.1	La pila di protocolli 802.11	146
D.4.2	Lo strato fisico di 802.11	146
D.4.3	Il protocollo del sottostrato MAC di 802.11	146
D.4.4	Servizi	147
D.5	Commutazione nello strato data link	147
D.5.1	Bridge tra due 802	148
D.5.2	Internetworking locale	148
D.5.3	Bridge spanning tree	149
D.5.4	Bridge remoti	149
D.5.5	Ripetitori, hub, bridge, switch, router, gateway	149
E	Capitolo 5 - Strato network	150
E.1	Architettura dello strato network	150
E.2	Algoritmi di routing	150
E.2.1	Principio di ottimalità	150
E.2.2	Routing basato sul percorso più breve	150
E.2.3	Flooding	150
E.2.4	Routing basato sul vettore delle distanze	150
E.2.5	Routing basato sullo stato dei collegamenti	150
E.2.6	Routing gerarchico	150
E.2.7	Routing broadcast	150
E.3	Algoritmi per il controllo della congestione	150
E.4	Qualità del servizio	150
E.4.1	Requisiti	150
E.4.2	Tecniche per una buona qualità	150
E.5	Collegamento tra reti	151
E.5.1	Differenze tra le reti	151

E.5.2	Connessione tra le reti	151
E.5.3	Circuiti virtuali concatenati	151
E.5.4	Collegamento tra reti senza connessione	151
E.5.5	Routing in una internetwork	151
E.6	Lo strato network in internet	151
E.6.1	Il protocollo IP	151
E.6.2	Gli indirizzi IP	151
E.6.3	Protocolli di controllo internet	151
E.6.4	OSPF	151
E.6.5	BGP	151
E.6.6	Internet multicasting	151
E.6.7	IPv6	151
F	Capitolo 6 - Strato trasporto	152
F.1	Richiesta connessione e protocollo Three-way Handshake . . .	152
F.2	Rilascio della connessione	153
F.3	Introduzione all'UDP	154
F.4	TCP	154
F.4.1	Introduzione	154
F.4.2	Modello di servizio di TCP	154
F.4.3	Protocollo TCP	155
F.4.4	Intestazione TCP	155
F.4.5	Connessione TCP	156
F.4.6	Rilascio connessione TCP	156
G	Capitolo 7 - Strato applicazione	157
G.1	DNS	157
H	Capitolo 8 - Sicurezza	158
H.1	Crittografia	158
H.1.1	Introduzione alla crittografia	158
H.1.2	Cifrari a sostituzione	158
H.1.3	Blocchi monouso	158
H.1.4	Due principi crittografici fondamentali	159
H.2	Algoritmi a chiave simmetrica	159
H.2.1	DES	159
H.2.2	AES	160
H.2.3	Modalità di cifratura	161
H.3	Algoritmi a chiave pubblica	161
H.4	Message digest	161

H.4.1	MD5	161
H.4.2	SHA-1	161
H.5	Sicurezza delle comunicazioni	161
H.5.1	IPsec	161
H.5.2	Firewall	161
H.5.3	Sicurezza wireless	161
H.6	Replay attack	162
H.7	Sicurezza del naming	162
H.7.1	DNS spoofing	162
H.7.2	DNS sicuro	162

1 Cosa si intende per serie di Fourier?

1.1 Cos'è?

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

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

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

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

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

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

1.2 Pregi

Un pregio sicuramente è il fatto che scomporre un segnale in più componenti permette uno studio più preciso del segnale.

1.3 Difetti

—

1.4 Ambiti d'uso

Viene ampiamente usata nelle comunicazioni in generale, per la trasmissione dei dati, la scomposizione del segnale in più sinusoidi migliora la comprensione delle onde. Si passerà poi alle varie modulazioni per ovviare ai problemi dovuti alle attenuazioni o alle distorsioni.

2 Bitrate e Baudrate

2.1 Cosa sono?

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

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

2.2 Pregi

Grazie a queste unità di misura è possibile dare una rappresentazione quantitativa della velocità di trasmissione del mezzo.

2.3 Difetti

—

2.4 Ambiti d'uso

Queste metriche vengono utilizzate nelle reti wireless e cablate.

3 Descrivere i vari tipi di cavo e confrontarli

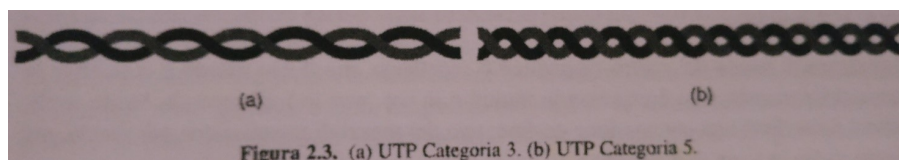
I principali tipi di cavo utilizzato nelle telecomunicazioni sono: il doppino, il cavo coassiale e la fibra ottica.

3.1 Il doppino, cos'è?

È un cavo composto da due conduttori di rame isolati, spessi circa 1mm e avvolti uno intorno all'altro in una forma elicoidale. L'intreccio è utile per annullare i campi elettromagnetici generati dai due conduttori, i quali si annullano a vicenda. Esistono diverse varietà di doppini, i più importanti per le telecomunicazioni sono gli UTP3 e UTP5 (UTP= Unshielded Twisted Pair, doppini non schermati). Le differenze tra i doppini di categoria 3 e

categoria 5 sta nel numero di spire per centimetro: minor numero di spire per cm negli UTP3 e maggiore negli UTP5. Un maggior numero di spire permette di migliorare la qualità del segnale trasmesso su lunghe distanze, a scapito però della quantità di materiale necessario. Esistono anche categorie superiori, i quali gestiscono segnali con banda più ampia.

I doppini si possono utilizzare per trasmettere segnali analogici e digitali, l'ampiezza di banda dipende dal diametro del cavo e dalla distanza percorsa.



3.1.1 Pregi

Costano poco e hanno una discreta velocità trasmissiva.

3.1.2 Difetti

L'ampiezza di banda fornita non è tra le migliori e sono vulnerabili ai campi elettromagnetici.

3.1.3 Ambiti d'uso

Vengono utilizzati prevalentemente nel sistema telefonico.

3.2 Il cavo coassiale, cos'è?

È un cavo composto da un nucleo conduttore coperto da un rivestimento isolante, a sua volta circondato da un conduttore cilindrico, solitamente realizzato con una calza di conduttori sottili, che infine è avvolto da una guaina protettiva di plastica. La costruzione e la schermatura del cavo coassiale forniscono ampiezza di banda ed eccellente immunità al rumore. Ne esistono di due tipi, a 50Ω per le trasmissioni digitali e a 75Ω per quelle analogiche; non c'è una motivazione tecnica per questa distinzione.

La banda disponibile dipende dalla qualità, dalla lunghezza del cavo e dal rapporto segnale-rumore del segnale dati. Per molti ambiti il cavo coassiale è stato sostituito dalla fibra ottica per i tratti più lunghi.

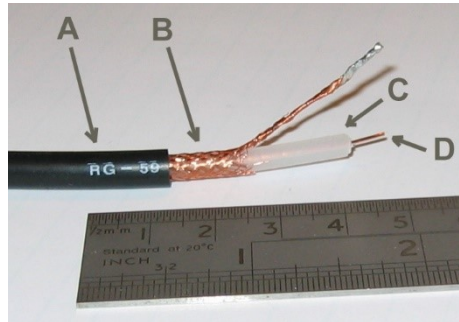


Figura 1: D: nucleo, C: rivestimento isolante, B: conduttore cilindrico, A: guaina protettiva

3.2.1 Pregi

Hanno un'isolamento quasi totale dai campi elettromagnetici grazie ai vari rivestimenti isolanti.

3.2.2 Difetti

Su grandi tratti non sono molto efficienti in termini di banda, vengono infatti sostituiti dalla fibra ottica in quei casi.

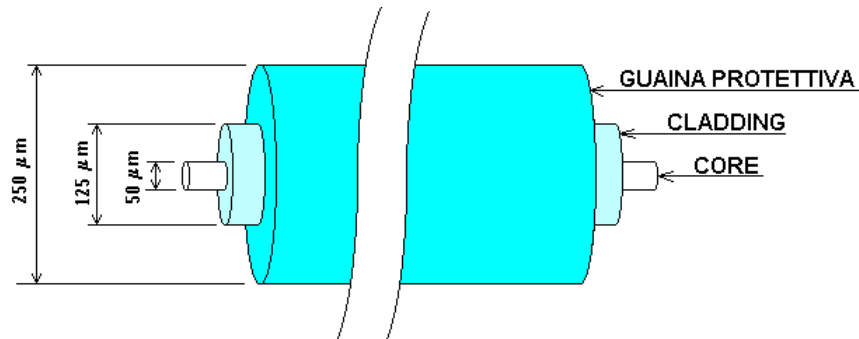
3.2.3 Ambiti d'uso

Il cavo coassiale è molto utilizzato per le reti metropolitane e le televisioni via cavo.

3.3 Fibra ottica, cos'è?

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

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



Esistono due tipi di fibra, la monomodale e la multimodale. La monomodale è più costosa e utilizzata soprattutto per le lunghe distanze, in cui la luce può propagarsi solo in linea retta senza rimbalzare. Nella multimodale invece può contenere più raggi che rimbalzano ad angoli diversi, in questo caso si dice che ogni raggio ha una modalità diversa, da qui il nome multimodale.

Le fibre si possono collegare in diversi modi:

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

3.3.1 Pregi

Rispetto al cavo in rame classico, la fibra apporta diversi vantaggi:

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

- Le fibre non perdono la luce ed è difficile intercettare i dati, questo le rendono molto più sicure rispetto ai cavi in rame.

3.3.2 Difetti

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

3.3.3 Ambiti d'uso

La fibra è molto utilizzata nelle LAN e nei sistemi di trasmissioni a lunga distanza.

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

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

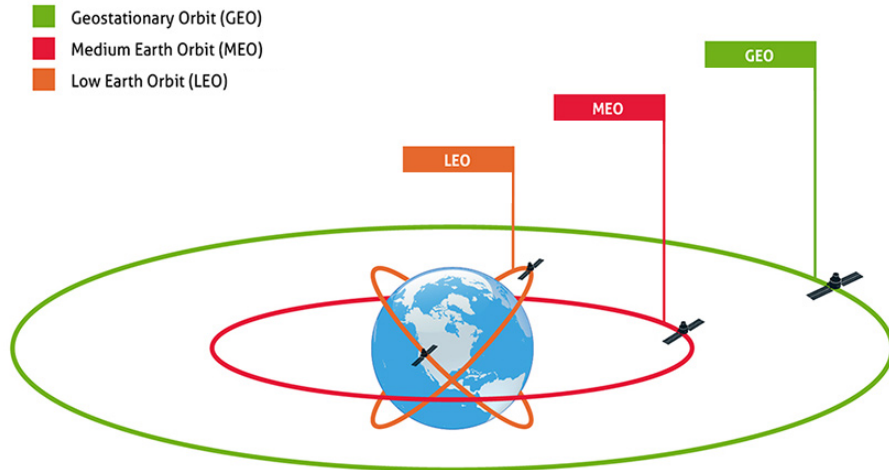
La collocazione dei satelliti è importante, ed è determinata da alcuni fattori:

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

Esistono quindi 3 zone in cui i satelliti possono essere collocati:

- LEO: sotto la fascia di Van Allen inferiore
- MEO: tra la fascia Van Allen inferiore e quella superiore

- GEO: molto al di sopra della fascia Van Allen superiore



4.1 Cosa sono?

GEO GEO (Geostationary Earth Orbit), sono collocati nella fascia più alta, disposti con un intervallo di 2° nel piano equatoriale, così da evitare interferenze. Di conseguenza c'è posto per “solo” 180 satelliti di questo tipo. La loro dimensione è importante e la gestione dell'allocatione degli slot orbitali è motivo di disputa tra paesi, stazioni televisive e militari. Per mantenere la loro posizione, sono dotati di razzi motori che permettono manovre correttive; di solito il carburante per farlo basta per 10 anni. Oltre alla posizione anche le frequenze sono oggetto di dispute, perchè possono interferire con quelle degli utilizzatori delle microonde. Vengono quindi assegnate solo certe frequenze per i satelliti, ognuna con i loro problemi (meteo, affollamento e simili).

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

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

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

4.2 Pregi

Sono di facile utilizzo, basta alzare un'antenna sul tetto di casa per ottenere una maggior ampiezza di banda. Sono importanti per la connessione mobile. Trovano applicazione per portare connessione in terreni inospitali o scarsamente dotati di infrastrutture.

4.3 Difetti

Le fibre ottiche per molti versi sono più comode e versatili rispetto ai satelliti, in quanto la loro velocità è di gran lunga superiore. Un sistema di satelliti è più costoso (?) rispetto alla fibra ottica.

4.4 Ambiti d'uso

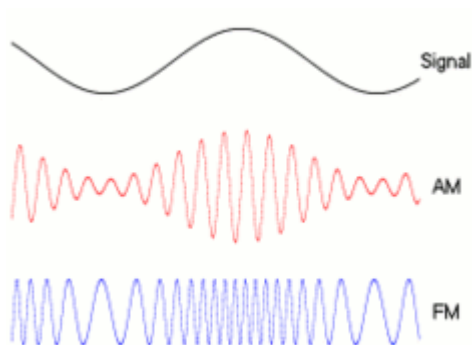
Trovano applicazione in luoghi inospitali e privi di infrastrutture, trovano applicazione nelle trasmissioni broadcast e nelle comunicazioni mobile, dove quindi la fibra fatica ad arrivare.

5 Cos'è la modulazione di frequenza?

Durante l'invio di informazioni, il segnale può subire attenuazione, distorsione o venir disturbata dal rumore; questo porta ad evitare l'uso di un largo intervallo di frequenze. Sfortunatamente le onde quadre utilizzate nei segnali digitali utilizzano un ampio spettro di frequenza, e perciò sono soggette ad una forte attenuazione e alla distorsione.

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

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



5.1 Cos'è?

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

5.2 Pregi

Permette di ridurre i problemi di attenuazione e distorsione della linea.

5.3 Difetti

Necessita di circuiti complessi sia per la generazione del segnale sia per la sua ricezione. Questi problemi sono stati superati dalle attuali tecnologie.

5.4 Ambiti d'uso

Viene utilizzata soprattutto in ambito di broadcasting commerciale, è più usata della modulazione in ampiezza.

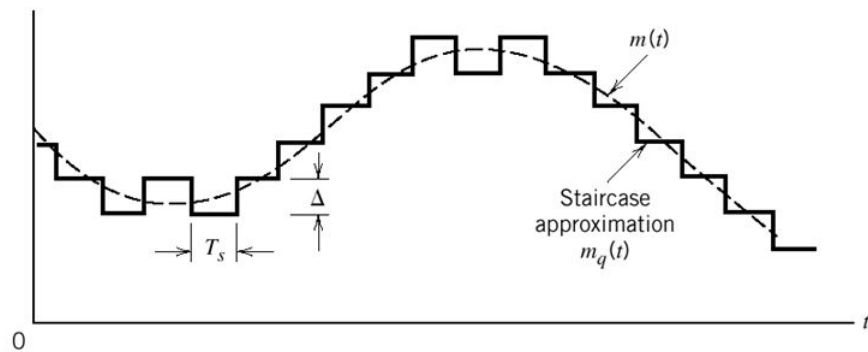
6 Cos'è la modulazione delta (delta modulation)?

6.1 Cos'è?

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

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

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



6.2 Pregi

Grazie a questa tecnica è possibile comprimere e digitalizzare il segnale analogico (e viceversa), con il risultato di gravare meno sulle linee e permettere comunicazioni più veloci (a discapito della precisione).

6.3 Difetti

—

6.4 Ambiti d'uso

Viene utilizzata nelle comunicazioni satellitari o nelle comunicazioni voce.

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

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

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

7.1 Cos'è?

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

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

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

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

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

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

7.2 Pregi

Interoperabilità tra reti diverse che fanno capo ad un unico standard internazionale. Introduzione della comunicazione di tipo digitale.

7.3 Difetti

—

7.4 Ambiti d'uso

è utilizzato appunto nella seconda generazione di telefoni cellulari, è il sistema più diffuso al mondo.

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

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

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

8.1 Cos'è?

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

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

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

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

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

8.2 Pregi

Grazie alla maggiore efficienza spettrale, il CDMA garantisce una maggior velocità di trasmissione dati. Provvede inoltre a garantire una maggior sicurezza rispetto ai predecessori, in quanto la demultiplazione è fattibile solo grazie alla conoscenza delle parole di codice.

8.3 Difetti

—

8.4 Ambiti d'uso

Viene utilizzata nei telefoni di seconda generazione, come alternativa a D-AMPS e GSM.

9 Il GPRS: Cos'è? Pregi e difetti

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

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

9.1 Cos'è?

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

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

Per inviare un pacchetto IP, una stazione mobile chiede uno o più slot inviando una richiesta alla stazione base. Se la richiesta arriva senza problemi, la stazione comunica all'apparecchio mobile la frequenza e gli slot che dovrà utilizzare per trasmettere il pacchetto. Una volta arrivato alla stazione base, il pacchetto è trasferito su Internet attraverso una connessione via cavo.

9.2 Pregi

Lo spreco di banda è inesistente, e viene utilizzata una tariffa a traffico e non a tempo come i suoi predecessori. GPRS aggiunge il supporto a PPP e IP.

9.3 Difetti

—

9.4 Ambiti d'uso

È una tecnologia a cavallo tra la seconda generazione e la terza generazione di telefoni cellulari. Viene utilizzata per scambi di pacchetti dati tramite celle basate su sistemi vocali.

10 Handoff cos'è e vari tipi

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

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

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

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

Nel caso di hard handoff la vecchia stazione di base rilascia il telefono prima che la nuova lo acquisisca. Se la nuova non è in grado di prendere il controllo del dispositivo (ad esempio se non è disponibile nessuna frequenza) il segnale viene interrotto bruscamente, con il risultato di terminazione brusca di una possibile chiamata.

10.1 Pregi

Il soft handoff è più performante in quanto non si perde continuità di chiamata. L'hard handoff non necessita che il dispositivo sia in grado di gestire più frequenze contemporaneamente.

10.2 Difetti

Il soft handoff richiede che il dispositivo sia in grado di gestire più frequenze contemporaneamente. L'hard handoff può causare la caduta di linea con la conseguente perdita di chiamata nel caso in cui una cella non sia in grado di prendere il dispositivo in un lasso di tempo breve.

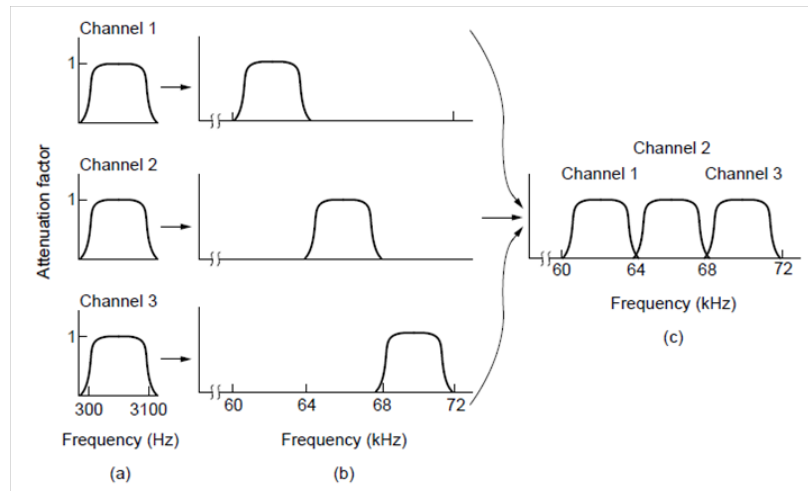
10.3 Ambiti d'uso

Questa tecnica viene utilizzata dai dispositivi mobili (cellulari appunto, che sfruttano le celle). Il soft handoff può essere utilizzato dai telefoni di generazione superiore alla seconda, mentre l'hard handoff da tutti.

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

11.1 FDM (Frequency Division Multiplexing) cos'è?

è una tecnica di condivisione delle risorse trasmissive di un canale di comunicazione. L'intero canale trasmissivo disponibile è diviso in sotto canali, ognuno costituito da una banda di frequenza e separato da un altro grazie ad un piccolo intervallo di guardia. Questo permette la condivisione dello stesso canale da parte di dispositivi che utilizzano diverse regioni di frequenze e utenti che possono così comunicare contemporaneamente senza interferirsi tra loro.



11.1.1 Pregi

Permette di condividere un intero canale da più utenti, suddividendo le conversazioni in base alle diverse frequenze.

11.1.2 Difetti

Gli intervalli di guardia potrebbero essere uno spreco di banda utilizzato unicamente per la sicurezza.

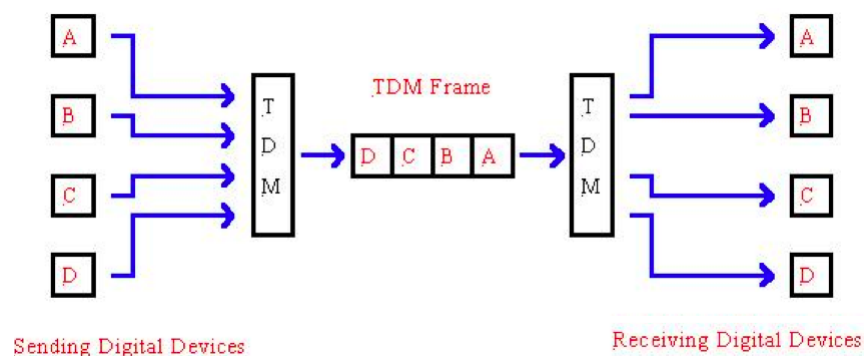
11.1.3 Ambiti d'uso

Questa tecnica è comunemente utilizzata nelle trasmissioni televisive, radiofoniche, telefoniche o di dati. Anche le reti cellulari utilizzano in parte

questo tipo di multiplazione per suddividere e assegnare l'intera capacità trasmissiva o banda radio disponibile alle varie celle di copertura servite da stazioni radio base.

11.2 TDM (Time Division Multiplexing) cos'è?

è una tecnica di condivisione di un canale di comunicazione secondo la quale ogni dispositivo ricetrasmittente ottiene a turno l'uso esclusivo dello stesso per un breve lasso di tempo. Il tempo di utilizzo del canale è diviso in frame tutti della stessa durata, questi frame sono ulteriormente divisi in slot.



11.2.1 Pregi

Più efficiente del TDM in quanto elimina la necessità degli intervalli di guardia.

11.2.2 Difetti

Necessita di un circuito di sincronizzazione temporale in ricezione per l'estrazione del time-slot di competenza.

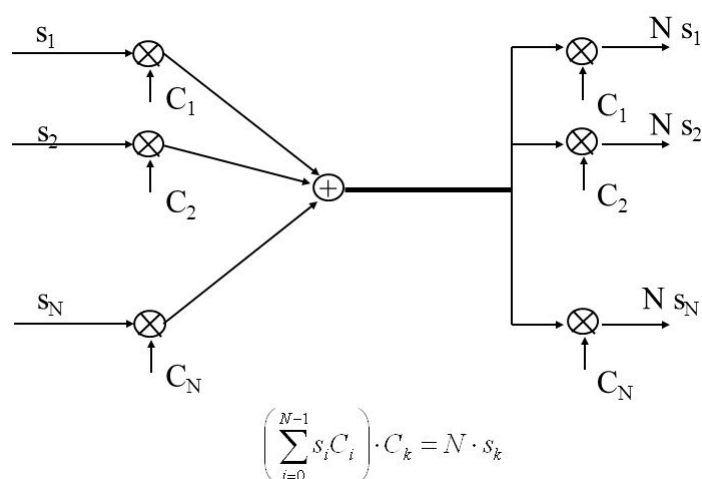
11.2.3 Ambiti d'uso

Utilizzata per le trasmissioni di fonia nella rete telefonica. Questo tipo di multiplazione è utilizzata molto nei sistemi a commutazione di circuito.

11.3 CDM (Code Division Multiplexing) cos'è?

Conosciuta anche come CDMA è il protocollo di accesso multiplo a canale condiviso. Offre una maggiore velocità di trasmissione di dati rispetto

a TDM e FDM. Questa tecnica è realizzata moltiplicando in trasmissione l'informazione generata per un'opportuna parola detta chip; la sequenza in uscita dal moltiplicatore sarà successivamente modulata e infine trasmessa sul canale. In ricezione il segnale ricevuto sarà costituito dalla somma vettoriale di tutti i segnali trasmessi dalle singole stazioni. Grazie all'ortogonalità dei chip delle sorgenti, l'estrazione dell'informazione associata a ciascuna sorgente potrà essere fatta moltiplicando il segnale ricevuto con il particolare codice associato alla determinata sorgente che si vuole estrarre.



11.3.1 Pregi

Rispetto a TDM e FDM, CDM garantisce una miglior efficienza dovuta al fatto che ciascun canale utilizza l'intera banda di frequenza assegnata e per tutto il tempo che desidera. La non-interferenza è assicurata grazie all'uso di codici ortogonali. Provvede inoltre a fornire una maggior sicurezza dovuta al fatto che i segnali si mescolano nel canale e per estrarne uno è necessario conoscere la parola corretta.

11.3.2 Difetti

Necessita di circuiti più complessi rispetto alle altre tecniche di condivisione di un canale.

11.3.3 Ambiti d'uso

è il protocollo più diffuso nelle reti wireless e nei dispositivi mobili di seconda generazione e successive.

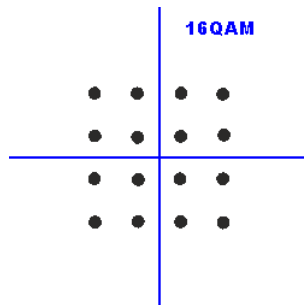
12 QAM e QAM16

QAM è un sistema di modulazione numerica di ampiezza in quadratura, sia digitale che analogica. Le portanti sono sinusoidi. Il termine quadratura indica che differiscono di 90° .

Il segnale in ingresso viene suddiviso e modulato per l'ampiezza. Nel caso di segnali digitali, si sommano i segnali modulati e si ottiene una forma d'onda che risulta una combinazione della modulazione di fase e quella d'ampiezza. Ciascun tipo di modulazione QAM è caratterizzato da un diagramma (costellazione) su cui sono rappresentati tutti gli stati della portante. La QAM, rispetto alla PSK (Phase shift keying), migliora l'immunità al rumore.

12.1 QAM16, cos'è?

QAM16 non è altro che un tipo di costellazione del QAM, utilizzando quattro ampiezze e quattro fasi, per un totale di 16 diverse combinazioni. Ogni modem ad alta velocità ha un suo schema di costellazione e può comunicare solo con altri modem che adottano lo stesso schema (anche se generalmente un modem riesce a emulare anche quelli più lenti).



12.2 Pregi

Permettono di inviare più bit per baud (simbolo), rispetto alle normali modulazioni.

12.3 Difetti

Ogni modem ha un suo schema a costellazione e può comunicare solamente con altri modem che adottano lo stesso schema. Questo problema è però in parte ovviato in quanto la maggior parte dei modem è in grado di emulare costellazioni più lente.

12.4 Ambiti d'uso

Facente parte dello strato fisico, questo tipo di modulazione è utilizzato come standard per modem telefonici.

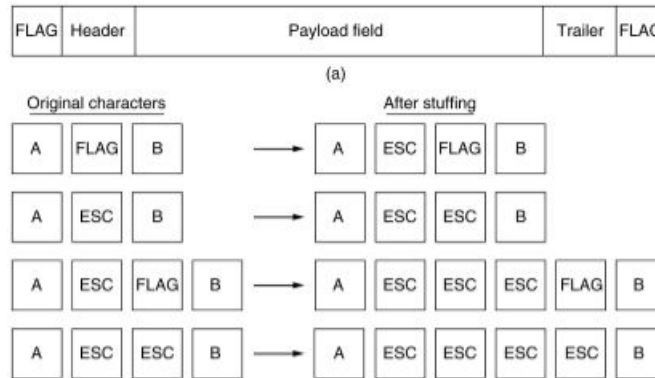
13 byte stuffing?

Lo strato data link deve servire lo strato network. Per farlo necessita di usare a sua volta le informazioni fornite dallo strato fisico, il cui scopo è quello di prendere un flusso di bit e cercare di portarli a destinazione. Non esiste nessuna garanzia per la correttezza dei dati, i bit potrebbero essere maggiori, minori, modificati ecc. Uno dei compiti dello strato data link è quello di rilevare ed eventualmente correggere questi errori.

13.1 Cos'è?

Il modo per rinvenire questi errori è quello di suddividere il flusso dei bit in frame, per poi controllarli. Uno dei metodi di framing è quello di utilizzare un flag byte con il byte stuffing.

Il byte stuffing prevede l'uso di un flag per delimitare l'inizio e la fine dei frame. In questo modo quando il destinatario perde la sincronizzazione può cercare il flag byte per trovare la fine del frame corrente. Due flag byte consecutivi indicano la fine di un frame e l'inizio del successivo. Per far sì che un flag byte sia contenuto internamente ai dati, bisogna utilizzare un byte di escape (ESC) prima di ogni occorrenza "accidentale" del byte flag nei dati. Successivamente lo strato data link della destinazione provvederà a rimuovere i byte di escape prima di passare i dati allo strato network; se anche un carattere ESC si trova dentro i dati, va preceduto da un ulteriore carattere ESC.



13.2 Pregi

Permette una suddivisione di bit in frame tramite l'uso di flag byte, inoltre risolve il problema della sincronia dei frame, grazie ai flag byte che li delimitano.

13.3 Difetti

Legato all'uso di caratteri da 8 bit (1Byte): non tutte le codifiche dei caratteri li usano.

Per effettuare lo stuffing la quantità di caratteri superflui è notevole.

Per risolvere questi problemi è stato creato il bit stuffing.

13.4 Ambiti d'uso

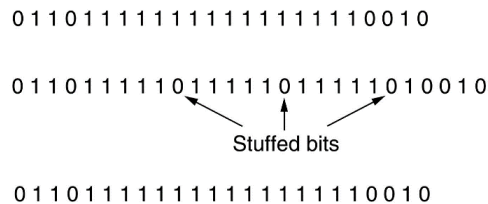
Metodo di framing dello strato Data-Link, viene utilizzato in prevalenza dal protocollo PPP per suddividere il flusso di bit in frame.

14 bit stuffing?

Lo strato data link deve servire lo stato network, per farlo necessita di usare a sua volta le informazioni fornite dallo strato fisico il cui scopo è quello di prendere un flusso di bit e cercare di portarli a destinazione. Non esiste nessuna garanzia per la correttezza dei dati, i bit potrebbero essere maggiori, minori, modificati ecc. Uno dei compiti dello strato data link è quello di rilevare ed eventualmente correggere questi errori.

14.1 Cos'è?

Per risolvere i problemi e le limitazioni provocate dal byte stuffing, viene sviluppata una nuova tecnica di framing, che prende il nome di bit stuffing, questa nuova tecnica permette di creare data frame che contengono sia un numero arbitrario di frame, sia codifiche di carattere con un numero arbitrario di bit. Ogni frame comincia e finisce con un gruppo speciale di bit "0111110" (flag byte). Ogni volta che lo strato data link della sorgente incontra cinque "1" consecutivi nei dati inserisce automaticamente un bit con valore 0 nel flusso in uscita. La destinazione quindi quando riceve cinque bit consecutivi con valore 1 seguiti da uno 0, automaticamente elimina lo 0. Con il bit stuffing il confine fra i due frame viene riconosciuto in modo inequivocabile tramite l'uso della sequenza flag.



14.2 Pregi

Risolve i problemi legati dall'uso di 8 bit per il flag byte del suo predecessore (byte stuffing): la poca compatibilità con molte codifiche di caratteri e lo spreco di banda.

Permette la suddivisione di bit in frame, facilmente individuabili grazie ai bit flag.

14.3 Difetti

—

14.4 Ambiti d'uso

Metodo di framing dello strato data link, utilizzato in protocolli che prevedono frame di dimensione fissa: il bit stuffing è utilizzato per raggiungere tale dimensione.

Utilizzato anche in alcuni protocolli che prevedono un flusso continuo di dati, gli "0" sono inseriti per assicurare la continuità del flusso.

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

I dati trasmessi nei collegamenti locali sono spesso soggetti ad errori, per la loro gestione sono state sviluppate due strategie di base: la prima si basa su una codifica a correzione d'errore mentre la seconda è una codifica a rilevazione d'errore. La prima introduce una ridondanza (in ciascun blocco trasmesso) tale da riuscire a ricostruire il messaggio in caso di anomalie. La seconda invece introduce ridondanza sufficiente solo a capire che c'è stato un errore, ma non di correggerlo. Un frame generalmente consiste di m bit di dati e r bit ridondanti per i controlli, la somma $n=m+r$ è la lunghezza totale del frame chiamata codeword di n bit. Date due codeword, per capire quanti bit corrispondenti sono differenti bisogna effettuare l'OR esclusivo e contare il numero di bit a "1" nel risultato, questo numero è chiamato distanza di Hamming.

15.1 Bit necessari per rilevare un errore

Detto questo, per trovare d errori è necessaria una codifica con distanza $d+1$, quando la destinazione vede una codeword non valida riesce a determinare che c'è stato un errore, ma non a correggerlo.

15.2 Bit necessari per rilevare e correggere un errore

Per correggere d errori è necessaria una codifica con distanza $2d+1$, in tal modo codeword legali sono distanziate in modo tale che anche con d cambiamenti la codeword originale è sempre più vicina di ogni altra, può quindi essere determinata univocamente. Un semplice esempio di codifica a rilevazione d'errore si può realizzare aggiungendo un bit di parità ai dati, calcolato in modo che il numero di "1" nella codeword sia sempre pari (o dispari). Entrambe le codifiche trovano uso in diversi ambienti.

15.3 Pregi

Rilevare semplicemente l'errore permette di diminuire la quantità di bit dati. Tuttavia rilevazione e correzione permette un minor numero di invii, e permette la ricostruzione autonoma del frames.

15.4 Difetti

La semplice rilevazione non permette la ricostruzione del dato, la rilevazione e correzione però necessita del doppio dei bit per poter essere attuata.

15.5 Ambiti d'uso

Strato data-link.

Nelle reti wireless conviene utilizzare una codifica a correzione dell'errore, così da ricostruire il messaggio in casi d'errore (se si dovesse solo rilevare e richiedere un'altro invio, il rischio della presenza di nuovi errori sarebbe alta, quindi conviene usare questa).

Nelle LAN invece, in cui gli errori sono più sporadici, è più conveniente utilizzare spesso quella a rilevazione, con conseguente richiesta di re-invio.

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

16.1 Cos'è?

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

Quando si utilizza una codifica di questo tipo, sorgente e destinazione devono mettersi d'accordo in anticipo su un polinomio generatore G(x). Che deve avere i bit di ordine più alto e più basso a "1". Per poter calcolare il checksum di un frame di m bit, quest'ultimo dev'essere più lungo del polinomio generatore. L'idea è quella di aggiungere un checksum alla fine del frame in modo che il polinomio rappresentato dal frame con checksum sia divisibile per G(x). Quando la destinazione riceve il frame con il checksum e prova a dividerlo per G(x). Se c'è un resto vuol dire che c'è stato un errore di trasmissione.

16.2 Esempio

Ora proviamo con l'esempio di un frame 10011101 con polinomio generatore $x^4 + x + 1$: Frame: 1 0 0 1 1 1 0 1 Generatore G(x): 1 0 0 1 1 Il grado di G(x) è 4, aggiungo 4 "0" al frame (ottenendo un nuovo frame M(x)) in modo da poter dividere le due parti ottenendo il resto da sottrarre al M(x). M(x)= 1 0 0 1 1 1 0 1 0 0 0 0 Effettuo la divisione:

```
10011 | 100111010000
      10011
      ---
      00
      00
      ---
      101
      000
      ---
      1010
      0000
      ---
      10100
      10011
      ---
      1110
      0000
      ---
      11100
      10011
      ---
      1111
```

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

16.3 Pregi

Richiede conoscenze matematiche modeste, è semplice da realizzare ed ha un ottimo grado di rilevazione degli errori su linee con elevato rumore di fondo.

16.4 Difetti

Purtroppo è utile solo per errori causati da interferenze, rumore o distorsione. L'algoritmo diventa inutile di fronte a tentativi intenzionali di manomissione dei dati.

16.5 Ambiti d'uso

Strato data-link.

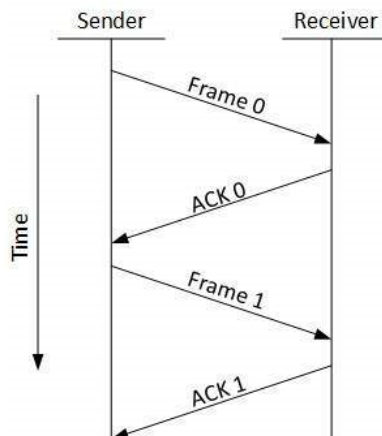
Utilizzato per individuare errori casuali nella trasmissione di dati. Per i tentativi intenzionali di manutenzione è meglio utilizzare algoritmi di hash quali MD5 e SHA1.

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

Durante la ricezione dei dati, il frame viene controllato, e a seconda se è integro o meno, si segue uno dei tre diversi protocolli più comuni: Stop-and-wait è il più semplice tra questi.

17.1 Cos'è?

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



17.2 Prego

Permette di gestire i pacchetti ricevuti, corretti o danneggiati, per poi passarli allo strato network.

17.3 Difetti

Perdita di dati, lentezza generale, limitato uso del canale di comunicazione. Senza l'utilizzo di piggybacking, o tecniche avanzate, questo protocollo risulta essere estremamente lento e che, a causa della mancata numerazione dei pacchetti, rischia di farne perdere numerosi.

17.4 Ambiti d'uso

Strato data-link.

Effettivamente questo protocollo non viene utilizzato a causa della parecchia inefficienza rispetto ad altri protocolli.

18 Cos'è il piggybacking?

Molti protocolli di comunicazione necessitano di inviare l'ACK come segnale di avvenuta ricezione del frame. Fatto per ogni singolo frame, questo invio rischia di intasare inutilmente il canale di comunicazione, allungando i tempi e incorrendo in molteplici errori.

18.1 Cos'è?

La tecnica del piggybacking permette di aggiungere l'ACK al frame di dati in uscita, utilizzando il campo ack nell'intestazione di questo. In questo modo l'acknowledgement si procura un passaggio gratis insieme al successivo frame dati trasmesso. Questo avviene quando arriva un frame di dati, la destinazione non invia subito un frame di controllo separato, ma aspetta che lo strato network gli passi il successivo pacchetto. Un problema può sorgere in caso di attesa molto lunga del pacchetto, poiché si rischia di far scattare il timer del mittente che re-invia il frame nell'attesa dell'ACK, in questo caso si decide un timeout in modo tale da fare piggybacking nel caso in cui il pacchetto da inviare è pronto in tempi celeri, altrimenti si invia l'ACK in modo indipendente.

18.2 Pregi

Miglior uso della banda disponibile. E visto che l'ACK viene inglobato nel frame e non inviato singolarmente, la banda viene meno congestionata.

18.3 Difetti

In caso di attesa eccessiva del pacchetto dallo strato network, l'ACK potrebbe non venire mai inviato, in quel caso non si attende e si invia l'ACK singolarmente.

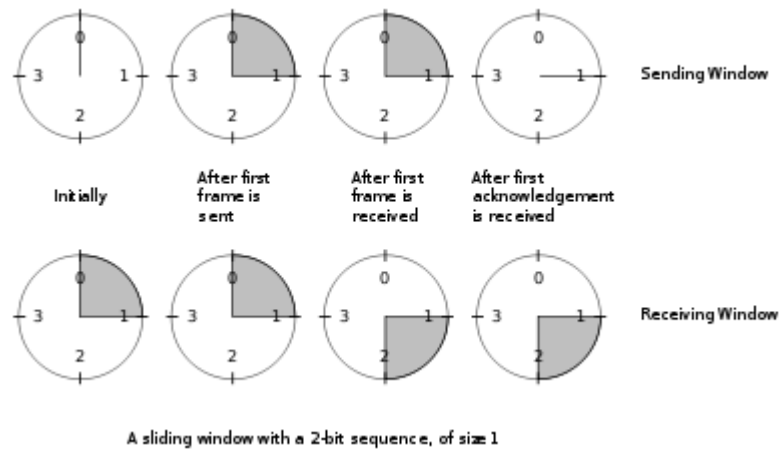
18.4 Ambiti d'uso

Utilizzato in molti protocolli di comunicazione che necessitano della conferma della ricezione di un determinato messaggio attraverso un ACK. Nelle reti LAN è molto adatta.

19 Si descriva la tecnica dello Sliding window

19.1 Cos'è?

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



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

19.2 Pregi

Questa classe di protocolli permette di sfruttare al meglio la banda sia in entrata che in uscita, i veri pregi si hanno in base alle dimensioni delle finestre invio/ricezione implementate dai diversi protocolli che sfruttano questa tecnica.

19.3 Difetti

—

19.4 Ambiti d'uso

Utilizzato prevalentemente dal protocollo TCP nei meccanismi di controllo di flusso e della congestione.

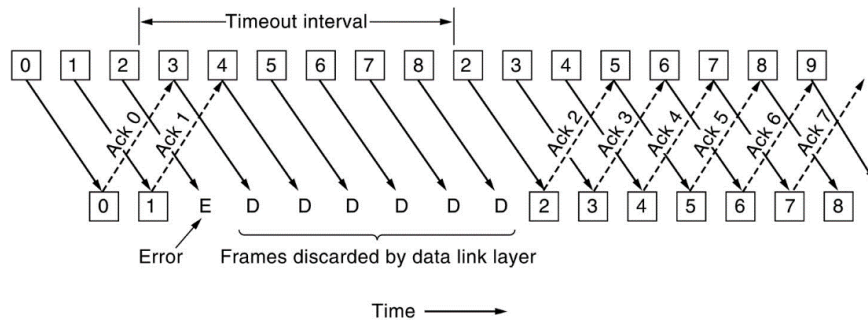
20 Si descriva l'idea dei protocolli "go back N", indicandone pregi e difetti

Il problema di ricezione dell'ack per ogni frame inviato, limitava di molto l'utilizzo della banda e rallentava le comunicazioni, per ovviare a questo

problema viene usata la tecnica di pipelining. Si decide quindi di inviare più frame prima di ricevere i vari ack aumentando di parecchio l'utilizzo della linea. Tuttavia, sorge un problema, cosa succede nel caso in cui si perdano dei frames? Per il ripristino degli errori in presenza di pipelining sono disponibili due approcci base. Tra questi go back n.

20.1 Cos'è?

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



20.2 Pregi

Grazie all'invio a raffica senza attendere l'ack corrispondente, questo protocollo ottimizza in maniera eclatante l'uso della banda (in caso di pochi

errori (nulli)).

20.3 Difetti

Può far perdere molta banda in caso di un'alta frequenza di errori.

20.4 Ambiti d'uso

Viene utilizzato in base alle risorse disponibili, in particolare, nei sistemi in cui la finestra di ricezione è scarsa, e la finestra di invio è più grande.

21 Si descriva cos'è la tecnica del selective repeat

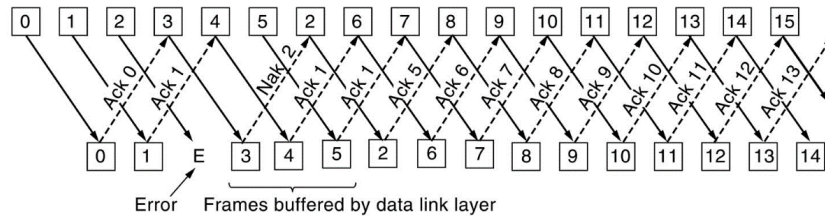
Il problema di ricezione dell'ack per ogni frame inviato limitava di molto l'utilizzo della banda e rallentava le comunicazioni. Per ovviare a questo problema viene usata la tecnica di pipelining. Si decide quindi di inviare più frame prima di ricevere i vari ack aumentando di parecchio l'utilizzo della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

21.1 Cos'è?

Con il selective repeat, quando viene ricevuto un frame in errore viene scartato, mentre i frame buoni ricevuti successivamente vengono salvati in un buffer; quando la sorgente va in timeout, solo il frame più vecchio senza ACK viene ritrasmesso. Se quel frame arriva correttamente, la destinazione può passare in sequenza allo strato network tutti i frame presenti nel buffer.

La ripetizione selettiva può inviare dei NACK (Not acknowledgement) quando trova un errore, così da stimolare la ritrasmissione prima dello scadere del timer. La ripetizione selettiva corrisponde ad avere una finestra di ricezione maggiore di 1.

Go back-n e il selective repeat hanno diverse conseguenze in termini di uso di banda e di spazio di buffer nello strato data link. Si può utilizzare un approccio o l'altro in base a quale risorsa è più scarsa.



21.2 Pregi

Aumentano di molto le performance, soprattutto grazie ai NACK che stimolano la ritrasmissione prima dello scadere del timer.

21.3 Difetti

Essendo una ricezione non sequenziale c'è il rischio che gli intervalli della prima finestra si sovrappongano con la successiva, e se Murphy attacca, si rischia di inviare allo strato network un pacchetto fallato. (è difficilotta da buttare giù vedi pag 226 del libro.).

21.4 Ambiti d'uso

Utilizzato in base alla disponibilità delle risorse, finestra di ricezione maggiore di 1.

22 Descrivere la differenza tra ALOHA e ALOHA-SLOTTED

22.1 Cos'è ALOHA?

ALOHA è un protocollo di rete per garantire le funzionalità di accesso multiplo al mezzo di trasmissione dati condiviso tra più utenti. Esistono due tipi di reti: quelle che utilizzano le connessioni punto-punto e quelle che usa canali broadcast; questo protocollo viene utilizzato per le seconde.

Inventato negli anni '70 nelle Hawaii, l'idea di fondo è di consentire agli utenti di trasmettere ogni volta che hanno dati da inviare. Questo naturalmente genera collisioni, tuttavia i canali broadcast danno la possibilità di verificare se il frame trasmesso è stato ricevuto correttamente o no; la stazione trasmittente ascolta il canale e determina il successo o insuccesso della

trasmissione. Le stazioni attendono un tempo variabile prima di provare a ritrasmettere un frame non andato a buon fine. Il successo dell'ALOHA puro è di circa 18%.

22.1.1 Pregi

Permette l'accesso multiplo allo stesso mezzo di trasmissione condiviso da più utenti (broadcast). (pregio?)

22.1.2 Difetti

Poco efficiente in comunicazioni con tante stazioni.

22.1.3 Ambiti d'uso

Protocollo di livello MAC, questo protocollo non è attualmente utilizzato. Creato tuttavia per l'utilizzo nelle connessioni di tipo broadcast, in cui il mezzo trasmissivo è condiviso da più di due punti.

22.2 Cos'è ALOHA Slotted?

Il protocollo Slotted ALOHA aggiunge al protocollo sopracitato la divisione del tempo in intervalli discreti, chiamati slot. Ogni stazione viene vincolata a cominciare la propria trasmissione solo all'inizio di uno slot temporale, se una stazione è pronta ad un certo istante, dovrà necessariamente attendere l'inizio dello slot successivo.

Lo svantaggio di questo protocollo è la necessità di un meccanismo di sincronizzazione che indichi alle varie stazioni quando possono cominciare la trasmissione. Questa divisione in slot migliora il grado di successo del doppio rispetto all'ALOHA puro, circa 36%.

Questi risultati non dovrebbero sorprendere, in quanto con stazioni che trasmettono a piacimento è molto facile incorrere in collisioni.

Questi protocolli caddero in disuso, fino a quando non si presentò il problema di allocare un canale condiviso da più utenti in competizione (ad esempio dopo l'invenzione dell'accesso ad Internet via cavo), di conseguenza slotted ALOHA tornò ad essere utilizzato.

22.2.1 Pregi

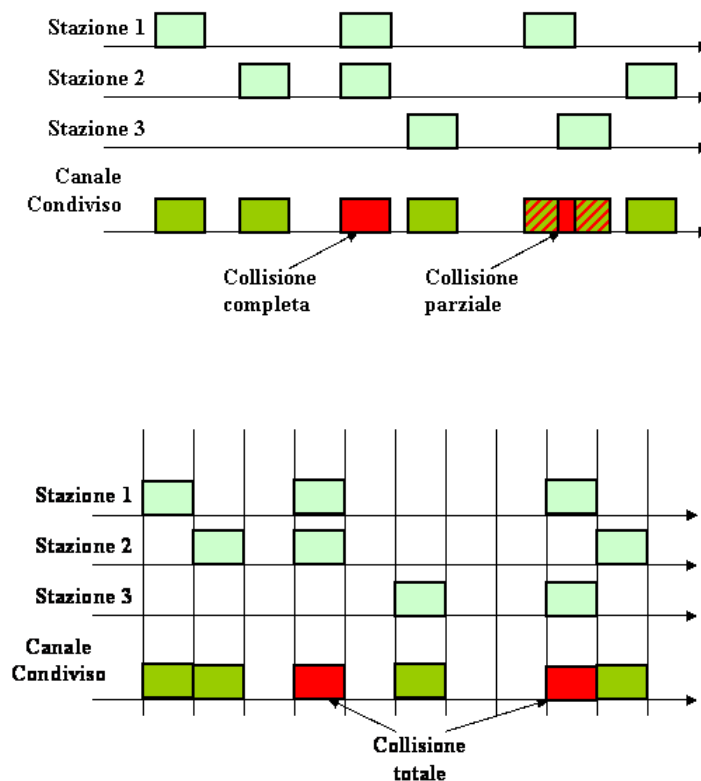
Migliora l'ALOHA puro, aumentando il grado di successo di circa il doppio.

22.2.2 Difetti

Necessita di un meccanismo di sincronizzazione che indichi alle varie stazioni quando trasmettere.

22.2.3 Ambiti d'uso

Protocollo di livello MAC, utilizzato nelle connessioni broadcast per condividere lo stesso mezzo trasmissivo da più utenti.



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

I protocolli ALOHA e le sue varianti permettevano di inviare dati ogniqualvolta si voleva, limitando però le percentuali di successo. Per migliorare i risultati di accesso multiplo ad un mezzo di trasmissione condiviso, vengono implementati protocolli in cui le stazioni rimangono in ascolto di una

portante e si comportano di conseguenza. Questi protocolli sono chiamati protocolli con rilevamento della portante.

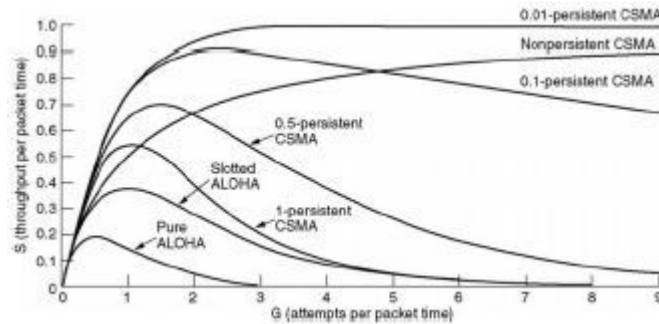
23.1 Cos'è?

Il CSMA è una tecnica di trasmissione dati che si basa su questi principi. Ogni dispositivo prima di avviare la trasmissione dei dati deve verificare se altri nodi stanno trasmettendo sul canale, rilevando la portante. Se il canale è libero iniziano a trasmettere, altrimenti attendono un tempo arbitrario prima di riprovare. Esistono diverse versioni di CSMA:

- CSMA 1-persistente: è il primo tra i protocolli CSMA, ha la particolarità di inviare con probabilità 1 sul canale in caso di nessun rilevamento. Questo migliora sicuramente ALOHA puro, tuttavia l'ingordigia di inviare non appena si libera il canale non rende immuni dalle collisioni, che potrebbero accadere in caso di stazioni che controllano nello stesso momento un canale vuoto e inviano contemporaneamente.
- CSMA non persistente: prima di trasmettere ogni stazione controlla il canale. Se lo trova libero inizia ad inviare i dati, ma se il canale è occupato la stazione non esegue un controllo continuo per trasmettere subito il proprio frame; invece attende per un intervallo casuale prima di ripetere l'algoritmo. Questo meccanismo permette di utilizzare meglio il canale ma allunga i ritardi.
- CSMA p-persistente: questa variante si applica su canali divisi in intervalli temporali. Quando è pronta a trasmettere, ogni stazione controlla il canale. Se lo trova libero, trasmette subito con una probabilità p , e rimanda fino all'intervallo successivo con probabilità $q=1-p$. Se anche quell'intervallo risulta libero la stazione trasmette oppure rimanda un'altra volta. Il processo si ripete finché il frame non è stato trasmesso.

Queste varianti migliorano enormemente il tasso di successo rispetto ad ALOHA e ALOHA-slotted.

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



23.2 Pregi

Migliora di molto le prestazioni di ALOHA e ALOHA-SLOTTED, un ulteriore miglioramento si ha quando si annulla la propria trasmissione in caso di collisione, così da risparmiare tempo e banda.

23.3 Difetti

—

23.4 Ambiti d'uso

CSMA/CA è utilizzato prevalentemente nelle connessioni in cui il rilevamento delle collisioni non è realizzabile, come le reti senza fili. Utilizzato nello standard IEEE 802.11. Una variante migliorante, che rileva le collisioni è il CSMA/CD il quale è utilizzato nelle LAN Ethernet.

24 Basic Bitmap

Nella gestione di accesso multiplo ad un mezzo di trasmissione condiviso, esistono diversi protocolli che gestiscono l'accesso gestendo le collisioni e garantendo l'accesso (ALOHA, slotted ALOHA, CSMA), tuttavia le collisioni sono sfavorevoli alle prestazioni del sistema, specialmente quando il cavo è lungo e i frame corti.

24.1 Cos'è?

Esistono protocolli che garantiscono la gestione degli accessi senza collisione, uno tra questi è il basic Bitmap (metodo a mappa di bit elementare). In questo protocollo ogni periodo di contesa è composto esattamente da N

intervalli ($N = \#$ stazioni). Ogni stazione è numerata, e se ha un frame da inviare deve inviare un “1” nell’intervallo corrispondente al suo numero. A nessun’altra stazione è concesso di trasmettere durante questo intervallo. Così facendo ogni stazione si “prenota” l’intervallo di trasmissione. Una volta trascorsi gli N intervalli, ogni stazione sa quali sono le stazioni che vogliono trasmettere, di conseguenza non ci sarà mai alcuna collisione. Questo è anche chiamato protocollo a prenotazione.

24.2 Pregi

Garantisce che non ci siano collisioni durante l’utilizzo di un canale condiviso.

24.3 Difetti

Protocollo sbilanciato, dà priorità alle stazioni con un numero basso, se una stazione “ i ” e una “ j ” vogliono trasmettere e $i < j$ allora i si aggiudica la posizione.

Contemporaneamente però le stazioni numerate con numeri bassi dovranno attendere di più rispetto a quelle con numeri più alti.

Ha bisogno di 1 bit di controllo per stazione, in reti con migliaia di utenti non è molto adatto.

24.4 Ambiti d’uso

Protocollo dello strato MAC.....

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

I dati vengono trasportati tramite un impulso elettrico. Ci possono essere molti dispositivi collegati allo stesso cavo con il rischio di collisioni e danneggiamento dei dati. Per evitare la collisione una stazione deve controllare se ci sono altre stazioni collegate allo stesso mezzo; esistono diversi protocolli che effettuano questo controllo evitando le collisioni. Il basic bitmap è uno di questi, tuttavia risulta elementare e su reti composte da molte stazioni risulta poco utilizzabile.

25.1 Cos'è?

Il collision free binary countdown o conteggio binario migliora il basic bitmap, utilizzando un sistema di assegnazione della linea in base ad una stringa binaria. Una stazione che desidera utilizzare il canale deve comunicare a tutti il proprio indirizzo sotto forma di stringa binaria, hanno tutti la stessa lunghezza.

I conflitti si evitano grazie ad una regola di arbitraggio: la stazione rinuncia ad inviare non appena si accorge che un'altra stazione con un "1" in una posizione di bit di ordine elevato che nel proprio indirizzo vale "0". Esempio: 0010, 0100, 1001, 1010, queste stazioni vogliono inviare, vengono inviati i primi bit: 0 (0010), 0 (0100), 1 (1001), 1 (1010), le stazioni con "0" più a sinistra capiscono che ci sono stazioni con numero più grande che stanno concorrendo e si fanno da parte, le altre due continuano: 0 (1001), 0 (1010); sono uguali quindi continuano, il terzo bit è "1" quindi la stazione 1001 si arrende, vince 1010 che può trasmettere.

L'efficienza è pari a $(d/d * \log_2 N)$ (con d numero di bit) ma può raggiungere anche il 100% se l'indirizzo del mittente costituisce l'intestazione del frame.

Si può notare uno sbilanciamento notevole in quanto le stazioni con numero maggiore risultano avere sempre la precedenza. Questo può essere ovviato facendo ruotare i valori delle stazioni ad ogni step, così quando una stazione riesce ad inviare viene spostata alla fine della coda, in modo da permettere a tutte le stazioni la possibilità di inviare.

Questo algoritmo è semplice, elegante ed efficiente, tuttavia attualmente non è utilizzato.

25.2 Pregi

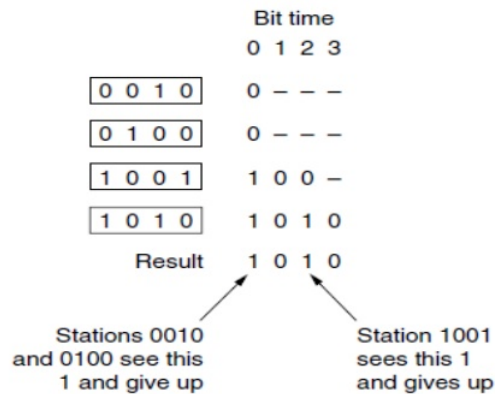
Migliora il problema della scarsa efficienza in caso di molte stazioni del basic bitmap. Garantisce comunicazioni senza collisioni. Ad alto carico l'efficienza del canale migliora.

25.3 Difetti

Da priorità alle stazioni con numero maggiore, con conseguente sbilanciamento. Problema risolto facendo ruotare i valori delle stazioni ad ogni step. A basso carico hanno un ritardo elevato.

25.4 Ambiti d'uso

Protocollo dello strato MAC. Attualmente non utilizzato.



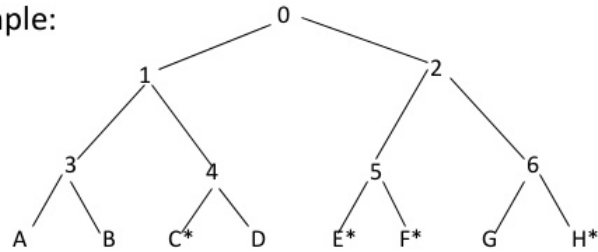
26 Spiegare cos'è l'adaptive tree walk protocol?

Per gestire la contesa di accesso ad un canale condiviso esistono protocolli con controllo della portante, con metodo della contesa tipo il CSMA o il metodo senza collisioni. Nelle situazioni di carico leggero la contesa è preferibile per il suo basso ritardo, tuttavia a carichi elevati diventa sempre più inefficiente. Il contrario avviene con i protocolli senza collisioni, a basso carico hanno un ritardo elevato ma al crescere del carico l'efficienza migliora.

26.1 Cos'è?

Adaptive tree walk protocol è un protocollo a contesa limitata che migliora ulteriormente le prestazioni dei protocolli sopracitati. Si può immaginare questo metodo come un albero binario, in cui le stazioni sono le foglie e sono divise nei vari rami. Inizialmente si prova a inviare ad altezza 0: se non vi è collisione si procede all'invio, in caso contrario ci si sposta sul sottoalbero sinistro e si ritenta; se il conflitto non c'è più si fa inviare la stazione che lo desidera (se non c'è conflitto vuol dire che nel sottoalbero sinistro c'è solo una stazione che vuole inviare). Dopo aver inviato si torna al nodo padre e si analizza il sottoalbero destro, ripetendo i test e scendendo nei sottoalberi in caso di conflitto.

Example:



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

26.2 Pregi

Garantisce un ritardo limitato in caso di basso carico e una buona efficienza in caso di carico più elevato.

26.3 Difetti

—

26.4 Ambiti d'uso

Utilizzato nelle connessioni con più stazioni che vogliono trasmettere nello stesso mezzo di trasmissione.

27 Ethernet e i vari tipi di cavo

27.1 Cos'è?

Ethernet è il sistema LAN più diffuso al mondo, è economico e facile da usare e la diffusione delle componenti hardware ne ha facilitato l'adozione. È adeguata all'utilizzo con TCP/IP.

Nasce con l'intento di ottenere una trasmissione affidabile su cavo coassiale in condizioni di traffico contenuto, ma in grado di tollerare possibili picchi di carico. Per regolamentare l'accesso al mezzo trasmissivo era stato adottato un protocollo di accesso multiplo del tipo CSMA/CD.

Il nome Ethernet si riferisce al cavo (definito "etere"). Andiamo quindi ad elencare le tipologie di cavi utilizzati in questo standard. Generalmente vengono utilizzati 4 tipi di cavo.

27.2 10base5

Il più vecchio è il modello 10base5 chiamato anche thick Ethernet. Questo cavo assomiglia ad un tubo giallo con segni a intervalli di 2,5m che indicano la posizione delle spine. Le connessioni sono generalmente realizzate mediante spine a vampiro (spilli spinti nel nucleo centrale del cavo coassiale). La notazione 10Base5 indica che opera a 10Mbps, utilizza un sistema di segnali a banda base e può supportare segmenti lunghi fino a 500m. Questo cavo è ormai obsoleto.

27.3 10base2

Il secondo cavo in ordine di tempo è stato il cavo 10base2 o thin Ethernet, più facile da piegare rispetto al precedente e le connessioni sono realizzate usando connettori BNC (giunzioni a "T" più affidabili e facili da usare rispetto alle spine a vampiro). Il thin Ethernet è più economico e semplice da installare, però può essere lungo al massimo 185 metri e può supportare non più di 30 macchine.

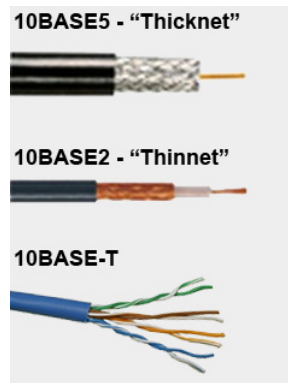
27.4 10base-T

Per trovare guasti in questi mezzi è usata la tecnica TDR (Time Domain Rectory) che sostanzialmente misura il ritardo dell'eco dell'impulso immesso nel cavo. La tecnica TDR per la ricerca di guasti è difficile e onerosa da utilizzare, ci si è spostati quindi sulla terza tipologia di cablaggio 10Base-T, ormai diventata uno standard grazie alla facilità di gestione e all'uso di cablaggi preesistenti.

Questo sistema di cablaggio utilizza hub di controllo tramite doppipli telefonici, che sono largamente usati e semplici da gestire, ogni macchina si interfaccia con l'hub tramite cavo dedicato, rendendo così semplice aggiungere o rimuovere una stazione e individuare le interruzioni. Il suo svantaggio è rappresentato dalla lunghezza massima dei cavi che partono dall'hub: 100 metri. Esiste una versione più veloce del 10Base-T chiamata 100Base-T.

27.5 10base-F

Il quarto tipo di cavi per Ethernet si chiama 10base-F e utilizza le fibre ottiche. È un'alternativa costosa a causa del prezzo dei connettori e dei terminatori, ma offre un'eccellente immunità alle interferenze e consente di collegare edifici o hub molto lontani. 10Base-F nonostante il costo consente inoltre una buona sicurezza in quanto i dati trasmessi sulla fibra sono difficili da intercettare.



27.6 Pregi

Sistema LAN più diffuso, economico e facile da utilizzare. I primi due tipi di cavo non vale la pena analizzarli perchè ormai sono obsoleti, i 10base-T sono sicuramente più economici rispetto ai 10base-F che tuttavia provvedono a garantire un'eccellente immunità alle interferenze e una velocità molto superiore alla controparte in rame. Grazie all'utilizzo degli hub i guasti sono semplici da localizzare e correggere.

27.7 Difetti

I 10base-T hanno una lunghezza massima molto limitata: 100 metri dall'hub. I 10base-F costano molto.

27.8 Ambiti d'uso

I primi due non sono utilizzati, il 10base-T è diventato una tipologia standard di cablaggio nello standard Ethernet, i 10base-F vengono utilizzati largamente in tutte le nuove reti ad alta velocità.

28 Codifica Manchester

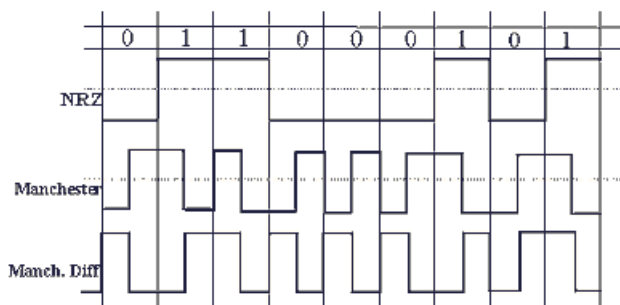
La codifica binaria del segnale “0” viene indicato con 0 volt mentre “1” utilizzando 5 volt, questo fa sorgere numerosi problemi, in quanto altre stazioni potrebbero interpretare erroneamente il segnale (a causa degli 0 volt, una stazione potrebbe confondere l’assenza del segnale con uno “0”). Si può passare a +1 volt per “1” e -1 volt per “0”, ma rimane il problema dei ricevitori che possono campionare il segnale in maniera diversa. Per risolvere questo problema sono state inventate due tecniche implementate in Ethernet: codifica Manchester e codifica Manchester differenziale.

28.1 Codifica Manchester cos’è?

Queste codifiche sono dette auto-sincronizzanti in quanto non necessitano di un segnale di sincronia esterno. Queste codifiche suddividono ogni bit codificato in due, nella codifica Manchester lo “0” viene rappresentato da un segnale Basso-Alto, mentre l’”1” viene rappresentato da un segnale Alto-Basso (esistono due convenzioni opposte riguardo la rappresentazione dei segnali “1” e “0”). Così facendo anche in caso di dissincronia, i dati in questo formato permettono un flusso auto-sincronizzante.

28.2 Codifica Manchester differenziale cos’è?

La codifica Manchester differenziale invece differisce da quella originale nella rappresentazione dei bit: questa infatti si basa sulla verifica di transizioni all’inizio di un intervallo. La presenza di una di queste infatti (che siano alto-basso o basso-alto) identifica un valore, la mancanza di transizione invece indica il valore opposto. Per convenzione il bit 1 viene rappresentato dalla mancanza di transizione all’inizio del suo intervallo, mentre lo 0 è indicato con un cambiamento di segnale nello stesso periodo.



28.3 Pregi

Si risolve il problema di ambiguità dovuto al segnale 0 volt=bit 0. Queste codifiche permettono l'auto sincronizzazione del segnale.

28.4 Difetti

Occupano il doppio della banda della codifica binaria elementare, perchè gli impulsi sono larghi la metà.

28.5 Ambiti d'uso

Tutti i sistemi Ethernet adottano la codifica Manchester perché è più semplice, mentre la Manchester differenziale è utilizzata da altre LAN.

29 Cos'è il binary exponential backoff?

La caratteristica principale del CSMA/CD (algoritmo che controlla il canale prima di trasmettere ed evita le collisioni analizzando la portante) è che una volta rilevata una collisione, si attende un intervallo prima di ritrasmettere. Questo intervallo viene calcolato ogni volta tramite l'algoritmo di backoff esponenziale.

29.1 Cos'è?

Dopo una collisione il tempo viene diviso in intervalli discreti, la cui lunghezza è uguale al tempo di propagazione di andata e ritorno del caso peggiore sul mezzo di trasmissione. Dopo la prima collisione, ogni stazione aspetta 0

o 1 intervalli temporali prima di ritentare. Se due stazioni collidono e ognuna sceglie lo stesso numero casuale, la collisione si ripeterà. Dopo la seconda collisione ogni stazione sceglie 0, 1, 2 o 3 a caso e rimane in attesa per quel numero di intervalli temporali. In generale quindi, dopo le collisioni, viene scelto un numero casuale compreso tra 0 e 2^i-1 e si salta quel numero di intervalli. Il limite di collisioni è 16, dopodiché il chip di controllo getta la spugna e manda un errore.

29.2 Pregi

Si adatta dinamicamente al numero di stazioni che tentano di trasmettere. Assicura un basso ritardo quando poche stazioni collidono e garantisce un intervallo di tempo ragionevole quando invece la collisione coinvolge molte stazioni

29.3 Difetti

—

29.4 Ambiti d'uso

Utilizzato nel protocollo di accesso multiplo CSMA/CD, e serve per decidere/calcolare il tempo di entrata di una stazione nel canale (dopo una collisione).

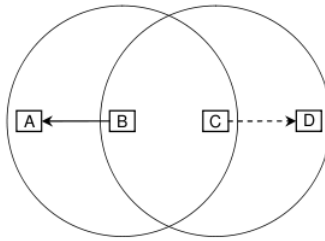
30 Stazione nascosta e stazione esposta: cosa sono e cosa fanno?

Al crescere del numero di computer e dispositivi mobili aumenta anche la domanda di collegare tali apparecchi al mondo esterno. Nascono così le LAN wireless, le quali permettono la connessione dei dispositivi senza bisogno di cavi.

Tuttavia, questo porta a dei problemi di conflitto in caso di scambio di dati. Utilizzando banalmente il sistema CSMA per evitare le collisioni, si arriverebbe ad ascoltare le altre trasmissioni, e trasmettere in caso di nessun'altra connessione attiva. Questo però può portare a due diversi problemi: problema della stazione nascosta e stazione esposta.

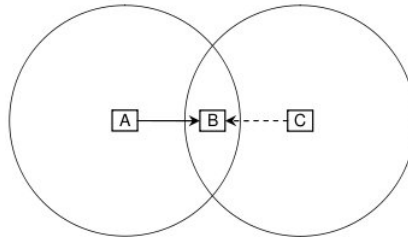
30.1 Stazione nascosta, cos'è?

La stazione nascosta non è altro che una stazione che vuole inviare, ma non riesce a ricevere i segnali dei concorrenti a causa della sua distanza eccessiva. Supponiamo di avere A, B e C. A vuole inviare a B e prima di farlo ascolta se ci sono altre connessioni; non ne sente e procede all'invio. Tuttavia, C, è troppo distante perché A lo senta, ma abbastanza vicino a B per inviargli dati, così lo fa e va in conflitto con l'invio di A.



30.2 Stazione esposta, cos'è?

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



31 Bluetooth

31.1 Cos'è?

Bluetooth è uno standard wireless che permette il collegamento di dispositivi di calcolo, di comunicazione e accessori vari mediante un sistema radio wireless a basso costo, bassa potenza e portata ridotta.

L'unità di base di un sistema Bluetooth è la piconet, composta da un nodo master e da diversi nodi slave (non più di 7), situati nel raggio di 10 metri. Più piconet possono trovarsi nella stessa stanza e possono essere collegate tramite un nodo ponte; un insieme di piconet è chiamato scatternet.

Tutto si basa sulla comunicazione tra nodo master e nodo slave. Il master controlla il clock e decide quale dispositivo può comunicare in ogni intervallo temporale.

I tipi di collegamenti si suddividono in due tipi principali: orientati alla connessione o senza connessione. Il primo richiede di stabilire una connessione tra i dispositivi prima di inviare i dati, mentre in quello senza connessione il trasmettitore può in qualsiasi momento iniziare a inviare i propri pacchetti purché conosca l'indirizzo del destinatario.

Bluetooth definisce inoltre due tipi di collegamenti a supporto delle applicazioni voce e trasferimento dati: un servizio asincrono senza connessione (ACL) ed un servizio sincrono orientato alla connessione (SCO). ACL supporta il traffico dati e si basa su un servizio di tipo best-effort (ovvero un servizio che non dà alcuna garanzia dell'effettiva consegna dei dati né tantomeno livelli di qualità o priorità garantiti). Supporta connessioni a commutazione di pacchetto, connessioni punto-multipunto (multicast) e connessioni simmetriche o asimmetriche. SCO invece è un collegamento che supporta connessioni con un traffico di tipo real-time e multimediali, prevede connessioni a commutazione di circuito, connessioni punto-punto e connessioni simmetriche.

Bluetooth ha protocolli raggruppati in strati, che non seguono né modello OSI né TCP/IP.

32 Si descriva l'algoritmo statico Flooding

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. Lo strato network sfrutta particolari algoritmi detti algoritmi di routing per instradare correttamente i pacchetti nei vari percorsi. Esistono diversi modi per farlo, in quanto ci sono molti fattori da tenere in considerazione, però possiamo suddividerli in due grandi tipi: algoritmi non adattivi e algoritmi adattivi.

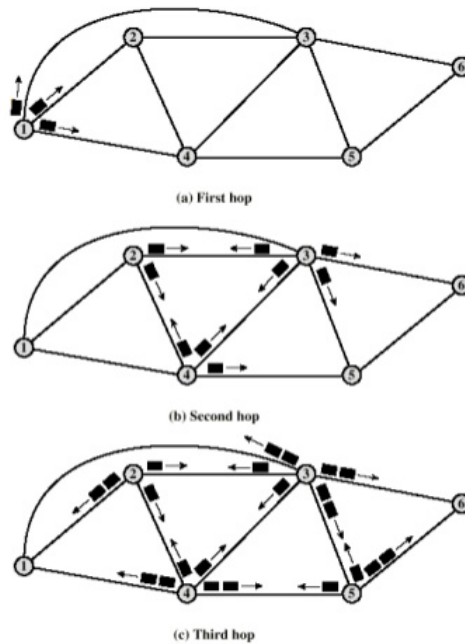
Gli algoritmi non adattivi basano le loro decisioni su misure e stime del traffico e della topologia corrente, viene calcolato il percorso all'avvio della rete, in modalità fuori linea e viene scaricato nei router. Questa procedura si chiama anche routing statico. Gli algoritmi adattivi invece cambiano le loro decisioni secondo le modifiche apportate alla topologia e al traffico.

32.1 Cos'è?

L'algoritmo di Flooding è un algoritmo statico, in cui ogni pacchetto in arrivo è inviato a tutte le linee tranne quella da cui proviene.

Una variante un po' più pratica è chiamata flooding selettivo. In questo algoritmo i router non trasmettono ogni pacchetto verso tutte le linee, ma solo attraverso quelle che vanno approssimativamente nella direzione corretta. Nella maggior parte delle applicazioni questo algoritmo non è molto utilizzato, salvo casi particolari (i militari lo utilizzano, in quanto un gran numero di router potrebbero saltare in aria, aver questo metodo di trasmissione di pacchetti accerta la ricezione dei dati).

Questo algoritmo viene utilizzato anche come metrica di confronto per altri algoritmi di routing, in quanto sceglie sempre il percorso più breve (scegliendoli tutti LOL), di conseguenza nessun algoritmo può produrre un ritardo più breve (ignorando il tempo di elaborazione dati generato dal processo di flooding).



32.2 Pregi

Semplice da attuare e assicura la ricezione del pacchetto alla stazione desiderata.

32.3 Difetti

Spreco evidente di banda, pacchetti duplicati e rischio di cicli infiniti.

32.4 Ambiti d'uso

Strato Network. Questo algoritmo viene utilizzato come metrica di confronto per altri algoritmi di routing, in quanto sceglie sempre il percorso più breve (tra i molteplici). Utilizzato anche in ambito militare in quanto la duplicazione dei pacchetti può essere una nota positiva a causa del rischio di bombardamenti.

33 Descrivere il distance vector routing

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. Per fare questo vengono utilizzati diversi algoritmi che si possono raggruppare in due grandi gruppi: algoritmi adattivi e non adattivi. Gli algoritmi non adattivi sono anche detti statici, in quanto basano i loro calcoli sulla rete "a freddo" senza tener conto del carico istantaneo o dei problemi di linea; un esempio è l'algoritmo di Flooding.

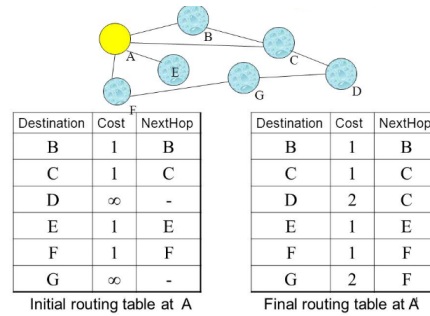
Generalmente le moderne reti di computer utilizzano algoritmi adattivi, o dinamici se vogliamo. Tra i più popolari ci sono il distance vector routing e il linkstate routing.

33.1 Cos'è?

Gli algoritmi di routing basati sul vettore delle distanze (distance vector routing) operano facendo in modo che ogni router conservi una tabella (vettore) che definisce la miglior distanza conosciuta per ogni destinazione e la linea che lo conduce ad essa. Queste tabelle vengono aggiornate scambiando informazioni con i router vicini.

Questo algoritmo è basato sull'algoritmo di Bellman-Ford (che calcola i cammini minimi su un grafo). Ogni router misura la "distanza" (secondo una metrica che può includere vari fattori) che lo separa dai nodi adiacenti ricevendo i dati dai router vicini. A partire da tali dati, utilizzando l'algoritmo di Bellman-Ford, il router costruisce una tabella che associa ad ogni destinazione conosciuta la stima della distanza che lo separa dalla destinazione e il primo passo del percorso calcolato. Questo aggiornamento viene

fatto periodicamente e dopo sufficienti scambi ciascun router avrà una riga per ogni altro nodo nella rete.



33.2 Pregi

Ogni router ha il percorso migliore per arrivare a tutti i suoi nodi adiacenti.

33.3 Difetti

Impiega troppo tempo a raggiungere la convergenza.

Non tiene conto della banda della linea quando sceglie i percorsi.

Possibilità che si creino i cicli, potenzialmente infiniti.

33.4 Ambiti d'uso

Strato network per instradare i pacchetti ai vari router della rete, algoritmo adattivo (dinamico).

34 Descrivere Linkstate routing

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. Per fare questo vengono utilizzati diversi algoritmi che si possono raggruppare in due grandi gruppo: algoritmi adattivi e non adattivi. Gli algoritmi non adattivi sono anche detti statici, in quanto basano i loro calcoli sulla rete "a freddo" senza tener conto del carico istantaneo o dei problemi di linea; un esempio è l'algoritmo di Flooding.

Generalmente le moderne reti di computer utilizzano algoritmi adattivi, o dinamici se vogliamo. Tra i più popolari ci sono il distance vector routing e il linkstate routing.

34.1 Cos'è?

Gli algoritmi di routing basati sullo stato dei collegamenti (linkstate routing) è il sostituto del distance vector routing. L'idea di questo algoritmo si basa su 5 punti:

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

Un router, prima di tutto, cerca di scoprire chi sono i suoi vicini: lo fa inviando uno speciale pacchetto “HELLO” su ogni linea punto-punto; il router all'altro capo risponde fornendo la propria identità (si noti che i nomi devono essere globalmente unici, in quanto si necessita una non ambiguità durante lo scambio di pacchetti).

Il passo successivo è la misurazione del costo della linea, avviene tramite l'invio di uno speciale pacchetto “ECHO” al quale l'altra parte deve rispondere immediatamente, in base al tempo di andata/ritorno si può ottenere una stima ragionevole del ritardo.

Dopo aver raccolto le informazioni necessarie per lo scambio, ogni router deve costruire un pacchetto contenente tutti i dati. Il pacchetto inizia con l'identità del trasmittente, un numero di sequenza, l'età (contatore che viene decrementato ogni secondo, al raggiungere dello 0 le informazioni provenienti da quel router vengono scartate) e una lista dei vicini. Per ogni vicino è riportato il ritardo misurato. I pacchetti vengono creati periodicamente, oppure in caso di avvenimenti speciali: interruzione della linea o modifica/spengimento/accensione di un vicino.

La parte più delicata dell'algoritmo è la distribuzione affidabile dei pacchetti che contengono la descrizione dello stato dei collegamenti. Durante la distribuzione e l'installazione, i router che ricevono i primi pacchetti cambieranno i loro percorsi, rischiando di creare inconsistenze, cicli, computer irraggiungibili e così via. L'idea fondamentale è quella di utilizzare l'algoritmo di flooding (inviare ogni pacchetto ad ogni linea in uscita (tranne da dov'è arrivato)) un computer che riceve un pacchetto con le informazioni sullo stato della connessione:

- Se è duplicato il pacchetto viene scartato

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

Esistono diversi miglioramenti per questo metodo di distribuzione di pacchetti, ma sarebbe troppo lunga da elencare.

Dopo aver accumulato una serie completa di pacchetti sullo stato della connessione, il router può costruire l'intero grafo della sottorete, lo fa utilizzando localmente l'algoritmo di Dijkstra (algoritmo per la costruzione di grafi, simile a quello di Bellman-Ford, non può essere però utilizzato in caso di cammini negativi).

Questo algoritmo è molto utilizzato nelle reti reali in quanto può gestire reti composte da molti nodi, converge rapidamente al cammino minimo, difficilmente genera cicli ed è facile da comprendere in quanto ogni nodo ha la mappa completa della rete. Il principale svantaggio è la complessità di realizzazione, anche dovuta alla notevole capacità di memoria ed elaborazione richiesti dai router.

34.2 Pregi

Può gestire reti molto caotiche.
 Converge velocemente al cammino minimo.
 Difficilmente genera cicli.
 Facile da comprendere.

34.3 Difetti

Difficile da realizzare, a causa della notevole capacità di memoria ed elaborazione richiesta dai router.

34.4 Ambiti d'uso

Strato network, sostituito al distance vector routing. Molto utilizzato nelle reti attuali visti i numerosi pregi.

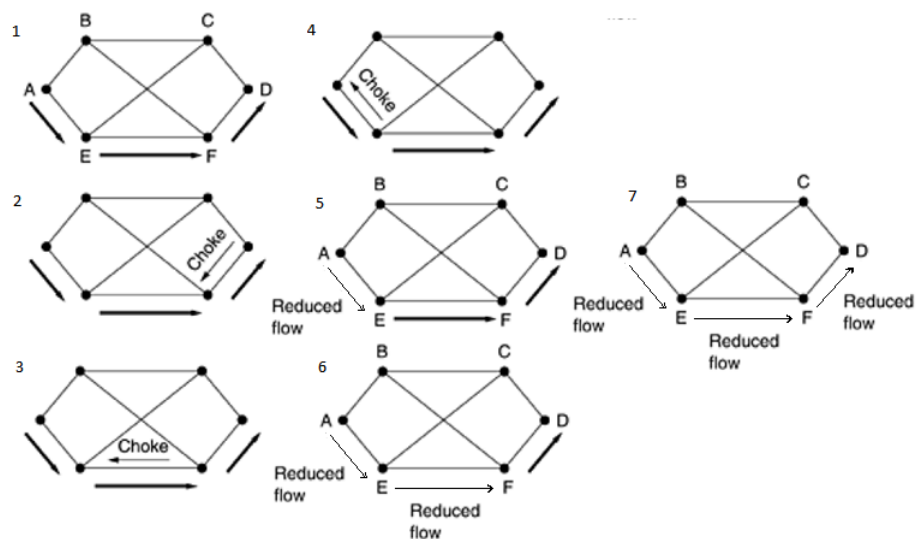
35 Choke packet

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. La decisione del mi-

glier percorso viene effettuato dagli algoritmi di routing (flooding, linkstate o distance vector). Purtroppo, per molteplici motivi, le reti potrebbero congestionarsi, più computer vogliono inviare pacchetti alla stessa destinazione che, non riuscendo ad elaborarli tutti ne perde, questo causa la ritrasmissione che causa ulteriori ingorghi. Questo problema è la congestione ed è un punto critico che va regolamentato.

35.1 Cos'è?

Il choke packet è uno speciale pacchetto utilizzato per il controllo di flusso in una rete. Un router che rileva una congestione, invia all'host originale del pacchetto un choke packet per avvertirlo di diminuire il flusso. Quando l'host sorgente riceve il pacchetto speciale diminuisce il flusso (tipicamente lo dimezza) e ignora i successivi choke packet (generalmente ne arrivano in rapida successione), passato un tempo prefissato l'host si rimette all'ascolto, se arrivano altri choke packet in quel frangente diminuisce ulteriormente il flusso, altrimenti riprende gradualmente la velocità normale.



35.2 Pregi

Permette di risolvere la congestione di una linea tramite l'uso di uno speciale pacchetto.

35.3 Difetti

Lento a reagire, purtroppo l'host produttore di pacchetti che genera la congestione, ci mette un certo tempo per ricevere il choke packet e prendere provvedimenti. Un miglioramento si ha con il Choke packet hop-by-hop (altro algoritmo per risolvere la congestione).

35.4 Ambiti d'uso

Strato network, algoritmo di controllo della congestione.

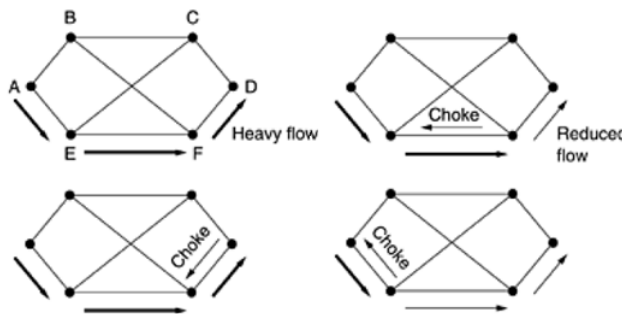
36 Choke packet hop-by-hop

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. La decisione del miglior percorso viene effettuato dagli algoritmi di routing (flooding, linkstate o distance vector). Purtroppo, per molteplici motivi, le reti potrebbero congestionarsi, più computer vogliono inviare pacchetti alla stessa destinazione che, non riuscendo ad elaborarli tutti ne perde, questo causa la ritrasmissione che causa ulteriori ingorghi. Questo problema è la congestione ed è un punto critico che va regolamentato.

36.1 Cos'è?

Il hop-by-hop choke packet è un miglioramento della sua versione precedente (choke packet). Choke packet aveva il problema di aver un tempo di reazione per prendere provvedimenti troppo lento, il che causava una grossa perdita di dati prima di risolvere il problema.

Hop-by-hop choke packet risolve questo problema limitando tutte le stazioni che attraversa in maniera immediata, senza dover attendere di arrivare all'host sorgente.



36.2 Pregi

Rispetto al choke packet originale, da sollievo più veloce alla rete.

36.3 Difetti

Richiede maggior utilizzo dei buffer di trasmissione nei router tra mittente e destinatario.

36.4 Ambiti d'uso

Strato network, algoritmo di controllo della congestione, miglioramento del choke packet.

37 Load shedding

La funzione principale dello strato network è quella d'instradare i pacchetti dal computer sorgente al computer di destinazione. La decisione del miglior percorso viene effettuato dagli algoritmi di routing (flooding, linkstate o distance vector). Purtroppo, per molteplici motivi, le reti potrebbero congestionarsi, più computer vogliono inviare pacchetti alla stessa destinazione che, non riuscendo ad elaborarli tutti ne perde, questo causa la ritrasmissione che causa ulteriori ingorghi. Questo problema è la congestione ed è un punto critico che va regolamentato.

37.1 Cos'è?

Quando gli algoritmi di choke packet (puro e hop-by-hop) non bastano per gestire la congestione, i router possono utilizzare la tecnica load shedding che, molto banalmente elimina dei pacchetti casuali in caso di sovraffollamento.

Lo scartare pacchetti casuali non è sempre la scelta migliore, per migliorare l'algoritmo infatti la scelta può basarsi sull'applicazione in esecuzione. Esistono due criteri generali per identificare queste scelte, wine e milk.

Wine dà più importanza ai pacchetti vecchi, scarta di conseguenza quelli nuovi (vecchio è meglio del nuovo), milk invece al contrario dà importanza maggiore ai pacchetti nuovi (nuovo è migliore del vecchio).

Questa tecnica permette numerose applicazioni e metodi per implementarla (oltre a wine e milk). Questo permette di tenere sotto controllo possibili momenti di congestione.

37.2 Pregi

Risolve la congestione in modo brutale, quando il choke packet non basta.

37.3 Difetti

Scarta pacchetti senza un criterio sufficientemente preciso da evitare di scartare pacchetti importanti.

37.4 Ambiti d'uso

Strato network, metodo brutale utilizzato per risolvere la congestione delle linee.

38 Red (Random Early Detection)

Nello strato network esistono numerosi algoritmi di instradamento per portare un pacchetto da una destinazione ad un mittente (flooding, distance vector, linkstate). Quando questa linea si congestionata esistono algoritmi che permettono di gestire la congestione e risolvere il problema (choke packet e load shedding). Risulta tuttavia più semplice gestire la congestione appena viene rilevata, non cercare di porvi rimedio dopo averle dato il tempo di bloccare tutta la linea.

38.1 Cos'è?

Questa osservazione porta all'idea di scartare i pacchetti prima che il buffer sia completamente pieno. Da qui nasce un celebre algoritmo usato per mettere in pratica questo schema: **RED** (Random Early Detection).

Red fa in modo che i router scartino i pacchetti prima che la situazione diventi senza speranza (early). Per stabilire quando è il momento giusto per iniziare a scartare i pacchetti, i router mantengono una media mobile delle lunghezze delle code. Quando la lunghezza media su una linea supera una soglia di guardia allora quella determinata linea è considerata congestionata e prende le dovute azioni di correzione. Il massimo che può fare purtroppo è scegliere un pacchetto a caso dalla coda che ha attivato "l'azione difensiva" e scartarlo. Per segnalare il rischio di congestione il router potrebbe inviare un choke packet per chiedere la diminuzione di flusso, tuttavia questo congestionerebbe ulteriormente le linee.

Scartando il pacchetto, la sorgente lo invierà nuovamente a causa del mancato acknowledgement.

38.2 Pregi

Risolve le congestioni prima che sia troppo tardi e sia necessario scartare pacchetti con il load shedding.

38.3 Difetti

Non può sapere esattamente che pacchetto ha causato il superamento della soglia (di conseguenza non sa chi è il reale mittente), di conseguenza non è il massimo della precisione.

38.4 Ambiti d'uso

Viene utilizzato prevalentemente nelle reti in cui le sorgenti rispondono ai pacchetti perduti rallentando il flusso.

Nelle reti wireless la perdita dei pacchetti è causata dal rumore nella maggior parte dei casi, di conseguenza non si rallenta il flusso e RED è impossibile da utilizzare.

39 Reverse Path Forwarding

I router spesso necessitano di inviare messaggi a molti o a tutti gli altri host. Questi tipi di trasmissioni sono dette trasmissioni broadcast.

L'algoritmo di routing più quotato per questo genere di trasmissioni è sicuramente quello di flooding, in quanto invia i pacchetti a tutte le stazioni vicine (tranne quella da cui ha ricevuto il pacchetto). Un problema di questa tecnica è sicuramente lo spreco di banda e la creazione di troppi pacchetti. Per ovviare a questo problema sono stati creati numerosi algoritmi che cercano di migliorare questo sistema di broadcasting.

39.1 Cos'è?

Con il Reverse path forwarding, il router che riceve un pacchetto controlla se gli è giunto da una linea che normalmente è utilizzata per inviare i pacchetti alla sorgente (ovvero che sia la linea con cammino minimo da lui alla sorgente). In caso affermativo, c'è una forte probabilità che il pacchetto broadcast abbia seguito il percorso migliore dalla sorgente fino a lui, di conseguenza lo copia e lo inoltra a tutte le linee (tranne quella da cui l'ha ricevuto). Se invece il pacchetto broadcast è giunto attraverso una linea diversa dalla preferita per raggiungere la sorgente, il pacchetto viene scartato in quanto è probabile si tratti di un duplicato.

39.2 Pregi

Implementazione facile ed efficiente: non richiede di conoscere la mappa della sottorete, liste di destinazione o mappe di bit per ogni pacchetto. Previene il problema dell'IP spoofing (falsificazione dell'indirizzo del mittente).

39.3 Difetti

—

39.4 Ambiti d'uso

Strato Network, tecnica usata nei moderni router con lo scopo di assicurare un cammino di pacchetti privi di loop.

40 Quality of Service (QoS)

Un flusso di pacchetti da una sorgente a una destinazione è chiamato, appunto, flusso. Ogni flusso viene regolamentato per il percorso da effettuare e quando effettuarlo, i metodi di gestione della congestione e così via.

40.1 Cos'è?

Ogni flusso ha le sue esigenze, in base all'applicazione che sta servendo, possiamo quindi caratterizzare queste esigenze in quattro parametri primari: affidabilità, ritardo, jitter e banda. Insieme, questi parametri determinano la QoS (Quality of Service), ossia la qualità del servizio richiesta dal flusso.

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

- **Jitter:** Il Jitter non è altro che la variazione del segnale in modo casuale. Questo può portare ad una ricezione di dati in intervalli irregolari, applicazioni come può essere la posta elettronica o il trasferimento file non sono molto soggette a questo problema. Lo sono invece per applicazioni di login remoto o di streaming video, a causa della variazione casuale della trasmissione, il risultato è terribile.
- **Banda:** ogni applicazione differisce per l'esigenza di banda, posta elettronica e accesso remoto non ne richiede molta, il video in tutte le sue forme invece sì.

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

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

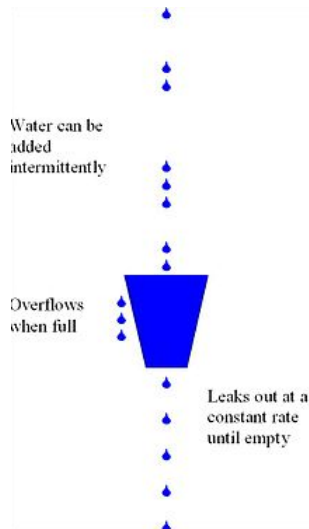
41 Leaky bucket, pregi e difetti

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

41.1 Cos'è?

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

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



41.2 Pregi

Burst di dati che potrebbero congestionare la rete vengono catturati dall'algoritmo che li distribuisce equamente.

41.3 Difetti

Ampie porzioni di risorse di rete non verranno utilizzate quando il volume del traffico è molto basso.

Quando la coda si riempie troppo i pacchetti in eccesso vengono brutalmente scartati.

41.4 Ambiti d'uso

Strato Network. Utilizzato nelle reti a commutazione di pacchetto, per controllare che le trasmissioni dei pacchetti siano ben delimitati in banda e velocità di trasmissione.

42 Descrivere il token bucket, pregi e difetti

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

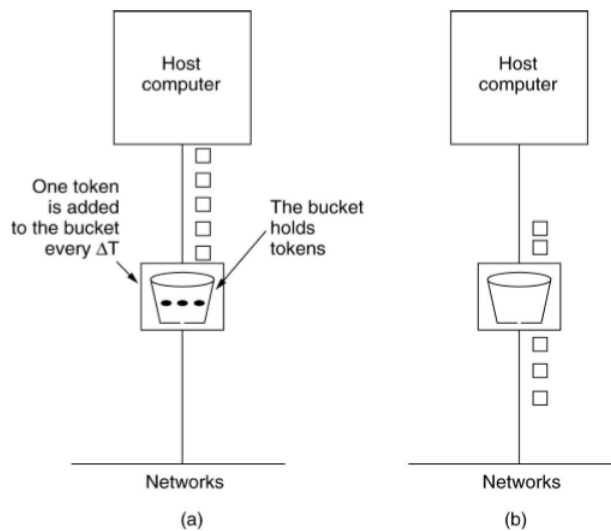
Per molte applicazioni è meglio permettere all'output di accelerare un po' quando ci sono burst di dati, perciò serve un algoritmo più flessibile e che non perda mai dati.

42.1 Cos'è?

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

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

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



42.2 Pregi

Al contrario del leaky bucket, usando quest'algoritmo non scarta nessun pacchetto.

Gestisce meglio i burst improvvisi, dando una risposta più veloce.

42.3 Difetti

Un potenziale difetto può essere che consente di trasmettere grandi raffiche di dati, che potrebbero causare congestione. (non sicura).

42.4 Ambiti d'uso

Strato Network, utilizzato per gestire il traffico in una rete dati, finalizzato a regolare l'output di trasmissione.

43 Descrivere l'ARP

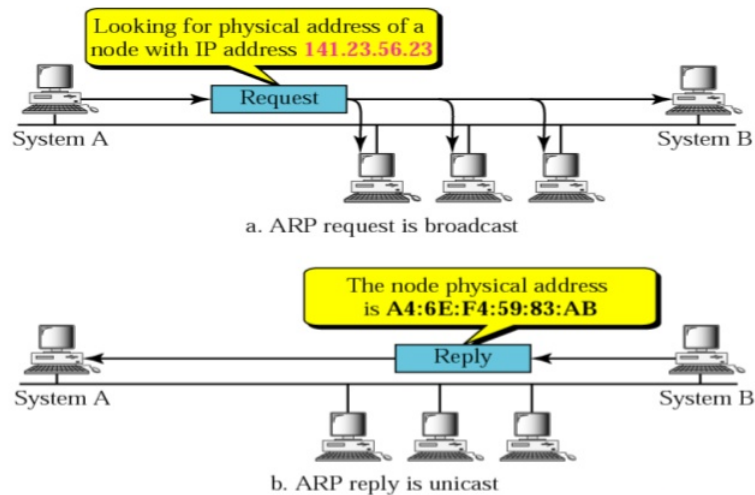
Ogni macchina di Internet ha uno o più indirizzi IP, tuttavia questi non possono essere utilizzati per inviare pacchetti, in quanto l'hardware che opera sullo strato data link non comprende gli indirizzi Internet. Bisogna trovare un modo per associare l'indirizzo Ethernet a 48 bit (indirizzo MAC) con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

43.1 Cos'è?

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

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

ARP Operation



43.2 Pregi

Permette la trasmissione di pacchetti ad un host anche senza conoscere l'indirizzo MAC (necessario per instaurare una connessione a livello data-link).

43.3 Difetti

Non autentica le risposte, il che lo rende molto vulnerabile a possibili attacchi.

43.4 Ambiti d'uso

Utilizzato nel protocollo IPv4 e operante a livello di accesso alla rete. Viene utilizzato tutte le volte che un host collegato ad una LAN deve inviare un messaggio ad un host nella stessa LAN conoscendo solamente l'indirizzo IP.

44 Si descriva DHCP e il suo funzionamento

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

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

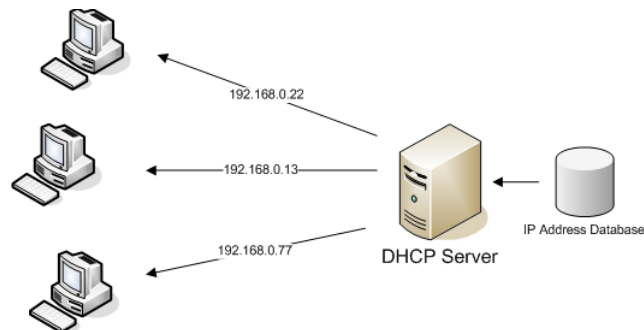
Per risolvere questo problema BOOTP viene esteso e chiamato in modo diverso, cioè DHCP (Dynamic Host Configuration Protocol), che permette un'assegnazione manuale o automatica degli indirizzi IP. Questo protocollo ha ampiamente sostituito RARP e BOOTP.

44.1 Cos'è?

DHCP si basa sull'idea di un server speciale che assegna gli indirizzi IP agli host che ne richiedono uno. Questo server non deve trovarsi sulla stessa LAN, il che comporta che potrebbe non essere raggiunto dalle trasmissioni broadcast, perciò è necessario installare in ogni LAN un agente di inoltro DHCP.

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

Per evitare questa eventualità, gli indirizzi IP sono assegnati secondo una tecnica chiamata di leasing, ovvero a scadenza di tempo. Prima che questo scada l'host deve fare richiesta di rinnovo dell'indirizzo, se non riesce a farla o se viene rifiutata, l'host non può più utilizzare quell'indirizzo IP.



44.2 Pregi

Permette di associare indirizzi IP avendo l'indirizzo MAC di un'host.

44.3 Difetti

Non include nessun meccanismo di autenticazione, il che lo rende vulnerabile a possibili attacchi

44.4 Ambiti d'uso

Protocollo di rete a livello applicativo, utilizzato ampiamente nelle reti odierne.

45 IPV6

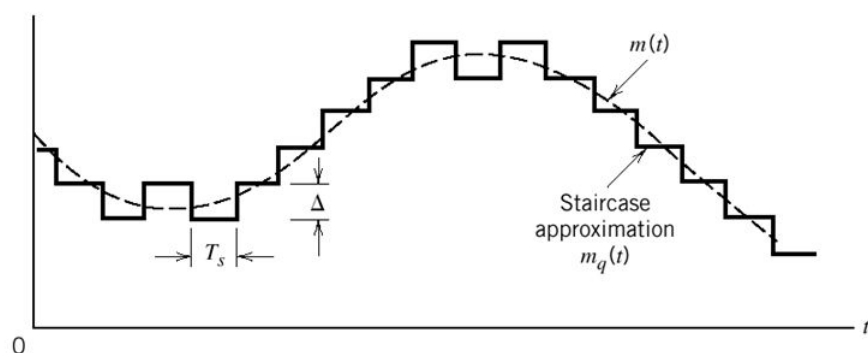
Un indirizzo IP, è un'etichetta numerica che identifica univocamente un dispositivo (host) collegato ad una rete informatica che utilizza l'Internet Protocol come protocollo di rete.

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

IPv6 è un upgrade dell'IPv4 e conta di risolvere i problemi di numero, in quanto riuscirebbe a gestire 2^{128} indirizzi diversi. IPv6 oltre a colmare il problema della quantità di indirizzi migliora e semplifica l'intestazione: infatti prevede solo 8 campi rispetto ai 13 dell'IPv4. Questo consente al router di elaborare i pacchetti più velocemente. Sempre riguardo l'elaborazione dei

pacchetti, IPv6 migliora il supporto per le opzioni, rendendo campi che prima erano obbligatori, opzionali. Un altro grande passo avanti riguarda la sicurezza.

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



45.1 Pregi

Aumenta di molto gli indirizzi gestibili rispetto all'IPv4.

Migliora e semplifica l'intestazione, consentendo una elaborazione di pacchetti più veloce.

Migliora il supporto per le opzioni e migliora la sicurezza.

45.2 Difetti

Non è compatibile con il predecessore, quindi l'introduzione a questo nuovo protocollo è lenta.

45.3 Ambiti d'uso

Protocollo di rete, utilizzato per gli indirizzi di rete.

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

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

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

46.1 IPv4

IPv4 è il protocollo più usato e la sua tecnologia può supportare al massimo 2^{32} indirizzi univoci, numero che sta iniziando a diventare stretto. Un datagramma IP di questa versione è costituito da una parte di intestazione e una parte di testo. L'intestazione è di 20B fissi e una parte opzionale di lunghezza variabile, consiste in 13 campi.

46.2 IPv6

IPv6 è l'evoluzione dell'IPv4 e conta di risolvere molti dei suoi problemi, può supportare al massimo 2^{128} indirizzi univoci. Un datagramma IP di questa versione è costituito da una parte di intestazione e una parte di carico utile. L'header è costituito dai primi 40 byte e contiene 8 campi, il carico utile invece va da un minimo di 1280 byte e arriva fino a 65535 byte (in modalità standard).

46.3 IPv4, primi 32bit

- Version [4 bit]: indica la versione del pacchetto IP; per IPv4, ha valore 4.
- Internet Header Length (IHL) [4bit]: indica la lunghezza (in word da 32 bit) dell'header del pacchetto IP; tale lunghezza può variare da 5 word (20 byte) a 15 word (60 byte) a seconda della presenza e della lunghezza del campo facoltativo.

- Type of Service (TOS) [8 bit]: Nelle specifiche iniziali, questo campo avrebbe dovuto specificare il modo e la precedenza con cui l'host ricevente doveva trattare il datagramma; Ad esempio, un host poteva scegliere una bassa latenza, mentre un altro preferire un'alta affidabilità. Nella pratica questo uso del campo TOS non ha preso piede.
- Total Length [16 bit]: Indica la dimensione (in byte) dell'intero pacchetto, comprendendo header e dati.

46.4 IPv4, secondi 32bit

- Identification [16 bit]: Inizialmente sarebbe dovuto essere utilizzato per identificare in modo univoco i vari frammenti in cui può essere spezzato un pacchetto IP. Sperimentazioni successive però hanno suggerito di utilizzarlo per aggiungere la funzionalità di tracciamento dei pacchetti. Serve per determinare quale datagramma appartiene al frammento appena arrivato (tutti i frammenti di un datagramma hanno lo stesso campo identification).
- Flags [3 bit]: Bit utilizzati per il controllo del protocollo e della frammentazione dei datagrammi. Il primo è Reserved sempre settato a "0" (bit inutilizzato in poche parole), successivamente troviamo DF (Don't Fragment) se settato a "1" indica che il pacchetto non deve essere frammentato, se non è possibile inviarlo senza frammentazione, il pacchetto viene scartato. L'ultimo bit di flag è MF (More Fragments) se settato a "0" indica che il pacchetto è l'ultimo frammento (o il solo frammento del pacchetto originario), perciò tutti gli altri frammenti dello stesso pacchetto avranno MF settato a "1".
- Fragment Offset [13 bit]: Indica l'offset (misurato in blocchi di 8 byte) di un particolare frammento relativamente all'inizio del pacchetto IP originale: il primo frammento ha offset 0, i successivi avranno valore multiplo di 8byte e indica la posizione del frammento nel datagramma. Il valore massimo è pari a 65536 byte.

Bit	0	4	8	16	19	24	31
Version	HLEN		Service Type		Total Length		
Identification				Flags	Fragment Offset		
Time to Live		Protocol		Header Checksum			
Source IP Address							
Destination IP Address							
Options							Padding

46.5 IPv6, primi 32bit

- Version [4 bit]: Indica la versione del datagramma IP: per IPv6, ha valore 6 (lel).
- Traffic Class [8 bit]: Permette di gestire le code di priorità, assegnando ad ogni pacchetto una classe di priorità rispetto ad altri pacchetti provenienti dalla stessa sorgente. Viene usata anche per controllare la congestione.
- Flow Label [20 bit]: Campo ancora in fase sperimentale, usato dal mittente per etichettare una sequenza di pacchetti come se fossero nello stesso flusso. Supporta la gestione del QoS (Quality of Service) consentendo ad esempio di specificare quali etichette abbiano via libera rispetto ad altre. I pacchetti con flow label diverso da “0” avranno trattamenti speciali dai router.

46.6 IPv6, secondi 32bit

- Payload Length [16 bit]: è la dimensione del payload (carico utile), ovvero il numero di byte di tutto il contenuto presente dopo l’header.
- Next Header [8 bit]: Indica quale tipo di processo di trasporto è in attesa di quei dati (UDP, TCP o altri). Simile al campo protocol dell’IPv4 con cui condivide i valori.
- Hop Limit [8 bit]: Indica il tempo di vita del pacchetto, il suo valore viene decrementato di 1 ogni volta che il pacchetto passa da un router, quando arriva a 0 viene scartato. Simile al campo Time to live presente nell’IPv4.

Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

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

47 Frame Ethernet

47.1 Cos'è?

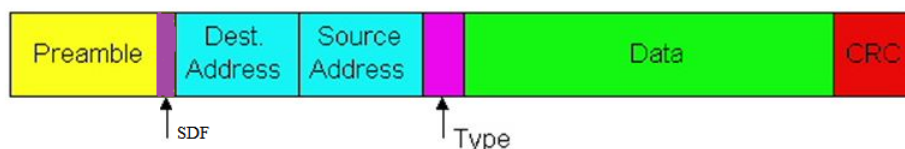
Un frame Ethernet è l'unità trasportata nel livello Data Link. Esistono diverse versioni di questo frame; ora analizziamo la versione IEEE 802.3.

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

- Preambolo [7 byte]: contenente “10101010” e serve per sincronizzare il clock del ricevitore con quello del trasmettitore.
- SFD [1 byte]: Start of the Frame, “10101011” indica al destinatario che dal prossimo byte comincerà il frame vero e proprio.
- MAC address di destinazione [6 byte]: Indica l'indirizzo di destinazione, il bit di ordine più elevato vale “0” per gli indirizzi ordinari e “1” per quelli di gruppo. Con gruppo si intende una trasmissione multicast, che differisce dalla broadcast, più rozza ma che non richiede alcuna gestione. Per una trasmissione broadcast basta mettere tutti i bit a “1”.
- MAC address sorgente [6 byte]: indica l'indirizzo sorgente del frame.
- Type [2 byte]: Indica al ricevitore cosa deve fare del frame. Sullo stesso computer si possono usare più protocolli dello stato network

contemporaneamente, questo campo indica il processo a cui passare il frame.

- Dati [da 46 a 1500 byte]: Questo campo contiene i dati veri e propri, non può essere nullo in quanto Ethernet richiede frame lunghi almeno 64 byte (dal destination address al checksum inclusi). Perciò se la parte occupata dai dati è lunga meno di 46 byte il campo successivo viene utilizzato per riempire il frame.
- Pad [0-46 byte]: Come descritto sopra, se il frame dati è inferiore a 46 byte, questo campo provvede a riempire i byte mancanti, così che vengano accettati dal protocollo Ethernet.
- Checksum [4 byte]: Contiene codice CRC per il rilevamento degli errori (senza correzione).



48 Si descriva l'header UDP

Lo stato di trasporto è il cuore dell'intera gerarchia dei protocolli. Il suo compito è fornire il trasporto dei dati, affidabile ed efficiente in termini di costi, dal computer di origine a quello di destinazione, indipendentemente dalla rete o dalle reti fisiche effettivamente utilizzate. Nello stato di trasporto ci sono due protocolli principali, che si distinguono dal fatto che uno è orientato alla connessione l'altro è senza connessione (TCP e UDP).

Senza connessione: lo scambio di dati a pacchetto tra mittente e destinatario non richiede l'operazione preliminare di creazione di un circuito su cui instradare l'intero flusso.

48.1 Cos'è UDP?

UDP (User Datagram Protocol) è un protocollo dello stato di trasporto senza connessione. Non gestisce il riordinamento dei pacchetti né la ritrasmissione di quelli persi, il che lo rendono di minor affidabilità rispetto al TCP. In compenso è molto rapido ed efficiente per applicazioni leggere o

time sensitive (audio video real-time). UDP fornisce servizi basilari: Moltiplicazione delle connessioni tramite assegnazione delle porte e verifica degli errori mediante una checksum inserita in un campo dell'header.

48.2 Header UDP

L'header dell'UDP è così formato:

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

Infine sono presenti i dati del messaggio.

48.3 Pregi

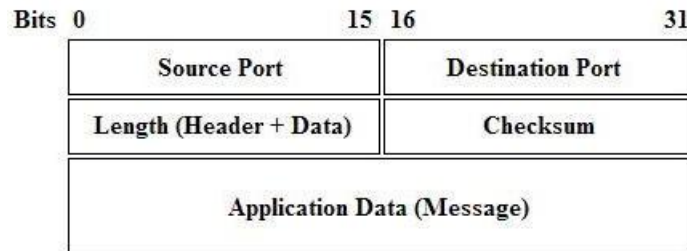
Rapido ed efficiente per applicazioni leggere e che necessitano di velocità di trasmissione.

48.4 Difetti

Non gestisce il riordinamento dei pacchetti e la ritrasmissione di quelli persi. Non da nessuna affidabilità.

48.5 Ambiti d'uso

UDP viene utilizzato dalle applicazioni di rete che sono elastiche riguardo alla perdita dei dati e strettamente dipendenti dal tempo, si usa inoltre per comunicazioni in broadcast (tutti i terminali in una rete) e multicast (tutti i terminali iscritti ad un servizio).



49 Descrivere l'header TCP/IP e commentarlo

Lo stato di trasporto è il cuore dell'intera gerarchia dei protocolli. Il suo compito è fornire il trasporto dei dati, affidabile ed efficiente in termini di costi, dal computer di origine a quello di destinazione, indipendentemente dalla rete o dalle reti fisiche effettivamente utilizzate. Nello stato di trasporto ci sono due protocolli principali, che si distinguono dal fatto che uno è orientato alla connessione l'altro è senza connessione (TCP e UDP).

Orientato alla connessione: I dispositivi utilizzano un protocollo di comunicazione per stabilire una connessione end-to-end tra gli agenti della comunicazione prima della trasmissione di qualsiasi tipo di dato.

49.1 Cos'è TCP?

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

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

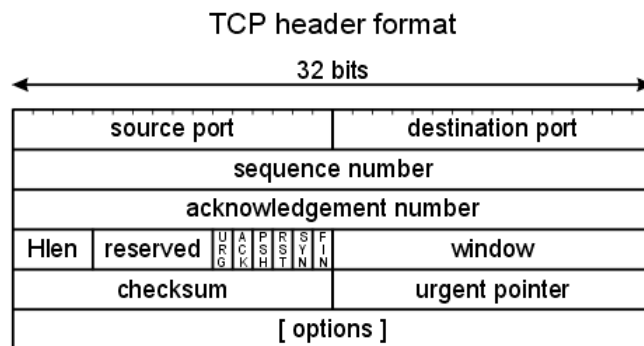
49.2 Header TCP

L'header del TCP è formato nel seguente modo:

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

- Destination port [16 bit]: Identifica il numero di porta sull'host destinatario.
- Sequence number [32 bit]: Indica lo scostamento (in byte) dell'inizio del segmento TCP interno al flusso completo, a partire dall'ISN (initial sequence number), negoziato all'apertura della connessione.
- Acknowledgment number [32 bit]: Ha senso solo se il flag ACK è impostato a "1", e conferma la ricezione di una parte del flusso di dati nella direzione opposta, indicando il valore del prossimo Sequence number che l'host mittente del segmento TCP si aspetta di ricevere.
- Data offset [4 bit]: Indica la lunghezza (in word da 32 bit) dell'header del segmento TCP; può variare in base alla presenza e alla lunghezza del campo facoltativo Options.
- Reserved [4 bit] Bit non utilizzati. Predisposti per sviluppi future dell'applicazione.
- Flags [8 bit]: Bit utilizzati per il controllo del protocollo:
 - CWR (Congestion Window Reduced): Se impostato a "1" indica che l'host sorgente ha ricevuto un segmento TCP con flag ECE (prossimo) impostato a "1". QUESTA è NUOVA, NON CREDO SERVA
 - ECN (Explicit Congestion Notification): se impostato a "1" indica che l'host supporta L'ECN durante il 3-way handshake. QUESTA è NUOVA, NON CREDO SERVA
 - URG: Se impostato a "1" indica che nel flusso sono presenti dati URGENTI alla posizione (offset) indicata nel campo Urgent pointer.
 - ACK: Se impostato a "1" indica che il campo Acknowledgment number è valido;
 - PSH: Se impostato a "1" indica che i dati in arrivo devono essere passati subito ai livelli superiori senza che vengano bufferizzati.
 - RST: Se impostato a "1" indica che la connessione non è valida; usato in caso di errore grave; Utilizzato per la reimpostazione della connessione diventata incongruente.
 - SYN: Indica che l'host mittente del segmento vuole stabilire una connessione e specifica nel campo Sequence number il valore dell'ISN; utilizzato per stabilire le connessioni. Chi invia il SYN deve attendere dall'host remoto un SYN/ACK.

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



49.3 Pregi

Possiede funzionalità di controllo di flusso e controllo della congestione (attraverso la sliding window). Da grande affidabilità nel trasporto di pacchetti nella rete.

49.4 Difetti

Utilizza molta banda per fornire tutte le feature, feature che per molte applicazioni non sono utili, con conseguente spreco di banda nei loro casi.

49.5 Ambiti d'uso

Strato di trasporto, presente nei terminali. Implementato all'interno del sistema operativo. Usato nella stragrande maggioranza delle applicazioni internet che richiedono una consegna affidabile di pacchetti (che UDP non può garantire).

50 Cos'è il DNS?

50.1 Cos'è?

Protocollo dello strato applicativo, **DNS** (Domain Name System) è un sistema per la risoluzione di nomi degli host in indirizzi IP. L'essenza del DNS è l'invenzione di uno schema di denominazione gerarchico basato su dominio, e di un sistema di database distribuito per l'implementazione di questo schema di denominazione.

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

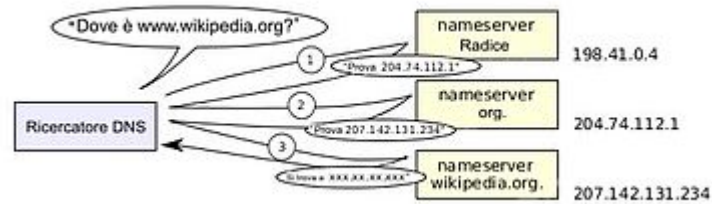
Questa tecnica è utile in quanto l'ampia diffusione di internet anche per utenti non tecnici non è pratica a memorizzare indirizzi IP numerici, per questo modificandoli in nomi testuali sono più semplici da memorizzare e utilizzare.

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

- It denota il dominio di primo livello;
- Ciaofede è un dominio di secondo livello, cioè il nome che caratterizza questo sito web (insieme a .it).

- www è il dominio di terzo livello ed identifica un particolare host all'interno del dominio ciaofede.it.

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



50.2 Pregi

Garantisce una maggior chiarezza per l'utente medio.

50.3 Difetti

—

50.4 Ambiti d'uso

Strato Applicativo.

Utilizzato per la risoluzione di nomi della rete.

Utilizzato molto nei web server, in cui con un singolo indirizzo IP si possono ospitare più siti web.

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

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

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

rendere un messaggio non comprensibile/leggibile a persone non autorizzate a leggerlo.

51.1 Cos'è il cifrario a sostituzione

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

51.2 Cos'è il cifrario a trasposizione

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

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

51.3 Differenze tra i due

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

52 Si descriva il block cipher

52.1 Cos'è

Block cipher è un algoritmo a chiave simmetrica (tecnica di cifratura in cui la chiave è la stessa sia per la crittazione sia per la decrittazione) operante su un gruppo di bit di lunghezza finita organizzati in un blocco. Questo tipo di algoritmi sono composti da due parti, una che cifra (E) e un'altra che decifra (E_1). Dati n bit in entrata in blocco, l'algoritmo cifra n bit in blocco. Per eseguire la crittazione e la decrittazione è possibile implementarli tramite semplici circuiti elettrici, come ad esempio la P-box (scatola di permutazione) o la S-box (scatole di sostituzione).

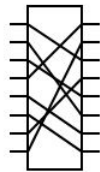
52.2 P-box

La P-box permette di trasporre 8 bit, se un input è lineare 01234567, l'output è 24506713, ovviamente la P-box lavora alla velocità della luce, in quanto non sono necessari calcoli, però è necessario conoscere la chiave di cifratura (ossia come sono disposti i collegamenti interni della P-box).

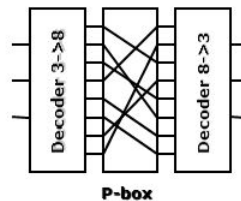
52.3 S-box

la S-box invece è un altro tipo di circuito che sostituisce il numero di bit del messaggio, mescolandoli. Se il messaggio in entrata ha m bit, l'output è da n . Ad esempio si ha un input di 8 bit, l'output sarà da 3 bit permutati dagli 8, servirà poi una S-box per decifrare il messaggio e tornare agli 8 bit originali.

P-box: 8 lines



S-box: 3 lines



52.4 Pregi

Combinati insieme, P-box e S-box, creano un sistema crittografico molto performante.

52.5 Difetti

Singolarmente questi metodi non sono molto affidabili, S-box è molto vulnerabile agli attacchi basati sul tempo.

52.6 Ambiti d'uso

Utilizzati in crittografia per cifrare blocchi di dati (a differenza degli algoritmi di flusso che cifrano un solo elemento alla volta).

53 Si descriva l'algoritmo DES e triplo DES

53.1 Cos'è DES?

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

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

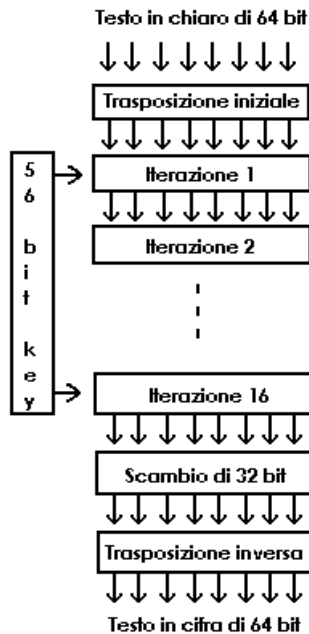
DES è formato da 19 stadi distinti:

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

53.2 Cos'è Triplo-DES?

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

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



53.3 Pregi

Permettono una cifratura a blocchi rispetto al singolo elemento come la cifratura a flusso.

Triplo DES migliora la poca sicurezza del DES.

Triplo DES è compatibile con DES grazie alla sua composizione, basta porre $K_1 = K_2$.

53.4 Difetti

A causa della dimensione ridotta della chiave (64 bit) DES non è molto sicuro.

Usando questi metodi crittografici un testo in chiaro produrrà sempre il medesimo testo cifrato.

Entrambi soffrono di una prestazione software.

Entrambi gli algoritmi sono stati sostituiti da AES.

53.5 Ambiti d'uso

Nell'ambito della crittografia, stanno cadendo in disuso a causa delle scarse prestazioni, sostituiti da AES.

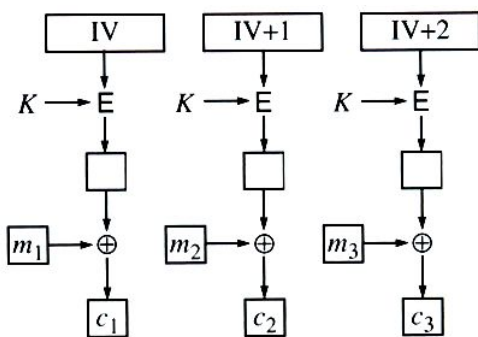
54 Counter Mode Cipher

54.1 Causa della creazione

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

54.2 Cos'è?

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



54.3 Pregi

Permette la decifratura di blocchi di dati in ordine non sequenziale, non necessita quindi di decrittare tutti i blocchi a lui precedenti.

54.4 Difetti

Se si utilizza la stessa chiave e lo stesso IV per due differenti messaggi, avendo i due messaggi cifrati è possibile bypassare la sicurezza facendo lo XOR dei due messaggi, ottenendo la chiave.

54.5 Ambiti d'uso

Viene utilizzato nella cifratura come alternativa agli algoritmi che cifrano i dati basandosi su blocchi precedenti.

Utile ad esempio se si necessita di effettuare ricerche non sequenziali dei dati.

55 Cipher block chaining

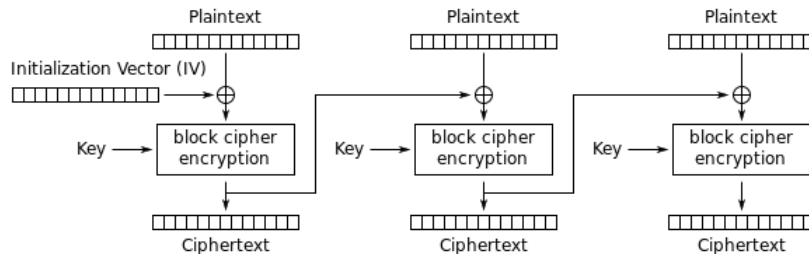
DES, triplo DES e AES, utilizzano un cifrario a sostituzione monoalfabetica che usa caratteri lunghi. Usando sempre la stessa chiave, ottenendo sempre blocchi di testo cifrato uguali (per testo in chiaro uguale), risulta semplice (con un po' di forza bruta) compromettere la sicurezza dei blocchi cifrati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

55.1 Cos'è?

Un modo per evitare questo problema è collegare tutti i blocchi cifrati in modo diverso, questa tecnica è chiamata Cipher block chaining. In questo metodo, ogni blocco di testo in chiaro è messo in XOR con il precedente blocco cifrato prima di eseguire la cifratura vera e propria.

Così facendo a blocchi di testo in chiaro uguali non corrispondono più blocchi di testo cifrato identici. Per il primo blocco di questa catena lo XOR viene calcolato con un blocco di dati casuali (vettore di inizializzazione IV), che è trasmesso (in chiaro) insieme al testo cifrato.

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



55.2 Pregi

Migliora il problema dei cifrari che utilizzano sempre la stessa chiave (DES/TRIPLDES/AES), ovvero il problema di generare sempre blocchi uguali per testi uguali.

55.3 Difetti

Per decifrare un blocco in mezzo al flusso bisogna prima decrittare tutti i blocchi a lui antecedenti.

55.4 Ambiti d'uso

Nell'ambito della cifratura, viene utilizzato quando è necessario un livello di sicurezza maggiore rispetto a AES, in quanto produce testo cifrato diverso per blocchi di testo in chiaro uguali.

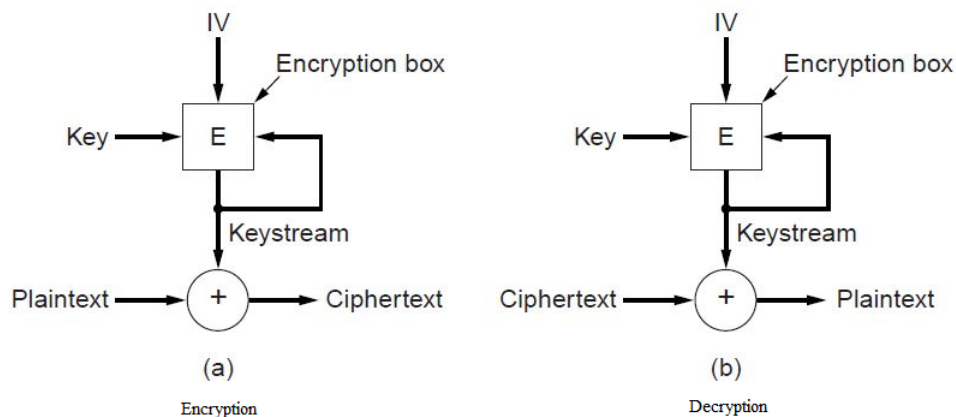
56 Stream cipher

56.1 Cos'è?

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

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

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



56.2 Pregi

Garantisce alta elasticità agli errori.

56.3 Difetti

Ha il rischio di keystream riutilizzato se non si sta attenti.

56.4 Ambiti d'uso

Utilizzato per cifrare dati in applicazioni in cui è necessario che un bit di errore non rovini 64 bit di testo in chiaro.

57 RSA

57.1 Causa della creazione

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

Una variante per le chiavi simmetriche (stessa chiave per decifrare e cifrare) è stato dato dalle chiavi asimmetriche (o chiavi pubbliche/private). Questo sistema richiede che ogni utente sia in possesso di due chiavi, una pubblica per la cifratura e una privata per la decifratura, quella pubblica può

essere condivisa al mondo, mentre quella privata dev'essere in possesso solo del proprietario. Così facendo chiunque può scrivere un messaggio cifrato a chi vuole, basta cifrarlo con la chiave pubblica della persona interessata, la persona interessata poi userà la sua chiave privata per decifrarlo.

57.2 Cos'è?

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

- Si scelgono due numeri primi, p e q (tipicamente di 1024 bit)
- Si calcola $n=p*q$ e $z=(p-1)*(q-1)$.
- Si sceglie un numero primo relativamente a z , detto d .
- Si trova e tale che $e*d=1 \bmod z$.

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

La sicurezza del metodo è basata sulla difficoltà di scomporre in fattori i numeri molto grandi.

57.3 Pregi

Algoritmo molto robusto, che permette lo scambio di chiavi con una sicurezza quasi assoluta.

57.4 Difetti

Richiede chiavi di almeno 1024 bit, il che rende l'algoritmo molto lento.

57.5 Ambiti d'uso

Viene utilizzato per lo scambio dati con persone sconosciute.

58 Si descriva la tecnica di attacco “Birthday attack”

58.1 Firme digitali

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

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

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

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

58.2 Cos'è il birthday attack

Il birthday attack è un esempio per dimostrare che, per forzare una MD di m bit, bastano solamente $2^{m/2}$ operazioni. L'idea per quest'attacco viene da una tecnica che i professori di matematica usano spesso nei corsi di matematica: “Quanti studenti ci devono essere in una classe perché la probabilità che due persone abbiano lo stesso compleanno superi il 50%?” (23). Con 23 persone possiamo formare $(23*22)/2=253$ coppie differenti, ognuna ha probabilità $1/365$ di essere quella buona, di conseguenza la percentuale di possibilità supera facilmente il 50%.

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

59 Sicurezza in 802.11

59.1 Cos'è?

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

59.2 Come funziona

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

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

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

59.3 Pregi

Provvede una sicurezza basilare

59.4 Difetti

Non è per nulla affidabile visto che l'IV si ripete generando il pericolo di riutilizzo del keystream.

59.5 Ambiti d'uso

Ormai obsoleto, viene sostituito da sistemi più sicuri.

60 Si descriva la sicurezza di Bluetooth

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

60.1 Livelli di sicurezza

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

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

60.2 Pregi

Diverse modalità di sicurezza, sicurezza implementata in diversi strati per mantenerla alta.

60.3 Difetti

Questo sistema di sicurezza purtroppo non protegge nel caso di furto del dispositivo.

60.4 Ambiti d'uso

Utilizzato nelle connessioni bluetooth.

61 La tecnica di attacco reflection attack

61.1 Cos'è?

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

In questa tipologia di attacco sono necessari due interlocutori, A e B, e dev'essere aprire più conversazioni contemporaneamente con la vittima (B). C, il nostro malintenzionato, seguendo alcune procedure e scambi multipli riesce a simulare l'identità di A, imbrogliando B, e potenzialmente aver accesso a tutte le conoscenze private di A che conosce B. (immaginando che B sia una banca, C che finge di essere A, ha libero accesso ai suoi soldi, non è proprio una cosa carina).

61.2 Regole per evitarlo

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

- Fare in modo che chi inizia l'autenticazione provi la sua identità prima che lo faccia chi risponde.
- Far sì che entrambi gli interlocutori utilizzino chiavi differenti per provare la propria identità.
- Far sì che gli interlocutori usino (per le richieste) numeri presi da insiemi diversi.

- Rendere il protocollo resistente a attacchi che coinvolgono una seconda sessione parallela.

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

62 Replay attack

62.1 Cos'è?

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

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

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

62.2 Metodi per evitarlo

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

63 Algoritmo Diffie-hellman

63.1 Cos'è?

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

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

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

63.2 Pregi

Scambio di chiavi sicuro in canale di comunicazione pubblico.

63.3 Difetti

Soggetto all'attacco "man-in-the-middle".

63.4 Ambiti d'uso

Algoritmo alla base di numerosi protocolli usati nelle telecomunicazioni che permettono una comunicazione sicura dalla sorgente al destinatario. Usato in TCP/IP.

64 Attacco Man in the middle

64.1 Cos'è?

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

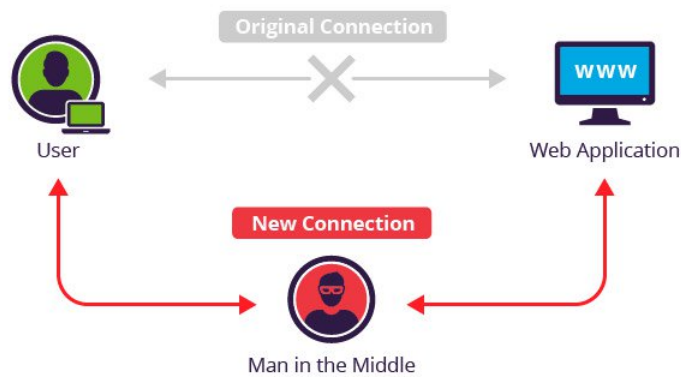
L'attaccante dev'essere in grado di frapporsi tra le due parti e intercettare i messaggi, così facendo può simulare la risposta per entrambi. Potenzialmente questo attacco è fattibile verso qualsiasi conversazione che utilizza chiave pubblica.

Un esempio del suo funzionamento è il seguente:

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

64.2 Come evitarlo

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



65 DNS spoofing

65.1 Cos'è?

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

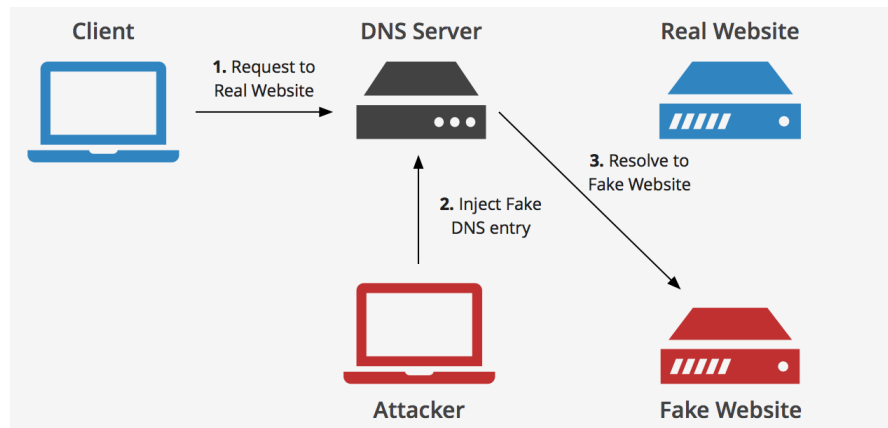
Il protocollo DNS invece ha il compito di trasformare un indirizzo letterale (ad esempio `www.fedesimpy.it`) in indirizzo numerico o IP (`202.159.222.222`). Il DNS Spoofing si svolge quindi nel modo seguente:

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

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

65.2 Possibile soluzione

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



A Capitolo 1 - Introduzione

A.1 Tipi di collegamento

Ci sono due tipi di collegamento:

- **Poin-to-Point** - la comunicazione avviene tra due macchine tramite dei pacchetti.
- **Broadcast** - esiste un canale condiviso da tutte le macchine; una volta inviato un pacchetto viene ricevuto da tutti e viene processato solo dalla macchina che ha l'indirizzo indicato nel pacchetto; è possibile anche mandare un pacchetto a tutte le macchine della rete con un codice speciale nel campo indirizzo del pacchetto.

A.2 Classificazione delle reti

Classificazione delle reti in base alla distanza dei processori:

- PAN - Personal Area Network
- LAN - Local (Stanza/Edificio)
- MAN - Metropolitan (Città)
- WAN - Wide (Nazione/Continente)
- Internet (Pianeta)

A.3 Architettura delle reti

L'architettura delle reti è composta da livelli e protocolli. Una rete è organizzata come una pila di livelli i quali offrono servizi ai livelli superiori, senza dare dettagli implementativi.

Un livello di un computer comunica con lo stesso livello di un altro computer. Le entità su uno stesso livello sono detti *peer* (pari). Tuttavia i dati non passano direttamente da un livello n_A ad un livello n_B , ma dovranno essere passati ai sottolivelli di A per poi risalire i livelli di B.

Le regole e le convenzioni per la comunicazione tra livelli pari sono note come **protocolli** di livello. Un protocollo indica come deve avvenire la comunicazione tra le parti (es: il formato e significato dei pacchetti).

Infine, tra i livelli sono presenti le **interfacce**, che definiscono i *servizi* (cioè un insieme di primitive/operazioni) che il livello inferiore mette a disposizione del soprastante.

In una rete strutturata bene è possibile sostituire l'implementazione di un livello perché quella nuova dovrà solo rendere disponibile al livello soprastante gli stessi servizi della vecchia.

A.3.1 Progettare una rete

I punti chiave da tenere in considerazione quando si progetta una rete sono:

- Affidabilità
 - individuare gli errori e, se possibile, correggerli;
 - trovare un percorso valido tra sorgente e destinatario (routing/instradamento);
- Evoluzione della rete
- Allocazione delle risorse
 - gestire una banda condivisa;
 - impedire che una sorgente veloce inondi un ricevitore lento (flow control) per evitare una congestione;
- Sicurezza della rete

A.3.2 Tipi di servizi offerti da un livello

Un livello può offrire un servizio orientato alla connessione o senza connessione.

Il primo richiede di stabilire una connessione, usarla e rilasciarla una volta terminato. In questo servizio le informazioni inviate mantengono l'ordine di partenza.

Nel servizio senza connessione ogni pacchetto viene mandato al destinatario indipendentemente dai messaggi successivi, quindi non c'è sicurezza che l'ordine sia mantenuto.

Inoltre c'è una questione legata all'affidabilità. Un servizio è considerato affidabile se riceve sempre tutti i pacchetti e di solito avviene tramite una conferma di ricezione. La conferma tuttavia rallenta le prestazioni del servizio, quindi è necessario valutare nei singoli casi se ne vale la pena: ad esempio in un servizio di streaming è più importante la velocità per un servizio più fluido piuttosto che l'affidabilità per una qualità migliore dell'audio/video.

Un esempio di primitive di un servizio orientato alla connessione sono: Listen, Connect, Accept, Receive, Send, Disconnect.

A.4 Modelli di reti

Esistono due architetture di rete principali utilizzate come modello: OSI e TCP/IP.

Il primo utilizza 7 livelli:

1. fisico
2. data link
3. rete
4. trasporto
5. sessione
6. presentazione
7. applicazione

Il secondo utilizza 4 livelli:

1. link - livello di accesso alla rete per spedire i pacchetti IP.
2. internet - livello che gestisce l'indirizzamento dei nodi e l'instradamento, assegnando ad ogni nodo un indirizzo IP e indicando il percorso migliore verso il destinatario.
3. trasporto - livello che gestisce la comunicazione, tramite protocollo TCP o UDP.
4. applicazione - livello più vicino all'utente che gestisce le sessioni e la presentazione; alcuni protocolli di questo livello sono HTTP e DNS.

Il libro e il corso utilizza un modello ibrido a 5 livelli:

1. fisico - indica come vengono trasmessi i bits tramite segnali elettrici o simili.
2. link - indica come mandare i messaggi ai computer (es. Ethernet, 802.11).
3. rete - indica come combinare link multipli per spedire pacchetti tra computer distanti
4. trasporto - gestisce la comunicazione, tramite protocollo TCP o UDP.
5. applicazione - programmi che usano il network

B Capitolo 2 - Strato fisico

L'obiettivo dello strato fisico è quello di trasportare i bits da una macchina ad un'altra. Per farlo si possono usare diversi mezzi fisici con proprie caratteristiche. I mezzi di trasmissione possono essere guidati (es: cavi) o non guidati (wireless, satelliti).

Le informazioni possono essere trasmesse su cavi sfruttando proprietà come voltaggio o corrente. Usando questi valori, si può modellare il comportamento del segnale e analizzarlo matematicamente.

B.1 Serie di Fourier e Banda passante

Fourier afferma che una funzione periodica con periodo T può essere costruita come la somma di un numero n di seni e coseni. Da ciò deriva la serie di Fourier, una formula che permette di ricostruire la suddetta funzione periodica. Nel contesto delle reti, un segnale che ha durata finita può essere immaginato come un pattern che viene ripetuto con l'intervallo T e $2T$ identico all'intervallo 0 a T . In questo modo, conoscendo periodo e ampiezza è possibile ricostruire la funzione del segnale, permettendo un'analisi e modellazione più facile del segnale. Il problema è che i mezzi di trasmissione perdono parte della potenza del segnale, generando una distorsione. Un cavo riesce a trasmettere frequenze senza attenuazione in un intervallo che va da 0 a f_c (frequenza di cutoff). Questo intervallo è detto Banda passante (*bandwidth*) e dipende da diversi fattori del mezzo di trasmissione (materiali, lunghezza e spessore di un cavo, ecc). Le frequenze che vanno oltre vengono attenuate. La frequenza di cutoff non è ben definita, quindi di solito si pone l'intervallo da 0 fino alla frequenza dove la potenza del segnale è dimezzata. Questi sono detti segnali baseband. A volte vengono utilizzati dei filtri che possono modificare la banda passante, per esempio alzando l'intervallo da un valore maggiore di zero: è il caso delle trasmissioni wireless. Questi sono segnali passband.

B.2 Mezzi di trasmissione guidati

B.2.1 Mezzi magnetici

I mezzi magnetici sono un comune mezzo di trasporto per dati (cd, dcd, hdd) che in alcuni casi può risultare più conveniente se considerato un rapporto $\text{dimensioneDati}/\text{tempoTrasferimento}$. Per esempio può essere più comodo trasportare un camion di hard disk piuttosto che spedire lo stesso quantitativo di dati tramite la rete. Anche se le connessioni stanno diventando sem-

pre più veloci, in alcuni casi i mezzi magnetici possono rimanere la miglior soluzione (sempre da considerare il contesto).

B.2.2 Il doppino

Il doppino è un cavo composto da due conduttori in rame isolati di 1mm, attorcigliati in modo elicoidale (simile al DNA). Questa forma permette di eliminare i campi elettromagnetici che si verrebbero a formare se fossero paralleli. Un segnale è trasmesso come differenza di voltaggio tra i due cavi, in modo da evitare i disturbi da rumori esterni(?). L'uso più comune è per il telefono e l'accesso ad internet con l'ADSL. Il doppino può estendersi per chilometri, ma dopo certe distanze è necessario un ripetitore altrimenti il segnale diventa troppo attenuato. Il prezzo del doppino è ridotto e ha una velocità di trasmissione moderata. Si possono usare per segnali sia analogici che digitali e la larghezza di banda dipende dallo spessore del cavo e dalla distanza percorsa, tuttavia è limitata.

Esistono diversi tipi di cavi che utilizzano il doppino, come Cat 3 e Cat 5. Questi consistono in due cavi isolati attorcigliati tra loro, raggruppati con altre coppie (4 totali), ricoperti da una protezione in plastica. La differenza tra le due tipologie sta nel numero di spire per metro: maggior numero di spire significa una maggior qualità del segnale su lunghe distanze. Esistono categorie superiori come Cat 6 e 7 che supportano segnali con una maggiore larghezza di banda (fino a 500 MHz).

B.2.3 Il cavo coassiale

Il cavo coassiale è un mezzo trasmissivo che permette una maggior larghezza di banda (fino a qualche GHz) rispetto al doppino grazie alla migliore schermatura, permettendo di viaggiare a maggiori velocità a lunghe distanze. In particolare, il cavo è composto da un nucleo conduttore in rame, ricoperto da un materiale isolante, il quale a sua volta è ricoperto da un conduttore cilindrico intrecciato (tipo una rete), protetto da una guaina in plastica. Esistono due tipi di cavi coassiali, usati in base al tipo di segnale. Il 50Ω viene usato per i segnali digitali, mentre il 75Ω per i segnali analogici e per la televisione. Questo cavo veniva usato anche nel campo della telefonia, ma ormai sta venendo rimpiazzato dalla fibra ottica. Viene ancora usato per la tv via cavo e per le MAN.

B.2.4 Fibra ottica

Un sistema di trasmissione ottico si basa su una fonte luminosa, un mezzo di trasmissione e un ricevitore. La presenza di luce indica un 1 mentre l'assenza uno 0. Nel caso della fibra ottica, si utilizza una sottilissima fibra di vetro come nucleo, attraverso la quale viaggia la luce. Alle estremità un ricevitore che "legge" i segnali luminosi e li traduce in segnali elettrici. La buona riuscita della trasmissione del raggio luminoso sta negli indici di rifrazione dei componenti della fibra ottica. Grazie ad essi il raggio luminoso rimane nella fibra e continua il suo percorso fino a destinazione. Infatti il core è ricoperto da un rivestimento di vetro (cladding) che ha un indice di rifrazione più basso, e a sua volta è ricoperto da uno strato protettivo in plastica. Di solito le fibre sono raggruppate in fasci, a loro volta protetti da una guaina esterna.

In base allo spessore del nucleo, la fibra cambia il proprio nome. Se un raggio al suo interno è propagato grazie ai rimbalzi della rifrazione, si dice multimodale (50 microns). Se la fibra è abbastanza sottile da far procedere il raggio quasi in linea retta, si dice monomodale (8-10 microns). Quest'ultima è più costosa ma più efficiente sulle lunghe distanze.

Ci sono tre modi per connettere la fibra ottica:

- collegamento della parte finale ad un connettore in apposite prese, con una perdita del 10-20% del segnale luminoso ma una facile riconfigurazione del sistema
- attaccate meccanicamente, cercando di allinearle al meglio, con una perdita del 10% del segnale
- fusione delle due parti, generando una piccola attenuazione

Le fonti luminose possono essere LED (basso data rate, multimodale, low cost) o laser semiconduttori (alto data rate, sia mono che multimodale, costoso).

Il ricevitore che converte il segnale luminoso in elettrico ha un limite di data rate di 100 Gbps. Inoltre l'interferenza termica può risultare un problema, quindi conviene utilizzare raggi luminosi abbastanza potenti da essere rilevati.

La fibra ottica è una tecnologia relativamente recente, di conseguenza non tutti gli addetti hanno le conoscenze necessarie per installarla od utilizzarla correttamente; può anche danneggiarsi se si piega troppo. Inoltre la trasmissione è monodirezionale, quindi sono richiesti due cavi per andata e ritorno, e le interfacce sono più costose.

Tuttavia ha una maggior ampiezza di banda, richiede meno ripetitori (uno ogni 50km contro uno ogni 5 di quelli in rame), il che porta ad un risparmio, è più sottile, richiedendo quindi meno spazio, è più sicura perché non è possibile intercettare la luce ed infine è più adatta ai luoghi inospitali, in quanto subisce meno interferenze.

B.3 Mezzi wireless

B.3.1 Spettro elettromagnetico

Lo spostamento degli elettroni crea onde elettromagnetiche: il numero di oscillazioni al secondo di un'onda è detta frequenza (misurata in Hz), mentre la distanza tra due massimi è detta lunghezza d'onda (indicata da λ). Un'antenna collegata ad un circuito elettrico riesce a trasmettere onde elettromagnetiche. Nel vuoto le onde viaggiano tutte alla velocità della luce, nei cavi la velocità scende a $2/3$ di quella della luce.

Lo spettro elettromagnetico è composto da diversi tipi di onde in base alla frequenza: radio, microonde, infrarosso, luce visibile, ultravioletti, raggi x e raggi gamma. Queste si possono usare per trasmettere segnali; le ultime tre sarebbero le migliori ma non vengono usate per la difficoltà nel generarle e sono dannose per gli esseri viventi.

Di solito si usa una banda di frequenza ristretta per avere una migliore ricezione, ma in alcuni casi si utilizza la banda larga con due varianti:

- spettro distribuito a frequenza variabile (frequency hopping), dove il trasmettitore salta da una frequenza all'altra centinaia di volte al secondo (adottato dal 802.11)
- spettro distribuito a sequenza diretta (direct sequence)

B.3.2 Trasmissioni radio

Le onde radio sono onde a bassa frequenza, facili da generare, che possono viaggiare per lunghe distanze e attraversano facilmente gli edifici. Queste onde sono omnidirezionali, cioè si espandono in tutte le direzioni, quindi non necessitano che il trasmettitore e il ricevitore siano allineati. Le onde radio sono soggette a interferenze da motori e da altri dispositivi elettrici.

A bande basse (VLF, LF, MF), le onde radio seguono il terreno e si possono ricevere fino a 1000km. Le stazioni radio AM usano le MF che permettono di attraversare facilmente gli edifici. Le bande alte (HF, VHF) sfruttano i rimbalzi contro la ionosfera per ottenere trasmissioni a distanze maggiori.

B.3.3 Trasmissioni a microonde

Sopra i 100MHz le onde viaggiano quasi in linea retta, rendendo possibile la messa a fuoco. Si concentra l'energia in un unico raggio trasmesso tramite un'antenna parabolica, tuttavia è richiesto che sia allineata con l'antenna ricevente. Se da un lato è una limitazione non da poco, dall'altro permette di trasmettere più raggi in parallelo senza interferenze. Quando le antenne sono lontane, entra in gioco la curvatura della terra e sono quindi necessari dei ripetitori. Più sono in alto le antenne, maggiore è la distanza raggiungibile.

Esiste un problema con le microonde. Anche se sono dirette, possono divergere e rifrangere sugli strati più bassi dell'atmosfera, arrivando fuorifase con le dirette, il che può annullare il segnale. L'effetto è detto multipath fading e può essere determinato dalle condizioni climatiche e dalla frequenza. La richiesta di spettro ha portato ad utilizzare frequenze più alte, ma queste hanno il problema di venire assorbite dall'acqua. In entrambi i casi, la soluzione è interrompere la trasmissione in caso di pioggia e utilizzare altri mezzi.

Nonostante questi problemi, le microonde sono molto utilizzate per le comunicazioni telefoniche a lunga distanza, nella telefonia cellulare e nella televisione. Rispetto a mezzi come la fibra, basta una semplice antenna e non è richiesto alcun diritto di passaggio. È inoltre più economica da installare. Esiste però un altro problema, ovvero il bisogno di più frequenze dello spettro. Sono stati stipulati degli accordi per gestire le frequenze utilizzabili (Come? Concorso di bellezza, lotteria, non assegnandole).

B.3.4 Infrarossi

Queste onde sono utilizzate per la comunicazione a cortoraggio (esempio i telecomandi). È un sistema economico ma che non attraversa gli ostacoli solidi. Tuttavia questa limitazione torna comoda in determinate situazioni perché non riuscendo ad attraversare i muri non crea interferenze.

B.3.5 Trasmissioni a onde luminose

La trasmissione utilizzando laser è unidirezionale e richiede quindi due laser e due rilevatori. L'ampiezza di banda offerta è elevata, a costo ridotto e di facile installazione. Tuttavia puntare il laser richiede molta precisione e non posso attraversare pioggia e nebbia. Anche le giornate serene possono creare problemi in quanto il caldo può creare correnti di convezione che deviano il raggio.

B.4 Satelliti

Un satellite è composto da tanti transponder che ascoltano una diversa porzione dello spettro elettromagnetico. Quando riceve un segnale in arrivo, il relativo transponder lo amplifica e lo ritrasmette con frequenza diversa per evitare interferenze. Esistono tre tipi di satelliti in base alla loro posizione: GEO, MEO, LEO.

Vai a §4 per il confronto delle tre tipologie.

B.5 Rete telefonica pubblica commutata

Il PSTN, ovvero Public Switched Telephone Network, rete telefonica pubblica commutata, è uno dei sistemi di comunicazione esistenti.

Il sistema telefonico è strutturato secondo una gerarchia multilivello ad alta ridondanza. Da ogni telefono partono due cavi di rame collegati alla centrale locale (la più vicina). Se la chiamata avviene tra due utenti collegati alla stessa centrale, questa crea una connessione elettrica tra i due e rimane aperta fino al termine della chiamata. Se invece i due telefoni sono collegati a due centrali diverse, le centrali locali si collegano con una centrale interurbana che crea la connessione. Se tuttavia non si collegano alla stessa centrale interurbana, cercano di collegarsi a stazioni intermedie di livello superiore.

I collegamenti locali utilizzano il doppino con segnali analogici, mentre le linee utilizzano le fibre ottiche digitali per collegare le centrali di commutazione.

B.5.1 Collegamenti locali

Il collegamento locale, spesso chiamato anche "ultimo miglio", utilizza tutt'ora la trasmissione analogica. Innanzitutto, per spedire dati digitali devono essere convertiti in analogici dal modem. Una volta giunta la centrale, i dati vengono riconvertiti in digitale. Il ricevente farà la conversione inversa. Il segnale analogico viene trasmesso tramite la variazione di tensione, quindi il segnale ricevuto non sarà mai identico, il che può determinare errori. I problemi sono 3:

- attenuazione, rappresenta la perdita di energia causata dalla propagazione del segnale e dipende dalla frequenza
- distorsione, il segnale si modifica a causa della differenza di velocità con cui si propagano i componenti di Fourier attraverso il cavo

- rumore, cioè l'energia indesiderata generata da sorgenti esterne al trasmettitore

Modem Dato che i problemi descritti sopra sono molto legati alla frequenza, conviene che venga utilizzato un intervallo ridotto. I segnali digitali tuttavia usano un ampio spettro di frequenza e sono quindi molto soggetti ad attenuazione e distorsione. Si utilizza come soluzione la trasmissione AC, introducendo un tono continuo, detto portante d'onda sinusoidale, nell'intervallo 1000-2000 Hz. Modulando ampiezza, frequenza e fase si possono trasmettere le informazioni. Nella modulazione d'ampiezza di usano due ampiezze diverse per indicare 1 o 0. Nella modulazione di frequenza si utilizzano due o più toni. Nella modulazione di fase l'onda portante è spostata di 0 o 180 a intervalli uniformi.

Il modem accetta i bit in ingresso e produce la portante utilizzando i metodi di modulazione (e viceversa).

Il numero di campioni al secondo è misurato in baud. Durante ogni baud viene trasmesso un simbolo, quindi una linea a n baud trasmette n simboli al secondo. Questa misura è detta Baudrate, che è diverso dal Bitrate. Il Bitrate indica quanti bit al secondo (bps) vengono trasmessi, mentre il Baudrate indica il numero di simboli trasmessi. Quindi la differenza tra i due è determinato da quanti bit rappresenta un simbolo ed è determinato dalla tecnica di modulazione utilizzata. Se viene utilizzato il voltaggio $0V=0$ e $1V=1$, allora Bitrate e Baudrate equivalgono, ma se ogni simbolo è composto da 2 o più bit, il Bitrate sarà conseguentemente maggiore. Quando ci sono 4 possibili cambi di fase e quindi un simbolo descrive 2 bit, la tecnica di modulazione è detta QPSK (Quadrature Phase Shift Keying).

Un'altra tecnica di modulazione è la QAM-16, la quale utilizza 4 bit per simbolo (4 ampiezze e 4 fasi). Se vengono utilizzati 5 bit è detta QAM-32, 6 bit QAM-64.

I diagrammi di costellazione indicano le combinazioni valide di ampiezza e fase. Un modem può comunicare solo con altri model che usano la stessa costellazione, ma sono molto soggette ad errori in quanto basta un'alterazione dell'ampiezza o della fase per perdere informazioni. Per risolvere questo problema sono stati introdotti bit di parità per implementare codice di correzione di errori. Questi schemi sono detti TCM (Trellis Coded Modulation). Lo standard V32 usa 4 bit di dati e uno di parità. Il V32 bis usa 6 bit di dati e 1 di parità. Ci sono anche versioni superiori.

I modem moderni permettono la trasmissione bidirezionale utilizzando frequenze diverse. Una connessione che permette di viaggiare **contempora-**

neamente in entrambi i sensi è detta full duplex, mentre half duplex se solo una direzione è supportata. Se permette di viaggiare solo in una direzione è detta simplex (es: fibra ottica).

DSL, Digital Subscriber Line I collegamenti locali che usano il modem si collegano al commutatore con un filtro che limita la frequenza, mentre chi utilizza le tecnologie DLS si connettono ad un diverso commutatore che non presenta il filtro. Quindi il limite non è più il filtro, bensì le proprietà fisiche del mezzo.

Il primo ADSL divideva lo spettro tra:

- servizio telefonico
- upstream
- downstream

La tecnica di divisione è detta multiplexing a divisione di frequenza. Il metodo alternativo è il DMT (Discrete MultiTone), che divide in 256 canali lo spettro. Il canale 0 è per la voce, i canali 1-5 non usati, uno per upstream e uno per downstream, gli altri a disposizione dei dati dell'utente. Quelli liberi per i dati di solito vengono distribuiti secondo il provider tra up e down.

B.6 Linee e multiplexing

Le aziende telefoniche hanno organizzato il sistema per utilizzare un unico collegamento fisico sia per la banda larga che per quella stretta. Per fare ciò viene utilizzato il multiplexing, che si distingue in due tipologie:

- FDM: Frequency division multiplexing, dove lo spettro è diviso in bande di frequenza e ogni utente ha a disposizione solo alcune parti
- TDM: Time division multiplexing, dove la banda viene scambiata per intero tra gli utenti per breve tempo

B.6.1 Multiplexing a divisione di frequenza

[...]

B.6.2 Multiplexing a divisione di lunghezza d'onda

Questo multiplexing è utilizzato per i canali in fibra ottica. [...]

B.6.3 Multiplexing a divisione di tempo

[...]

B.7 Commutazione (*Switching*)

B.7.1 Commutazione di circuito

La commutazione di circuito è la tecnica che crea il percorso fisico tra i due telefoni comunicanti. Quando una chiamata arriva ad una centrale di commutazione, viene stabilita una connessione fisica tra la linea entrante e quella d'uscita della centrale. Questo tipo richiede di configurare il percorso **prima** di iniziare a trasmettere i dati.

B.7.2 Commutazione di messaggio

Questa commutazione non richiede un percorso fisico prestabilito. Quando viene inviato un blocco di dati, questo viene inviato alla prima centrale e vengono instradate un passo alla volta. Ad ogni passo viene controllato che il blocco ricevuto non contenga errori e poi ritrasmesso. Una rete che utilizza questa tecnica è detta *store and forward*. Il blocco può essere di qualsiasi dimensione, richiedendo dischi capaci di memorizzarli temporaneamente, e possono occupare per un tempo considerevole una linea.

B.7.3 Commutazione di pacchetto

Per risolvere i problemi della commutazione di messaggio, si utilizza quella di pacchetto che impone una dimensione massima del pacchetto e si assicura che non occupino per troppo tempo una linea. Un altro vantaggio è che un pacchetto che fa parte di un messaggio può essere mandato prima che finisca di arrivare il successivo. Come per quella di messaggio, non è richiesta la preparazione fisica del percorso prima della trasmissione. I pacchetti possono seguire strade diverse e non arrivare in ordine.

La commutazione di circuito riserva l'ampiezza di banda per tutto il percorso, mentre quella di pacchetto no. Quindi la prima soluzione garantisce il servizio, con spreco di risorse, mentre il secondo no. Anche quella di pacchetto usa la tecnica *store and forward*. Un'altra differenza è che la commutazione di circuito dà libertà di velocità, formato e framing, mentre in quella di pacchetto sono dipendenti dall'onda portante. Ultima differenza riguarda l'addebito: per il circuito dipende da tempo e distanza, per il pacchetto dipende dal volume dei dati.

B.8 Sistema telefonico mobile

B.8.1 Prima generazione - voce analogica

Prima versione: sistema telefonico per auto, che usava un pulsante per attivare il trasmettitore e disattivare il ricevitore. Quindi una sola direzione alla volta.

Seconda versione: IMTS, usa due frequenze, una per trasmettere e una per ricevere. La frequenza disponibile era limitata, quindi richiedeva del tempo per avere la linea libera.

AMPS è il sistema telefonico mobile avanzato da cui deriva la versione digitale D-AMPS. Un'area geografica è divisa in celle di 10-20Km, ognuna delle quali utilizza frequenze diverse da quelle vicine. Il vantaggio di questa organizzazione è che celle vicine (ma non quelle adiacenti) possono usare le stesse frequenze, a differenza del IMTS che si estendeva per 100Km. Si ottiene quindi una maggiore capacità del sistema e riducendo la grandezza delle celle si riesce ad aumentare ulteriormente la capacità, richiedendo anche meno potenza per i trasmettitori. Il principale problema è trovare una posizione elevata per le antenne base, che sono gestite dalla stazione base, di solito al centro di ogni cella. La stazione è composta da un computer e un trasmettitore/ricevitore connesso all'antenna. Le stazioni sono collegate a dei commutatori per il mobile, cioè il MTSO (Mobile Telephone Switching Office). Se la rete è piccola si collegano allo stesso commutatore, altrimenti si crea una gerarchia a livelli simile alla rete telefonica cablata. Viene utilizzata la commutazione di pacchetto.

Quando un telefono abbandona una cella perché il segnale di sta affievolendo, la stazione base verifica la potenza del segnale delle celle adiacenti e trasferisce la gestione del dispositivo. Il telefono è informato del cambiamento e se era in corso una chiamata viene forzato a passare su un altro canale. Questo processo è detto **handoff**. Esistono due tipi:

- soft handoff, dove la nuova stazione acquisisce la gestione del telefono prima di interrompere il segnale; non c'è perdita di continuità ma il telefono deve essere capace di gestire le due frequenze contemporaneamente (solo la terza generazione di telefoni riesce)
- hard handoff, la vecchia stazione rilascia il telefono prima che la nuova lo acquisisca; è un processo abbastanza veloce, ma la chiamata può venire interrotta se la stazione non è in grado di gestire il nuovo dispositivo

AMPS usa 832 canali duplex composti da una coppia di simplex. AMPS usa FDM (Frequency Division Multiplexing) per separare i canali. I canali sono divisi in 4 categorie:

- controllo, dalla base al telefono, per gestire il sistema
- paging, dalla base al telefono, per notificare la chiamata all'utente
- accesso, bidirezionale, per impostare chiamata e canale
- dati, bidirezionale, per voce e dati

Ogni telefono ha una PROM dove sono predeterminati 21 canali per il controllo, il numero seriale e il numero di telefono. Il telefono trasmette queste informazioni in un pacchetto in broadcast per collegarsi alla stazione base più vicina.

Quando si effettua una chiamata, viene trasmesso tramite il canale di accesso il numero da chiamare e la propria identità. Una volta che la richiesta raggiunge la stazione, questa comunica con il MTSO che cerca un canale libero per la chiamata. Quando trovato, viene trasmesso il numero nel canale di controllo e il telefono passa al canale vocale in attesa di risposta.

B.8.2 Seconda generazione - voce digitale

Per la seconda generazione sono utilizzati 4 sistemi qui esposti.

D-AMPS È la seconda generazione di AMPS, orientata al digitale. La versione digitale utilizza le stesse frequenze di AMPS, quindi vengono divisi i canali tra digitali e analogici. La ripartizione può cambiare dinamicamente in base al tipo di dispositivi presenti nella cella. Sta al MTSO della cella la gestione della distribuzione.

Per gestire l'aumento di carico, è stata prevista una nuova banda di frequenza.

Il segnale vocale viene raccolto dal microfono, digitalizzato e compresso dal *vocoder*. Questo processo è molto importante per la telefonia mobile con D-AMPS perché offre un ottimo miglioramento utilizzando il TDM. [...]

GSM [...]

CDMA [...]

PDC Usato solo in Giappone, non approfondito.

B.8.3 Terza generazione - voce e dati digitali

Per la terza generazione si puntava ad un'unica tecnologia per semplificare la diffusione e lo sviluppo dei dispositivi che dovevano utilizzarla. Ci sono state diverse proposte e dopo una selezione rimasero due possibilità: W-CDMA e CDMA2000. Il primo utilizzava una modulazione a spettro distribuito a sequenza diretta, pensato per interagire con GSM, in modo da poter entrare nelle celle di quest'ultimo senza perdere le chiamate. La seconda proposta si basava anch'essa sulla modulazione a spettro distribuito a sequenza diretta, ma non punta all'interazione con GSM.

Nel frattempo alcuni operatori proposero alcuni schemi detti *2.5G*; uno è EDGE, un GSM con un bit in più per baud. Il bit in più porta anche a più errori. L'altra proposta è GPRS, una rete a pacchetti costruita sopra D-AMPS e GSM. Questa permette di inviare/ricevere pacchetti IP in una cella vocale; vengono riservati alcuni slot temporali al traffico di pacchetti e la stazione base definisce il numero e la posizione degli slot. Gli slot disponibili sono divisi in canali logici, la stazione base determina l'associazione tra i canali logici e time slot. Un canale logico è usato per scaricare i pacchetti dalla stazione base nella stazione mobile e ogni pacchetto indica il destinatario.

Per inviare un pacchetto IP, una stazione mobile chiede uno o più slot inviando una richiesta alla stazione base. Se la richiesta arriva senza problemi, la stazione comunica all'apparecchio mobile la frequenza e gli slot che dovrà utilizzare per trasmettere il pacchetto. Una volta arrivato alla stazione base, il pacchetto è trasferito su Internet attraverso una connessione via cavo.

C Capitolo 3 - Strato data link

C.1 Progetto dello strato data link

Lo strato data link ha diverse funzioni, tra cui:

- fornire un servizio di interfaccia per lo strato network
- gestire gli errori di trasmissione
- regolare il flusso dati

Per svolgere le sue funzioni, lo strato data link riceve i pacchetti dallo strato network e li incapsula in frame. Un frame contiene header, carico e coda.

C.1.1 Servizi forniti allo strato network

Il servizio principale è quello di trasferire i dati tra gli strati network di due macchine differenti. Alcuni servizi forniti sono:

- unacknowledged senza connessione
- acknowledged senza connessione
- acknowledged orientato alla connessione

Il primo consiste nell'invio di frame senza che la macchina di destinazione debba dare l'acknowledgement, ovvero la conferma della ricezione. Non viene creata una connessione logica e non ci si assicura che il frame arrivi a destinazione. Si utilizza quando gli errori di trasmissione sono limitati, così da permettere la correzione direttamente agli strati superiori e quando si vuole una comunicazione real-time dove il ritardo è peggio di una ricezione di dati parzialmente errati (es: chiamate, stream video).

Il secondo offre una maggiore affidabilità in quanto è richiesto l'acknowledgement. Se non viene ricevuto entro un certo intervallo, può essere rispedito il frame. Anche questo non usa una connessione logica. L'acknowledgement può essere richiesto direttamente dallo strato network, ma si presenta un problema di prestazioni. Il strato network può richiedere la spedizione dell'intero pacchetto nel caso non arrivi l'acknowledgement, che non ha limiti di dimensioni. Un frame invece è di dimensione ridotta e limitata, per cui è più facile gestire il reinvio del singolo frame rispetto al pacchetto intero.

Il terzo tipo è il più affidabile. Oltre alla richiesta di acknowledgement, deve stabilire una connessione con il destinatario prima di iniziare la trasmissione. I frame sono numerati ed è garantito l'arrivo nell'ordine corretto. Il trasferimento dei dati avviene in 3 fasi: stabilita la connessione, trasmissione dei frame, rilascio della connessione.

C.1.2 Suddivisione in frame

Lo strato data link deve ricevere dallo strato fisico i dati sottoforma di bit e verificare che siano corretti ed eventualmente correggerli. Per fare ciò viene suddiviso il flusso di bit in una serie di frame e viene calcolato il checksum (vai a §??) per ogni frame. Una volta giunto a destinazione il frame, viene ricalcolato il checksum e se è differente da quello del frame, lo strato sa che c'è stato un errore e prende i relativi provvedimenti.

La suddivisione non è un'operazione banale. Ci sono diversi metodi per farlo, spiegati di seguito.

Conteggio dei caratteri Questo metodo usa un campo dell'intestazione per indicare il numero di caratteri nel frame. In questo modo quando viene letto il frame sa dove termina. Il problema è che un errore può alterare il conteggio, mandando il destinatario fuori sincronia. Anche utilizzando il checksum non è possibile sapere dove inizia il frame successivo. Per questi problemi, il metodo non è più usato.

Byte stuffing Un secondo metodo utilizza un byte all'inizio e alla fine del frame come flag byte. Di solito i byte utilizzati sono gli stessi. Questo metodo permette di trovare il frame successivo nel caso un errore faccia perdere la sincronia. Tuttavia il problema di questo metodo si presenta quando vengono trasmessi file binari, in quanto il valore del flag byte potrebbe essere presente nel frame. Per risolvere questo problema è possibile usare la tecnica del Byte stuffing, ovvero viene inserito un carattere di escape prima di ogni occorrenza nel frame del byte flag, in modo da distinguerli effettivamente dai flag; lo strato data link di destinazione rimuoverà gli escape.

Bit stuffing Il Byte stuffing è limitato perché è legato a caratteri di 8 bit, ma se si usano codifiche diverse risulta un problema.

Con la nuova tecnica è possibile usare sia un numero arbitrario di bit, sia codifiche varie. Ogni frame comincia e finisce con il gruppo di bit 01111110, di fatto un flag byte. Se nel flusso vengono letti 5 bit 1 consecutivi, viene

messo un bit 0 in coda, mentre nella destinazione verrà rimosso. Questa tecnica è detta bit stuffing.

C.1.3 Controllo errori

Problema: assicurarsi che i frame arrivino tutti a destinazione e nell'ordine corretto.

Un modo è quello di utilizzare un acknowledgement, positivo o negativo, per notificare l'arrivo del frame. Tuttavia, anche l'acknowledgement può andare perso. Si utilizza quindi un timer che parte insieme all'invio del frame. Se viene ricevuto l'acknowledgement, viene ignorato il timer, altrimenti allo scadere del tempo viene rispedito il frame. Per evitare doppioni, i frame hanno un numero di sequenza in modo che se la destinazione aveva già ricevuto il frame possa ignorarlo.

C.1.4 Controllo di flusso

Il controllo del flusso consiste nella gestione della velocità di trasmissione dei frame, in modo da non congestionare il destinatario se non riesce ad elaborare ciò che riceve abbastanza velocemente.

C.2 Rilevazione e correzione errori

Gli errori di trasmissione è un problema difficile da evitare, in particolare per i collegamenti locali che sono ancora analogici.

C.2.1 Codici per la correzione degli errori

Per gestire gli errori ci sono due possibilità. O si aggiungono dei dati ridondanti di parità che permettono di ricostruire il contenuto del blocco (codifica a correzione d'errore), o si utilizza abbastanza ridondanza da poter identificare la presenza di un errore, senza però poterla correggere, e vengono quindi ritrasmessi (codifica a rilevazione d'errore). I canali affidabili come la fibra utilizzano la rilevazione, mentre quelli più soggetti a disturbi come il wireless usano la correzione.

Ma in cosa consiste un errore?

Un frame è composta da m bit di dati e r bit ridondanti, con un totale di n bit. Gli n bit sono detti codeword. Date le due parole, si possono confrontare con lo XOR per vedere quanti bit sono differenti; il numero di bit è detta la distanza di Hamming ed indica il numero di errori su singoli bit per convertire da una sequenza all'altra.

La rilevazione e la correzione degli errori dipende dalla distanza di Hamming. Per trovare d errori è necessaria una codifica con $d+1$ di distanza; in questo modo riesce a rilevarli, ma non a correggerli. Per correggere d errori è invece necessaria una codifica con $2d+1$ di distanza, in modo che anche con d cambiamenti, la codeword originale rimane la più vicina a quella modificata ed è ricavabile univocamente.

Le codifiche di Hamming riescono a correggere solo errori singoli. Si riesce a correggere gli errori burst sfruttando un trucco, ovvero inviando i dati di una matrice per colonna invece che per riga.

C.2.2 Codifiche a rilevazione d'errore

Su canali più affidabili, la rilevazione basta in quanto gli errori sono meno frequenti e risulta più efficiente rimandare i dati danneggiati. Questo perché maggiore è la grandezza del blocco, maggiore è il numero di bit di controllo richiesti.

In alternativa alla tecnica della matrice, si usa la codifica polinomiale (CRC - Cycle Redundancy Check). Questa tecnica considera le sequenze di bit come polinomi a coefficienti con valori uguali a 0 o 1. Un frame di k bit è un polinomio di grado $k-1$ con k termini.

Esempio: $110001 \rightarrow 1*x^5 + 1*x^4 + 0*x^3 + 0*x^2 + 0*x^1 + 1*x^0 \rightarrow x^5 + x^4 + 1$

Per utilizzare la codifica polinomiale, sorgente e destinazione devono definire un polinomio generatore $G(x)$. I bit di ordine più alto e più basso devono essere uguali a 1. Il checksum di un frame è calcolabile se il polinomio relativo al frame è di grado maggiore (banalmente deve avere più bit) rispetto al polinomio generatore. Si aggiunge un checksum alla fine del frame in modo che il relativo polinomio sia divisibile per $G(x)$. Se c'è un resto, significa che c'è stato un errore.

Calcolare il checksum:

1. dato il grado g di $G(x)$, aggiungere g bit con valore zero in coda al frame, ottenendo il polinomio $M(x)$
2. fare la divisione $M(x) / G(x)$
3. sottrarre il resto dalla $M(x)$; ne risulta il frame con il checksum pronto alla trasmissione con polinomio $T(x)$

Divisione e sottrazione vanno effettuate in modulo 2: la sottrazione equivale allo XOR, mentre la divisione sono fatte come nel binario normale ma con le differenze in modulo 2.

Questo metodo riesce a risolvere gli errori provocati da interferenza, rumore e distorsione.

C.3 Protocolli data link elementari

Un frame è composto da 4 campi: kind, seq, ack, info. I primi 3 contengono informazioni di controllo e fanno parte dell'header, mentre info contiene i dati effettivi. Kind indica se ci sono dati nel frame. Seq contiene i numeri di sequenza. Ack contiene l'acknowledgement.

Lo strato network passa un pacchetto con un'intestazione di tipo network allo strato data link, il quale pone il pacchetto nel campo info di un frame.

C.3.1 Simplex senza restrizioni

Protocollo in cui i dati sono trasferiti in una sola direzione (simplex) e non ci sono altre restrizioni (buffer infinito, strati pronti, tempo di elaborazione ignorabile, in canale non perde mai frame). E' chiaramente un protocollo non realistico, solo d'esempio.

Il mittente invia i dati alla massima velocità possibile in un loop infinito. Nel loop viene preso il pacchetto dallo strato network, costruisce il frame e instrada il frame. Il destinatario attende l'arrivo di un frame, salvato nel buffer; viene prelevato dal buffer e passato il contenuto del frame allo strato network, infine torna ad attendere.

C.3.2 Simplex stop-and-wait

In questo protocollo si assume il traffico simplex e l'assenza di errori, ma con la restrizione più realistica di una velocità di elaborazione non più infinita. Il problema da considerare quindi è la gestione del flusso, in modo che il mittente non inondi il ricevente con una velocità di trasmissione maggiore di quella di elaborazione. Se ci vuole un intervallo t per elaborare un frame, il mittente non dovrebbe trasmettere più di un frame per t . Se inoltre non ci sono meccanismi di buffer, il mittente non deve trasmettere il nuovo frame finché il precedente non è stato prelevato dallo strato fisico o verrebbe sovrascritto. La soluzione al problema è l'utilizzo di un frame senza informazioni che viene rispedito al mittente quando il pacchetto è stato fatto passare allo strato network, in modo da notificare il mittente per l'invio di un nuovo frame. Il pacchetto funge da acknowledgement e blocca il mittente fino a quando non arriva il frame. Questi protocolli basati sull'attesa dell'acknowledgement sono detti **stop-and-wait**. Data la richiesta di far viaggiare

i frame in entrambe le direzioni, è necessaria un'alternanza del flusso e un canale fisico half-duplex può bastare.

Il mittente prende il pacchetto dallo strato network, costruisce il frame e instrada il frame. A questo punto attende l'acknowledgement; quando lo riceve, manda un altro frame. Il destinatario invece processa il frame e prima di tornare in attesa manda il frame di acknowledgement al mittente.

C.3.3 Simplex per canali rumorosi

Protocollo per una situazione normale, sempre simplex, dove i frame possono essere danneggiati o persi. Se il frame è danneggiato, viene usato il checksum per verificare la correttezza. Per far fronte al problema della perdita di frame, sia dati, sia di acknowledgement, si utilizza un timer e il numero di sequenza dei frame. Il problema successivo è decidere quanti bit usare per il numero di sequenza. L'unica ambiguità possibile è tra il frame stesso e il successivo, quindi è sufficiente un bit.

Il mittente prima memorizza in una variabile locale il numero di sequenza del successivo frame da inviare, poi crea il frame, lo instrada e fa partire il timer. Rimane in attesa: riceve un acknowledgement positivo, o un acknowledgement con problemi, o il scade il timer. Nel primo caso prende in carico il frame successivo, negli altri due viene rimandato il frame. Il destinatario riceve il frame, controlla il numero di sequenza: se è valido, lo processa, lo passa allo strato network, ritorna l'acknowledgement e aggiorna la variabile del numero di sequenza.

C.4 Protocolli sliding window

Questi protocolli sono utilizzati per le trasmissioni in entrambe le direzioni, full duplex. Si possono usare due canali separati simplex, ma di solito quello di ritorno è sprecato; conviene usare un unico canale e gestire entrambe le direzioni. Una miglioria successiva è la tecnica del piggy-backing, ovvero quando arriva un frame dati, non viene restituito subito il frame di acknowledgement, bensì viene aggiunto al frame di dati successivo passato dallo strato network, in modo da "risparmiare" un viaggio e sfruttare al meglio la banda. Infatti aggiungere il campo ack nell'intestazione è più conveniente rispetto a creare un intero frame con sua intestazione, checksum e acknowledgement. Il problema di questa tecnica è l'estendersi dell'attesa dell'acknowledgement. Per quanto tempo deve aspettare lo strato data link prima di mandare l'acknowledgement in maniera indipendente?

I protocolli seguenti sono strettamente legati al buffer, in quanto il mittente avrà una "finestra d'invio", ovvero un insieme di frame che può inviare, e il destinatario ha una "finestra di ricezione", ovvero un insieme di frame che può ricevere. Le due finestre non devono essere grandi uguali e possono avere dimensione variabili. Queste danno una maggior libertà di invio dei frame, ma il passaggio allo strato network deve comunque mantenere l'ordine. I numeri di sequenza nella finestra d'invio indica i frame trasmessi o in transito, che sono attesi dell'acknowledgement. Quando arriva un pacchetto dallo strato network il limite superiore aumenta di uno, mentre quando arriva un acknowledgement il limite inferiore aumenta di uno. Se la finestra di invio contiene n frame, il mittente dovrà avere almeno n buffer per mantenere i frame fino all'arrivo dell'acknowledgement.

C.4.1 Sliding window a 1 bit

Questo protocollo utilizza una finestra di un bit, risultando quindi simile al protocollo stop-and-wait. La differenza è che ora la trasmissione è full duplex. Di conseguenza può accadere che entrambi i computer vogliano mandare un pacchetto, creando ridondanza in quanto vengono mandati pacchetti duplicati senza che siano necessari.

C.4.2 Go back N e Ripetizione selettiva

Il tempo per trasmettere un frame sommato al tempo per ricevere l'acknowledgement a volte non è trascurabile (nei precedenti protocolli era considerato tale). Infatti si può arrivare a sprecare fino al 90% di tempo durante il quale il sorgente rimane in attesa per inviare un nuovo pacchetto. Il problema deriva dalla richiesta di far attendere il sorgente. Con la tecnica detta pipelining si attenua il problema, inviando n frame nell'intervallo totale di transito (dall'invio alla ricezione dell'ack) senza riempire completamente la finestra. Il numero di frame inviabili indica la grandezza della finestra. Maggiore è il ritardo di trasmissione, maggiore sarà la grandezza della finestra. Il prodotto tra banda e ritardo di trasmissione indica la capacità della pipeline. Usandola tutta, il sorgente opera a massima efficienza. Dati:

- c - capacità del canale
- d - dimensione del frame
- T - tempo totale di propagazione

l'utilizzo della linea è uguale a $d/(d+cT)$. Se $d < cT$, l'efficienza sarà minore del 50%.

Con il pipelining, se dei frame vengono danneggiati o persi si verificano diversi problemi. Il destinatario non sa cosa fare con i frame seguenti a quello danneggiato. Per ripristinare gli errori ci sono due tecniche, una delle quali è il go back N.

Questa tecnica richiede di scartare tutti i frame successivi a quello danneggiato senza mandare l'acknowledgement per questi. In particolare il sorgente manda tutto in sequenza, non sapendo se arrivano errati a destinazione, finché non termina i frame della finestra. Quando scade il timer dell'acknowledgement che non sarà ricevuto, il mittente rimanda i frame in sequenza a partire da quello danneggiato, anche se i successivi erano corretti. Il destinatario invece, quando riceve il frame danneggiato si rifiuta di accettare tutti i successivi finché non riceve quello con il numero di sequenza atteso. Di fatto questo protocollo utilizza una finestra di ricezione con 1 frame.

L'altra tecnica per ripristinare gli errori è la ripetizione selettiva. In questo caso viene scartato solo il frame danneggiato, mentre i successivi corretti vengono messi in un buffer. Quando il sorgente va in timeout rimanda il frame danneggiato. Il destinatario lo riceve e passa allo strato network il frame ricevuto più tutti quelli nel buffer, mantenendo l'ordine corretto e ritornando l'ack. In particolare, quando il ricevente trova un frame danneggiato, viene mandato un NAK, un acknowledgement negativo. Il NAK migliora le prestazioni in quanto triggera il sorgente a rimandare il pacchetto prima che scada il timer. Se venisse perso il NAK, ci sarebbe comunque il timer del sorgente. Questo protocollo utilizza una finestra di ricezione maggiore di 1. La dimensione massima della finestra dovrebbe essere uguale alla metà della sequenza dei numeri; invece il numero di buffer della destinazione deve essere uguale alla dimensione della finestra.

I due approcci dipendono molto dall'uso della banda e del buffer. Il primo si basa sulla banda, dovendo rimandare tutto, il secondo sul buffer, dato che salva i frame corretti in attesa di quello mancante.

C.5 Esempi di protocolli

C.5.1 HDLC - High-level Data Link Control

Questo protocollo è orientato ai bit e utilizza il bit stuffing. Il frame di questo protocollo ha il campo address, control, data e checksum. Address indica il terminale; control è usato per i numeri di sequenza; data contiene

le informazioni; checksum è il codice di ridondanza. Il frame è delimitato dal flag 01111110. [...]

C.5.2 PPP - protocollo punto a punto

Il PPP è un protocollo data link usato da internet. Tra le caratteristiche ci principali ci sono:

- metodo di framing
- protocollo per la gestione della connessione - LCP (Link Control Protocol)
- una modalità per negoziare le opzioni dello strato network in modo indipendente dalla sua implementazione

Il frame PPP assomiglia a quello HDLC, tuttavia è orientato ai caratteri, quindi usa il byte stuffing. Il flag usato è sempre quello di HDLC; i caratteri di escape vengono aggiunti su tutto il frame (non solo sui dati) dopo il calcolo del checksum e vengono tolti in ricezione prima del ricalcolo del checksum. Ha il campo address sempre impostato a 11111111 per indicare che tutte le stazioni devono accettarlo; segue il campo control che di default vale 00000011. Dato che questi campi sono costanti, LCP permette di omettere questi campi nella configurazione. Il campo protocol indica il tipo di pacchetto contenuto nel campo payload. L'ultimo campo contiene il checksum. [...]

D Capitolo 4 - Sottostrato MAC

Il sottostrato MAC riguarda i canali multiaccesso, ovvero i canali usati delle reti broadcast. C'è bisogno di regolamentare l'accesso al canale in qualche modo.

D.1 Il problema dell'assegnazione del canale

Come assegnare un singolo canale broadcast tra diversi utenti in competizione?

D.1.1 Assegnazione statica

Di solito per condividere un canale tra più utenti si usa il multiplexing a divisione di frequenza FDM. La banda viene suddivisa in parti uguali le quali sono assegnate agli utenti. Ognuno ha una propria frequenza, quindi non c'è interferenza tra loro. FDM funziona bene se non ci sono troppi utenti e se il numero è abbastanza costante. Se non lo è, ci sono dei problemi. Se gli utenti sono minori della divisione della banda, ci sarà uno spreco; se sono di più, alcuni utenti non riusciranno a comunicare.

In generale, un'assegnazione statica è poco efficiente perché anche mantenendo costanti gli utenti, quando non usano il canale quella banda rimane inutilizzata. Anche con TDM la situazione non cambia molto.

D.1.2 Assegnazione dinamica

Ci sono 5 premesse riguardo il problema dell'assegnazione del canale.

- Modello della stazione: n stazioni indipendenti che generano frame in trasmissione; quando viene generato un frame, la stazione attende finché non viene spedito
- Presupposto del canale singolo: un solo canale per trasmettere e ricevere
- Presupposto della collisione: due frame trasmessi assieme si sovrappongono creando distorsione e rendendo il frame non valido; le stazioni possono rilevare questo evento detto collisione e richiedere la ritrasmissione del frame
- Tempo continuo e Tempo diviso in intervalli: nel primo caso la trasmissione può avvenire in qualsiasi istante, mentre nel secondo il tempo è

diviso in slot e la trasmissione di un frame coincide sempre con l'inizio di un intervallo

- Occupazione del canale verificabile o meno: le stazioni possono o meno verificare se un canale è occupato; se possono verificare, la trasmissione dipende dall'esito, se non possono mandano il frame a priori

D.2 Protocolli ad accesso multiplo

D.2.1 Aloha

Aloha è un sistema sviluppato inizialmente per collegare le isole della Hawaii, basato su una trasmissione radio broadcast con singolo canale. Ne esistono due versioni.

Aloha puro L'idea di base è quello di consentire agli utenti di trasmettere ogni qual volta ne avessero bisogno. Anche se ci sono collisioni, la proprietà di feedback della trasmissione broadcast permette al trasmettitore di scoprire se il frame è danneggiato. Se non è possibile ascoltare il canale, è necessario un sistema di acknowledgement. Se il frame è stato distrutto, il trasmettitore attenderà per un tempo **casuale** prima di ritrasmettere il frame altrimenti si ripeterà la collisione. I sistemi con un canale condiviso dove si possono generare conflitti si dicono sistemi a contesa.

I frame trasmessi sono tutti della stessa lunghezza e vengono inviati completamente a caso. Se anche un solo bit va in collisione, entrambi i due frame vanno buttati. Non c'è modo di capire se c'è stato un conflitto parziale o totale.

Aloha slotted Alcuni anni dopo venne proposta l'alternativa slotted Aloha, la quale permette di duplicare la capacità del sistema dividendo il tempo in intervalli discreti, dove ogni intervallo corrisponde un frame. In questo sistema non viene inviato un frame in un momento a caso, ma solo all'inizio dell'intervallo successivo. Questa soluzione riduce le collisioni, ma richiede un meccanismo di sincronizzazione per gestire l'invio dei frame solo all'inizio di un intervallo.

Questa tecnica fu rispolverata quando fu inventato l'accesso a internet via cavo, dovendo gestire un canale condiviso.

D.2.2 Protocolli ad accesso multiplo con rilevamento della portante

Con i protocolli Aloha si hanno molte collisioni. Se invece le stazioni rimangono in ascolto di una portante è possibile migliorare le prestazioni.

CSMA persistente e non Un esempio di questi protocolli è il CSMA 1-persistente. Una stazione prima di trasmettere ascolta il canale per sapere se è occupato. Se lo è attende e appena si libera manda un frame; in caso di collisione la stazione rimane in attesa di un intervallo casuale per poi rimandare il frame. 1-persistente indica che la stazione trasmette con probabilità 1 quando il canale è libero (cioè lo fa sempre). Il problema è che il ritardo di propagazione potrebbe creare l'illusione di avere un canale libero, quando in verità il canale è già stato occupato ma il segnale non ha ancora raggiunto la stazione che ne richiede l'utilizzo. Anche con ritardo zero potrebbe verificarsi una collisione in quanto due stazioni potrebbero attendere contemporaneamente. Questo protocollo risulta migliore dell'Aloha puro.

Un altro protocollo è detto CSMA non persistente, il quale se trova il canale occupato non rimane subito in attesa, bensì riprova dopo un intervallo casuale. Si ha un migliore utilizzo del canale ma aumenta i ritardi.

Esiste anche il CSMA p-persistente, dove p indica la probabilità di trasmettere nel canale se è libero. A differenza del 1-persistente, la probabilità sarà minore di 1, quindi potrebbe non trasmettere subito e rimandare a più tardi.

CSMA con rilevamento delle collisioni Esiste un miglioramento dei CSMA persistenti, con un protocollo detto CSMA/CD (collision detection). In questo protocollo, quando una stazione inizia la trasmissione e rileva la collisione, termina subito la trasmissione; dopo un intervallo di tempo casuale ritenta la trasmissione. In questo modo si risparmia tempo e banda. Viene molto usato nel sottostrato MAC delle LAN.

Piccola nota: nessun protocollo del sottostrato MAC garantisce consegna affidabile. Potrebbero non esserci collisioni, ma il ricevitore potrebbe comunque copiare in frame non correttamente.

D.2.3 Protocolli senza collisione

Nei seguenti protocolli si presuppone che ci siano N stazioni identificate da un indirizzo che va da 0 a $N-1$ e che il ritardo sia trascurabile. Questi protocolli risolvono la contesa senza creare collisioni.

Protocollo a mappa di bit elementare In questo protocollo, ogni periodo di contesa è composto da N intervalli. Ogni stazione indicherà tramite un bit se deve trasmettere un frame. Il bit viene posto nel rispettivo intervallo in base all'indirizzo della stazione (stazione 0 in 0, stazione $N-1$ in $N-1$). Al termine degli N intervalli, tutte le stazioni sono a conoscenza di chi ha bisogno di trasmettere e lo fanno secondo l'ordine dell'indirizzo. Essendo prestabilito l'ordine, non avverranno collisioni. Al termine della fase di trasmissione, ci sarà un nuovo periodo di contesa dove si ripeterà il processo di "prenotazione". Ogni stazione può porre il proprio bit "pronto" solo nel suo intervallo e può farlo se ha effettivamente il frame preparato. Se la stazione diventa pronta ma il suo intervallo è passato, dovrà attendere la prossima fase di contesa.

Questo tipo di protocolli sono detti protocolli a prenotazione.

Conteggio binario Il problema del metodo della mappa è la richiesta del bit di controllo: se ci sono tante stazioni, sono richiesti tanti bit (uno per stazione). Un'alternativa è quella di utilizzare indirizzi binari per le stazioni. Una stazione che vuole trasmettere lo comunica agli altri tramite il proprio indirizzo, spedito sotto forma di stringa partendo dal bit più a sinistra. Dato che gli indirizzi sono tutti lunghi uguali, i bit nella stessa posizione sono elaborati tramite OR: se il risultato è un 1, tutte le stazioni con bit 0 si arrendono; poi si passa al confronto del bit successivo con le stazioni rimanenti e se risulta uno 0 si passa al bit successivo, se un 1, si arrendono quelle con lo 0 e si prosegue, finché non rimane una stazione e sarà quella che spedisce il frame. Questo protocollo è detto conteggio binario e chiaramente introduce un livello di priorità tra le stazioni (max priorità l'indirizzo più grande), che in base alle situazioni può essere vantaggioso o meno.

Al momento è un protocollo inutilizzato nonostante la semplicità.

D.2.4 Protocolli a contesa limitata

Meglio i protocolli a contesa o senza collisioni? Il primo è preferibile per il basso ritardo quando il carico è leggero, ma al crescere del carico peggiora l'efficienza. Il secondo funziona all'opposto.

I protocolli a contesa limitata si pongono a metà strada tra i due. Questi protocolli dividono le stazioni in gruppi (anche non esclusivi) e in ogni gruppo le stazioni competono tra loro per un determinato intervallo: il gruppo 0 per l'intervallo 0, il gruppo 1 per l'1, e così via. Il trucco sta nel ripartire

le stazioni nel modo ottimale. La soluzione migliore è quella di assegnare dinamicamente in base al carico.

Adaptive Tree Walk Questo metodo sfrutta gli alberi binari. Nel primo intervallo di contesa (0), tutte le stazioni tentano di acquisire il controllo. Se non riescono perché c'è una collisione, le stazioni vengono divise in due gruppi e nel successivo intervallo (1) provano ad ottenere il canale quelle del secondo nodo. Se la trasmissione avviene con successo, l'intervallo successivo (2) va al nodo 3, altrimenti si suddivide il 2 in due sottogruppi e così via.

A carico elevato si dovrebbe iniziare già a livelli più bassi dell'albero.

D.2.5 Protocolli LAN Wireless

Esempio di LAN wireless: un ufficio con stazioni base (o access point) sparsi e collegate tra loro tramite cavi. Regolando la potenza del segnale attorno a 3-4 metri, si ottiene una situazione dove le stanze sono considerabili come delle celle. Una cella ha un unico canale che copre tutta la banda ed è disponibile a tutte le stazioni. Nel caso della LAN wireless il problema non è il trasmettitore bensì il ricevente. Infatti considerando delle stazioni con portata limitata, dove A raggiunge B, B raggiunge C, ma A e C non comunicano direttamente, potrebbe accadere che A cerca di comunicare con B, mentre C che non sente A pensa sia tutto libero e cerca di comunicare con B. Il risultato è che A e C creeranno una collisione, danneggiando i frame. Questo **problema** è detto **della stazione nascosta**. All'inverso, se B trasmette ad A e C controlla la banda portante per trasmettere a D, siccome rileva la trasmissione di B pensa che anche D sia occupato. In questo caso si dice **problema della stazione esposta**.

MACA e MACAW MACA (Multiple Access with Collision Avoidance) è uno dei primi protocolli per LAN wireless. Il trasmettitore invita il ricevitore ad inviare un piccolo frame per indicare che alle stazioni vicine che è occupato, in modo da poter inviare subito dopo il frame dati effettivo. In particolare: A vuole trasmettere a B; manda un RTS (request to send) a B che contiene la lunghezza del frame dati in arrivo; B risponde con un CTS (clear to send) che contiene la lunghezza dei dati, copiata dal RTS. In questo modo A può mandare il frame quando ha ricevuto la CTS.

Le stazioni vicine ad A che ricevono RTS devono stare in silenzio per attendere che CTS arrivi ad A. Viceversa, le stazioni vicine a B che ricevono CTS devono stare in silenzio per permettere la trasmissione del frame dati.

In caso di collisione verrà effettuato un secondo invio con intervallo di tempo casuale.

Esiste poi la versione migliorata MACA per wireless, ovvero MACAW. In questo protocollo è stato introdotto un frame ack dopo la trasmissione dati avvenuta con successo, ed è stata aggiunta la possibilità di bloccare le stazioni vicine che stanno mandando un RTS quando ce n'è già uno in viaggio verso la stessa destinazione.

D.3 Ethernet

Gli standard più importanti:

- 802.3 - Ethernet
- 802.11 - LAN wireless

Hanno sottostrati fisici e sottostrati MAC differenti, ma hanno la stessa interfaccia verso lo strato network.

D.3.1 Cablaggio Ethernet

Ethernet è il nome del cavo utilizzato per 802.3 e ne esistono 4 tipi. Il modello più vecchio è il 10base5, o thick Ethernet. Il cavo è piuttosto spesso e le connessioni sono realizzate mediante spine a vampiro (?). Il nome indica che opera a 10Mbps con segnali a banda base e sopporta segmenti lunghi fino a 500 metri.

Il secondo cavo è 10Base2 o thin Ethernet; come per il precedente, dal nome si sa che opera a 10Mbps con segnali a banda base e sopporta segmenti lunghi fino a 200 metri circa. In questo caso le connessioni sono fatte mediante connettori BNC che formano giunzioni a T; sono più facili da usare e più affidabili. Questo cavo è economico, semplice da installare, ma supporta solo segmenti di 185 metri e un massimo di 30 macchine.

I guasti sono un problema per le connessioni cablate; per questo esistono tecniche per rintracciare i guasti, come la TDR (Time Domain Reflectometry), la quale usa un impulso per vedere se è tutto apposto. Se ci sono guasti o ostacoli si genera un eco che torna indietro e cronometrando il tempo di ricezione dell'eco è possibile identificare la distanza dell'origine dell'eco.

Dal problema del tracciamento guasti, si è passati all'utilizzo di hub; le stazioni sono collegate agli hub tramite doppini non condivisi. Questo hub non elabora il traffico. Questa configurazione permette di aggiungere e rimuovere stazioni facilmente ed ha una facile individuazione le interruzioni della linea. Tuttavia i cavi che partono dall'hub possono raggiungere solo i

100/200 metri. Nonostante questo è diventato uno standard per la facilità di gestione e per l'uso dei cablaggi presistenti. Lo schema presentato è detto 10Base-T.

Un altro tipo di cavi è il 10Base-F che utilizza le fibre ottiche. Questa alternativa è costosa a causa del prezzo di connettori e terminatori, ma è immune alle interferenze e permette i collegamenti a lunghe distanze (1km).

D.3.2 La codifica Manchester

Utilizzare una codifica binaria corretta è un problema non indifferente, perché vanno scelti valori che non possono creare ambiguità. Deve essere ben chiaro quando si ha l'inizio e la fine di un bit. Esistono due tecniche: la codifica di Manchester e la codifica di Manchester differenziale.

La prima utilizza un periodo di bit diviso in due intervalli uguali, dove l'1 binario è identificato da un picco di tensione nel primo intervallo e un livello basso nel secondo intervallo. Lo zero binario è l'opposto. Il cambio di tensione in mezzo al periodo di bit permette al ricevitore di sincronizzarsi con il trasmettitore; tuttavia occupa il doppio della banda rispetto alla codifica elementare.

La codifica di Manchester differenziale è un'alternativa dove un 1 binario è identificato dall'assenza di cambio di tensione tra un periodo di bit e un altro, mentre se avviene una transizione identifica uno zero. Questa codifica è più complessa ma ha una maggiore immunità ai rumori. Tuttavia Ethernet usa la Manchester base.

D.3.3 Il protocollo del sottostrato MAC Ethernet

Esistono due varianti di frame: quello DIX Ethernet e quello dello standard IEEE. Lo standard apporta solo delle piccole modifiche a due campi (type diventa length, preamble viene ridotto), tuttavia DIX aveva già preso piede a tal punto che pochi erano disposti a passare al nuovo standard. Tuttavia il campo type prima della creazione dello standard era sempre maggiore di 1500, quindi se è più corto viene considerato come campo length dello standard. Con questo compromesso si riuscì ad usare entrambi i frame.

Più nello specifico, il frame DIX è composto da:

- preamble
- indirizzo di destinazione
- indirizzo d'origine

- type
- dati
- riempimento
- checksum

Preamble è di 8 byte e contiene lo schema di bit 10101010.

I due indirizzi sono di 6 byte. In particolare l'indirizzo di destinazione ha il bit più a sinistra che identifica un indirizzo ordinario (0) o un indirizzo di gruppo (1). Con l'indirizzo di gruppo è possibile far ascoltare a molte stazioni un singolo indirizzo e tutte lo ricevono (trasmissione multicast). Se l'indirizzo è composto da soli 1 è riservato alla trasmissione broadcast.

Type di 2 byte indica al ricevitore cosa fare con quel frame.

I dati raggiungono i 1500 byte di massimo; è inoltre necessario che il frame in totale sia lungo almeno 64 byte, per distinguere dai frame danneggiati. Inoltre la lunghezza minima serve per dare il tempo di impedire la trasmissione di un frame quando viene rilevata la possibilità di collisione. Maggiore è la velocità della rete, maggiore deve essere la lunghezza minima del frame.

Il checksum di 4 byte e contiene il checksum CRC per rilevare (ma non correggere) gli errori.

D.3.4 Algoritmo di backoff esponenziale binario

L'algoritmo di backoff esponenziale binario è utilizzato per gestire l'attesa casuale dopo una collisione. È stato scelto perché si adatta in base al numero di stazioni che tentano di trasmettere. L'algoritmo assicura un basso ritardo quando si hanno poche collisioni e una gestione accettabile quando avvengono molte collisioni.

L'algoritmo procede in questo modo: dopo una collisione il tempo viene diviso in intervalli lunghi quanto il tempo di propagazione di andata e ritorno nel caso peggiore ($2t$); ogni stazione aspetta 0 o 1 intervalli temporali prima di riprovare; se due stazioni collidono perché usano lo stesso intervallo, aumenta la scelta degli intervalli casuali (0, 1, 2, 3); ad ogni passo si continua ad aumentare il numero di intervalli d'attesa, che andrà da 0 a $2^i - 1$, dove i indica il numero di collisioni. L'algoritmo ha come tetto massimo 10 collisioni, per un totale di 1023 intervalli. Se ci sono ancora collisioni, a 16 viene lanciato un errore.

D.3.5 Prestazioni di Ethernet

[...]

D.3.6 Ethernet commutata

Al crescere del numero di stazioni, il traffico aumenta e l'aumento della velocità non basta a risolvere il problema. La soluzione è lo switch (commutatore), che ha da 4 a 32 schede di linea, le quali hanno da 1 a 8 connettori, di solito collegati a doppietti 10base-T verso i computer.

Una stazione che vuole trasmettere un frame Ethernet, prima invia un frame standard allo switch, il quale controlla se la destinazione è collegata alla stessa scheda di linea. Se è nella stessa scheda, passa il frame direttamente, altrimenti viene passato alla scheda corretta.

Problema: se due macchine trasmettono sulla stessa scheda?

Ci sono due possibilità. Se la scheda è costruita con le porte che formano una LAN locale, le collisioni vengono rilevate e gestite come in una rete CSMA/CD. In questo modo è possibile una sola trasmissione per scheda, ma più trasmissioni in parallelo su schede diverse. Ogni scheda costituisce il proprio dominio di collisione.

La seconda possibilità prevede un buffer per ogni porta che memorizza i frame in arrivo. Quando ottiene tutto il pacchetto può controllare se il destinatario è nella stessa scheda o se serve spostarlo nella scheda appropriata. Ogni porta è un dominio di collisione separato, quindi non ci sono collisioni.

D.3.7 Fast Ethernet

Nonostante l'aumentare della velocità, l'utente non è mai soddisfatta. Vengono allora proposte due LAN ottiche su topologie ad anello: FDDI e Fibre Channel. Non ebbero molto successo, ma aprirono la strada ad una maggiore velocità. Lo standard infatti decise di mantenere il 802.3 ma con velocità superiore, in modo da mantenere la compatibilità con le LAN esistenti. Venne così creato Fast Ethernet (o anche il poco usato 802.3u). Di fatto la differenza sta nel tempo di bit ridotto da 100 a 10 nanosecondi. Per questa versione era tollerata solo l'architettura 10base-T. Con quali cavi?

Il doppietto cat-3 era una prima scelta data la sua diffusione, tuttavia non riusciva a trasportare 200 Megabaud (ovvero 100 Mbps con codifica Manchester) per 100 metri, come richiesto dal 10Base-T. Venne quindi permesso il cat-3, ma consigliato il cat-5 e la fibra ottica. Abbiamo quindi, rispettivamente, 100Base-T4, 100Base-TX, 100Base-FX, con le ultime due full duplex a 100Mbps.

Lo schema Cat 3 necessita di 4 doppini: uno in ricezione, uno in trasmissione e gli altri due si adeguano alla direzione di trasmissione. I segnali trasmessi sono ternari, cioè possono contenere 0,1 o 2. In questo modo si riesce a raggiungere la velocità obiettivo di 100 Mbps. Questo schema è chiamato 8B/6T.

Il modello basato sul Cat 5 è più semplice ed utilizza solo due doppini, uno in ricezione e uno in trasmissione. In questo caso viene usato uno schema chiamato 4B/5B. Questo sistema è full duplex, ovvero le stazioni possono trasmettere e ricevere contemporaneamente a 100 Mbps.

Il modello che utilizza la fibra ottica usa due cavi multimodali, uno per direzione. Quindi il sistema è full duplex con 100 Mbps in ogni direzione e può raggiungere 2 km tra stazione e hub. Per i modelli 100Base-T è possibile utilizzare sia switch che hub; invece il modello a fibra ottica consente solo lo switch dove ogni cavo collegato crea un dominio di collisione verso se stesso.

D.3.8 Gigabit Ethernet

Dopo la Fast Ethernet iniziarono a lavorare su una Ethernet ancora più veloce, ovvero la gigabit Ethernet. Anche in questo caso si puntava ad avere una trasmissione più veloce mantenendo la compatibilità con le versioni precedenti. Le configurazioni gigabit Ethernet sono tutte punto a punto, di conseguenza ogni stazione è collegata ad un solo hub e switch. Sono supportate sia il full duplex che l'half duplex. Quella normale è la full duplex, utilizzata quando c'è uno switch centrale collegato al computer alle stazioni del perimetro. Tutte le linee hanno buffer e non è possibile avere quelle collisioni, quindi non è necessario controllare se il canale è già utilizzato e di conseguenza non si utilizza il protocollo CSMA/CD. Si utilizza la half duplex quando i computer sono collegati ad un hub; in questo caso le collisioni sono ancora possibili quindi si utilizza il protocollo CSMA/CD. Data la velocità di trasmissione, un frame è trasmesso così velocemente da limitare la distanza a 25 metri. Questo è inaccettabile, di conseguenza sono state aggiunte due funzionalità dallo standard. La prima è chiamata **Carrier extension**, aggiunge i dati di riempimento dopo il frame normale e viene rimosso quando viene ricevuto. Essendo una modifica hardware non sono richiesti cambiamenti al software. La seconda funzionalità è detta **Frame bursting** e permette di inviare una sequenza concatenata di più frame in una sola trasmissione; se non viene raggiunta la dimensione di 512 Byte, viene compensata dal metodo sopracitato; in questo modo si arriva ad un raggio di 200 metri un valore già più accettabile. Esistono 4 tipi di configurazione

che utilizzano cavi diversi: 1000Base-SX/LX/CX/T, le prime due con fibra, le ultime due con diversi tipi di doppini.

D.3.9 Retrospectiva su Ethernet

Punti vincenti: semplicità e flessibilità.

Semplice si traduce in affidabile, economico e facile da mantenere. Flessibile in quanto funziona con TCP/IP ed è in grado di evolversi dove serve.

D.4 LAN Wireless

D.4.1 La pila di protocolli 802.11

I protocolli utilizzati dalle varianti 802 sono tutti simili. Lo strato fisico è simile a quello OSI, lo strato datalink è suddiviso in due o più sottostrati. In 802.11 il sottostrato MAC gestisce l'allocazione del canale, il sottostrato LLC nasconde le differenze tra le varianti di 802 in modo da renderle indistinguibili allo strato network.

D.4.2 Lo strato fisico di 802.11

[...]

D.4.3 Il protocollo del sottostrato MAC di 802.11

Il sottostrato MAC di 802.11 si differenzia leggermente da quello di 802.3, in quanto l'ambiente wireless complica le cose. Per esempio ci sono i problemi della stazione esposta e della stazione nascosta (§D.2.5). Inoltre le trasmissioni sono quasi tutte half duplex. Per questi motivi non viene utilizzato CSMA/CD, bensì una variante detta CSMA/CA, ovvero Collision Avoidance.

In particolare, 802.11 supporta due modalità operative: DCF (Distributed Coordination Function), che non utilizza nessun controllo centrale, e PCF, dove invece la stazione base controlla l'intera cella.

Quando viene usato DCF, si usa CSMA/CA che controlla sia il canale fisico, sia quello virtuale.

Questo protocollo rileva la portante prima della trasmissione e usa il backoff esponenziale dopo le collisioni, a differenza di CSMA/CD, il backoff di partenza è casuale e non attende una collisione per essere settato.

[...]

D.4.4 Servizi

Lo standard definisce 9 servizi che ogni LAN wireless deve fornire, 5 di distribuzione e 4 di stazione. Quelli di distribuzione riguardano l'appartenenza alla cella e l'interazione con le altre celle, mentre quelli di stazione si occupano delle attività dentro la cella. I servizi sono:

- Associazione - utilizzato dalle stazioni mobili per collegarsi alle stazioni base
- Separazione - si interrompe la relazione tra le due stazioni
- Riassociazione - la stazione mobile cambia la stazione base preferita (es: per cambiare cella)
- Distribuzione - indica come saranno instradati i frame verso la destinazione
- Integrazione - traduce dal formato 802.11 al formato richiesto dalla destinazione
- Autenticazione - solo le stazioni autenticate possono trasmettere i dati
- Invalidamento - invalida una stazione precedentemente autenticata che vuole lasciare la stazione
- Riservatezza - le informazioni devono essere cifrate
- Trasferimento dati - per il trasferimento

D.5 Commutazione nello strato data link

È possibile connettere più LAN tramite dispositivi detti bridge, che operano nello strato data link. I bridge esaminano gli indirizzi dello strato datalink per l'instradamento senza esaminare il carico utile, permettendo di trasportare diversi tipi di pacchetto. I router all'opposto instradano in base agli indirizzi del pacchetto.

Alcuni motivi per creare LAN differenti che vengono poi connesse tra loro sono:

- rendere indipendenti le LAN dei dipartimenti diversi
- collegare aziende su edifici diversi, lontani tra loro

- suddividere una LAN logica in più LAN fisiche per gestire meglio il carico
- per collegare più LAN suddivise per i limiti di distanza (es: 2,5 Km in caso di Ethernet)
- per garantire una maggiore affidabilità in caso di nodi difettosi
- per ottenere una maggiore sicurezza dell'azienda

D.5.1 Bridge tra due 802

Come funziona un bridge? Un pacchetto dallo strato di rete viene passato allo strato LLC che aggiunge l'intestazione relativa, poi passa al sottostrato MAC dove viene aggiunta la sua intestazione, per esempio 802.11; infine giunge allo strato fisico fino ad arrivare alla stazione base, dove viene rilevata la richiesta di passaggio tra due LAN di tipi diversi. Il passaggio avviene tramite il bridge, che "traduce" il frame risalendo gli strati del bridge, fino a riscendere per passare allo strato fisico della seconda LAN. Purtroppo non è così banale, in quanto ci sono diversi problemi. Ad esempio i formati dei frame differiscono, richiedendo una conversione particolare; le due LAN possono trasmettere a velocità diverse; inoltre c'è la diversa lunghezza dei frame in base al tipo di 802; un'altra questione è la sicurezza, in quanto alcune versioni supportano la crittografia, mentre altri no; infine la qualità del servizio, che viene garantito in modi diversi.

D.5.2 Internetworking locale

Come già accennato, i bridge possono essere usati per connettere LAN anche dello stesso tipo. In questo caso, i bridge accettano tutti i frame in arrivo, ma scartano quelli che appartengono già alla stessa LAN, ovvero quei frame che non hanno bisogno di attraversare il bridge per cambiare LAN. Nel decidere dove e se inoltrarli, il bridge utilizza l'indirizzo di destinazione e lo confronta con una tabella delle destinazioni. Appena creata la connessione le tabelle sono vuote e il bridge manda il frame a tutte le LAN tranne a quella di input; con il tempo riesce a riempire la tabella con gli indirizzi corretti e potrà inviare solo alla LAN che contiene la stazione richiesta. Questo è detto algoritmo di apprendimento all'indietro. In particolare la costruzione avviene salvando gli indirizzi della sorgente, memorizzando in che LAN si trova.

D.5.3 Bridge spanning tree

Per aumentare l'affidabilità è possibile collegare più LAN con bridge paralleli, tuttavia questo crea anelli nella topologia. Per evitare il problema, viene costruito uno spanning tree, un grafico ad albero che evita i percorsi ad anello.

D.5.4 Bridge remoti

Delle LAN distanti possono essere connesse tra loro tramite bridge remoti, ovvero una coppia di bridge che sono in comunicazione tra loro tramite una linea punto a punto.

D.5.5 Ripetitori, hub, bridge, switch, router, gateway

Nonostante la funzione simile, vale la pena confrontare ripetitori, hub, bridge, switch, router, gateway. Innanzitutto, operano su strati diversi: ripetitori e hub nel fisico, bridge e switch nel data link, router nel network, gateway nel trasporto e applicazioni (due tipi diversi).

E Capitolo 5 - Strato network

E.1 Architettura dello strato network

E.2 Algoritmi di routing

E.2.1 Principio di ottimalità

E.2.2 Routing basato sul percorso più breve

E.2.3 Flooding

E.2.4 Routing basato sul vettore delle distanze

E.2.5 Routing basato sullo stato dei collegamenti

E.2.6 Routing gerarchico

E.2.7 Routing broadcast

E.3 Algoritmi per il controllo della congestione

E.4 Qualità del servizio

E.4.1 Requisiti

E.4.2 Tecniche per una buona qualità

Sovradimensionamento

Utilizzo dei buffer

Traffic shaping

Leaky bucket

Token bucket

- E.5 Collegamento tra reti
 - E.5.1 Differenze tra le reti
 - E.5.2 Connessione tra le reti
 - E.5.3 Circuiti virtuali concatenati
 - E.5.4 Collegamento tra reti senza connessione
 - E.5.5 Routing in una internetwork
- E.6 Lo strato network in internet
 - E.6.1 Il protocollo IP
 - E.6.2 Gli indirizzi IP
 - E.6.3 Protocolli di controllo internet
 - E.6.4 OSPF
 - E.6.5 BGP
 - E.6.6 Internet multicasting
 - E.6.7 IPv6

F Capitolo 6 - Strato trasporto

Il livello di trasporto si basa sul livello di rete per fornire il trasporto dei dati tra due macchine secondo il livello di affidabilità desiderato e indipendentemente dalle reti fisiche. L'obiettivo finale è fornire un servizio efficiente, efficace ed affidabile ai suoi utenti. Per fare ciò usa i servizi forniti dallo strato di rete. L'hardware/software usato per svolgere il lavoro è detto **entità di trasporto**.

Per molti aspetti lo strato trasporto può sembrare simile a quello network, ma il fatto è che questo strato è essenziale per garantire affidabilità che lo strato network, basato sulla rete, non può dare.

Grazie alle primitive fornite dallo strato, i programmatori possono scrivere codice senza preoccuparsi della sottorete.

In seguito verrà usato TPDU (transport protocol data unit) per indicare i messaggi inviati da un'entità di trasporto ad un'altra. Quindi, riprendendo gli altri "contenitori" degli altri strati, avremo TPDU dentro un pacchetto, il quale è dentro un frame (trasporto -> network -> datalink). Ogni carico utile di ogni livello ha la propria intestazione.

F.1 Richiesta connessione e protocollo Three-way Handshake

Il Three-way handshake è un protocollo che entra in gioco quando si deve stabilire una connessione. Infatti stabilire una connessione è un'operazione tutt'altro che facile. Al normale "percorso" CONNECTION REQUEST - CONNECTION ACCEPTED, la rete può perdere, ritardare, corrompere o duplicare i pacchetti, creando diversi problemi. In particolare, l'esistenza dei duplicati ritardati è il nodo centrale del problema e può essere affrontato in diversi modi. Una possibilità è l'utilizzo di indirizzi di trasporto monouso oppure si può assegnare ad ogni connessione un identificatore inserito in ogni TDPU. Entrambe le possibilità hanno diversi problemi.

La soluzione è cercare di distruggere i pacchetti obsoleti rimasti in circolo, impostando una durata massima di vita del pacchetto. Il valore massimo di durata può essere prefissato utilizzando una o più tecniche tra le seguenti:

- progettazione di sottoreti limitate che impediscono ai pacchetti di essere ripetuti ciclicamente
- inserimento di un contatore di salti in ogni pacchetto che viene decrementato ad ogni salto e se raggiunge lo zero viene scartato

- applicazione di un contrassegno temporale in ogni pacchetto; verrà scartato se diventa troppo vecchio secondo un tempo stabilito

Oltre al pacchetto, anche i suoi acknowledgment devono essere distrutti. Consideriamo quindi un valore T che indica il tempo dopo il quale si può essere certi che tutte le tracce del pacchetto sono scomparse (sia pacchetto che acknowledgment). La sorgente etichetta i segmenti con numeri di sequenza che non verranno riutilizzati per T secondi. In questo modo ci sarà un unico pacchetto con quel numero di sequenza in sospeso.

Nel caso di malfunzionamento, è possibile far rimanere le entità inattive per T secondi in modo da far scadere gli eventuali segmenti vecchi, così da essere sicuri di non usare numeri di sequenza già utilizzati. Tuttavia su reti complesse non conveniva, quindi fu proposto un orologio per ogni host implementato come contatore binario che abbia tanti bit quanti quelli del numero di sequenza. Quando viene instaurata la connessione, i k bit di ordine più basso dell'orologio sono usati come primo numero di sequenza, quindi ogni connessione inizia con numeri diversi. Una volta stabilito il primo numero di sequenza, si può utilizzare un qualsiasi protocollo sliding window.

Il metodo dell'orologio risolve il problema dei segmenti duplicati, ma non c'è modo di ricordare i numeri tra una connessione e l'altra, quindi non sappiamo se un segmento di richiesta di connessione sia duplicato o meno. La soluzione è il three-way handshake che richiede la verifica reciproca da parte dei peer utilizzando tre messaggi. Il primo host manda la richiesta di connessione con un numero di sequenza x ; l'host 2 risponde con un ack che conferma x e contiene il suo numero di sequenza iniziale. L'host 1 allora invia il primo segmento dati e conferma a sua volta la scelta del numero di sequenza iniziale dell'host 2. Nel caso di richiesta di connessione duplicata, l'host 2 reagisce normalmente, ma al terzo messaggio l'host 1 rifiuta il tentativo di connessione. Se invece si hanno sia la richiesta che l'ack ritardati, l'host 2 reagisce normalmente restituendo il numero y , successivamente l'host riceve il secondo segmento ritardato che ha però un ack su un numero diverso da y , per cui capisce che è un duplicato.

F.2 Rilascio della connessione

Il rilascio della connessione è più semplice e può essere simmetrico o asimmetrico. In quello asimmetrico, una delle due parti interrompe la connessione; è improvviso e può far perdere di dati. Il rilascio simmetrico tratta la connessione come se fosse composta da due connessioni separate unidirezionali,

quindi le rilascia separatamente. In questo caso, anche se una delle due parti ha inviato il pacchetto DISCONNECT, può continuare a ricevere dati.

Anche per il rilascio conviene usare il three-way handshake, anche se in questo caso non è infallibile. Ogni messaggio passa la richiesta di disconnessione e il ricevente deve confermare con una richiesta di rilascio; infine il primo risponde con l'ack. in questo caso, ogni messaggio ha un timer per triggerare la rispedizione nel caso qualcosa vada storto.

F.3 Introduzione all'UDP

UDP (User Datagram Protocol) è un protocollo di trasporto senza connessione, permette cioè di inviare datagrammi IP senza dover stabilire una connessione. UDP trasmette segmenti con un'intestazione di 8 byte seguita dal carico utile. L'intestazione contiene le porte dell'origine e della destinazione. Il campo UDP length include l'intestazione e i dati, mentre UDP checksum contiene il checksum.

UDP non si occupa del controllo del flusso, degli errori o della ritrasmissione.

Questo protocollo è particolarmente utile per il multimediale (streaming) e per le situazioni client/server, dove è richiesta una risposta breve ad una breve richiesta al server. Se non viene ricevuta la risposta, allora va in timeout e riprova. Questo tipo di utilizzo viene effettuato dal DNS.

F.4 TCP

F.4.1 Introduzione

TCP (Transport Control Protocol) è un protocollo di trasporto creato per fornire affidabilità per un internetwork inaffidabile. Un internetwork ha diversi parametri che possono variare e TCP cerca di adattarsi dinamicamente. Un'entità di trasporto TCp riceve i dati dell'utente, li suddivide in pezzi di dimensione massima uguale a 64KB e invia ogni pezzo in un datagramma IP autonomo. Nel ricevente i datagrammi vengono usati per ricostruire il flusso di byte originali. TCP ha il compito di segnalare gli errori, richiedere la ritrasmissione e riordinare i datagrammi se non sono nell'ordine corretto.

F.4.2 Modello di servizio di TCP

Il servizio TCP è ottenuto creando punti finali da parte del mittente e ricevente, ovvero i socket. Ogni socket ha un indirizzo composto dall'indirizzo

IP dell'host e da un numero di 16 bit locale all'host, che indica la porta. Per avere un servizio è necessario stabilire una connessione tra i due socket.

Un socket supporta più connessioni alla volta e una connessione è identificata dalla coppia dei due socket utilizzati.

I numeri di porta inferiori a 1024 sono le well-known ports, porte speciali dedicate ai servizi standard.

Tutte le connessioni TCP sono full-duplex punto a punto. Non supporta né il broadcasting, né il multicasting.

Una connessione TCP è un flusso di byte e non di messaggi, quindi un messaggio può essere trasmesso spezzato in blocchi di byte più piccoli o con altri messaggi.

TCP ha la capacità di decidere se inviare subito i dati ricevuti da un'applicazione o se salvarli in un buffer per raggrupparli e inviarli insieme ad altri. L'applicazione può avere però richieste particolare e chiedere che sia spedito subito tramite il flag PUSH.

F.4.3 Protocollo TCP

Una funzionalità importante del protocollo è il fatto che ogni byte ha un proprio numero di sequenza a 32bit.

I dati vengono scambiati sotto forma di segmenti. Un segmento consiste di un'intestazione di 20 byte seguita da 0 (ack) o più byte di dati. Sta a TCP decidere la grandezza massima dei segmenti e può decidere se dividere o combinare i messaggi. Il limite superiore però è di 65535 byte, che deve starci nel carico utile di IP. Ogni rete ha un MTU (Maximum Transfer Unit) e il segmento deve stare sotto la soglia. Di solito è di 1500 byte.

Le entità TCP usano il protocollo sliding window.

F.4.4 Intestazione TCP

L'intestazione di un segmento è di 20 byte. Due campi sono dedicati alla porta d'origine e a quella di destinazione. I campi *numero di sequenza* e *numero di acknowledgement* svolgono le solite funzioni. Il campo *lunghezza dell'header TCP* indica quante parole di 32 bit sono contenute nell'intestazione; è necessario perché il campo options ha una lunghezza variabile. Seguono 6 bit inutilizzati e 6 bit per 6 flag, come URG (puntatore urgente), ACK (acknowledgement è valido), PSH (push), RST (reimposta la connessione), SYN (stabilisce una connessione), FIN (rilascia la connessione). Il campo successivo *window size* indica la dimensione della finestra per lo sliding window e in particolare quanti byte possono essere inviati a partire

da quello che ha ricevuto l'acknowledgement. Seguono il campo checksum e l'urgent pointer. Una volta finita l'intestazione, sono presenti il campo *options* per opzioni aggiuntive e i dati effettivi.

F.4.5 Connessione TCP

Le connessioni vengono stabilite secondo il three-way handshake. Un host richiede la connessione inviando un segmento con bit SYN a 1 e ACK a 0 e attende la risposta. L'host ricevente controlla se alla porta indicata nel frame è in ascolto; in caso negativo risponde rifiutando la connessione, altrimenti risponde con un segmento di acknowledge per dare il via libera al primo host, che manda il segmento di dati.

Se due host tentano una connessione sugli stessi socket, solo una delle due andrà a buon fine in quanto i socket sono identificativi della connessione.

F.4.6 Rilascio connessione TCP

Il rilascio avviene in maniera simmetrica, dove ogni parte può inviare un segmento con il bit FIN impostato per dire che ha finito di trasmettere e può essere chiusa la connessione. Nel senso opposto può continuare la trasmissione finché non termina e viene rilasciata del tutto la connessione.

Per rilasciare la connessione servirebbero 4 segmenti (2 FIN e 2 ACK), ma è possibile raggruppare il primo ACK con il secondo FIN in modo da averne solo tre.

Se ad un FIN non arriva la risposta, un timer rilascia la connessione nella direzione del FIN inviato.

G Capitolo 7 - Strato applicazione

Lo strato applicazione e dove si trovano effettivamente le applicazioni. Ci sono comunque dei protocolli di supporto per permettere alle applicazioni di funzionare. Uno di questi è il DNS.

G.1 DNS

Il DNS (Domain name system) è un protocollo per la gestione dei nomi. I siti web e le altre risorse possono essere accedute direttamente tramite l'indirizzo IP, ma non risulta molto user-friendly in quanto per l'utente è difficile memorizzare l'indirizzo della risorsa richiesta. Il DNS serve per tradurre gli indirizzi IP in nomi comprensibili e viceversa. Infatti, se per l'utente il nome è più comprensibile, il network comprende solo l'indirizzo IP, per cui è richiesta la traduzione inversa da nome a indirizzo. Un altro problema che ha portato alla creazione del DNS era la necessità di un sistema centralizzato, che permettesse di gestire i nomi senza avere duplicati.

Il DNS quindi è un sistema centralizzato con un database distribuito dove viene implementato lo schema gerarchico dei nomi basato su dominio. Viene utilizzato principalmente per mappare indirizzi IP e nomi del relativo host. Per mappare un nome con il suo indirizzo IP, viene chiamata una procedura detta **resolver** con il nome come parametro. Questa invia la query al server DNS e viene ritornato l'indirizzo IP; sia la query, sia la risposta sono spediti come pacchetti UDP.

La gerarchia dei nomi è divisa in diversi livelli. Internet è diviso in più di 250 domini di primo livello contenenti i vari host. Ogni dominio è partizionato in sottodomini, anch'essi partizionati ecc. Il primo livello è distinto tra generici (com, org, edu, ecc) e nazioni (it, uk, jp, ecc). Il secondo livello spesso indica l'azienda. Il nome di un dominio può essere assoluto o relativo. Se termina con il punto è assoluto; se è relativo, il reale significato dipende dal contesto. I nomi sono case-insensitive e di lunghezza massima di 255 caratteri.

Ogni dominio può essere associato ad un insieme di record delle risorse. Quando il DNS riceve un nome, restituisce i record associati, tra cui quello che indica l'indirizzo IP. Un record è identificato dalla quintupla:

Domain_name Time_to_live Class Type Value

Il Type A è il più importante in quanto è il record che contiene l'indirizzo IP. Questo record può non essere univoco.

Il server del DNS non è unico, altrimenti verrebbe sovraccaricato. Quindi i nomi sono divisi in zone, che risiedono su server diversi.

H Capitolo 8 - Sicurezza

H.1 Crittografia

Quando si parla di crittografia vanno distinti due termini: cifrario, ovvero la trasformazione carattere per carattere del messaggio, e codice, che rimpiazza ogni parola con un'altra parola (non più usati).

H.1.1 Introduzione alla crittografia

Un messaggio da cifrare è detto testo in chiaro e sono trasformati in testo cifrato da un funzione secondo una chiave di cifratura. Decifrare è l'operazione legittima di lettura dei dati, traducendoli nel messaggio originale, mentre decriptare è l'attività di decifrazione da parte dell'intruso.

Secondo il principio di Kerckhoff, tutti gli algoritmi di cifratura devono essere pubblici e solo le chiavi sono segrete. Infatti di solito cercare di tenere nascosto l'algoritmo non è produttivo, mentre averlo pubblico può portare a collaborazioni e miglioramenti.

Dato che la segretezza sta nella chiave, la sua lunghezza è la parte fondamentale. Più è lunga, più è difficile da decriptare.

H.1.2 Cifrari a sostituzione

Il cifrario a sostituzione sostituisce una o più lettere con una o più lettere. Uno dei cifrari più antichi è quello di Cesare, che effettuava uno slittamento dell'alfabeto di 3 lettere: A diventa D, B diventa E, ecc. In generale, si può usare questo metodo usando una chiave k per spostare di k lettere l'alfabeto. Questa cifratura è detta sostituzione monoalfabetica.

Il passaggio successivo è stato far cambiare la corrispondenza lettera in chiaro e lettera cifrata in maniera più casuale. La chiave è la stringa che corrisponde all'intero alfabeto.

Anche se questo sistema sembra sicuro per il gran numero di combinazioni, più testo cifrato si ha a disposizione e più facile è decriptare il testo grazie alle proprietà statistiche dei linguaggi. Basterà usare diagrammi o trigrammi più comuni (coppie o triple di lettere), o cercare di individuare una parola che è probabile che sia presente.

H.1.3 Blocchi monouso

[...]

H.1.4 Due principi crittografici fondamentali

I due principi crittografici fondamentali sono la ridondanza e l'attualità. Il primo principio afferma che tutti i messaggi cifrati devono contenere una qualche forma di ridondanza, cioè un'informazione non necessaria al messaggio. Questo per evitare che gli intrusi possano creare dati casuali con il rischio che vengano interpretati come validi. La ridondanza però renderebbe più facile decriptare: quindi difende contro gli intrusi attivi, ma meno da quelli passivi.

Il secondo principio afferma che è necessario avere la possibilità di verificare che ogni messaggio ricevuto sia attuale, recente, in modo da poter prevenire attacchi di tipo ripetizione, dove un intruso manda messaggi vecchi spacciandoli per nuovi.

H.2 Algoritmi a chiave simmetrica

Questi algoritmi usano la stessa chiave per cifrare e decifrare. Gli algoritmi possono essere implementati in software o hardware (es: P-box, scatola di permutazione con input a 8 bit).

H.2.1 DES

DES (Data Encryption Standard) cifra il testo in chiaro in blocchi di 64 bit che generano 64 bit di testo cifrato. Utilizza una chiave a 56 bit e ha 19 stadi, dove nel primo viene fatta la trasposizione dei 64 bit di testo in chiaro, indipendentemente dalla chiave, mentre nell'ultimo stadio avviene l'inverso del primo. Quelli intermedi hanno la stessa funzione, ma parametrizzati da diverse funzioni della chiave. Ogni stadio intermedio prende due ingressi a 32 bit e produce due uscite a 32 bit: quello di sinistra è la copia dell'originale di destra, mentre quello di destra è lo XOR tra i bit di sinistra, quelli di destra e della chiave di stadio.

Quando IBM si rese finalmente conto che la chiave di cifratura era troppo corta, decise di usare una cifratura tripla. Vengono usate due chiavi e tre stadi: nel primo il testo in chiaro viene cifrato con DES usando la chiave K_1 , nel secondo viene usato DES in modalità di decifrazione usando K_2 , infine un'altra cifratura con chiave K_1 . Questa alternativa migliorata è detta **triplo DES**.

Domanda 1: perchè solo 2 chiavi e non 3? Perchè i 112 bit erano ritenuti sufficienti, mentre 168 avrebbe richiesto molto lavoro senza vantaggi effettivi. Domanda 2: perchè cifra-decripta-cifra e non cifra-cifra-cifra? Il motivo

è per mantenere la compatibilità con i sistemi che usavano un solo DES, ponendo $K_1 = K_2$.

H.2.2 AES

AES (Advanced Encryption Standard) è lo standard successivo a DES. Questo algoritmo è un cifrario simmetrico a blocchi, con struttura interamente pubblica (DES non lo era), supporta chiavi fino a 256 bit, è implementabile sia via software, sia hardware e doveva essere pubblicato senza vincoli.

Questo algoritmo deriva da un concorso pubblico; ci furono diverse proposte e alla fine quella definita vincitrice fu quella di Rijndael.

AES definisce che la dimensione del blocco doveva essere di 128 bit, mentre quella della chiave poteva essere di 128 o 256 bit. Ci sono quindi le versioni 128/128 e 128/256, ma già la prima è sufficientemente sicura.

Come DES, AES usa sostituzioni e permutazioni in diversi round (10 a 128 bit) e a differenza di DES le operazioni coinvolgono byte interi.

AES opera utilizzando matrici di 4x4 byte chiamate stati (states). Quando l'algoritmo ha blocchi di 128 bit in input, la matrice State ha 4 righe e 4 colonne; se il numero di blocchi in input diventa di 32 bit più lungo, viene aggiunta una colonna allo State, e così via fino a 256 bit. In pratica, si divide il numero di bit del blocco in input per 32 e il quoziente specifica il numero di colonne.

C'è un passaggio iniziale:

AddRoundKey – Ogni byte della tabella viene combinato con la chiave di sessione, la chiave di sessione viene calcolata dal gestore delle chiavi. Successivamente per cifrare sono previsti diversi round o cicli di processing: ogni round (fase) dell'AES (eccetto l'ultimo) consiste dei seguenti quattro passaggi:

- SubBytes – Sostituzione non lineare di tutti i byte che vengono rimpiazzati secondo una specifica tabella.
- ShiftRows – Spostamento dei byte di un certo numero di posizioni dipendente dalla riga di appartenenza.
- MixColumns – Combinazione dei byte con un'operazione lineare, i byte vengono trattati una colonna per volta.
- AddRoundKey – Ogni byte della tabella viene combinato con la chiave di sessione, la chiave di sessione viene calcolata dal gestore delle chiavi.

Il numero di round o cicli di processamento/elaborazione crittografica dei quattro passaggi precedenti è 10 con l'ultimo round che salta il passaggio MixColumns. A seguito la descrizione di ogni singolo passaggio.

La fase di decifratura non è identica a quella di cifratura dal momento che gli step sono eseguiti in ordine inverso. Tuttavia, si può definire un cifrario inverso equivalente ai passi dell'algoritmo usato per la cifratura, usando la funzione inversa a ogni step e un different key schedule. Funziona siccome il risultato non cambia quando si scambiano la fase di SubBytes con quella di ShiftRows, e quella di MixColumns con una fase aggiuntiva di AddRoundKey.

L'algoritmo è molto sicuro e veloce; nell'implementazione hardware riesce ad essere anche più veloce.

H.2.3 Modalità di cifratura

I cifrari a blocchi sono "ripetitivi", nel senso che dato un testo in chiaro e una chiave, l'output sarà sempre uguale. Questo può essere un problema per la sicurezza.

Modalità ECB Dato un testo in chiaro, con DES viene suddiviso in blocchi da 8 byte fino a raggiungere l'ultimo, che eventualmente viene riempito per raggiungere la grandezza richiesta. Questa tecnica è nota come ECB (Electronic Code Book). Anche se i blocchi sono cifrati, è possibile manipolare il "libro" dei blocchi sapendo il contesto, senza il bisogno di decriptarli.

Modalità stream cipher La modalità stream cipher cifra un vettore di inizializzazione per ottenere un blocco in uscita; questo blocco viene cifrato per ottenere un secondo blocco in uscita, e così via. La sequenza di blocchi è detta keystream e viene utilizzata come un blocco monouso e utilizzata in XOR con il testo in chiaro per ottenere il testo cifrato.

L'uso ripetuto dello stesso keystream espone il testo cifrato ad attacchi di keystream riutilizzato.

H.3 Algoritmi a chiave pubblica

Gli algoritmi a chiave pubblica sono stati proposti per risolvere un problema: le chiavi sono il punto primario, vanno distribuite ma senza lasciare che un intruso possa ottenerle. Questi nuovi algoritmi propongono di usare chiave

di cifratura e decifratura diversi e non deducibili tra loro, e di rendere la chiave di cifratura pubblica insieme all'algoritmo.

H.4 Message digest

H.4.1 MD5

H.4.2 SHA-1

H.5 Sicurezza delle comunicazioni

H.5.1 IPsec

H.5.2 Firewall

H.5.3 Sicurezza wireless

802.11

WAP 2.0

H.6 Replay attack

H.7 Sicurezza del naming

H.7.1 DNS spoofing

H.7.2 DNS sicuro