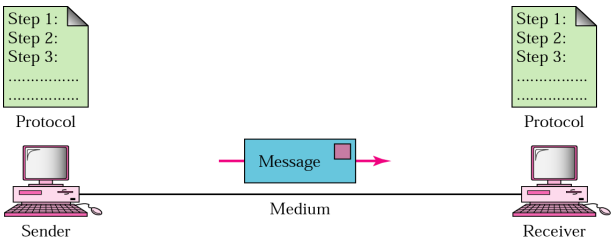
CENEVAL: Redes

Material Recopilado por:
Ing. Mario De la Fuente Martínez

Figure 1.1 *Five components of data communication*



Códigos

- Binario
- De Longitud Fija
- De Longitud Variable.

ASCII, de longitud Fija

	0	1	2	3	4	5	6	7
0	NUL	DLE	spc	0	@	P	`	p
1	SOH	DC1	!	1	A	Q	a	q
2	STX	DC2	"	2	B	R	b	r
3	ETX	DC3	#	3	C	S	c	s
4	EOT	DC4	$	4	D	T	d	t
5	ENQ	NAK	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	'	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	\	l	|
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	

Figure 1.2 *Simplex*

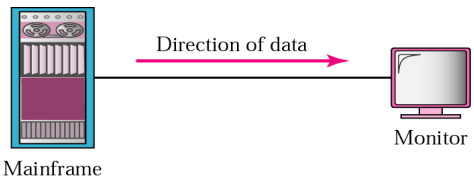


Figure 1.3 *Half-duplex*

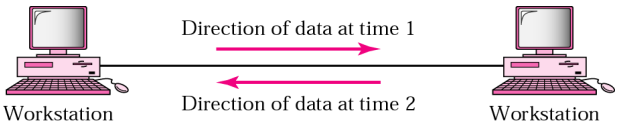


Figure 1.4 *Full-duplex*

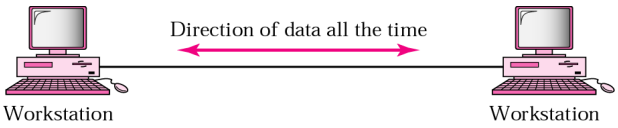


Figure 1.5 *Point-to-point connection*

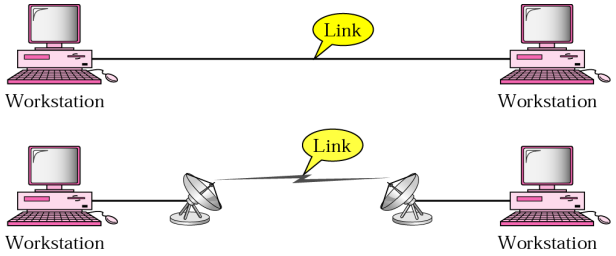


Figure 1.6 *Multipoint connection*

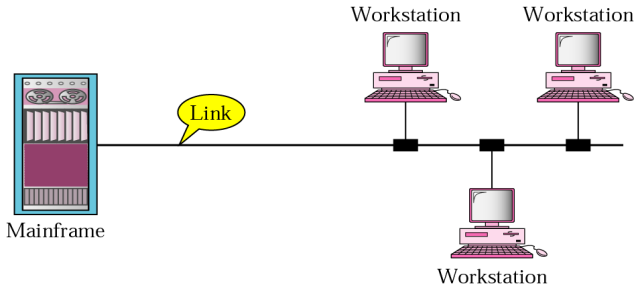


Figure 1.7 *Categories of topology*

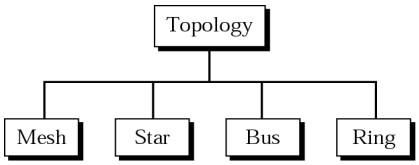


Figure 1.8 *Fully connected mesh topology (for five devices)*

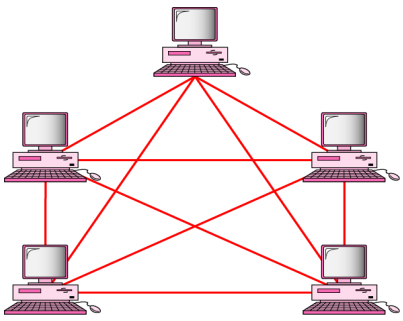


Figure 1.9 *Star topology*

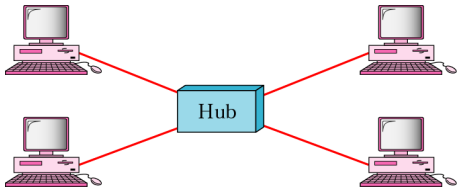


Figure 1.10 *Bus topology*

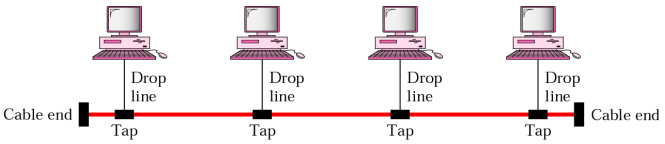


Figure 1.11 *Ring topology*

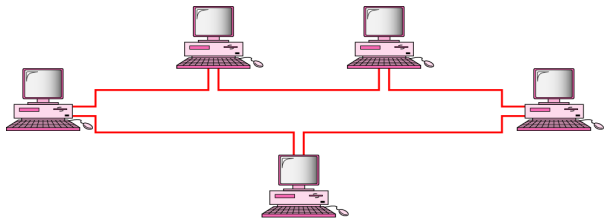


Figure 1.12 *Categories of networks*

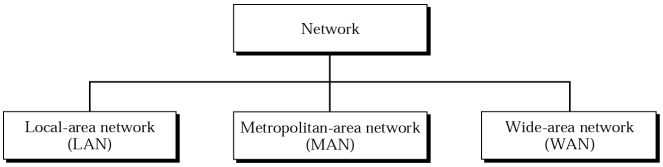
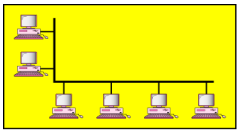
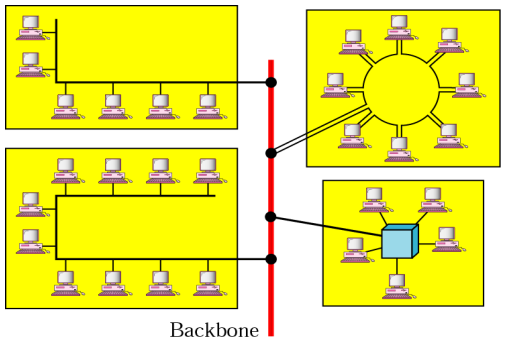


Figure 1.13 *LAN*



a. Single-building LAN

Figure 1.13 *LAN (Continued)*



b. Multiple-building LAN

Figure 1.14 *MAN*

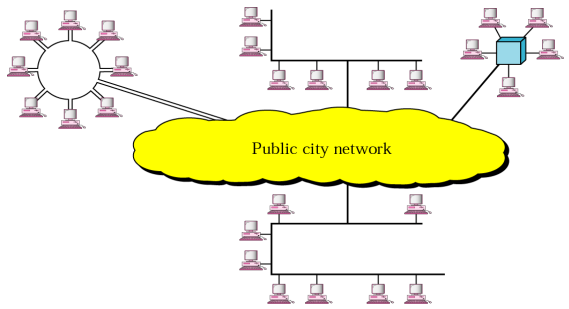


Figure 1.15 *WAN*

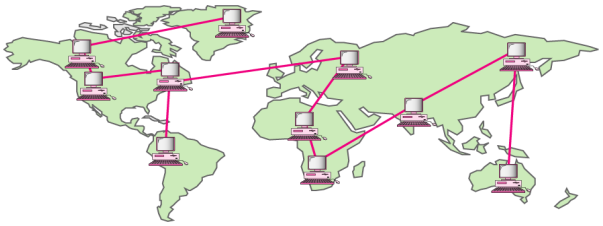
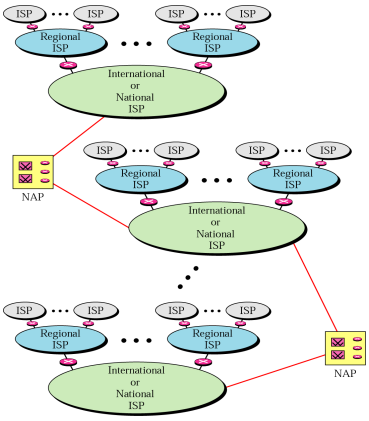


Figure 1.16 *Internet today*



Chapter 2

Network Models

Figure 2.1 *Sending a letter*

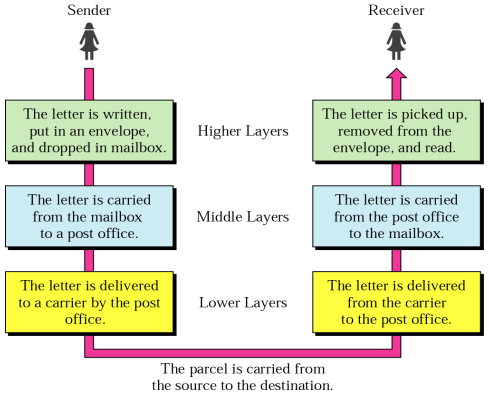


Figure 2.3 *Peer-to-peer processes*

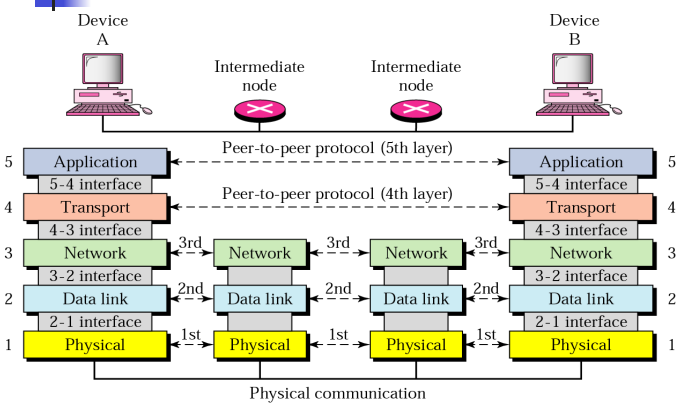
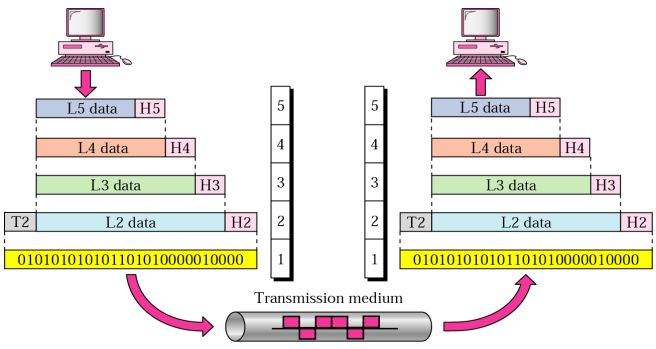


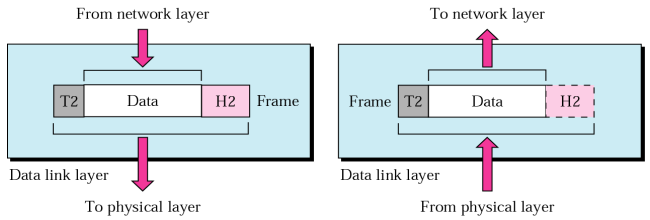
Figure 2.4 *An exchange using the Internet model*



Note:

The physical layer is responsible for transmitting individual bits from one node to the next.

Figure 2.6 *Data link layer*



Note:

The data link layer is responsible for transmitting frames from one node to the next.

Figure 2.8 *Example 1*

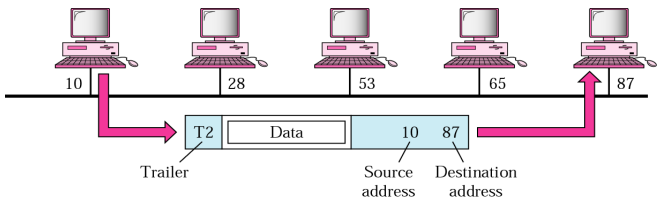
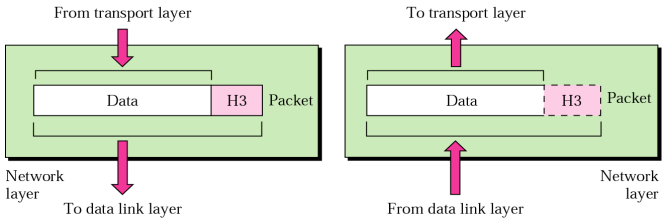


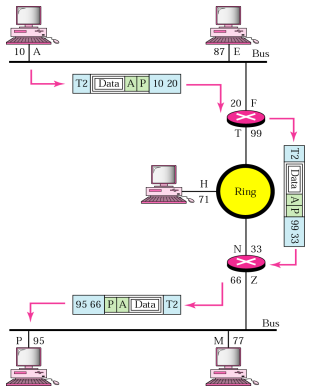
Figure 2.9 *Network layer*



Note:

The network layer is responsible for the delivery of packets from the original source to the final destination.

Figure 2.11 *Example 2*



Note:

The transport layer is responsible for delivery of a message from one process to another.

Figure 2.14 *Example 3*

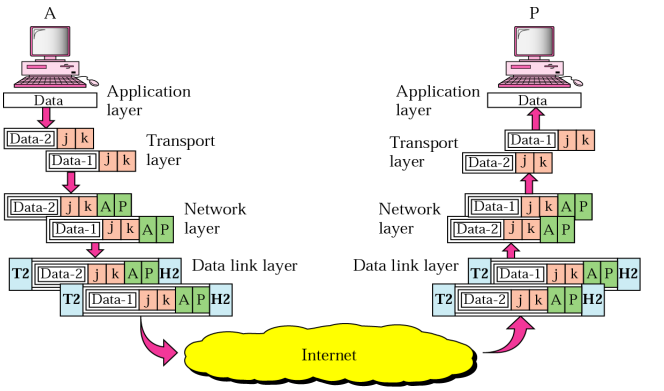
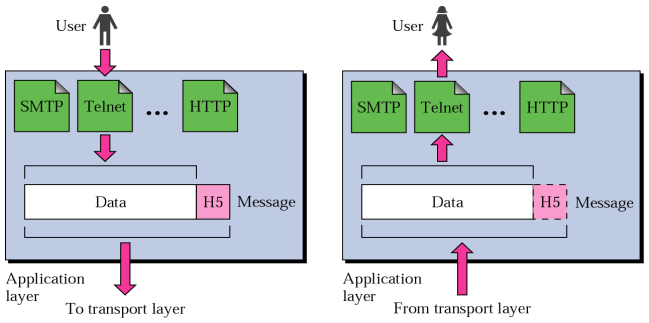


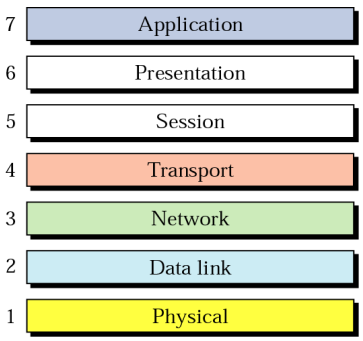
Figure 2.15 *Application layer*



Note:

The application layer is responsible for providing services to the user.

Figure 2.17 *OSI model*



Chapter 3

Signals

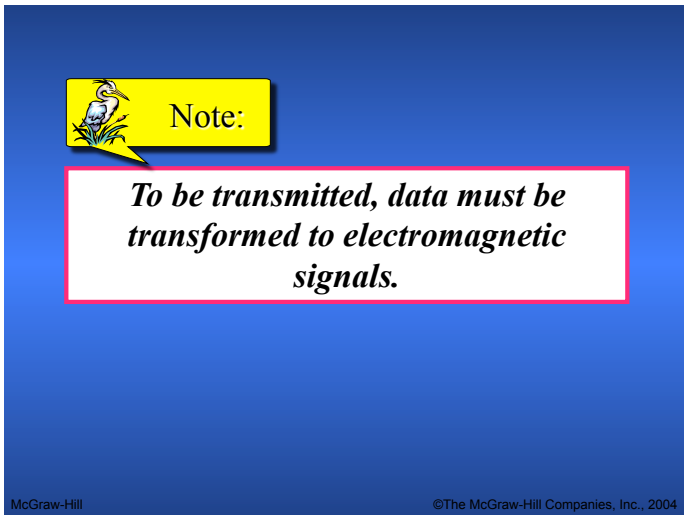


Figure 3.1 Comparison of analog and digital signals

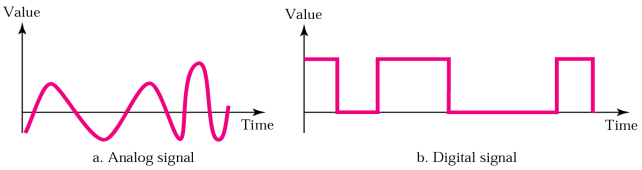


Figure 3.3 *Amplitude*

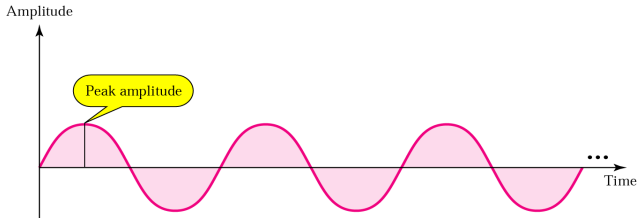


Figure 3.4 *Period and frequency*

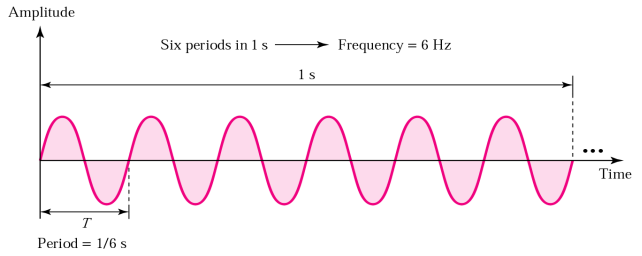


Figure 3.5 *Relationships between different phases*

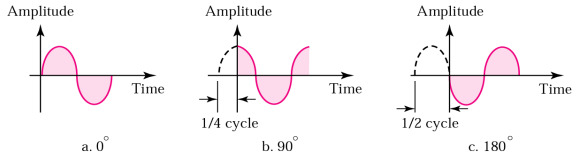


Figure 3.12 *Signal corruption*

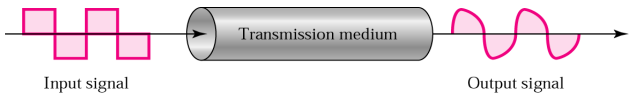


Figure 3.16 *A digital signal*

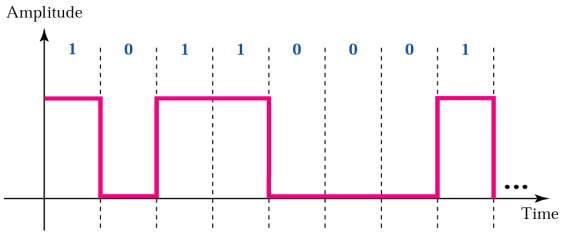


Figure 3.17 *Bit rate and bit interval*

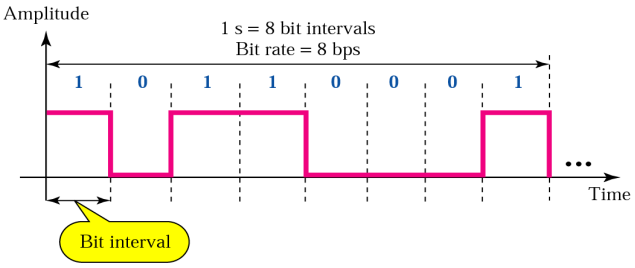


Figure 3.20 *Impairment types*

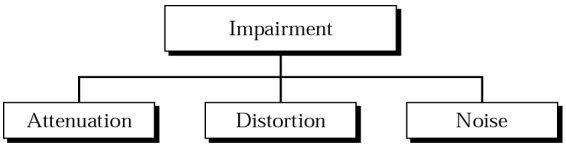


Figure 3.21 *Attenuation*

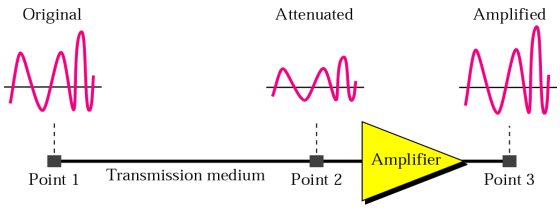


Figure 3.23 *Distortion*

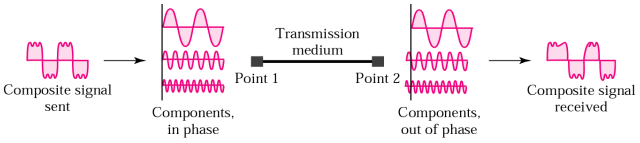
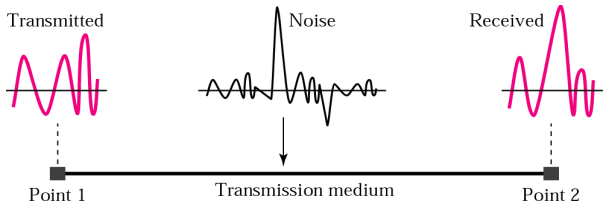


Figure 3.24 *Noise*



Chapter 4

Digital Transmission

Figure 4.1 *Line coding*

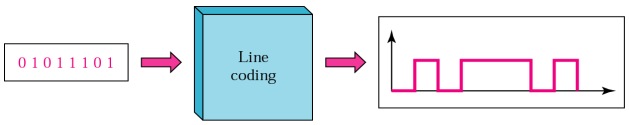
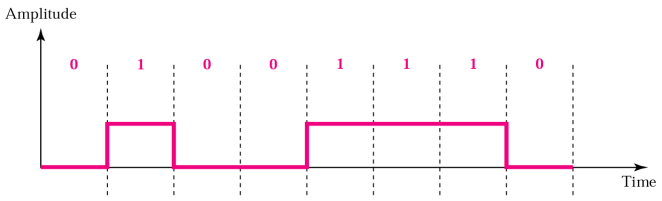


Figure 4.6 *Unipolar encoding*



Note:

A good encoded digital signal must contain a provision for synchronization.

Figure 4.10 *Manchester encoding*

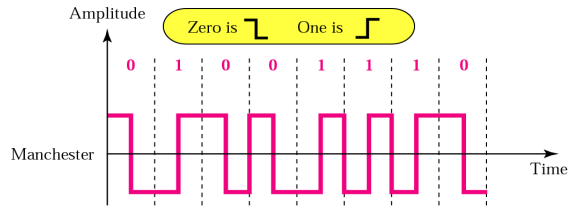


Figure 4.15 *Block coding*

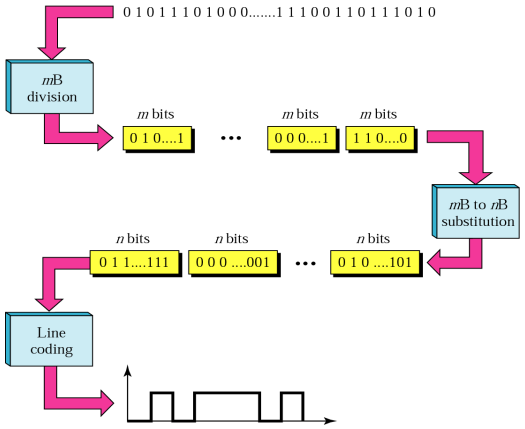


Figure 4.16 *Substitution in block coding*

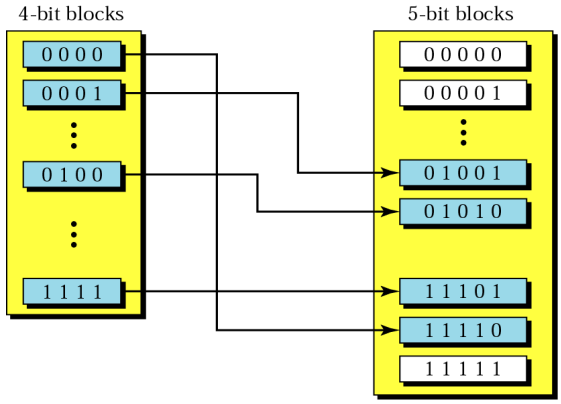
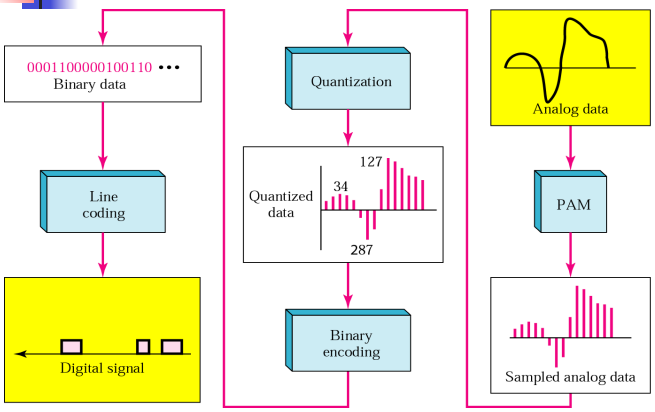


Figure 4.22 *From analog signal to PCM digital code*



Note:

According to the Nyquist theorem, the sampling rate must be at least 2 times the highest frequency.

Figure 4.24 *Data transmission*

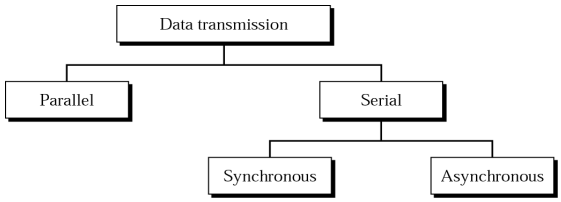


Figure 4.25 *Parallel transmission*

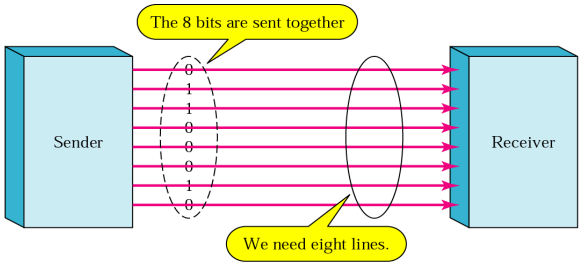


Figure 4.26 *Serial transmission*

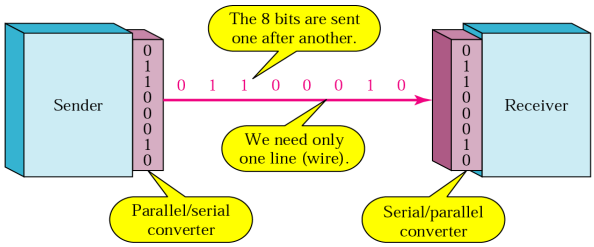


Figure 4.27 *Asynchronous transmission*

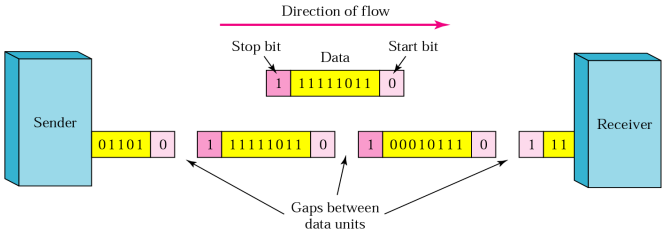
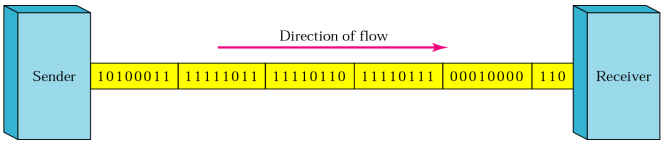


Figure 4.28 *Synchronous transmission*



Chapter 5

Analog Transmission

Figure 5.1 *Digital-to-analog modulation*

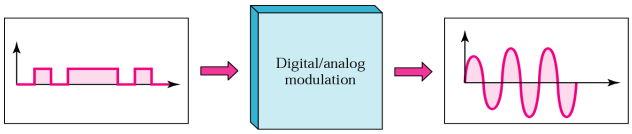
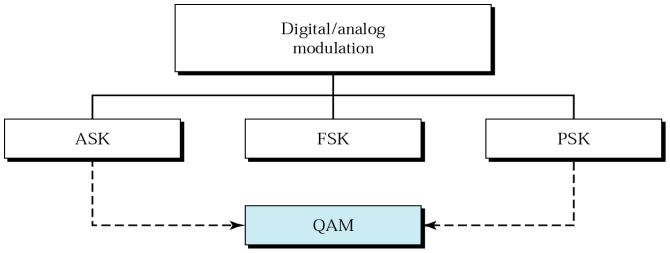


Figure 5.2 *Types of digital-to-analog modulation*



Note:

Bit rate is the number of bits per second. Baud rate is the number of signal units per second. Baud rate is less than or equal to the bit rate.

Figure 5.3 *ASK*

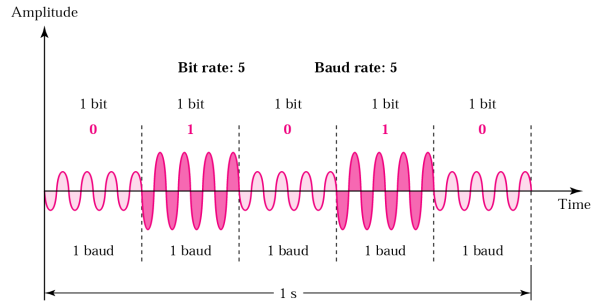


Figure 5.6 *FSK*

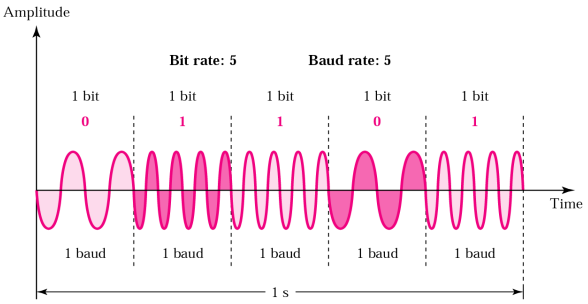


Figure 5.8 *PSK*

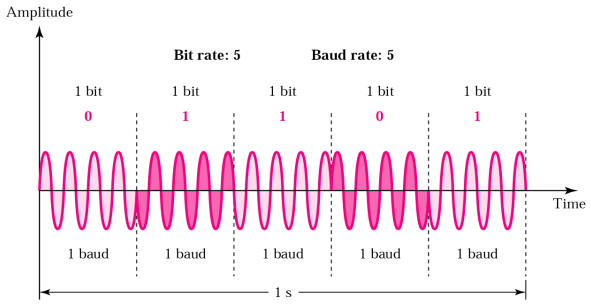
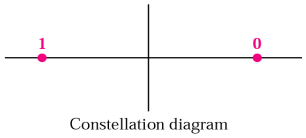


Figure 5.9 *PSK constellation*

Bit	Phase
0	0
1	180

Bits



Constellation diagram

Figure 5.10 *The 4-PSK method*

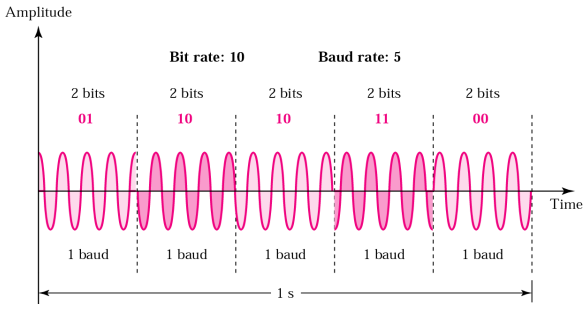
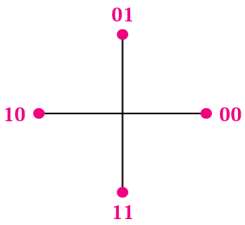


Figure 5.11 *The 4-PSK characteristics*

Dibit	Phase
00	0
01	90
10	180
11	270

Dibit
(2 bits)



Constellation diagram

Modem stands for modulator/ demodulator.

5.3 Modulation of Analog Signals

Amplitude Modulation (AM)

Frequency Modulation (FM)

Phase Modulation (PM)

Figure 5.24 *Analog-to-analog modulation*

Figure 5.25 *Types of analog-to-analog modulation*

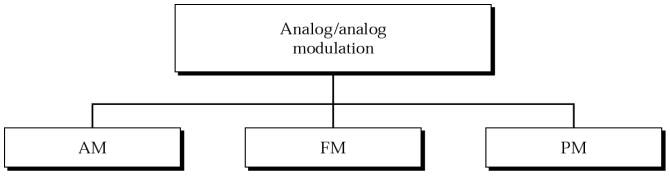


Figure 5.26 *Amplitude modulation*

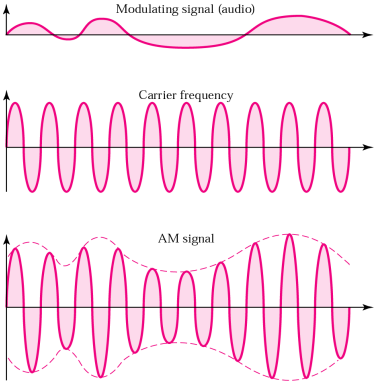


Figure 5.28 *AM band allocation*

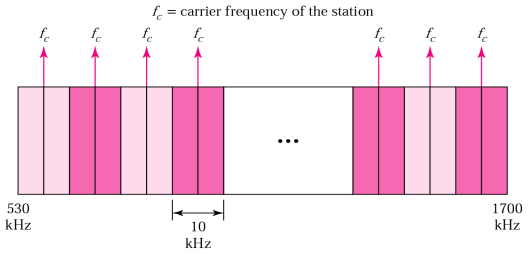


Figure 5.29 *Frequency modulation*

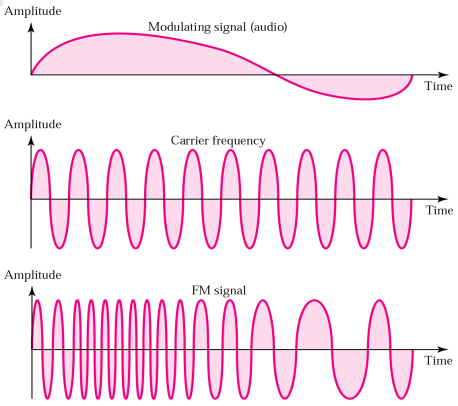
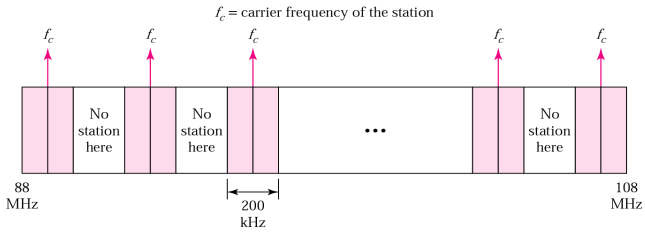


Figure 5.31 *FM band allocation*



Chapter 6

Multiplexing

Figure 6.1 *Dividing a link into channels*

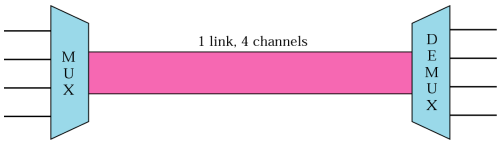


Figure 6.2 *Categories of multiplexing*

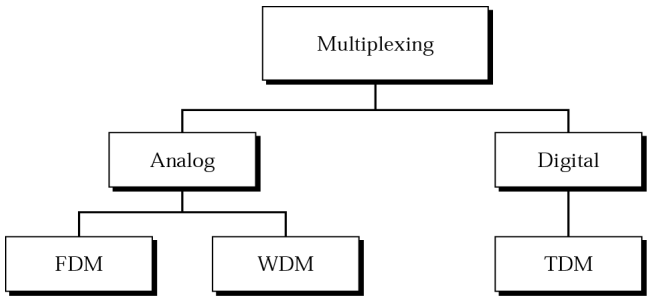


Figure 6.3 *FDM*

Figure 6.4 *FDM process*

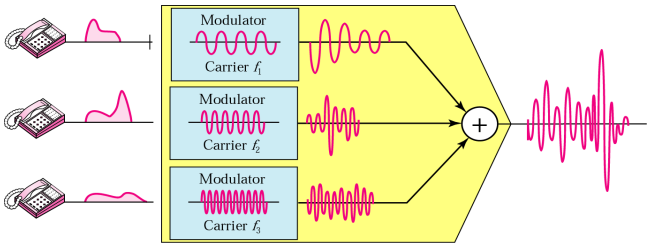


Figure 6.5 *FDM demultiplexing example*

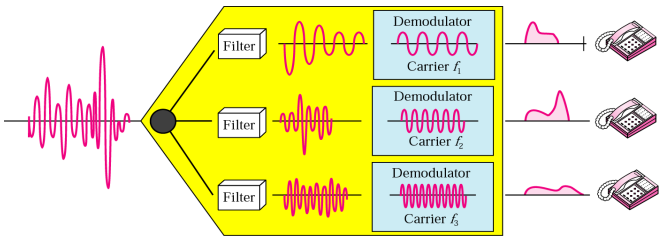


Figure 6.10 *WDM*

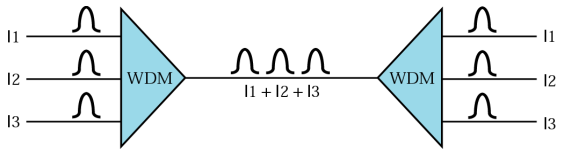


Figure 6.12 *TDM*

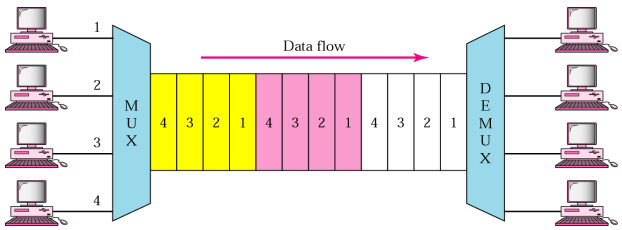


Figure 6.13 *TDM frames*

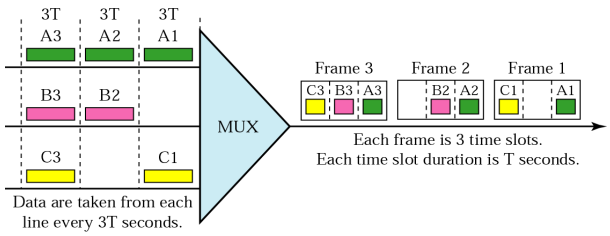
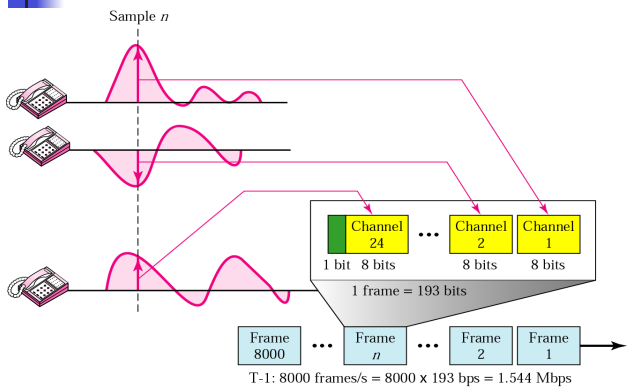


Figure 6.20 *T-1 frame structure*



Chapter 7

Transmission Media

Figure 7.1 *Transmission medium and physical layer*

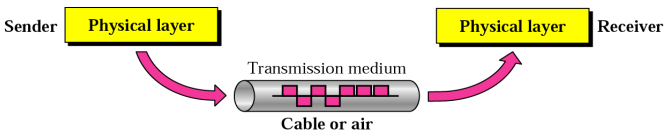


Figure 7.2 **Classes of transmission media**

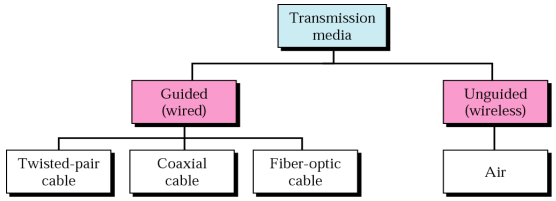


Figure 7.3 *Twisted-pair cable*

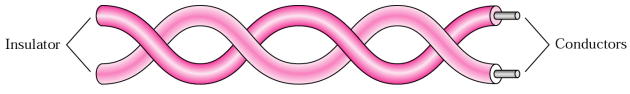


Figure 7.4 *UTP and STP*

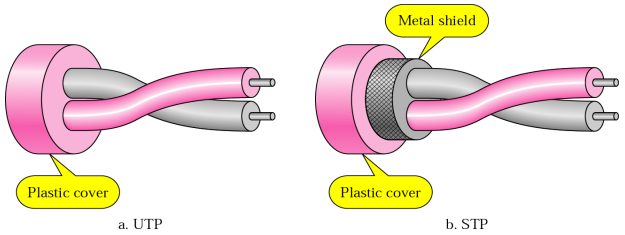


Figure 7.7 *Coaxial cable*

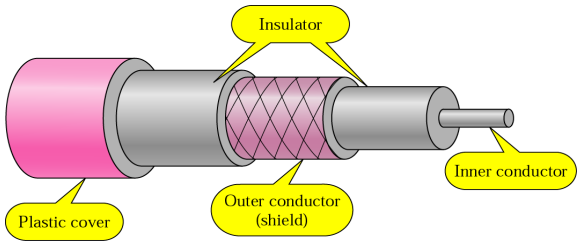


Figure 7.11 *Optical fiber*

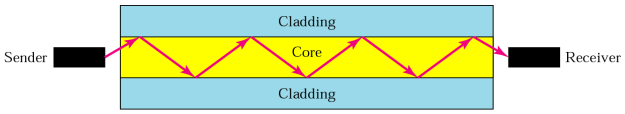
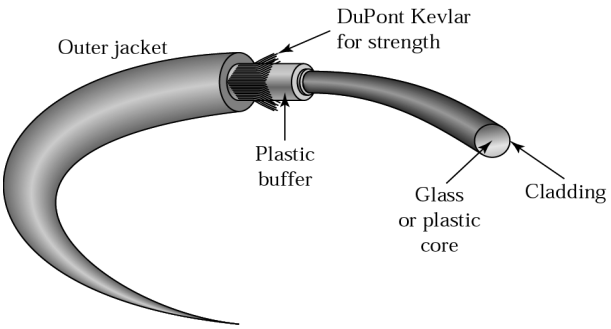
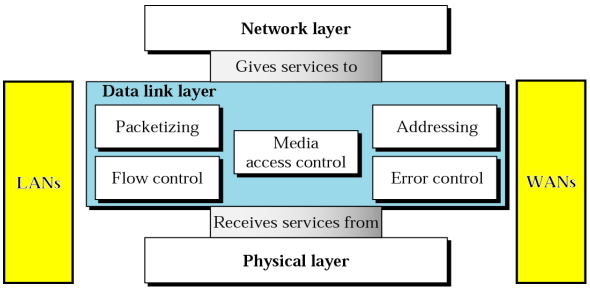


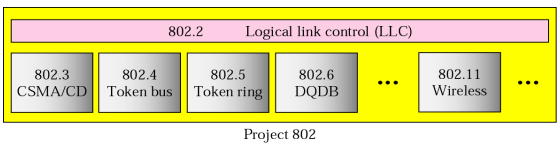
Figure 7.14 *Fiber construction*



Position of the data-link layer



IEEE standards for LANs



Project 802

Chapter 10

Error Detection and Correction

Note:

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.

10.1 Types of Error

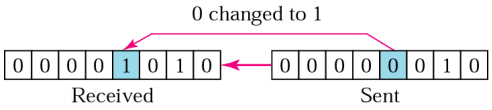
Single-Bit Error

Burst Error

Note:

In a single-bit error, only one bit in the data unit has changed.

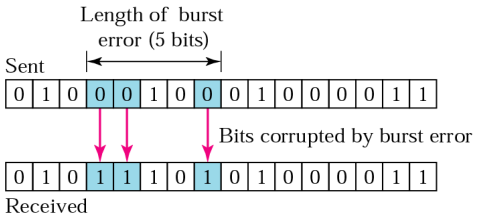
10.1 *Single-bit error*



Note:

A burst error means that 2 or more bits in the data unit have changed.

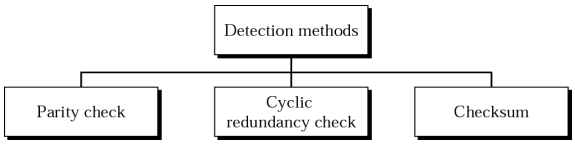
10.2 *Burst error of length 5*



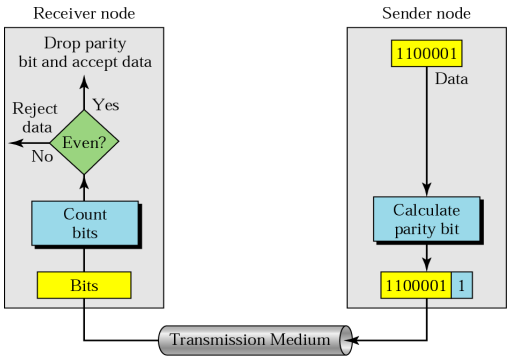
Note:

Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.

10.4 Detection methods



10.5 Even-parity concept



Example 1

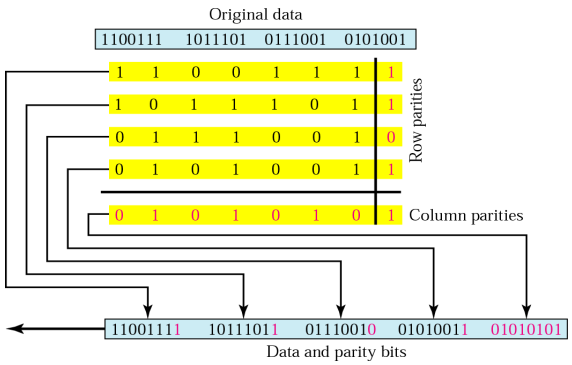
Suppose the sender wants to send the word *world*. In ASCII the five characters are coded as

1110111 1101111 1110010 1101100 1100100

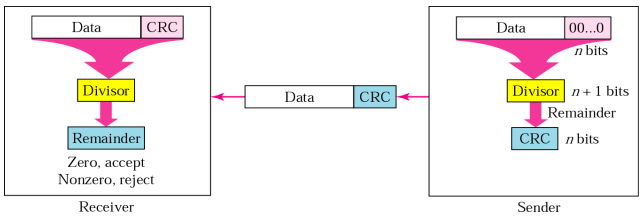
The following shows the actual bits sent

11101110 11011110 11100100 11011000 11001001

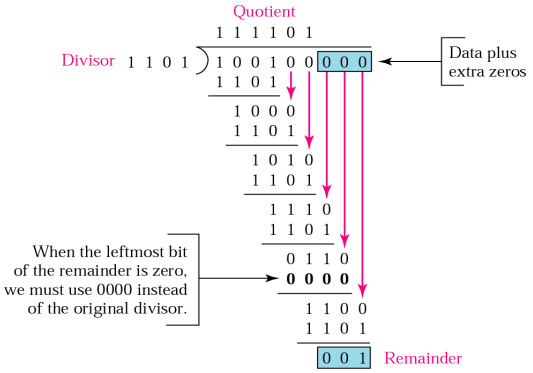
10.6 Two-dimensional parity



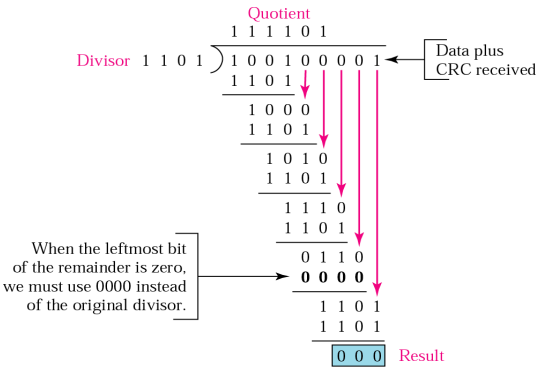
10.7 CRC generator and checker



10.8 Binary division in a CRC generator



10.9 Binary division in CRC checker



10.11 A polynomial representing a divisor

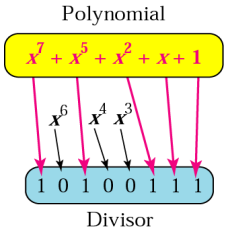
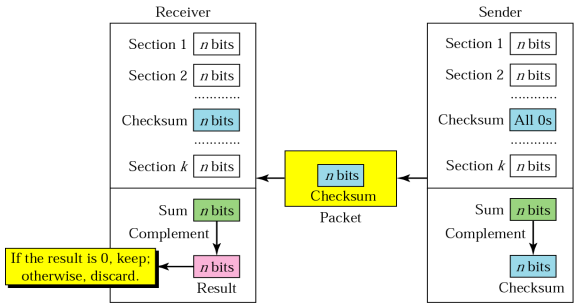


Table 10.1 Standard polynomials

Name	Polynomial	Application
CRC-8	$x^8 + x^2 + x + 1$	ATM header
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$	ATM AAL
ITU-16	$x^{16} + x^{12} + x^5 + 1$	HDLC
ITU-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	LANs

10.12 Checksum



Example 7

Suppose the following block of 16 bits is to be sent using a checksum of 8 bits.

10101001 00111001

The numbers are added using one's complement

10101001
00111001

Sum 11100010

Checksum **00011101**

The pattern sent is 10101001 00111001 **00011101**

Example 8

Now suppose the receiver receives the pattern sent in Example 7 and there is no error.

10101001 00111001 00011101

When the receiver adds the three sections, it will get all 1s, which, after complementing, is all 0s and shows that there is no error.

	10101001
	00111001
	00011101
Sum	11111111
Complement	**00000000** means that the pattern is OK.

10.3 Correction

Retransmission

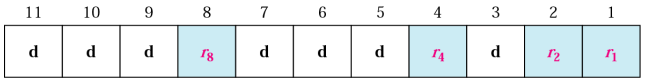
Forward Error Correction

Burst Error Correction

Table 10.2 Data and redundancy bits

Number of data bits m	Number of redundancy bits r	Total bits m + r
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

10.14 *Positions of redundancy bits in Hamming code*



Chapter 11

Data Link Control and Protocols

11.1 Flow and Error Control

Flow Control

Error Control

Note:

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

Note:

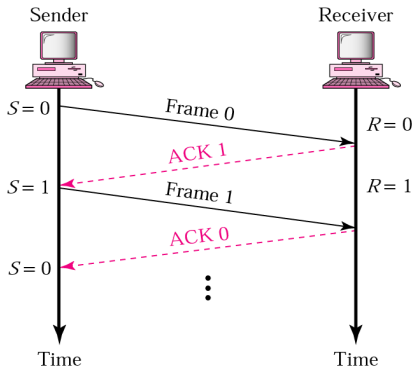
Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

11.2 Stop-and-Wait ARQ

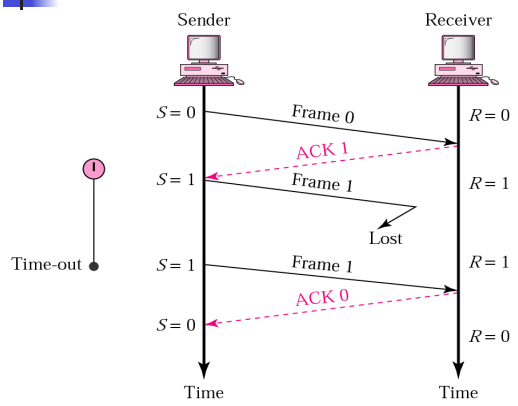
Operation

Bidirectional Transmission

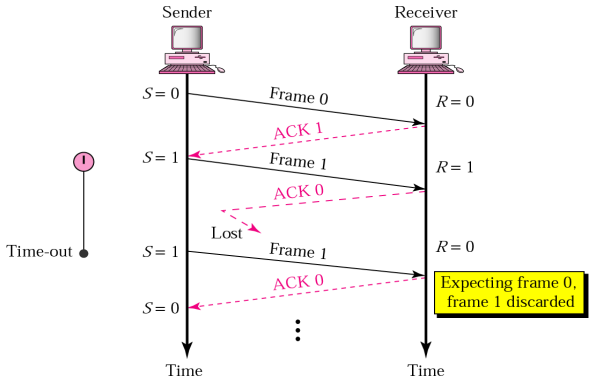
11.1 Normal operation



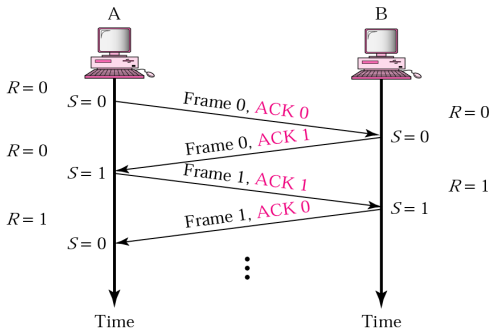
11.2 Stop-and-Wait ARQ, lost frame



11.3 Stop-and-Wait ARQ, lost ACK frame



11.5 Piggybacking



Chapter 14

Local Area Networks: *Ethernet*

Figure 14.4 Ethernet addresses in hexadecimal notation

06-01-02-01-2C-4B

Figure 14.16 A network with and without a bridge

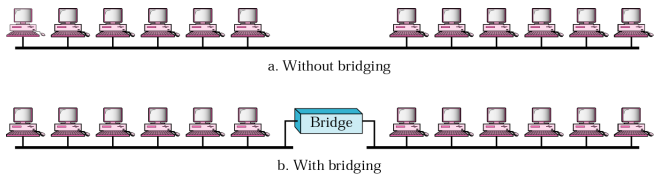


Figure 14.17 Collision domains in a nonbridged and bridged network

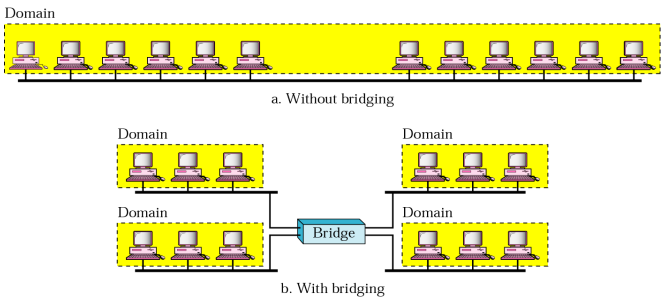


Figure 14.18 Switched Ethernet

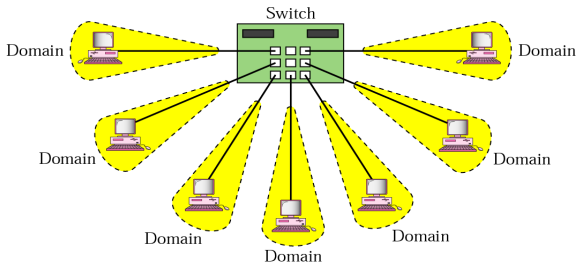


Figure 16.1 Connecting devices

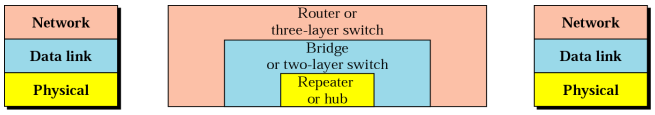


Figure 16.2 Repeater

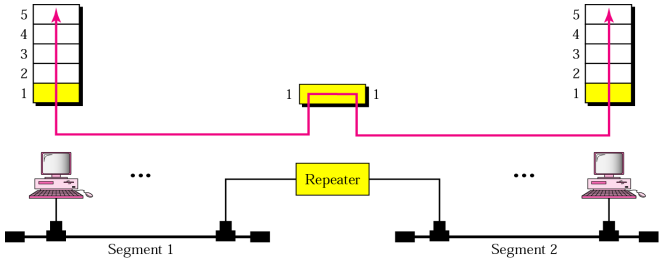


Figure 16.4 Hubs

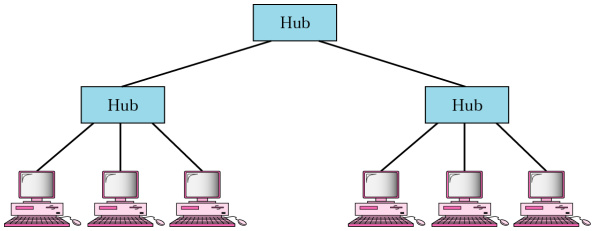


Figure 16.5 Bridge

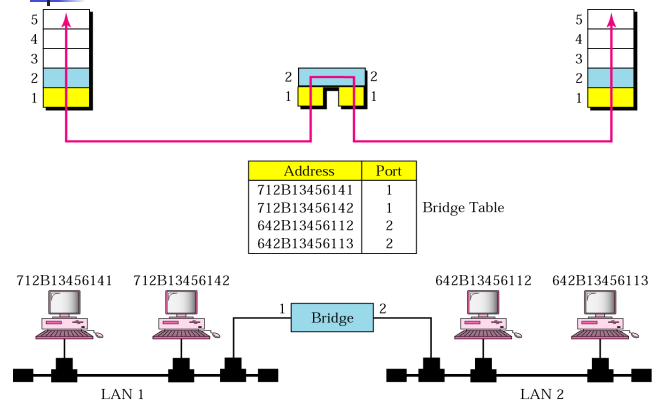


Figure 16.14 A switch connecting three LANs

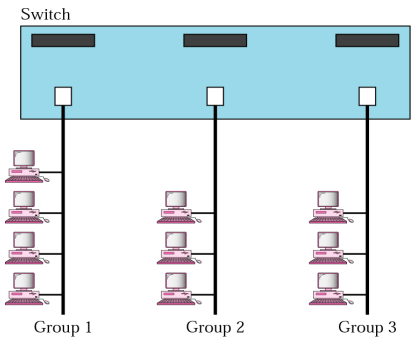


Figure 16.15 A switch using VLAN software

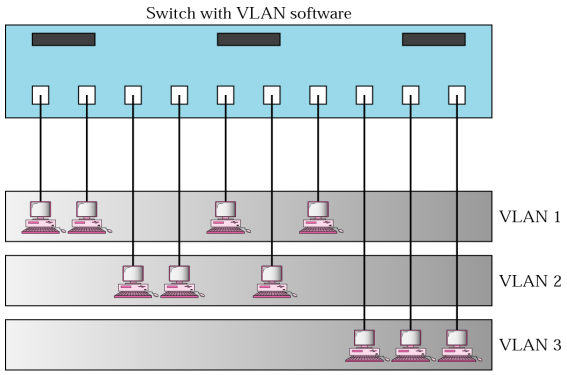
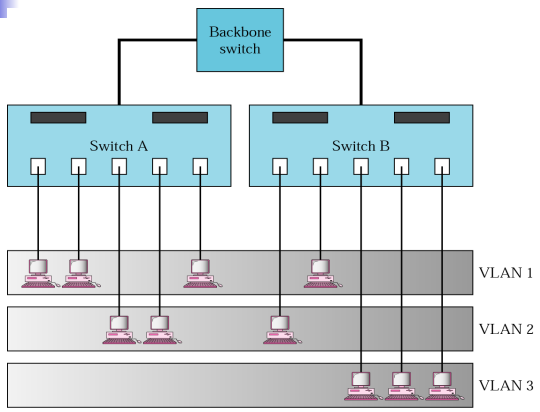


Figure 16.16 Two switches in a backbone using VLAN software



Sockets

¿Qué es un socket?

- Es una interfaz de acceso a la capa de transporte.
- Un socket provee de una interfaz general para comunicar procesos. No sólo a procesos locales dentro de una máquina, sino a procesos distribuidos en una redes de computadoras.
- Unión de IP + #Puerto + Protocolo de Nivel Transporte (TCP o UDP)

Requisitos para comunicación

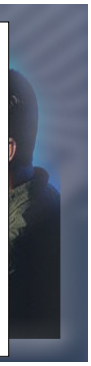
- Dirección de la computadora.
- Puerto.
- Analogía:
  - Número telefónico
  - Extensión.

SEGURIDAD EN REDES COMPUTACIONALES

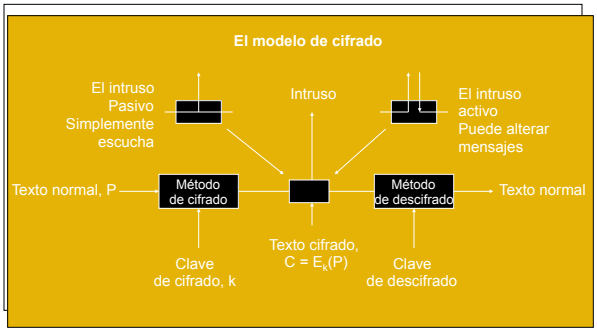
Areas principales

- Confidencialidad de la información (se preocupa por mantener la información fuera del alcance de usuarios no autorizados).
- Autentificación (Se encarga de determinar con quien se está hablando antes de revelar cualquier información).
- No repudiación (se encarga de las firmas)
- Integridad de la información (se asegura de que el mensaje recibido realmente fue el enviado).

- Los mecanismos de seguridad en redes de computadoras se basan principalmente en criptografía en la capa de aplicación.



Modelo de cifrado



Criptografía tradicional

- En la criptografía tradicional, se mantenía secreto el método de codificación de los mensajes y, si éste era descubierto, era necesario crear uno nuevo.

Criptografía por sustitución

- Cifrado por sustitución: cada letra o grupo de letra se remplaza por otra letra o grupo de letra. (Cifrado de César) El alfabeto se desplaza K posiciones. K es la clave de cifrado.
- Cifrado por sustitución monoalfabética. Cada uno de los símbolos del texto normal tiene una correspondencia con algún otro símbolo.
- Intruso: uso de estadísticas de los lenguajes.

Criptografía por sustitución

- Ejemplo:

Alfabeto normal: a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabeto cifrado: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

```
Texto normal : clase de redes
Texto cifrado: ESQLT RT KTRTL
```

- En este ejemplo la clave es la cadena de 26 letras del alfabeto.

Criptografía por transposición

- Clave: PRIVADO
- Mensaje: esteesunmensajemuysecreto

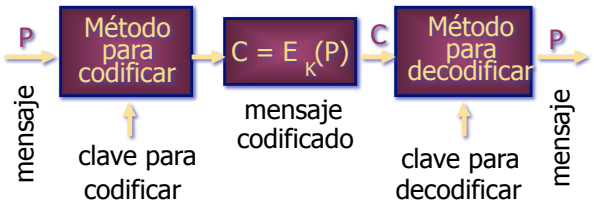
P	R	I	V	A	D	O
5	6	3	7	1	2	4
e	s	t	e	e	s	u
n	m	e	n	s	a	j
e	m	u	y	s	e	c
r	e	t	o	a	b	c

Mensaje cifrado: essasaebteutujccenersmmeenyo

Criptografía moderna

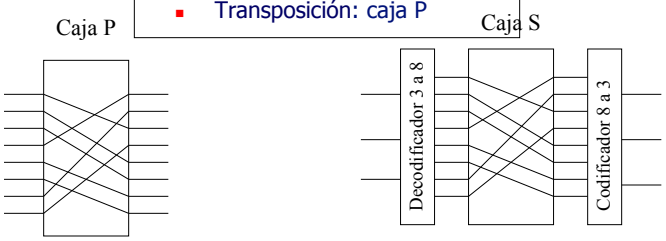
- Usa el mismo principio de que la tradicional (transposición y sustitución)
- Pero con un enfoque diferente :
  - El método de codificación es complejo y conocido.
  - Se utilizan claves, las cuales se mantienen secretas, para codificar o decodificar los mensajes.

Criptografía moderna



Criptografía moderna

- Existen circuitos para realizar las dos técnicas básicas de codificación:
  - Substitución: caja S
  - Transposición: caja P



Algoritmos de clave Pública

- Los algoritmos de clave secreta son seguros mientras no se conozca la clave.
- Su principal problema es la distribución de la clave, ya que utilizan la misma clave para codificar y decodificar.

Algoritmos de clave Pública

- La clave pública se utiliza para cifrar mensajes y es conocida por todos.
- La clave que se utiliza para descifrar es secreta y solamente la conoce la persona a quien va dirigido el mensaje, de tal forma que solamente ella lo puede descifrar.

Algoritmo RSA

- Para codificar (cifrar) un bloque P se calcula $C = P^e$ módulo n.
- Para decodificar (descifrar) C se calcula $P = C^d$ módulo n.
- La clave pública: (e, n).
- La clave privada: (d, n).

Algoritmo RSA

- La seguridad del método se basa en la dificultad de factorizar números grandes.
- Para factorizar números de 200 digitos se requiere de 4 mil millones de años de tiempo de cómputo.

Algoritmo RSA

- RSA al igual que DES es un algoritmo de sustitución monoalfabética. Debe de usarse alguna forma de encadenamiento.
- En la práctica se usa RSA principalmente para intercambiar una llave de sesión para poder usar DES o IDEA durante toda la sesión.
- RSA es muy lento para encriptar volúmenes grandes de datos.

FIRMAS ELECTRÓNICAS

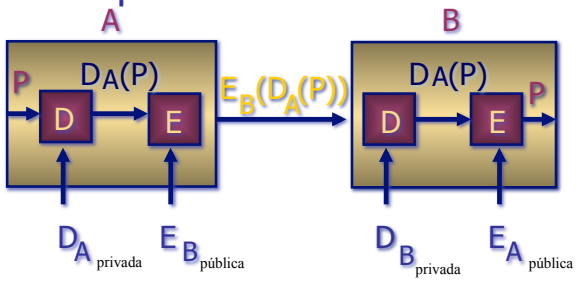
Firmas Electrónicas

- Las firmas electrónicas deben cumplir las siguientes funciones:
  - El receptor puede verificar la identidad de quien envía.

Firmas Electrónicas

- Quien envía no puede desconocer posteriormente el contenido el mensaje.
- El receptor no puede confeccionar o alterar el mensaje.

Firmas electrónicas usando llaves publicas



Al tener B $D_A(P)$ y P, A no puede negar que envió el mensaje P a B, ya que es el único que puede generar $D_A(P)$. (El algoritmo para D y E puede ser RSA)

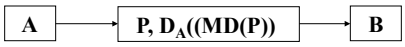
COMPENDIOS DE MENSAJES

Compendios de Mensajes

- Codificar un mensaje requiere mucho cómputo. Para simplificar el proceso, se crearon los compendios de mensajes (MD=Message digest).
- Un compendio de un mensaje se genera al aplicar una función de "Hashing" a un mensaje, lo cual produce una cadena de bits de longitud fija.

Compendios de Mensajes

- En este esquema, se envía el mensaje normal (P) y se envía el compendio del mensaje codificado.



D_A es un criptosistema.

- Sirve para validar identificación y ... Pero no para mantener sectreto el mensaje.

Domain Name System

Víctor Acevedo
<vacevedo@nic.mx>

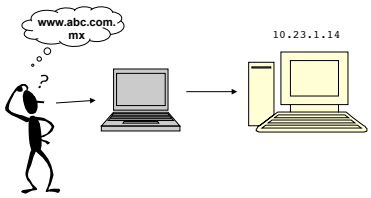
Introducción al DNS

- Utilizamos DNS cada vez que hacemos uso de un servicio de Internet, como el correo electrónico, http, telnet o ftp
- La finalidad del DNS es facilitar la comunicación con los equipos ubicados en la red; haciendo referencia por nombre en vez de direcciones numéricas.

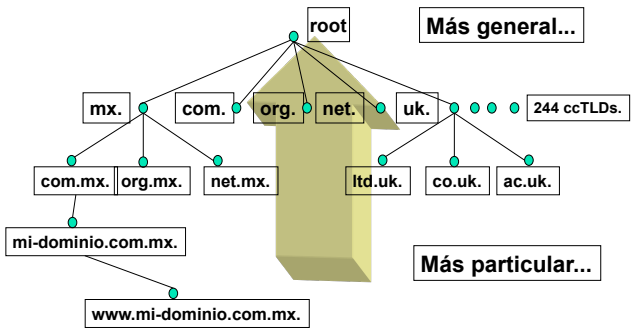
¿Por qué utilizar DNS ?

- Las máquinas se comunican con números (direcciones IP y MAC address). Los humanos nos comunicamos con las máquinas a través de nombres.

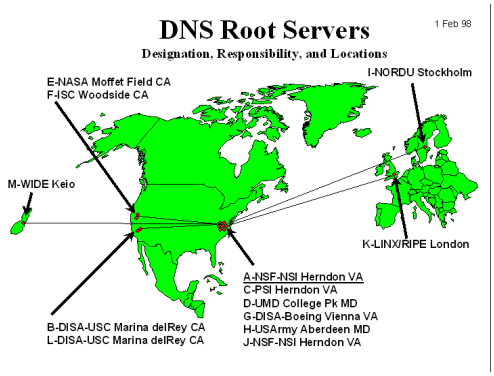
Y esto nos resulta más fácil...



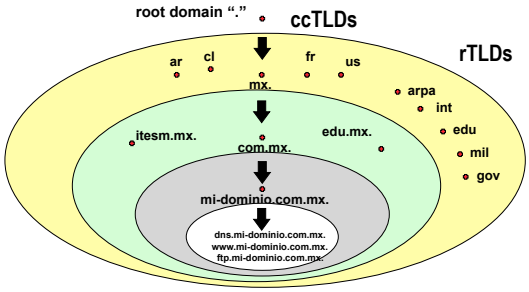
Estructura Jerárquica



Root-Servers



Delegación de dominios



Un día en la vida de un Servidor de Nombres

El proceso de resolución

theone.victor.com.mx

theone# ping www.madelafu.com.mx

El proceso de resolución

- La estacion **theone**, consulta su servidor de nombres configurado **pregun.tame.com.mx**, por la dirección de **www.madelafu.com.mx**

pregun.tame.com.mx

¿Cuál es la IP de www.madelafu.com.mx ?

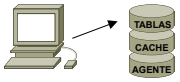
theone.victor.com.mx

theone# ping www.madelafu.com.mx

El proceso de resolución

- Consulta en sus tablas si tiene el dominio **www.madelafu.com.mx**

pregun.tame.com.mx

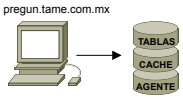


theone.victor.com.mx

theone# ping www.madelafu.com.mx

El proceso de resolución

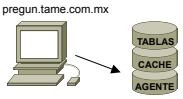
• No encuentra en Tablas, consulta en su memoria CACHE si tiene información sobre **.mx**, **com.mx**, **madelafu.com.mx** o **www.madelafu.com.mx**



theone# ping www.madelafu.com.mx

El proceso de resolución

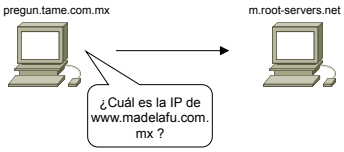
• No encuentra información en su CACHE el agente busca en otros servidores



theone# ping www.madelafu.com.mx

El proceso de resolución

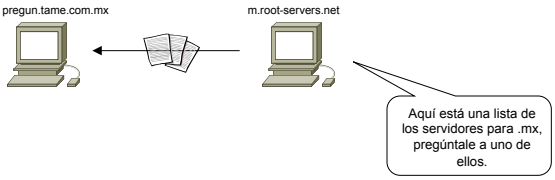
• El servidor de nombres **nombres**, consulta un root-server por **www.madelafu.com.mx**



theone# ping www.madelafu.com.mx

El proceso de resolución

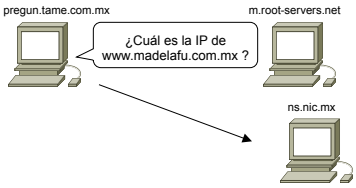
• El root-server **m**, envía a **pregun.tame.com.mx** los servidores autoritativos para **.mx**, este proceso se conoce como **referral**



theone# ping www.madelafu.com.mx

El proceso de resolución

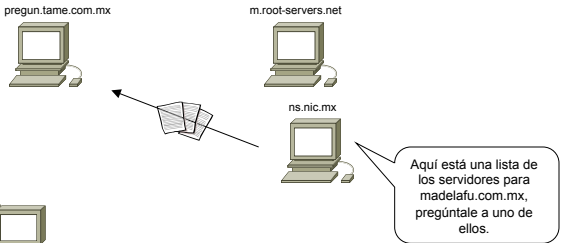
• El name server **pregun.tame.com.mx**, consulta al name server **ns.nic.mx** por la dirección de **www.madelafu.com.mx**



theone# ping www.madelafu.com.mx

El proceso de resolución

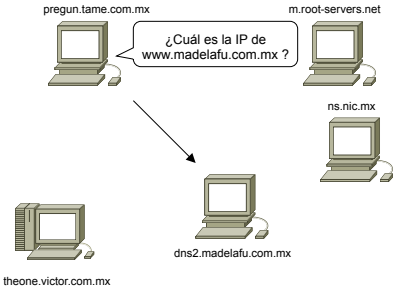
• **ns.nic.mx** contesta a **pregun.tame.com.mx** con la lista de servidores de nombres de **madelafu.com.mx**



theone# ping www.madelafu.com.mx

El proceso de resolución

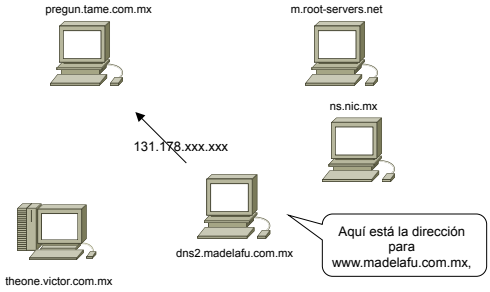
• El name server **pregun.tame.com.mx**, consulta al name server **dns2.madelafu.com.mx** por la dirección de **www.madelafu.com.mx**



theone# ping www.madelafu.com.mx

El proceso de resolución

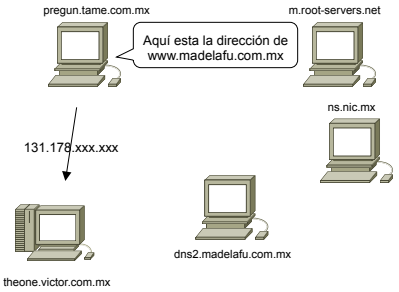
• dns2.madelafu.com.mx contesta con la dirección IP de **www.madelafu.com.mx**



theone# ping www.madelafu.com.mx

El proceso de resolución

• **pregun.tame.com.mx** contesta a **theone.victor.com.mx** con la dirección IP de **www.madelafu.com.mx**



theone# ping www.madelafu.com.mx