

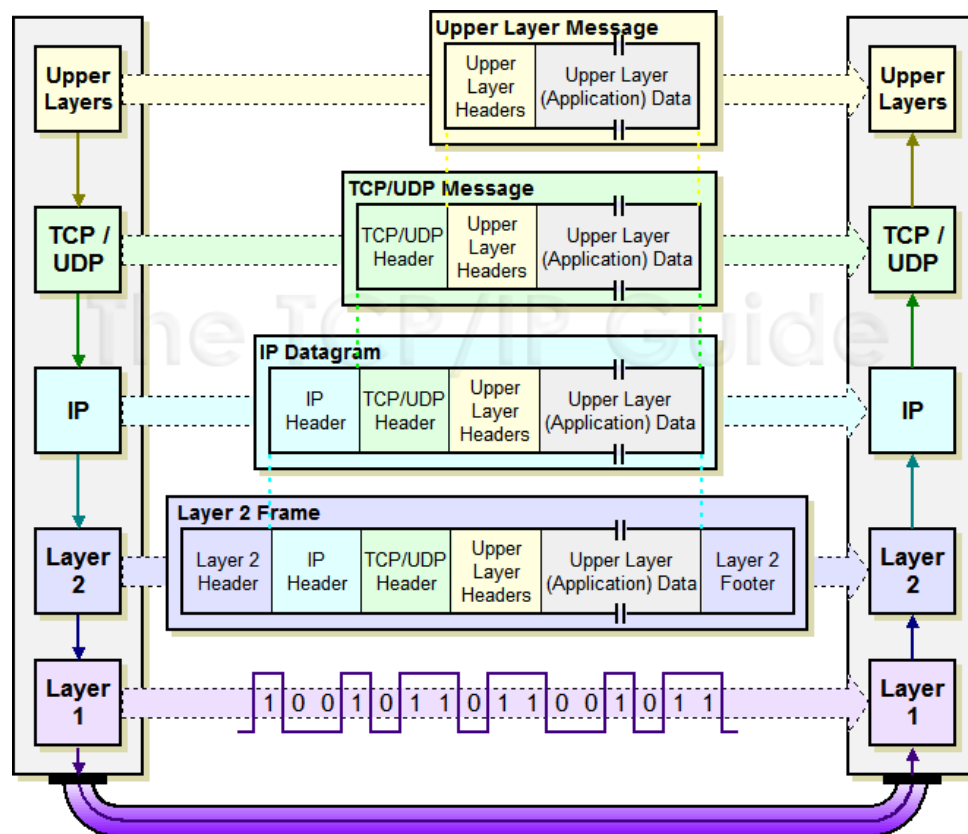
Trabajo de laboratorio nº 6

Trabajo práctico Redes de Información

Alumna: Victoria Ruiz Schulze

Curso: K4573

2do cuatrimestre 2022



Índice

Trabajo práctico Redes de Información	1
Tareas de análisis	3
a. Análisis del tráfico que produce un protocolo orientado a la conexión	3
b. Análisis del tráfico que produce un protocolo no orientado a la conexión.	5
c. DHCP – HTTP – HTTPS – FTP – DNS	6

Tareas de análisis

a. Tráfico que produce un protocolo orientado a la conexión

1. Se analiza una **secuencia de tramas TCP**. Encapsulamiento: Ethernet II > IPv4 > TCP.

2a. Conexión TCP.

- Para establecer la conexión TCP se utilizan 3 segmentos ("three-way handshake").
SYN > SYN-ACK > ACK
- Para cerrar la conexión se usan 4 segmentos.
FIN-ACK > ACK > FIN-ACK > ACK

Establecimiento de la conexión:

Protocolo	Source	Destination	Info
TCP	145.254.160.237	65.208.228.223	3372 → 80 [SYN] Seq=0 Win=8760 L
TCP	65.208.228.223	145.254.160.237	80 → 3372 [SYN, ACK] Seq=0 Ack=1
TCP	145.254.160.237	65.208.228.223	3372 → 80 [ACK] Seq=1 Ack=1 Win=
HTTP	145.254.160.237	65.208.228.223	GET /download.html HTTP/1.1

Fin de la conexión:

TCP	65.208.228.223	145.254.160.237	80 → 3372 [FIN, ACK] Seq=18365 Ack=480
TCP	145.254.160.237	65.208.228.223	3372 → 80 [ACK] Seq=480 Ack=18366 Win=
TCP	145.254.160.237	65.208.228.223	3372 → 80 [FIN, ACK] Seq=480 Ack=18366
TCP	65.208.228.223	145.254.160.237	80 → 3372 [ACK] Seq=18366 Ack=481 Win=

2b. Conexión lógica (sockets)

La confiabilidad y los mecanismos de control de flujo requieren que TCP inicialice y mantenga cierta información de estado para cada flujo de datos. La combinación de este estado, incluyendo sockets, números de secuencia y tamaños de ventana, se llama conexión lógica. Cada conexión se identifica unívocamente por el par de sockets usados por los procesos emisor y receptor.

Un socket, tanto para TCP como UDP, viene definido por los siguientes parámetros:

- Protocolo de la capa de transporte utilizado: TCP o UDP
- Dirección IP de origen.
- Dirección IP de destino.

- Puerto de origen o local.
- Puerto de destino o remoto.

Estos parámetros permiten que cada una de las conexiones que se realicen sean únicas, y que tanto el origen como el destino puedan identificar unívocamente la conexión al intercambiar datos.

2c. Transferencia de datos a través de un canal.

La conexión capturada se dio en 43 paquetes. Los primeros 3 fueron usados para el establecimiento de la conexión, y los últimos 4, para el cierre. Por ende, se usaron 36 paquetes para la transferencia de datos.

2d. En el nivel de transporte, TCP proporciona los siguientes servicios:

- Ordenamiento y reensamble. Cada PDU tiene un número de secuencia y de confirmación, que permiten llevar registro de los paquetes recibidos y enviados en orden.
- Fiabilidad. TCP utiliza un esquema de reconocimientos acumulativos, es decir, el receptor informa con el número de reconocimiento de hasta qué octeto del flujo de datos enviados ha recibido correctamente. Sabe que lo ha recibido correctamente porque el paquete tiene un campo de Checksum que garantiza la entrega libre de errores tanto de la cabecera como de los datos del paquete.
- Control de errores: con el campo Checksum se verifica si el paquete llegó libre de errores. En caso de no recibir un ACK, después de un tiempo el emisor retransmitirá el mensaje.
- Control de flujo. TCP implementa el "modelo de otorgamiento de créditos" para controlar el flujo. Cada extremo de la comunicación le indica al otro cuántos bytes tiene permitidos enviarle antes de esperar una confirmación. Además, con cada confirmación se envía nuevamente el valor de esa ventana/window.
- Multiplexación. Se logra usando puertos.
- Conexión Full Duplex. Gracias al uso de números de secuencia y confirmación diferentes por parte de emisor y receptor, ambos pueden enviar mensajes concurrentemente.

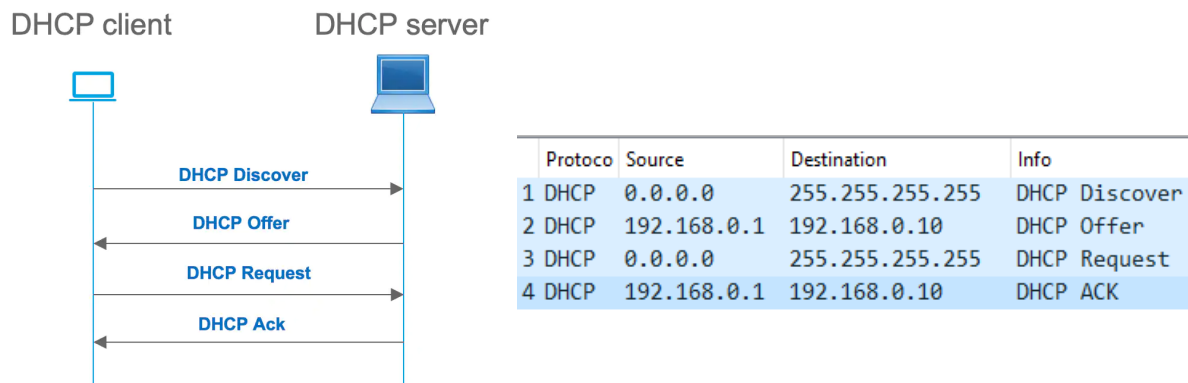
2e. Cierre de conexión.

Se utilizan un total de cuatro segmentos para liberar, dos para el transmisor y dos, para el receptor.

b. Tráfico que produce un protocolo no orientado a la conexión.

1. Se analiza una **serie de comunicaciones de DHCP**, encapsulados en el protocolo UDP.

2. Comunicación de tramas:



2a. UDP proporciona los siguientes servicios en el nivel de transporte:

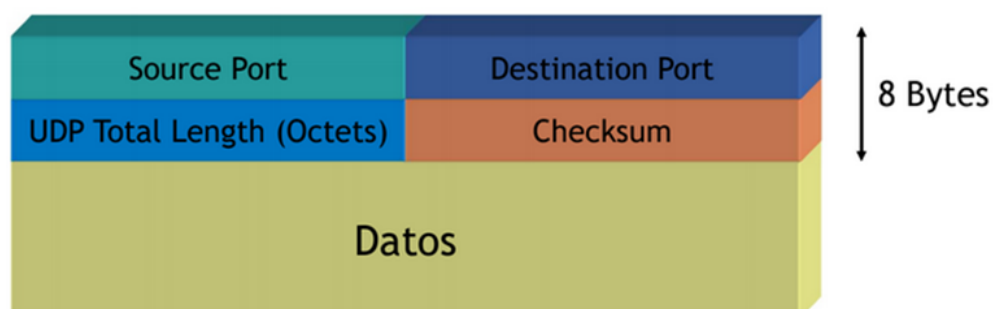
- Control de errores. Opcionalmente, el protocolo UDP puede contener un campo de checksum en su cabecera, que permite detectar errores tanto en la cabecera como en los datos. No permite corregir errores.
- Multiplexación. Como en TCP, se logra usando puertos.

Por otro lado, NO ofrece los servicios de:

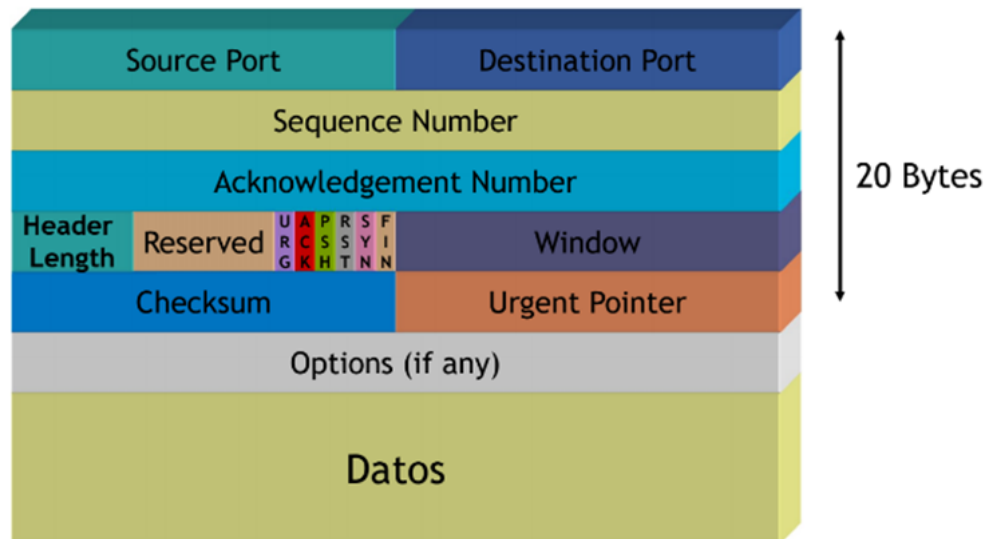
- Conexión. No es un protocolo orientado a la conexión. No mantiene un estado de la comunicación.
- Fiabilidad. No es confiable, no envía notificaciones en caso de descartes, no re-ordena paquetes.
- Control de Flujo. No lo realiza.

3. Encapsulamiento TCP y UDP.

a. Trama UDP



b. Trama TCP



c. DHCP - HTTP - HTTPS - FTP - DNS

Protocolo	Puerto	Encapsulado en...
DHCP	67/68	UDP
DNS	53	UDP/TCP
HTTP	80	TCP
HTTPS	443	TCP
FTP	20 (Data) 21 (Command)	TCP

Trama DHCP

```
> Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: Dell_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.10
> User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 308
  Checksum: 0x2233 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  UDP payload (300 bytes)
> Dynamic Host Configuration Protocol (Offer)
```

Trama DNS

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: AsustekI_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: QuantaCo
> Internet Protocol Version 4, Src: 192.168.170.8, Dst: 192.168.170.20
> User Datagram Protocol, Src Port: 32795, Dst Port: 53
  Source Port: 32795
  Destination Port: 53
  Length: 36
  Checksum: 0x85ed [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  > [Timestamps]
  UDP payload (28 bytes)
> Domain Name System (query)
```

Trama HTTP

```
> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (
> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
> Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, L
> Hypertext Transfer Protocol
```

Trama HTTPS (TLS)

- > Frame 47: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on inter
- > Ethernet II, Src: Sagemcom_cf:61:ac (4c:19:5d:cf:61:ac), Dst: Tp-LinkT_f8:96:8c
- > Internet Protocol Version 4, Src: 52.177.138.113, Dst: 192.168.0.149
- > Transmission Control Protocol, Src Port: 443, Dst Port: 64266, Seq: 1, Ack: 1372
- ▼ Transport Layer Security
 - > TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol