

Redes y Comunicaciones

TCP/IP

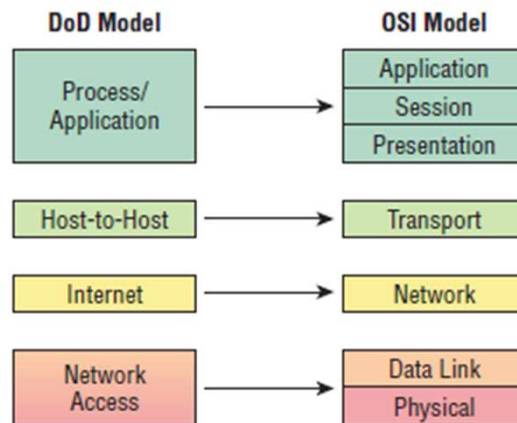
Presentación elaborada por el profesor: Álvaro Pachón y fue adaptada para este curso.

Agenda

- Resumen TCP/IP
- Direccionamiento IPv4
- Ejercicio
- Preguntas próxima clase

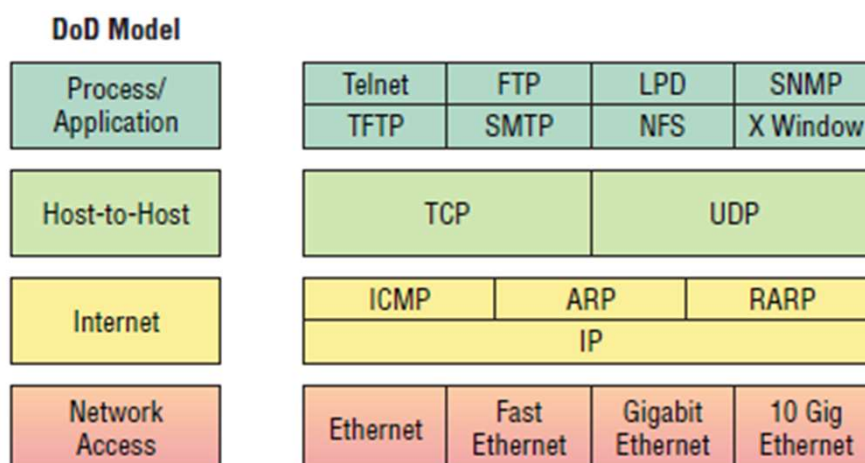
3- Modelo TCP/IP.

1- Pila **ESTRATIFICADA** y **JERÁRQUICA** de protocolos.



3

3- Modelo TCP/IP.



4

3- Modelo TCP/IP.

3.1. Nivel Físico

- A- Transporta bits en una trama a través de un enlace.
- B- Requerimiento: MEDIO DE TRANSMISIÓN.
- C- Mensajero: SEÑAL.
- D- Unidad lógica: BIT.

5

3- Modelo TCP/IP.

3.2. Nivel de Enlace

- A- Encapsula un datagrama en una TRAMA.
- B- Envía tramas a través del enlace de datos.
- C- NO se define protocolo específico= f(tecnología).
- D- Protocolo = Diferentes servicios:
 - a- Detección de Errores.
 - b- Detección/Corrección de errores.

6

3- Modelo TCP/IP.

3.3. Nivel de Red

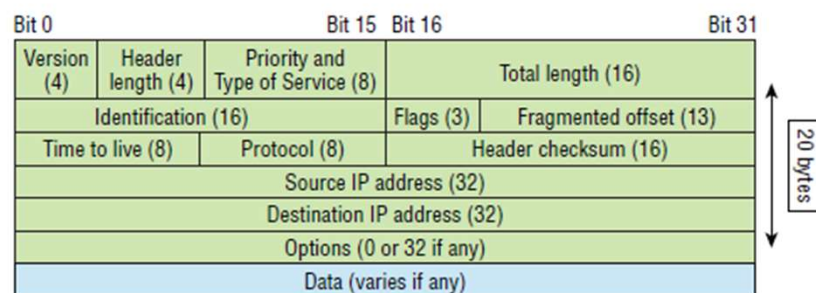
- A- Permite el intercambio entre FUENTE/DESTINO.
- B- Comunicación: HOST-a-HOST
- C- Aspecto clave: RUTA.
- D- Protocolo: Internet Protocol (IP).
 - a- Define el formato del DATAGRAMA.
 - b- Define estructura de las direcciones.
 - c- Responsabilidad: Enrutamiento.
 - d- Protocolo NO orientado a conexión.

7

3- Modelo TCP/IP.

Paquete IP:

IP header



8

3- Modelo TCP/IP.

H- Paquete IP:

Version IP version number.

Header length Header length (HLEN) in 32-bit words.

Priority and Type of Service Type of Service tells how the datagram should be handled. The first 3 bits are the priority bits, now called the differentiated services bits.

Total length Length of the packet, including header and data.

Identification Unique IP-packet value used to differentiate fragmented packets from different datagrams.

Flags Specifies whether fragmentation should occur.

Fragment offset Provides fragmentation and reassembly if the packet is too large to put in a frame. It also allows different maximum transmission units (MTUs) on the Internet.

Time To Live The time to live (TTL) is set into a packet when it is originally generated. If it doesn't get to where it's supposed to go before the TTL expires, boom—it's gone. This stops IP packets from continuously circling the network looking for a home.

Protocol Port of upper-layer protocol; for example, TCP is port 6 or UDP is port 17. Also supports Network layer protocols, like ARP and ICMP, and can be referred to as the Type field in some analyzers. We'll talk about this field more in a minute.

Header checksum Cyclic redundancy check (CRC) on header only.

Source IP address 32-bit IP address of sending station.

Destination IP address 32-bit IP address of the station this packet is destined for.

Options Used for network testing, debugging, security, and more.

Data After the IP option field, will be the upper-layer data.

9

3- Modelo TCP/IP.

3.3. Nivel de Red

D- Protocolos de enrutamiento Unicast y Multicast.

E- Protocolos auxiliares:

a- ICMP (*Internet Control Message Protocol*).

b- IGMP (*Internet Group Management Protocol*).

c- DHCP (*Dynamic Host Configuration Protocol*)

d- ARP (*Address Resolution Protocol*)

10

3- Modelo TCP/IP.

3.4. Nivel de Transporte

- A- Permite conexión lógica extremo-a-extremo.
- B- Maneja **SEGMENTO** enviado a través de la conexión lógica.
- C- Protocolos:
 - a- **TCP (Transport Control Protocol).**
 - b- **UDP (User Datagram Protocol).**

11

3- Modelo TCP/IP.

D- Formato SEGMENTO TCP

TCP segment format

16-bit source port		16-bit destination port	
32-bit sequence number			
32-Bit Acknowledgment Number			
4-bit header length	Reserved	Flags	16-bit window size
16-bit TCP checksum		16-bit urgent pointer	
Options			
Data			

12

3- Modelo TCP/IP.

D- Formato SEGMENTO TCP

Source port This is the port number of the application on the host sending the data, which I'll talk about more thoroughly a little later in this chapter.

Destination port This is the port number of the application requested on the destination host.

Sequence number A number used by TCP that puts the data back in the correct order or retransmits missing or damaged data during a process called sequencing.

Acknowledgment number The value is the TCP octet that is expected next.

Header length The number of 32-bit words in the TCP header, which indicates where the data begins. The TCP header (even one including options) is an integral number of 32 bits in length.

Reserved Always set to zero.

Code bits/flags Controls functions used to set up and terminate a session.

Window The window size the sender is willing to accept, in octets.

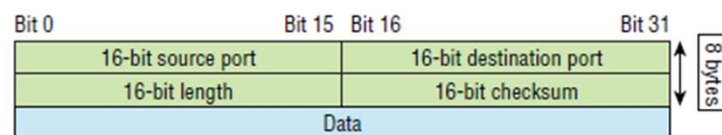
Checksum The cyclic redundancy check (CRC), used because TCP doesn't trust the lower layers and checks everything. The CRC checks the header and data fields.

13

3- Modelo TCP/IP.

E- Formato SEGMENTO UDP

UDP segment



Source port Port number of the application on the host sending the data

Destination port Port number of the application requested on the destination host

Length Length of UDP header and UDP data

Checksum Checksum of both the UDP header and UDP data fields

Data Upper-layer data

14

3- Modelo TCP/IP.

3.5. Nivel de Aplicación

A- Comunicación a nivel de PROCESOS.

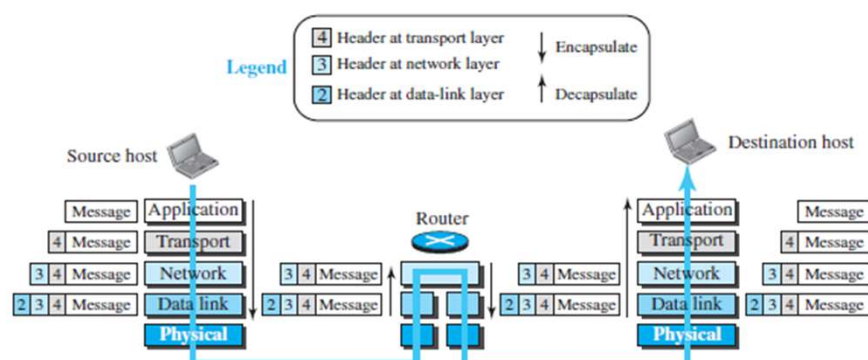
B- Protocolos:

- a- HTTP (*Hypertext Transfer Protocol*).
- b- SMTP (*Simple Mail Transfer Protocol*).
- c- FTP (*File Transfer Protocol*).
- e- DNS (*Domain Name System*).
- f- SSH (*Secure SHell*).

15

3- Modelo TCP/IP.

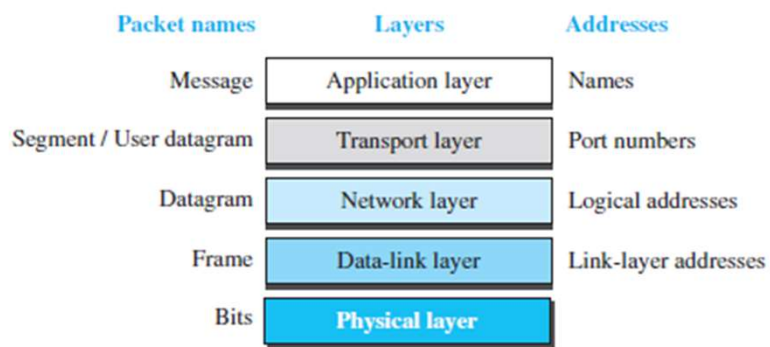
A- Encapsulamiento/Desencapsulamiento.



16

3- Modelo TCP/IP.

B- Direcccionamiento.



17

3- Modelo TCP/IP.

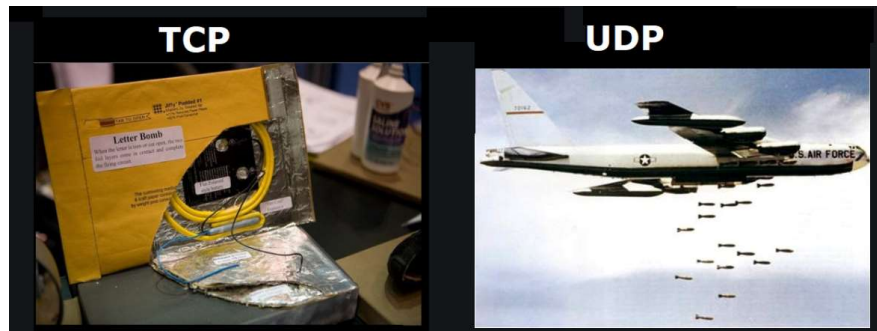
F- TCP vs UDP

Key features of TCP and UDP

TCP	UDP
Sequenced	Unsequenced
Reliable	Unreliable
Connection-oriented	Connectionless
Virtual circuit	Low overhead
Acknowledgments	No acknowledgment
Windowing flow control	No windowing or flow control of any type

18

3- Modelo TCP/IP.

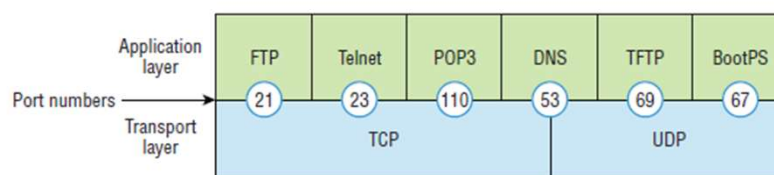


19

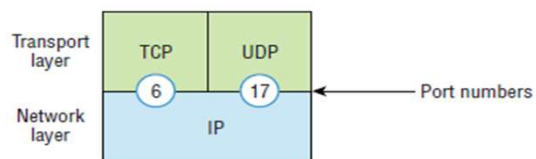
3- Modelo TCP/IP.

G- Números de puertos (TCP,UDP):

Port numbers for TCP and UDP



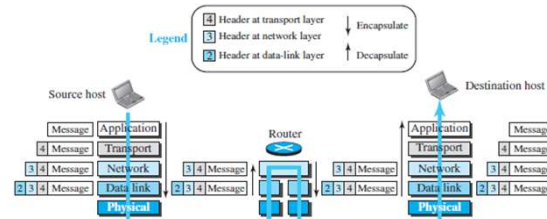
The Protocol field in an IP header



20

3- Modelo TCP/IP.

Ejemplo:

[illegible]

3- Modelo TCP/IP.

[illegible]

3- Modelo TCP/IP.

C:\Users\alejo\Desktop\Wireshark 1.127\c1.v1102-0-g768978 from master-112

File Edit View Go Capture Window Statistics Help

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
5585	1.0397/04	192.168.231.61	192.168.231.63	TCP	60	508 dropbox LAN SYN discovery PRODUCE
5585	1.057815	192.168.231.61	255.255.255.255	UDP-LSP-DI	508	dropbox LAN SYN discovery Protocol
5586	1.260385	192.168.230.77	50.97.149.90	TLVSL-2	180	client key Exchange, change Cipher Spec, Hello Request, H
5587	1.274713	f680::288b:fdd3:e927::ff02::1:2		DHCPv6-P	173	solicit Id: 0x5e162b Cid: 00010001199f16f390b1c93f23e
5587	1.2864014	50.97.149.90	192.168.230.77	TCP	60	64104->64104 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440
5589	1.2864709	192.168.230.77	23.154.108	TCP	54	64104->http [ACK] Seq=1 Acks=2801 Win=65792 Len=0
5590	1.285453	192.168.230.77	23.154.108	HTTP	609	GET /content/damnantthumbna1/3d5738341ebc64dbde920904c
5591	1.2862043	151.101.6.2	192.168.230.77	TCP	60	http [ACK] [ACK] Seq=1 Acks=2801 Win=34816 Len=0
5592	1.2692107	192.168.230.77	151.101.6.2	TCP	1454	(TCP segment of a reassembled PDU)
5593	1.2692118	192.168.230.77	151.101.6.2	TCP	186	GET /elpais/tcr/3jsont?m=1533A4263A10_279&data=7b%2c21c
5594	1.2724277	192.168.230.77	216.58.222.226	QUIC	1392	CID: 17077540981487145675, Seq: 1
5595	1.2724760	192.168.230.77	216.58.222.226	QUIC	343	CID: 17077540981487145675, Seq: 2
5596	1.2743351	50.97.149.90	192.168.230.77	TCP	1454	(TCP segment of a reassembled PDU)
5597	1.2743581	50.97.149.90	192.168.230.77	TCP	1454	(TCP segment of a reassembled PDU)
5598	1.2743631	192.168.230.77	50.97.149.90	TCP	54	64095->https [ACK] seq=3173 ack=6117 win=65792 Len=0
5599	1.2743649	50.97.149.90	192.168.230.77	TCP	1454	(TCP segment of a reassembled PDU)
5600	1.2743677	50.97.149.90	192.168.230.77	TLVSL-2	q67	Amification nara

Frame 590: 609 bytes on wire (4872 bits), 609 bytes captured (4872 bits) on #0
Ethernet II, Src: Dell41:ef:46 (d0:d6:e5:41:ef:46), Dst: Cisco_e1:1e:3f (00:22:90:e1:1e:3f)
Internet Protocol Version 4, Src: 192.168.230.77 (192.168.230.77), Dst: 23.154.108 (23.154.108)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT - ECN-Capable Transport)
Total Length: 595
Identification: 0xf025 (3877)
Flags: 0x02 (Don't Fragment)
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
Source: 192.168.230.77 (192.168.230.77)
Destination: 23.154.108 (23.154.108)
[Source GeoIP: unknown]
[Destination GeoIP: unknown]
Transmission Control Protocol, Src Port: 64104 (64104), Dst Port: http (80), Seq: 1, Ack: 1, Len: 555
Hypertext Transfer Protocol

23

3- Modelo TCP/IP.

[illegible]

24

3- Modelo TCP/IP.

[illegible]