@ P. Siagian

Komunikasi Data & Jaringan Komputer

Network Communication

Transmisi Data
Pengkodean Data
Teknik Komunikasi Data Digital
Data Link Control
Multiplexing
Switching
Medium Access Sublayer
Multiple Access Control (MAC) Protocols
Network Layer

https://github.com/siagianp

https://www.youtube.com/@AmelOline/video

https://github.com/amelcharolinesgn2/IoT_simulator-mqtt-NodeRed

github.com/amelcharolinesgn2/ANJAR

Scopes

- Transmisi Data
- ***Pengkodean Data***
- Teknik Komunikasi Data Digital
- Data Link Control
- Multiplexing
- Switching
- Medium Access Sublayer
- Multiple Access Control (MAC) Protocols
- Network Layer

TRANSMISI DATA

Outline

- Konsep Komunikasi Data
- Media & Periperal Komunikasi
- Jaringan & Protokol Komunikasi
- Perangkat Jaringan
- Topologi Jaringan Komputer
- Jenis Jaringan

Konsep Komunikasi Data

Konsep Komunikasi Data

Pengertian Komunikasi data

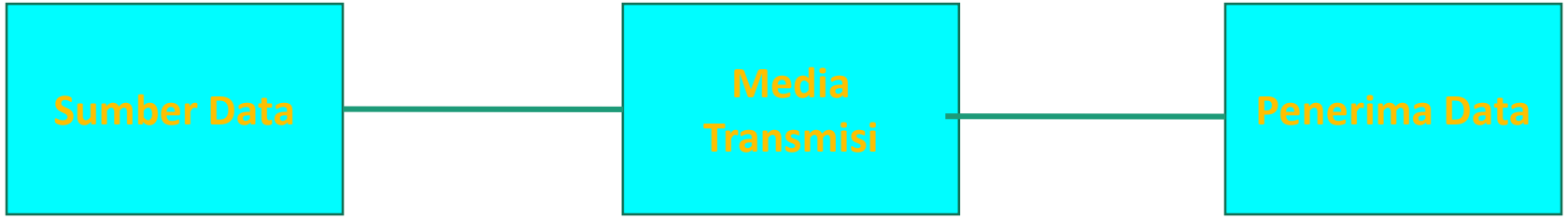
- Pengiriman data menggunakan transmisi elektronik dari terminal/*computer* satu ke terminal lain/*computer* lain

Contoh terminal data (yang umum): printer, monitor PC, keyboard, scanner, dll.

Konsep Komunikasi Data

Elemen Komunikasi data

- Sumber Data
- Media Transmisi
- Penerima Data



Konsep Komunikasi Data

Sumber data

- Elemen yang bertugas mengirimkan informasi/data
  - Contoh: telepon, fax, terminal,dll
- Sumber Data dilengkapi oleh *Transmitter*
  - Transmitter: mengubah/mengkodekan data yg akan dikirim.
- Output Transmitter pada Sumber Data:
  - pulsa listrik, gelombang elektromagnetik, pulsa digital
  - contoh Transmitter: modem

Konsep Komunikasi Data

Media Transmisi

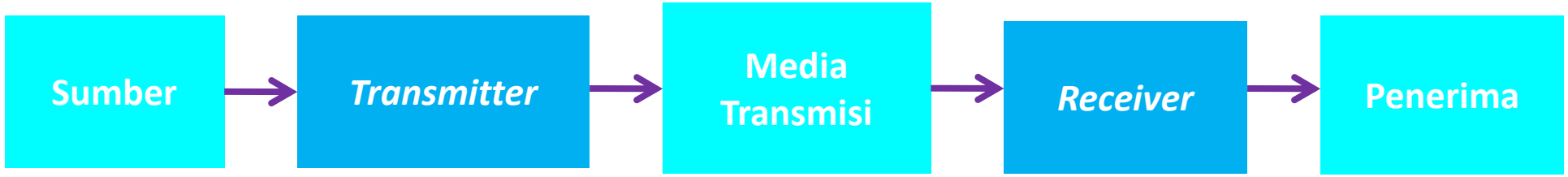
- Media yang digunakan untuk mengirimkan data dari sumber data ke penerima data
- Media Transmisi terdiri dari 2 katagori/jenis:
  - media transmisi fisik
  - media transmisi non fisik.
- Media Transmisi Fisik
  - contoh: kawat tembaga, kabel coaxial, kabel serat optic.
- Media Transmisi Non Fisik
  - contoh: gelombang elektromagnetik

Konsep Komunikasi Data

Penerima Data

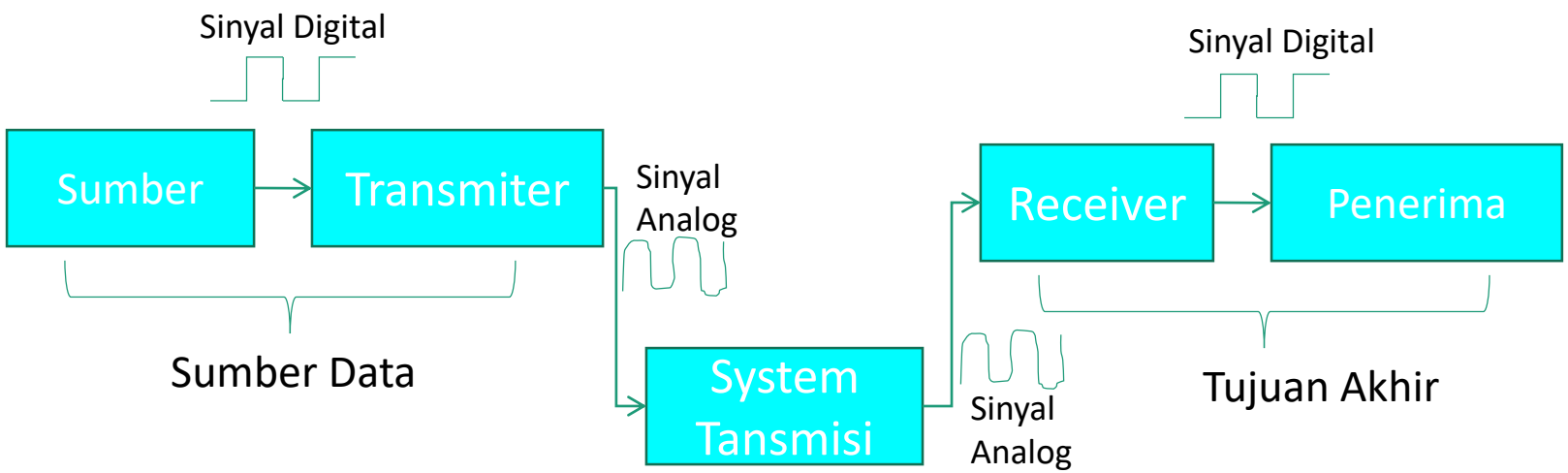
- Elemen yang bertugas menerima informasi/data
- Contoh: telepon, fax, terminal, dll.
- Penerima Data dilengkapi oleh *Receiver*
- Receiver : mengubah pengkodekan oleh transmitter supaya bisa dikenali oleh perangkat destination.

Konsep Komunikasi Data



Penjabaran tiga elemen utama komunikasi data

Konsep Komunikasi Data



Sistem Transmisi; dapat berupa transmisi 1 atau 2 arah (sebagai media komunikasi)

Konsep Komunikasi Data

Perangkat Terminal data (*Data Terminal Equipment)*

- Implementasi Komunikasi Data saat ini:
  - Reservasi Tiket secara online
  - Mesin ATM pada perbankan
  - Bank dengan sistem online
  - Internet & E-mail
  - Teleconference (audio/video)
  - LAN / WAN / MAN
  - GSM / CDMA
  - GPS (Global Positioning System), dll

Media & Periperal Komunikasi

Media & Pheriperal Komunikasi

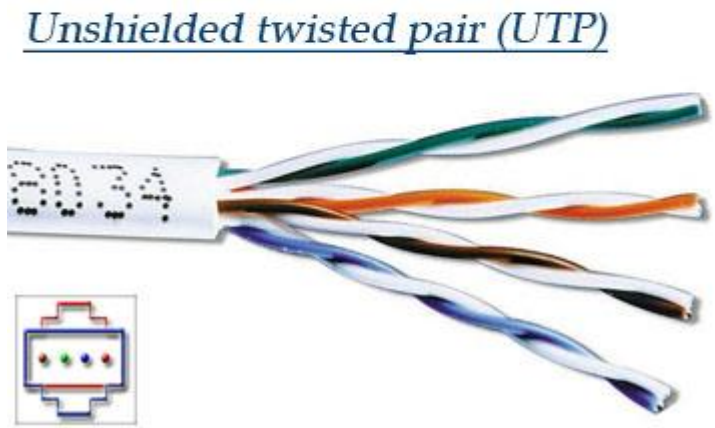
Media Transmisi

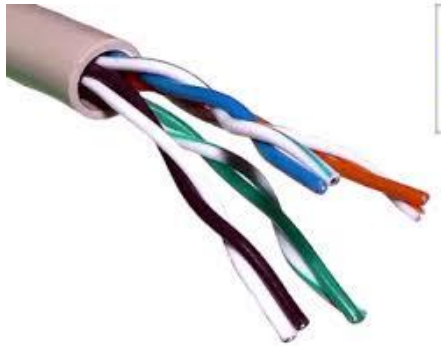
Media untuk menghantarkan data/informasi terbagi menjadi 2 (dua) yaitu

1. **Menggunakan Kabel**
2. **Tanpa Kabel (*Wireless*)**

Media & Pheriperal Komunikasi

- **Media Transmisi-> Kabel-> *Twisted Pair* (Untiran)**
- Kabel ini terbuat dari tembaga dimana beberapa pasang kabel diuntir dan dijadikan satu.
- Ada 2 jenis *twisted pair* yaitu STP & UTP



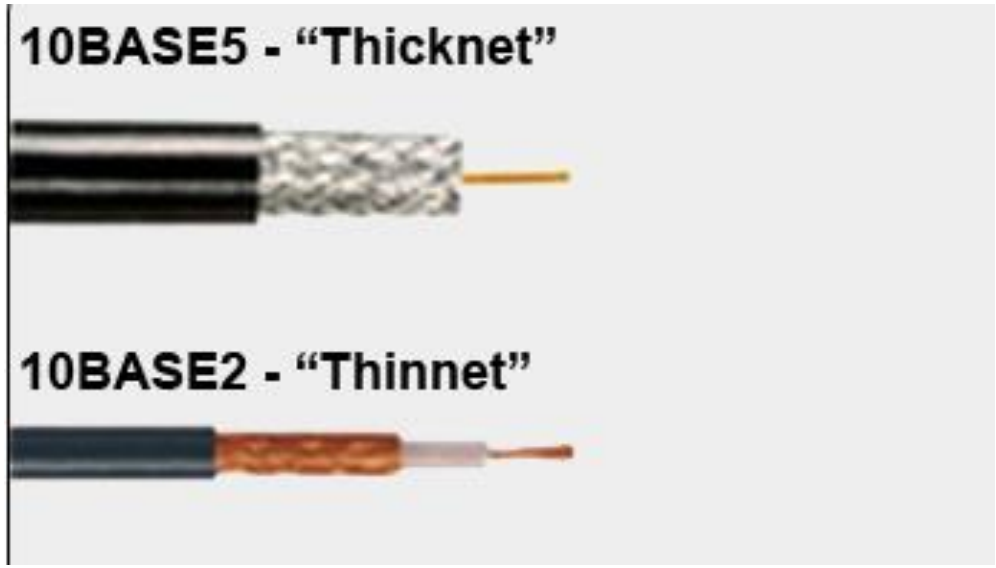


Media & Pheriperal Komunikasi

- **Media Transmisi-> Kabel-> *Coaxial***
- Pada jenis ini, kabel utama yang terbuat dari tembaga akan dikelilingi oleh anyaman halus kabel tembaga lainnya dan diantaranya terdapat isolasi

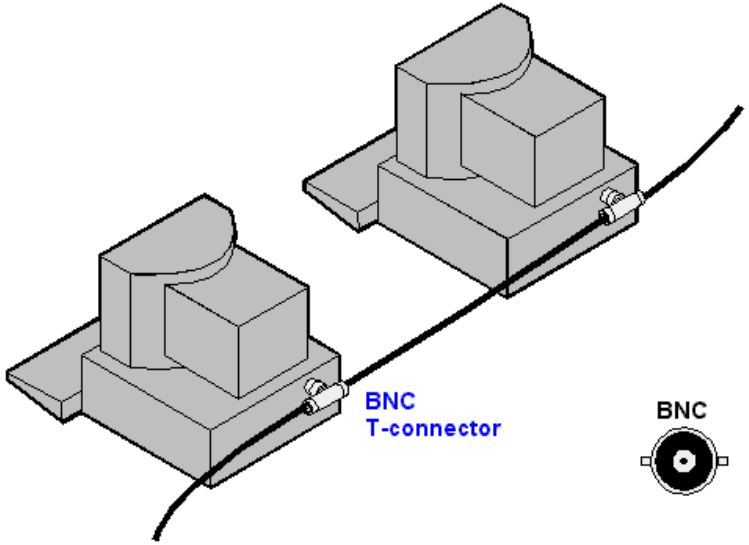
Media & Pheriperal Komunikasi

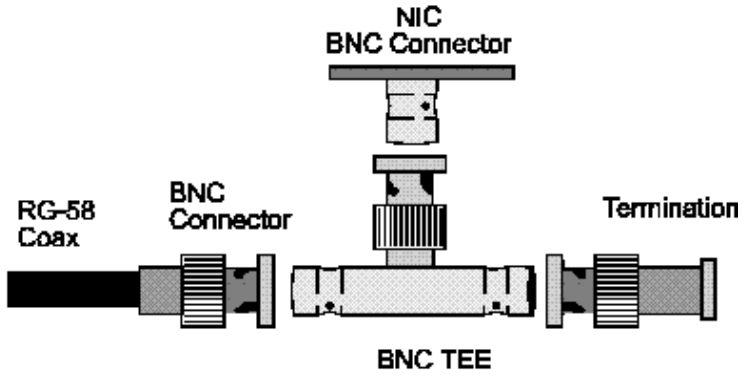
- **Media Transmisi-> Kabel-> *Coaxial***
- Coaxial terdapat dua jenis yaitu *Thicknet* (ukuran besar) & *Thinnet* (ukuran kecil)



Media & Pheriperal Komunikasi

- **Media Transmisi-> Kabel-> *Coaxial***
- Membutuhkan BNC *Connector* untuk menyambungkan kabel coaxial





Media & Pheriperal Komunikasi

- **Media Transmisi-> Kabel-> *Fiber Optic***
- *Fiber optic* terdiri atas suatu gelas fiber yang sangat tipis dan dapat dipergunakan untuk menyalurkan data dalam jumlah dan kecepatan yang sangat tinggi

Media & Pheriperal Komunikasi

Perbandingan Media Transmisi Kabel

Pilihan	Thinnet	Thicknet	Twisted	Fiber Optic
Biaya/Harga	Lebih mahal dari twisted	Lebih mahal dari thinnet	Paling murah	Paling mahal
Jangkauan	185 meter	500 meter	100 meter	2000 meter
Transmisi	10 Mbps	10 Mbps	1 Gbps	>1 Gbps
Fleksibilitas	Cukup	Kurang	Paling	Tidak
Kemudahan Instalasi	Gampang	Gampang	Sangat Gampang	Sulit
Ketahanan terhadap interferensi	Baik	Baik	Rentan	Tidak terpengaruh interferensi

Media & Pheriperal Komunikasi

Media Transmisi-> Tanpa Kabel (*Wireless*)

- Tidak memerlukan koneksi fisik
- Cocok untuk jarak jauh
- Menggunakan gelombang elektromagnetik
- Contoh peralatan dengan media transmisi tanpa kabel: telphone selular, radio, parabola, *wireless adapter, bluetooth adapter, NIC wireless,* dll.

NIC Wireless

Wi FI

JARINGAN & Protokol Komunikasi

Pengertian Jaringan (Network)

- Sistem komputer yang saling berhubungan, telepon, atau perangkat lain yang dapat berkomunikasi dengan yang lain dan berbagi aplikasi dan data

(William,2010)

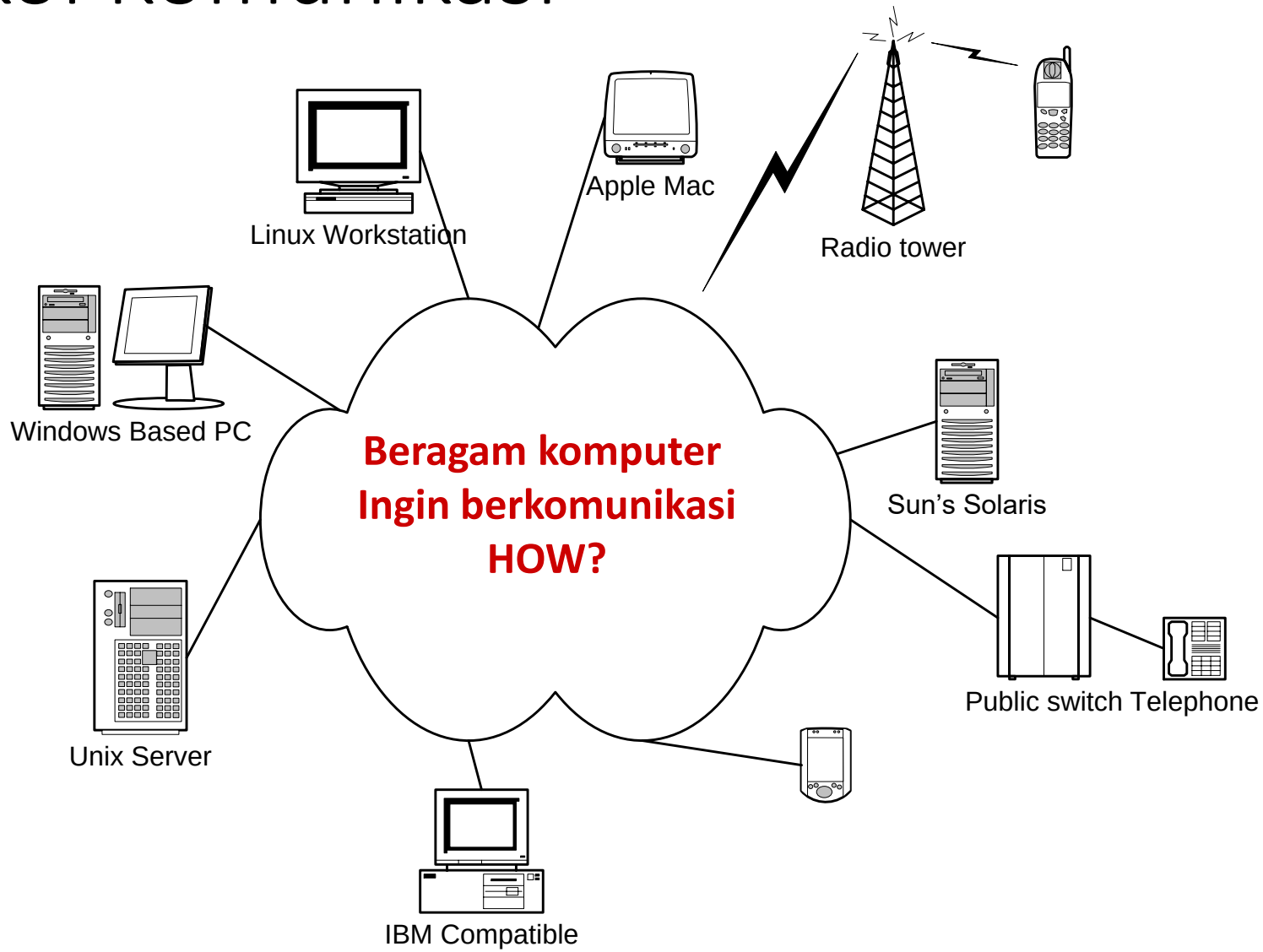
- Berbagi informasi dan sumber daya di antara komputer yang berbeda telah menyebabkan sistem komputer yang terhubung

(Brookshear,2011)

Keuntungan Jaringan (Network)

- Berbagi perangkat periferal
- Berbagi program dan data
- Komunikasi yang lebih baik
- Keamanan informasi
- Akses ke database

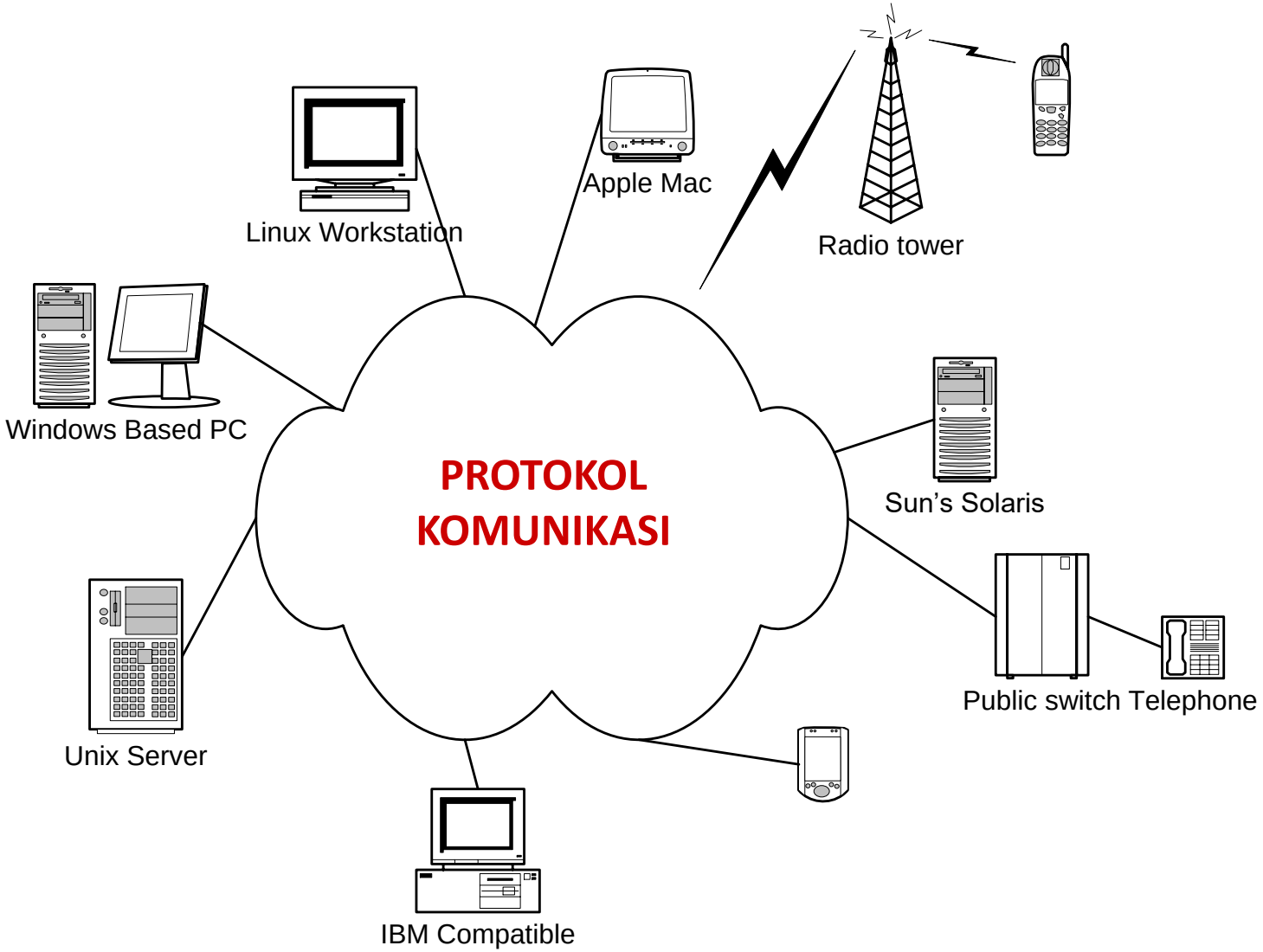
Protokol Komunikasi



Protokol Komunikasi

- Perlu membuat aturan agar beragam peralatan dapat saling berkomunikasi.
  - Sama seperti beragam bangsa perlu bahasa standar supaya dapat saling berkomunikasi
- Aturan tersebut dikenal dengan nama protokol komunikasi.
- Misalnya: bagaimana mengirim pesan, data, informasi dan fungsi lainnya dari pengirim ke penerima agar dapat diterima dengan benar

Protokol Komunikasi



Protokol Komunikasi

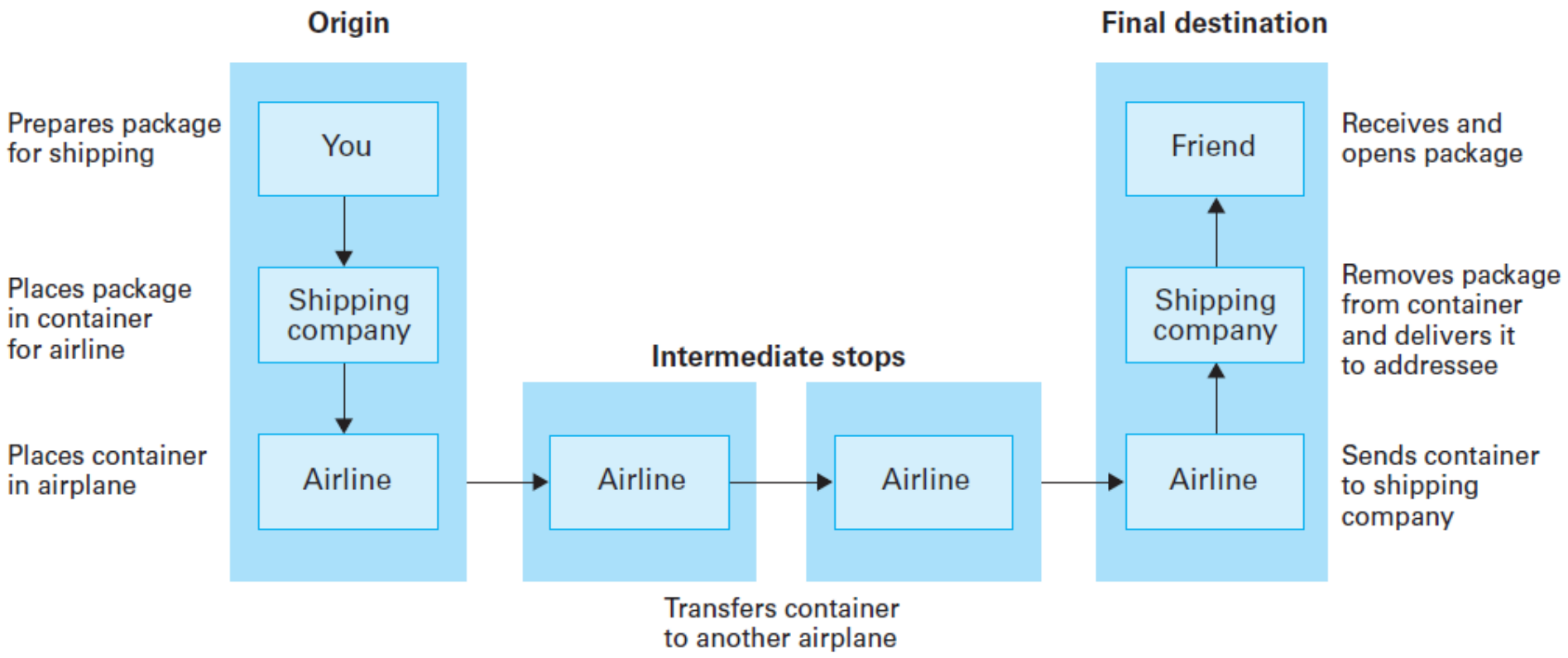
- Protokol komunikasi yang paling umum digunakan adalah protokol TCP/IP

- Dikembangkan oleh ARPA (*Advance Research Project Agency*) tahun 1969

- Memiliki kemampuan:
  - Menghubungkan berbagai jenis sistem operasi
  - Mendukung komunikasi kecepatan tinggi
  - Menangani jaringan yang komplek dan luas

Protokol Komunikasi

- Dalam internet, pesan dikirim melalui hirarki unit software yang melakukan tugas – tugas yang sesuai dengan yang harus dilakukan



Protokol Komunikasi

- TCP/IP atau *Transmission Control Protocol/Internet Protocol,* terdiri dari beberapa lapisan (*layers*) yang mempunyai tugas masing-masing

Application	Menyediakan akses aplikasi ke jaringan, ex: FTP, HTTP, dll
Transport	Memecah data menjadi paket-paket data &, memeriksa semua paket terkirim
Internet	Mengirim paket-paket data ke tujuan
Network Interface	Menentukan rute pengiriman paket
Physical	Menentukan karakteristik kabel yg digunakan, mentransfer, menentukan cara bit-bit dikodekan

Layers TCP/IP

PERANGKAT jaringan

Perangkat Jaringan

Beberapa perangkat jaringan yang sering digunakan antara lain:

- *NIC*
- *Hub*
- *Switch*
- *Repeater*
- *Router*

Perangkat Jaringan

***Network Interface Card* (NIC)**

- *Network Interface Card* (NIC) atau biasa disebut LAN card, digunakan sebagai piranti yang harus tersedia jika ingin menghubungkan komputer (PC) ke jaringan
- Baik dengan menggunakan kabel maupun *wireless* (tanpa kabel)

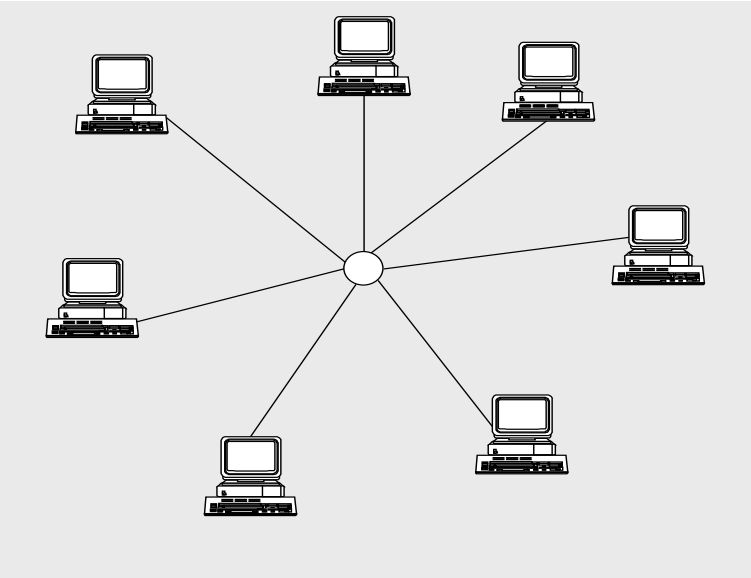
NIC

NIC Wireless

Perangkat Jaringan

Hub

- Piranti yang mempunyai banyak port (*multi port*) sebagai pusat pada jaringan topologi bintang (*star*)
- Hub aktif menghubungkan saluran antar server
- Hub pasif berfungsi membagi saluran dari *server* ke beberapa saluran pada tiap komputer



Perangkat Jaringan

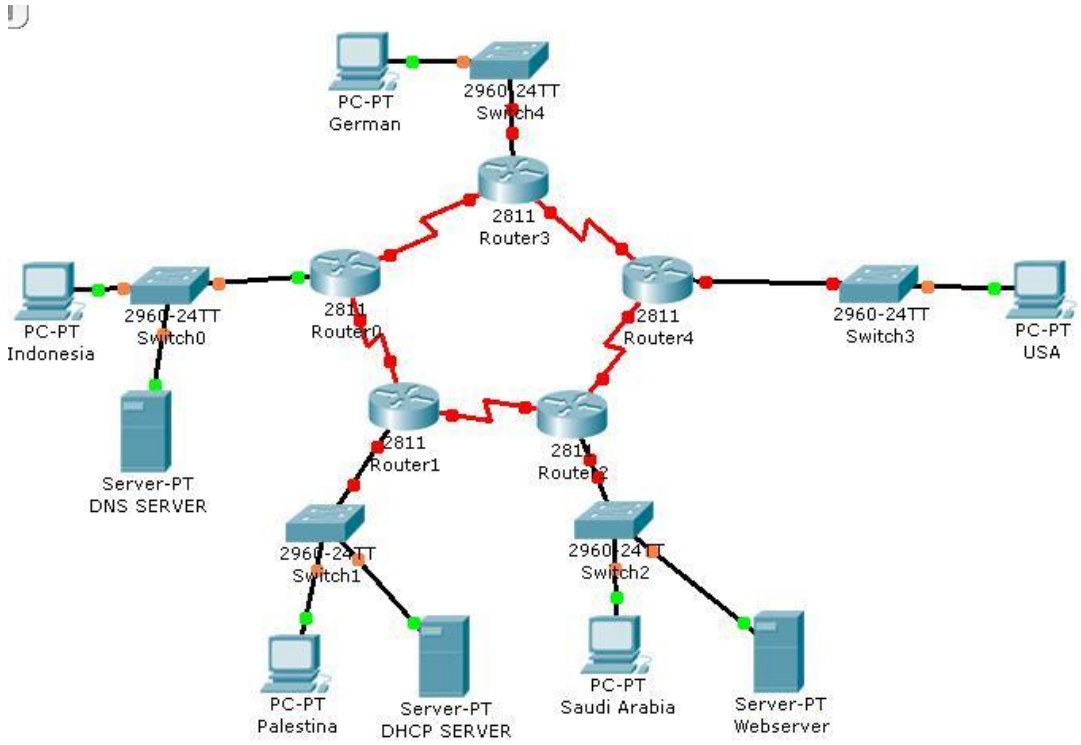
Switch

- Sama dengan Hub, namun memiliki perbedaan fungsi. Jika hub, informasi yang datang dikirimkan semua ke komputer (broadcast).
- Switch memiliki fasilitas routing, sehingga informasi yang diterima hanya dikirimkan ke komputer tujuan

Perangkat Jaringan

Router

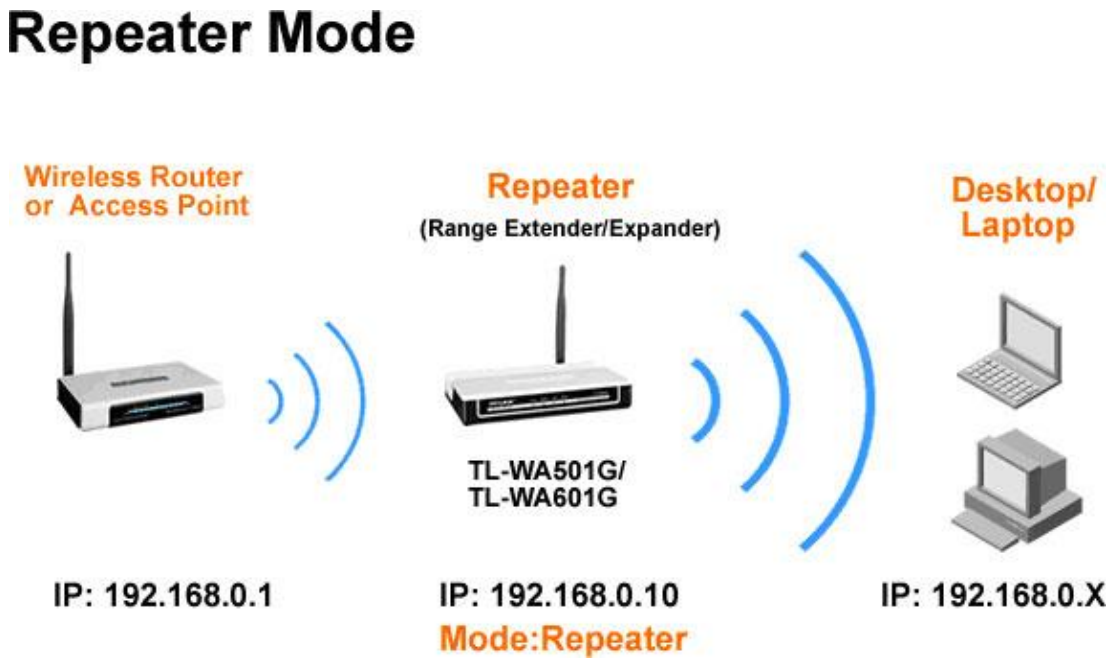
- Piranti yang digunakan untuk menghubungkan jaringan lokal (menghubungkan lebih dari satu LAN)



Perangkat Jaringan

Repeater

- Untuk mengcover daerah-daerah yang lemah sinyal dari Server (pemancar)
- Untuk memperjauh sinyal dari Server (pemancar)



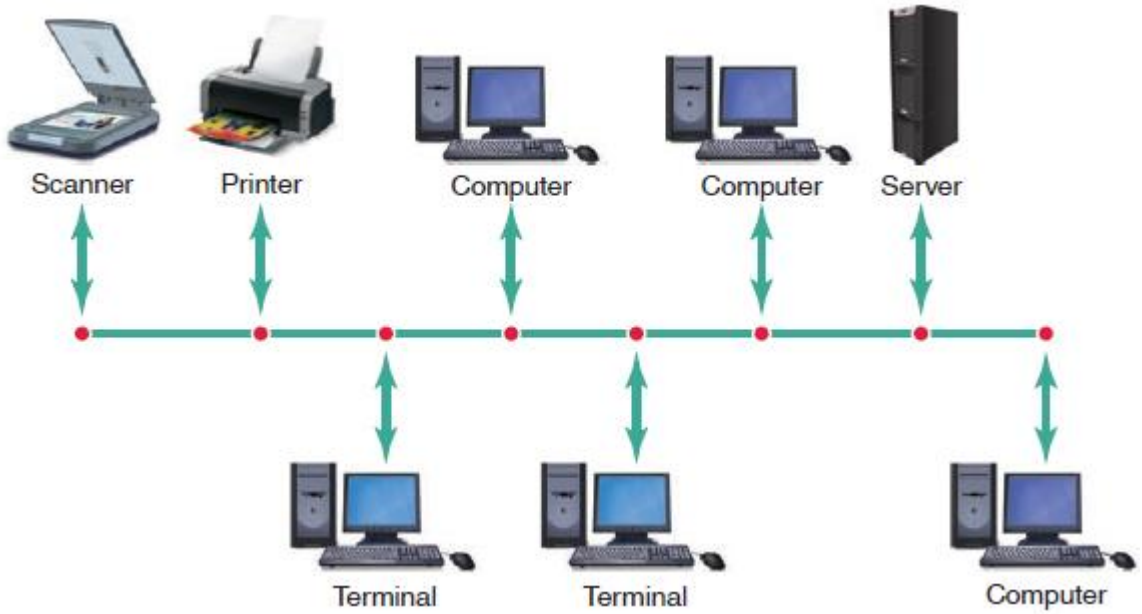
Topologi jaringan KOMPUTER

Topologi Jaringan Komputer

- Susunan jaringan komputer dapat diatur dalam berbagai bentuk yang disebut dengan topologi
- Topologi dasar jaringan komputer :
  - Bus network
  - Ring network
  - Star network

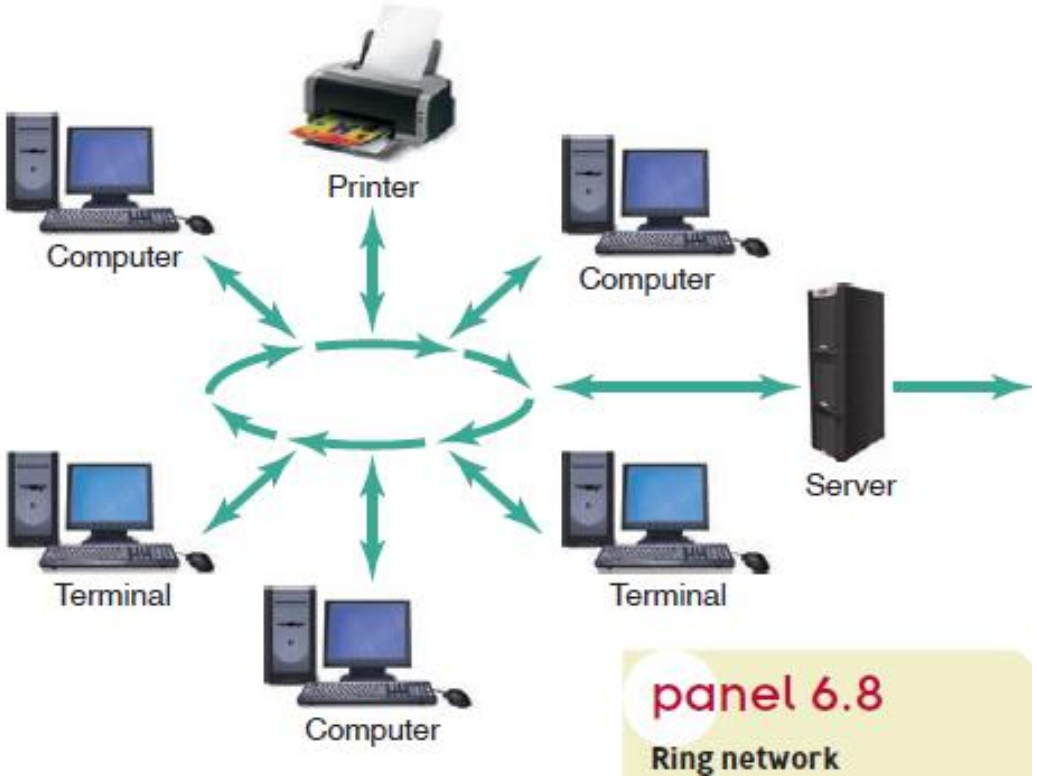
Bus Network

- Semua node dihubungkan ke kabel tunggal yang disebut “bus” yang mempunyai dua buah “endpoint”
- Setiap perangkat komunikasi pada jaringan mengirimkan pesan elektronik ke perangkat lainnya



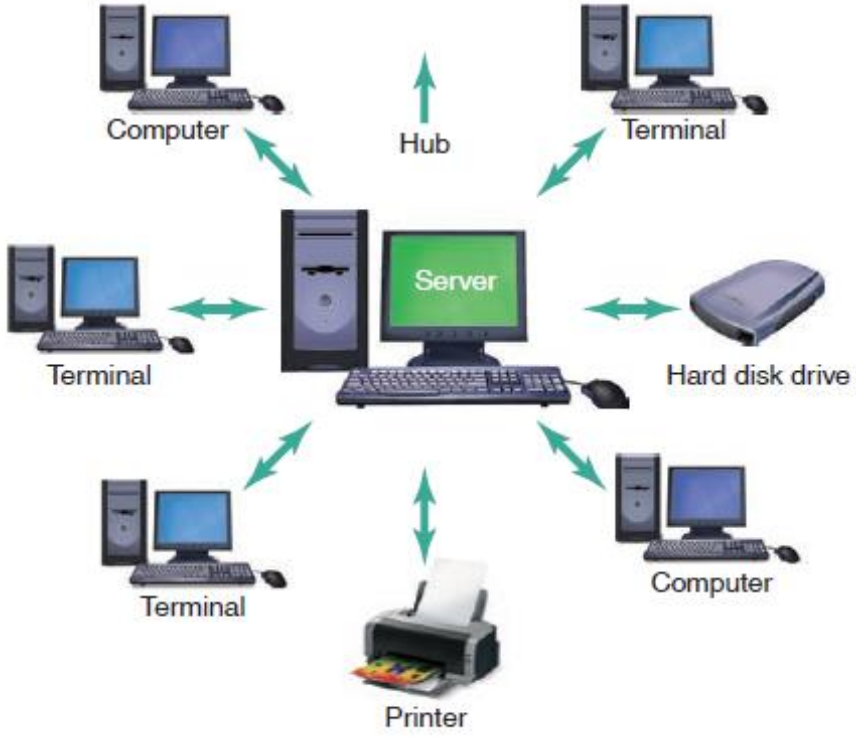
Ring Network

- Semua komputer dan perangkat komunikasi dihubungkan satu kesinambungan
- Tidak terdapat endpoint



Star Network

- Semua komputer dan perangkat komunikasi dihubungkan secara langsung ke server utama
- Semua pesan elektronik dihubungkan melalui hub utama ke tujuan



JENIS JARINGAN

Jenis Jaringan

- Jaringan yang terdiri dari gabungan perangkat komputer, media penyimpanan, dan perangkat komunikasi dapat dibagi menjadi beberapa kategori yang diberdasarkan jangkauan geografis dan tujuannya, yakni :
  - Wide Area Network (WAN)
  - Metropolitan Area Network (MAN)
  - Local Area Network (LAN)
  - Home Area Network (HAN)
  - Personal Area Network (PAN)

Jenis Jaringan

- **WAN**

  jaringan komunikasi yang mencakup wilayah geografis yang luas, seperti negara atau seluruh dunia

- **MAN**

  jaringan komunikasi yang mencakup wilayah kota atau daerah pinggiran kota

- **LAN**

  LAN menghubungkan komputer dan perangkat pada area geografis yang terbatas seperti perkantoran dalam satu gedung atau beberapa gedung yang berdekatan

Jenis Jaringan

- **HAN**

  menggunakan kabel atau nirkabel untuk menghubungkan perangkat digital dalam wilayah rumah

- **PAN**
  - Berbeda dengan HAN, PAN tidak menggunakan kabel
  - PAN atau wireless PAN menggunakan teknologi nirkabel jarak dekat untuk menghubungkan perangkat elektronik pribadi

- PENGKODEAN DATA, Multiplexing

Transmisi Data
Pengkodean Data, Multiplexing
Teknik Komunikasi Data Digital
Data Link Control
Multiplexing
Switching
Medium Access Sublayer
Network Layer

Encoding

- Karakter data yang akan dikirim dari suatu titik ke titik lain tidak dapat dikirimkan secara langsung. Perlu proses pengkodean pada setiap titik. Dengan kata lain, karakter-karakter data tersebut harus dikodekan terlebih dahulu dengan kode yang dikenal oleh setiap terminal yang ada.

- Tujuan dari pengodean adalah menjadikan setiap karakter dalam sebuah informasi digital kedalam bentuk biner agar dapat ditransmisikan. Suatu terminal yang berbeda menggunakan kode biner yang berbeda untuk mewakili suatu karakter.

- Kode-kode yang digunakan untuk keperluan komunikasi data pada sistem komputer dari sejak komputer ditemukan sampai pada komunikasi data modern memiliki perbedaan dari generasi ke generasi. Hal ini disebabkan oleh semakin besar dan kompleksnya data yang akan dikirim atau dipergunakan.

- Secara umum ada beberapa kode yang digunakan dalam komunikasi data diantaranya adalah:
  1. BCD (*Binary Coded Decimal*)
  2. SBCDIC (*Standard Binary Coded Decimal Interchange Code*)
  3. EBCDIC (*Extended Binary Coded Decimal Interchange Code*)
  4. BOUDOT
  5. ASCII (*American Standard Code for Information Interchange*)
  6. UNICODE (*Universal code)*

BCD

- Merupakan kode biner yang digunakan hanya untuk mewakili nilai digit desimal dari 0-9.
- BCD menggunakan kombinasi 4 bit sehingga ada 16 kombinasi yang bisa diperoleh dan hanya 10 kombinasi yang digunakan.
- Kode BCD sudah jarang digunakan untuk komputer dan transmisi data sekarang ini karena tidak dapat mewakili huruf atau simbol karakter khusus.
- BCD hanya digunakan oleh komputer generasi pertama.

Tabel Binary Coded Decimal

BCD 4 bit	Digit Desimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9

SBCDIC

- Merupakan kode biner yang dikembangkan dari BCD.
- SBCDIC menggunakan kombinasi 6 bit sehingga lebih banyak kombinasi yang bisa dihasilkan. Yaitu 64 kombinasi kode.
- Ada 10 kode untuk digit angka dan 26 kode untuk alphabet dan sisanya untuk karakter khusus tertentu.
- SBCDIC digunakan pada komputer generasi kedua.

Tabel Standard Binary Coded Decimal Interchange Code

SBCDIC BA8421	Karakter	SBCDIC BA8421	Karakter
001010	0	100001	J
000001	1	100010	K
000010	2	100011	L
000100	4	100101	N
000101	5	100110	O
000110	6	100111	P
000111	7	101000	Q
001000	8	101001	R
001001	9	010010	S
110001	A	010011	T
110010	B	010100	U
110011	C	010101	V
110100	D	010110	W
110101	E	010111	X
110110	F	011000	Y
110111	G	011001	Z
111000	H		
111001	I		

EBCDIC

- EBCDIC adalah kode 8 bit yang memungkinkan untuk mewakili karakter 256 kombinasi karakter.
- Pada EBCDID, *high order bits* atau 4 bit pertama disebut *Zone bits* dan *low order bits* atau 4 bit kedua disebut dengan *numeric bit.*

Tabel Extended Binary Coded Decimal Interchange Code

	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-A	-B	-C	-D	-E	-F
0-	NUL 00	SOH 01	STX 02	ETX 03	SEL	HT 09	RNL	DEL 7F	GE	SPS	RPT	VT 0B	FF 0C	CR 0D	SO 0E	SI 0F
1-	DLE 10	DC1 11	DC2 12	DC3 13	RES ENP	NL	BS 08	POC	CAN 18	EM 19	UBS	CU1	IFS 1C	IGS 1D	IRS 1E	IUS ITB 1F
2-	DS	SOS	FS	WUS	BYP INP	LF 0A	ETB 17	ESC 1B	SA	SFE	SM SW	CSP	MFA	ENQ 05	ACK 06	BEL 07
3-			SYN 16	IR	PP	TRN	NBS	EOT 04	SBS	IT	RFF	CU3	DC4 14	NAK 15		SUB 1A
4-	SP 20	RSP A0	â E2	ä E4	à E0	á E1	ã E3	å E5	ç E7	ñ F1	[5B	. 2E	< 3C	(28	+ 2B	! 21
5-	& 26	é E9	ê EA	ë EB	è E8	í E0	î EE	ï EF	ì ED	ß DF	] 5D	$ 24	* 2A	) 29	; 3B	^ 5E
6-	- 2D	/ 2F	Â C2	Ä C4	À C0	Á C1	Ã C3	Å C5	Ç C7	Ñ D1	¦ A6	, 2C	% 25	_ 5F	> 3E	? 3F
7-	ø F8	É C9	Ê CA	Ë CB	È C8	Í CD	Î CE	Ï CF	Ì CC	` 60	: 3A	# 23	@ 40	' 27	= 3D	" 22
8-	Ø D8	a 61	b 62	c 63	d 64	e 65	f 66	g 67	h 68	i 69	« AB	» BB	ð F0	ý FD	þ FE	± B1
9-	° B0	j 6A	k 6B	l 6C	m 6D	n 6E	o 6F	p 70	q 71	r 72	ª AA	º BA	æ E6	¸ B8	Æ C6	¤ A4
A-	µ B5	~ 7E	s 73	t 74	u 75	v 76	w 77	x 78	y 79	z 7A	¡ A1	¿ BF	Ð D0	Ý DD	Þ DE	® AE
B-	¢ A2	£ A3	¥ A5	· B7	© A9	§ A7	¶ B6	¼ BC	½ BD	¾ BE	¬ AC	| 7C	¯ AF	¨ A8	´ B4	× D7
C-	{ 7B	A 41	B 42	C 43	D 44	E 45	F 46	G 47	H 48	I 49	SHY AD	ô F4	ö F6	ò F2	ó F3	õ F5
D-	} 7D	J 4A	K 4B	L 4C	M 4D	N 4E	O 4F	P 50	Q 51	R 52	¹ B9	û FB	ü FC	ù F9	ú FA	ÿ FF
E-	\ 5C	÷ F7	S 53	T 54	U 55	V 56	W 57	X 58	Y 59	Z 5A	² 82	Ô D4	Ö D6	Ò D2	Ó D3	Õ D5
F-	0 30	1 31	2 32	3 33	4 34	5 35	6 36	7 37	8 38	9 39	³ 83	Û D8	Ü DC	Ù D9	Ú DA	EO

Kode Boudot

- Kode Boudot terdiri atas 5 bit yang dipergunakan pada terminal teletype dan teleprinter. Karena kombinasi ini terdiri dari 5 bit maka hanya terdiri dari 25 sampai 32 kombinasi dengan kode huruf dan gambar yang berbeda.

Tabel Kode Boudout

Kode`	Karakter Letter	Karakter Figure
11000	A	-
10011	B	?
01110	C	:
10010	D	$
10000	E	3
10110	F	!
01011	G	&
00101	H	#
01100	I	8
11010	J	‘
11110	K	(
01001	L	)
00111	M	.
00110	N	,
01101	P	0
11101	Q	1
01010	R	4
10100	S	BELL
00001	T	5
11100	U	7
01111	V	;
11001	W	2
10111	X	/
10101	Y	6
10001	Z	“
11111	LTRS	LTRS
11011	FIGS	FIGS
00100	SPC	SPC
00010	CR	CR
01000	LF	LF
00000	NULL	NULL

ASCII Code

- Kode ASCII mempunyai lebar data 7 bit
- Kode ASCII memiliki 128 bit kombinasi yang selalu digunakan.
- Dari 128 kombinasi tersebut 32 kode diantaranya digunakan untuk fungsi-fungsi kendali seperti SYN, STX.
- Sisa karakter lain digunakan untuk karakter-karakter alphanumerik dan sejumlah karakter khusus seperti =, / . ?
- Pada dasarnya kode ASCII merupakan kode alfanumerik yang paling popular dalam teknik komunikasi data.

Tabel Kode ASCII

Dec	Hx	Oct	Char		Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL	(null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH	(start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX	(start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX	(end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT	(end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ	(enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK	(acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL	(bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS	(backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB	(horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF	(NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT	(vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF	(NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR	(carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO	(shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI	(shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE	(data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1	(device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2	(device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3	(device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4	(device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK	(negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN	(synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB	(end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN	(cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM	(end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB	(substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC	(escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS	(file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS	(group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS	(record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US	(unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

www.LookupTables.com

Unicode

- Orang-orang di negara-negara yang berbeda menggunakan karakter berbeda untuk menuliskan kata-kata dalam bahasa ibu mereka.
- Unicode memiliki lebar data 16 bit sehingga mampu menampung huruf, angka, karakter khusus dan karakter control sebanyak 65536 kombinasi
- Kode ASCII termasuk ke dalam kodoe Unicode.
- Contoh kode unicode adalah kode untuk bahasa china,jepang, arab, armenian (yunani),dll

- Unicode Bahasa Armenian

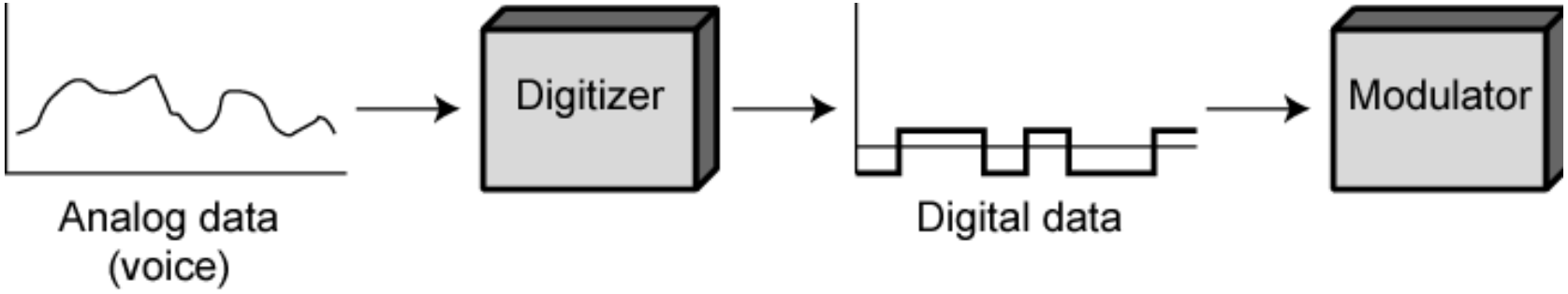
Armenian

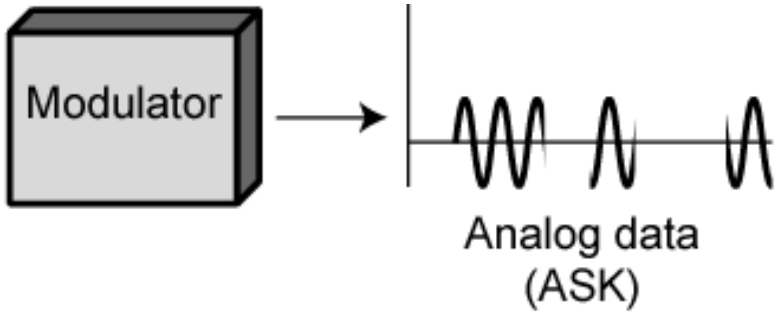
	0533	0534	0535	0536	0537	0538
0		Հ	Ր		Տ	Ո
1	Ա	Ձ	Ց	Ա	Ձ	Ց
2	Բ	Ղ	Բ	Բ	Ղ	Բ
3	Գ	Ճ	Գ	Գ	Ճ	Գ
4	Դ	Մ	Դ	Դ	Մ	Դ
5	Ե	Յ	Ե	Ե	Յ	Ե
6	Զ	Ն	Զ	Զ	Ն	Զ
7	Է	Շ		Է	Շ	Է
8	Ը	Ո		Ը	Ո	
9	Թ	Չ	՝	Թ	Չ	՝
A	Ժ	Պ	՞	Ժ	Պ	՞
B	Ի	Ջ	՟	Ի	Ջ	
C	Լ	Ռ	ՠ	Լ	Ռ	
D	Խ	Ս	ա	Խ	Ս	
E	Ծ	Վ	բ	Ծ	Վ	
F	Կ	Տ	գ	Կ	Տ	

Teknik Pengkodean

- Teknik Pengkodean merupakan hal yang sangat penting dalam komunikasi data karena pada proses inilah sinyal yang ada diubah ke bentuk tertentu yang dimengerti oleh peralatan tertentu.

Digitalisasi Data Analog





Jenis Teknik Pengkodean

Teknik Encoding

1. Data digital, sinyal digital
2. Data analog, sinyal digital
3. Data digital, sinyal analog
4. Data analog, sinyal analog

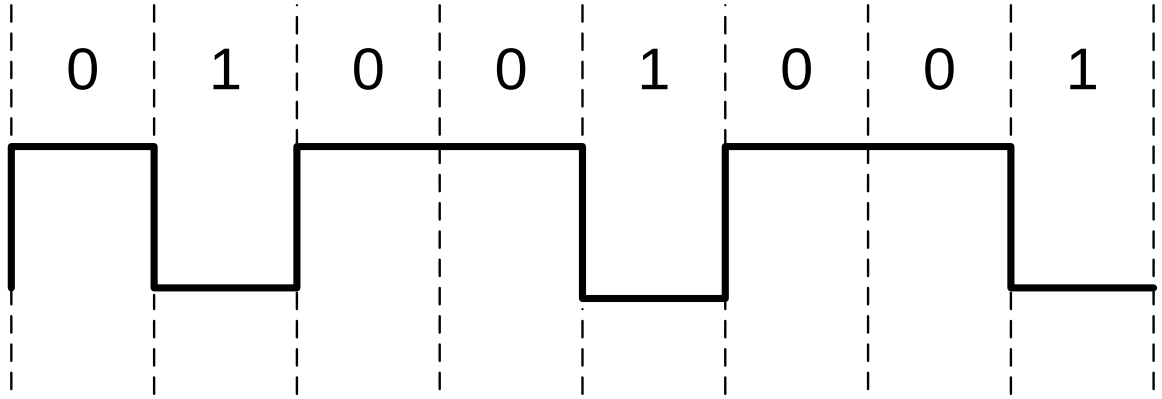
1. Data Digital,Sinyal Digital

- Sinyal digital

- Deretan voltase yang terputus-putus.
- Tiap pulsa merupakan elemen sinyal.
- Sinyal unipolar adalah semua elemen sinyal memiliki tanda yang sama.
- Sinyal polar adalah sinyal yang memiliki tanda berbeda, sinyal positif, negatif ataupun nol.
- Sinyal dinyatakan dengan mark dan space, mark = 1 dan space=0

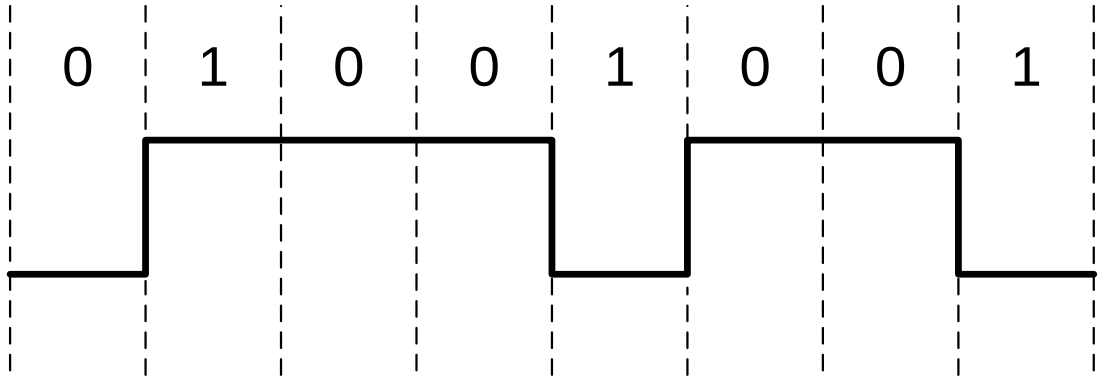
1. Non Return To Zero Level (NRZL)

- Suatu kode di mana tegangan negatif dipakai untuk mewakili suatu binary dan tegangan positif dipakai untuk mewakili binary lainnya.
- Biasanya bit 0 mewakili tegangan tinggi dan bit 1 mewakili tegangan rendah.
- Contoh:



2. Non Return To Zero Inverted (NRZI)

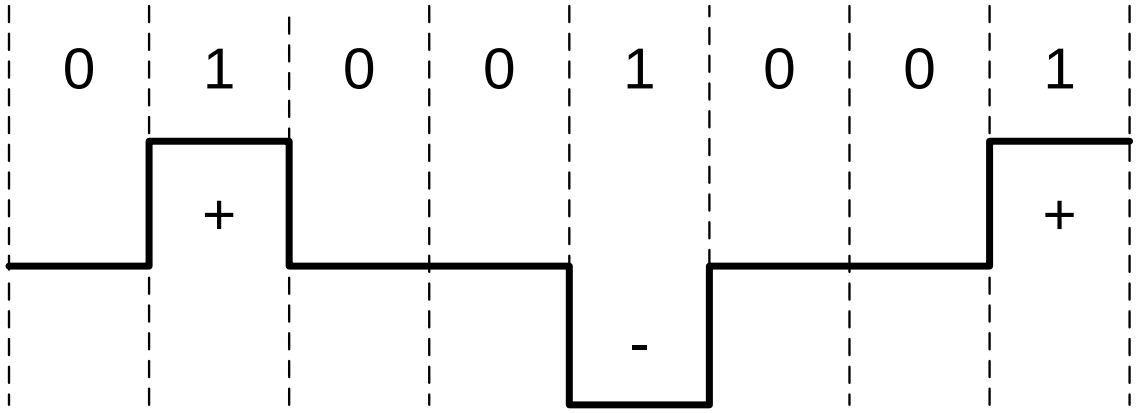
- Suatu kode di mana suatu transisi (low ke high atau high ke low) pada awal suatu bit time akan dikenal sebagai biner 1.
- Ditengah transisi (low ke high) bernilai biner 0
- Ditengah transisi (high ke low) bernilai biner 1
- Jika tidak ada transisi (low ke low atau high ke high)maka nilai biner mengikuti nilai sebelumnya.
- Contoh:



Jenis-jenis Pengkodean Data Digital,Sinyal Digital

3. Bipolar-AMI

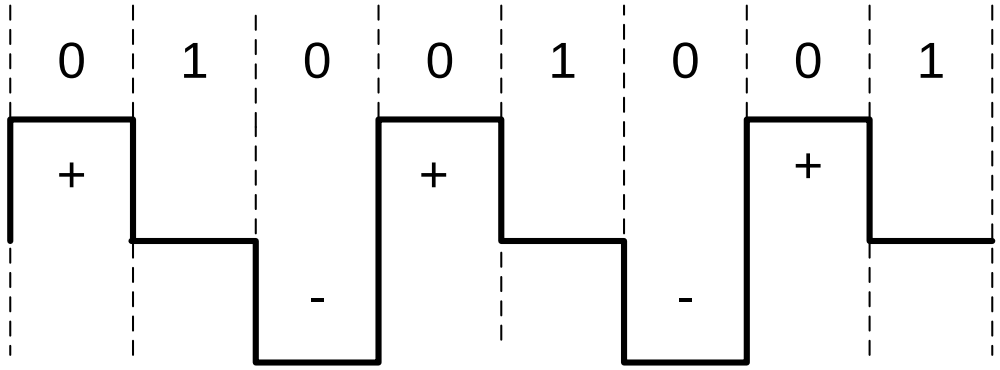
- Suatu kode dimana binary ‘0’ diwakili dengan tidak adanya sinyal garis dan binary ‘1’ diwakili oleh suatu pulsa positif atau negatif yang berubah-ubah polaritasnya.
- Binary ‘1’ diawal transmisi adalah pulsa positif, kemudian jika bertemu dengan binary ‘1’ yang lain akan ditandai dengan pulsa negatif dan seterusnya polaritasnya akan bergantian.
- Contoh:



Jenis-jenis Pengkodean Data Digital,Sinyal Digital

4. Pseudoternary

- Suatu kode dimana binary ‘1’ diwakili dengan tidak adanya sinyal garis dan binary ‘0’ diwakili oleh suatu pulsa positif atau negatif yang berubah-ubah polaritasnya.
- Binary ‘0’ diawal transmisi adalah pulsa positif, kemudian jika bertemu dengan binary ‘0’ yang lain akan ditandai dengan pulsa negatif dan seterusnya polaritasnya akan bergantian.
- Contoh:



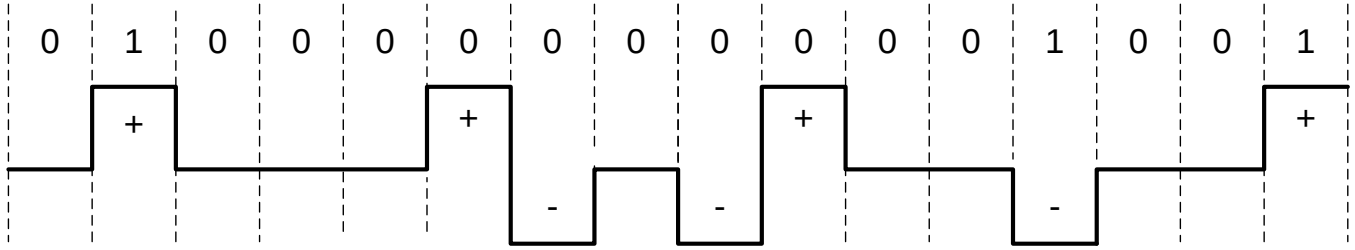
Jenis-jenis Pengkodean Data Digital,Sinyal Digital

4. B8ZS (Bipolar with 8-Zero Substitution)

- Suatu kode yang mengikuti aturan Bipolar-AMI tetapi dimana jika:

1. Jika terjadi oktaf dari semua nol dan pulsa terakhir yang mendahului oktaf ini adalah positif, maka 8 nol dari oktaf tersebut di encode sebagai 000+-0-+
2. Jika terjadi oktaf dari semua nol dan pulsa terakhir yang mendahului oktaf ini adalah negatif, maka 8 nol dari oktaf tersebut di encode sebagai 000-+0+-

- kemudian setelah substitusi oktaf binary ‘0’, mengikuti aturan Bipolar-AMI kembali.
- Contoh:



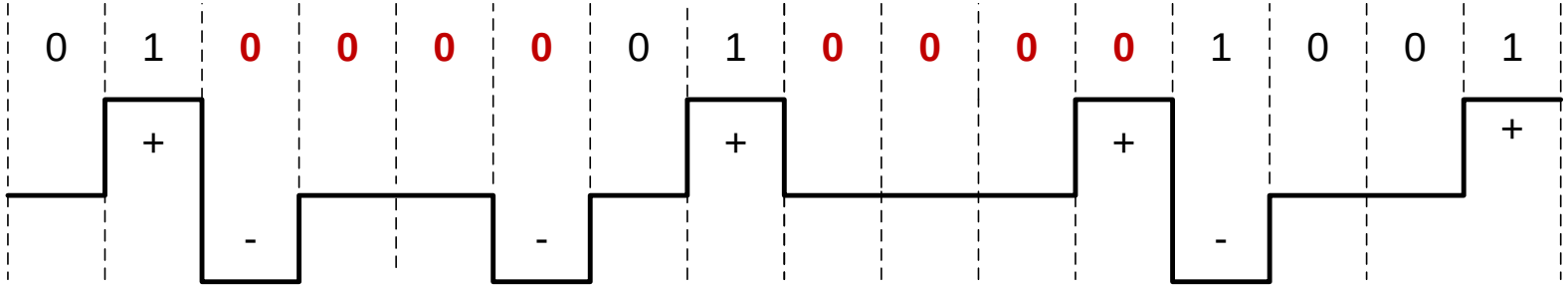
Jenis-jenis Pengkodean Data Digital,Sinyal Digital

4. HDB3

- Suatu kode yang mengikuti aturan Bipolar-AMI tetapi dimana jika terjadi 4 dari semua nol maka:

Polaritas dari Pulsa akhir	Jumlah dari pulsa-pulsa bipolar karena subsitusi terakhir	
	Genap	Ganjil
-	000-	+00+
+	000+	-00-

- kemudian setelah substitusi empat binary ‘0’, mengikuti aturan Bipolar-AMI kembali.
- Contoh:



2. Data Digital,Sinyal Analog

- Jaringan Telepon Umum
- 300Hz sampai 3400Hz Menggunakan modem (modulator-demodulator)

1. **Amplitude shift keying (ASK)**

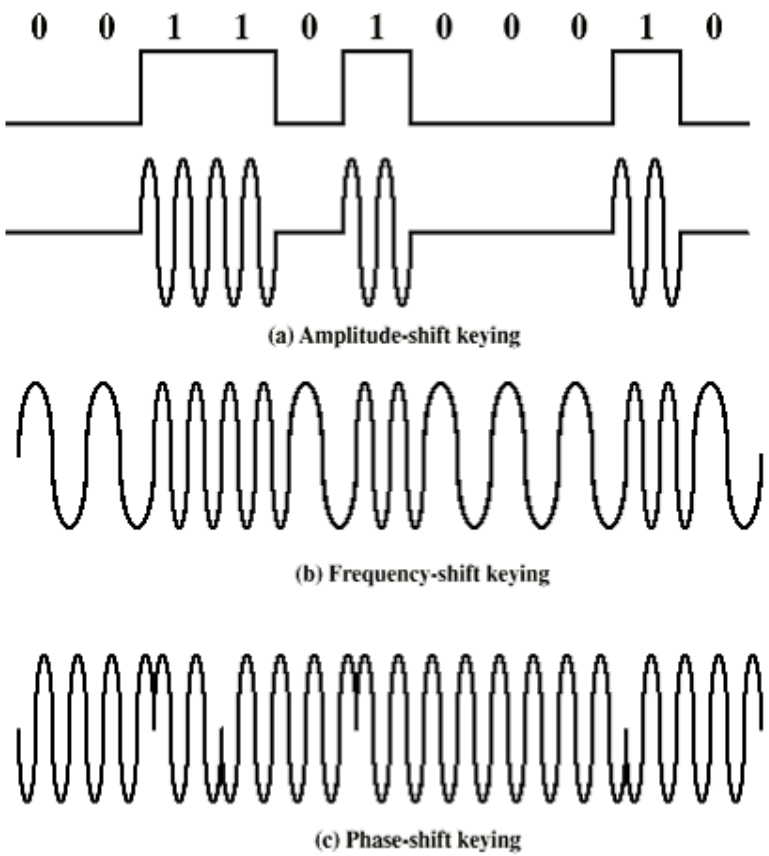
$$s(t) = \begin{cases} A\cos(2\pi f_c t + \theta_c) & \text{binary 1} \quad \text{--> sinyal carrier} \\ 0 & \text{binary 0} \end{cases}$$

2. **Frequency shift keying (FSK)**

$$s(t) = \begin{cases} A\cos(2\pi f_1 t + \theta_c) & \text{binary 1} \\ A\cos(2\pi f_2 t + \theta_c) & \text{binary 0} \end{cases}$$

3. **Phase shift keying (PK)**

$$s(t) = \begin{cases} A\cos(2\pi f_c t + \pi) & \text{binary 1} \\ A\cos(2\pi f_c t) & \text{binary 0} \end{cases}$$



3. Data Analog, sinyal Digital

- Teknik yang digunakan adalah Pulse Code Modulation (PCM) dan Delta Modulation (DM)

1. **Pulse Code Modulation**

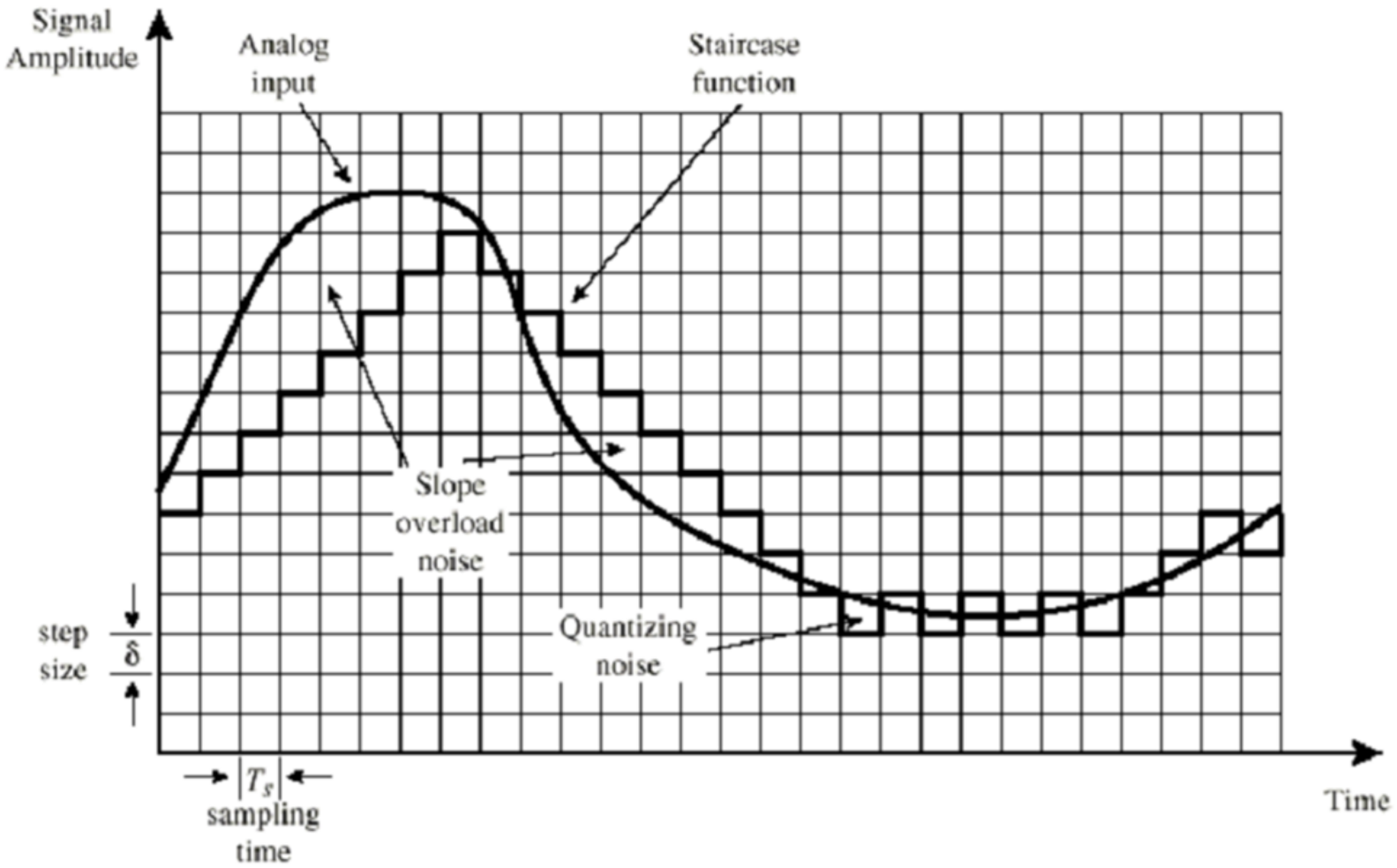
- Teknik yang menggunakan frekuensi sampling yang harus lebih besar atau sama dengan dua kali frekuensi tertinggi sinyal
- Jika frekuensi sampling lebih besar maka dinyatakan dengan biner ‘1’ dan sebaliknya.

2. **Delta Modulation (DM)**

- Proses dimana suatu input analog didekati dengan suatu fungsi yang bergerak naik atau turun dengan satu level quantization pada setiap interval sampling dan outputnya diwakilkan sebagai bit biner tunggal untuk setiap sampel.

3. Data Analog, sinyal Digital

Contoh : Delta Modulation (DM)



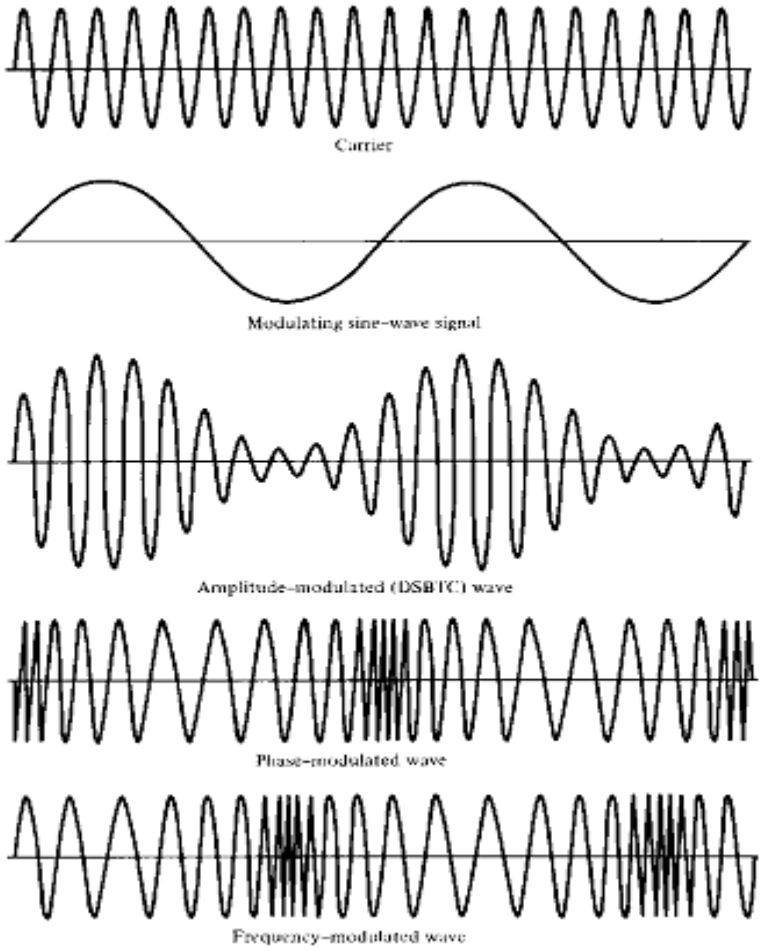
4. Data Analog,Sinyal Analog

- Kenapa perlu modulasi Data Analog :

- Frekuensi tinggi dapat memberikan trasmisi yang lebih efisien

- Tipe ini terbagi atas:

1. **Amplitudo**
2. **Frequency**
3. **Phase**



PENGKODEAN DATA / *DATA ENCODING*

- Data yang dikirimkan antar perangkat harus dimengerti oleh pihak pengirim maupun penerima.
- Oleh karena itu, data harus diubah bentuknya dalam bentuk khusus atau yang biasa disebut dengan SANDI dalam melakukan komunikasi data.
- Coding adalah penggambaran dari satu set simbol menjadi set simbol yang lain
- Skema Pengkodean adalah memetakan secara sederhana mulai dari bit-bit data sampai menjadi elemen sinyal. Teknik pengkodean yang paling sederhana adalah Pulse Code Modulation (PCM).

SISTEM SANDI

1. ASCII (*American Standard Code for Information Interchange*)
   a. Paling banyak/umum digunakan
   b. Merupakan sandi 7 bit
   c. Terdapat 128 macam simbol
   d. Transmisi asinkron terdiri dari 10 atau 11 bit yaitu : 1 bit awal, 7 bit data, 1 bit paritas, 1 atau 2 bit akhir

2. Sandi *Baudot Code* (CCITT Alfabet No 2 / Telex code)
   a. Terdiri dari 5 bit
   b. Terdapat 32 macam simbol
   c. Transmisi asinkron terdiri 7 bit, yaitu 1 bit awal, 5 bit data dan 1 bit akhir

SISTEM SANDI

3. Sandi 4 atau 8
   a. Merupakan sandi dari IBM dengan kombinasi yang diperbolehkan adalah 4 buah “1” dan 4 buah “0”
   b. Terdapat 70 karakter yang dapat diberi sandi
   c. Transmisi asinkron membutuhkan 10 bit, yaitu 1 bit awal, 8 bit data dan 1 bit akhir
4. BCD (*Binary Code Decimal*)
   a. Sandi 6 bit
   b. Terdapat 64 kombinasi bit
   c. Transmisi asinkron membutuhkan 9 bit, yaitu 1 bit awal, 6 bit data , 1 bit paritas dan 1 bit akhir
5. EBCDIC (*Extended Binary Coded Decimal Interchange Code*)
   a. Sandi 8 bit untuk 256 karakter
   b. Transmisi asinkron membutuhkan 11 bit, yaitu 1 bit awal, 8 bit data, 1 bit paritas dan 1 bit akhir

PENGELOMPOKAN KARAKTER

Pada komunikasi data, informasi yang dipertukarkan terdiri dari 2 group, yaitu :

1. Karakter data
2. Karakter kendali

   Digunakan untuk mengendalikan transmisi data, bentuk (format data), hubungan naluri data dan fungsi fisik terminal

PENGELOMPOKAN KARAKTER KENDALI

1. **TRANSMISI CONTROL**

   Berfungsi untuk mengendalikan data pada saluran. Transmisi control terdiri dari beberapa jenis, diantaranya :

   a. **SOH (Start of Header)**

      Digunakan sebagai karakter pertama yang menunjukkan bahwa karakter berikutnya adalah *header*

   b. **STX (Start of Text)**

      Digunakan untuk mengakhiri *header* dan menunjukkan awal dari *text*/informasi

   c. **ETX (End of Text)**

      Digunakan untuk mengakhiri *text*

   d. **EOT (End of Transmision)**

      Untuk menyatakan bahwa transmisi dari *text* baik satu atau lebih telah berakhir

   e. **ENQ (Enquiry)**

      Untuk meminta agar *remote station* memberi tanggapan

PENGELOMPOKAN KARAKTER KENDALI

1. **TRANSMISI CONTROL**

   Berfungsi untuk mengendalikan data pada saluran. Transmisi control terdiri dari beberapa jenis, diantaranya :

   f. **ACK (Acknowledge)**

      Berfungsi untuk memberi tanggapan positif kepada pengirim dari penerima

   g. **NAK (Negatif Acknowledge)**

      Merupakan tanggapan negatif dari penerima ke pengirim

   h. **SYN (Synchronous)**

      Digunakan untuk transmisi sinkron dalam menjaga atau memperoleh sinkronisasi antar peralatan terminal

   i. **ETB (End of Transmition Block)**

      Digunakan untuk menyatakan akhir dari blok data yang ditransmisikan, bila data dipecah menjadi beberapa blok

   j. **DLE (Data Link Escape)**

      Mengubah arti karakter berikutnya, digunakan untuk lebih mengendalikan transmisi data

PENGELOMPOKAN KARAKTER KENDALI

2. Format Effectors

   Digunakan untuk mengendalikan tata letak fisik informasi pada tampilan layar

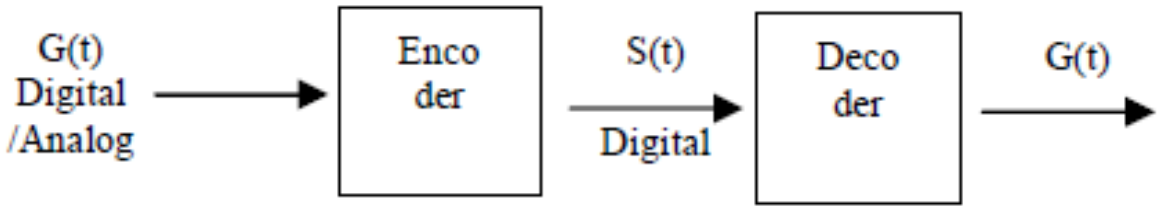
3. Device Control

   Digunakan untuk mengendalikan peralatan tambahan dari terminal

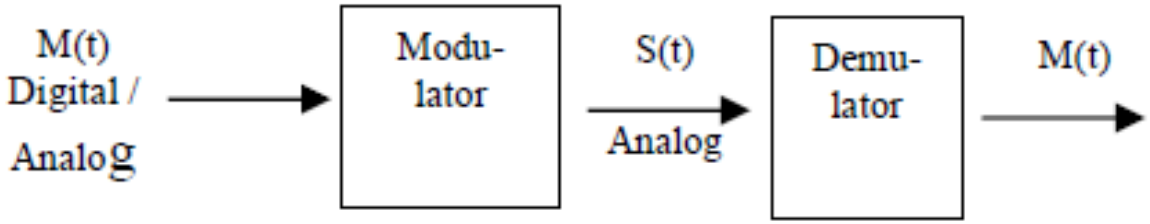
4. Information Separators

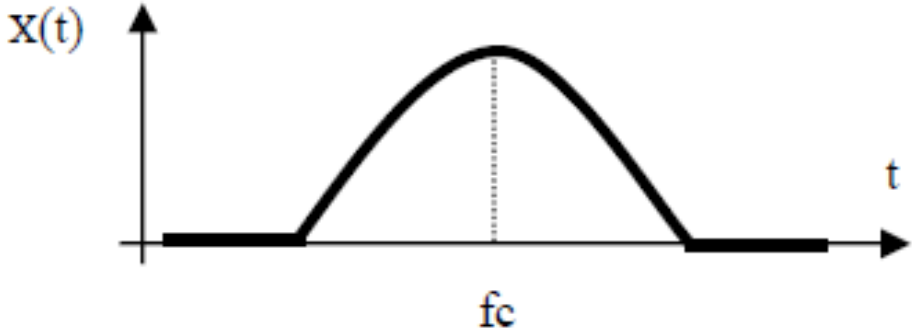
   Digunakan untuk mengelompokkan data secara logis

Digital Signalling dengan teknik encoding



Analog Signalling dengan teknik modulation





- Komunikasi data selalu menggunakan sinyal digital
- Kelemahan sinyal digital : jarak pendek
- Sinyal analog : jarak tempuh jauh
- Sinyal digital mengenal dua keadaan biner (0 dan 1)
- **Teknik modulasi** : merupakan teknik yang digunakan untuk mengirimkan sinyal digital

Modulasi : digital – analog – digital
Demodulasi : digital – analog
Gelombang pembawa sinyal disebut carrier dan berbentuk sinusoidal

Teknik modulasi merupakan dasar dari frequency
Modulasi adalah proses encoding sumber data dalam suatu sinyal carrier dengan frequensi fc.

3 jenis modulasi :

1. Amplitudo
   Tinggi rendahnya tegangan dari sinyal analog
2. Frequency
   Jumlah gelombang sinyal analog dalam 1 detik
3. Phase
   Besarnya sudut dari sinyal analog pada saat tertentu

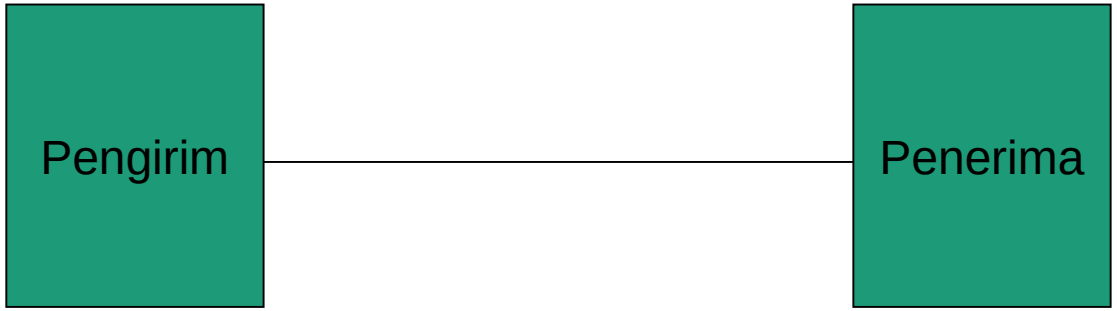
TEKNIK KOMUNIKASI DATA DIGITAL

Transmisi Data
Pengkodean Data
Teknik Komunikasi Data Digital
Data Link Control
Multiplexing
Switching
Medium Access Sublayer
Network Layer

Teknik komunikasi data digital

2. Serial Transmission

antara pengirim dan penerima dihubungkan hanya oleh 1 jalur transmisi untuk pengiriman jarak jauh



Contoh : keyboard ke prosesor, prosesor ke printer, LAN, MAN, WAN

Lebih unggul mana?

Masing-masing punya keunggulan

Paralel :

Cepat, karena beberapa bit dapat dikirim bersamaan melalui jalur yang berbeda. Tetapi sangat mahal, sehingga hanya untuk pengiriman jarak pendek

Serial :

Lambat tetapi murah, sehingga dikembangkan lebih lanjut

Serial transmission

1. Asynchronous

- Tidak perlu sinkronisasi clock antara pengirim dan penerima
- Strategi dari metode ini yaitu mencegah problem timing dengan tidak mengirim aliran bit panjang yang tidak putus-putus.
- Melainkan data ditransmisi per karakter pada suatu waktu, dimana tiap karakter adalah 5 sampai 8 bit panjangnya.

- Timing atau synchronisasi harus dipertahankan antara tiap karakter.
- Receiver mempunyai kesempatan untuk men-synchron-kan awal dari tiap karakter baru.
- Asynchronous sering disebut juga sebagai Asynchronous Transfer Mode (ATM).
- Contoh: modem, mesin fax, TCP/IP, mail, buletin board, RS-232, com #, USB,dll

untuk setiap data yang dikirim terdiri :

a. start bit : 1 buah bit, bit 0

sebagai tanda dimulainya pengiriman 1 buah data

b. bit-bit data

jumlahnya tergantung sistem yang digunakan

c. bit paritas : 1 buah bit,

- digunakan sebagai error detection
- paritas ganjil atau genap

d. stop bit : 1 buah bit, bit 1

sebagai tanda berakhirnya pengiriman 1 buah data

- Keuntungan Komunikasi asynchronous adalah:
  - Sederhana dan murah tetapi memerlukan tambahan 2 sampai 3 bit per karakter untuk synchronisasi.
  - Persentase tambahan dapat dikurang dengan mengirim blok-blok bit yang besar antara start dan stop bit, tetapi akan memperbesar kumulatif timing error.

Serial Transmission

2. Synchronous

- proses pengirim dan penerima diatur sedemikian rupa sehingga memiliki pengaturan yang sama, sehingga dapat diterima dan dikirim denan baik.
- umumnya pengaturan ini didasarkan pada waktu dalam mengirimkan sinyal.
- waktu ini diatur oleh denyut listrik secara periodik yang disebut *clock* .
- dengan kata lain synchronous adalah sistem operasi untuk kejadian yang terjadi pada waktu bersamaan, berkelanjutan dan dapat diprediksi.
- contoh: chating , Ethernet

- perlu sinkronisasi clock pengirim dan penerima, alatnya : bit-bit sinkronisasi
- data dan bit-bit tambahan dikirimkan dalam frame-frame dan dipisahkan sesuai jenisnya

- Dengan transmisi synchronous, ada level lain dari synchronisasi yang perlu agar receiver dapat menentukan awal dan akhir dari suatu blok data.
- Untuk itu, tiap blok dimulai dengan suatu pola preamble bit dan diakhiri dengan pola postamble bit. P
- ola-pola ini adalah kontrol informasi.
- Frame adalah data plus kontrol informasi.

- Format yang tepat dari frame tergantung dari metode transmisinya, yaitu :
  1. Transmisi *character-oriented* merupakan blok data diperlakukan sebagai rangkaian karakter-karakter (biasanya 8 bit karakter) dan semua kontrol informasi dalam bentuk karakter.
  2. Transmisi *bit-oriented* yaitu blok data diperlakukan sebagai serangkaian bit-bit dan kontrol informasi dalam bentuk 8 bit karakter.

- Keuntungan transmisi synchronous :
  1. Efisien dalam ukuran blok data, sedangkan transmisi asynchronous memerlukan 20% atau lebih tambahan ukuran.
  2. Kontrol informasi kurang dari 100 bit.

Contoh alat

- Sinkon

. Asinkron

Perbedaan antara synchronous dengan asynchronous yang terutama tergantung dari ada tidaknya jeda antara pertukaran pesan dan fleksibilitas waktu antar pengguna komunikasi tersebut.

- Keuntungan dari Komunikasi Digital :
  1. Error hampir selalu dapat dikoreksi.
  2. Mudah menampilkan sinyal, seperti encryption.
  3. Range dinamis yang lebih besar (perbedaan nilai terendah terhadap tertinggi) dapat dimungkinkan.
  4. Sistem komunikasi digital juga memiliki kualitas data yang baik, karena dapat dilakukan pengecekan kesalahan dalam transmisi datanya.

- Sedangkan kerugian dari komunikasi digital :
  1. Biasanya memerlukan badwidth yang lebih besar.
  2. Memerlukan sinkronisasi.

- Review

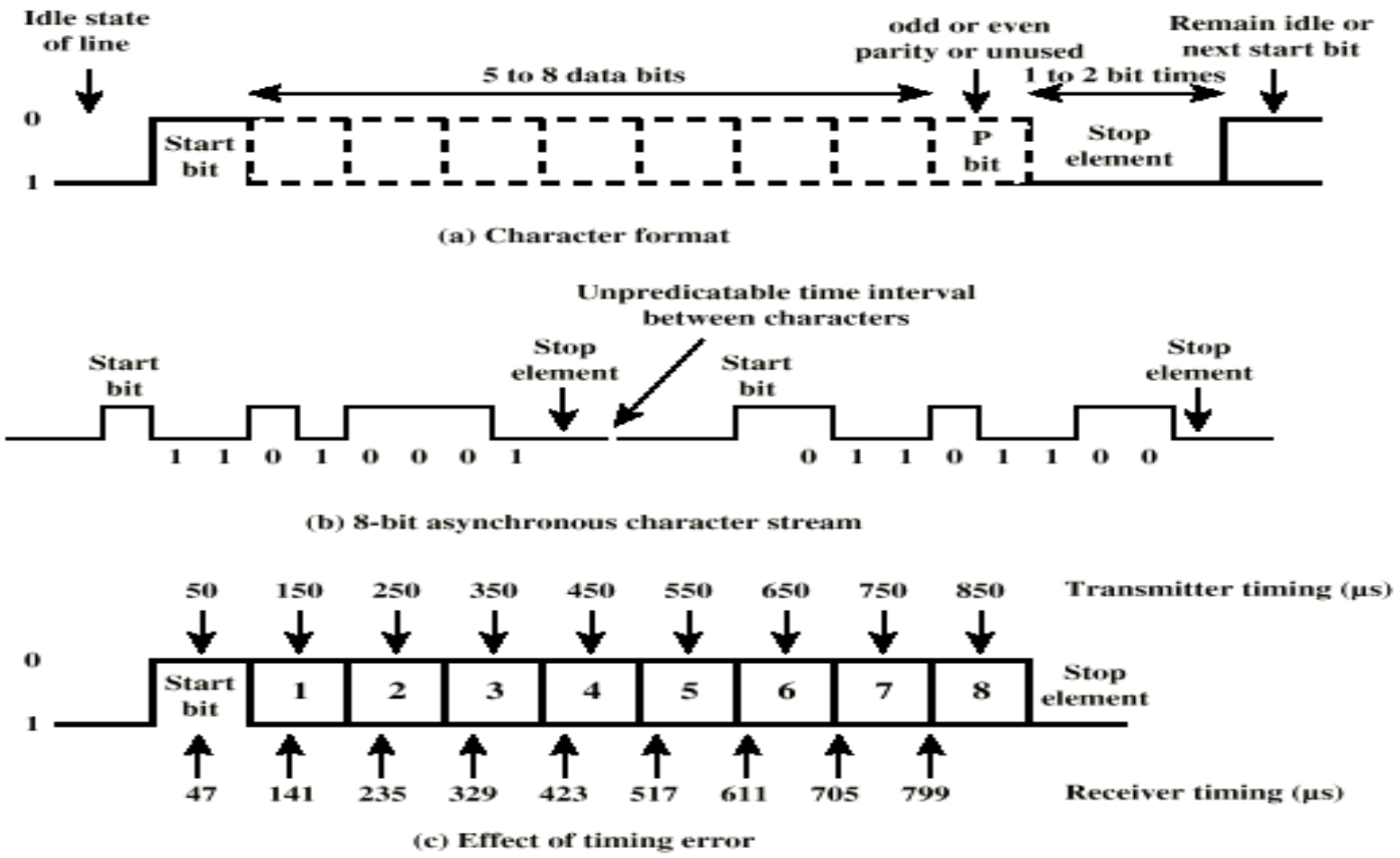
Transmisi Asinkron dan Sinkron

- Masalah waktu membutuhkan mekanisme untuk menyamakan antara transmiter dan receiver
- Dua salusi
  - Asinkronisasi
  - Sinkronisasi

Asinkron

- Data ditransmisikan dalam karakter setiap waktu
  - 5 to 8 bits
- Timing (waktu) hanya memerlukan pertahanan dalam tiap karakter
- Sinkronisasi ulang tiap karakter

Asinkron diagram



Asinkron

- Pada aliran yang tetap, interval diantara karakter adalah sama (panjang elemen stop)
- Dalam keadaan tidak lancar,receiver mengecek untuk transisi 1 ke 0
- Saat 7 interval sample berikutnya (panjang karakter)
- Melihat untuk 1 ke 0 untuk karakter berikutnya
- Simple
- Murah
- Overhead pada 2 atau 3 bit per karakter (~20%)
- Baik untuk data dengan jarak yang panjang (keyboard)

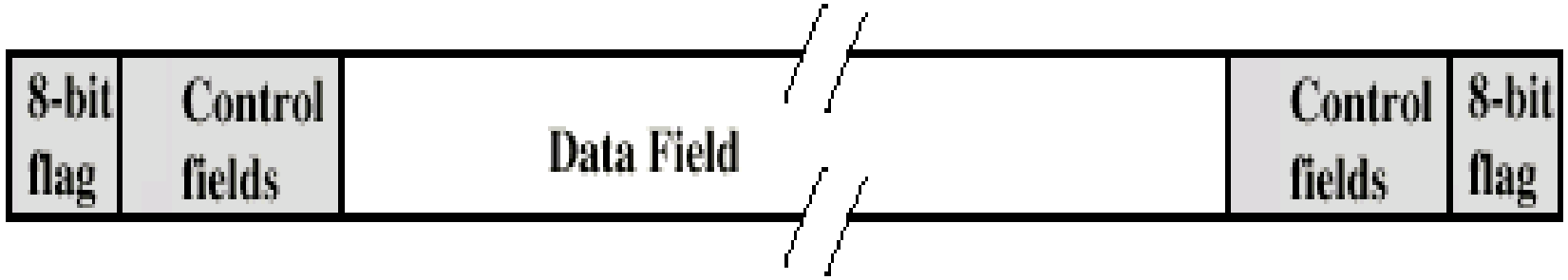
Sinkron-level bit

- Block pada transmisi data tanpa start atau stop bits
- Clock harus sama (sinkron)
- Dapat menggunakan jalur clock yang terpisah
  - Baik untuk jarak dekat
  - Perusakan subjek
- Meletakkan sinyal clock dalam data
  - Encoding Manchester
  - Menemukan kembali carrier (pada modulasi digital)

Sinkron-level block

- Membutuhkan petunjuk saat start dan end pada block
- Menggunakan preamble dan postamble
- Yaitu series pada karakter SYN (hex 16)
- Yaitu block pada 11111111 patterns ending dalam 11111110
- Lebih efisien (Overhead lebih kecil) daripada asinkron

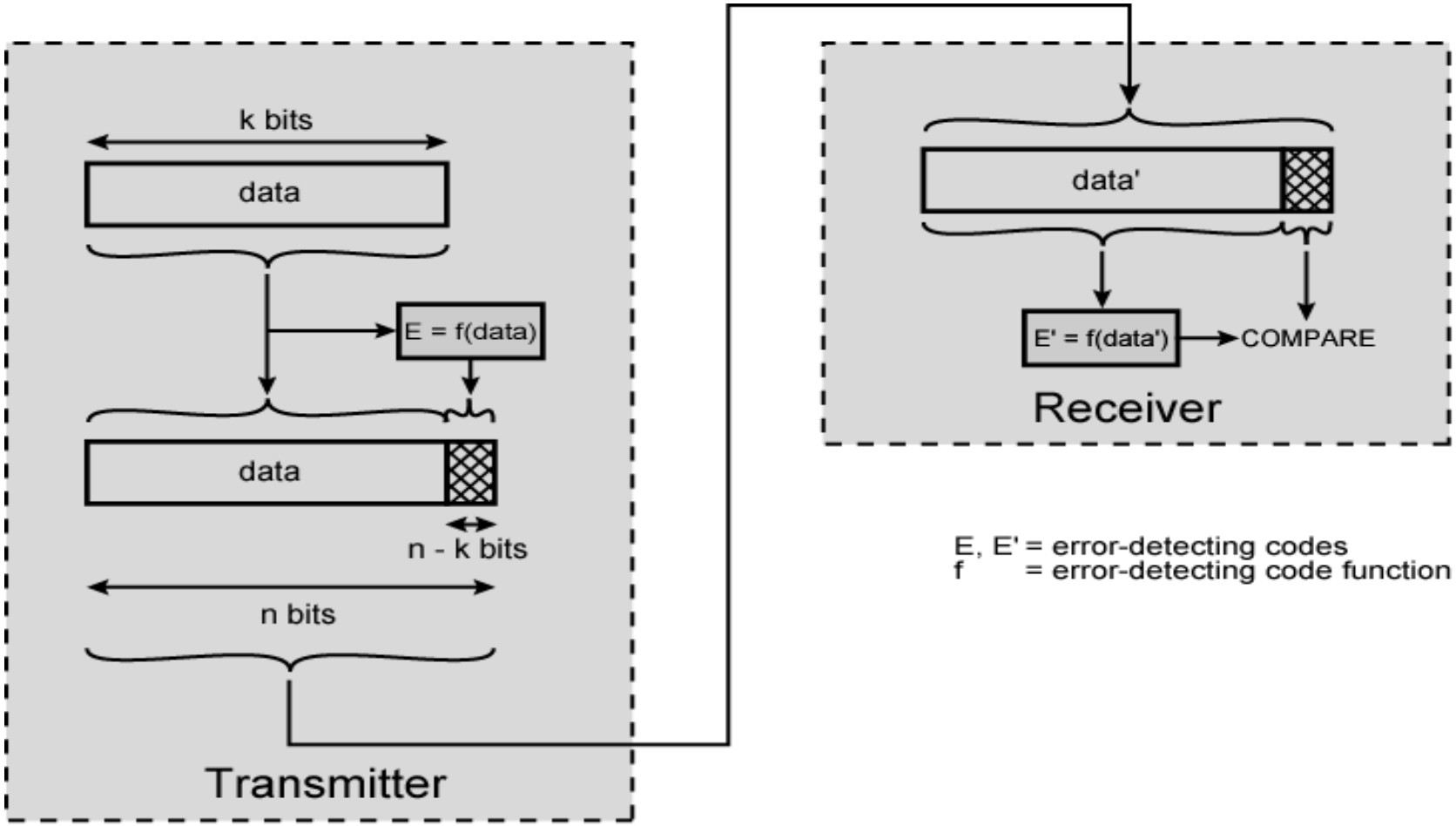
Sinkron (diagram)



Tipe-tipe error

- Error terjadi ketika ada perubahan diantara transmitter dan receiver
- Error single bit
  - Diantara satu bit
  - Bit yang berdekatan tidak efektif
  - White noise
- Burst errors
- Panjang *B*
- Impulse noise
- Memudar dalam wireless
- Efek lebih besar saat kecepatan data tinggi

Proses Pendeteksian Error



Pendeteksian Error

- Bit tambahan yang dibuat oleh transmitter untuk mendeteksi error code
- Parity
- Nilai dari Parity bit merupakan karakter even (even parity) atau odd (odd parity) dalam satu angka
- Even number dari bit error berarti tidak terdeteksi

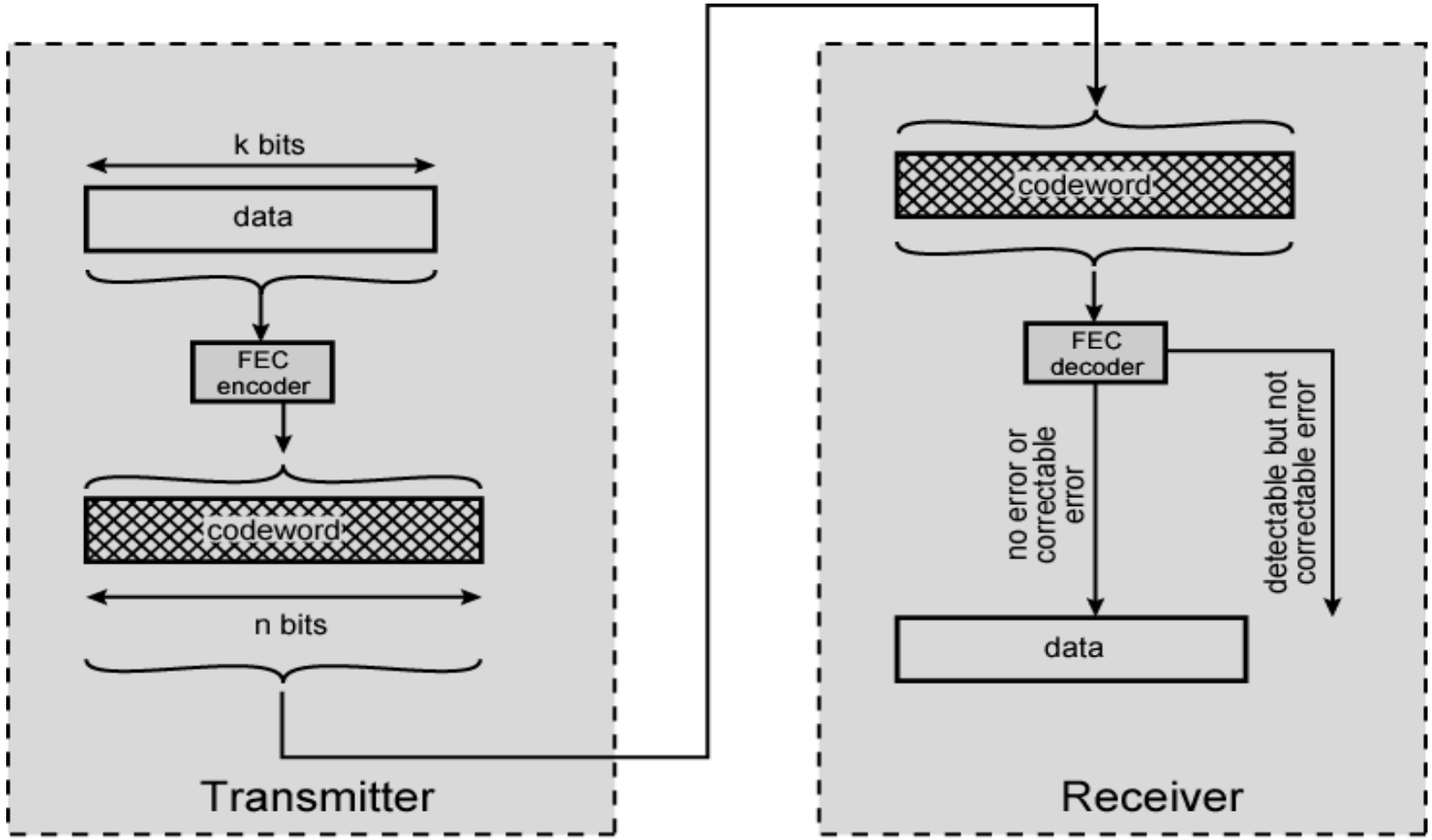
Cyclic Redundancy Check

- Untuk block pada transmitter k bit transmitter membangkitkan *n* bit sequence
- Transmit *k+n* bits yang tepat membagi menjadi beberapa angka
- Receiver membagi frame dengan angka
  - Jika tidak ada peringatan, diasumsikan tidak ada error
- Untuk materi, lihat Stallings bab 6

Koreksi Error

- Koreksi pada pendeteksian error memerlukan block data yang dikirimkan kembali (lihat bab 7)
- Tidak ada yang tepat untuk aplikasi wireless
  - Kecepartan bit error tinggi
    - Lebih banyak pengiriman ulang
- Waktu tunggu perambatan lebih lama dibandingkan pengiriman frame
- Diperlukan koreksi error untuk penerimaan bit dalam basic

Diagram Proses Koreksi Error



Proses Koreksi Error

- Tiap *k* bit block mapped untuk *n* bit block (*n*>*k*)
  - Codeword
  - Forward error correction (FEC) encoder
- Codeword dikirim
- Diterima bit string yang sama untuk pengiriman tetapi masih ada error
- Diterima codeword lalu dirubah ke FEC decoder
  - Jika ada error, dikeluarkan data block original
  - Beberapa error dapat dideteksi dan dikoreksi
  - Beberapa error dapat dideteksi tetapi tidak dapat dikoreksi
  - Beberapa error tidak dapat dideteksi
    - Hasil yang tidak dikoreksi dari FEC

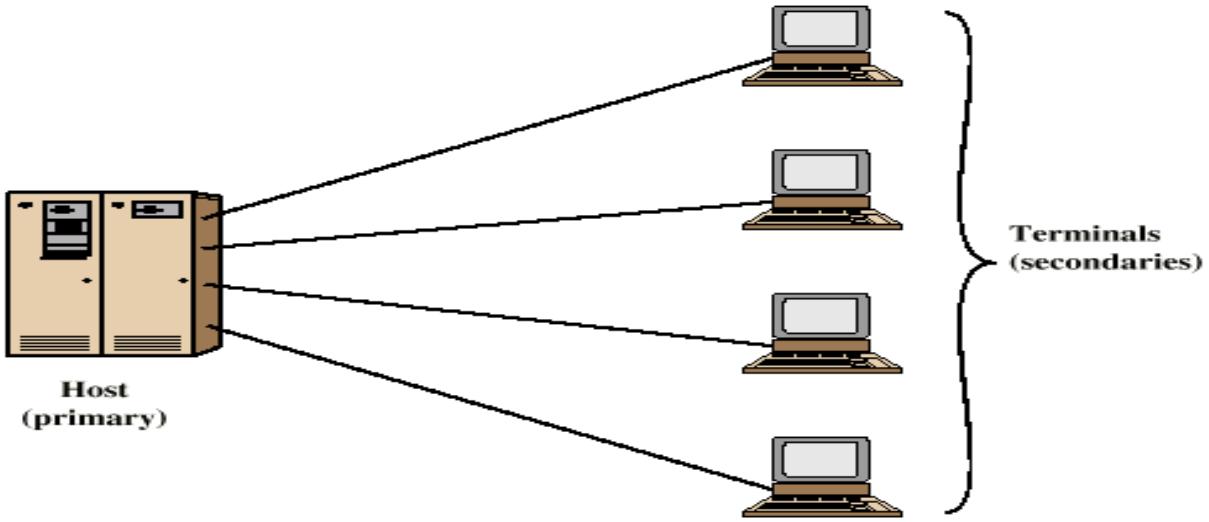
Bekerja pada Koreksi Error

- Membuat redundancy untuk pengiriman pesan
- Dapat menarik kesimpulan pada level kecepatan error
- E.g. koreksi code block error
  - Secara umum membuat ($n - k$) bits menjadi end pada block
    - *Meberikan* n bit block (codeword)
    - Semua original k bits termasuk dalam codeword
  - Beberapa pemetaan FEC k bit input kedalam n bit codeword seperti original k bits tidak terlihat
- Kembali untuk materilihat bab 6

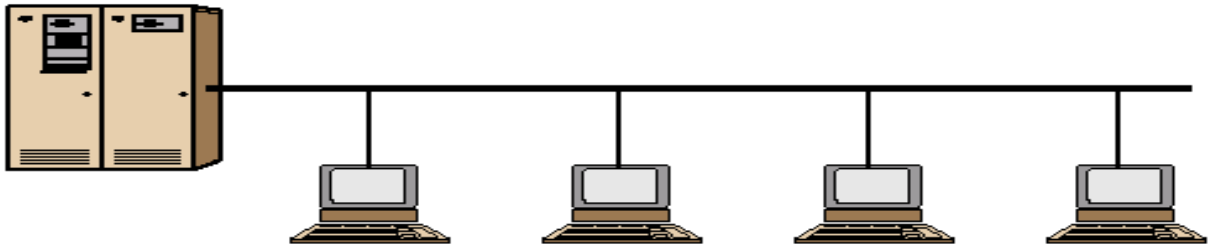
Konfigurasi Saluran

- Topology
  - Fisik menyusun stasiun dalam media
  - Point to point
  - Multi point
    - Komputer dan terminals, local area network
- Half duplex
  - Hanya satu stasiun yang mungkin dikirimkan dalam satu waktu
  - Membutuhkan satu data path
- Full duplex
  - Simultan antara dua stasiun saat pengiriman dan penerimaan
  - Membutuhkan dua data paths (atau echo canceling)

Konfigurasi Tradisional



(a) Point-to-point

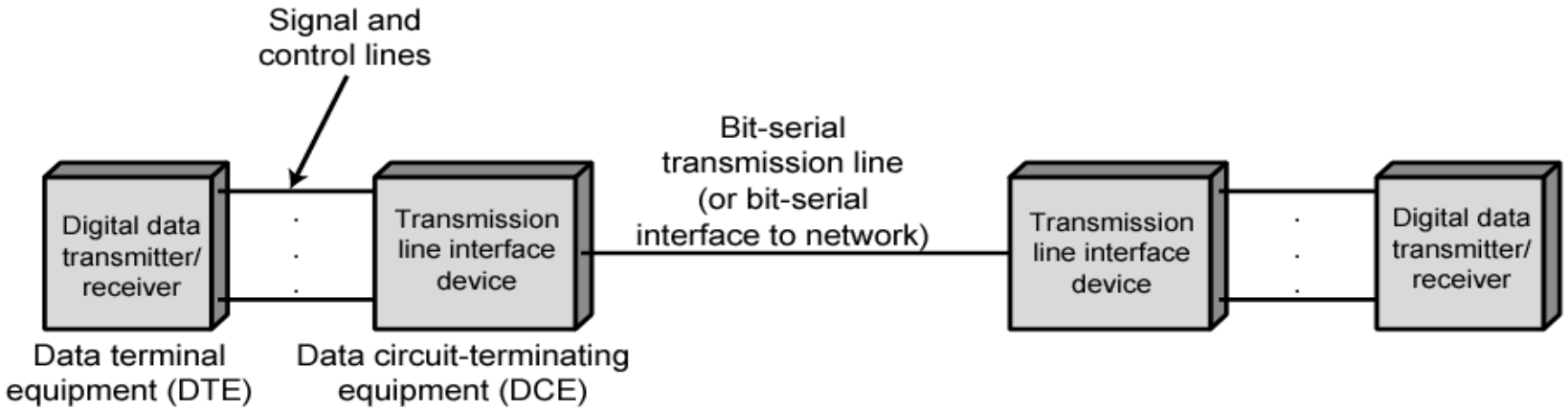


(b) Multipoint

Interfacing

- Peralatan pemrosesan data (atau perlengkapan terminal data, DTE) tidak selalu termasuk fasilitas pengiriman data
- Dibutuhkan interface yang disebut data circuit terminating equipment (DCE)
  - e.g. modem, NIC
- Pengiriman DCE bit dalam media
- Komunikasi data DCE kontrol info dengan DTE
  - Dilakukan pertukaran circuit
  - Dibutuhkan standar interface yang bersih

Interfacing Komunikasi Data



(a) Generic interface to transmission medium

(b) Typical configuration

Karakteristik Interface

- Mechanical
  - Connection plugs
- Electrical
  - Voltage, timing, encoding
- Fungsi
  - Data, control, timing, grounding
- Procedur
  - Sequence of events

V.24/EIA-232-F

- ITU-T v.24
- Hanya fungsi yang spesifik dan prosedur
  - Referensi standar lain untuk electrical dan mechanical
- EIA-232-F (USA)
  - RS-232
  - Mechanical ISO 2110
  - Electrical v.28
  - Functional v.24
  - Procedural v.24

Spesifikasi Mechanical

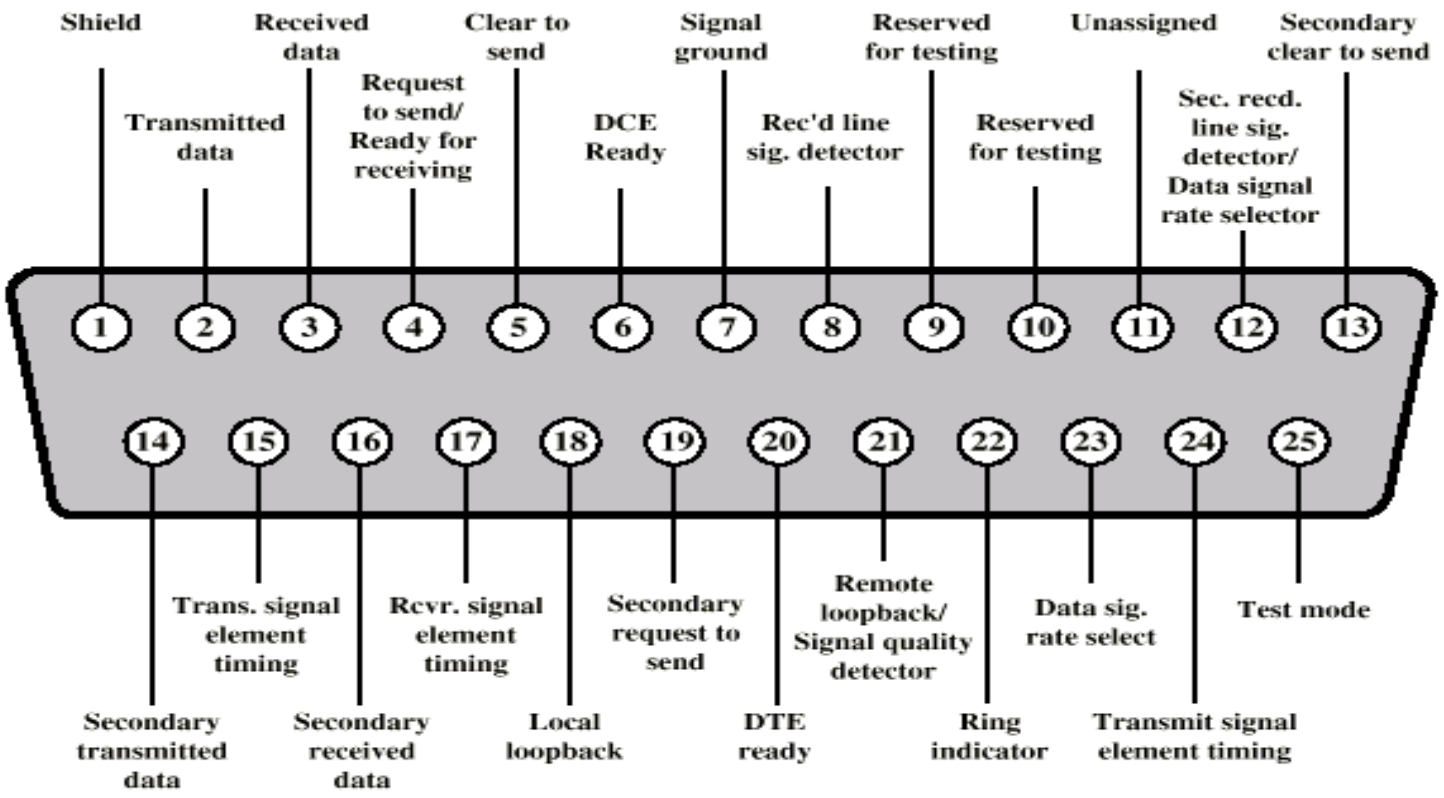


Figure 6.5 Pin Assignments for V.24/EIA-232 (DTE Connector Face)

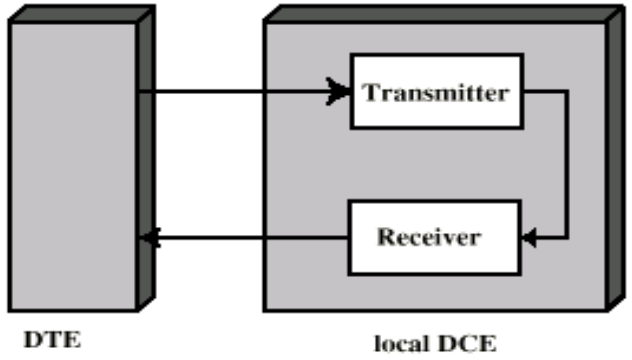
Spesifikasi Electrical

- Sinyal digital
- Hasil penerjemahan sebagai data atau control, bergantung dalam circuit
- Lebih dari -3v adalah binary 1, lebih dari +3v adalahbinary 0 (NRZ-L)
- Kecepatan Signal < 20kbps
- Jarak<15m
- Untuk control, lebih dari -3v adalah off, +3v adalah on

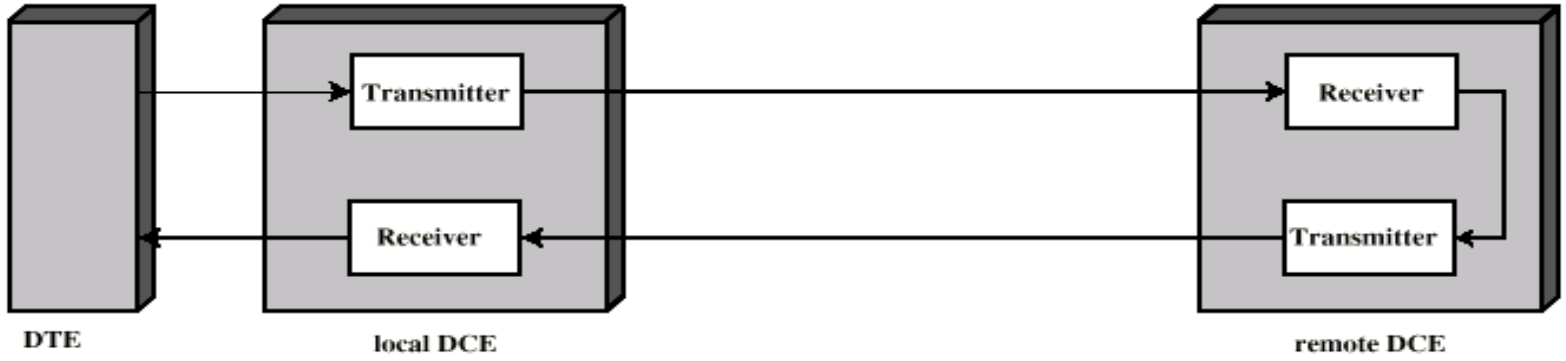
Spesifikasi Fungsi

- Kategori grup circuit
  - Data
  - Control
  - Timing
  - Ground
- Satu circuit dalam tiap arah
  - Full duplex
- Dua circuit data kedua
  - Mengijinkan halt atau flow control dalam operasi half duplex
- (Lihat tabel dalam Stallings bab 6)

Local dan Remote Loopback



(a) Local loopback Testing

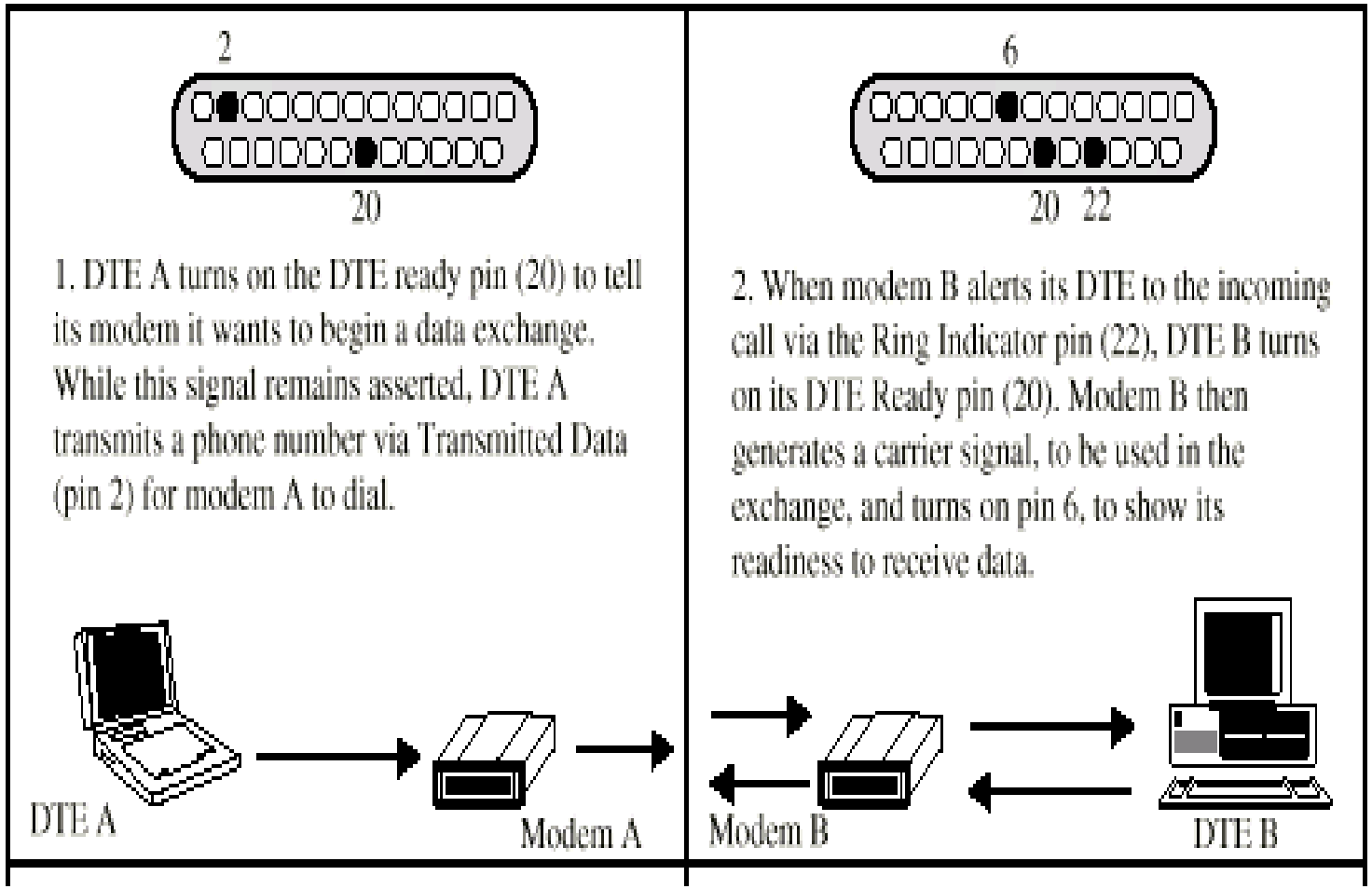


(b) Remote loopback Testing

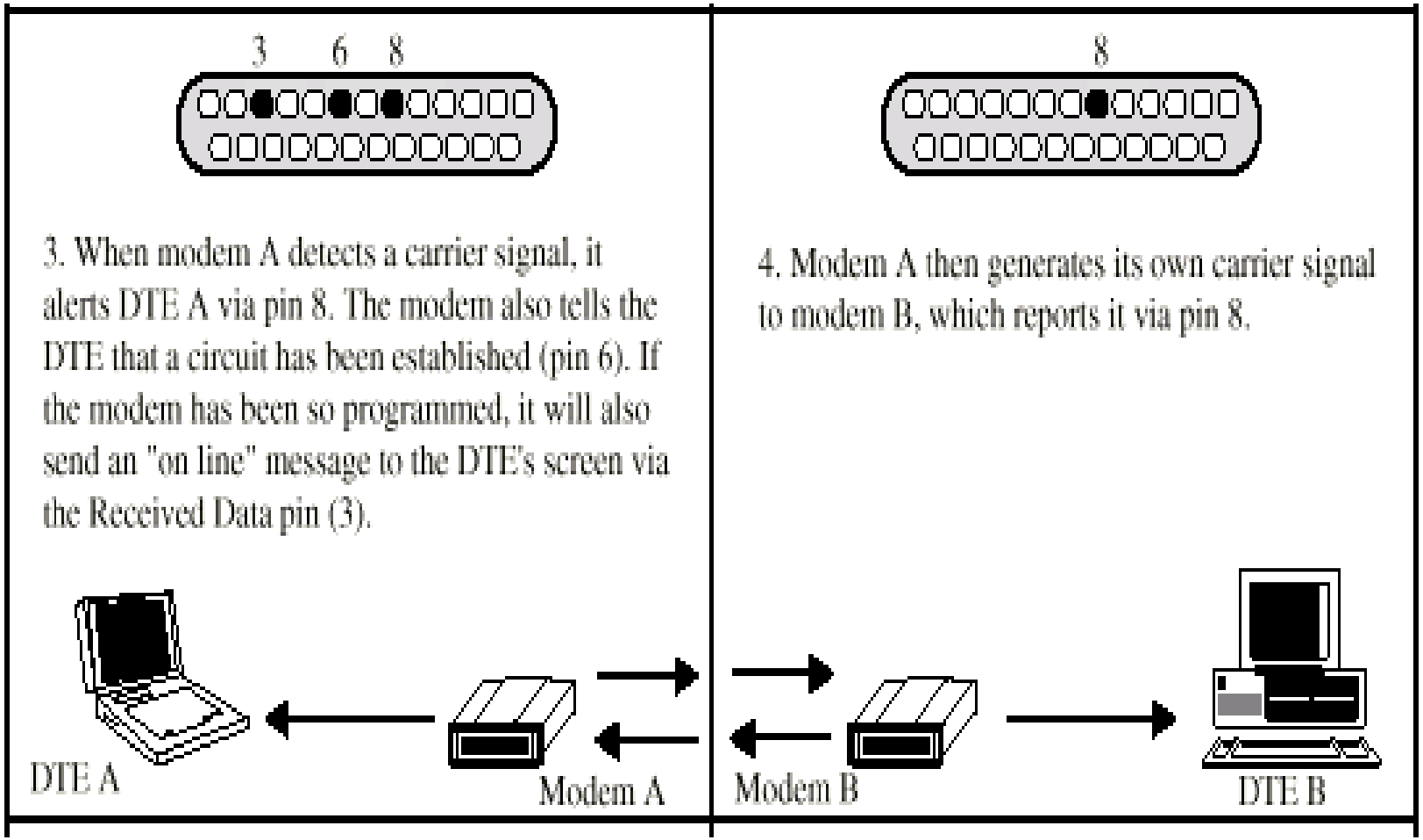
Spesifikasi Prosedur

- E.g. Asynchronous private line modem
- Ketika diputar menyala dan siap, modem (DCE) menyatakan DCE siap
- Ketika DTE siap mengirimkan data, menyatakan permintaan untuk dikirim
  - Mode penerimaan dihambat juga dalam half duplex
- Modem merespon ketika siap oleh pernyataan Clear to send
- DTE mengirimkan data
- Ketika data datang, local modem menyatakan Receive Line Signal Detector dan mengantarkan data

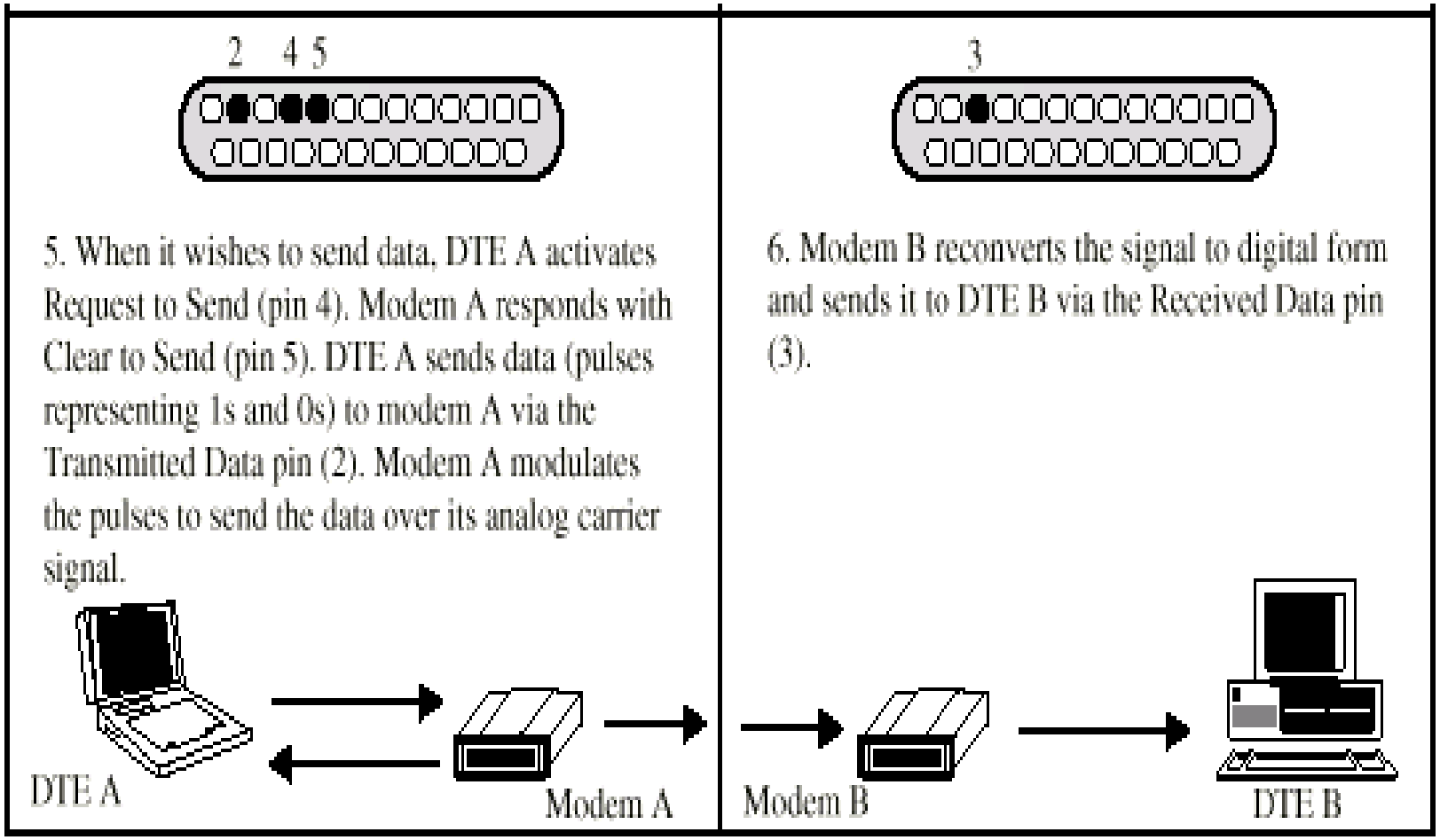
Dial Up Operation (1)



Dial Up Operation (2)



Dial Up Operation (3)



Null Modem

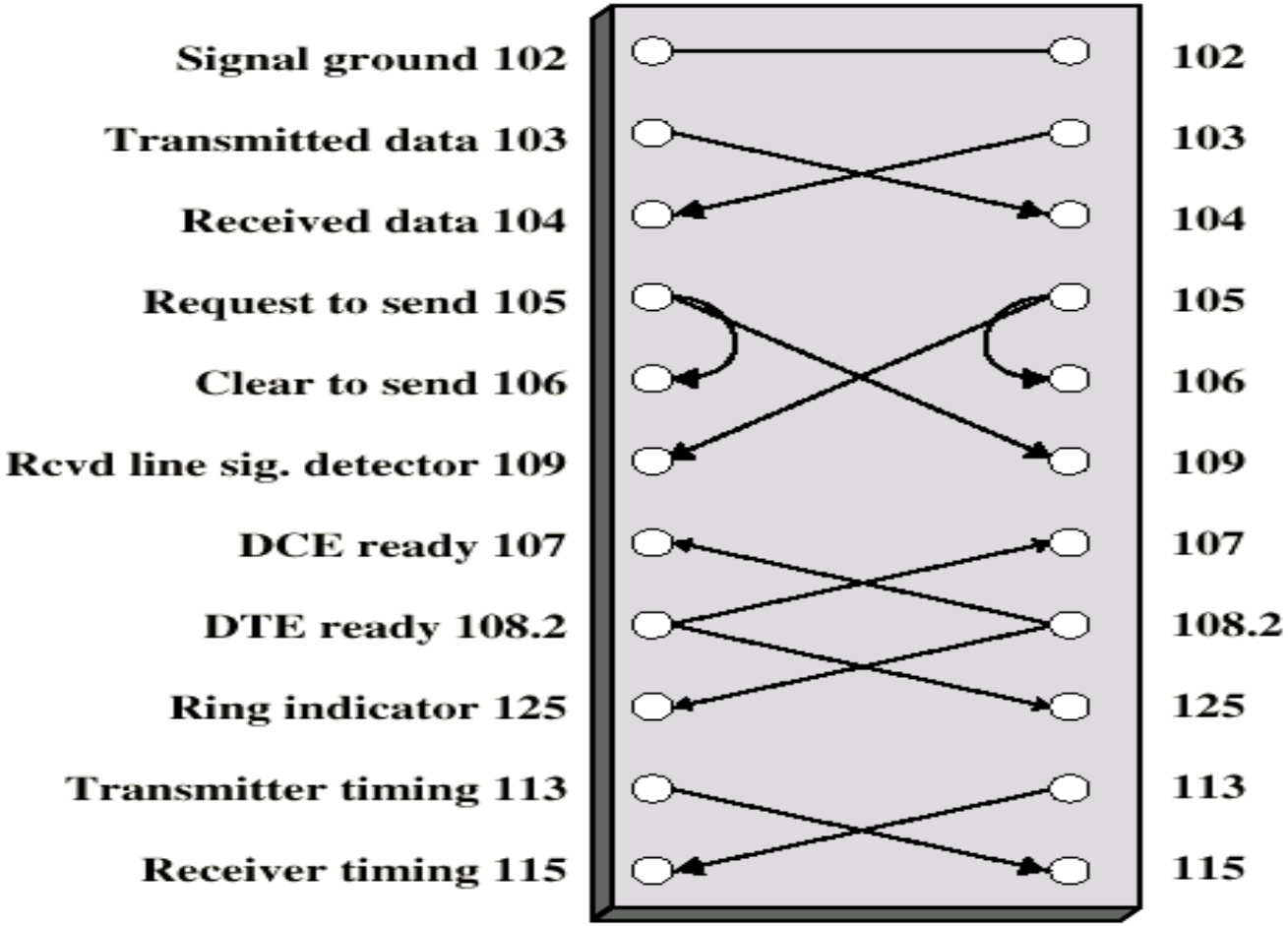
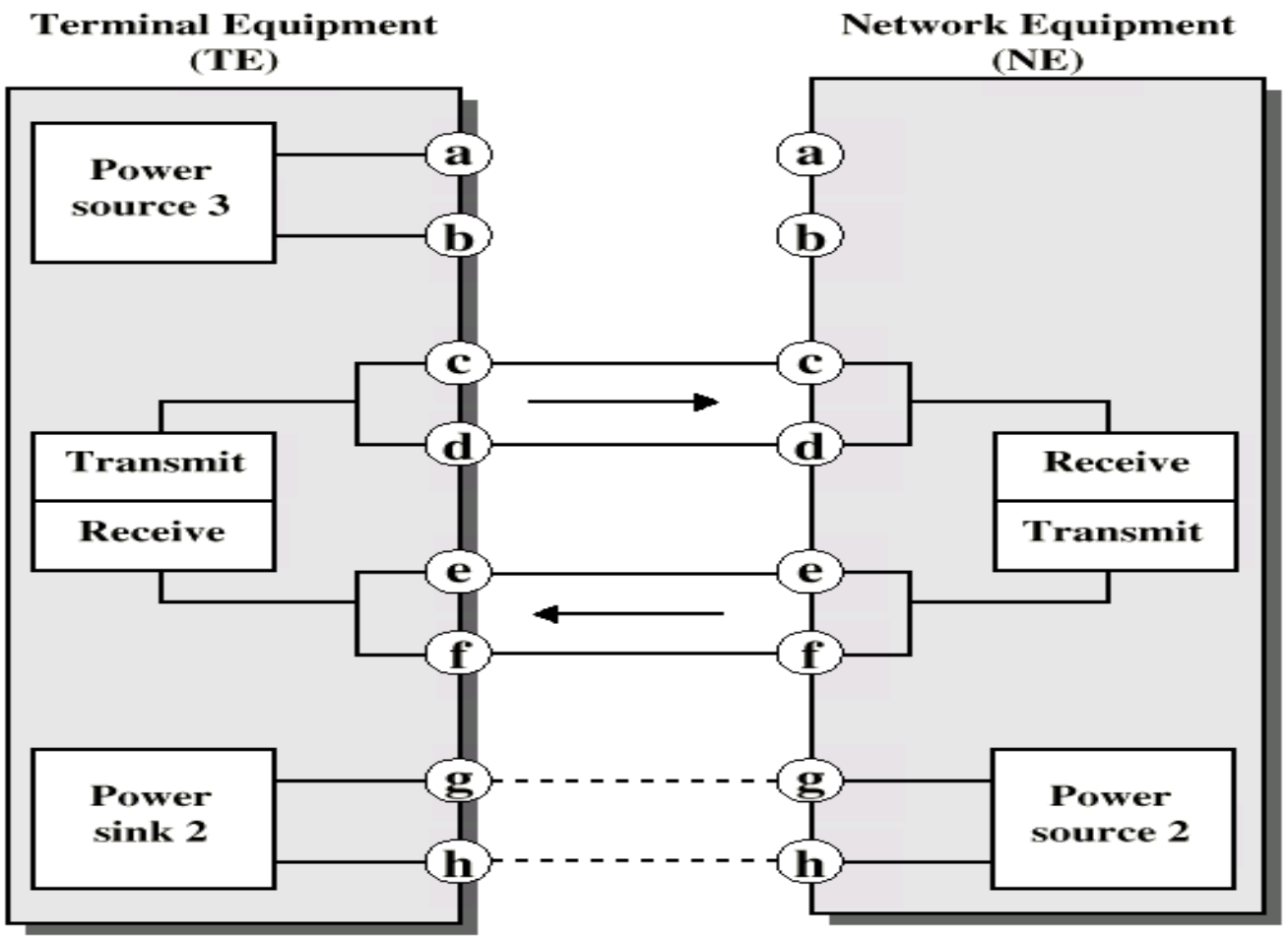

Signal ground 102
Transmitted data 103
Received data 104
Request to send 105
Clear to send 106
Rcvd line sig. detector 109
DCE ready 107
DTE ready 108.2
Ring indicator 125
Transmitter timing 113
Receiver timing 115
102
103
104
105
106
109
107
108.2
125
113
115

Diagram interface fisik ISDN



Interface fisik ISDN

- Konneksi antara perlengkapan terminal (c.f. DTE) dan perlengkapan jaringan terminating (c.f. DCE)
- ISO 8877
- Kables terminal dalam matching dengan 8 kontak
- Pengiriman/ penerimaanmembawa kedua data dan kontrol

Spesifikasi Electrical ISDN

- Balanced transmission
  - Carried dalam dua lines, e.g. twisted pair
  - Signals seperti currents down one conductor dan yang lain naik
  - Signaling yang berbeda
  - Mengandalkan hasil dalam direction pada tegangan
  - Banyak toleransi noise dan generates less
  - (tidak balanced, e.g. RS-232 digunakan jalur single signal dan ground)
  - Mengandalkan data encoding dalam kecepatan data
  - Kecepatan dasar 192kbps menggunakan pseudoternary
  - Kecepatan primer menggunakan alternative mark inversion (AMI) and B8ZS or HDB3

Foreground Reading

- Stallings bab 6
- Web pages from ITU-T on v. specification
- Web pages on ISDN

Data Link Control

Transmisi Data
Pengkodean Data, Multiplexer
Teknik Komunikasi Data Digital
Data Link Control
~~Multiplexing~~
Switching
Medium Access Sublayer
Network Layer

Outlines

Jalur Konfigurasi (Line Configuration)

Flow Control

Pengendalian Kesalahan (Error Control)

Data Link Protocol

Data Link Services

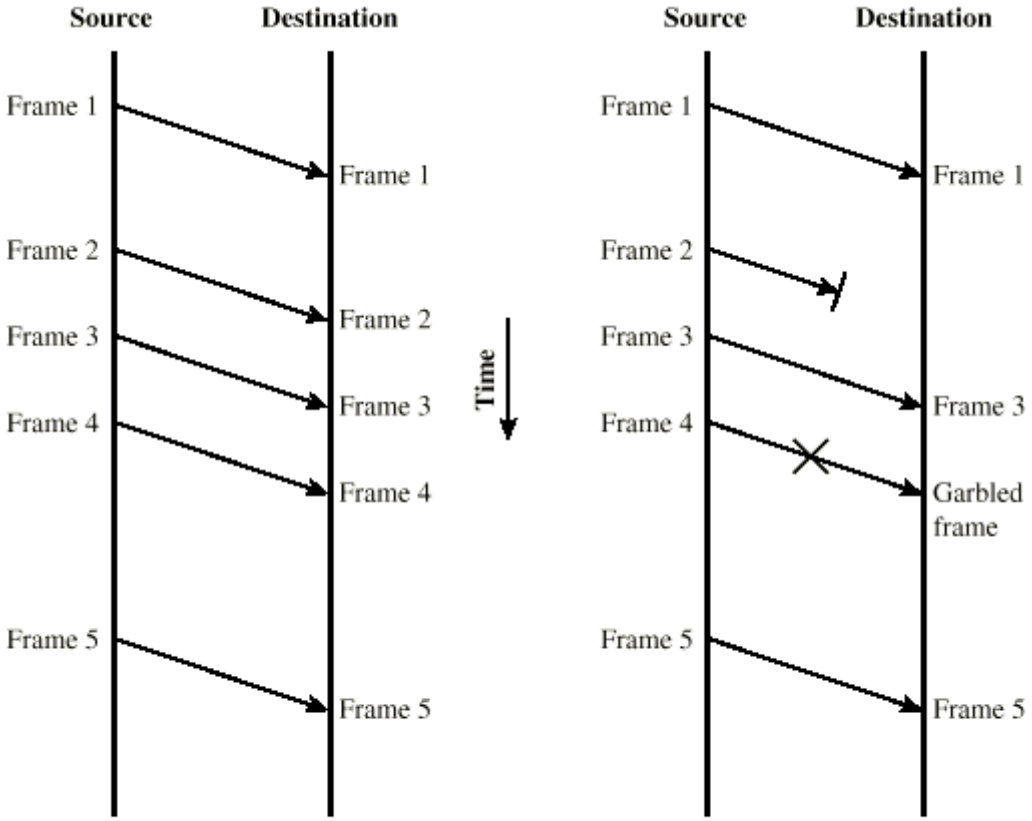
- Connection-oriented services: memberikan pengiriman paket terurut bebas error
  - setting-up koneksi: setting up variables dan alokasi buffer
  - transfer paket: paket ‘dikemas’ dlm frame data link
  - penutupan koneksi

- Connectionless service
  - acknowledged service
  - unacknowledged service

Kontrol Aliran

- Menjamin pengiriman tidak membanjiri penerima
  - Mencegah buffer overflow (kepenuhan)
- Waktu Transmisi
  - Waktu diambil untuk mengeluarkan semua bit ke dalam media transmisi
- Waktu Propagasi
  - Waktu sebuah bit menyelesaikan perjalanan di jalurnya

Model Frame Transmisi



(a) Error-free transmission

(b) Transmission with losses and errors

Stop dan Wait

- Source mengirimkan frame
- Destination menerima frame dan mengirim kembali dengan acknowledgement
- Source menunggu (wait) ACK sebelum mengirimkan frame berikutnya
- Destination bisa menghentikan (stop) aliran dengan tidak mengirimkan ACK
- Hal ini bisa bekerja dengan baik untuk beberapa frame yang besar

Fragmentasi

- Block data yang besar bisa dipisah kedalam frame-frame kecil
  - Terbatasnya ukuran buffer
  - Error bisa dideteksi lebih dini (ketika seluruh frame diterima)
  - Ketika ada error, perlu mentransmisikan kembali frame-frame kecil
  - Mencegah satu stasiun menggunakan media untuk jangka waktu yang lama
- Stop dan wait menjadi inadequate

Stop and Wait Link Utilization

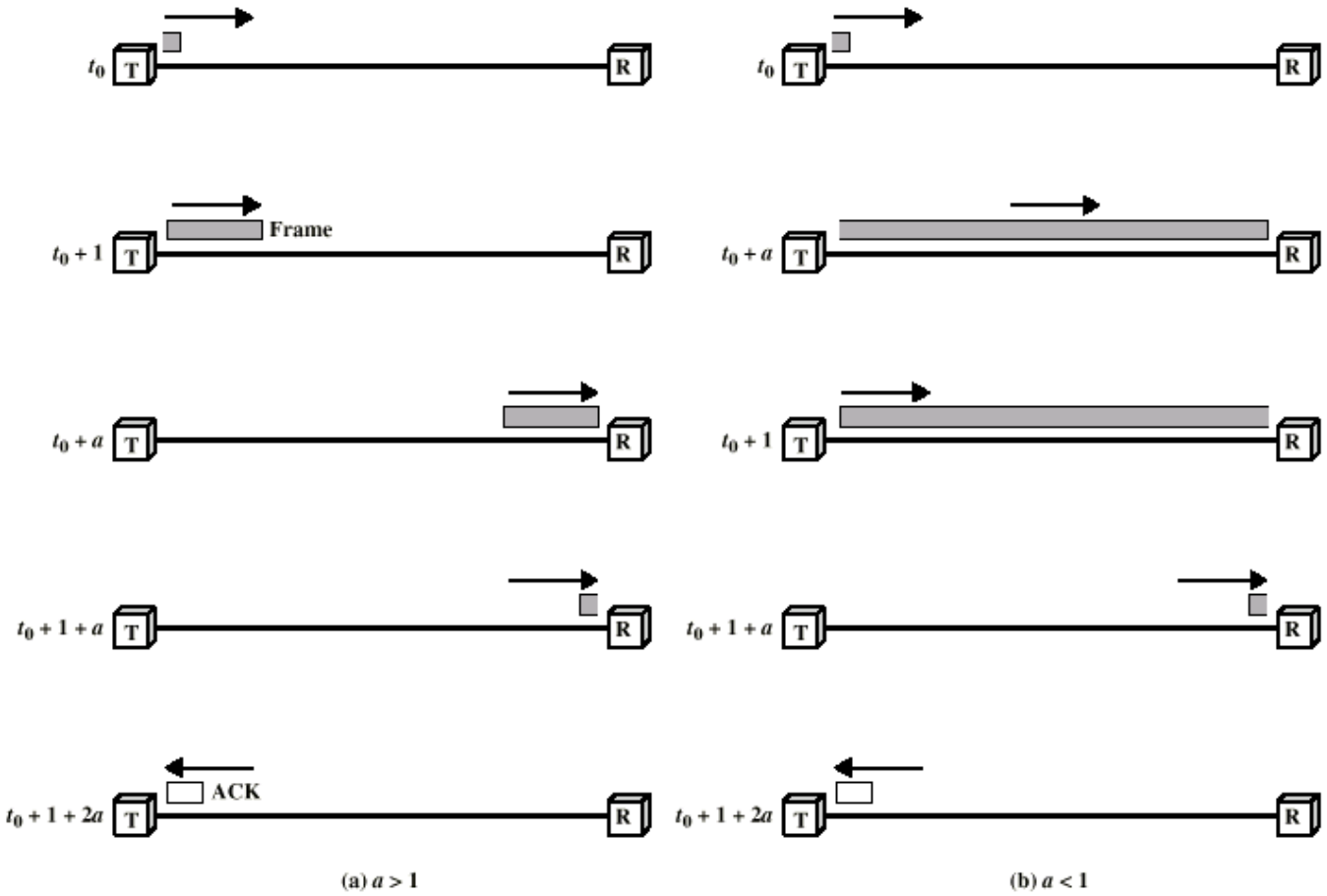
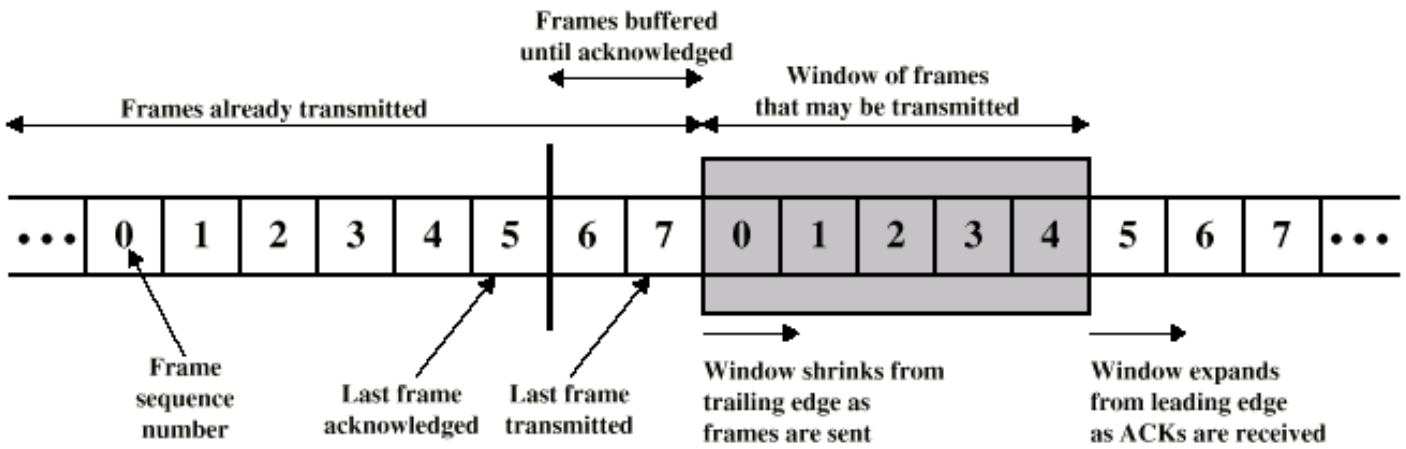


Figure 7.2 Stop-and-Wait Link Utilization (transmission time = 1; propagation time = a)

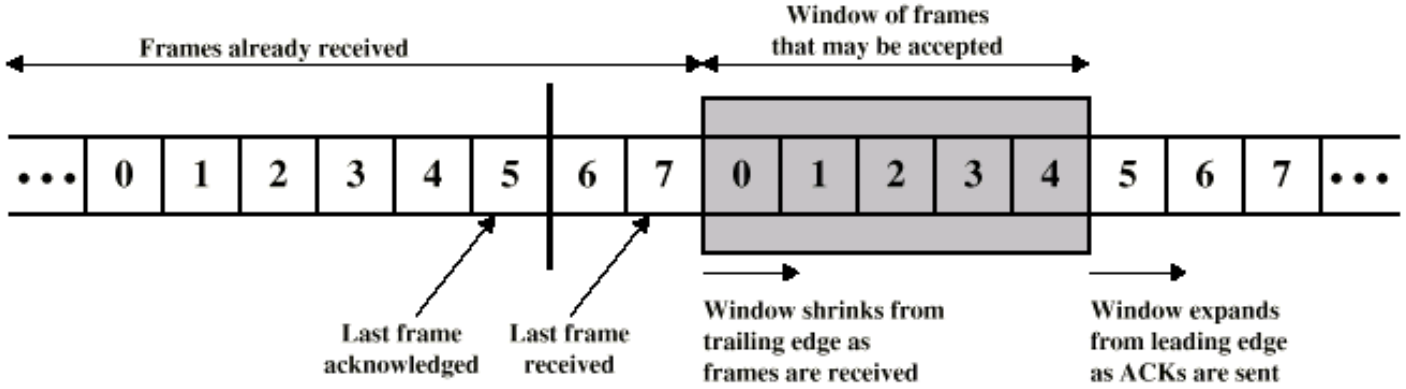
Sliding Windows Flow Control

- Banyak frame bisa dalam kondisi transit
- Receiver mempunyai lebar buffer W
- Transmitter dapat mengirimkan sampai W frame tanpa ACK
- Setiap frame diberi nomor
- ACK mencakup nomor frame berikutnya yang diharapkan
- Deretan nomor dikaitkan dengan ukuran field (k)
  - Frame-frame diberi nomor modulo 2^k

Diagram Sliding Window

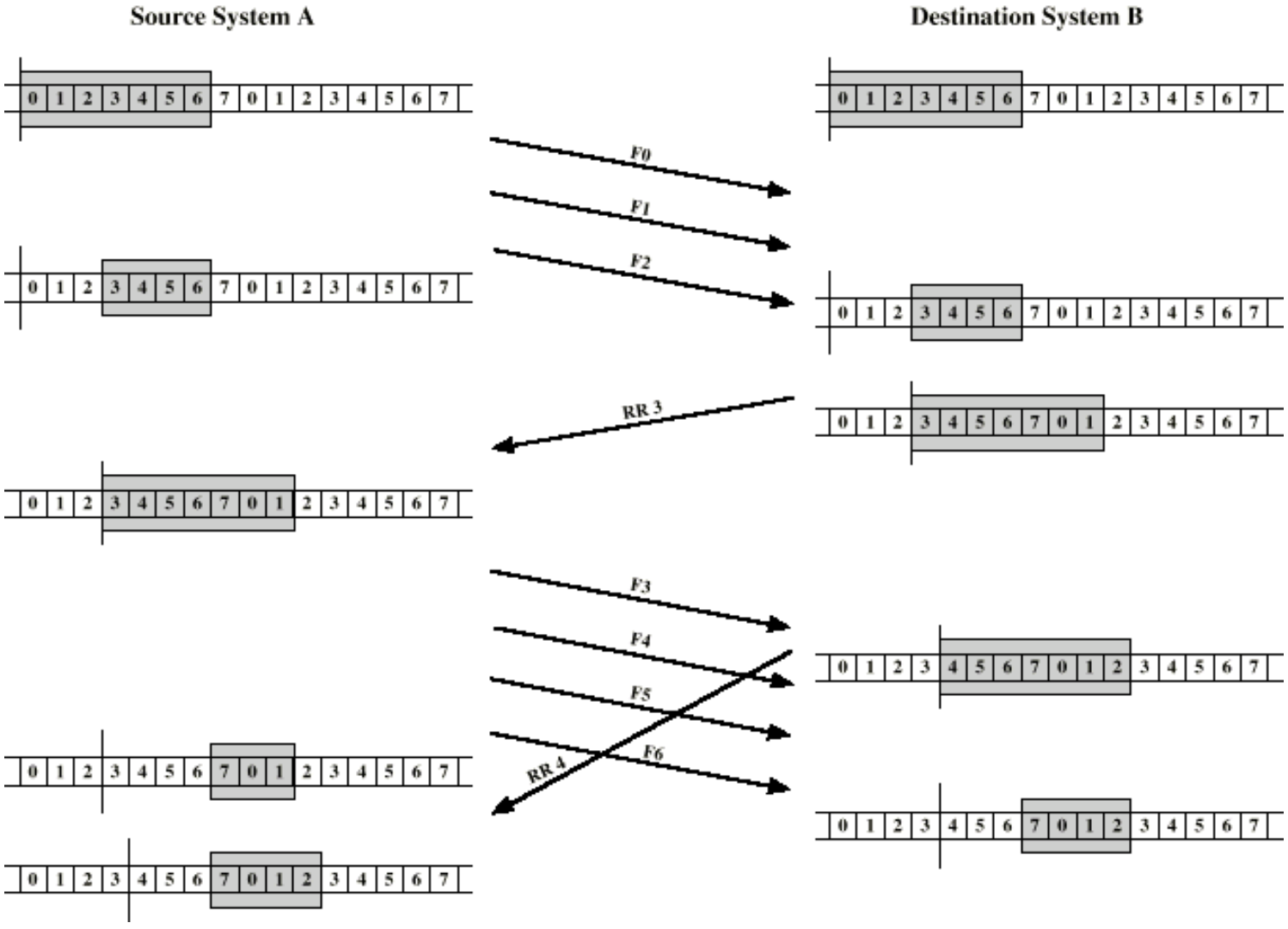


(a) Sender's perspective



(b) Receiver's perspective

Contoh Sliding Window



Perbaikan Sliding Window

- Receiver dapat menerima (acknowledge) frame tanpa persetujuan transmisi berikutnya (Receive Not Ready)
- Harus mengirimkan sebuah “normal acknowledge” untuk memperbaiki pengiriman (resume)
- Jika duplex, menggunakan “piggybacking”
  - Jika tidak ada data untuk dikirmkan, menggunakan frame acknowledgement
  - Jika ada data tetapi tidak ada acknowledgement untuk mengirim, mengirim lagi nomor acknowledgement terakhir, atau mengambil ACK valid flag (TCP)

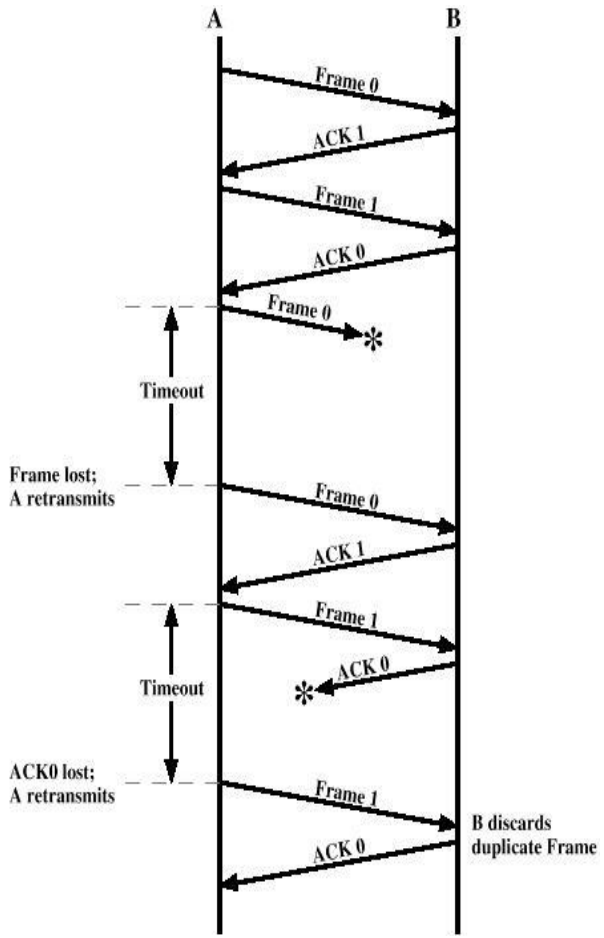
Automatic Repeat Request (ARQ)

2. Automatic Repeat Request (ARQ)

- Terdapat 3 versi dari ARQ, yaitu:
  - Stop and wait ARQ
  - Go Back N ARQ
  - Selective Reject ARQ

1. Stop and Wait ARQ

- Stasiun sumber mentransmisi suatu frame tunggal dan kemudian harus menunggu suatu acknowledgment (ACK) dalam periode tertentu. Tidak ada data lain dapat dikirim sampai balasan dari stasiun tujuan tiba pada stasiun sumber. Bila tidak ada balasan maka frame ditransmisi ulang. Bila error dideteksi oleh tujuan, maka frame tersebut dibuang dan mengirim suatu Negative Acknowledgment (NAK), yang menyebabkan sumber mentransmisi ulang frame yang rusak tersebut.



- Bila sinyal acknowledgment rusak pada waktu transmisi, kemudian sumber akan habis waktu dan mentransmisi ulang frame tersebut. Untuk mencegah hal ini, maka frame diberi label 0 atau 1 dan positive acknowledgment dengan bentuk ACK0 atau ACK1 : ACK0 mengakui menerima frame 1 dan mengindikasi bahwa receiver siap untuk frame 0. Sedangkan ACK1 mengakui menerima frame 0 dan mengindikasi bahwa receiver siap untuk frame 1.

Stop dan Wait - Pros and Cons

- Mudah
- Tidak efisien

2. Go Back N (1)

- Berdasarkan pada sliding window
- Jika tidak ada error, ACK seperti biasanya dengan frame berikutnya diharapkan
- Menggunakan window untuk mengontrol jumlah frame-frame yang tidak diketahui
- Jika error, kirim balik dengan rejection
  - Buang frame tsb dan semua frame yang akan tiba sampai frame yang salah diterima kembali dengan benar
  - Transmitter harus go back dan mengirim ulang frame tsb dan semua frame yang berdekatan berikutnya

Go Back N - Frame yang rusak

- Receiver mendeteksi error didalam frame *i*
- Receiver mengirimkan rejection-*i*
- Transmitter mengambil rejection-*i*
- Transmitter mengirim ulang frame *i* dan semua deretannya

Go Back N - Frame hilang (1)

- Frame *i* hilang
- Transmitter mengirimkan *i+1*
- Receiver mengambil frame *i+1* keluar dari deretan
- Receiver mengirimkan reject *i*
- Transmitter go back ke frame *i* dan mengirim ulang

Go Back N - Frame hilang (2)

- Frame *i* hilang dan tidak ada frame tambahan yang telah dikirim
- Receiver tidak mengambil apa-apa dan tidak mengirimkan acknowledgement maupun rejection
- Transmitter menjalani time out dan mengirimkan frame acknowledgement dengan P bit diset ke 1
- Receiver menginterpretasikan ini sebagai command dimana mengetahui nomor frame berikutnya yang diharapkan (frame *i*)
- Transmitter kemudian mengirim ulang frame *i*

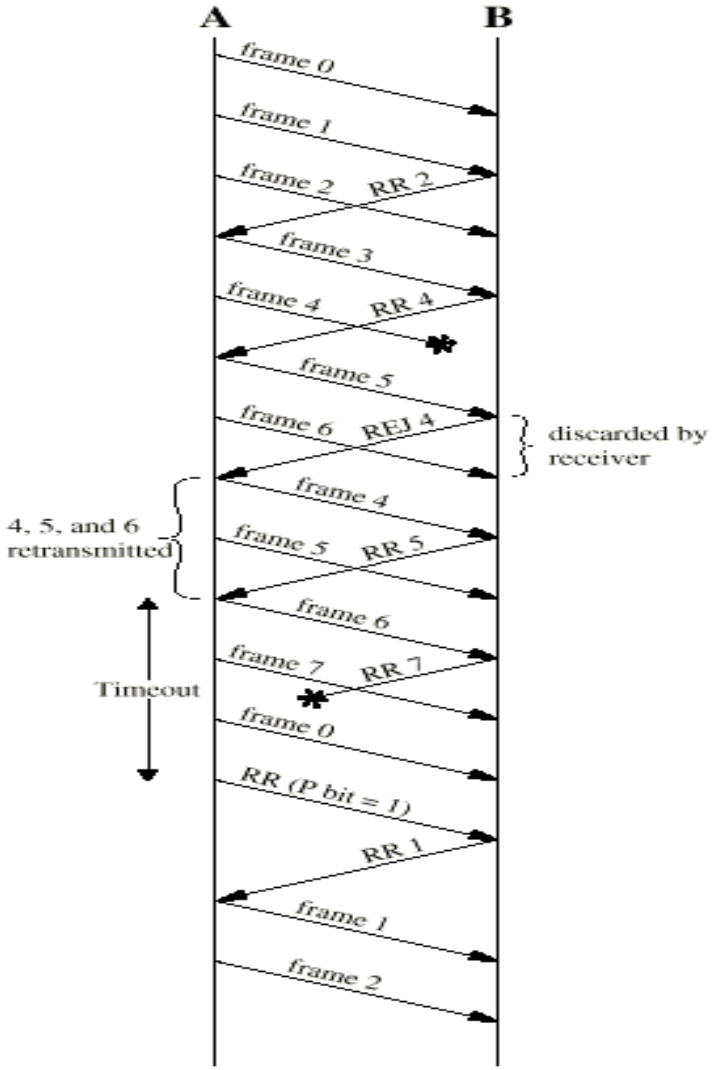
Go Back N - Acknowledgement yang rusak

- Receiver mengambil frame *i* dan mengirimkan acknowledgement (*i+1*) dimana ini hilang
- Acknowledgement terakumulasi, sehingga acknowledgement berikutnya (*i+n*) bisa tiba sebelum transmitter terkena time out pada frame *i*
- Jika transmitter terkena time out, akan mengirimkan acknowledgement dengan P bit diset seperti sebelumnya
- Hal ini dapat diulang dalam sejumlah waktu sebelum suatu prosedur reset diinisialisasi

Go Back N - Rejection Rusak

- Seperti Frame hilang (2)

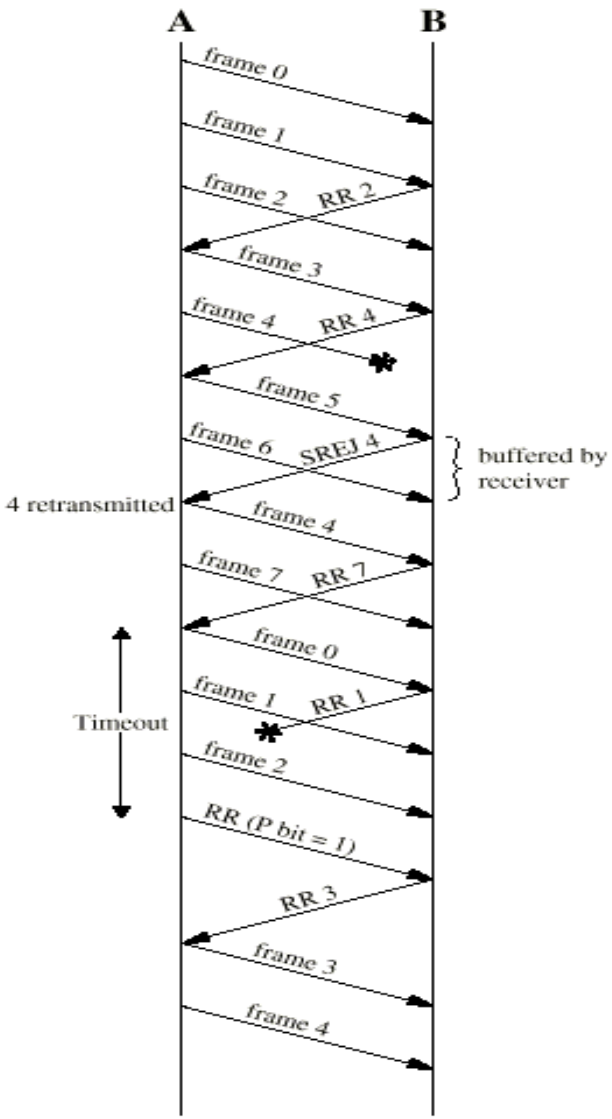
Go Back N - Diagram



3. Selective Reject (1)

- Disebut juga “selective retransmission”
- Hanya frame-frame yang ditolak yang dikirim ulang
- Frame-frame bagian deretannya diterima oleh receiver dan disimpan di buffer
- Meminimalkan retransmission
- Receiver harus mengelola buffer yang cukup besar
- Login yang lebih kompleks didalam transmitter

Selective Reject - Diagram



Sejarah DLL Protocols

- SDLC - Synchronous Data Link Control (IBM)
- HDLC - High-level Data Link Control (ISO & CCITT)
- ADCCP - Advanced Data Communications Control Protocol (ANSI)
- LLC - Logical Link Control (IEEE 802.2)
- ISO 33009, ISO 4335 Data Link Control

High Level Data Link Control

- HDLC
- ISO 33009, ISO 4335

Jenis Stasiun HDLC

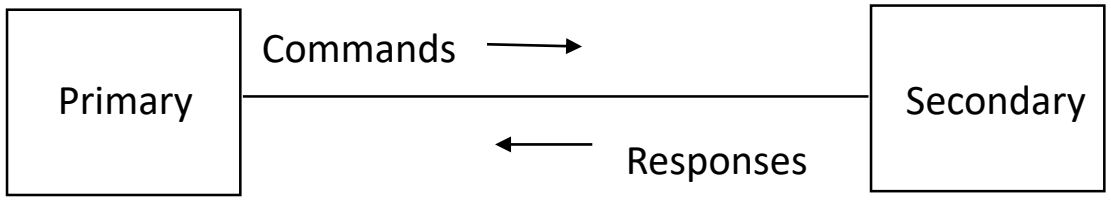
- Primary station
  - Mengendalikan operasi hubungan(link)
  - Frame-frame yang dibicarakan disebut “command”
  - Mengelola logical link terpisah terhadap setiap secondary station
- Secondary station
  - Dibawah kendali primary station
  - Frame-frame yang dibicarakan disebut “response”
- Combined station
  - Bisa mengenai command dan response

Konfigurasi Hubungan HDLC

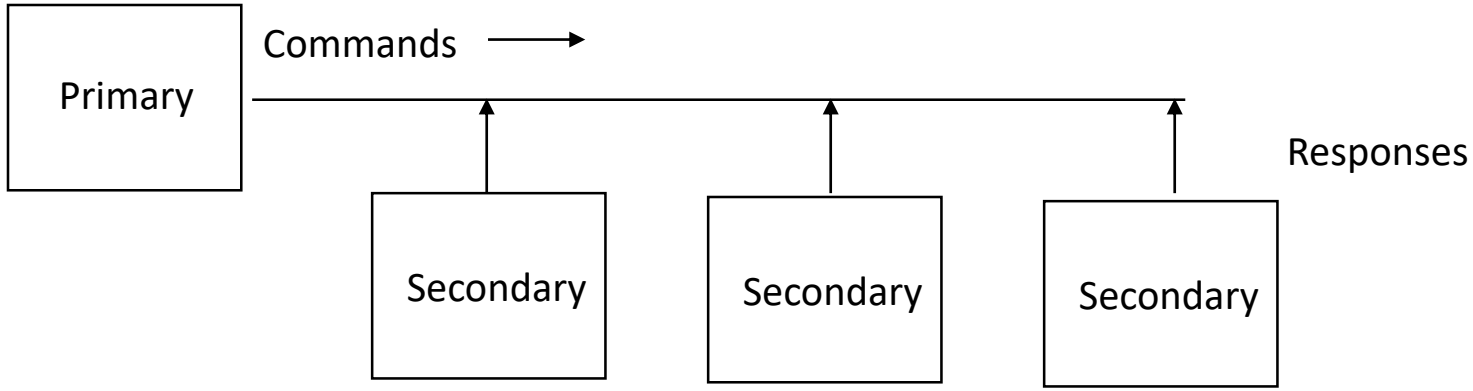
- Unbalanced
  - Satu stasiun primary dan satu atau lebih secondary
  - Mampu mendukung full duplex dan half duplex
- Balanced
  - Dua combined stations
  - Mendukung full duplex dan half duplex

Konfigurasi HDLC

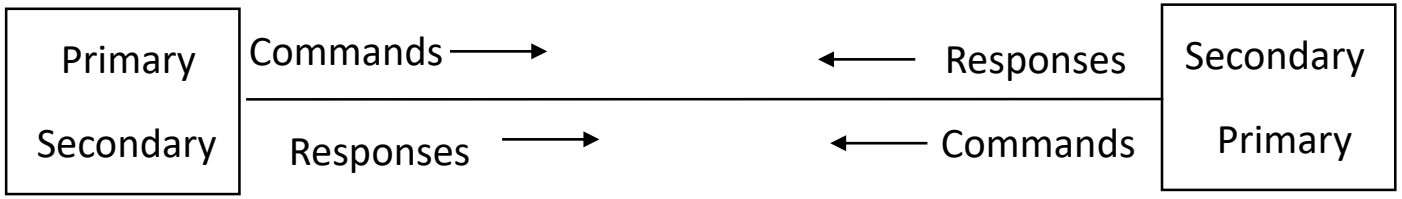
Unbalanced Point-to-point link



Unbalanced Multipoint link



Balanced Point-to-point link between Combined Stations



Mode Transfer HDLC (1)

- Normal Response Mode (NRM)
  - Konfigurasi Unbalanced
  - Primary mengawali transfer ke secondary
  - Secondary hanya bisa mengirimkan data sebagai response kepada command dari primary
  - Digunakan pada jalur multi-drop
  - Host Komputer sebagai primary
  - Terminal sebagai secondary

Mode Transfer HDLC (2)

- Asynchronous Balanced Mode (ABM)
  - Konfigurasi Balanced
  - Kedua station bisa mengawali pengiriman tanpa izin agar diterima
  - Paling banyak digunakan
  - Tidak ada “polling overhead”

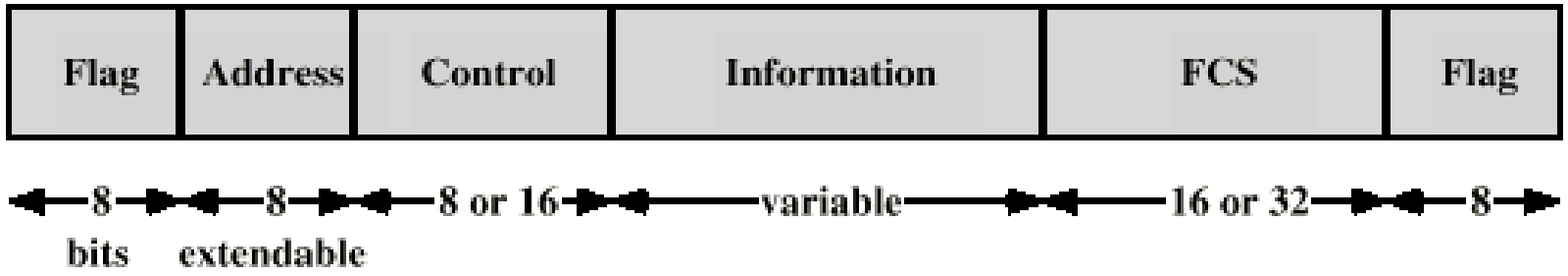
Mode Transfer HDLC (3)

- Asynchronous Response Mode (ARM)
  - Konfigurasi Unbalanced
  - Secondary bisa mengawali pengiriman tanpa izin dari primary
  - Primary bertanggung jawab terhadap jalur
  - Jarang digunakan

Struktur Frame

- Transmisi Sinkron
- Semua transmisi dalam frame
- Format frame tunggal untuk semua pertukaran data dan control

Diagram Struktur Frame



Flag Fields

- Menandai batas frame pada kedua ujung
- 01111110
- Bisa close satu frame dan open yang lain
- Receiver mencari deretan flag untuk sinkronisasi
- Bit stuffing digunakan untuk mencegah kebingungan terhadap data yang mengandung 01111110
  - 0 disisipkan setelah setiap deretan lima buah bit 1
  - Jika receiver mendeteksi lima buah bit 1 maka akan mengecek bit berikutnya
  - Jika 0, maka dihapus
  - Jika 1 dan bit ketujuh adalah 0, diterima sebagai flag
  - Jika bit keenam dan ketujuh adalah 1, pengirim mengindikasikan abort (gagal)

Bit Stuffing

- Contoh dengan error yang mungkin

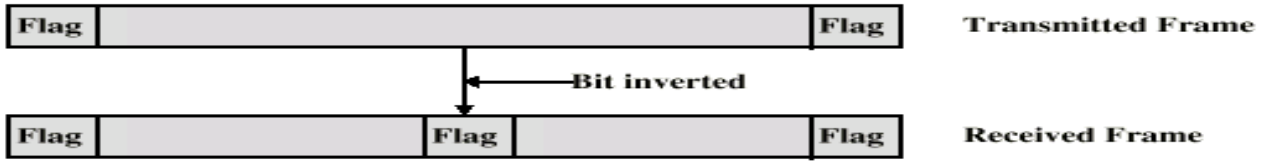
Original Pattern:

11111111111101111111011111110

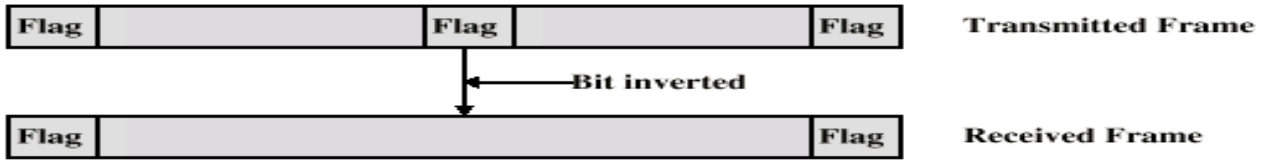
After bit-stuffing

11111011111101101111101011111010

(a) Example



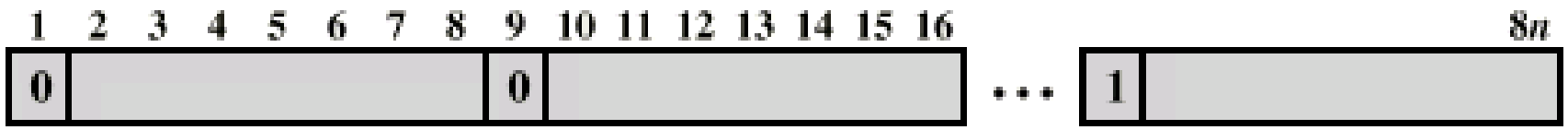
(b) An inverted bit splits a frame in two



(c) An inverted bit merges two frames

Address Field

- Memberi Identifikasi kepada secondary station yang telah atau akan menerima frame
- Biasanya panjangnya 8 bit
- Bisa lebih panjang lagi sampai kelipatan 7 bit
  - LSB setiap octet mengindikasikan bahwa ini merupakan octet terakhir (1) atau bukan (0)
- Semua bit satu (11111111) di-broadcast

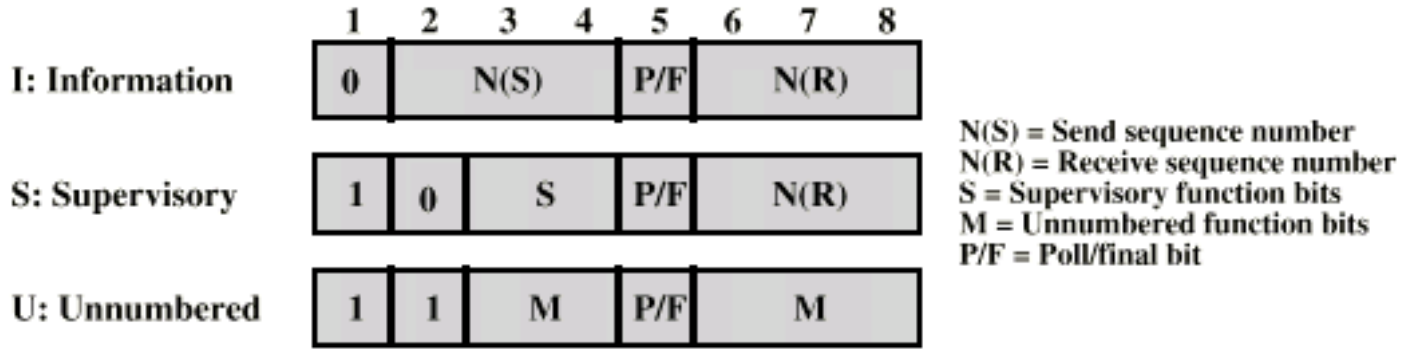


(b) Extended Address Field

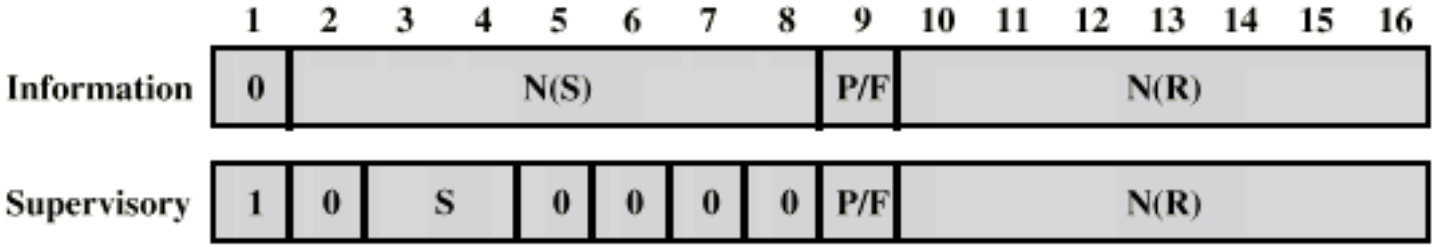
Control Field

- Berbeda untuk jenis frame yang beda
  - Information - data yang akan ditransmisikan ke user (next layer up)
    - Flow dan error control piggybacked pada frame information
  - Supervisory - ARQ ketika piggyback tidak digunakan
  - Unnumbered - Link control tambahan
- Satu atau dua bit pertama dari control field mengidentifikasikan jenis frame
- Bit-bit sisanya dijelaskan nanti saja

Diagram Control Field



(c) 8-bit control field format



(d) 16-bit control field format

Bit Poll/Final

- Digunakan bergantung pada context
- Command frame
  - P bit
  - 1 untuk solicit (poll) response dari peer
- Response frame
  - F bit
  - 1 mengindikasikan response untuk soliciting command

Information Field

- Hanya didalam information dan beberapa frame-frame tidak bernomor
- Harus mengandung nomor integral dari octet
- Panjang variabel

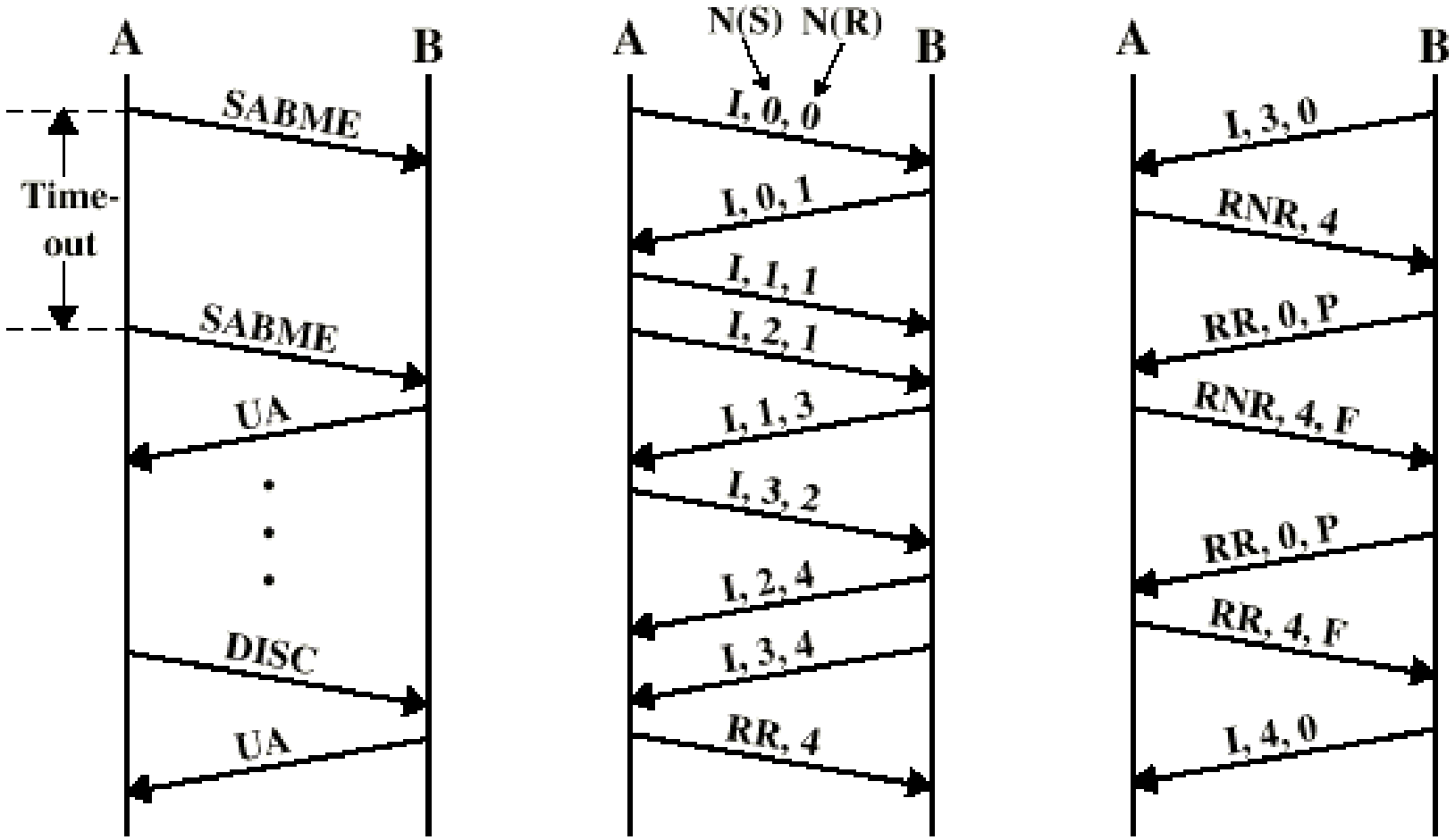
Frame Check Sequence Field

- FCS
- Pendeteksian kesalahan
- 16 bit CRC
- Optional 32 bit CRC

Operasi HDLC

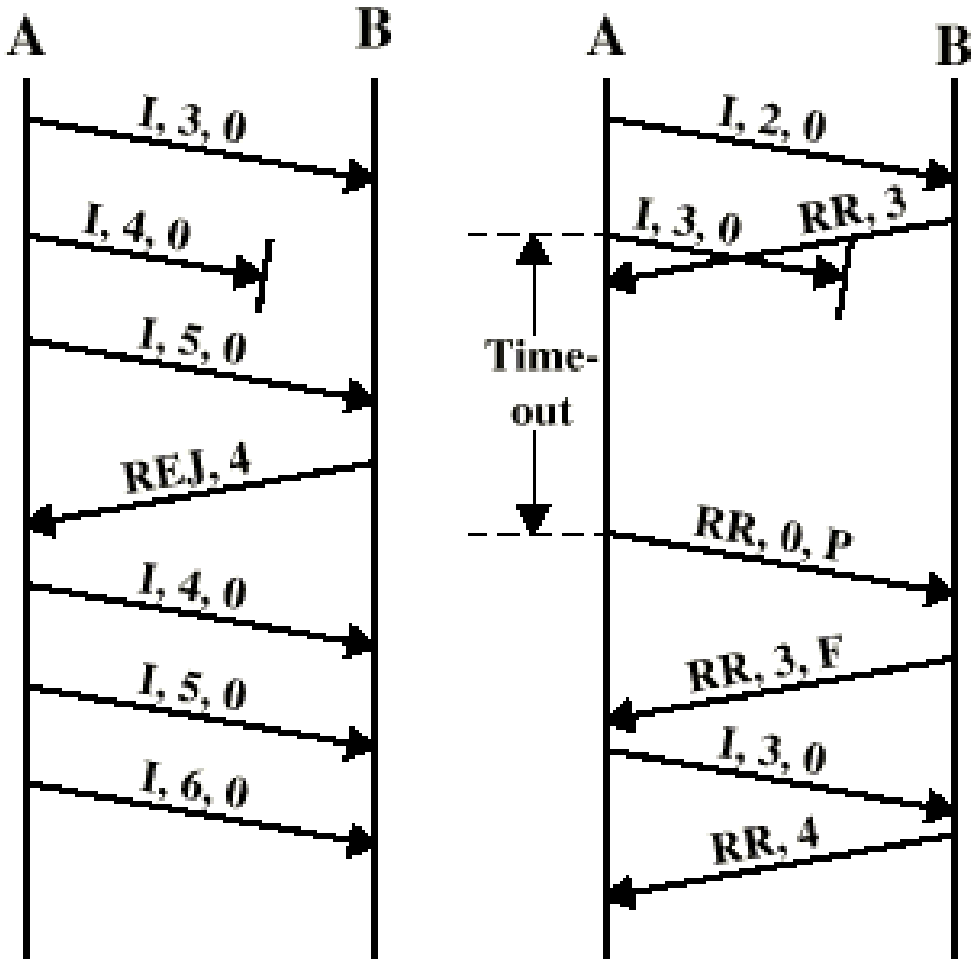
- Pertukaran informasi, supervisory dan frame-frame tidak bernomor
- Tiga fase
  - Initialization
  - Data transfer
  - Disconnect

Contoh Operasi (1)



(a) Link setup and disconnect (b) Two-way data exchange (c) Busy condition

Contoh Operasi (2)



(d) Reject recovery (e) Timeout recovery

Protokol DLC lain (LAPB,LAPD)

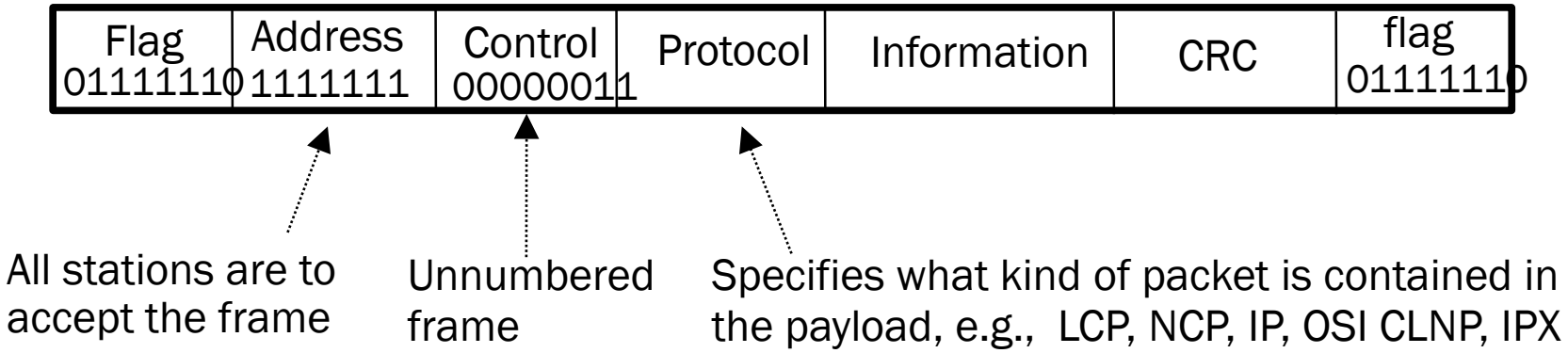
- Link Access Procedure, Balanced (LAPB)
  - Bagian dari X.25 (ITU-T)
  - Subset dari HDLC - ABM
  - Point to point link antara system dan packet switching network node
- Link Access Procedure, D-Channel
  - ISDN (ITU-D)
  - ABM
  - Selalu angka-angka deretan 7-bit (tidak ada 3-bit)
  - 16 bit address field mengandung dua sub-addresses
    - Satu untuk device dan satu untuk user (next layer up)

Protokol DLC lain (LLC)

- Logical Link Control (LLC)
  - IEEE 802
  - Format frame yang berbeda
  - Link control dipisah antara medium access layer (MAC) dan LLC (berada paling atas pada MAC)
  - Tidak ada primary dan secondary - semua station adalah peer
  - Dua alamat diperlukan
    - Sender dan receiver
  - Pendeteksian kesalahan pada MAC layer
    - 32 bit CRC
  - Destination dan Source Access Points (DSAP, SSAP)

Protocol DLC Lainnya (PPP)

- PPP (Point-to-Point Link Protocol)
- Layout frame utk PPP:



Protokol DLC lain (Frame Relay) (1)

- Kemampuan Streamlined melalui jaringan packet switched kecepatan tinggi
- Digunakan sebagai tempat X.25
- Menggunakan Link Access Procedure for Frame-Mode Bearer Services (LAPF)
- Dua protokol
  - Control - mirip dengan HDLC
  - Core - subset dari control

Protokol DLC lain (Frame Relay) (2)

- ABM
- Angka-angka deretan 7-bit
- 16 bit CRC
- 2, 3 atau 4 octet address field
  - Data link connection identifier (DLCI)
  - Mengidentifikasi logical connection
- Lebih banyak pada frame relay terakhir

Protokol DLC lain (ATM)

- Asynchronous Transfer Mode
- Kemampuan Streamlined melampaui jaringan kecepatan tinggi
- Tidak didasarkan pada HDLC
- Format frame disebut “cell”
- Fixed 53 octet (424 bit)
- Detilnya nanti dulu

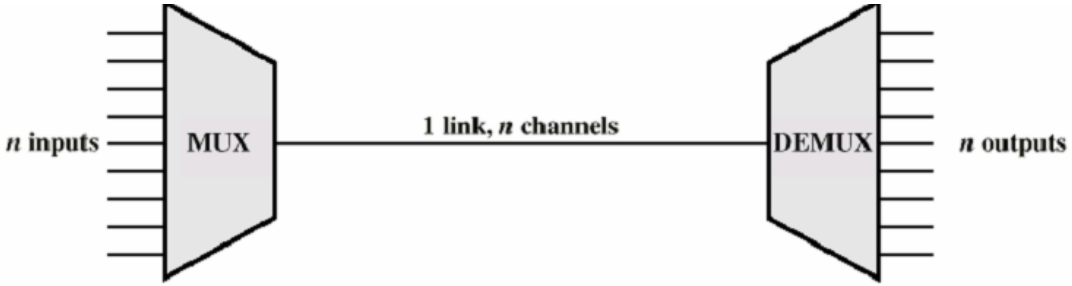
Multiplexing

Multiplexing

- **Multiplex** adalah teknik mengkombinasikan sejumlah sinyal (analog atau digital) untuk ditransmisikan melalui satu media atau saluran.
- Cara umum multiplexing adalah dengan mengkombinasikan sejumlah sinyal berkecepatan rendah melalui satu saluran berkecepatan tinggi.
- **Multiplexer** adalah suatu sirkuit yang berfungsi menggabungkan beberapa atau banyak sinyal elektrik menjadi 1 sinyal tunggal.
- Alasan penggunaan **multiplex :**

1. Menghemat biaya penggunaan saluran komunikasi
2. Memanfaatkan sumber daya seefisien mungkin
3. Kapasitas terbatas dari saluran telekomunikasi digunakan semaksimal mungkin
4. Karakteristik permintaan komunikasi pada umumnya memerlukan penyaluran data dari beberapa terminal ke titik yang sama

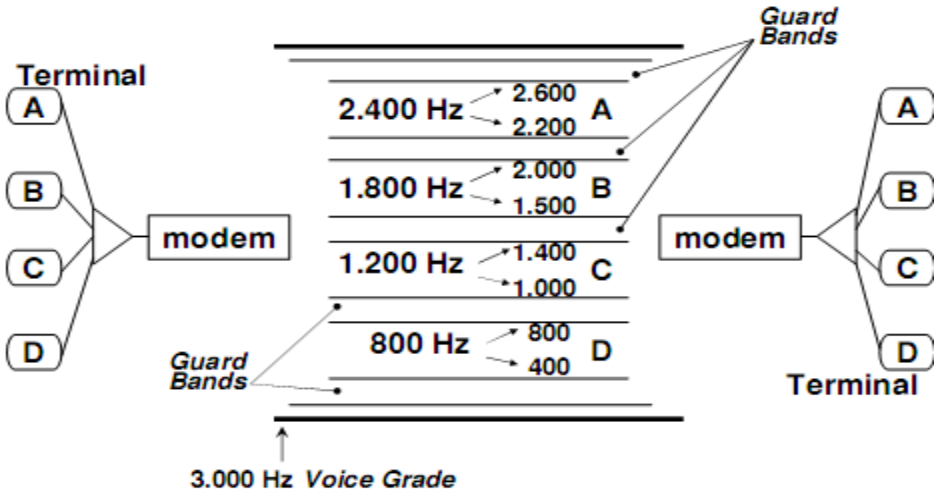
- **Fungsi multiplex:**
  1. Membantu berbagai koneksi pada sebuah mesin
  2. Memetakan banyak koneksi pada sebuah tingkatan antara sebuah koneksi dengan lainnya.



- **Keterangan:**
  1. Multiplexer harus dihubungkan ke demultiplexer melalui satu saluran tunggal.
  2. Saluran mampu membawa saluran n channel yang terpisah
  3. Multiplexer menggabungkan multiplexing data dari jalur input n dan mentransmisikannya melalui jalur berkapasitas tinggi
  4. Demultiplexer menerima aliran data yang sudah dimultiplexkan, kemudian memisahkan data berdasarkan channel, lalu mengirimkannya

Contoh FDM

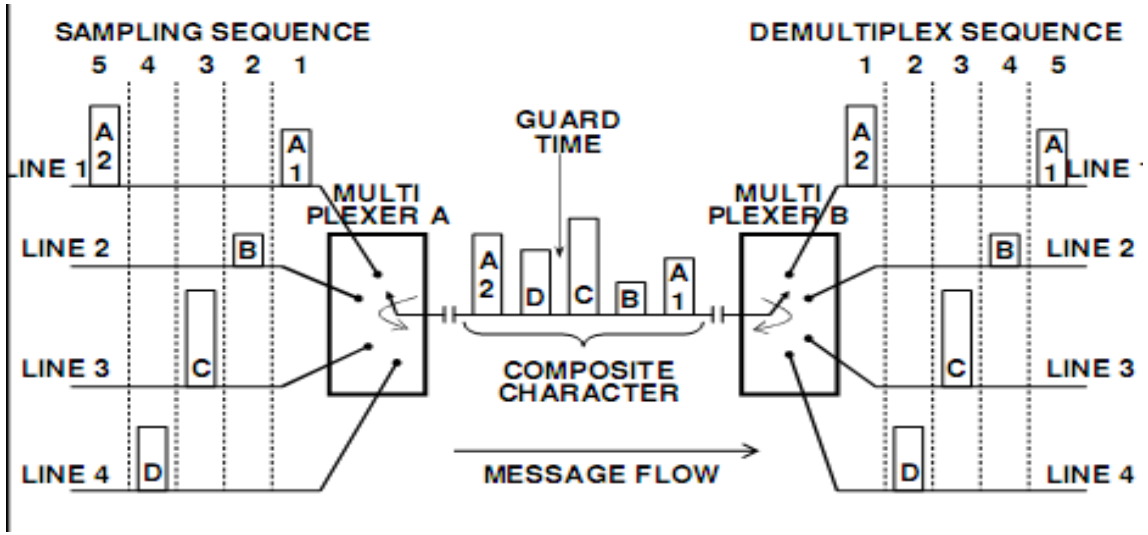
- Misalkan diketahui kanal komunikasi suara berupa kabel voice grade mempunyai lebar frekuensi 300 – 3000 Hz. Dg multiplexing FDM bisa menggunakan lebih dari 1 terminal. Untuk keperluan ini digunakan 4 pembawa, misalnya 600, 1200, 1800, 2400 Hz. Ini berarti data dari 4 buah sumber dpt dikirimkan ke tujuan secara bersamaan hanya dgn menggunakan sebuah saluran voice grade. Bilangan biner “1” diwakili oleh sinyal 800, 1400, 2000, 2600 Hz, sedangkan biner “0” diwakili oleh sinyal 400, 1000, 1600, 2200 Hz. Utk mencegah interferensi, tiap-tiap band dipisahkan oleh jalur selebar 200 Hz.
- Jadi penerima akan memisahkan sinyal yg diterima berdasarkan frekuensinya, lalu disalurkan ke tempat tujuan yg dikehendaki.



Teknik Multiplexing (2)

2. Time Division Multiplexing (TDM)

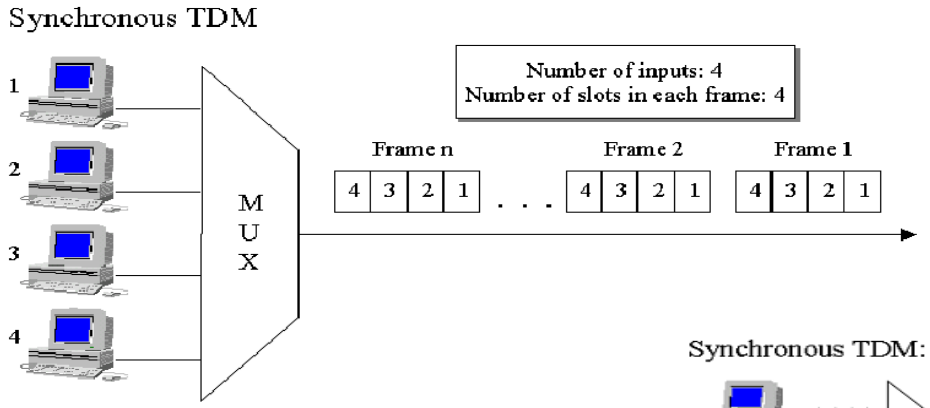
- Metodenya melewatkan banyak data pada sebuah satu sinyal dengan dibagi dalam beberapa segment / frame
- Pengiriman data menggunakan TDM dilakukan dg mencampur data berdasarkan waktu sinyal data tsb dikirimkan.
- TDM digunakan utk transmisi sinyal digital.
- Contoh : GSM pada telepon

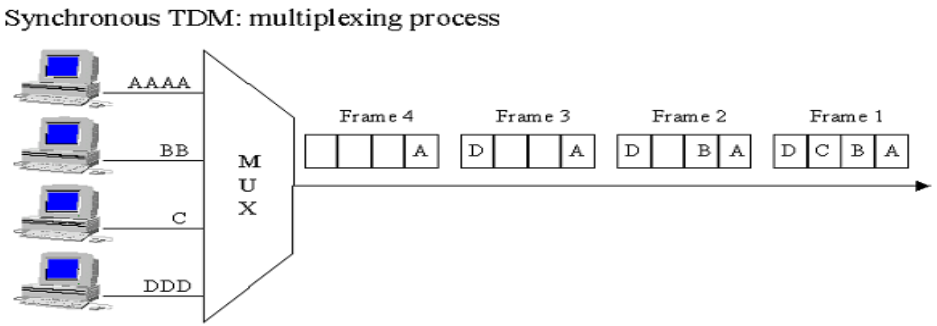


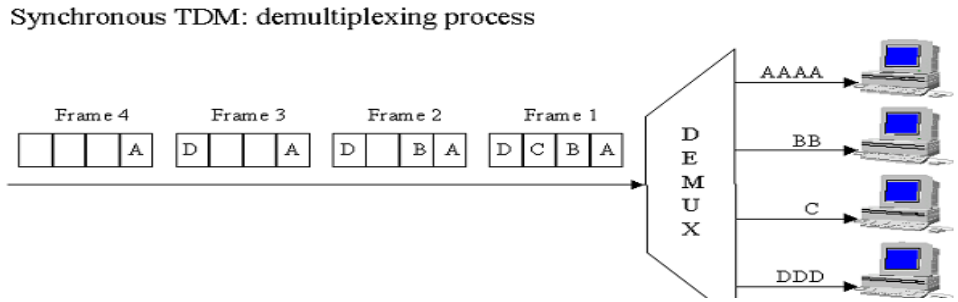
Jenis-Jenis TDM

1. Syncronous TDM

- Kedudukan data yang dikirim bersifat tetap





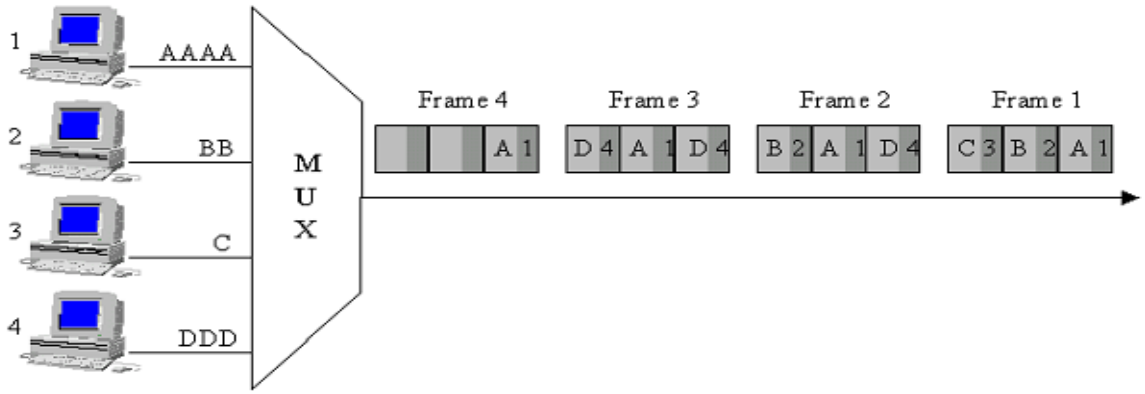


Jenis-Jenis TDM

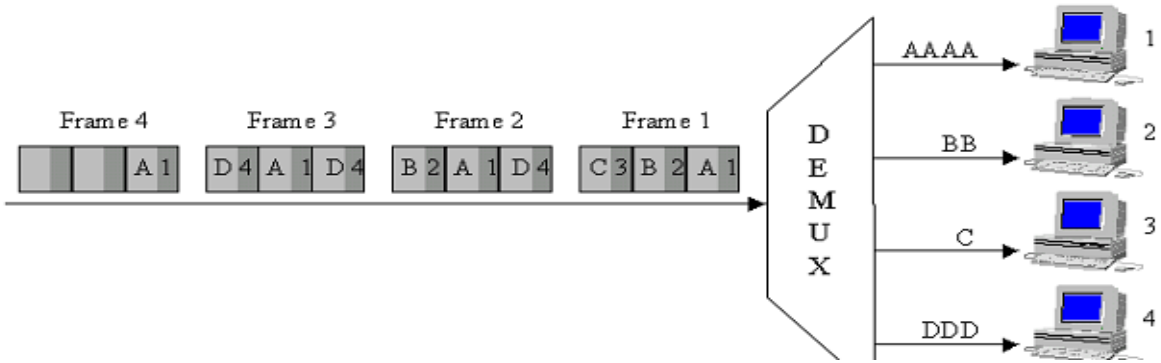
2. Asyncronous TDM

- Kedudukan data yang dikirim tidak bersifat tetap

Asynchronous TDM: multiplexing process



Asynchronous TDM: demultiplexing process



Ex

1. Ubahlah data digital berikut dengan menggunakan teknik NRZL, Bipolar-AMI, Pseudoternary, HDB3 dan B8ZS,ASK,FSK dan PSK.

a. A = 61h

b. 1000001100011

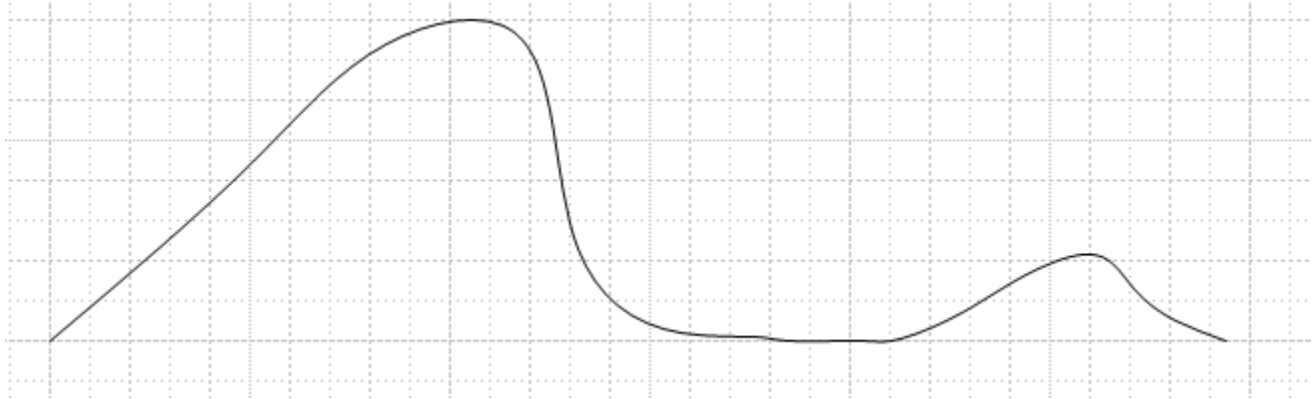
c. a = 41h

d. 1010000111000

e. 1000000001101

f. 10101010110000

2. Ubahlah data analog berikut ke dalam bentuk sinyal digital dengan metode Delta Modulation.



Switching

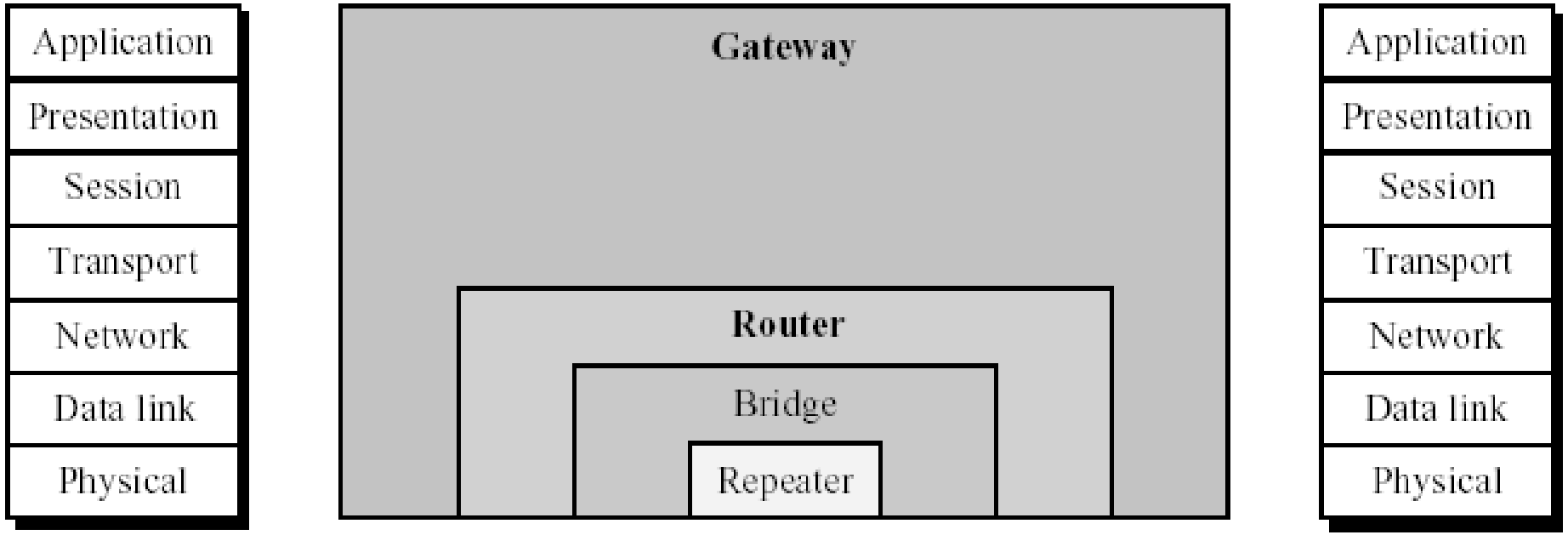
Bridge and Switch

Transmisi Data
Pengkodean Data
Teknik Komunikasi Data Digital
Data Link Control
~~Multiplexing~~
Switching
Medium Access Sublayer
Network Layer

Bridging dan Switching

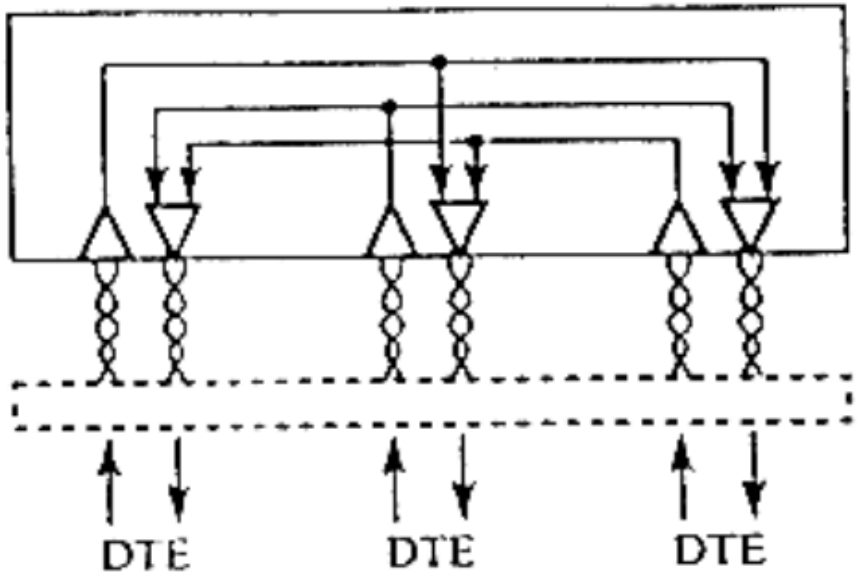
1. Filtering traffic berdasarkan MAC Address yang dilakukan bridges.
    - Contoh jaringan yang di bridging
    - Protocol independent
    - Spanning tree Protocol
    - Eliminasi bridging loops dengan spanning tree protocol
    - Memonitor traffic pada network yang di bridging
2. Filtering traffic berdasarkan MAC Address yang dilakukan Switch.
    - Full duplex operation
    - Mode of operation
    - Cut Trough
    - Store and forward
    - Fragment free
    - VLAN Technology
    - Trunking
    - Monitoring traffic
3. Membangun bentuk Local Area Network sederhana dengan menggunakan bridge dan switch

Memperluas Jangkauan LAN

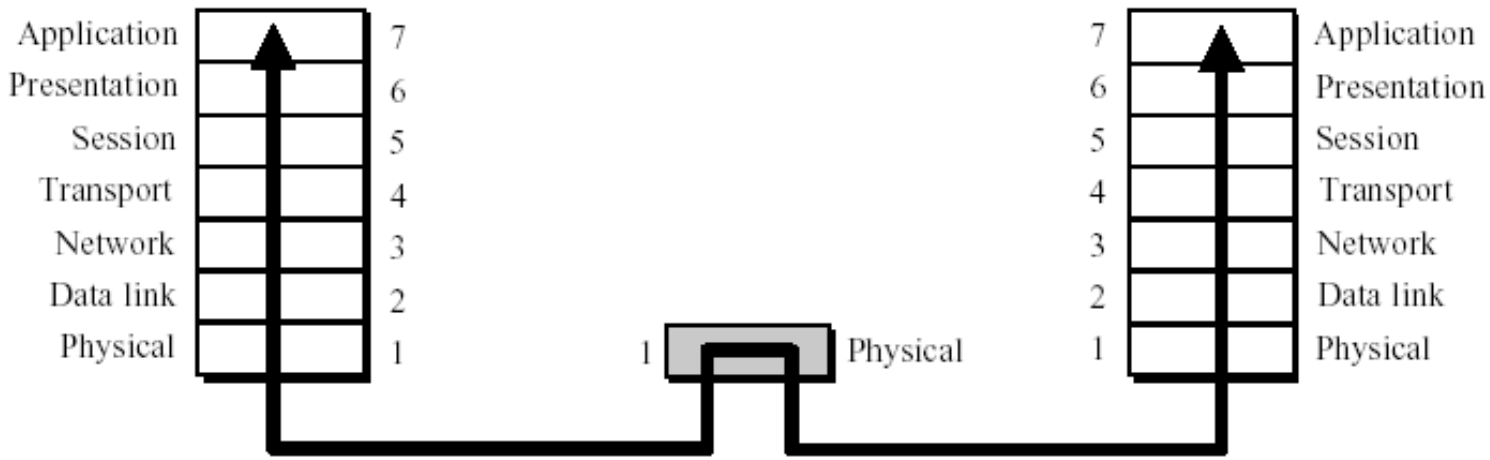


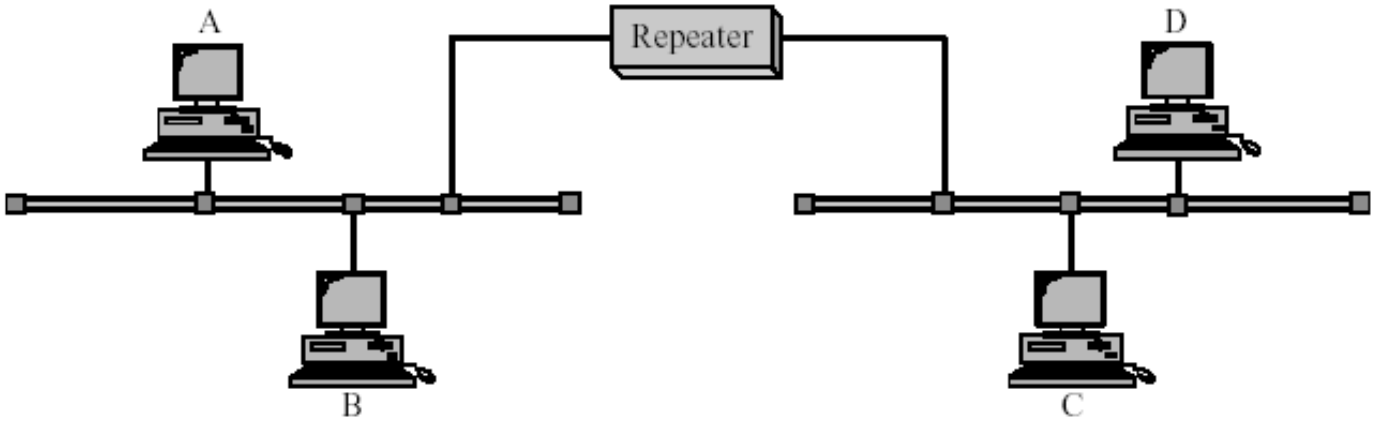
Repeater (Hub)

Seluruh DTE pada 10/100Base-T dihubungkan ke repeater (hub), maka repeater dibuat sedemikian rupa agar jaringan dapat dipandang sebagai suatu *shared network* (seperti halnya 10base-5 atau 10base-2)



Repeater





- Menghubungkan dua segmen LAN yang setipe
- Memperkuat sinyal dari satu segmen ke segmen yang lain
- Noise dan collision ikut disebarkan (tdk dapat memecah collision domain)
- Tidak mengerti format paket
- Known as hub

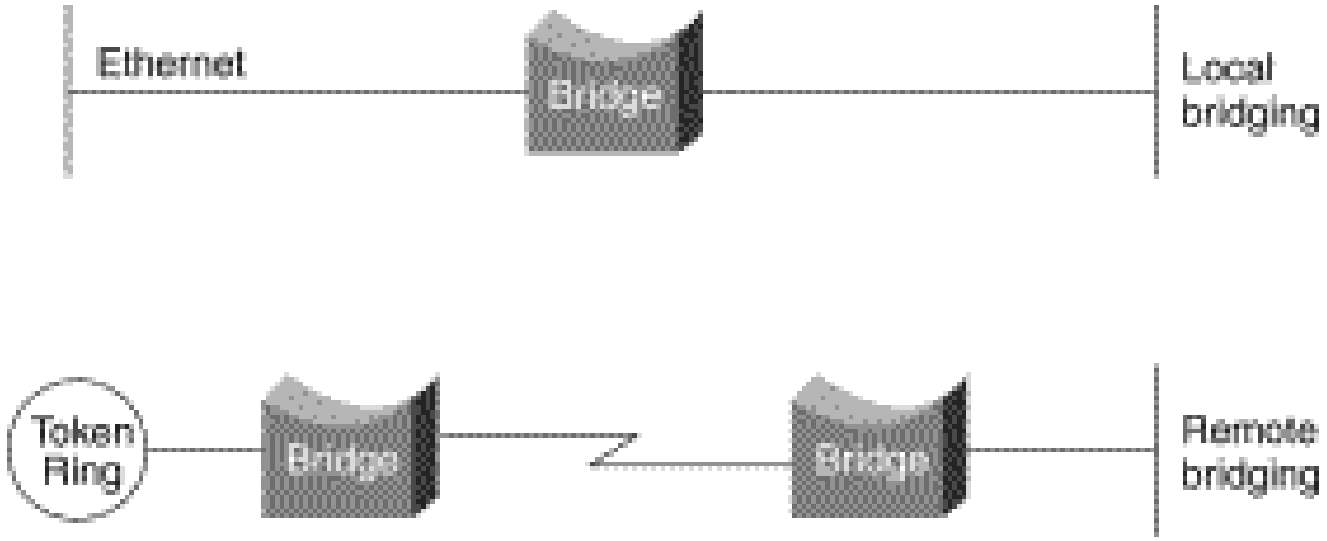
Bridge

- Perangkat layer 2
- Menghubungkan dua segmen LAN (bisa berbeda tipe)
- Mem-forward frame bila perlu
  - Dapat mengenal alamat hardware dan melakukan filtering terhadapnya
    - Noise dan collision tidak ikut disebarkan (tidak diforward)
    - Broadcast/multicast traffic diforward ke seluruh port
- Memungkinkan transmisi beberapa frame secara independent
- Bisa memecah *collision domain* tetapi tidak dapat memecah *broadcast domain*

Types of Bridges

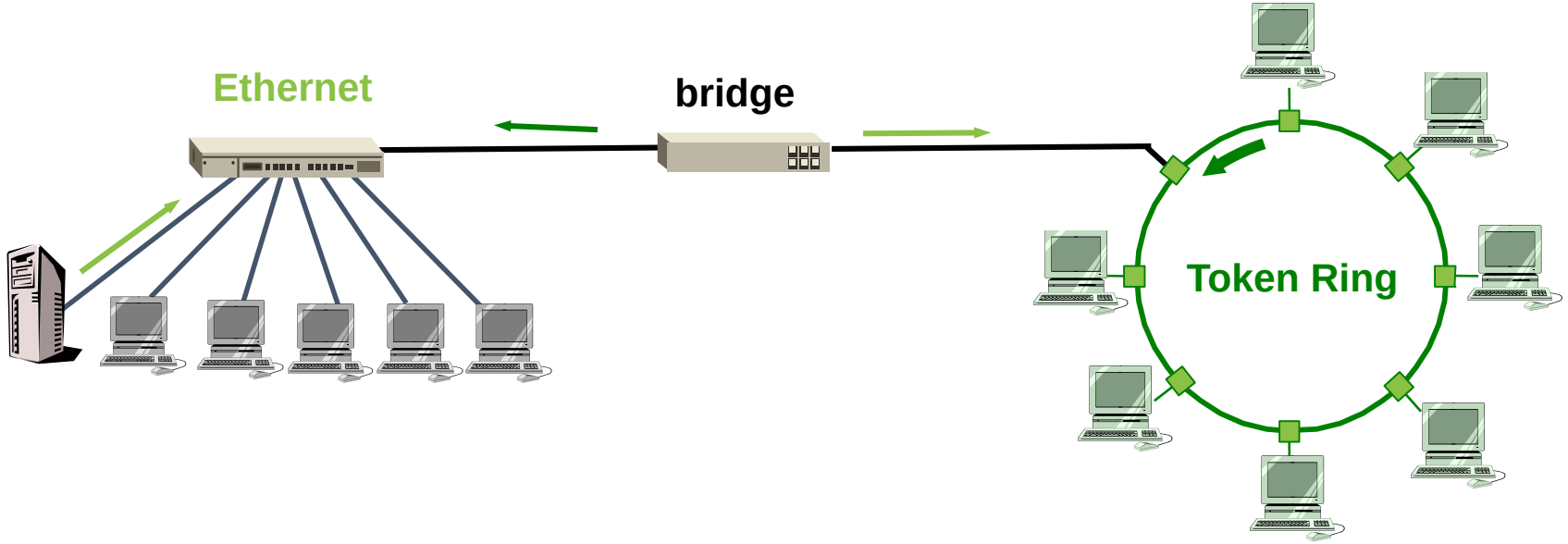
- *Local bridges* provide a direct connection between multiple LAN segments in the same area.
- *Remote bridges* connect multiple LAN segments in different areas, usually over telecommunications lines

Types of Bridges

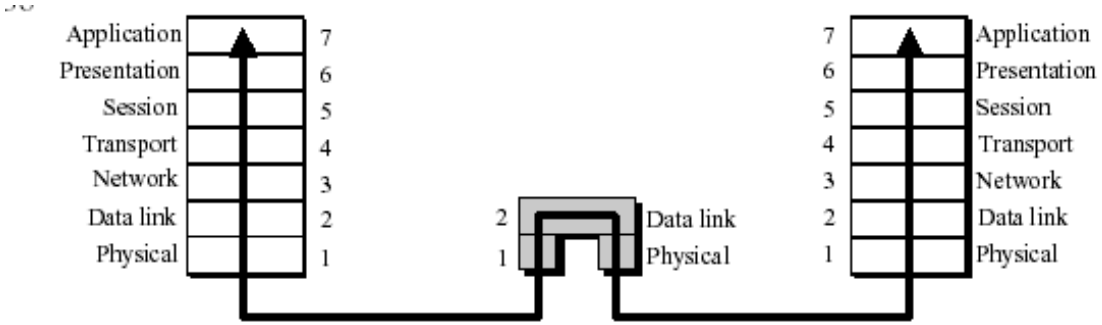


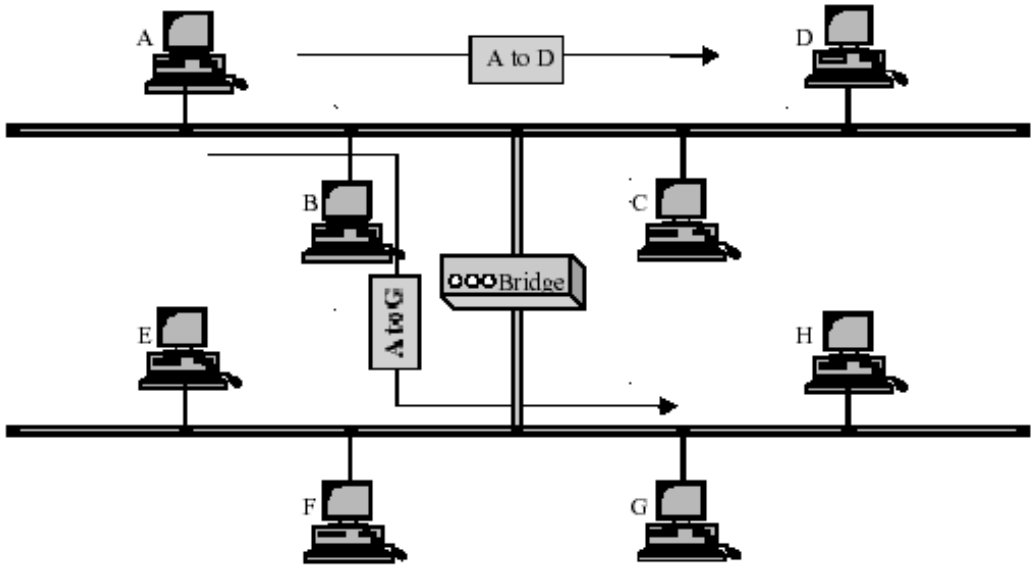
Local and Remote Bridges Connect LAN Segments in Specific Areas

- Sebuah bridge dapat:
  - menghubungkan segmen network
  - memfilter traffic dengan membaca packet addressnya
  - menghubungkan network yang berbeda (Ethernet dan Token Ring) jika level protokol yang lebih tingginya sama atau bisa ditranslasikan



- Sebuah bridge tidak dapat:
  - menentukan jalur mana yang paling efisien untuk mentransmisikan data
  - menyediakan fungsi traffic management (melewatkan kemacetan)
- Fungsi-fungsi bridge dapat dilakukan oleh sebuah server atau device bridge mandiri.
- Aturan umumnya adalah tidak boleh ada lebih dari empat bridge pada satu LAN.

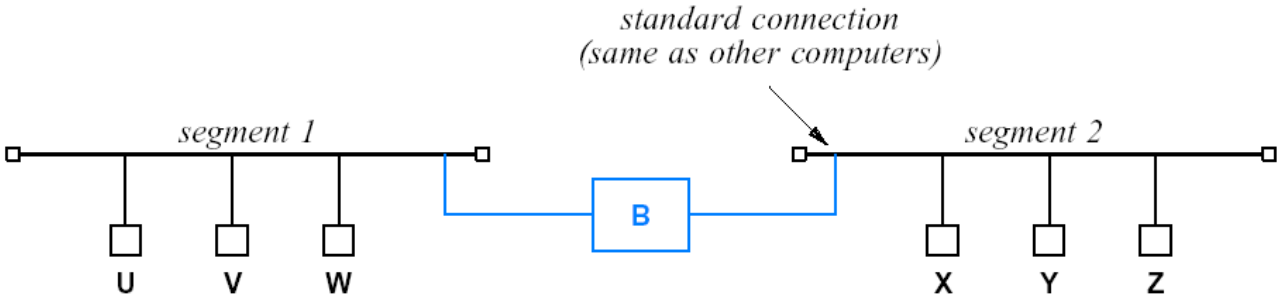

Application
Presentation
Session
Transport
Network
Data link
Physical
7
6
5
4
3
2
1
2
1
Data link
Physical
7
6
5
4
3
2
1
Application
Presentation
Session
Transport
Network
Data link
Physical


A
A to D
D
B
C
Bridge
A to G
E
H
F
G

Algoritma pada Bridge

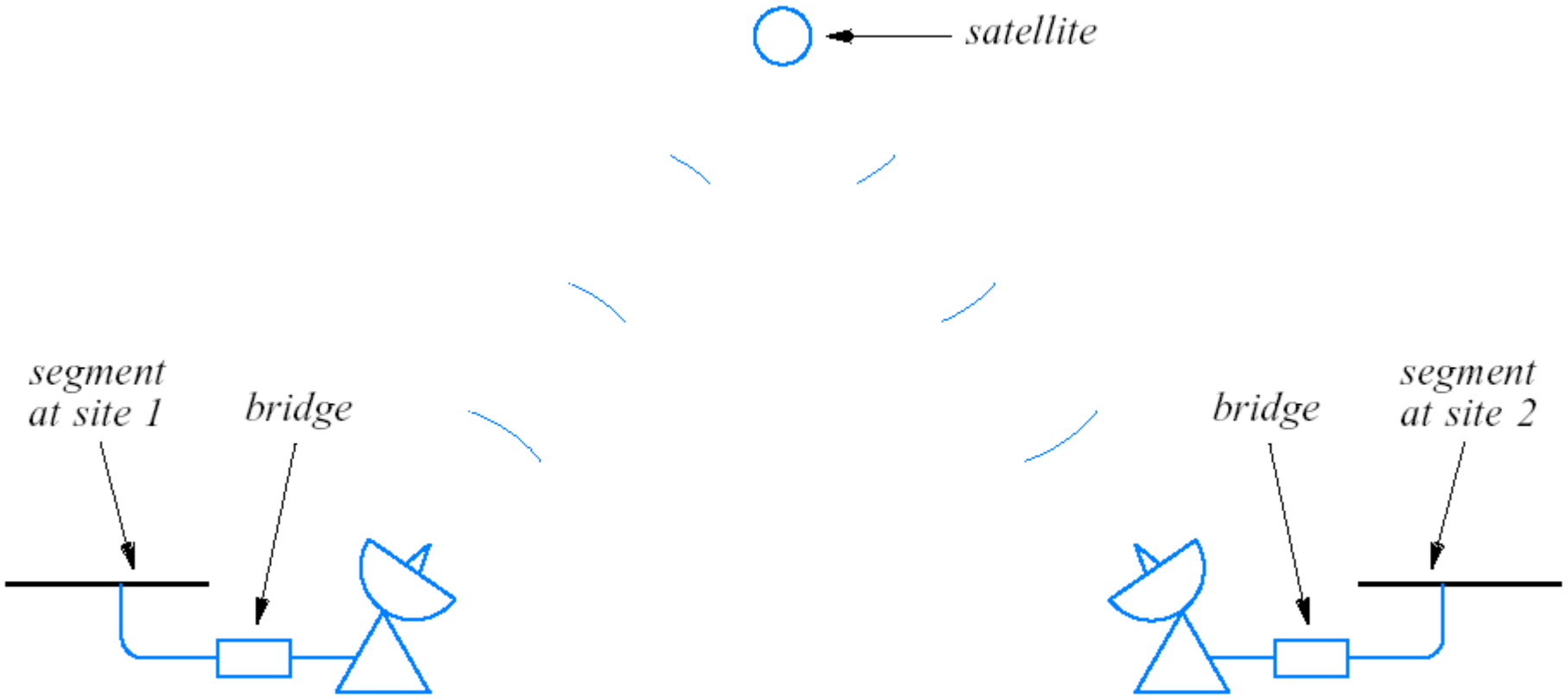
- Listen in promiscuous mode
  - It learns all of the traffics that come to its ports
- Mengamati *source address* dari frame yang masuk
  - Bridge menggunakan source address untuk dapat mengetahui lokasi suatu komputer

Ilustrasi pembelajaran yang dilakukan oleh suatu Bridge



Event	Segment 1 List	Segment 2 List
Bridge boots	–	–
U sends to V	U	–
V sends to U	U, V	–
Z broadcasts	U, V	Z
Y sends to V	U, V	Z, Y
Y sends to X	U, V	Z, Y
X sends to W	U, V	Z, Y, X
W sends to Z	U, V, W	Z, Y, X

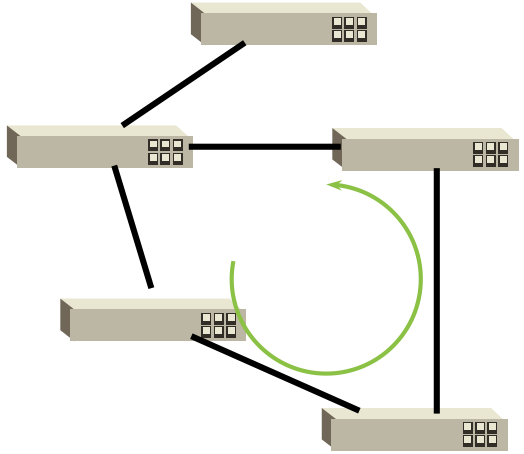
Satellite Bridging



- Beberapa jenis bridge:
  - Transparent (learning) bridge
    - Biasa digunakan pada jaringan Ethernet
    - Bridge dapat mengisi tabel forwarding-nya melalui pembelajaran sendiri (dengan mengamati alamat sumber)
    - Rawan terhadap masalah loop di jaringan
  - Source-routing bridge
    - Biasa digunakan pada jaringan Token Ring
    - Bridge sumber paket menentukan sendiri bridge dan LAN mana yang harus ditempuh oleh paket agar sampai ke tujuan
      - Bisa digunakan pula untuk mencegah loop pada jaringan menggunakan bridge
      - Cara lain untuk mencegah loop adalah dengan menerapkan Spanning Three Algorithm
  - Translation Bridge
    - Menghubungkan dua jaringan yang berbeda arsitektur
      - Misalnya antara Token Ring dengan Ethernet

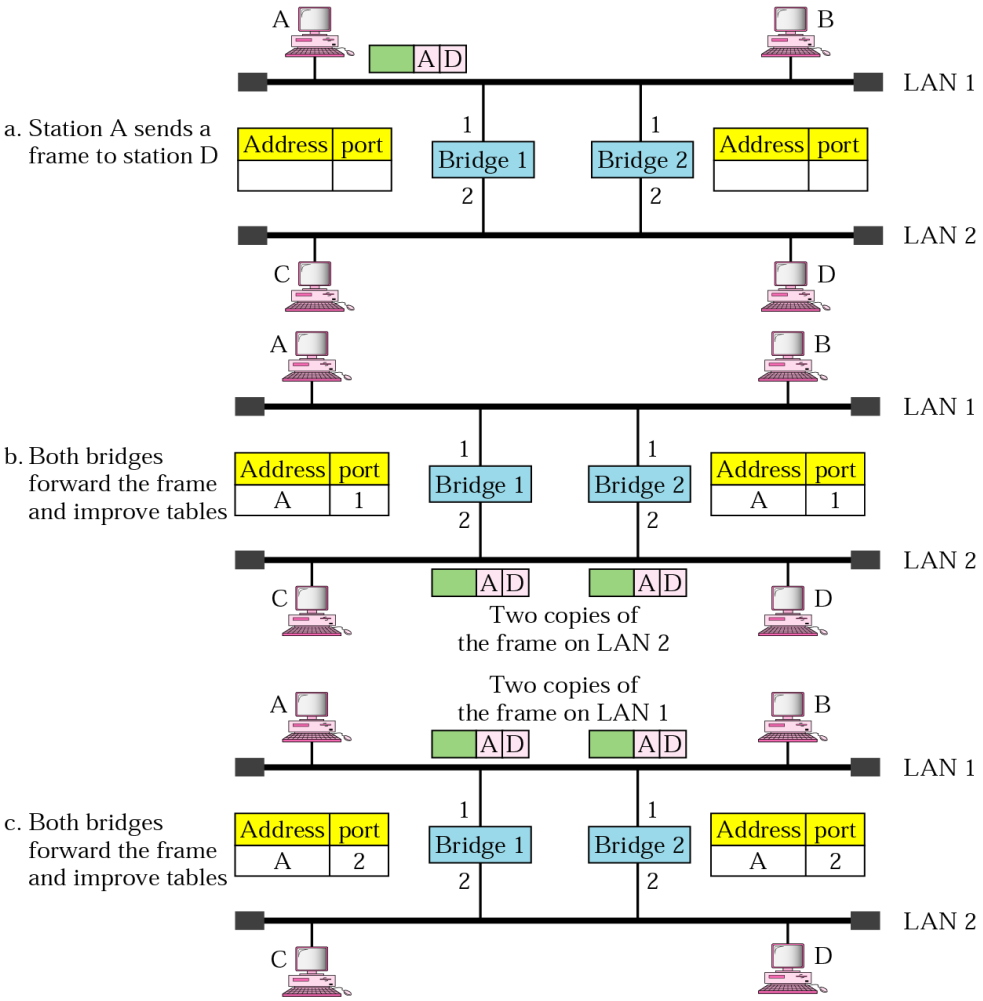
Spanning Tree Algorithm pada Bridge

- Jaringan yang menggunakan bridge tidak boleh membentuk suatu cycle (loop tertutup)
- Untuk mencegah adanya cycle, pada bridge diterapkan spanning tree algorithm
  - Memungkinkan suatu bridge untuk mengenali bridge yang lain
  - Dapat memutuskan cyles
    - Walaupun secara fisik topologinya bisa berbentuk loop tertutup

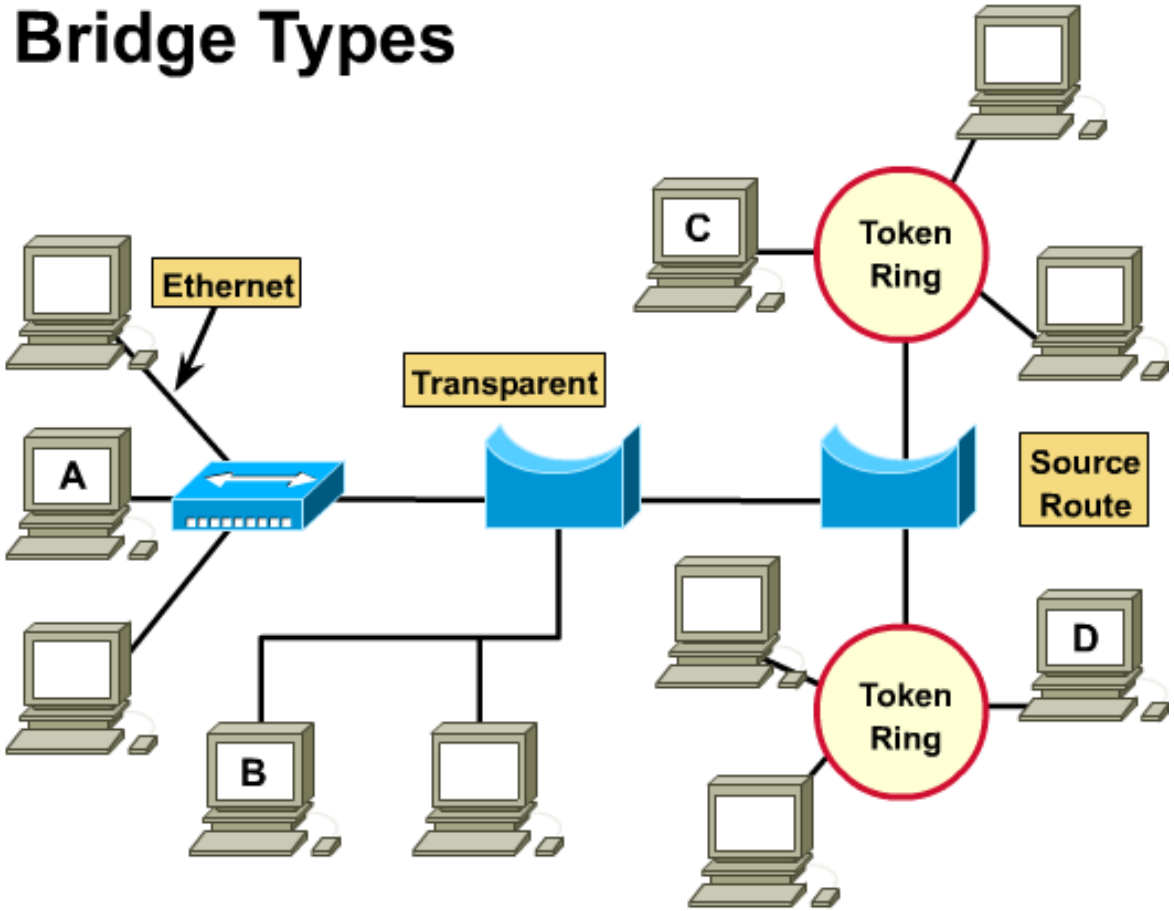


Loop

Loop problem



Bridge Types

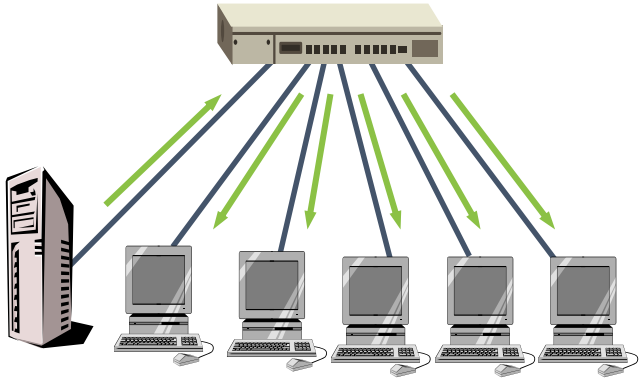


Switch

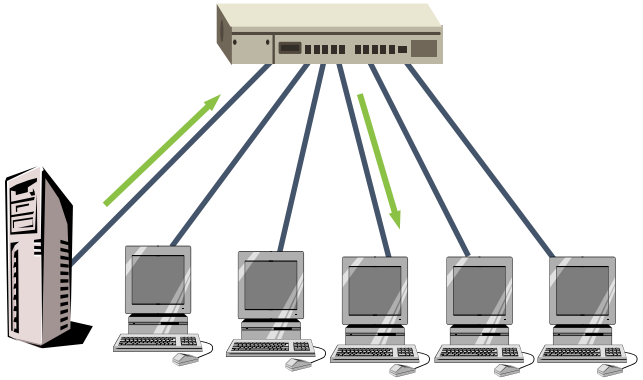
- Mampu mengenali frame (perangkat layer 2)
- Mengenali alamat
- Hanya mem-forward jika diperlukan
- Memungkinkan lebih dari satu pasang komputer berkomunikasi pada saat yang bersamaan

Perbedaan antara hub dan switch

Hub: shared media access



Switch: selective access



Beberapa terminologi

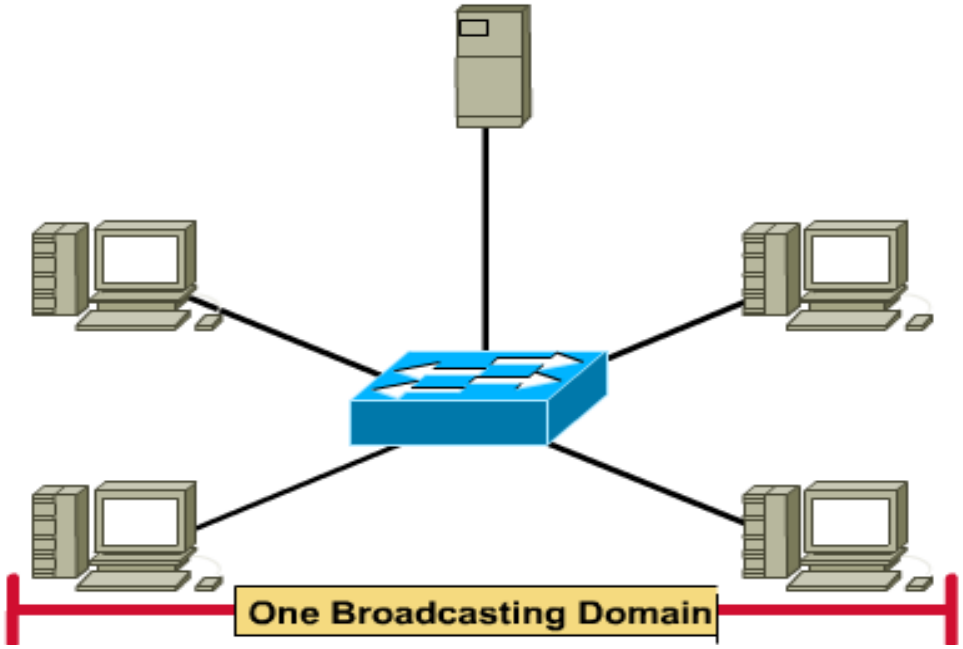
- Layer-2 switch (two-layer switch) adalah bridge yang memiliki banyak interface (multiport bridge) dan dirancang agar memiliki kecepatan yang lebih baik daripada bridge
- Layer-3 switch (three-layer switch) adalah router yang rancangannya lebih ditingkatkan agar memiliki kinerja lebih baik daripada router biasa
  - Layer-3 switch dapat menerima, mengolah dan mendistribusikan (dispatch) paket jauh lebih cepat daripada router biasa

What is Layer-2 switching?

- *Hardware based*
  - Menggunakan MAC address untuk melakukan penapisan (filtering)
- Switching berlangsung dengan cepat karena switch tidak memeriksa informasi header *network layer*
  - Hanya melihat *hardware address* sebelum memutuskan mem-forward frame atau men-dropnya
- Dapat digunakan untuk memecah *collision domain*
- Menaikkan bandwidth untuk setiap user karena setiap koneksi (interface) ke switch merupakan suatu *collision domain* sendiri sehingga kita dapat menghubungkan beberapa perangkat ke setiap interface

Keterbatasan *Layer-2 Switching*

- Tidak dapat memecah *broadcast domain*
  - Switch akan mem-forward frame broadcast (juga multicast) ke seluruh port yang ada pada switch
  - Agar switch hanya mem-forward frame broadcast kepada port tertentu, dapat dibuat suatu Virtual LAN (VLAN)
- Bila ukuran jaringan semakin besar dapat menyebabkan masalah besar juga akibat
  - Trafik broadcast dan multicast
  - Konvergensi *spanning tree* yang lambat
- Karena masalah-masalah inilah maka *layer-2 switching* tidak dapat menggantikan peran router dalam suatu *internetwork*


One Broadcasting Domain

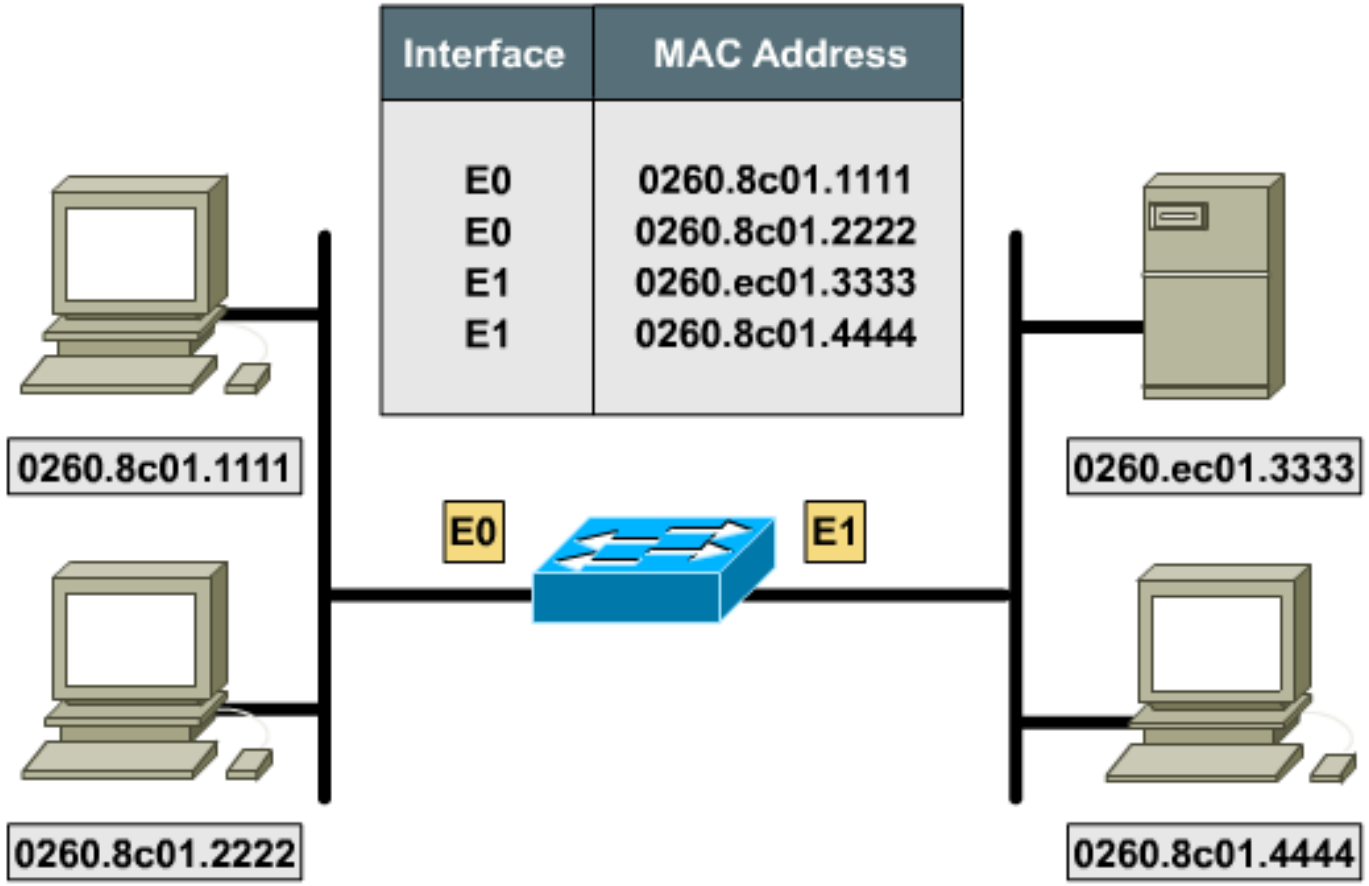
Bridging vs Layer-2 Switching

- Meskipun *layer-2 switching* dapat dianggap sebagai multiport bridge, tetapi ada perbedaan mendasar yang perlu diketahui yaitu:
  - Bridge berbasis *software* sedangkan *layer-2 switch* berbasis *hardware* dalam menentukan keputusan filtering
  - Setiap bridge hanya memiliki satu spaning tree sedangkan switch bisa banyak
  - Bridge hanya maksimum memiliki 16 port sedangan switch bisa memiliki ratusan port

Fungsi *Layer-2 Switching*

- Address Learning
  - Mengingat alamat *hardware* sumber dari frame yang diterima interface-nya serta memasukkan informasi ini ke database MAC
- Forward/filter decision
  - Ketika frame diterima sebuah interface pada switch, switch melihat alamat *hardware* tujuan lalu mencari interface keluar pada database MAC-nya
- Loop avoidance
  - Jika ada *multiple connection* antar switch untuk keperluan redudancy, maka dapat terjadi loop, untuk mencegahnya digunakan *spanning tree protocol (STP)*

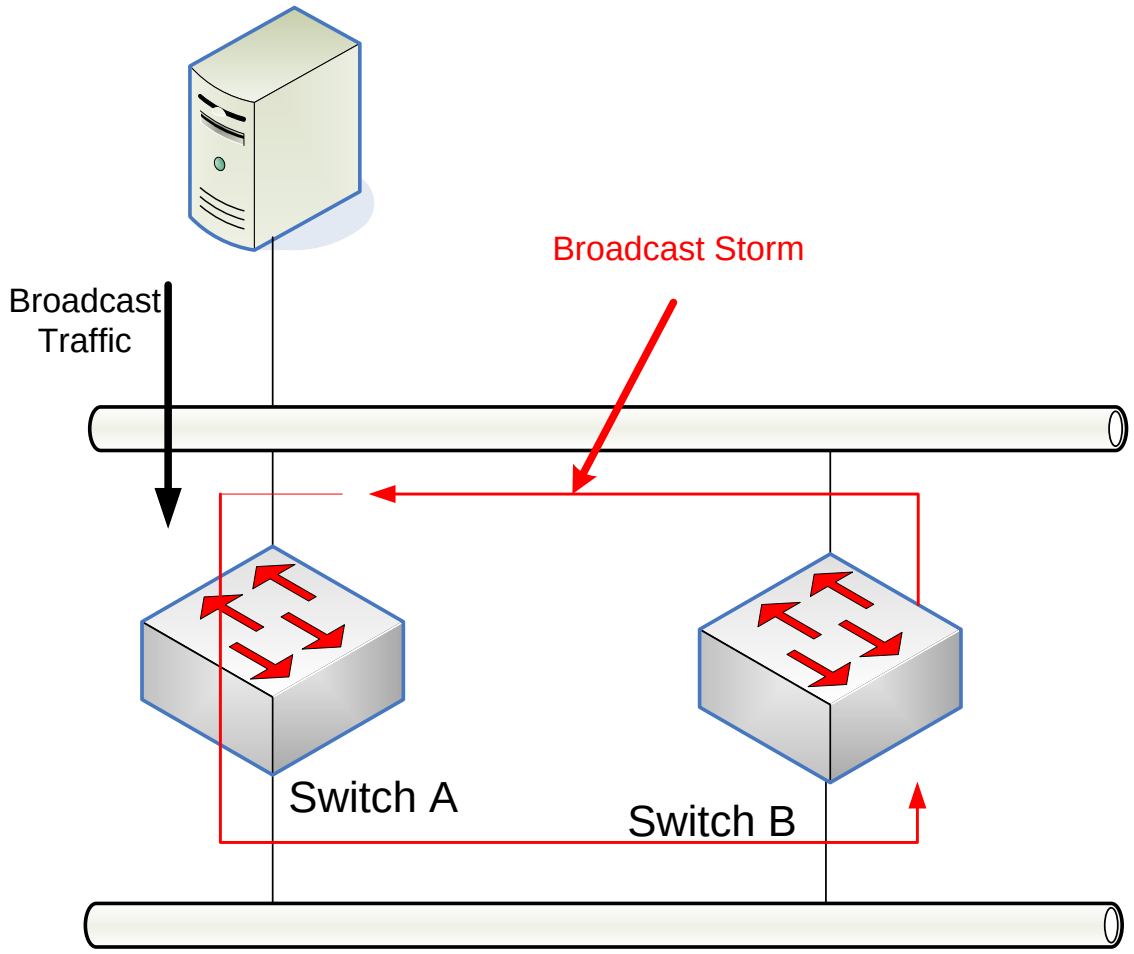
Switching Table



Interface	MAC Address
E0	0260.8c01.1111
E0	0260.8c01.2222
E1	0260.ec01.3333
E1	0260.8c01.4444

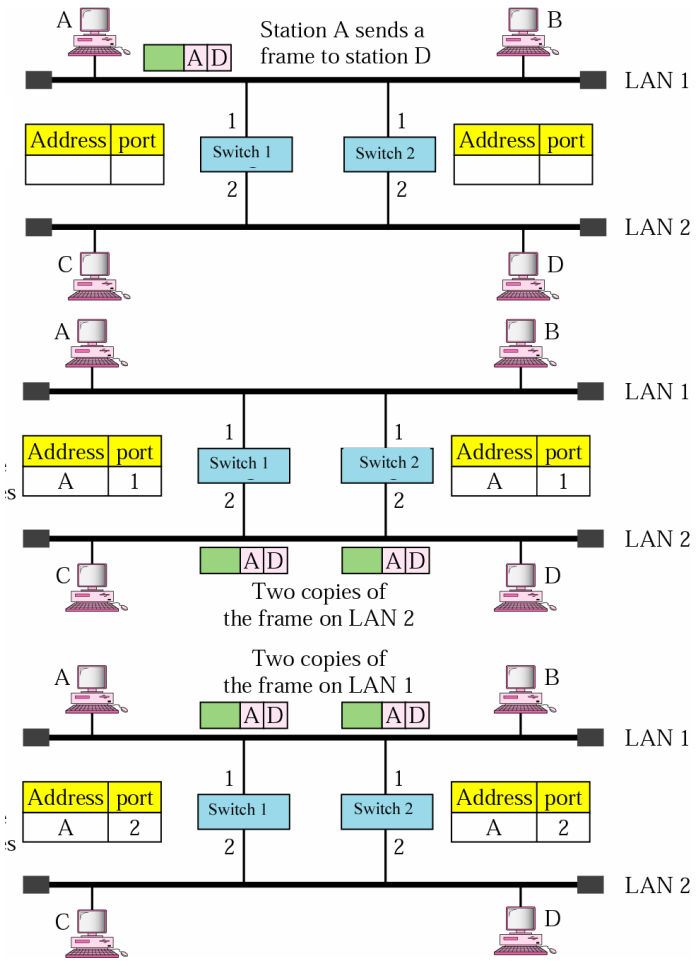
Loop avoidance

- Link redundant antar switch memang bermanfaat, tetapi ada beberapa masalah serius yang bisa timbul bila tidak ada mekanisme *loop avoidance*:
  - Switch bisa membanjiri jaringan oleh trafik broadcast (broadcast storm)



Loop Avoidance (2)

- Bisa terdapat lebih dari satu frame yang sama yang beredar pada jaringan multisegment
- Menimbulkan kebingungan pada pengisian tabel MAC akibat switch dapat menerima frame dari beberapa link
  - Switch jadi tidak mampu mem-forward frame karena switch terus melakukan updating terhadap tabel MAC → ini disebut *thrashing the MAC table*



Loop Avoidance (3)

- Bisa terjadi multiple loop di dalam jaringan
  - Ada loop di dalam loop
    - Bila ada broadcast storm, maka switch tidak dapat lagi melakukan packet switching
- Spanning-Tree Protocol dibuat untuk menanggulangi kemungkinan adanya loop di jaringan

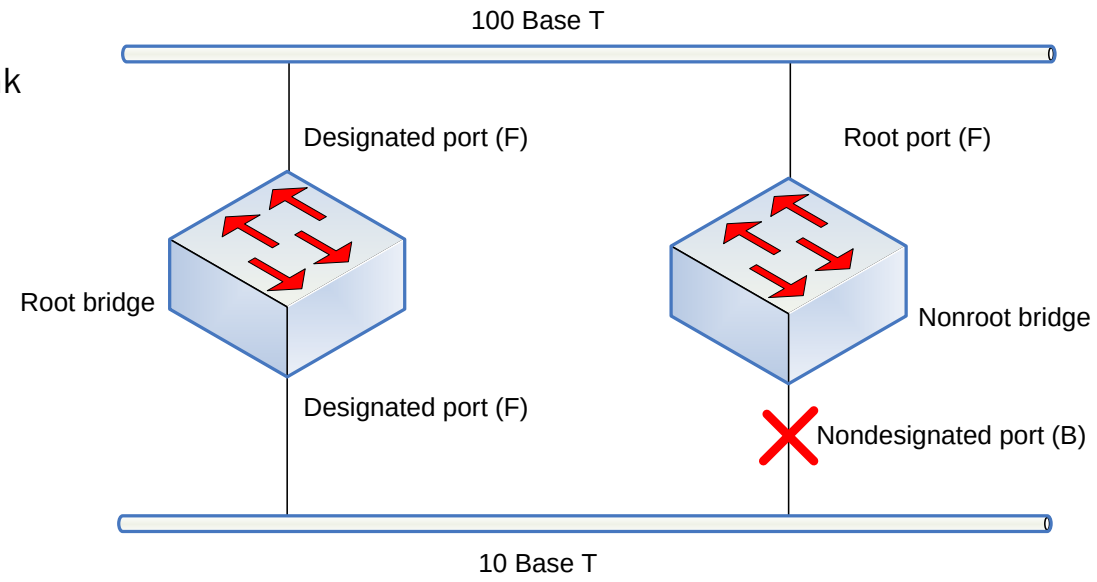
Spanning-Tree Protocol (STP)

- Dibuat pertama kali oleh Digital Equipment Corporation (DEC) [sekarang Compaq]
- Lalu IEEE membuat versi STP yang disebut 802.1d
  - Tidak kompatibel dengan versi DEC
  - Seluruh switch Cisco menjalankan STP versi IEEE802.1d
- Fungsi utama STP adalah mencegah adanya loop pada jaringan layer-2 (baik menggunakan bridge maupun switch)
- STP secara terus menerus memantau seluruh link pada jaringan agar tidak terjadi loop dengan mematikan link-link redundant

Cara kerja STP

- STP akan memutuskan (shut down) link redundant pada jaringan agar tidak ada loop pada jaringan
- Caranya dengan terlebih dulu memilih suatu *root bridge*
  - *Root bridge* akan menentukan topologi jaringan
  - Hanya boleh ada satu *root bridge* pada suatu jaringan tertentu
  - Port *root bridge* disebut *designated ports* yang disebut bekerja dalam keadaan *forwarding-state*
    - Port *fowading-state* akan menerima dan mengirimkan trafik
- Switch lain yang ada di dalam jaringan disebut *nonroot bridge*

- Port pada *nonroot bridge* yang memiliki jalur ke arah *root bridge* paling murah disebut *root port* dan akan digunakan untuk mengirim dan menerima trafik
  - Cost suatu link ditentukan berdasarkan bandwidth link tersebut
    - Link yang berkecepatan tinggi (bandwidth lebar) akan memiliki cost yang lebih murah daripada link yang berkecepatan lebih rendah
- Port yang jalur menuju root bridge-nya paling murah disebut *designated port*
  - Port lainnya dianggap *nondesignated port* dan tidak akan digunakan untuk menerima maupun mengirimkan trafik
    - Port ini disebut berada dalam mode *blocking*



Cara memilih *root bridge*

- Switch atau bridge yang menjalankan STP akan bertukar informasi menggunakan *Bridge Protocol Data Units* (BPDU)
  - BPDU mengirimkan pesan-pesan konfigurasi (configuration message) menggunakan frame multicast
  - *Bridge ID* dari setiap perangkat dikirimkan ke perangkat lain menggunakan BPDU
- *Bridge ID* digunakan untuk menentukan *root bridge* dan *root port*
  - *Bridge ID* berukuran 8 byte dan mengikutsertakan prioritas serta MAC address dari perangkat yang bersangkutan
  - Prioritas default pada seluruh perangkat yang menjalankan STP versi IEEE adalah 32,768

Cara memilih *root bridge* (2)

- Penentuan *root bridge* dilakukan dengan melihat prioritas bridge dan *MAC address*
- Jika dua switch atau bridge memilki prioritas yang sama, maka barulah *MAC address* digunakan untuk menentukan mana di antara keduanya yang memiliki prioritas paling rendah
  - Misalnya ada dua switch A dan B;keduanya memiliki prioritas 32,768 maka *MAC address* akan digunakan untuk menentukan switch yang prioritasnya paling rendah; misalnya *MAC address* switch A adalah 0000.0c00.1111.1111 sedangkan *MAC address* switch B adalah 0000.0c00.2222.2222, maka switch A-lah yang akan dipilih menjadi *root bridge*

Cara memilih *root bridge* (3)

Berikut contoh suatu BPDU yang dikirimkan oleh suatu switch Cisco 1900 (BPDU dikirimkan setiap 2 detik (default))

This is a root bridge

```
   Flags:  0x80        802.3
   Status: 0x00
   Packet Length:64
   Timestamp:          19:33:18.726314       02/28/2000
802.3 Header
   Destination:        01:80:c2:00:00:00
   Source:             00:b0:64:75:6b:c3
   LLC Length:         38
802.2 Logical Link Control (LLC) Header
   Dest. SAP:          0x42 802.1 Bridge Spanning Tree
   Source SAP:         0x42 802.1 Bridge Spanning Tree
   Command:            0x03 Unnumbered Information
802.1 - Bridge Spanning Tree
   Protocol Identifier:          0
   Protocol Version ID:          0
   Message Type:                 0 Configuration Message
   Flags:                        %00000000
   Root Priority/ID:  0x800      / 00:b0:64:75:6b:c0
   Cost of Path to Root:         0x00000000 (0)
   Bridge Priority/ID:0x8000     / 00:b0:64:75:6b:c0
   Port Priority/ID:  0x80       /0x03
   Message Age:                                        0/256 seconds
```

Cara memilih *designated port*

- Untuk menentukan satu buah atau beberapa port yang akan digunakan untuk berkomunikasi dengan *root bridge*, yang harus diperhatikan adalah cost dari jalur (path cost)
- Tabel di samping menunjukkan cost tipikal jaringan Ethernet

Speed	New IEEE Cost	Original IEEE Cost
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

Kondisi Port Spanning-Tree

- Kondisi (state) port yang terdapat pada bridge atau switch dapat bertransisi melalui empat kondisi:
  - **Blocking**
    - Pada kondisi ini bridge/switch tidak akan mem-forward frame pada port tersebut
    - Port masih bisa “mendengarkan” BPDU
    - Secara default,seluruh port berada di dalam kondisi *blocking* bila bridge/switch baru pertama kalai dinyalakan
  - **Listening**
    - Port “mendengarkan” BPDU untuk menjamin tidak ada loop di dalam jaringan sebelum mengirimkan data
  - **Learning**
    - Mempelajari MAC address dan mambangun tabel filter tetapi tidak mem-forward frame
  - **Forwarding**
    - Mengirimkan dan menerima seleuruh data pada port bridge

Kondisi Port Spanning-Tree (2)

- Biasanya, port switch berada di dalam kondisi *blocking* atau *forwarding*
  - *Forwarding port* memiliki cost jalur yang paling rendah ke *root bridge*
- Tetapi, jika terjadi perubahan topologi akibat adanya link yang rusak atau ada penambahan switch, maka port pada suatu switch akan berada dalam kondisi *listening* dan *learning*
- *Blocking port* digunakan untukmencegah loop pada jaringan
- Ketika suatu switch sudah menentukan jalur terbaik ke *root bridge* maka seluruh port lain berada di dalam kondisi *blocking*
  - Jangan lupa *blocked port* tetap dapat menerima BPDU
- Jika suatu switch menentukan bahwa suatu *blocked port* akan dijadikan sebagai *designated ports*, maka switch akan berada di dalam kondisi listening
  - Pada kondisi ini, switch men-cek seluruh BPDU yang diterima untuk menjamin tidak akan terbentuknya loop bila kondisi suatu port berubah menjadi *forwarding*

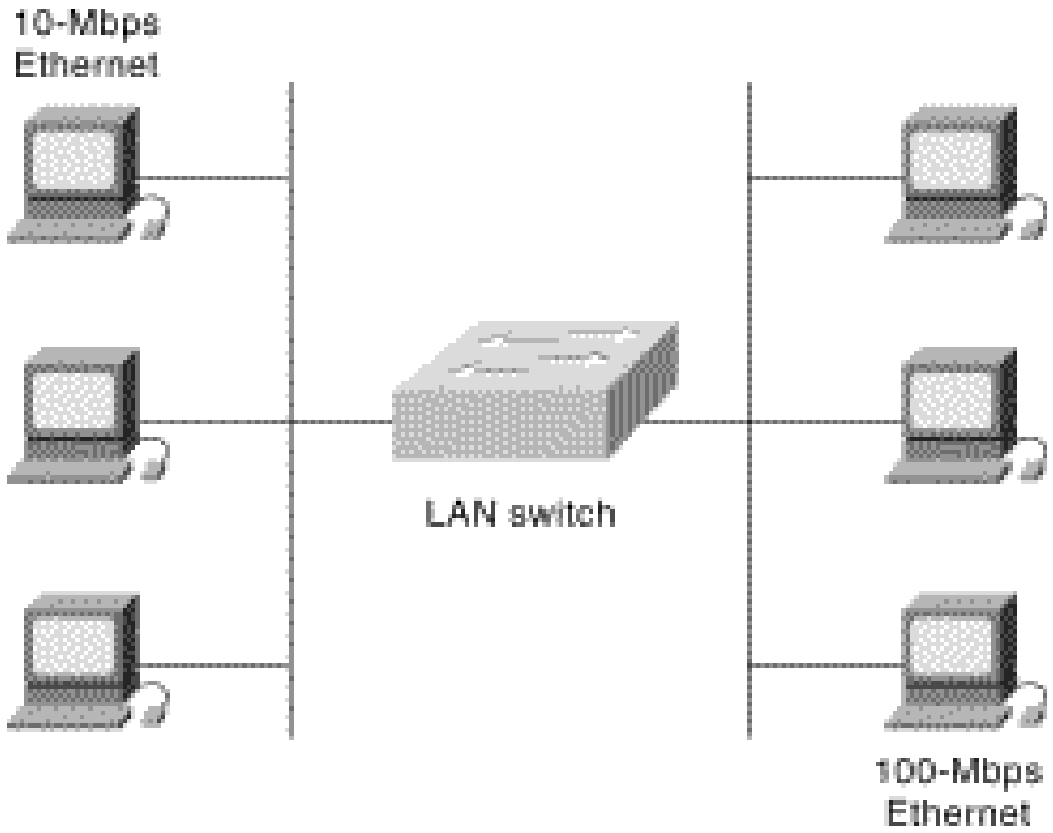
Convergence

- Konvergensi terjadi ketika bridge dan switch bertransisi ke kondisi *forwarding* atau *blocking*
  - Selama transisi, tidak ada data yang diforward
- Konvergensi penting untuk menjamin seluruh perangkat memiliki database yang sama
- Sebelum data dapat di-forward, seluruh perangkat harus di-update
- Masalah pada konvergensi adalah waktu yang diperlukan oleh perangkat-perangkat ini untuk melakukan update
- Biasanya diperlukan waktu 50 detik untuk berubah dari kondisi blocking ke forwarding
- Tidak dianjurkan untuk merubah timer STP, tetapi bila perlu timer dapat disetting
- *Forward delay* adalah waktu yang dibutuhkan oleh suatu port untuk berubah dari kondisi *learning* ke kondisi *forwarding*

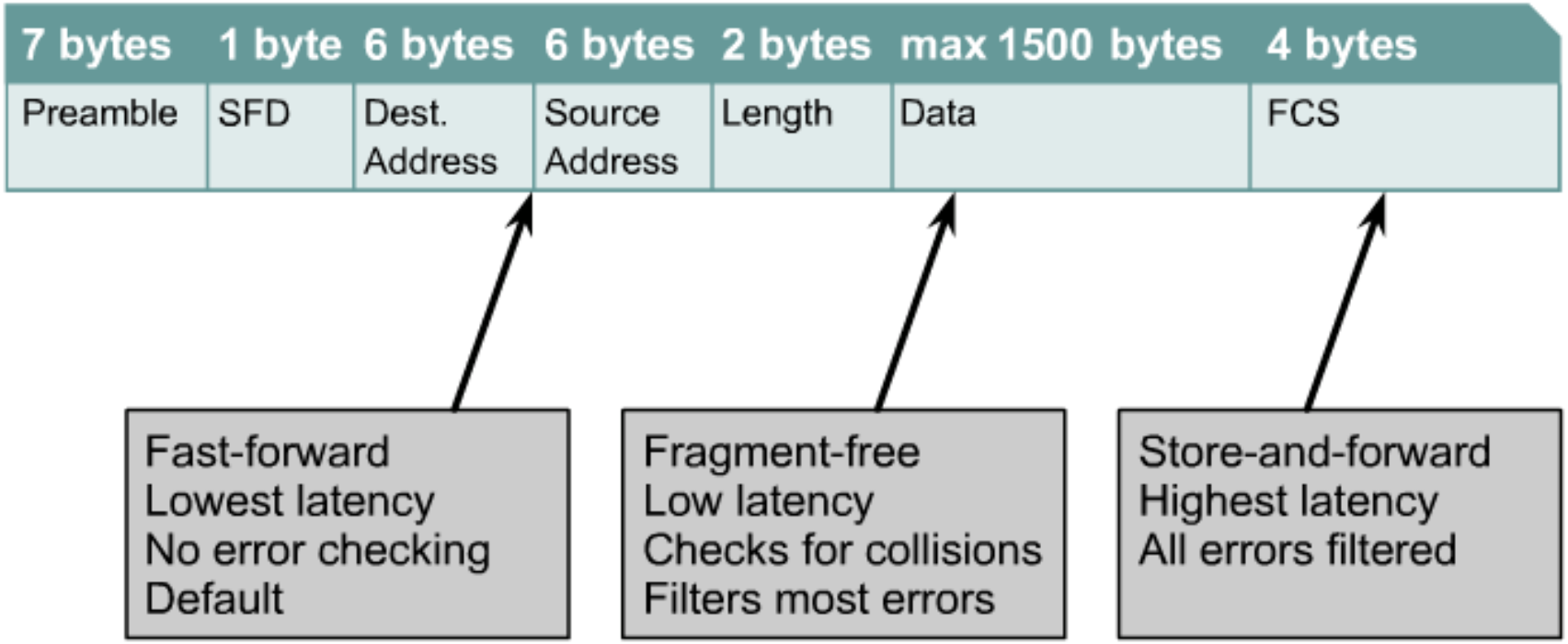
LAN Switch Type

- Latency pada switch dipengaruhi oleh mode switching yang digunakan
- Ada tiga macam mode switching, yaitu:
  - Store and Forward
    - Seluruh frame harus diperiksa oleh switch,CRC-nya dihitung, lalu dicarikan hardware address tujuannya
    - Frame dibuang jika :
      - CRC error
      - Terlalu pendek
      - Terlalu panjang
  - Cut-trough (real time/fast forward)
    - Frame tidak diperiksa keseluruhan,melainkan apabila hardware address sudah diterima switch langsung mencarikan hardware address tujuan
  - Fragment Free (Modified Cut-trough)
    - Pada mode ini, switch hanya mencek frame sampai 64 bytes pertama sebelum mem-forward frame
      - Hal ini dapat dilakukan karena pada umumnya error terjadi pada 64 bytes pertama
- Latency Store and Forward > Latency Fragment Free> Latency Cut-trough

LAN Switch



A LAN Switch Can Link 10-Mbps and 100-Mbps Ethernet Segments


7 bytes
1 byte
6 bytes
6 bytes
2 bytes
max 1500 bytes
4 bytes
Preamble
SFD
Dest. Address
Source Address
Length
Data
FCS
Fast-forward
Lowest latency
No error checking
Default
Fragment-free
Low latency
Checks for collisions
Filters most errors
Store-and-forward
Highest latency
All errors filtered

Adaptive Cut Through

- Kombinasi antara *cut through* dan *store and forward*
  - Switch menggunakan *cut-through* sampai tingkat error tertentu
  - Lalu switch akan menggunakan *store and forward*

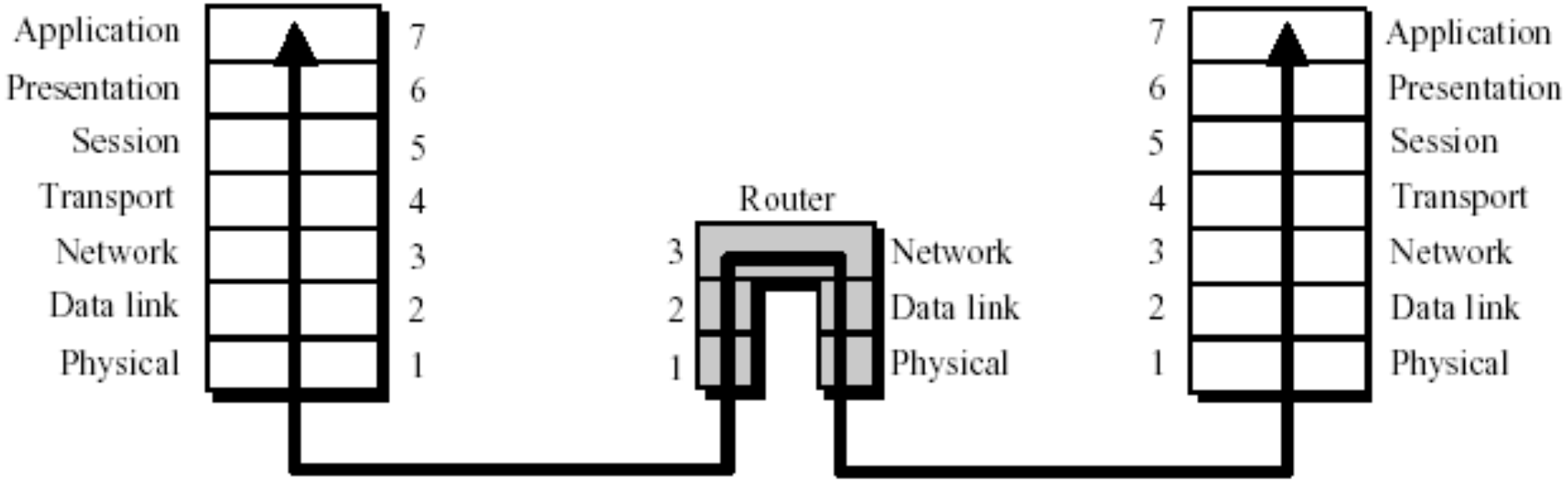
Result

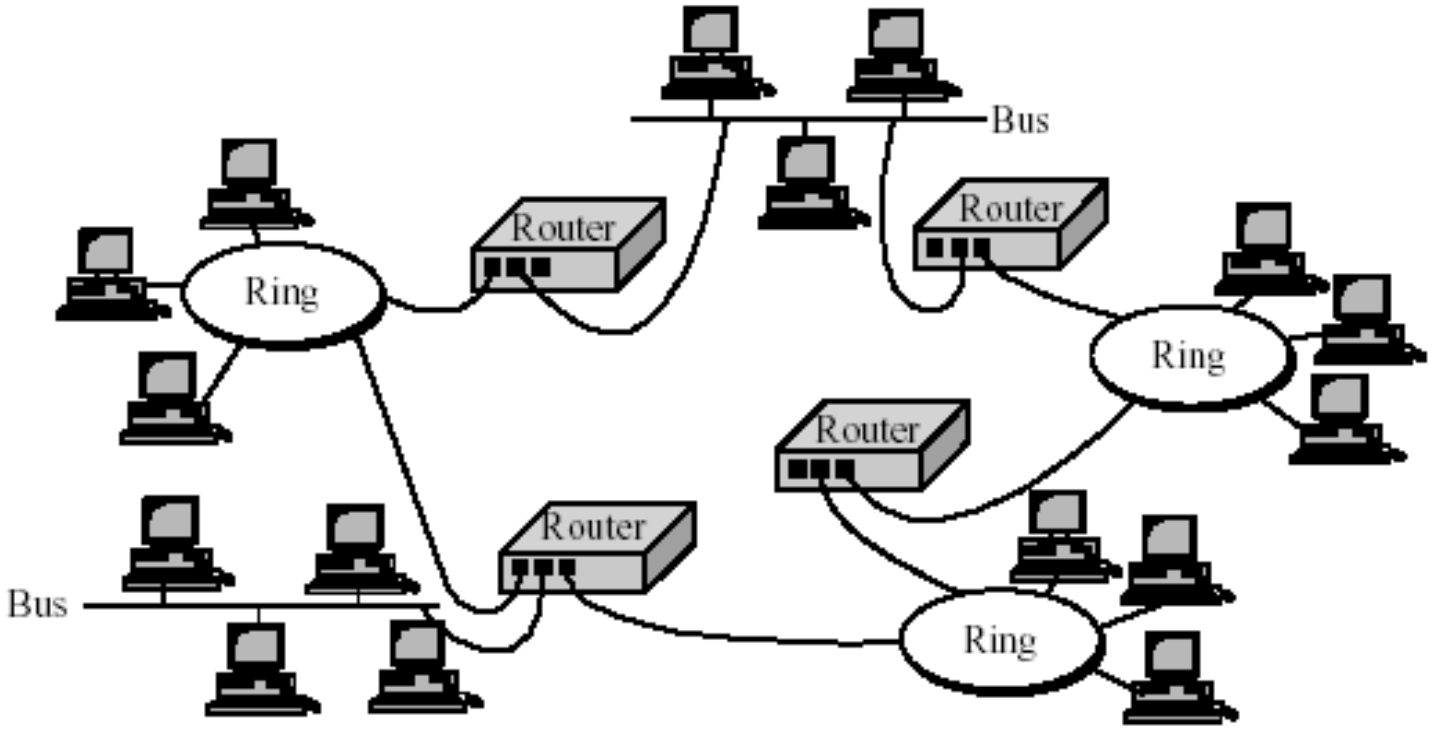
Notes

- **Spanning Tree Protocol** disingkat menjadi STP, Merupakan bagian dari standard IEEE 802.1 untuk kontrol media akses.
- Berfungsi sebagai protocol untuk pengaturan koneksi dengan menggunakan algoritma spanning tree.
- Kelebihan STP dapat menyediakan system jalur backup & juga mencegah loop yang tidak diinginkan pada jaringan yang memiliki beberapa jalur menuju ke satu tujuan dari satu host. Loop terjadi bila ada route/jalur alternative diantara host-host.
- Untuk menyiapkan jalur back up, STP membuat status jalur back up menjadi stand by atau diblock. STP hanya membolehkan satu jalur yang active (fungsi pencegahan loop) diantara dua host namun menyiapkan jalur back up bila jalur utama terputus.

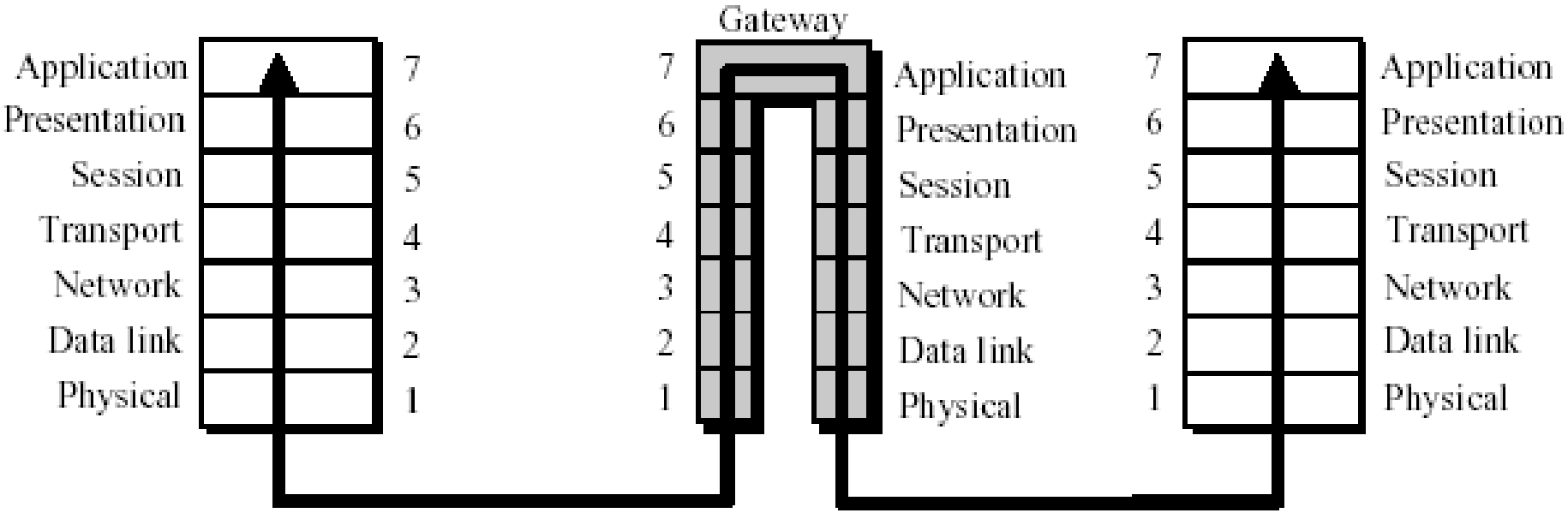
- Bila "cost" STP berubah atau ada jalur yang terputus, algoritma spanning tree merubah topology spanning tree dan mengaktifkan jalur yang sebelumnya stand by.
- Spanning tree memungkinkan desain jaringan untuk memasukkan cadangan (berlebihan) link untuk memberikan jalur cadangan otomatis jika sebuah link aktif gagal, tanpa bahaya jembatan loop, atau kebutuhan untuk manual mengaktifkan / menonaktifkan link cadangan ini.
- Jembatan loop harus dihindari karena mereka mengakibatkan banjir jaringan.
- STP didasarkan pada algoritma yang ditemukan oleh Radia Perlman sambil bekerja untuk Digital Equipment Corporation

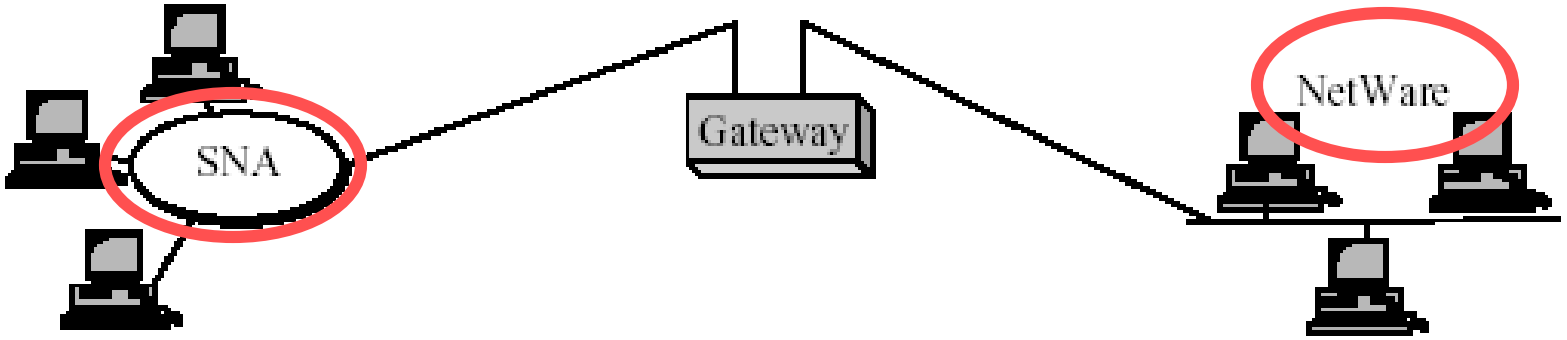
Router


Application
Presentation
Session
Transport
Network
Data link
Physical
7
6
5
4
3
2
1
Router
3
2
1
Network
Data link
Physical
7
6
5
4
3
2
1
Application
Presentation
Session
Transport
Network
Data link
Physical


Bus
Router
Router
Ring
Ring
Router
Router
Bus
Ring

Gateway


Gateway
Application
Presentation
Session
Transport
Network
Data link
Physical
7
6
5
4
3
2
1


SNA
Gateway
NetWare

Medium Access Sublayer

Multiple Access Control (MAC) Protocols

Transmisi Data
Pengkodean Data
Teknik Komunikasi Data Digital
Data Link Control
~~Multiplexing~~
Switching
Medium Access Sublayer
Data link
Network Layer

Medium Access Sublayer

Transmisi Data
Pengkodean Data
Teknik Komunikasi Data Digital
Data Link Control
~~Multiplexing~~
Switching
Medium Access Sublayer
Data link
Network Layer

Design Challenges in WMNs

- Hidden terminal problem
- Exposed terminal problem
- Control and management have to be *distributed* across all nodes.
- Multichannel networks:
  - distributed channel selection
  - channel assignment

Early MAC Schemes

ALOHA

- developed for packet radio nets
- when station has frame, it sends
- then listens for a bit over max round trip time
  - if receive ACK then fine
  - if not, retransmit
  - if no ACK after repeated transmissions, give up
- uses a frame check sequence (as in HDLC)
- frame may be damaged by noise or by another station transmitting at the same time (collision)
- any overlap of frames causes collision
- max utilization 18%

Slotted ALOHA

- time on channel based on uniform slots equal to frame transmission time
  - need central clock (or other sync mechanism)
- transmission begins at slot boundary
- frames either miss or overlap totally
- max utilization 37%
- both have poor utilization
- fail to use fact that propagation time is much less than frame transmission time

CSMA/CD

IEEE 802.3 MAC (Ethernet)

Ethernet (CSMA/CD)

- most widely used LAN standard
- developed by
  - Xerox - original Ethernet
  - IEEE 802.3
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - random / contention access to media

CSMA

- stations soon know transmission has started
- so first listen for clear medium (carrier sense)
- if medium idle, transmit
- if two stations start at the same instant, collision
  - wait reasonable time
  - if no ACK then retransmit
  - collisions occur at leading edge of frame
- max utilization depends on propagation time (medium length) and frame length

Nonpersistent CSMA

- Nonpersistent CSMA rules:
  1. if medium idle, transmit
  2. if medium busy, wait amount of time drawn from probability distribution (retransmission delay) & retry
- random delays reduces probability of collisions
- capacity is wasted because medium will remain idle following end of transmission
- nonpersistent stations are deferential

1-persistent CSMA

- 1-persistent CSMA avoids idle channel time
- 1-persistent CSMA rules:
  1. if medium idle, transmit;
  2. if medium busy, listen until idle; then transmit immediately
- 1-persistent stations are selfish
- if two or more stations waiting, a collision is guaranteed

P-persistent CSMA

- a compromise to try and reduce collisions and idle time
- p-persistent CSMA rules:
  1. if medium idle, transmit with probability p, and delay one time unit with probability (1–p)
  2. if medium busy, listen until idle and repeat step 1
  3. if transmission is delayed one time unit, repeat step 1
- issue of choosing effective value of p to avoid instability under heavy load

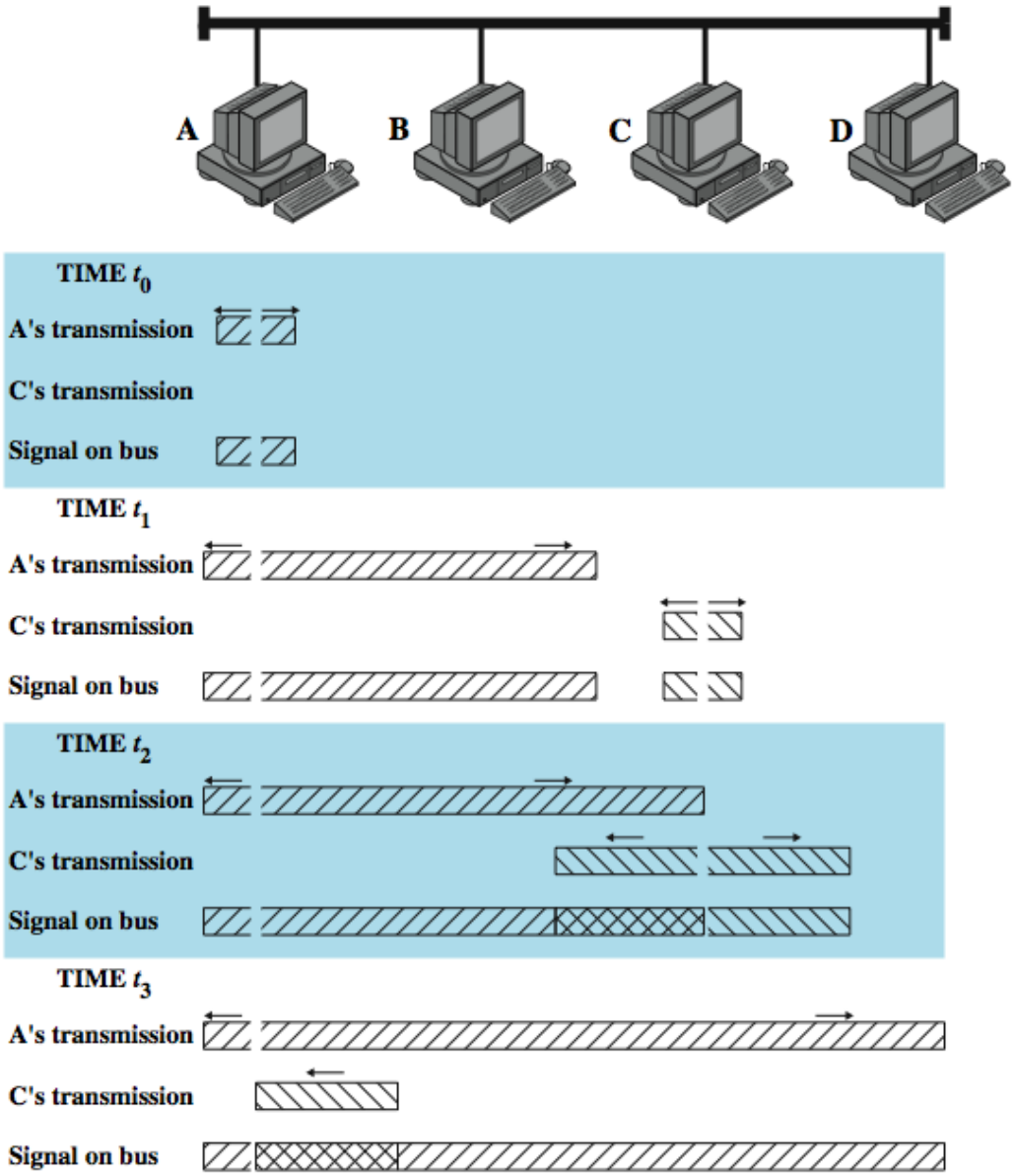
Value of p?

- have n stations waiting to send
- at end of tx, expected no of stations is np
  - if np>1 on average there will be a collision
- repeated tx attempts mean collisions likely
- eventually when all stations trying to send have continuous collisions hence zero throughput
- thus want np<1 for expected peaks of n
  - if heavy load expected, p small
  - but smaller p means stations wait longer

CSMA/CD Description

- with CSMA, collision occupies medium for duration of transmission
- better if stations listen whilst transmitting
- CSMA/CD rules:
  1. if medium idle, transmit
  2. if busy, listen for idle, then transmit
  3. if collision detected, jam and then cease transmission
  4. after jam, wait random time then retry

CSMA/CD Operation



Which Persistence Algorithm?

- IEEE 802.3 uses 1-persistent
- both nonpersistent and p-persistent have performance problems
- 1-persistent seems more unstable than p-persistent
  - because of greed of the stations
  - but wasted time due to collisions is short
  - with random backoff unlikely to collide on next attempt to send

Binary Exponential Backoff

- for backoff stability, IEEE 802.3 and Ethernet both use binary exponential backoff
- stations repeatedly resend when collide
  - on first 10 attempts, mean random delay doubled
  - value then remains same for 6 further attempts
  - after 16 unsuccessful attempts, station gives up and reports error
- 1-persistent algorithm with binary exponential backoff efficient over wide range of loads
- but backoff algorithm has last-in, first-out effect

Collision Detection

- on baseband bus
  - collision produces higher signal voltage
  - collision detected if cable signal greater than single station signal
  - signal is attenuated over distance
  - limit to 500m (10Base5) or 200m (10Base2)
- on twisted pair (star-topology)
  - activity on more than one port is collision
  - use special collision presence signal

CSMA/CA

IEEE 802.11 MAC

Medium Access Control

- MAC layer covers three functional areas
  - reliable data delivery
  - access control
  - security

Reliable Data Delivery

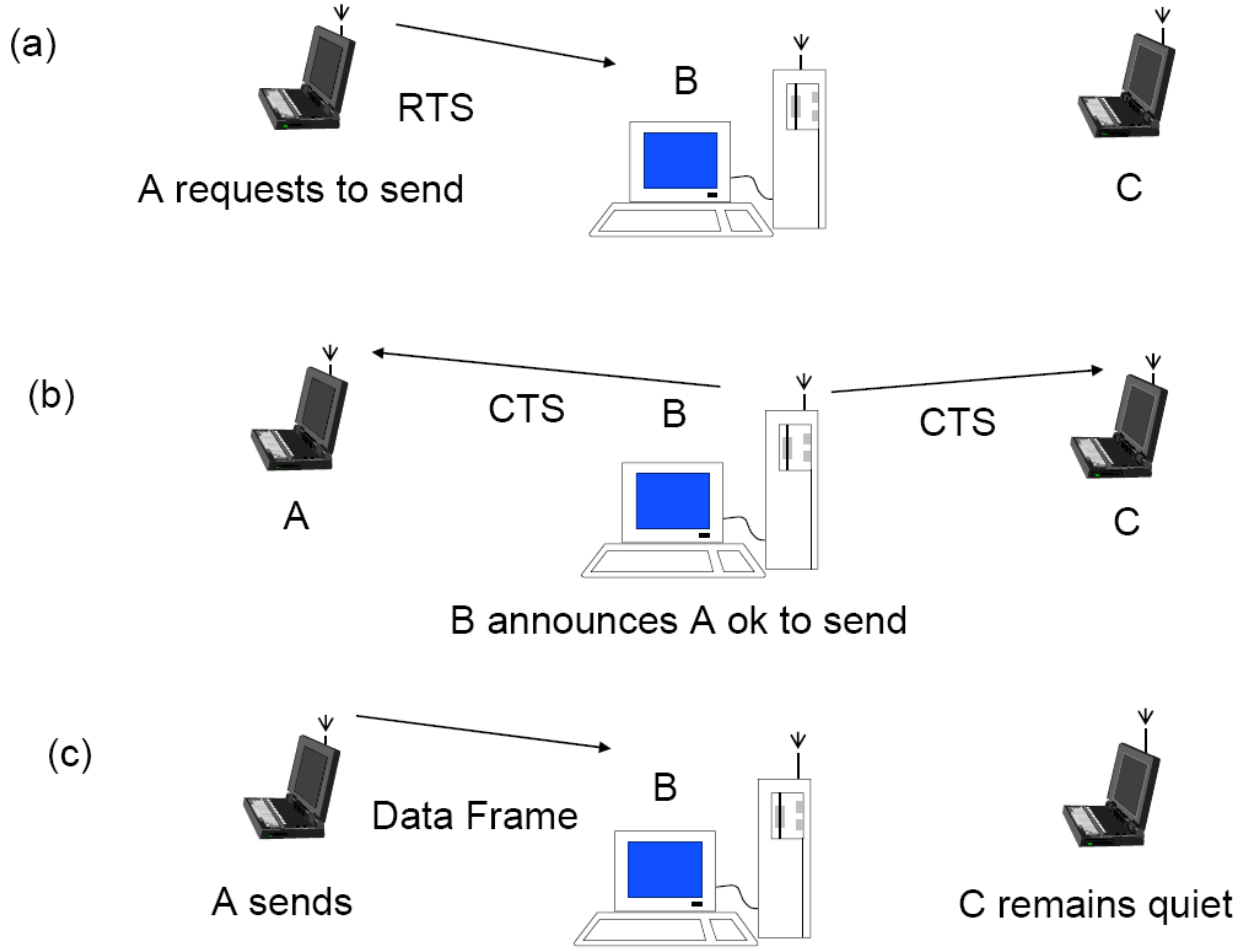
- 802.11 physical / MAC layers unreliable
  - noise, interference, and other propagation effects result in loss of frames
  - even with error-correction codes, frames may not successfully be received
- can be dealt with at a higher layer, e.g. TCP
- more efficient to deal with errors at MAC level
- 802.11 includes frame exchange protocol
  - station receiving frame returns acknowledgment (ACK) frame
  - exchange treated as atomic unit
  - if no ACK within short period of time, retransmit

Four Frame Exchange

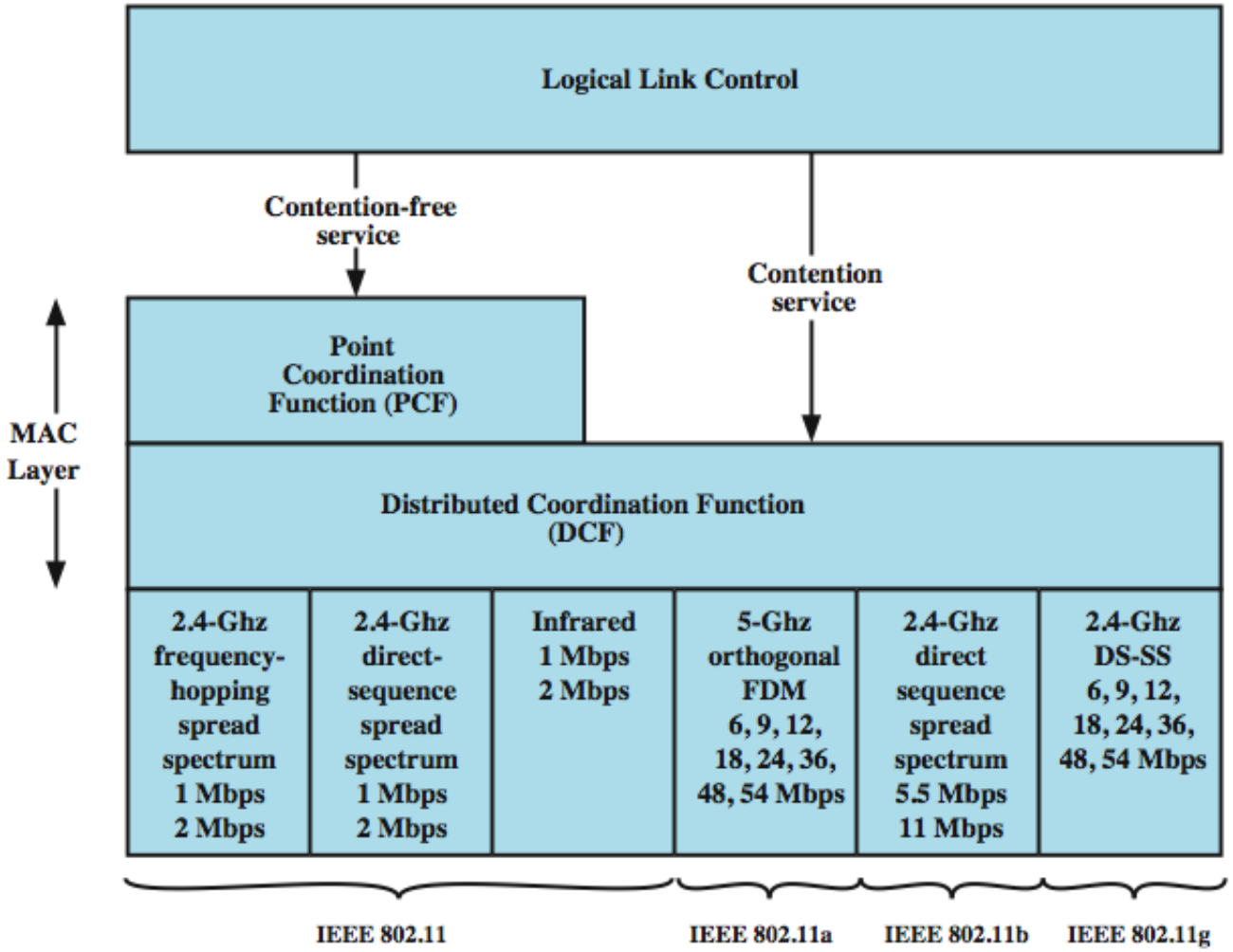
- Can use four-frame exchange for better reliability
  - source issues a Request to Send (RTS) frame to dest
  - destination responds with Clear to Send (CTS)
  - after receiving CTS, source transmits data
  - destination responds with ACK
- RTS alerts all stations within range of source that exchange is under way
- CTS alerts all stations within range of destination
- Other stations don’t transmit to avoid collision
- RTS/CTS exchange is required function of MAC but may be disabled

CSMA/CA

Fig. 6.70 (Leon-Garcia)



Media Access Control

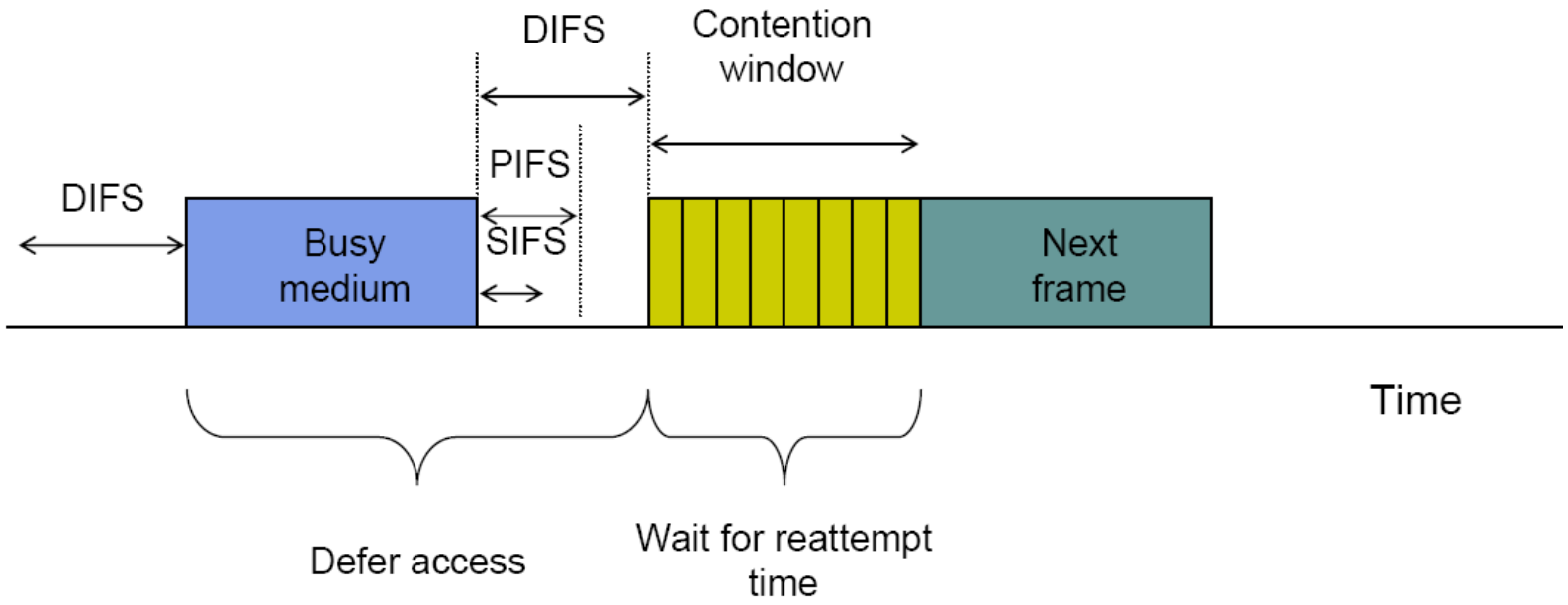


Distributed Coordination Function

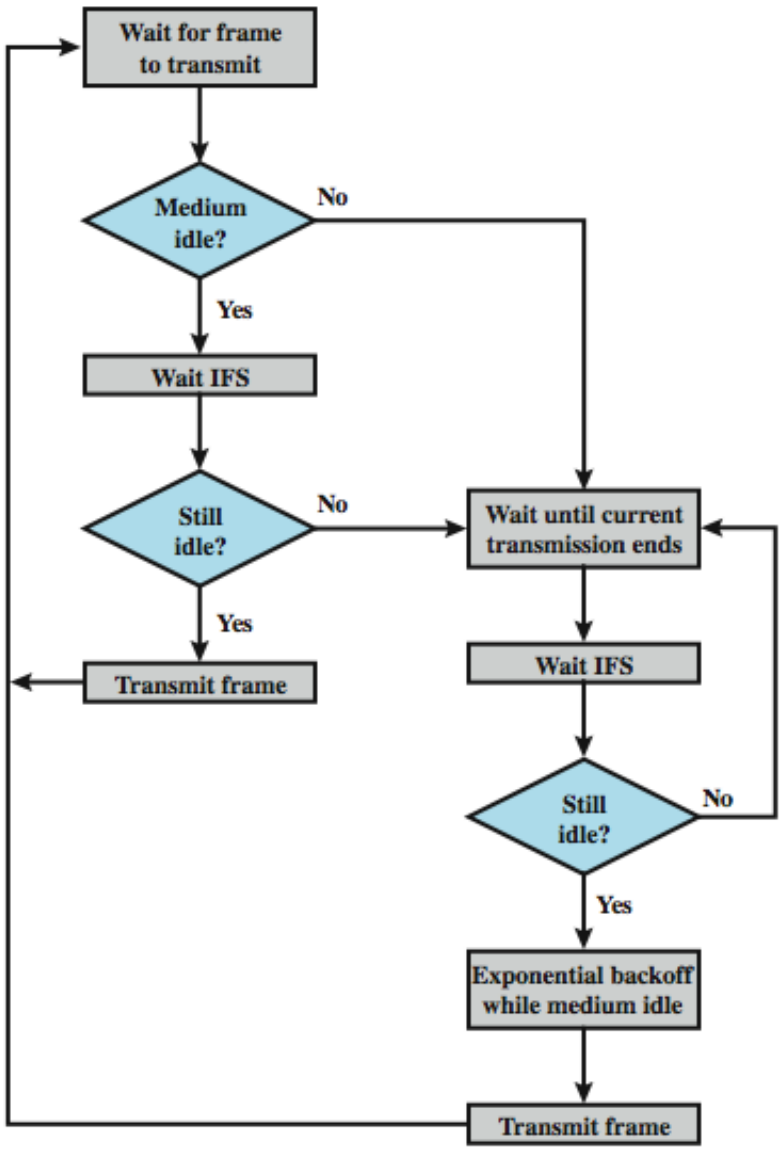
- DCF sublayer uses CSMA
  - if station has frame to send it listens to medium
  - if medium idle, station may transmit
  - else waits until current transmission complete
- No collision detection since on wireless network
- DCF includes delays that act as a priority scheme

Basic CSMA/C operations

Fig. 6.69 (Leon-Garcia)

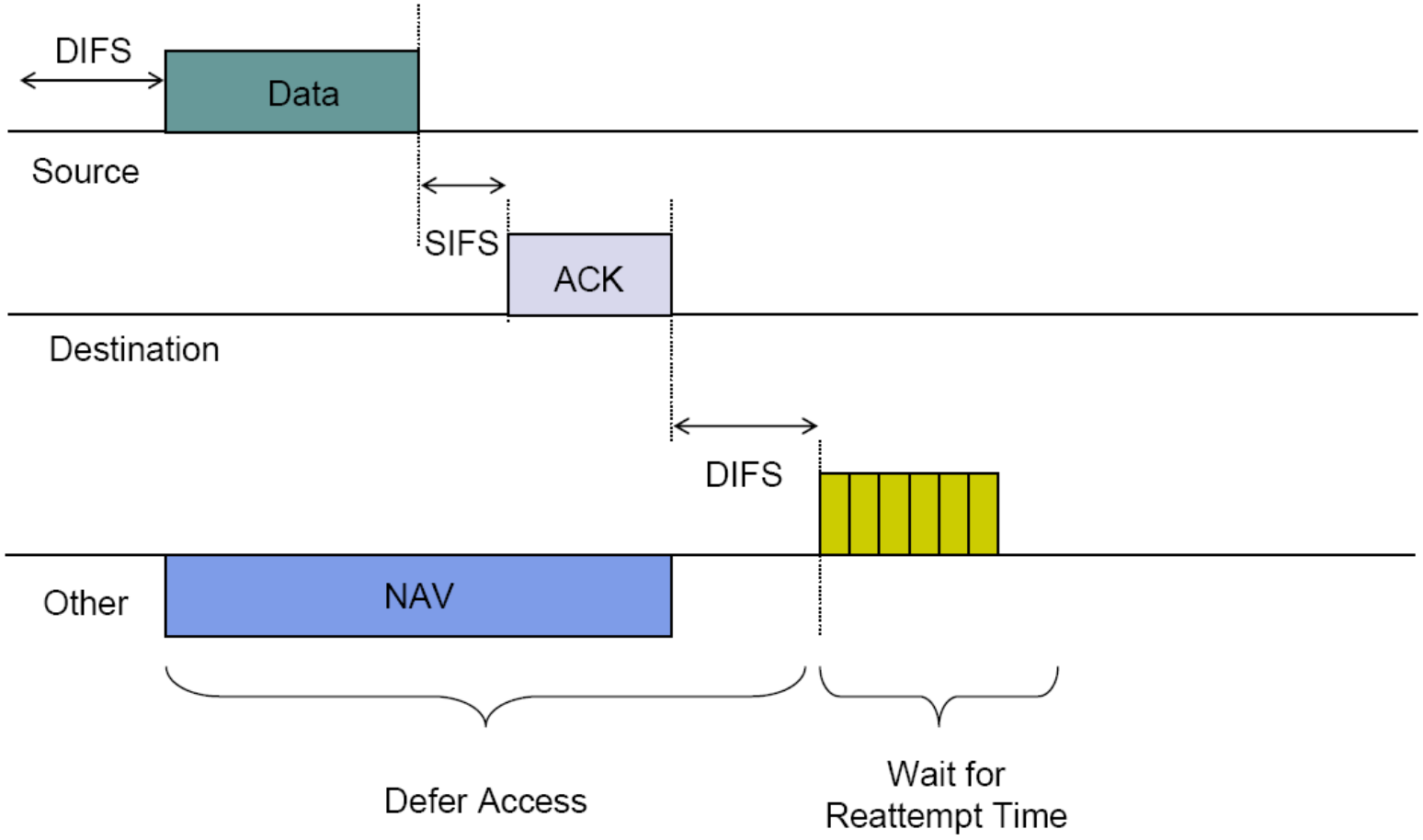


IEEE 802.11 Medium Access Control Logic



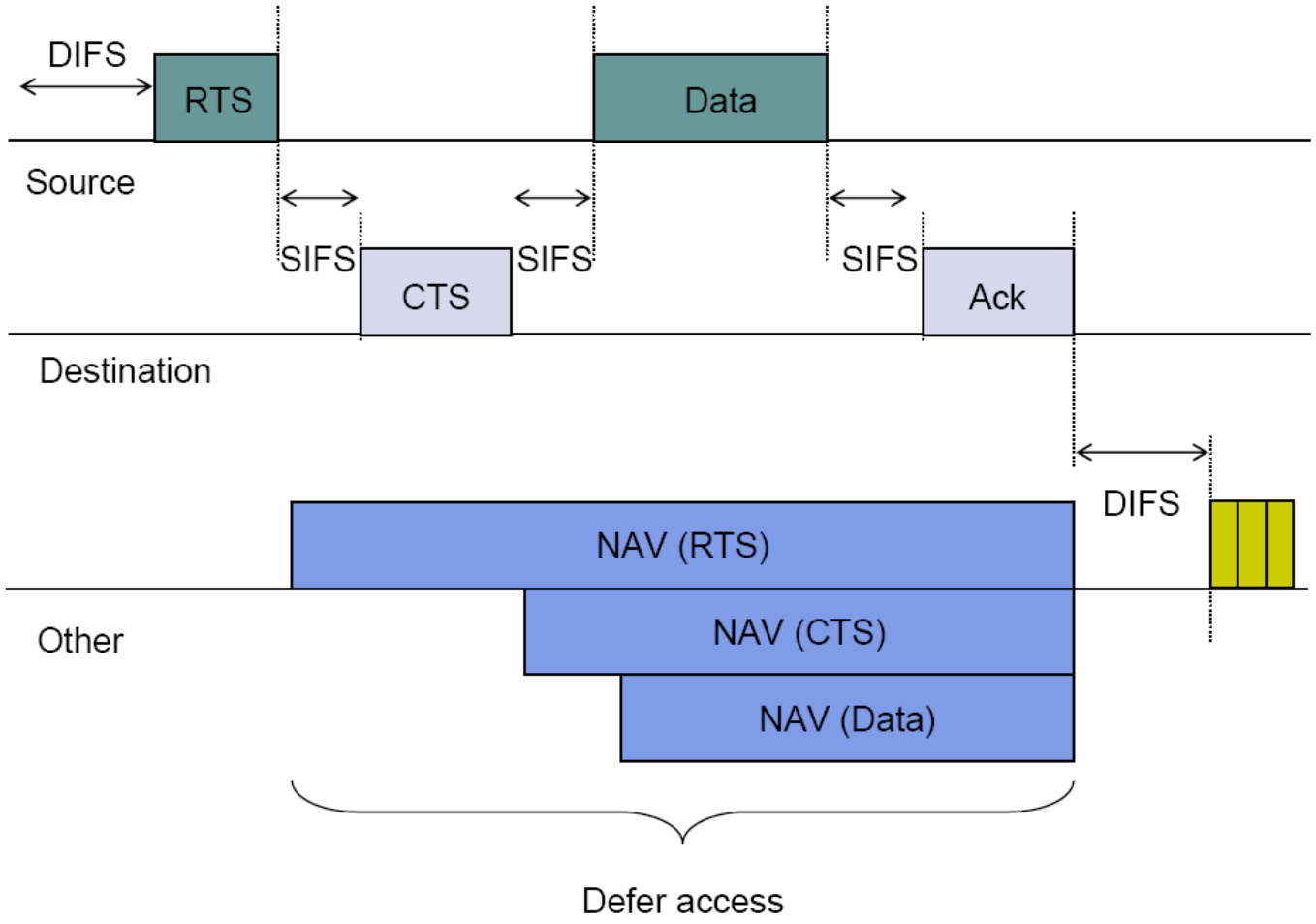
Transmission RTS/CTS

Fig. 6.71 (Leon-Garcia)



Transmission wit RTS/CTS

Fig. 6.72 (Leon-Garcia)



Priority IFS Values

- SIFS (short IFS)
  - for all immediate response actions (see later)
- PIFS (point coordination function IFS)
  - used by the centralized controller in PCF scheme when issuing polls
- DIFS (distributed coordination function IFS)
  - used as minimum delay for asynchronous frames contending for access

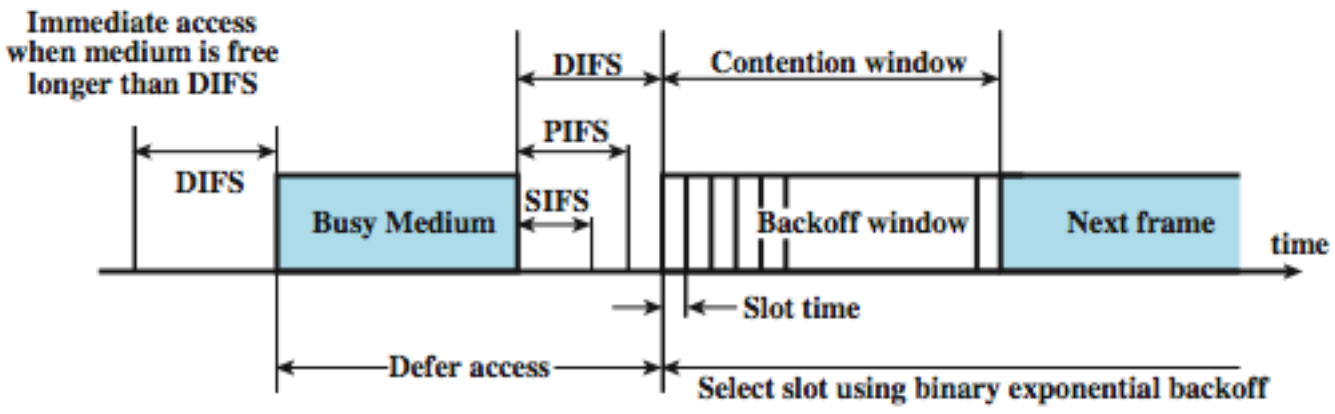
SIFS Use

- SIFS gives highest priority
  - over stations waiting PIFS or DIFS time
- SIFS used in following circumstances:
  - Acknowledgment (ACK)
    - station responds with ACK after waiting SIFS gap
    - for efficient collision detect & multi-frame transmission
  - Clear to Send (CTS)
    - station ensures data frame gets through by issuing RTS
    - and waits for CTS response from destination
  - Poll response
    - see Point coordination Function (PCF) discussion next

PIFS and DIFS Use

- PIFS used by centralized controller
  - for issuing polls
  - has precedence over normal contention traffic
  - but not SIFS
- DIFS used for all ordinary asynchronous traffic

IEEE 802.11 MAC Timing
Basic Access Method



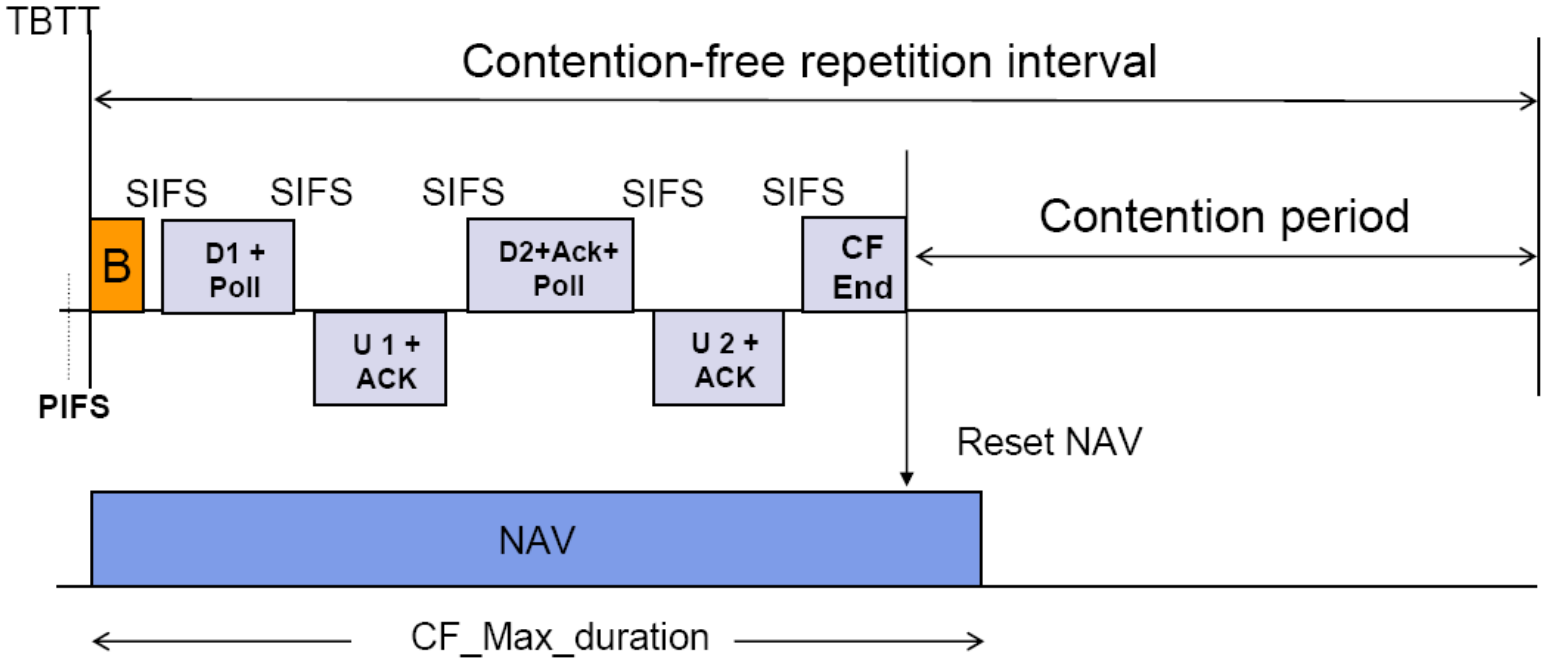
(a) Basic Access Method

Point Coordination Function (PCF)

- alternative access method implemented on top of DCF
- polling by centralized polling master (point coordinator)
- uses PIFS when issuing polls
- point coordinator polls in round-robin to stations configured for polling
- when poll issued, polled station may respond using SIFS
- if point coordinator receives response, it issues another poll using PIFS
- if no response during expected turnaround time, coordinator issues poll
- coordinator could lock out async traffic by issuing polls
- have a superframe interval defined
- not suitable for use in WMNs

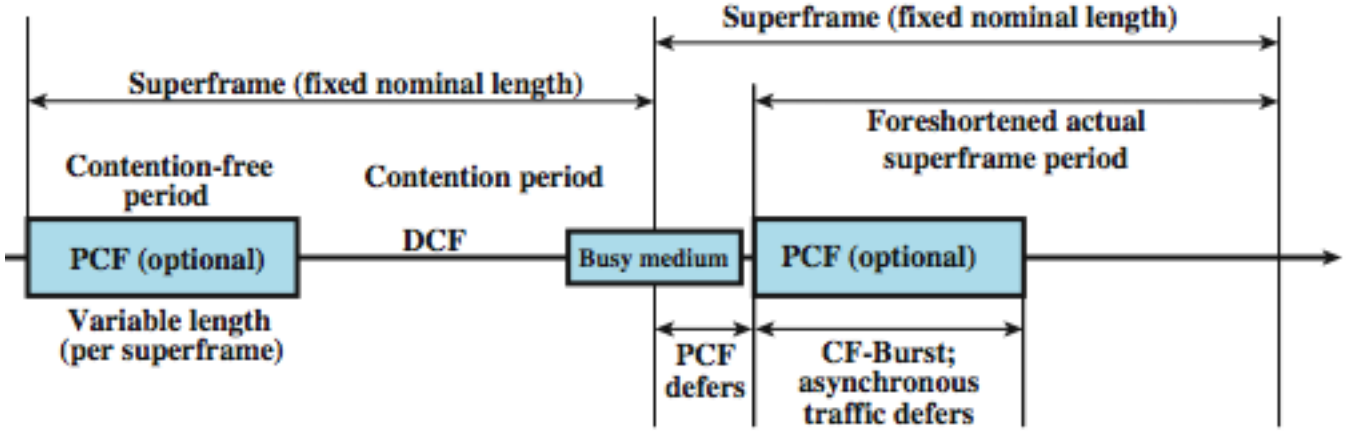
Point coordin
frame transfe

Fig. 6.73 (Leon-Garcia)



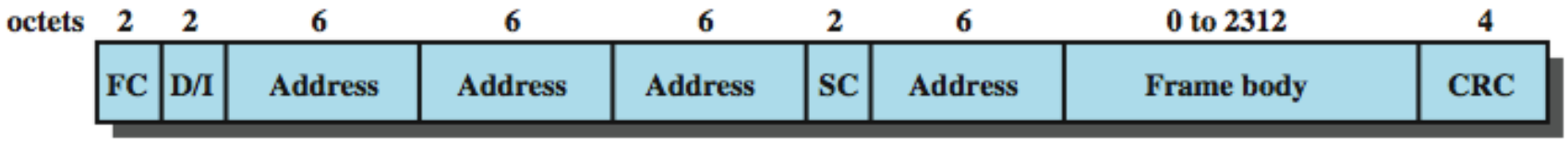
D1, D2 = frame sent by point coordinator
U1, U2 = frame sent by polled station
TBTT = target beacon transmission time
B = beacon frame

PCF Superframe Timing



(b) PCF Superframe Construction

IEEE 802.11 MAC Frame Format



FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

Control Frames

- Power Save-Poll (PS-Poll)
  - request AP transmit buffered frame when in power-saving mode
- Request to Send (RTS)
  - first frame in four-way frame exchange
- Clear to Send (CTS)
  - second frame in four-way exchange
- Acknowledgment (ACK)
- Contention-Free (CF)-end
  - announces end of contention-free period part of PCF
- CF-End + CF-Ack:
  - acknowledges CF-end to end contention-free period and release stations from associated restrictions

Data Frames – Data Carrying

- eight data frame subtypes, in two groups
- first four carry upper-level data
- Data
  - simplest data frame, contention or contention-free use
- Data + CF-Ack
  - carries data and acknowledges previously received data during contention-free period
- Data + CF-Poll
  - used by point coordinator to deliver data & req send
- Data + CF-Ack + CF-Poll
  - combines Data + CF-Ack and Data + CF-Poll

Data Frames – Not Data Carrying

- other four data frames do not carry user data
- Null Function
  - carries no data, polls, or acknowledgments
  - carries power mgmt bit in frame control field to AP
  - indicates station is changing to low-power state
- other three frames (CF-Ack, CF-Poll, CF-Ack + CF-Poll) same as corresponding frame in preceding list but without data

Management Frames

- used to manage communications between stations and APs
- such as management of associations
  - requests, response, reassociation, dissociation, and authentication

IEEE 802.11e MAC

802.11e MAC

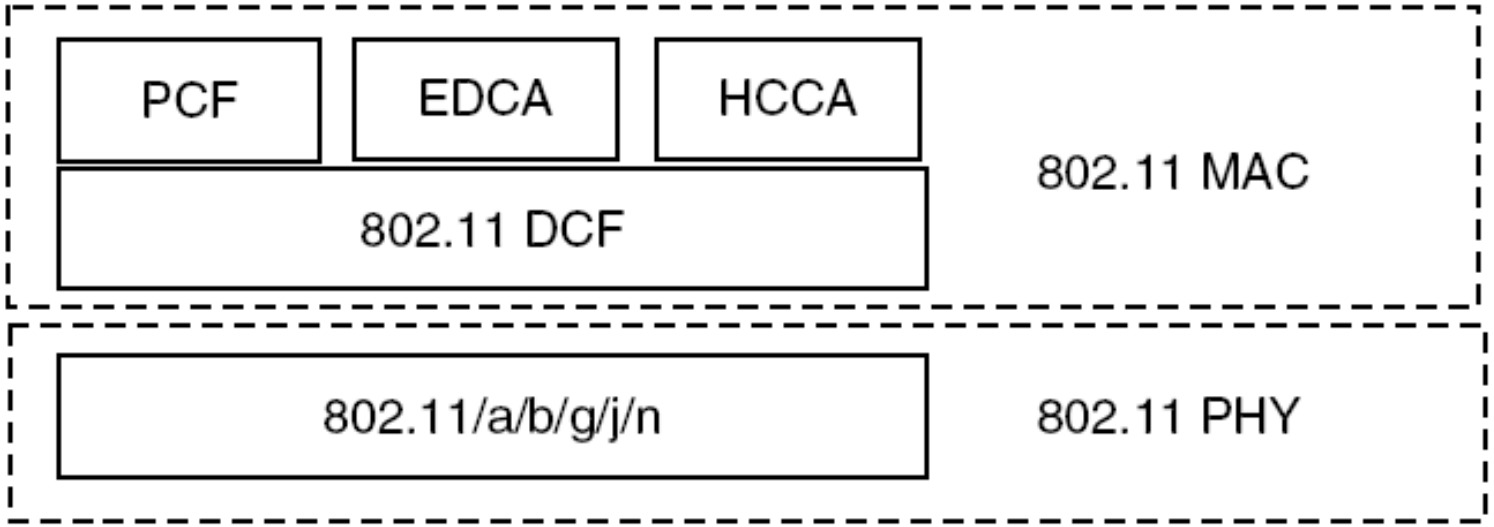
- Defines a number of QoS enhancements to 802.11 MAC
- See short descriptions at wikipedia.org

QoS Limitations of 802.11

- DCF (Distributed Coordination Function)
  - Only support best-effort services
  - No guarantee in bandwidth, packet delay and jitter
  - Throughput degradation in the heavy load
- PCF (Point Coordination Function)
  - Inefficient central polling scheme
  - Unpredictable beacon frame delay due to incompatible cooperation between CP and CFP modes
  - Transmission time of the polled stations is unknown

Overview of 802.11e

- Formed in Sept. 1999.
- The first draft was available in late 2001
- Aims to support both IntServ and DiffServ
- New QoS mechanisms – HCF (Hybrid Coordination Function): 2 modes
  - EDCA (Enhanced Distributed Channel Access)
    - contention-based, distributed
  - HCCA (HCF controlled channel access)
    - requires a central control entity and synchronization among nodes
    - not suitable for WMNs
- Backward compatible with DCF and PCF



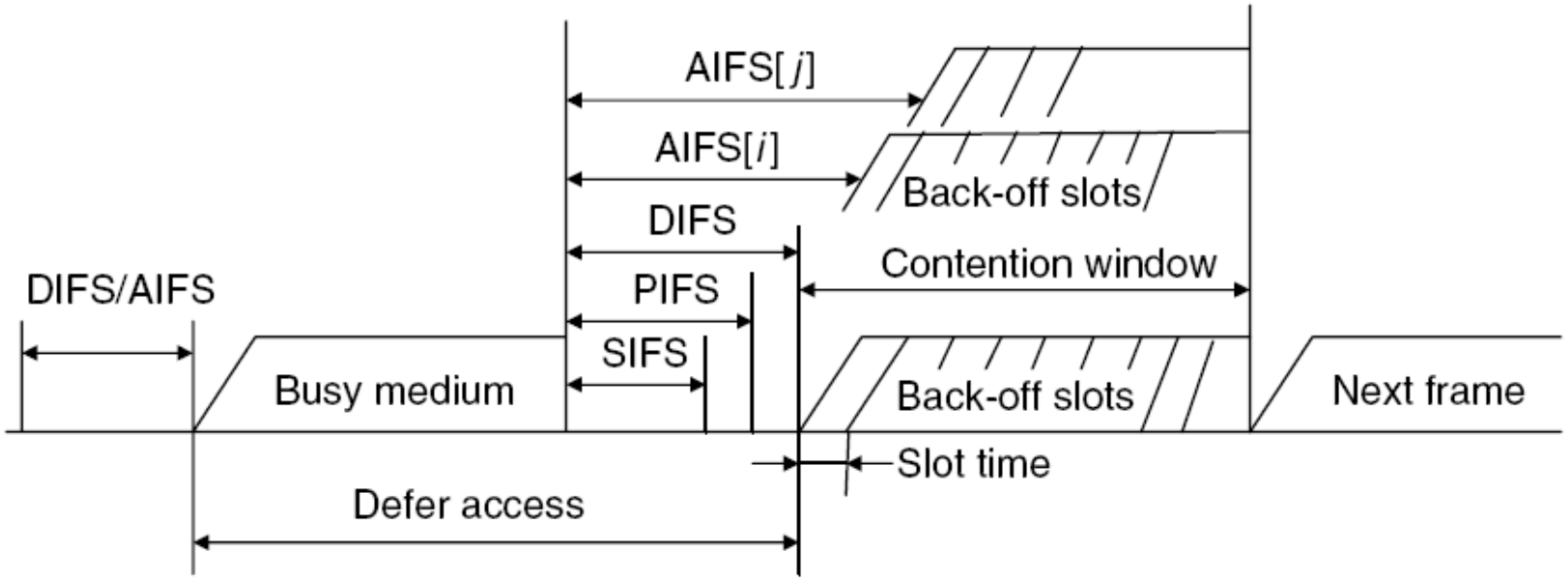
802.11e MAC architecture

Wireless Multimedia Extensions (WME)

- a.k.a Wi-Fi Multimedia (WMM)
- subset of 802.11e to be implemented by the industry
- 4 access categories (ACs): voice, video, best effort, and background
- no guaranteed throughput though
- suitable for simple applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones

EDCA

- enhances the original DCF by providing prioritized medium access based on access categories (ACs)
- IEEE 802.11e defines four ACs, each having its own queue and set of QoS parameters
- priority between ACs is realized by setting different values for the EDCA parameters
  - arbitration interframe space number (AIFSN),
  - minimum contention window (CWmin),
  - maximum contention window (CWmax),
  - transmission opportunity (TXOP) limit



Relationship of different IFSs

AC	CW_{min}	CW_{max}	AIFSN	TXOP Limit For 11b PHY	TXOP Limit For 11a PHY
Background (AC_BK)	CW_{min}	CW_{max}	7	0	0
Best effort (AC_BE)	CW_{min}	CW_{max}	3	0	0
Video (AC_VI)	$(CW_{min} + 1)/2 - 1$	CW_{min}	2	6.016 ms	3.008 ms
Voice (AC_VO)	$(CW_{min} + 1)/4 - 1$	$(CW_{min} + 1)/2 - 1$	2	3.264 ms	1.504 ms

Default EDCA parameter set

References

- WMN textbook, 5.1– 5.2
- Communication Networks by A. Leon-Garcia
- Data & Computer Communications by William Stallings

Multiple Access Control (MAC) Protocols

Copyright © The McGraw-Hill Companies, Inc. Permission required for reproduction or display.

Multiple Access

- **Broadcast link** used in LAN consists of multiple sending and receiving nodes connected to or use a single shared link

Broadcast links Examples

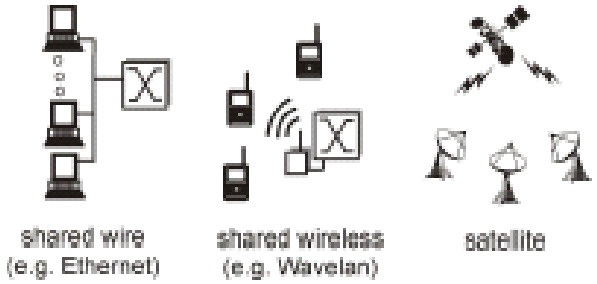
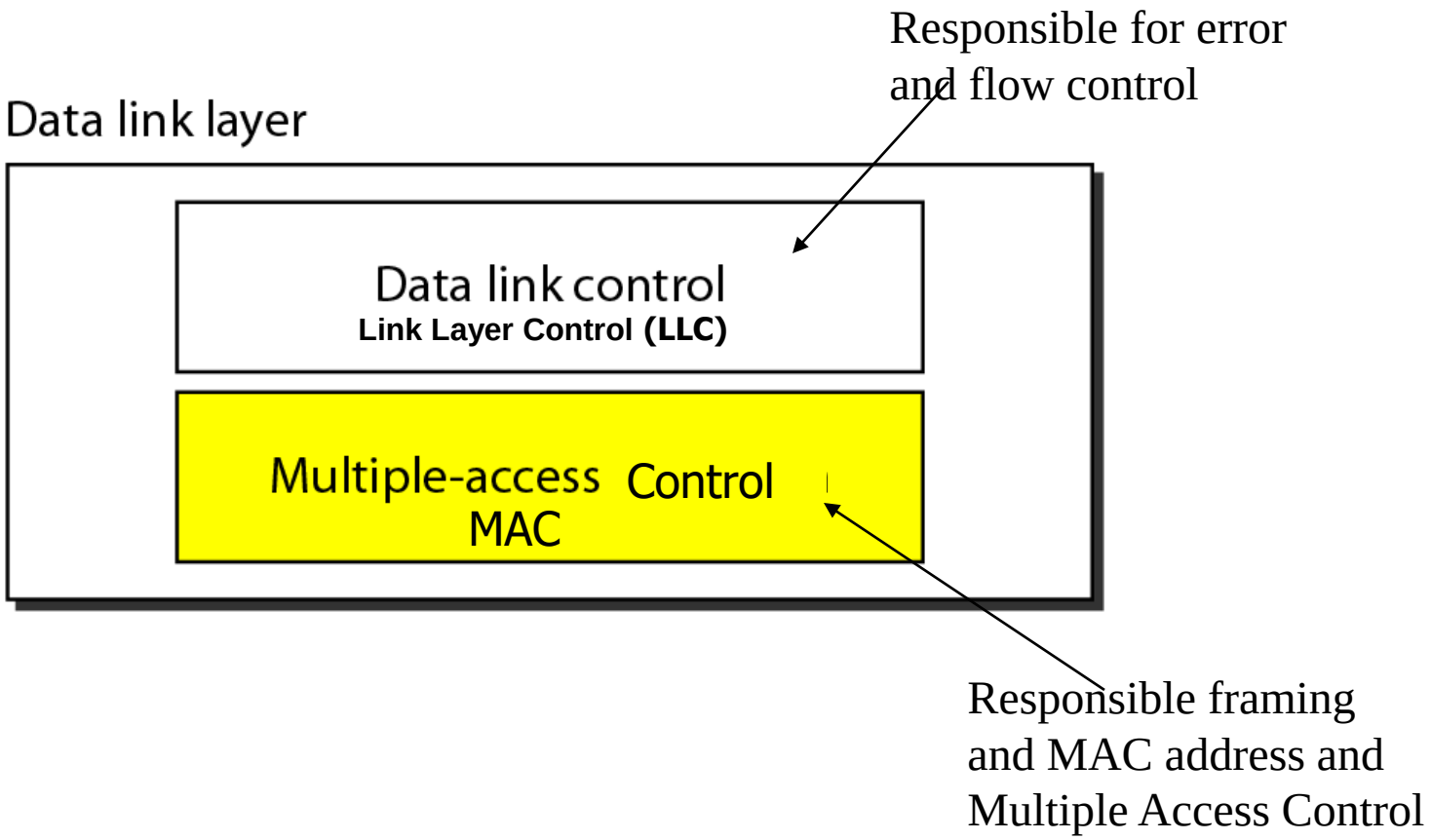


Figure 12.1 *Data link layer divided into two functionality-oriented sublayers*



Multiple Access

- **Problem**: When two or more nodes transmit at the same time, their frames <u>will collide</u> and the link bandwidth is **wasted** during collision
  - How to coordinate the access of multiple sending/receiving nodes to the shared link**???**

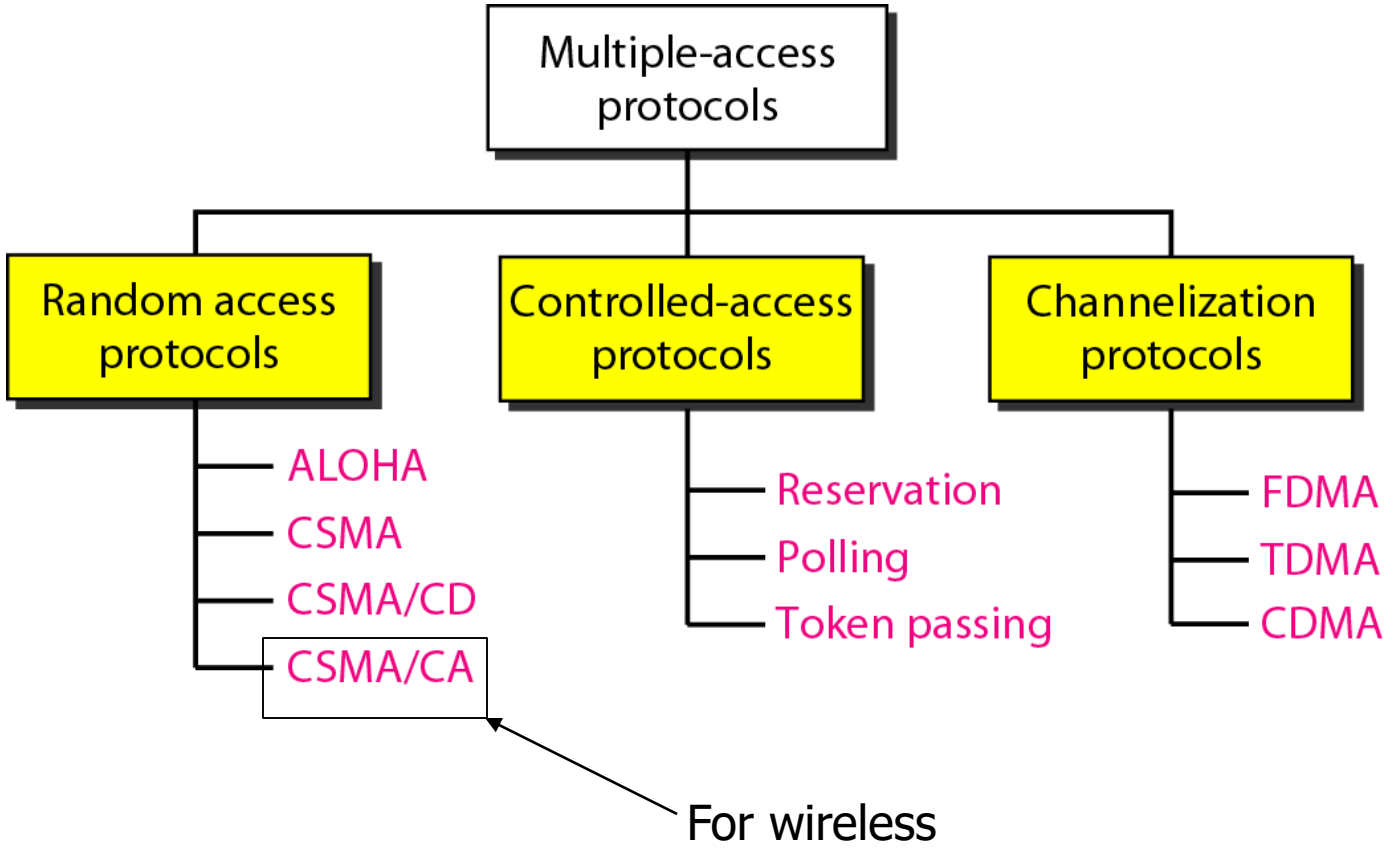
- **Solution**: We need a **protocol** to coordinate the transmission of the active nodes

- These protocols are called **Medium or Multiple Access Control (MAC) Protocols** belong to a **sublayer** of the data link layer called **MAC** (Medium Access Control)

- What is expected from Multiple Access Protocols:
  - Main task is to **minimize collisions** in order to **utilize the bandwidth** by:
    - Determining **when** a station can use the link (medium)
    - **what** a station should do when the link is **busy**
    - **what** the station should do when it is involved in **collision**

Terms

- **Throughput:** is the amount of data moved successfully from one place to another in a given time period.
- **propagation delay:** is the amount of time it takes for the head of the signal to travel from the sender to the receiver.


Multiple-access protocols
Random access protocols
Controlled-access protocols
Channelization protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token passing
FDMA
TDMA
CDMA
For wireless

Random Access

- Random Access (or contention) Protocols:
  - No station is superior to another station and none is assigned the control over another.
  - A station with a frame to be transmitted can use the link directly based on a procedure defined by the protocol to make a decision on whether or not to send.

ALOHA

ALOHA Random Access Scheme

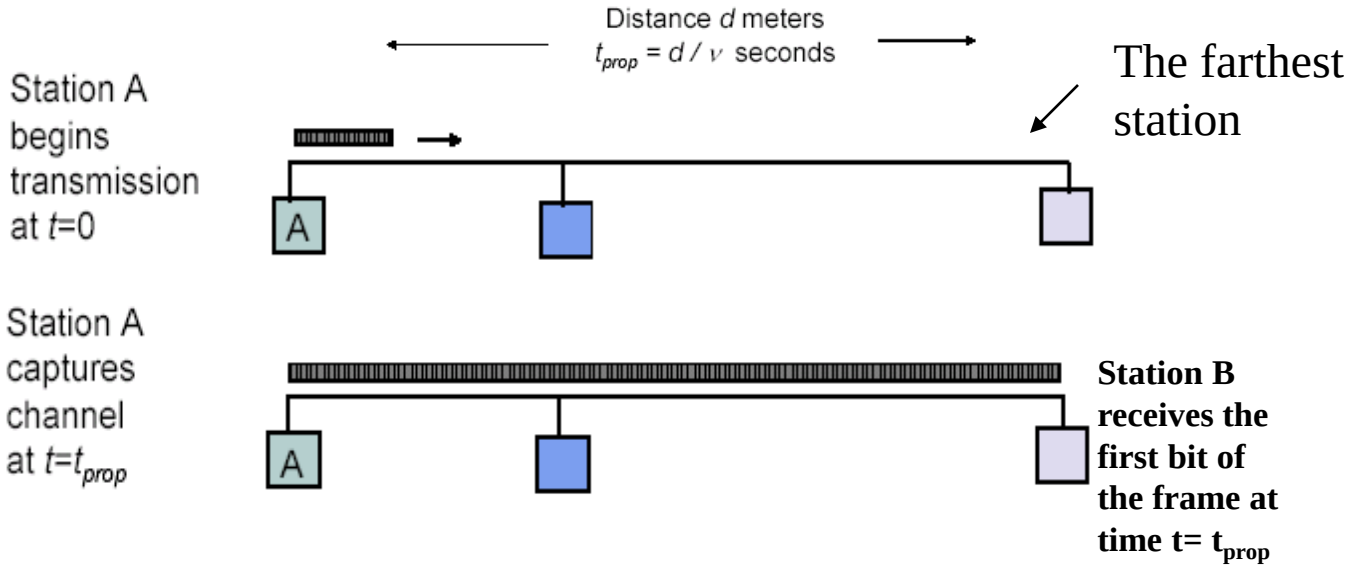
- It was developed at the University of Hawaii in the early 1970s to connect computers situated on different Hawaiian islands. The computers of the ALOHA network transmit on the same radio channel whenever they have a packet to transmit.
- From time-to-time packet transmission will collide, but these can be treated as transmission errors, and recovery can take place by retransmission. When traffic is very light, the probability of collision is very small, and so retransmissions need to be carried out infrequently.
- ALOHA scheme requires stations to use a **random retransmission time.** (This randomization is intended to spread out the retransmission and reduces the likelihood of additional collisions between stations.)
- ALOHA is the father of multiple access protocols.

1 Pure ALOHA

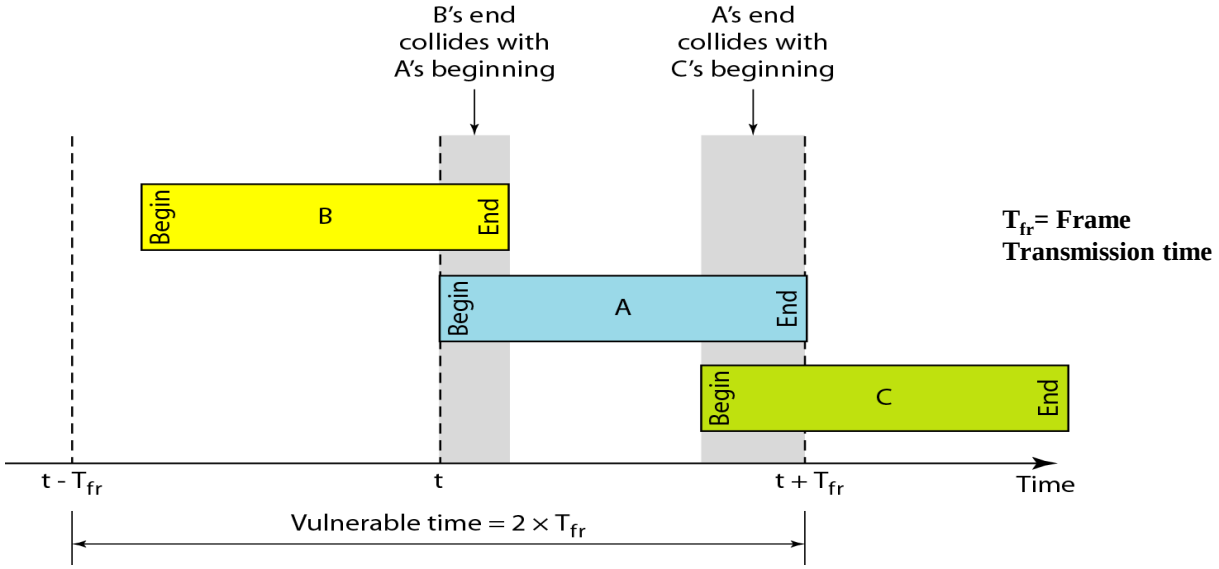
- All frames from any station are of fixed length (L bits)
- Stations transmit at equal transmission time (all stations produce frames with equal frame lengths).
- A station that has data can transmit at any time
- After transmitting a frame, the sender waits for an acknowledgment for an amount of time (**time out**) equal to the maximum round-trip propagation delay
- Time out= 2* t_{prop}
- If no ACK was received, sender assumes that the frame or ACK has been destroyed and resends that frame after it waits for a random amount of time
- If station fails to receive an ACK after repeated transmissions, it gives up.
- Channel utilization or efficiency or Throughput is the percentage of the transmitted frames that arrive successfully (without collisions)

Maximum Propagation Delay

- **Maximum propagation delay**(t_{prop}): time it takes for a bit of a frame to travel between the **<u>two most widely</u>** separated stations.



Critical time for pure ALOHA protocol

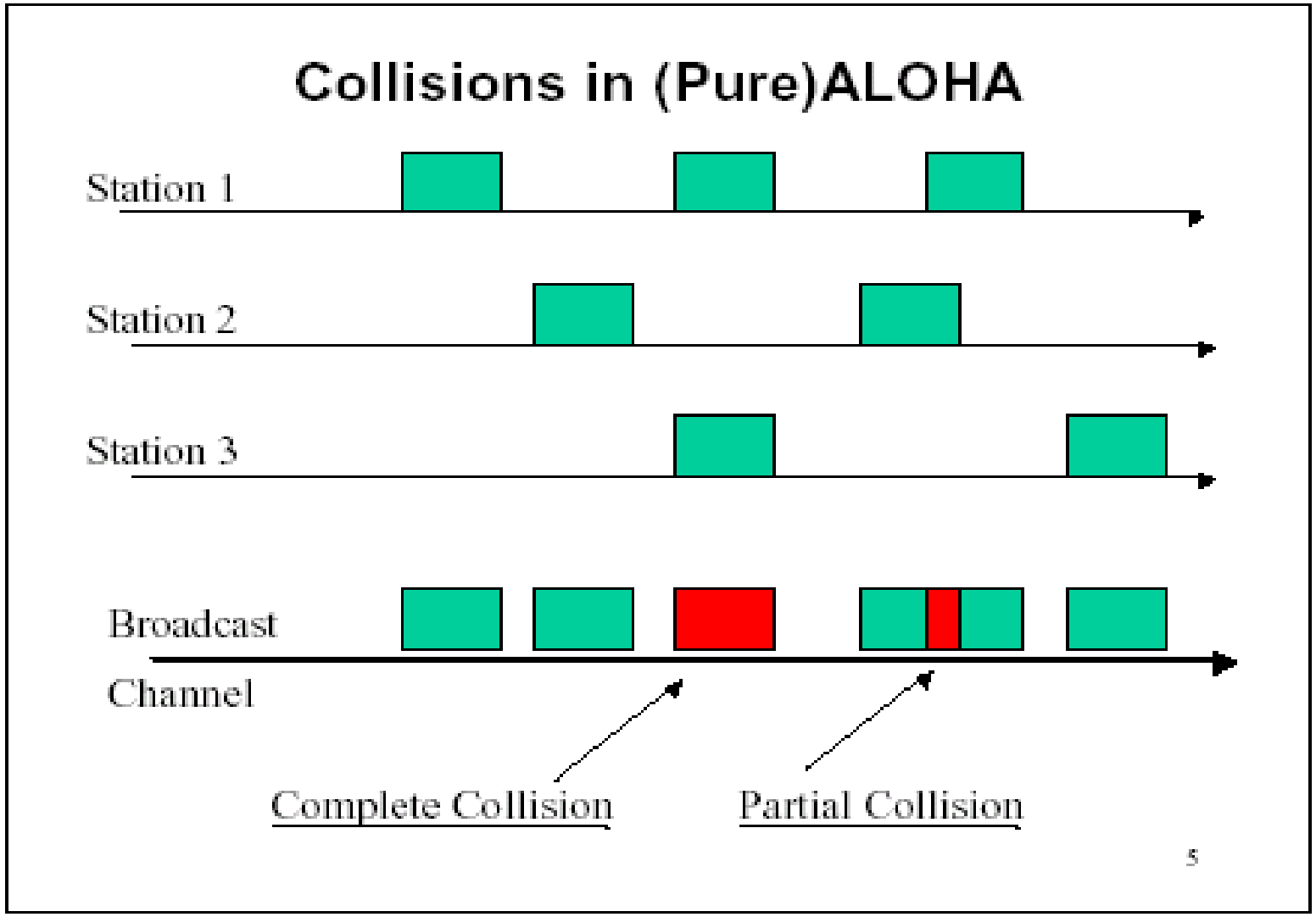


If the frame <u>transmission time</u> is T_{fr}, then the vulnerable time is = 2 T_{fr}.

This means no station should send during the T_{fr} before this station starts transmission and no station should start sending during the T-sec period that the current station is sending.

Pure ALOHA

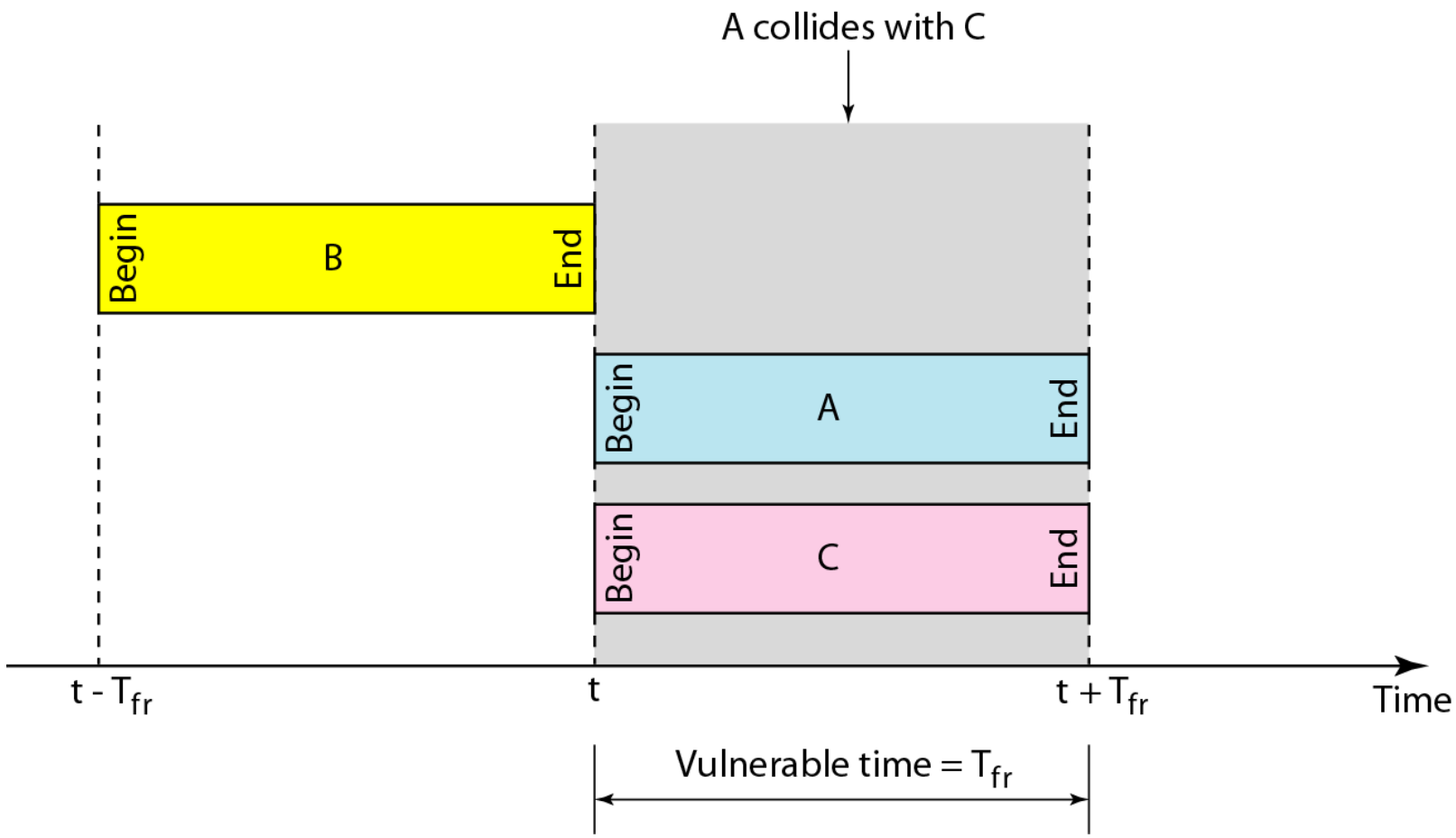
In pure ALOHA, frames are transmitted at completely **random** times.



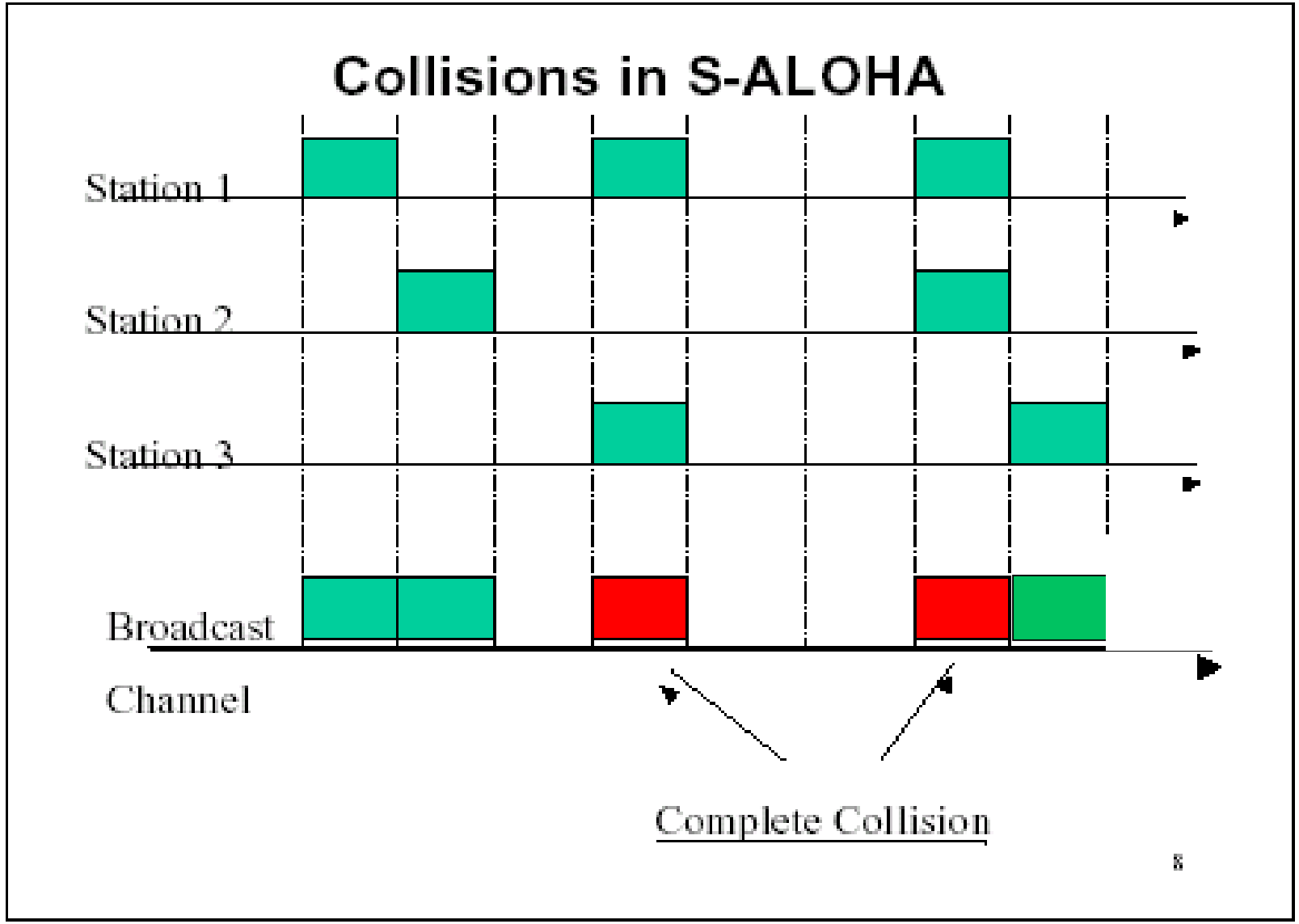
2 Slotted ALOHA

- Time is divided into slots equal to a frame transmission time (Tfr)
- A station can transmit at the beginning of a slot only.
- If a station misses the beginning of a slot, it has to wait until the beginning of the next time slot.
- A central clock or station informs all stations about the start of a each slot

In danger time for slotted ALOHA protocol



Random Access – Slotted ALOHA



ALOHA

- Advantage of ALOHA protocols
  - A node that has frames to be transmitted can **transmit continuously** at the **full rate of channel (R bps)** if it is the <u>only node</u> with frames
  - Simple to be implemented
  - No master station is needed to control the medium
- Disadvantage
  - If (M) nodes want to transmit, many collisions can occur and the rate allocated for each node will **not be on average R/M bps**
  - This causes low channel utilization

BASIS FOR COMPARISON	Pure ALOHA	Slotted ALOHA
Frame Transmission	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
Time	In Pure ALOHA the time is continuous.	In Slotted ALOHA the time is discrete.
Throughput	The maximum throughput occurs at G = 1/2 which is 18%	The maximum throughput occurs at G = 1 which is 37%.
Danger Time	$= 2\ T_{fr}$	$= T_{fr}$

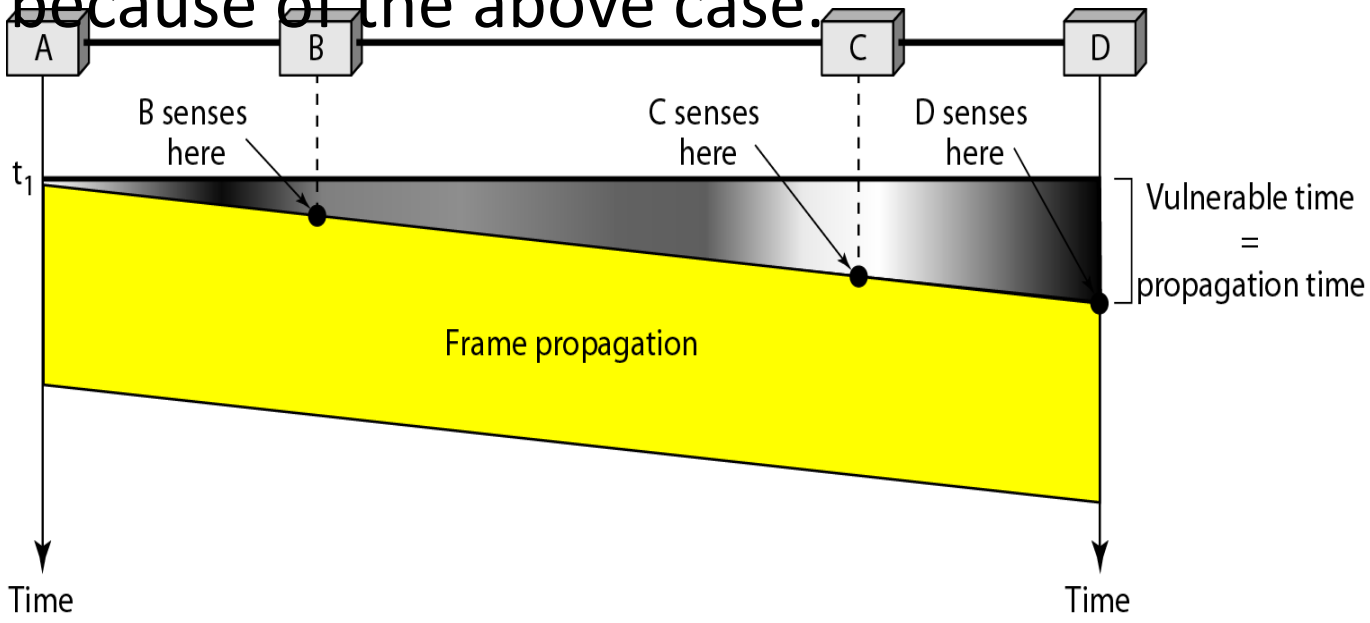
Random Access – Carrier Sense Multiple Access (CSMA)

Random Access – Carrier Sense Multiple Access (CSMA)

- A user wishing to transmit first listens to the medium to see if another transmission is in progress (carrier sense)
- Based on the fact that in LAN propagation time is very small
- ➔ If a frame was sent by a station, All stations knows immediately so they can wait before start sending
  - ➔ A station with frames to be sent, should sense the medium for the presence of another transmission (carrier) before it starts its own transmission
- This can reduce the possibility of collision but it cannot eliminate it.
  - Collision can only happen when more than one station begin transmitting within a short time (the propagation time period)

Random Access – Carrier Sense Multiple Access (CSMA)

- Vulnerable time for CSMA is the maximum propagation time
- The longer the propagation delay, the worse the performance of the protocol because of the above case.



Types of CSMA Protocols

Different CSMA protocols that determine:

- What a station should do when the medium is idle?
- What a station should do when the medium is busy?

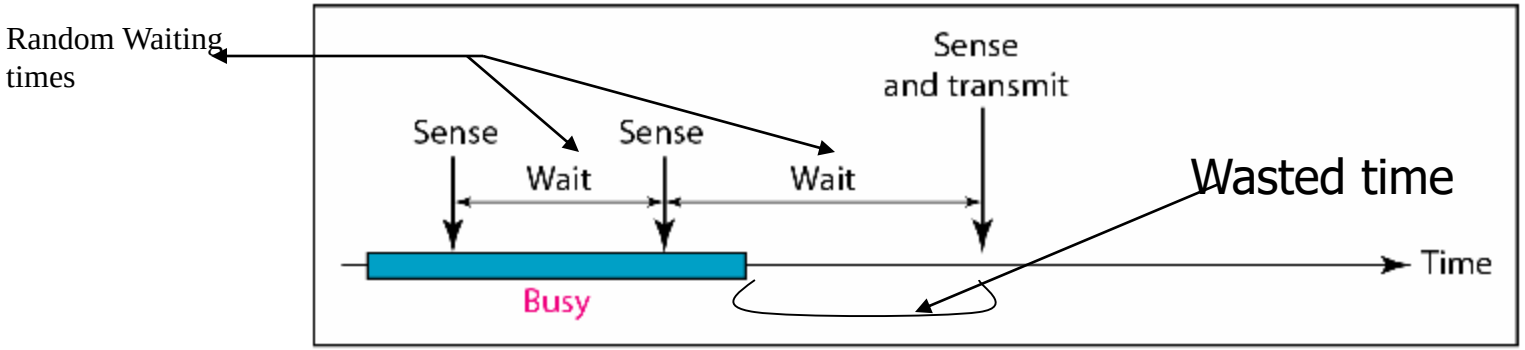
1. Non-Persistent CSMA
2. 1-Persistent CSMA
3. p-Persistent CSMA

1) Non-persistent CSMA

- A station with frames to be sent, should sense the medium:

1. If medium is idle, transmit; otherwise, go to 2
2. If medium is busy, (backoff) wait a random amount of time and repeat 1

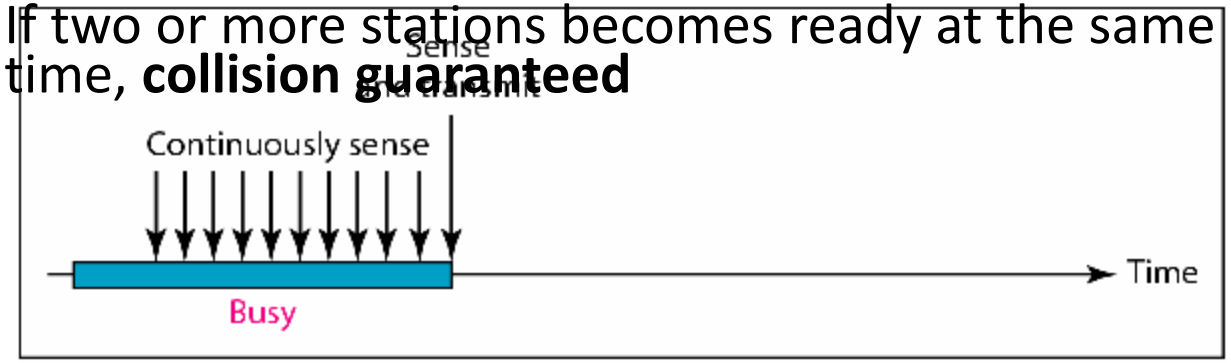
- Performance:
  - Random delays reduces probability of collisions because two stations with data to be transmitted will wait for different amount of times.
  - Bandwidth is wasted if waiting time (backoff) is large because medium will remain idle following end of transmission even if one or more stations have frames to send



b. Nonpersistent

2) 1-persistent CSMA

- To avoid idle channel time, 1-persistent protocol used
- Station wishing to transmit listens to the medium:
  1. If medium idle, **transmit** immediately;
  2. If medium busy, **continuously listen** until medium becomes idle; then transmit immediately with probability 1
- Performance
  - 1-persistent stations are **selfish**
  - If two or more stations becomes ready at the same time, **collision guaranteed**

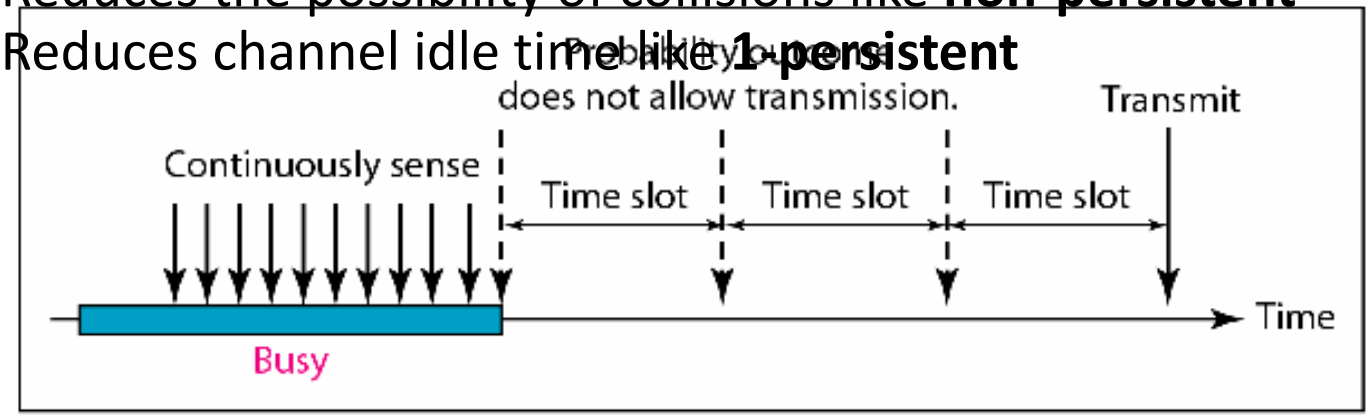


a. 1-persistent

3) P-persistent CSMA

- Time is divided to slots where each Time unit (slot) typically equals **maximum propagation delay**
- Station wishing to transmit listens to the medium:

1. If medium idle,
   - transmit with probability (**p**), OR
   - wait **one time unit (slot)** with probability (**1 – p**), then repeat 1.
2. If medium busy, **continuously listen until idle** and repeat step **1**
3. Performance
   - Reduces the possibility of collisions like **non-persistent**
   - Reduces channel idle time like **1-persistent**



c. p-persistent

3) P-persistent CSMA

- the time slot is usually set to the maximum propagation delay.
- as **p** decreases, stations wait longer to transmit but the number of collisions decreases
- Considerations for the choice of **p:**
- **(n x p)** must be **< 1** for stability, where **n** is maximum number of stations, i.e.,

$$p < 1/n$$

CSMA/CD (Collision Detection)

- CSMA (all previous methods) has an inefficiency:
  - If a collision has occurred, the channel is unstable until colliding packets have been fully transmitted
- CSMA/CD (Carrier Sense Multiple Access with Collision

Detection) overcomes this as follows:

  - While transmitting, the sender is listening to medium for collisions.
  - Sender stops transmission if collision has occurred reducing channel wastage .

CSMA/CD is Widely used for bus topology LANs (IEEE 802.3, Ethernet).

How does a node detect a collision?

Transceiver: **A node monitors the media while transmitting. If the observed power is more than transmitted power** of its own signal, it means collision occurred

CSMA/CD Protocol

- Use one of the CSMA persistence algorithm

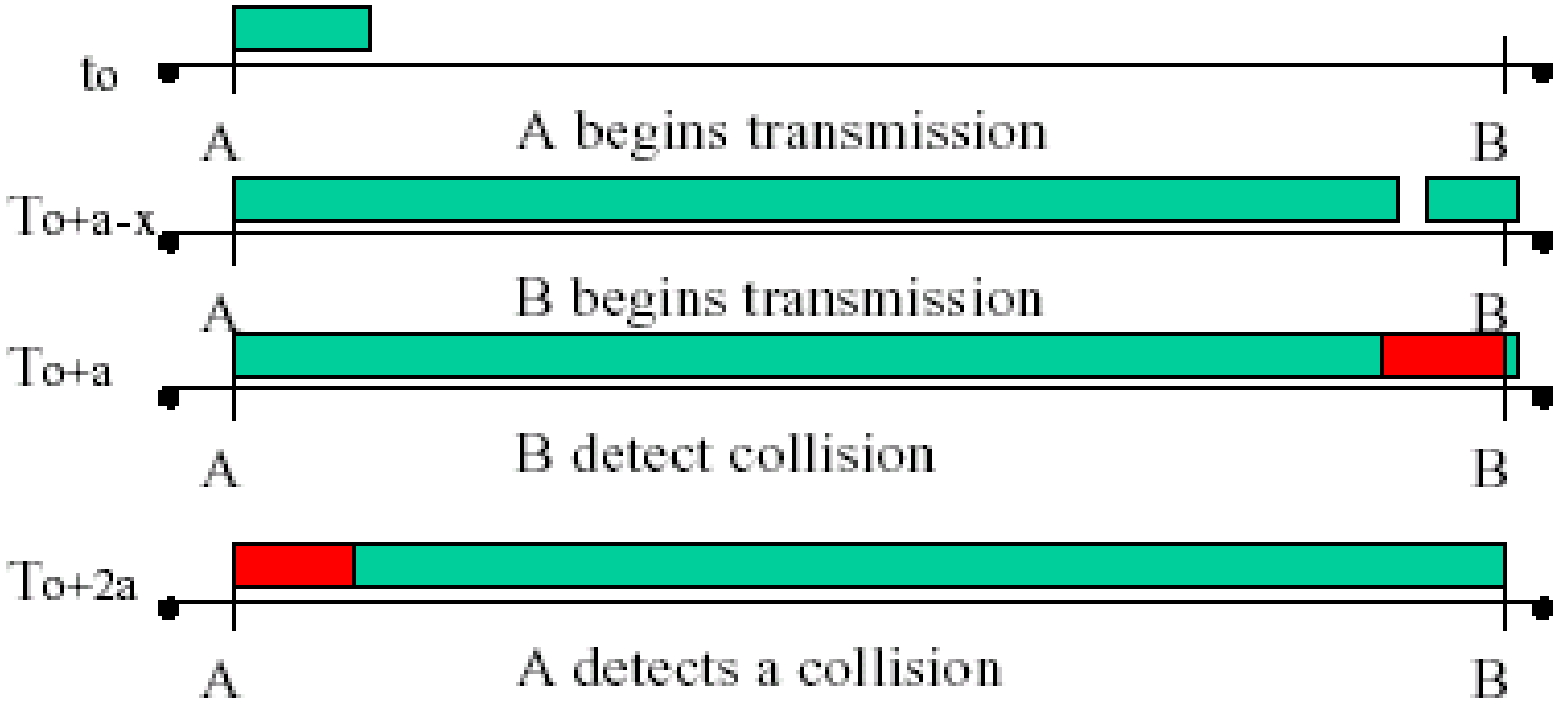
(non-persistent, 1-persistent, p-persistent) for transmission

- If a collision is detected by a station during its transmission then it should do the following:
  - Abort transmission and
  - Transmit a **jam signal** to notify other stations of collision so that they will discard the transmitted frame also to make sure that the collision signal will stay until detected by the furthest station
  - After sending the jam signal, backoff (wait) for a random amount of time, then
  - Transmit the frame again

CSMA/CD

- ***Question:*** How long does it take to detect a collision?
- ***Answer:*** *In the* ***worst case***, **twice the maximum propagation delay of the medium**

Note: **a = maximum propagation delay**



CSMA/CD

- Restrictions of CSMA / CD:
  - Packet transmission time should be at least as long as the time needed to detect a collision (2 * maximum propagation delay + jam sequence transmission time)
  - Otherwise, CSMA/CD does not have an advantage over CSMA

Controlled Access or Scheduling

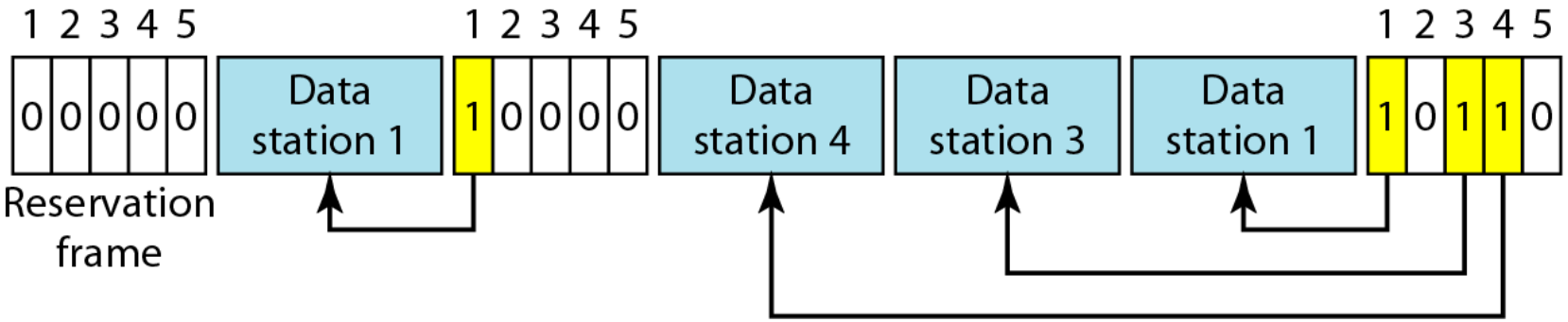
Controlled Access or Scheduling

- Provides **in order access** to shared medium so that every station has chance to transfer (**fair protocol**)

- ***Eliminates*** <u>collision completely</u>
- **Three methods** for controlled access:
  - Reservation
  - Polling
  - Token Passing

1-Reservation Access Method

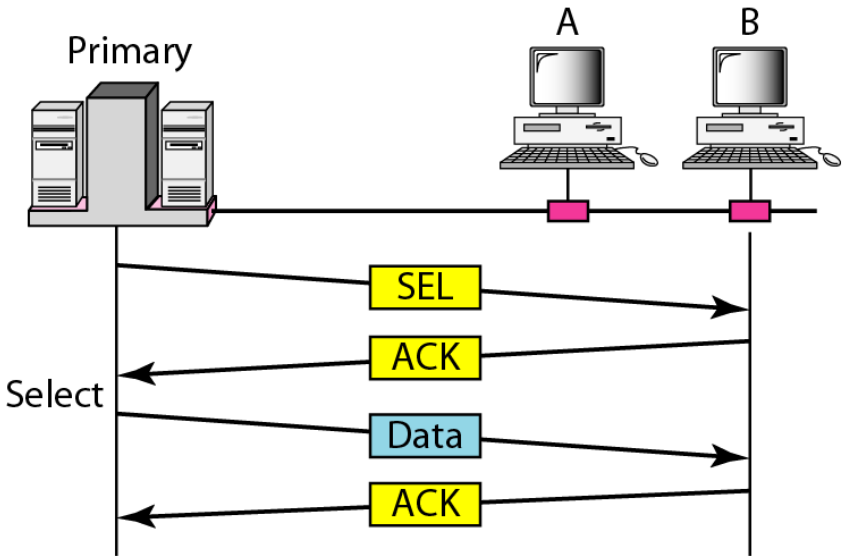
- Stations take turns transmitting a single frame at a full rate (R) bps
- Transmissions are organized into variable length cycles
- Each cycle begins with a reservation interval that consists of (N) minislots. One minislot for each of the N stations
- When a station needs to send a data frame, it makes a reservation in its own minislot.
- By listening to the reservation interval, every station knows which stations will transfer frames, and in which order.
- The stations that made reservations can send their data frames after the reservation frame.



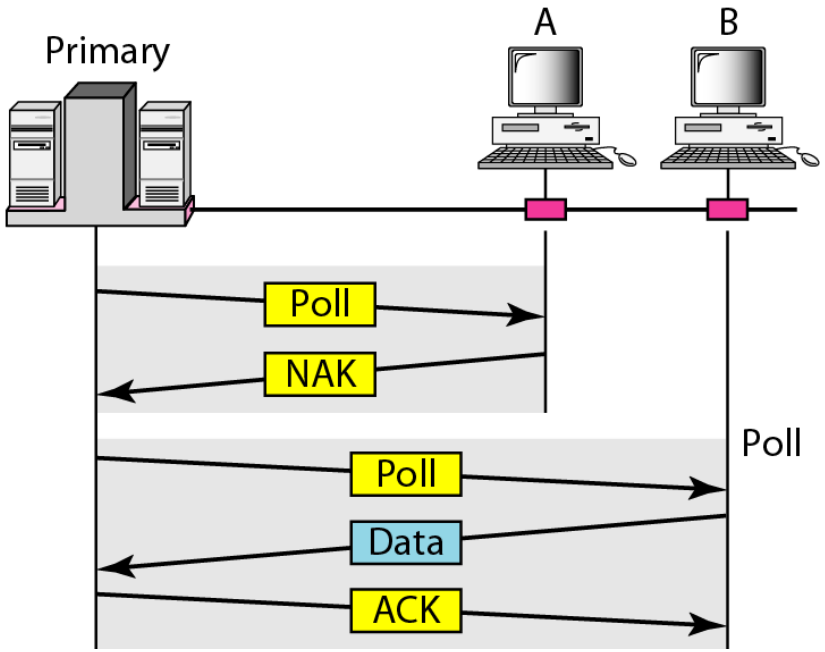
2- Polling

- Stations take turns accessing the medium
- Two models: **Centralized** and **distributed** polling
- **Centralized polling**
  - One device is assigned as **primary station** and the others as **secondary stations**
  - All data exchanges are done through the **primary**
  - When **the primary has a frame to send** it sends a **select** frame that includes the address of the intended secondary
  - When **the primary is ready to receive** data it send a **Poll** frame for each device to ask if it has data to send or not. If yes, **data** will be transmitted otherwise **NAK** is sent.
  - Polling can be done <u>in order</u> (Round-Robin) or based on <u>predetermined order</u>
- **Distributed polling**
  - **No primary and secondary**
  - Stations have a **known polling order** list which is made based on some protocol
  - ▶**station with the highest priority** will have the access right first, then it passes the access right to the **next station**

Select and poll functions in polling access method



Primary is sending to Secondary



Secondary is sending to Primary

3- Token-Passing network

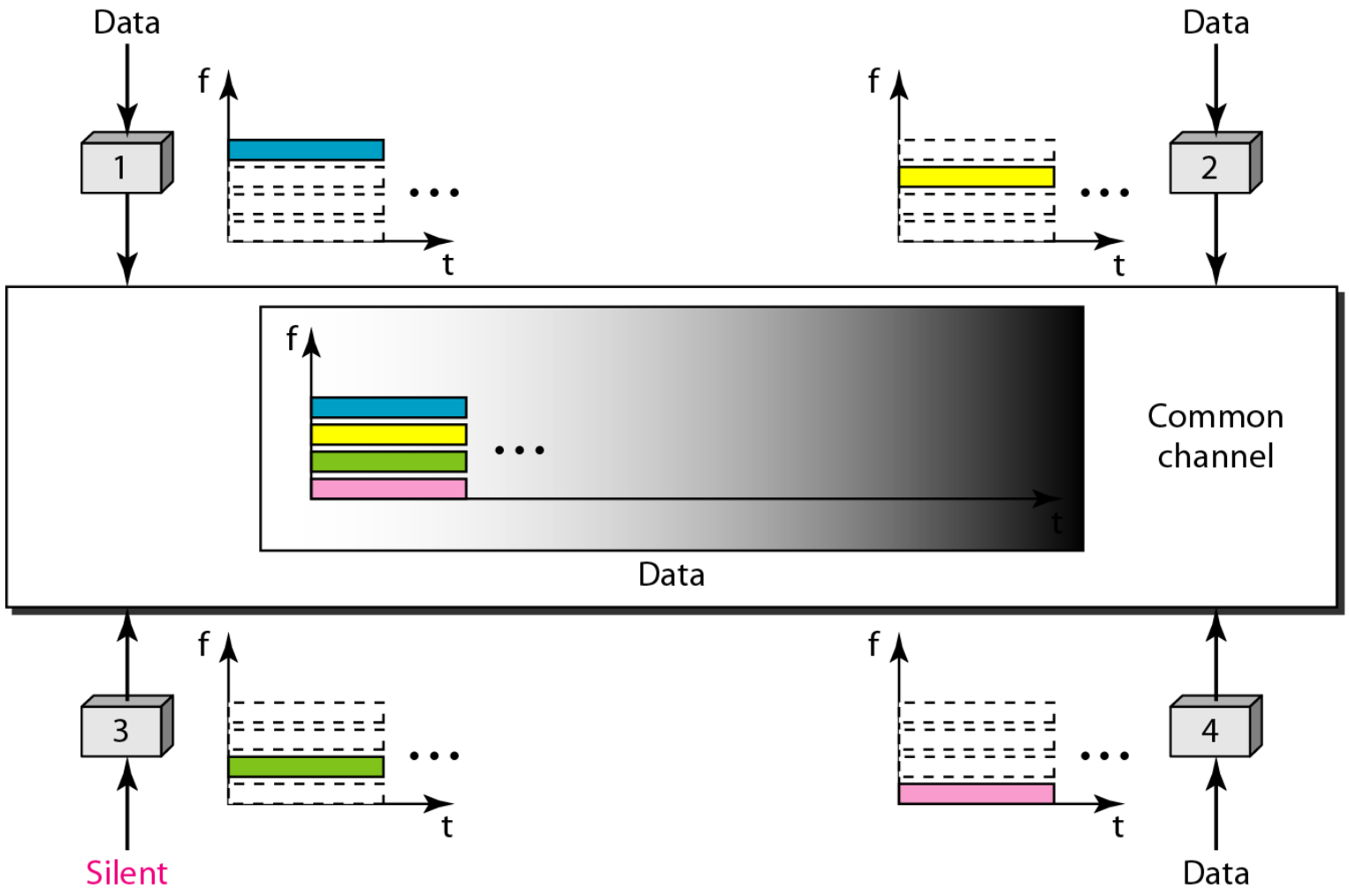
- **Station Interface is in two states**:
  - **Listen state**: Listen to the arriving bits and check the destination address to see if it is its own address. If yes the frame is copied to the station otherwise it is passed through the output port to the next station.
  - **Transmit state**: station captures a special frame called **free token** and transmits its frames. **Sending** station is responsible for **reinserting** the free token into the ring medium and for **removing** the transmitted frame from the medium.

Channelization

Channelization

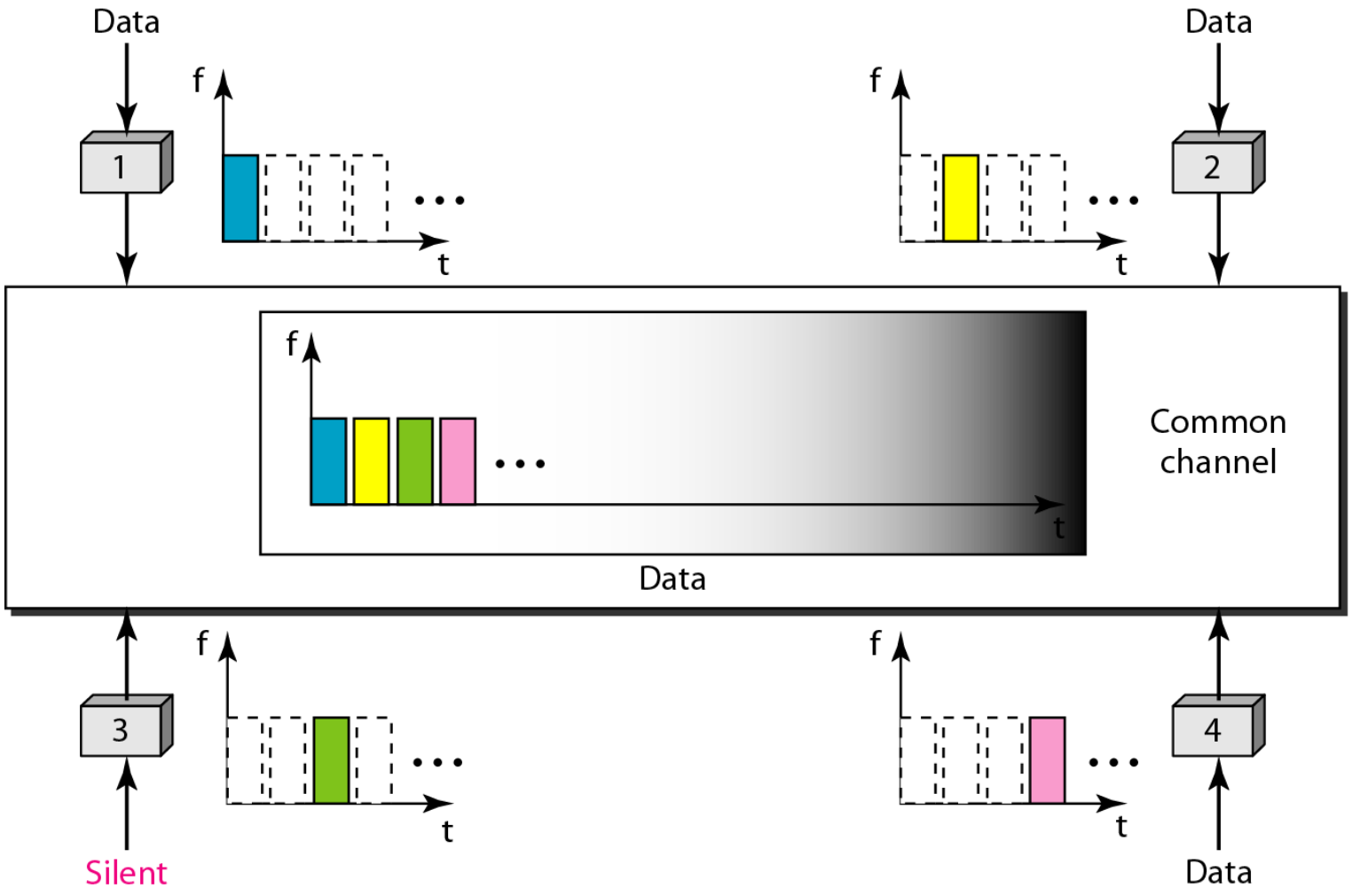
Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. In this section, we discuss three channelization protocols.

Frequency-division multiple access (FDMA)



- **FDMA:** Frequency Division Multiple Access:
  - Transmission medium is divided into **M** separate frequency bands
  - Each station transmits **continuously** on the assigned band
  - A node is **limited** to an average rate even when it is **the only node with frame** to be sent

Time-division multiple access (TDMA)



TDMA: Time Division Multiple Access

- **TDMA: Time Division Multiple Access**
  - The entire bandwidth capacity is a **single channel** with its capacity shared **in time** between **M** stations
  - A node must **always wait for its turn** until its slot time arrives even when it is the **only node** with frames to send

CDMA: Code Division Multiple Access

- **CDMA: Code Division Multiple Access**
  - In CDMA, **<u>one channel</u>** carries all transmissions **simultaneously**
  - Each station codes its data signal by a specific codes before transmission
  - The stations receivers use these codes to recover the data for the desired station

HDLC,PPP,Media access control

HDLC - Introduction

- High-level Data Link Control
- It is used in Datalink layer for multiple data transfer
- Bit oriented communication protocol
- Used to connect multiple network systems.It applies the ARQ protocol for application and establishes a full-duplex communication channel

HDLC Stations

- **Primary** - establishes and de-establishing primary data channel to share frames in the network known as commands. Performs data management for network
-
- **Secondary** - Works under command of primary station, and frames issued by this station are known as responses
-
- **Combined** - Both primary and secondary

HDLC Transfer models

- **NRM - Normal Response Model (NRM):**
- This model combines primary and secondary stations in point-to point or multi point network configuration to exchange commands from primary and responses from secondary.
- Here only Sender (primary node) and send the data packets. The receiver (secondary) just send the acknowledgement

Transfer model

- **Asynchronus Balanced Model (ABM):**
- Combined stations are installed in a point to point configuration for exchange commands and responses in balanced format.
- Here both sender and receiver can send data

HDLC Frame

HDLC Frame Format

FLAG	ADDRESS	CONTROL	INFORMATION	CRC	FLAG
8	8	8 or 16	variable	16 or 32	8

Flag Field: It marks the beginning of the frame and termination of the frame. Each frame starts and ends with the flag bit. It is defined by an 8 bit octet sequence 01111110.

Address Field: It encapsulates the receivers address.

Control Field: It contains information about the flow and error control in byte format

Payload/Information Field : This field carries the information that to be transfered

FCS Field : This field stands for Frame check Sequence and acts as error detection field in HDLC protocol
Which includes the 16 bit CRC check bit

Frame models

- **I- Frames - Information Frame** - It is applied to encapsulate the user information from upper layer in the model and then then transmit to network channel. The control bit will 0 indicating that this is a I-Frame model
-
- **S-Frame - Supervisory frames** - Used for error and data flow control and does not contain the information field in the frame format. First two bits of the control field in 1 and 0 indicating S-Frame
-
- **U-Frame - Un-numbered frame** - used for system management and exchanging information between the connected network devices

PPP- Introduction

- Used to make point to point communication.
- WAN protocol
- Widely used in broadband communication
- Home computers ----------> Servers

Services:

- Authentication
- Frames - Send frames between the data link layer of one device to another device
- Multilink - Newer version support multiple connection

PPP - Frame

- **Flag** : Indicating Beginning and Termination of frame. It is of the form 01111110
- **Address** : Address of the receiver. If we are trying to broadcast something then the address will 11111111
- **Control** : Error control
- **Protocol** : Tells what type of data is being transfered
- **Payload/Data** : Actual data
- **FCS**: Contains the CRC to correct the errors if any.

Byte stuffing

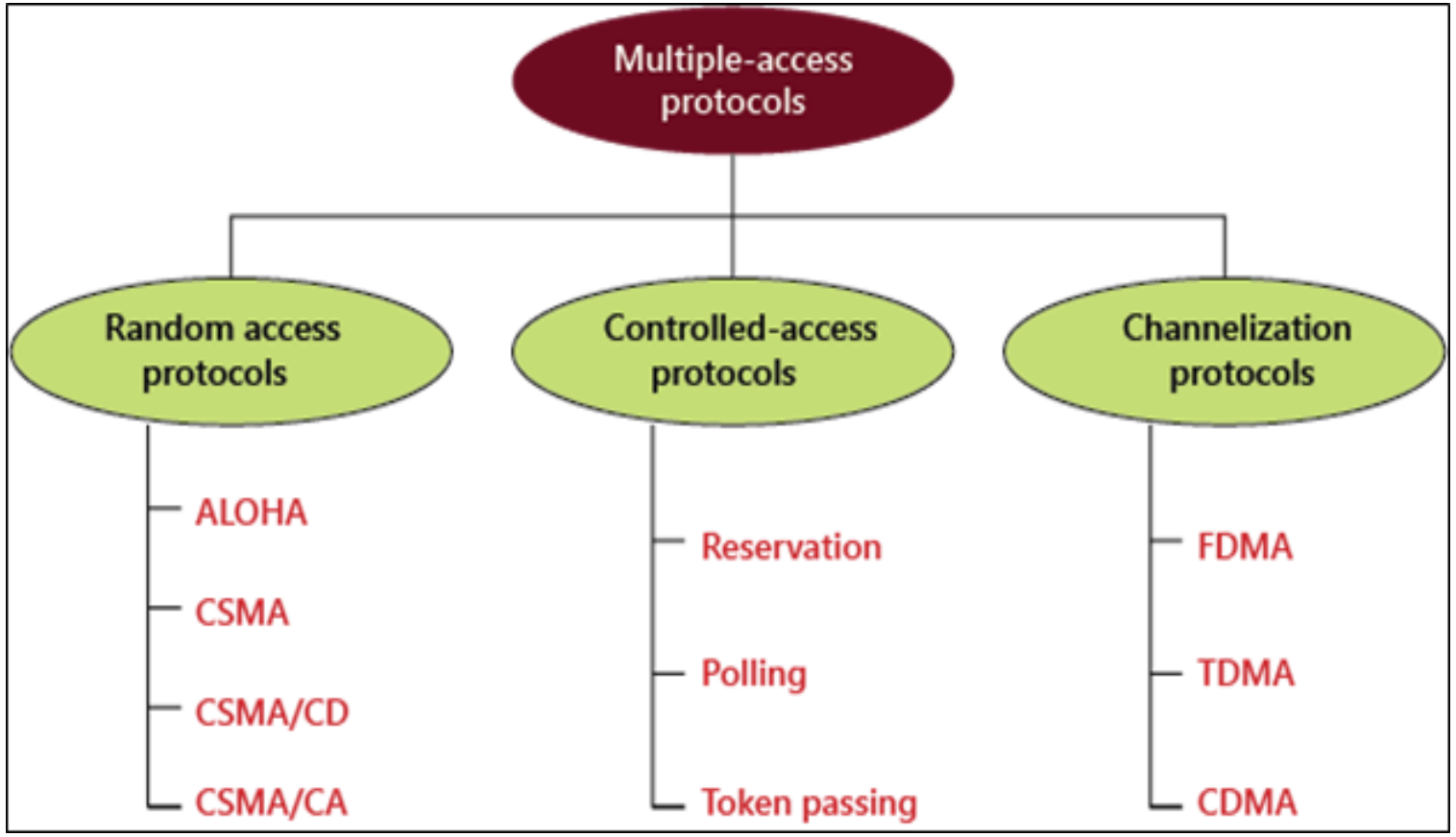
- Why byte stuffing ?
- It is process adding an extra byte whenever there is a flag sequence appear in payload. It is added so that the receiver will not take it as the end of the frame

Multiple access Control

- The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-
- Data Link Control
- Multiple Access Control

- **Data Link control –**
  The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.
- **Multiple Access Control –**
  If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.

Types of Multiple-access



Random Access Protocols

- **Random Access Protocol:** In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium’s state(idle or busy)

ALOHA

- **ALOHA –** It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.
- **Pure Aloha:**
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn’t come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.
- **Slotted Aloha:**
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

CSMA

- **CSMA –** Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle.
- **CSMA/CD –** Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.
- **CSMA/CA –** Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals.

Controlled Access

- **Reservation**
- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
  - Reservation interval of fixed time length
  - Data transmission period of variable frames.
- **Polling**
- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.

- **Token Passing**
- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.

Channelization

- **Channelization:**
  In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.
- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data.

Network Layer
Transport Layer

Transmisi Data
Pengkodean Data
Teknik Komunikasi Data Digital
Data Link Control
~~Multiplexing~~
Switching
Medium Access Sublayer
Network Layer

Outlines

Fungsi Network Layer

Protokol Komunikasi Data

Konsep Pengalamatan Logis (IP)

Konsep Pemanfaatan IP

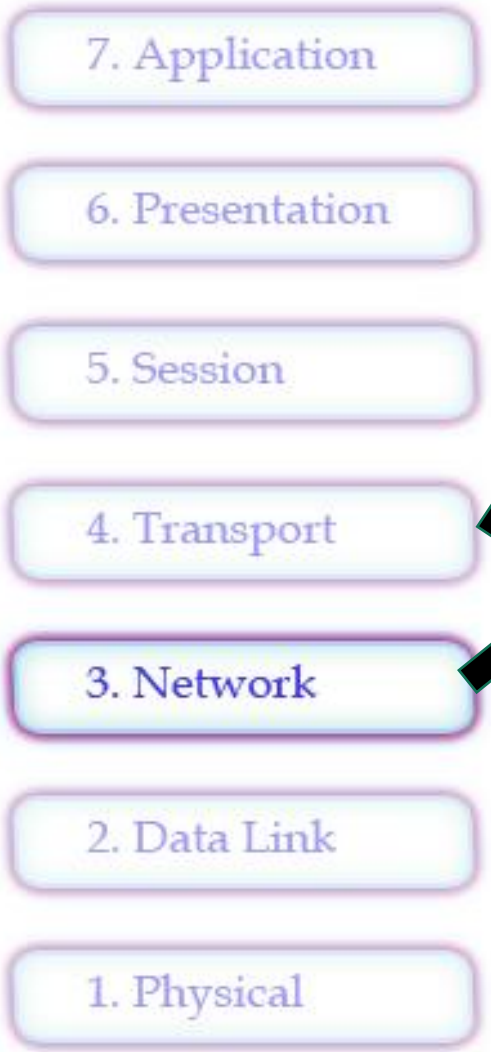
Konsep routing

Algoritma routing

Prinsip Kerja Router

Konsep Gateway

Netw



Transport layer digunakan oleh device-device sebagai penghubung antar proses / aplikasi.

Network layer digunakan sebagai penghubung antara satu device dengan device lainnya.

- ❑Addressing
- ❑Encapsulation
- ❑Routing
- ❑Decapsulation

Network Layer

- Addressing
  - Network layer menyediakan mekanisme pengalamatan logik yang unik untuk setiap device yang kita kenal sebagai IPv4 address.
- Encapsulation
  - Disisi mesin pengirim, PDU layer transport (segmen) akan di enkapsulasi dengan header layer network sehingga menjadi PDU layer 3 yang disebut packet.
  - Diantara informasi yang disertakan dalam header ini adalah informasi IP address dari device pengirim dan penerima.
- Decapsulation
  - Disisi mesin penerima, packet akan di dekapsulasi dan dibaca informasi pada headernya, jika IP address tujuan sesuai dengan IP address penerima maka packet akan diserahkan ke layer transport.

Network Layer

- Routing
  - Network layer juga menyediakan layanan untuk memandu jalannya packet agar sampai ke mesin tujuan.
  - Mesin pengirim dan penerima tidak selalu terhubung dalam 1 network yang sama, bahkan seringkali packet harus berjalan melalui beberapa network yang berbeda sebelum sampai ke network tujuan.
  - Device yang menghubungkan sebuah network dengan network lainnya dikenal sebagai router.
  - Router berfungsi untuk memilih jalur dan memandu arah jalannya paket agar bisa sampai ke network yang dituju, proses inilah yang disebut sebagai routing.
  - Setiap router yang harus dilalui oleh packet dalam perjalanannya menuju mesin penerima disebut sebagai hop.

IP

- IP adalah satu-satunya protokol layer 3 yang digunakan untuk membawa data user melalui network TCP/IP.
- IPv4 adalah versi IP yang paling banyak digunakan saat ini. IPv6 masih dalam tahap pengembangan dan belum banyak dipakai.
- Karakteristik :
  - Connectionless – tidak perlu menjalin koneksi sebelum pengiriman data.
  - Best Effort (Unreliable) – tidak ada fitur-fitur untuk menjamin data sampai ke tujuan.
  - Media Independent.

IP -> Connectionless

- Seperti halnya ketika kita mengirim surat/paket kepada seseorang tanpa ada pemberitahuan terlebih dahulu kepada penerima.
- Pengirim tidak tahu :
  - Apakah penerima ada atau tidak.
  - Apakah surat telah sampai atau tidak.
  - Apakah penerima dapat membaca surat yang dikirim atau tidak.
- Penerima tidak tahu :
  - Akan ada surat yang datang.
  - Kapan surat akan datang.
- Hal ini mengurangi overhead IP dibandingkan jika ada fitur-fitur reliability seperti protokol TCP.

IP -> Best Effort

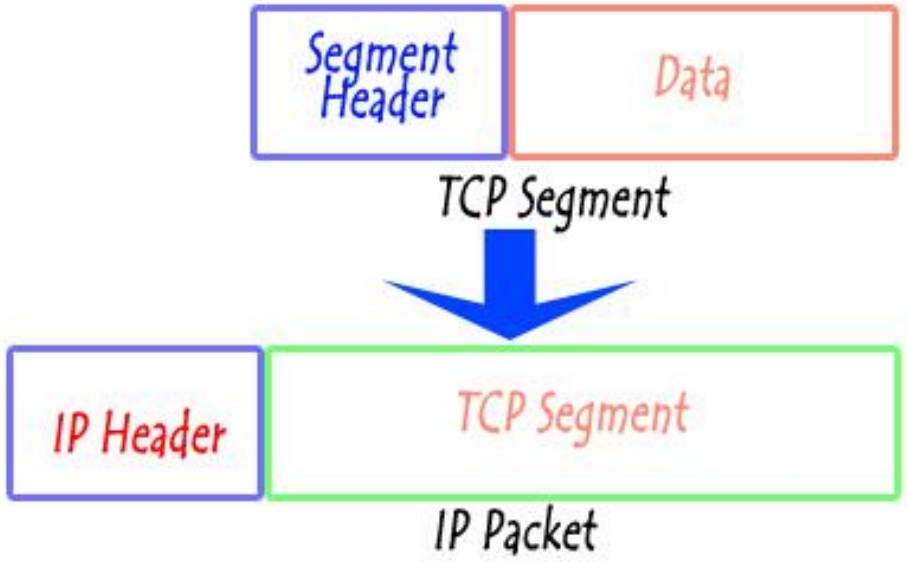
- Protokol IP bersifat unreliable, yang berarti tidak ada fitur-fitur yang mendukung reliability.
  - Beberapa paket bisa saja hilang dalam perjalanan.
- Header IP menjadi lebih kecil, sehingga overhead berkurang dan delay pengiriman paket berkurang.
- Unreliable disini bukan berarti IP tidak layak digunakan sebagai protokol komunikasi. Unreliable disini maksudnya IP tidak dilengkapi dengan fitur-fitur untuk memanage dan merecovery paket-paket korup atau hilang.
- Header pada IP tidak dibebani dengan field-field yang dibutuhkan untuk pengiriman data reliable, seperti ACK dan sebagainya.
- Tanggung jawab layanan fitur-fitur reliability diserahkan sepenuhnya kepada layer lain.

IP -> Media Independent

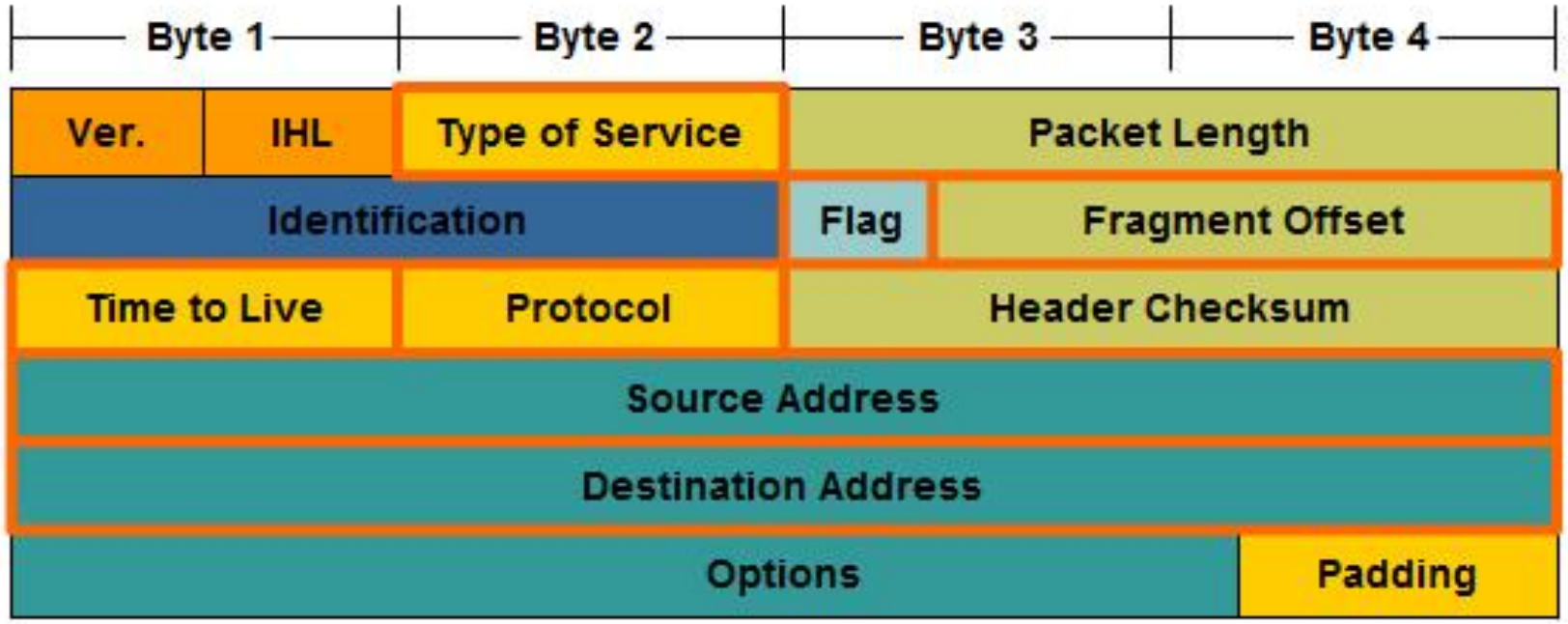
- Layer Network juga tidak perlu menyesuaikan dengan karakteristik dan jenis media apa yang digunakan dalam pengiriman data.
  - Komunikasi IP tidak terbatas pada media spesifik tertentu.
  - Komunikasi IP bisa melalui sinyal listrik kabel, sinyal optik fiber, maupun sinyal radio wireless.
- Ada satu karakteristik dalam media yang menjadi pertimbangan layer network, yakni MTU.
  - Maximum Transmission Unit (MTU), ukuran paket maksimum, dalam byte, yang bisa ditangani oleh network interface.
- Dalam beberapa kasus, router melakukan pemecahan paket menjadi lebih kecil untuk menyesuaikan ukuran paket dengan MTU media network yang dituju. Proses ini disebut sebagai fragmentation.

IP -> Enkapsulasi

- IP mengenkapsulasi segmen/datagram dari layer transport dengan IP Header agar data dapat dikirimkan ke mesin tujuan.
- Router membaca informasi pada IP Header ini untuk melakukan proses routing data.
- Dalam TCP/IP, PDU pada layer ne t.



IP ->



Ada 6 fields kunci yang perlu kita perhatikan pada IP Header:

- ❑IP Source address
- ❑IP Destination address
- ❑Time-to-Live (TTL)
- ❑Type-of-Service (ToS)
- ❑Protocol
- ❑Fragment Offset

IP -> Header

- IP Destination Address
  - IP address mesin yang dituju (penerima).
- IP Source Address
  - IP address mesin pengirim.
- Time to Live
  - Angka biner yang menunjukkan sisa ‘hidup’ sebuah paket. Nilai ini akan dikurangi 1 satuan setiap kali paket melewati sebuah router (hop).
  - Ketika nilai TTL mencapai angka = 0, maka paket akan di drop oleh router.
  - Mekanisme ini merupakan metode pencegahan terjadinya routing loop, sebuah problem routing yang menyebabkan paket terus berputar dalam network tanpa henti.

IP -> Header

- Protocol
  - Menunjukkan tipe protokol apa yang digunakan pada porsi data.
  - Misal : ICMP (01), TCP (06), UDP (17).
- Type of Service
  - Digunakan sebagai mekanisme Quality-of-Service (QoS) untuk menentukan prioritas setiap paket.
- Fragment Offset
  - Saat terjadi fragmentation, field 13 bit ini digunakan untuk mengidentifikasi susunan fragment-fragment paket untuk proses rekonstruksi.
- Flag
  - Field 3 bit digunakan untuk mengontrol ada tidaknya fragmentation.

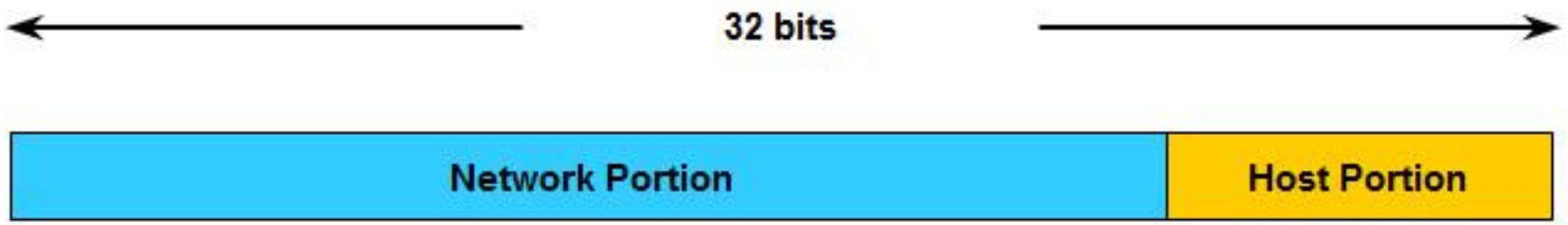
IP -> Header

- Version
  - Versi IP yang digunakan, IPv4 atau IPv6.
- Internet Header Length
  - Menunukkan ukuran header paket.
- Packet Length
  - Menunjukkan ukuran paket secara keseluruhan termasuk header.
- Header checksum
  - Mengecek error pada header paket. Paket akan di drop jika terdeteksi error pada header.

Networks -> Pengelompokan Device-Device

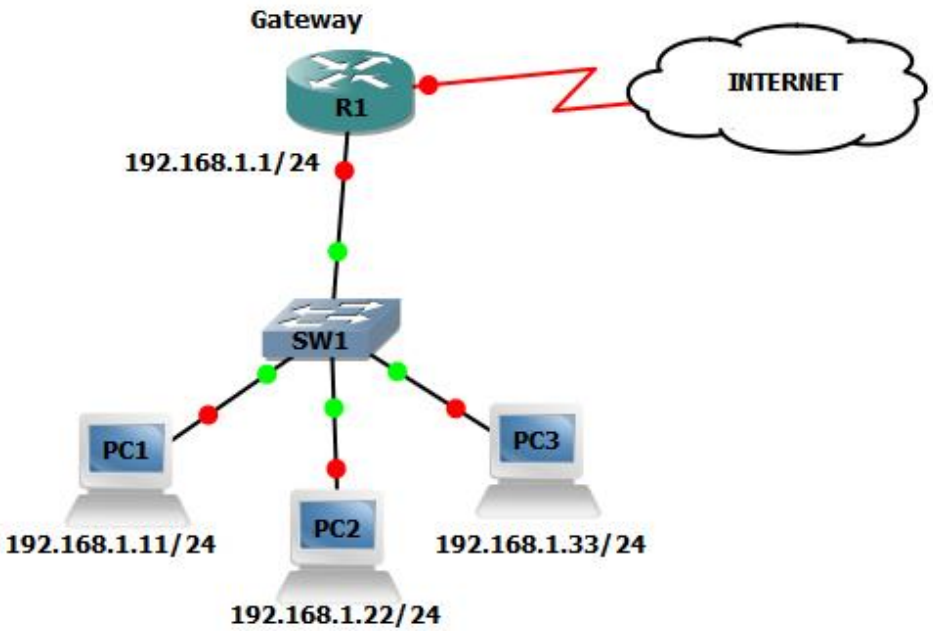
- Salah satu peran network layer adalah menyediakan mekanisme pengalamatan (IP address) dan pengelompokan device ke dalam satu network spesifik.
- Network yang besar juga bisa dipecah lagi menjadi beberapa kelompok network yang lebih kecil yang biasa disebut subnetwork atau subnet.
- Pengelompokan ini dapat berdasarkan lokasi, manfaat dan tujuan network, kepemilikan dan kewenangan, dll.
- Beberapa manfaat pengelompokan ini antara lain :
  - Performance
  - Security
  - Management address

Networks -> Pengelompokan Device-Device



- 32 bit IPv4 address terdiri dari 2 bagian bit, network dan host.
- Bagian network menunjukkan anggota network mana IP address tersebut, sedangkan host menunjukkan mesin itu sendiri.
- Dalam satu network yang sama, semua host memiliki bagian network yang sama.
- Total bit yang menunjukkan bagian network disebut prefix length, network dengan prefix /24 memiliki 24 bit bagian network.

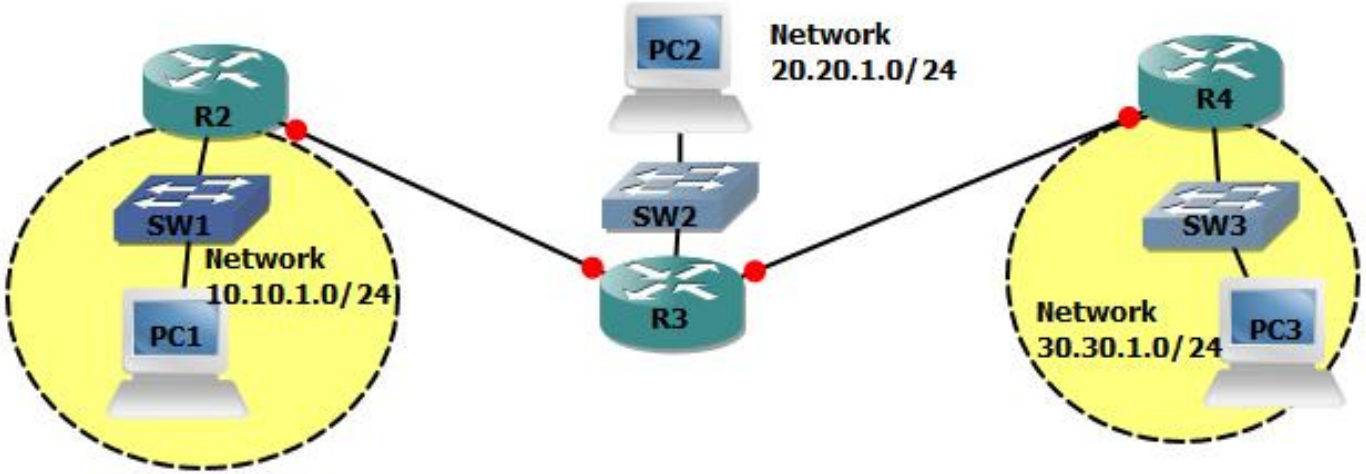
Routing



- Mesin-mesin dalam satu network saling berkomunikasi tanpa menggunakan device layer network sebagai perantara.
- Untuk berkomunikasi dengan mesin dalam network lain diperlukan device perantara mis: router sebagai gateway menuju network lain.
- Router memerlukan informasi routing (route) yang mendefinisikan kemana paket harus di forward untuk mencapai tujuan.

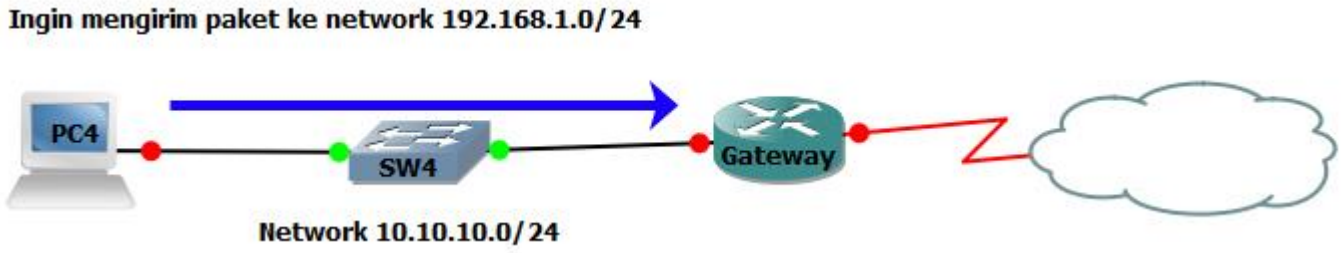
Routing

- Dalam proses routing, router menentukan kemana paket harus di forward berdasar informasi network tujuan yang ada pada IP Header paket.
- Jika network tujuan merupakan network yang terhubung langsung (directly connected) pada router, maka paket akan di forward langsung k
- Jika netwo t akan di forward ke



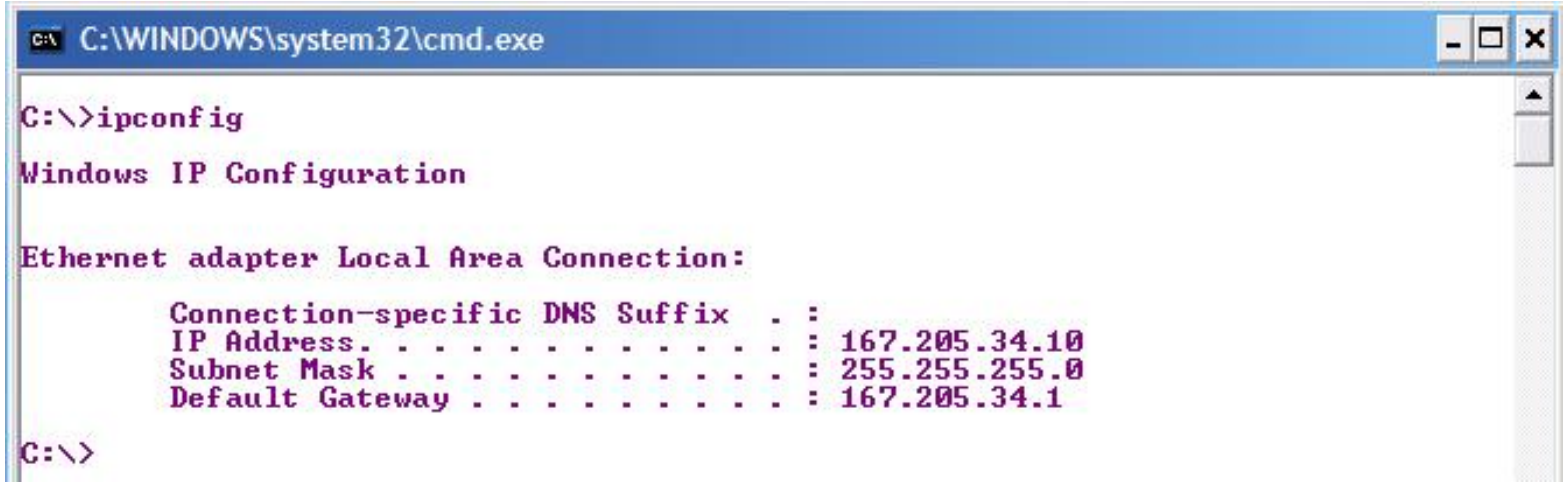
Routing -> Gateway

- Gateway atau default gateway diperlukan untuk mengirimkan data keluar dari network lokal.
- Gateway ini merupakan router yang salah satu interface-nya terhubung ke network lokal.
- Gateway harus memiliki bagian network yang sama dengan IP address mesin-mesin dalam network lokal.
- Ketika host tidak tahu harus kemana mengirimkan paket, maka host akan mengirimkannya ke address default gateway.



Routing -> Gateway

- Gunakan perintah ipconfig atau route untuk mengetahui konfigurasi IP address dan default gateway pada windows.
- Pada UNIX atau Linux gunakan perintah ifconfig dan route atau netstat -nr.



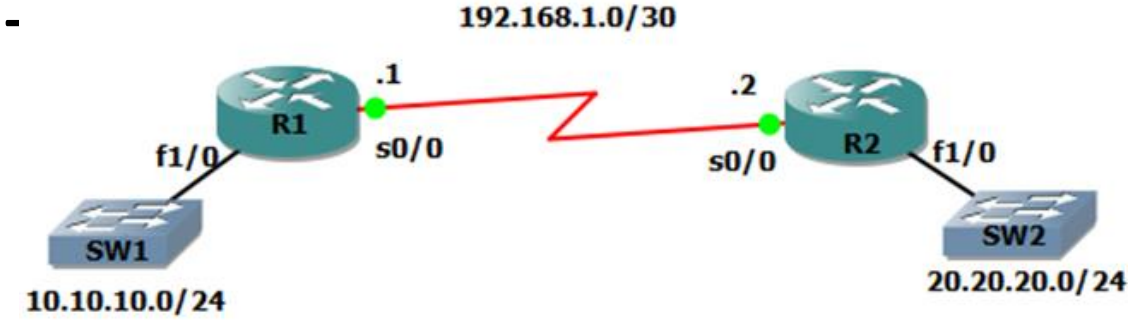
Routing -> Route

- Untuk mem-forward paket ke network tujuan, router memerlukan informasi routing (route) yang bersesuaian dengan network yang dituju.
- Route menunjukkan informasi next-hop-address, yakni IP address dari next-hop router dimana paket harus diserahkan agar bisa sampai ke network tujuan.
- Semua informasi routing akan disimpan dalam tabel routing.
- Router akan menambahkan informasi route tentang network-network yang terhubung langsung (directly connected) meskipun router belum dikonfigurasi apapun.
- Informasi routing dalam tabel routing berisi :
  - Network tujuan
  - Next-hop address
  - Metric

Routing -> Tabel Routing

- Semua informasi route oleh router akan disimpan dalam sebuah tabel routing.
- Informasi routing network yang terhubung langsung (directly connected) otomatis ditambahkan oleh router dalam tabel routing.
- Informasi routing dalam tabel routing dapat dibangun dengan 2 cara, static routing dan dynamic routing.
- Static Routing
  - Informasi route ditambahkan secara manual kedalam tabel routing.
- Dynamic Routing
  - Memanfaatkan protokol routing, router-router saling bertukar informasi routingsatu sama lain.
  - Update perubahan informasi routing juga akan disebarkan ke router-router lain.
  - Contoh protokol routing : RIP, EIGRP, OSPF, ISIS.

Routing ->



gunakan perintah show ip route untuk menampilkan tabel routing

```
Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet1/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
```

Sebelum ada konfigurasi apapun

next-hop address

```
Gateway of last resort is not set

     20.0.0.0/24 is subnetted, 1 subnets
R       20.20.20.0 [120/1] via 192.168.1.2, 00:00:04, Serial0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet1/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
```

Setelah ada konfigurasi protokol routing RIP

Routing -> Default Route

- Ketika router tidak memiliki informasi routing dari network tujuan sebuah paket, maka router akan mem-forward paket tersebut menggunakan default route.
- Default route ini equal dengan default gateway pada host.

```
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
R1(config)#
```

```
Gateway of last resort is 192.168.1.2 to network 0.0.0.0

     20.0.0.0/24 is subnetted, 1 subnets
R       20.20.20.0 [120/1] via 192.168.1.2, 00:00:25, Serial0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet1/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0
S*   0.0.0.0/0 [1/0] via 192.168.1.2
R1#
```

Routing -> Packet Processing

- Setelah router men-dekapsulasi frame pada layer 2, router membaca informasi network tujuan pada IP Header paket.
- Jika informasi network tujuan ada pada tabel routing
  - Paket akan dikirimkan ke next-hop address yang ada pada tabel routing.
- Jika tidak ada informasi network tujuan pada tabel routing, tapi router memiliki informasi default route.
  - Paket akan dikirimkan ke next-hop address dari default route.
- Jika tidak ada informasi network tujuan pada tabel routing dan router tidak memiliki informasi default route.
  - Paket akan di drop.
- Router meng-enkapsulasi ulang paket sebelum melakukan forwarding ke next-hop address.