Trabajo Práctico Final Integrador

Análisis de protocolos

Fecha de entrega: 7/7/2021

Franco, Juan Martín 149.615

juanmartin_franco@hotmail.com

1. **Reconstruya la topología de la red, indicando:**

   a) **Dispositivos existentes y su función.**
   b) **Direcciones de capa 2 y 3 de cada interface de cada uno.**

Segmento de Red → Brevetiro

Dispositivo	Dirección MAC	Dirección IP	Función
Interfaz	aa:11:b3:09:41:6a	52.253.123.1	Interfaz del router perteneciente al segmento Brevetiro.
Servidor WEB	aa:11:b3:5a:d6:0e	52.253.123.2	Servidor WEB de http://datos.example.com. Recibe peticiones y responde a las mismas.

Segmento de Red → Colpocorto

Dispositivo	Dirección MAC	Dirección IP	Función
Servidor Proxy	aa:11:b3:26:f3:f6	190.192.132.77	Cachear recursos, limitar el acceso a determinados sitios.
Interfaz	aa:11:b3:15:37:e7	190.192.132.1	Interfaz del router perteneciente al segmento Colpocorto.
Interfaz	aa:11:b3:67:60:62	190.192.132.43	Interfaz del router perteneciente al segmento Colpocorto.

Segmento de Red → Kortzclap

Dispositivo	Dirección MAC	Dirección IP	Función
Interfaz	aa:11:b3:b7:83:1e	124.133.177.76	Interfaz del router perteneciente al segmento Kortzclap
Servidor DNS	aa:11:b3:f3:eb:e4	124.133.177.193	Resuelve las consultas DNS realizadas.

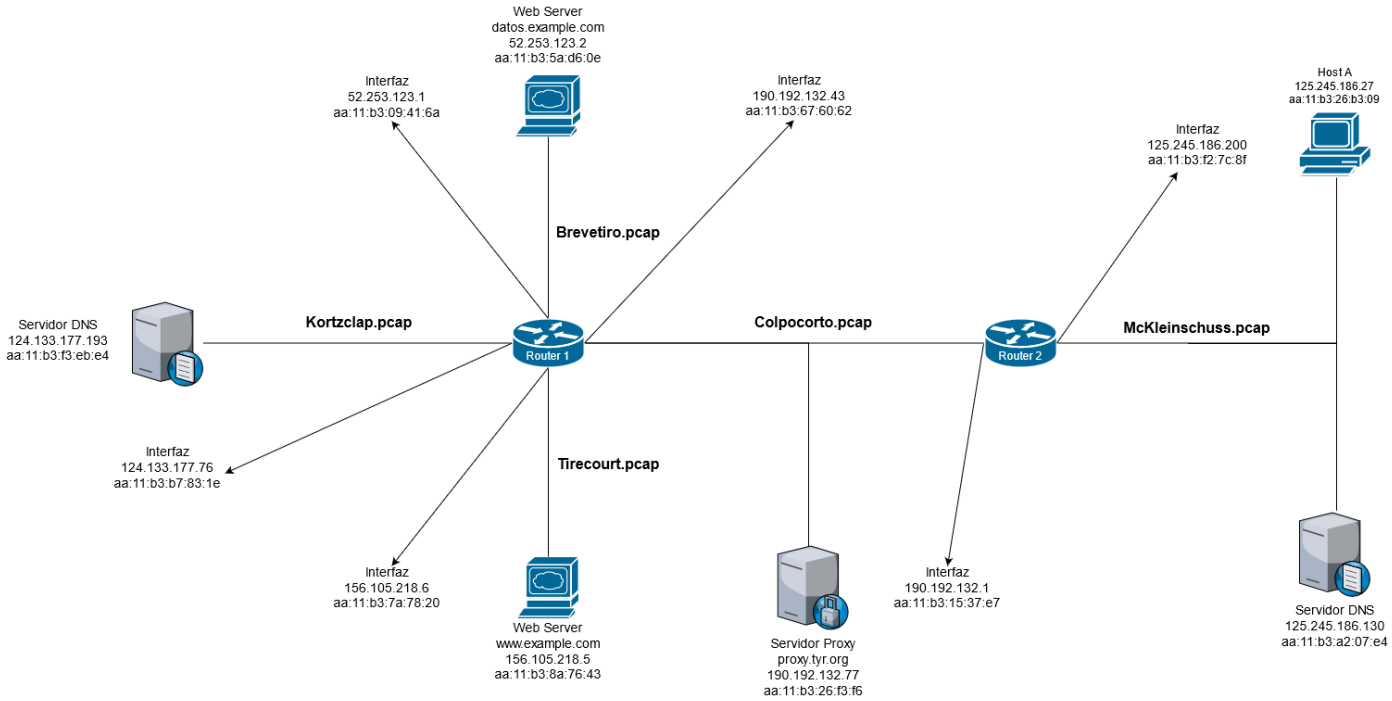
Segmento de Red → McKleinschuss

Dispositivo	Dirección MAC	Dirección IP	Función
Host	aa:11:b3:26:b3:09	125.245.186.27	Realiza consultas HTTP y DNS.
Servidor DNS	aa:11:b3:a2:07:e4	125.245.186.130	Resuelve las consultas DNS realizadas.
Interfaz	aa:11:b3:f2:7c:8f	125.245.186.200	Interfaz del router perteneciente al segmento McKleinschuss.

Segmento de Red → Tirecourt

Dispositivo	Dirección MAC	Dirección IP	Función
Servidor WEB	aa:11:b3:8a:76:43	156.105.218.5	Servidor WEB de www.example.com. Recibe peticiones y responde a las mismas.
Interfaz	aa:11:b3:7a:78:20	156.105.218.6	Interfaz del router perteneciente al segmento Tirecourt.

2. Arme el gráfico de topología con una herramienta adecuada y asigne a cada segmento de red el identificador de las capturas correspondientes (nombre del archivo .pcap).



3. **Resuelva las siguientes consignas:**

   a) **Realice gráficos con la distribución de mensajes por capas (unificando datos de todas las capturas).**

   Para la distribución de los mensajes por capas, utilizaré la herramienta de Wireshark, separando primero las distribuciones según cada captura para luego mezclar las 5 y obtener la distribución unificada:

   1 – Brevetiro.pcap:

Protocol	Percent Packets	Packets
Frame	100.0	12
Ethernet	100.0	12
Internet Protocol Version 4	83.3	10
Transmission Control Protocol	83.3	10
Hypertext Transfer Protocol	16.7	2
Line-based text data	8.3	1
Address Resolution Protocol	16.7	2

   2 – Colpocorto.pcap:

Protocol	Percent Packets	Packets
Frame	100.0	52
Ethernet	100.0	52
Internet Protocol Version 4	92.3	48
User Datagram Protocol	7.7	4
Domain Name System	7.7	4
Transmission Control Protocol	84.6	44
Hypertext Transfer Protocol	15.4	8
Line-based text data	7.7	4
Address Resolution Protocol	7.7	4

   3 – Kortzclap.pcap:

Protocol	Percent Packets	Packets
Frame	100.0	6
Ethernet	100.0	6
Internet Protocol Version 4	66.7	4
User Datagram Protocol	66.7	4
Domain Name System	66.7	4
Address Resolution Protocol	33.3	2

   4 - McKleinschuss.pcap:

Protocol	Percent Packets	Packets
Frame	100.0	32
Ethernet	100.0	32
Internet Protocol Version 4	87.5	28
User Datagram Protocol	12.5	4
Domain Name System	12.5	4
Transmission Control Protocol	75.0	24
Hypertext Transfer Protocol	12.5	4
Line-based text data	6.3	2
Address Resolution Protocol	12.5	4

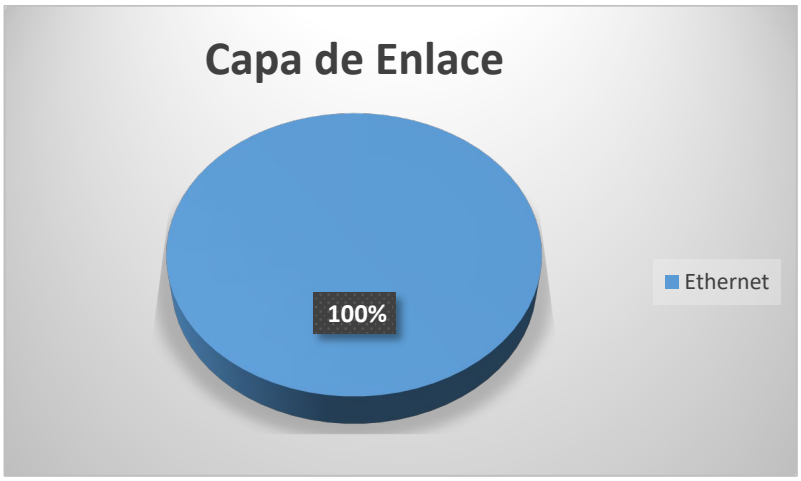
5 – Tirecourt.pcap:

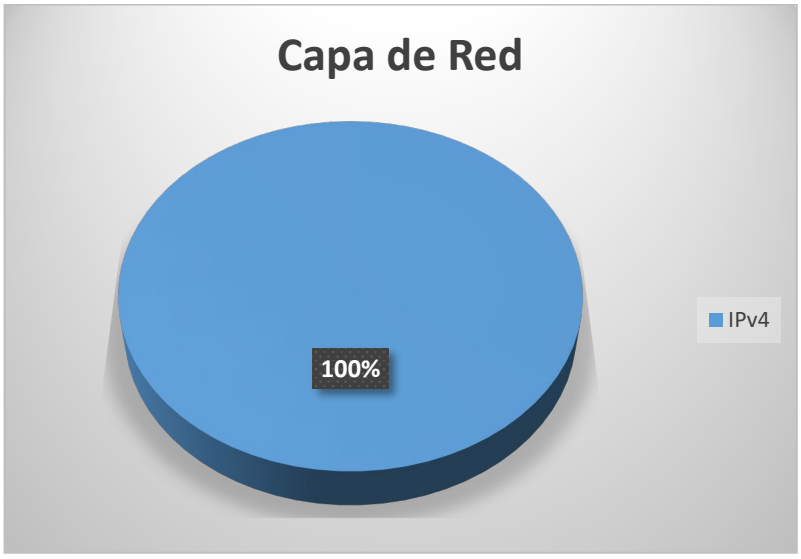
Protocol	Percent Packets	Packets
Frame	100.0	12
Ethernet	100.0	12
Internet Protocol Version 4	83.3	10
Transmission Control Protocol	83.3	10
Hypertext Transfer Protocol	16.7	2
Line-based text data	8.3	1
Address Resolution Protocol	16.7	2

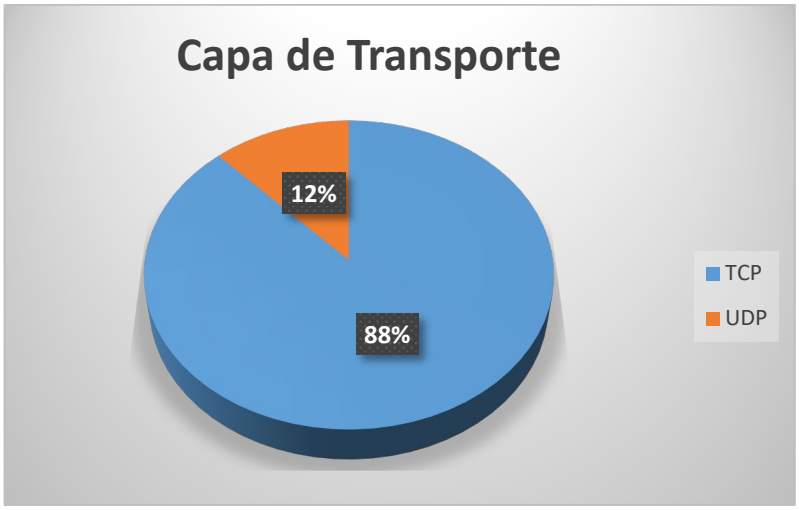
Total (las 5 capturas unificadas):

Protocol	Percent Packets	Packets
Frame	100.0	114
Ethernet	100.0	114
Internet Protocol Version 4	87.7	100
User Datagram Protocol	10.5	12
Domain Name System	10.5	12
Transmission Control Protocol	77.2	88
Hypertext Transfer Protocol	7.0	8
Line-based text data	3.5	4
Address Resolution Protocol	12.3	14

Por último, realicé un gráfico que muestre el porcentaje de cada protocolo por capa:







b) Identifique las conexiones TCP. Por cada una indique: dispositivo cliente, dispositivo servidor, finalidad, sockets de ambos (cliente y servidor).

Conexión TCP 1:

Conexión entre el host A y el proxy.

Dispositivo Cliente: 125.245.186.27 (Host A)

Dispositivo Servidor: 190.192.132.77 (Servidor Proxy)

Finalidad: Se establece la conexión con el proxy, el cual resolverá las consultas del host A.

Socket_Cliente: (125.245.186.27 : 53949)

Socket_Servidor: (190.192.132.77 : 3128)

Conexión TCP 2:

Conexión entre el servidor proxy y el servidor web que aloja www.example.com

Dispositivo Cliente: 190.192.132.77 (Servidor Proxy)

Dispositivo Servidor: 52.253.123.2 (Servidor WEB de datos.example.com)

Finalidad: El proxy realiza la petición del cliente (GET / HTTP 1.0) hacia el servidor web.

Socket_Cliente: (190.192.132.77: 36067)

Socket_Servidor: (52.253.123.2 : 80)

Conexión TCP 3:

Conexión entre el Host A y el proxy.

Dispositivo Cliente: 125.245.186.27 (Host A)

Dispositivo Servidor: 190.192.132.77 (Servidor Proxy)

Finalidad: Se establece la conexión con el proxy para que este último realice la misma hacia el servidor que aloja datos.example.com (la petición es: GET /cgi-bin/datos.pl)

Socket_Cliente: (125.245.186.27 : 53950)

Socket_Servidor: (190.192.132.77: 3128)

Conexión TCP 4:

Conexión entre el proxy y el servidor web que aloja datos.example.com.

Dispositivo Cliente: 190.192.132.77 (Servidor Proxy)

Dispositivo Servidor: 52.253.123.2 (Servidor WEB de datos.example.com)

Finalidad: Realizar una petición del tipo GET /cgi-bin/datos.pl al servidor http://datos.example.com.
Esta petición se realiza por la redirección dada dentro del código HTML de la página www.example.com

Socket_Cliente: (190.192.132.77 : 56651)

Socket_Servidor: (52.253.123.2 : 80)

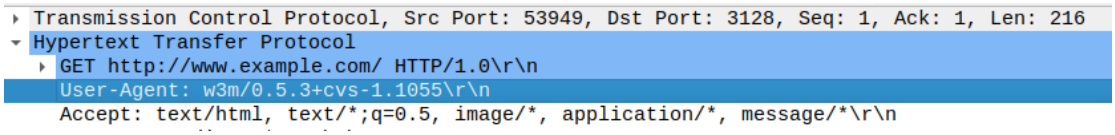
---

c) **Para la conexión TCP establecida entre el servidor proxy y el servidor www.example.com indique la finalidad de cada PDU intercambiada a nivel de transporte y aplicación.**

Adjunto imagen que contiene la finalidad de cada PDU dentro de dicho intercambio.

d) **Indique qué programa utilizó y qué es lo que ve en su pantalla el usuario que inicio el intercambio de mensajes analizado.**

El programa utilizado por el usuario que inició el intercambio de mensajes analizado es w3m, un navegador web basado en texto.
Esto se puede visualizar cuando hace la consulta, dentro de la sección Hypertext Transfer Protocol, en el campo llamado User-Agent.



Una vez realizada la petición, el usuario visualiza lo siguiente:

Hora de acceso: Tue Jun 15 18:36:12 2021

Accedido desde IP: 190.192.132.77 puerto: 56651

Hostname solicitado: datos.example.com

Referenciado desde: http://www.example.com/

e) **¿Cómo se logra la redirección desde www.example.com al contenido alojado en otro servidor? ¿Cuál es la alternativa recomendada para lograrlo?**

El usuario realiza un GET request a la dirección www.example.com.
Esta dirección, redirecciona automáticamente hacia el host indicado en el atributo content → http://datos.example.com/cgi-bin/datos.pl

```
<!DOCTYPE HTML>
<html>

<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta http-equiv="refresh" content="0;URL=http://datos.example.com/cgi-bin/datos.pl">
</head>

<body>
</body>

</html>
```

Me parece importante destacar esto dentro del código HTML:

- En la etiqueta meta, precisamente en el atributo content, la presencia del 0 seguido de la URL indica que el navegador debe esperar 0 segundos antes de redirigir hacia la URL indicada posteriormente.
  Esto evita que el cliente pueda visualizar algún tipo de contenido en la página antes de ser redirigido por el navegador.

Alternativa para redirigir:

Una alternativa posible para lograr la redirección desde el lado del servidor, podría ser implementar desde algún lenguaje de programación algún método, por ejemplo:

En Spring (Framework de Java) existe una forma de redirigir, mediante la utilización de “redirect” dentro de un método del controlador.
Esto lo que hace es realizar una nueva petición.
Una ventaja de utilizar esto es que sirve para redirigir tanto a archivos locales como también a URLs externas.

Ejemplo ilustrativo:

```
@GetMapping("/")
public String home(){
    return "redirect:https://www.google.com.ar";
}
```

f) ¿Cuáles son los servidores dns autorizados para los dominios tyr.org y example.com (dirección IP y nombre mnemónico)?

Para encontrar los servidores DNS autorizados debo conocer el registro NS dentro del RR correspondiente.
Para realizar esto, utilicé la herramienta dig con el siguiente comando:

```
dig -t NS tyr.org
```

Los servidores DNS autorizados para el dominio tyr.org son los siguientes:

1. dns.tyr.com, cuya dirección IP es 125.245.186.130

```
▾ Authoritative nameservers
  ▸ tyr.org: type NS, class IN, ns dns.tyr.org
▸ dns.tyr.org: type A, class IN, addr 125.245.186.130
```

Ahora, repito el procedimiento con example.com:

```
dig -t NS example.com
```

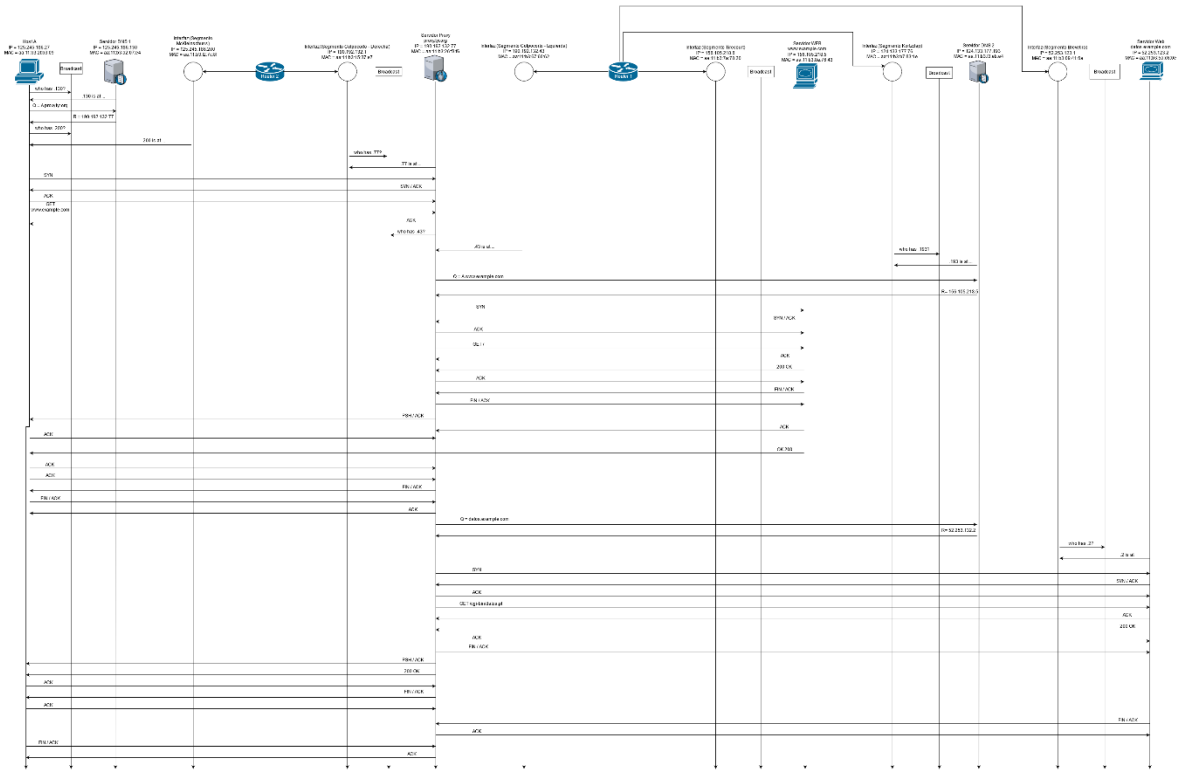
Los servidores DNS autorizados para el dominio example.com son los siguientes:

1. Stanley.example.com, cuya dirección IP es 40.130.16.34
2. Morrison.example.com, cuya dirección IP es 124.133.177.192

```
▾ Authoritative nameservers
  ▸ example.com: type NS, class IN, ns Stanley.example.com
  ▸ example.com: type NS, class IN, ns Morrison.example.com
▸ Stanley.example.com: type A, class IN, addr 40.130.16.34
▸ Morrison.example.com: type A, class IN, addr 124.133.177.192
```

g) Genere un diagrama de intercambio de mensajes en el tiempo que muestre de manera unificada como se sucedieron los mensajes, incluyendo TODOS los dispositivos involucrados en TODAS las capturas. Por cada mensaje identifique los

principales parámetros que hacen a la función del mismo. No utilice ningún software de generación automática del gráfico. El análisis debe corresponder a su interpretación de lo sucedido.



h) Confeccione una tabla con los diferentes protocolos involucrados, cantidad de PDUs, total en headers y total en datos. De allí, calcule el overhead[1] total y por protocolo generado para lograr la transferencia. Grafique adecuadamente.

[1] $Overhead = \frac{Total\_datos\_control\_Tx}{Total\_datos\_Tx}$

Adjunto archivo Excel con los datos.