



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

REDES DE INFORMACION

TRABAJOS PRÁCTICOS

ANÁLISIS DE TRAMAS ETHERNET

2020

DESCRIPCION DEL TRABAJO PRÁCTICO

• OBJETIVOS

- Comprender el funcionamiento de los protocolos IEEE 802.3, IEEE 802.11, IEEE 802.1D, IEEE 802.1Q, ARP, IP e ICMP, en un entorno de red LAN Ethernet con acceso a Internet.
- Analizar el tráfico en una LAN, entre un host Tx y otro Rx, para identificar procesos de encapsulamiento y de comunicación par-par.
- Verificar el funcionamiento de cada protocolo específico y su relación con los servicios que la capa OSI, en la que funciona cada protocolo, le proporciona a una capa superior.
- Comprender el proceso de fragmentación y reensamble de paquetes IP, así como la incidencia de la MTU de la red en dicho proceso.

DESCRIPCION DEL TRABAJO PRÁCTICO

- **CONOCIMIENTOS PREVIOS**

- Redes LAN Ethernet/IEEE 802.3 – Formato de tramas y paquetes. Funcionamiento del proceso de encapsulamiento.
- Protocolos de:

Capa de Enlace:

Ethernet: IEEE 802.3 Ethernet

IEEE 802.11: IEEE 802.11 wireless LANs

STP: IEEE 802.1D Spanning Tree Protocol

VLAN: IEEE 802.1Q Virtual Bridged Local Area Networks

Capa de Red:

ARP: Address Resolution Protocol (ARP)

IP: Internet Protocol (version 4)

IPv6: Internet Protocol (version 6)

ICMP: Internet Control Message Protocol (version 4)

Actividades previas

Software **Wireshark**, versión 3.X.X

<https://www.wireshark.org/>

Archivos de apoyo a la autopreparación:

https://www.wireshark.org/docs/wsug_html_chunked/index.html

Video online

<https://www.youtube.com/watch?v=shp42M7gbDE>

Otros materiales sobre modos de captura y análisis de seguridad con Wireshark:

https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Puede ser muy útil apoyar el estudio en los recursos en línea de Wireshark:

<https://wiki.wireshark.org/>



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

ANÁLISIS DE PROTOCOLO

¿Qué es?

¿Qué información proporciona?

Identificación inicial

1. Análisis de la red en la que está configurada la estación de trabajo.

Ejecute la aplicación WINIPCFG ó desde MS-DOS, IPCONFIG. Seleccione Liberar Todo y luego Renovar Todo.

Registre lo que ha verificado en la tabla que se encuentra a continuación:

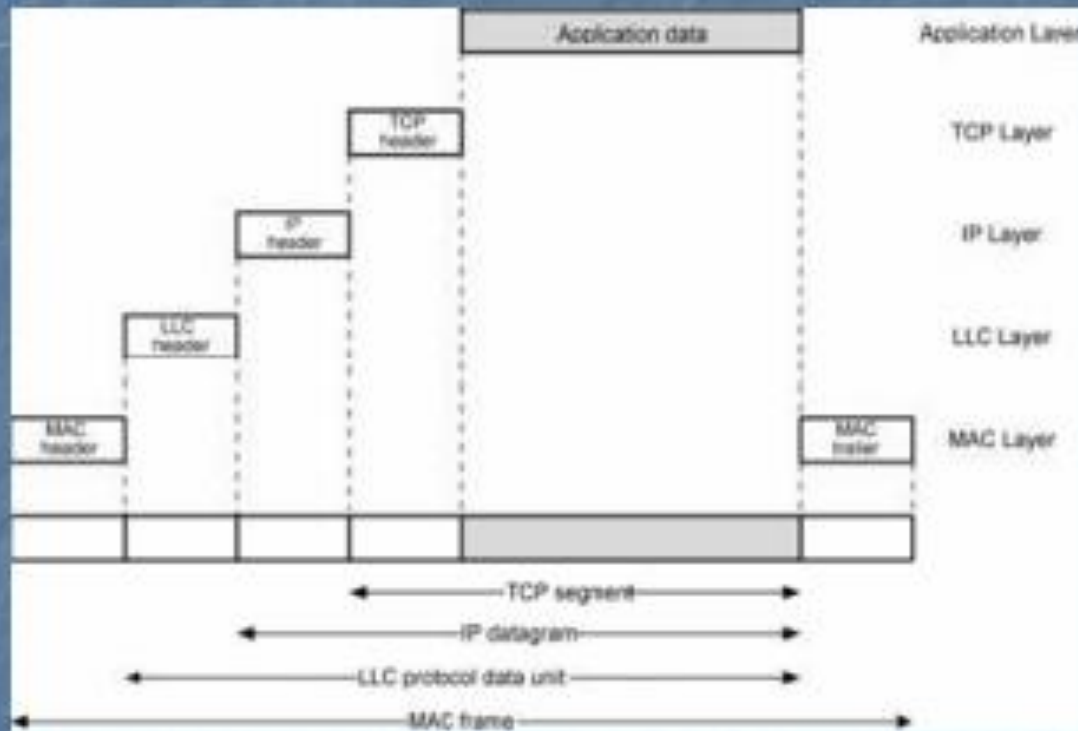
Nombre de la PC	
Dirección IP de la PC	
Máscara de Subred de la PC	
Puerta de enlace predeterminada	
Servidor DHCP de la Red	
Dirección MAC de la Placa de Red	
Servidor/es DNS	

¿Qué información identificamos?

- 1) ¿De qué clase es la dirección IP de la PC?
- 2) ¿Cuál es su máscara? ¿Es una máscara por defecto?
- 3) ¿La red tiene subredes?
- 4) ¿La red es pública o privada? ¿Qué direcciones de red de esta misma clase están reservadas?
- 5) ¿Cuántos hosts puede haber en la red como máximo?
- 6) ¿Cuál es la dirección de broadcast de la red?
- 7) ¿Es una red con colisiones? En caso afirmativo, ¿Cuántos dominios de colisión tiene?
- 8) ¿Es una red de broadcast? En caso afirmativo, ¿Cuántos dominios de broadcast tiene?
- 9) ¿Cómo se puede segmentar un dominio de colisión?
- 10) ¿Cómo se puede segmentar un dominio de broadcast?
- 11) ¿Esta red emplea direccionamiento IP estático o dinámico? ¿Cómo funciona el esquema empleado?

Análisis de una trama Ethernet

Formacion de la Trama Ethernet



Análisis de una trama Ethernet

FORMATO DE LAS TRAMAS ETHERNET

- ETHERNET DIX v2 (ETHERNET II)

- ETHERNET
IEEE 802.3



CABECERA 802.2 LLC

CABECERA 802.2 SNAP

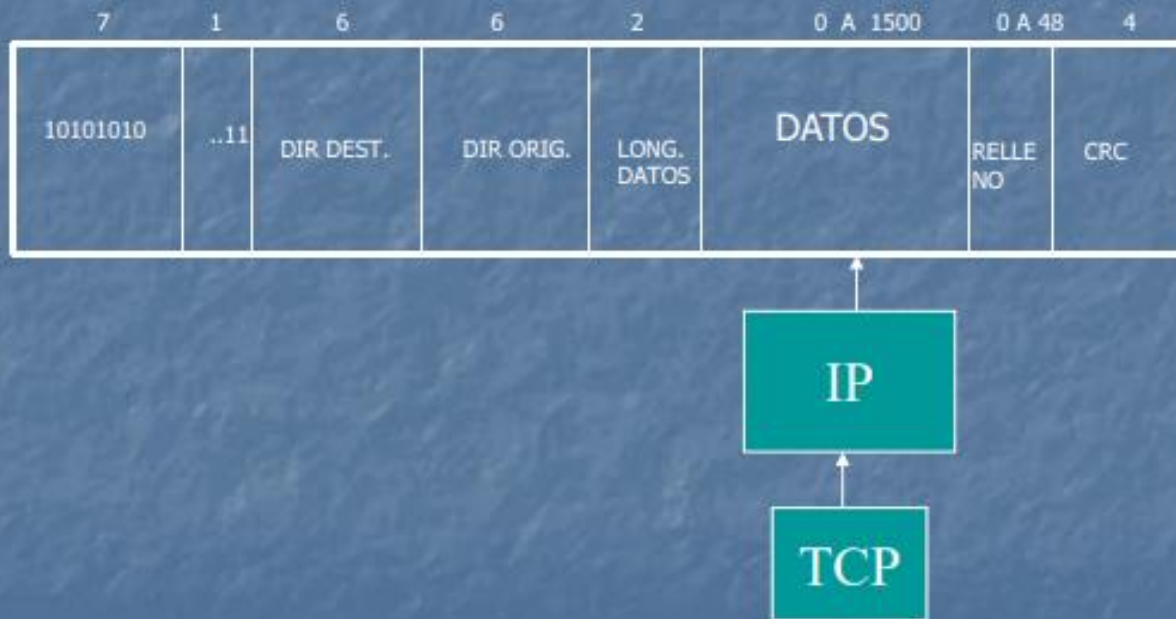
LLC: Logical Link Control

SNAP: Subnetwork Access Protocol

Ing. Rubén J. Fuenzalida

Análisis de una trama Ethernet

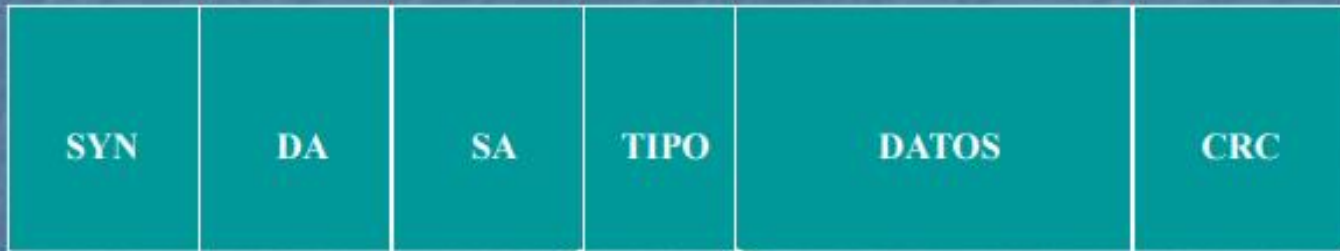
TRAMA ETHERNET



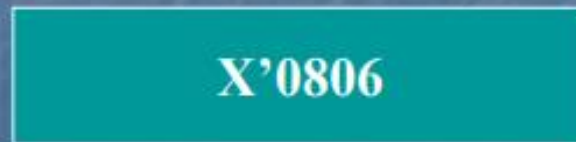
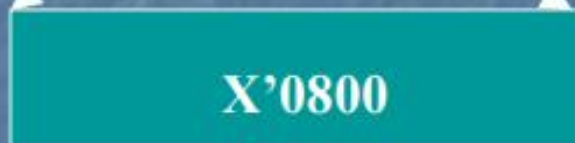
Análisis de una trama Ethernet II

ETHERNET DIX v2

La longitud del campo de datos se obtiene mediante interpretación del campo de datos.



NO UTILIZA
IEEE 802.2



Análisis de una trama Ethernet

TRAMA ETHERNET IEEE 802.3 CON CABECERA 802.2 LLC



DSAP Y SSAP se emplean para identificar el protocolo

Análisis de una trama Ethernet

TRAMA ETHERNET IEEE 802.3 CON CABECERA 802.2 SNAP



LONGITUD CAMPOS DE
DATOS: 1492 BYTES

DSAP Y SSAP: Hex AA CONTROL: Hex 03

PROTOCOLO ID: X'0000000800 PARA IP (5 BYTES)

Ethernet 802.3 LLC

Eth LLC cap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_0a:d7:40	STP-UplinkFast	LLC	60	U, func=UI; SNAP, OUI 0x00000c (Cisco Systems, Inc), PID 0x0115
2	0.000167	Cisco_0a:d7:40	STP-UplinkFast	LLAP	60	Unknown LLAP type (03)
3	0.000168	000f0000.00000...	01150ad7.0080010...	IPX	60	CISCO PING
4	0.000168	Cisco_0a:d7:40	STP-UplinkFast	ARP	60	Unknown ARP opcode 0x0115

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{C8AAF078-03B5-49B6-AD39-7ADFE9C665FE}, id 0

▼ IEEE 802.3 Ethernet

- ▼ Destination: STP-UplinkFast (01:00:0c:cd:cd:cd)
Address: STP-UplinkFast (01:00:0c:cd:cd:cd)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..1 = IG bit: Group address (multicast/broadcast)
- > Source: Cisco_0a:d7:40 (00:1d:e5:0a:d7:40)
Length: 46

▼ Logical-Link Control

- ▼ DSAP: SNAP (0xaa)
1010 101. = SAP: SNAP
.... ...0 = IG Bit: Individual
- ▼ SSAP: SNAP (0xaa)
1010 101. = SAP: SNAP
.... ...0 = CR Bit: Command
- > Control field: U, func=UI (0x03)
Organization Code: 00:00:0c (Cisco Systems, Inc)
PID: Unknown (0x0115)

> Data (38 bytes)

```
0000 01 00 0c cd cd cd 00 1d e5 0a d7 40 00 2e aa aa .....@.
0010 03 00 00 0c 01 15 0a d7 00 80 01 01 00 14 00 02 .....
0020 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Ready to load or capture

Packets: 12 · Displayed: 12 (100.0%)

Profile: Default

18:23
2/6/2020

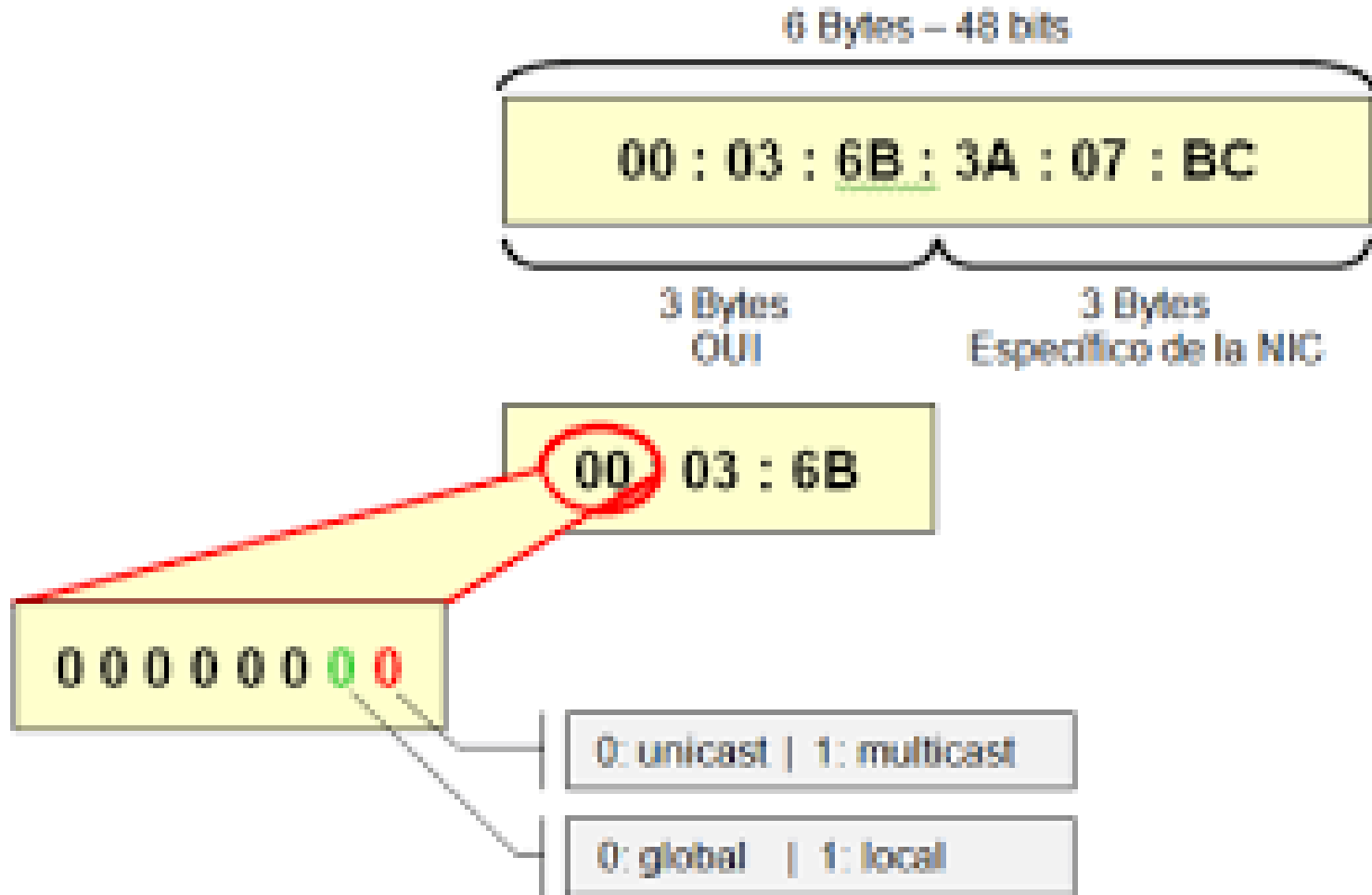
Dirección MAC

00:03:6B:3A:07:BC

Identificador Unico del fabricante (OUI)

Identificador del Producto (NIC)

Dirección MAC



Direccion MAC

- Ocupan 6 bytes
- 1 bit indica dirección individual o de grupo
- 1 bit indica direcciones locales o universales
- 22 bits asignados al fabricante
- 24 bits asignados al hardware (número de serie)

Análisis de una trama Ethernet

- **Inicie una captura con el Analizador y haga PING al Gateway (puerta de enlace) o a otra PC de su misma LAN y responda las siguientes preguntas, analizando una trama en particular:**
 - 1) ¿Cuáles son los campos de la trama? ¿Qué valores tiene cada campo y cuál es su significado?
 - 2) ¿Qué tamaño tiene el encabezado de la trama y cuáles son sus campos?
 - 3) ¿Qué tamaño tiene la cola de su trama? ¿Qué campo sirve para detectar errores y cuál es su valor?
 - 4) ¿Cuántos bytes corresponden a los datos? ¿Qué tamaño tiene este campo?
 - 5) ¿Qué protocolos de nivel 3 (TCP/IP) se encapsularon en las tramas?
 - 6) ¿Qué protocolos de nivel 4 y 5 (TCP/IP) se encapsularon en la trama?

Trama Ethernet 802.11

Network_Join_Nokia_Mobile.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Siemens_41:bd:...	Broadcast	802.11	110	Beacon frame, SN=3841, FN=0, Flags=....., BI=100, SSID=martinet3
2	0.102407	Siemens_41:bd:...	Broadcast	802.11	110	Beacon frame, SN=3842, FN=0, Flags=....., BI=100, SSID=martinet3
3	0.204810	Siemens_41:bd:...	Broadcast	802.11	110	Beacon frame, SN=3843, FN=0, Flags=....., BI=100, SSID=martinet3
4	0.307201	Siemens_41:bd:...	Broadcast	802.11	110	Beacon frame, SN=3844, FN=0, Flags=....., BI=100, SSID=martinet3
5	0.409590	Siemens_41:bd:...	Broadcast	802.11	110	Beacon frame, SN=3845, FN=0, Flags=....., BI=100, SSID=martinet3

> Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

> IEEE 802.11 Beacon frame, Flags:

Type/Subtype: Beacon frame (0x0008)

> Frame Control Field: 0x8000

.000 0000 0000 0000 = Duration: 0 microseconds

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

Transmitter address: Siemens_41:bd:6e (00:01:e3:41:bd:6e)

Source address: Siemens_41:bd:6e (00:01:e3:41:bd:6e)

BSS Id: Siemens_41:bd:6e (00:01:e3:41:bd:6e)

.... 0000 = Fragment number: 0

1111 0000 0011 = Sequence number: 3843

> IEEE 802.11 Wireless Management

```
0000 80 00 00 00 ff ff ff ff ff ff 00 01 e3 41 bd 6e .....A-n
0010 00 01 e3 41 bd 6e 30 f0 89 41 1d 69 02 00 00 00 ...A-n0-A-i...
0020 64 00 11 04 00 09 6d 61 72 74 69 6e 65 74 33 01 d....ma rtinet3-
0030 08 82 84 8b 96 24 30 48 6c 03 01 0b 05 04 00 01 ....$0H 1.....
0040 00 00 2a 01 04 2f 01 04 32 04 0c 12 18 60 dd 06 ..*-/.. 2....`..
0050 00 10 18 01 01 00 dd 16 00 50 f2 01 01 00 00 50 .....P.....P
0060 f2 02 01 00 00 50 f2 02 01 00 00 50 f2 02 .....P...P..
```

Network_Join_Nokia_Mobile.pcap

Packets: 1180 · Displayed: 1180 (100.0%)

Profile: Default

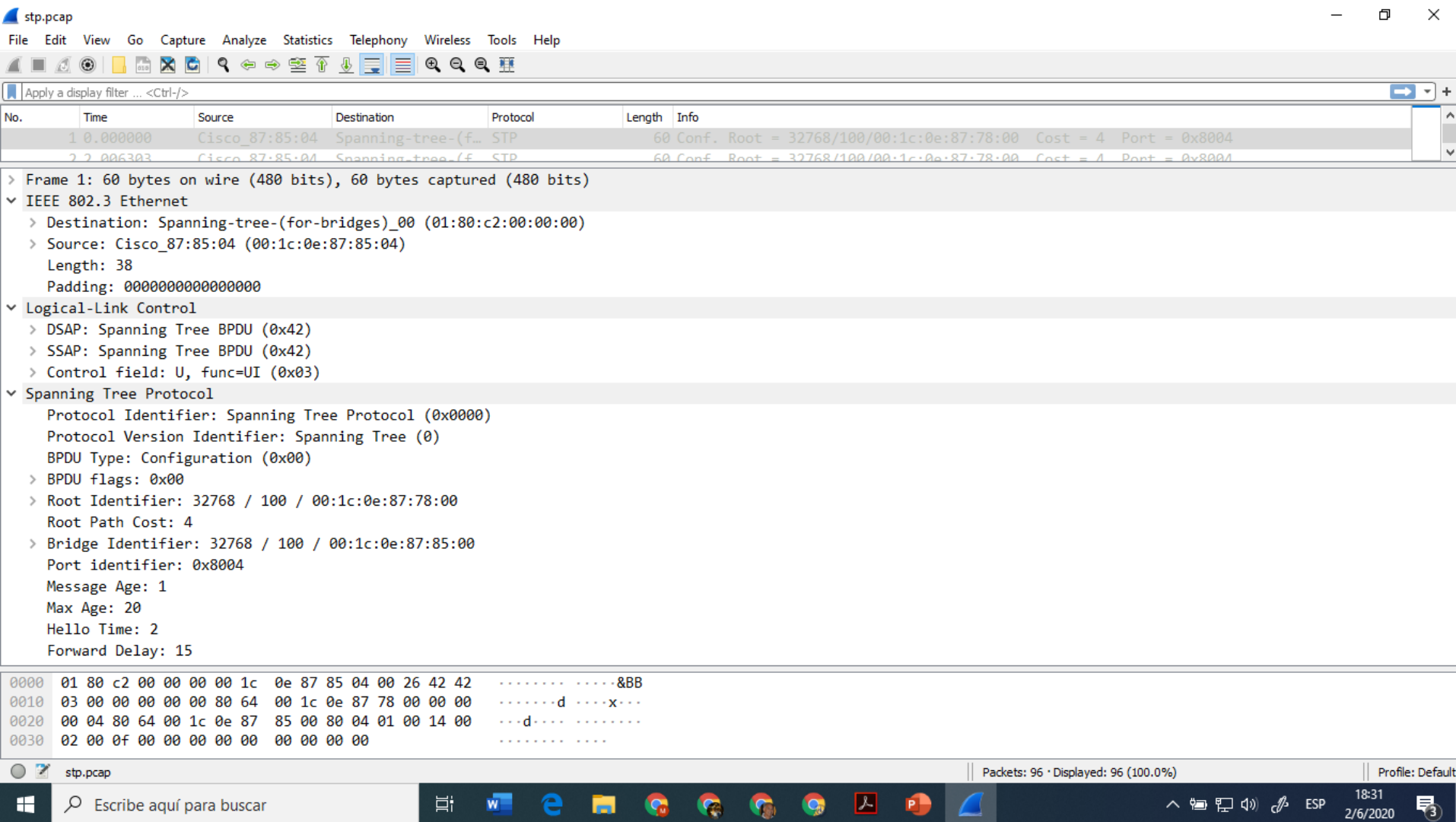
Escribe aquí para buscar



ESP

18:29
2/6/2020

Trama Ethernet STP



The image shows a Wireshark capture of an Ethernet Spanning Tree Protocol (STP) frame. The packet list at the top shows two packets, both of which are STP frames. The selected packet (No. 1) is expanded, showing the following details:

- Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- IEEE 802.3 Ethernet
 - Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
 - Source: Cisco_87:85:04 (00:1c:0e:87:85:04)
 - Length: 38
 - Padding: 0000000000000000
- Logical-Link Control
 - DSAP: Spanning Tree BPDU (0x42)
 - SSAP: Spanning Tree BPDU (0x42)
 - Control field: U, func=UI (0x03)
- Spanning Tree Protocol
 - Protocol Identifier: Spanning Tree Protocol (0x0000)
 - Protocol Version Identifier: Spanning Tree (0)
 - BPDU Type: Configuration (0x00)
 - BPDU flags: 0x00
 - Root Identifier: 32768 / 100 / 00:1c:0e:87:78:00
 - Root Path Cost: 4
 - Bridge Identifier: 32768 / 100 / 00:1c:0e:87:85:00
 - Port identifier: 0x8004
 - Message Age: 1
 - Max Age: 20
 - Hello Time: 2
 - Forward Delay: 15

The packet bytes at the bottom show the raw data of the frame, including the destination and source MAC addresses, the STP protocol identifier, and the BPDU flags.

stp.pcap

Packets: 96 · Displayed: 96 (100.0%)

Profile: Default

Escribe aquí para buscar

Trama Ethernet VLAN

vlan.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	131.151.32.129	131.151.32.21	X11	1518	Requests: FreePixmap, FreePixmap, ConfigureWindow, ConfigureWindow, ClearArea, Confi...
2	0.000105	131.151.32.129	131.151.32.21	X11	650	Requests: ConfigureWindowRequests: ConfigureWindow, ConfigureWindow, MapWindow, Conf...
3	0.003689	00056800.08000...	00000000.ffffff...	IPX RIP	64	Request
4	0.007671	131.151.32.129	131.151.32.21	X11	1518	Requests: ConfigureWindow, ConfigureWindow, ConfigureWindow, MapWindow, ConfigureWin...
5	0.007756	131.151.32.129	131.151.32.21	X11	350	Requests: ConfigureWindowRequests: ConfigureWindow, ConfigureWindow, MapWindow, Conf...
6	0.008329	131.151.32.21	131.151.32.129	TCP	70	6000 → 1162 [ACK] Seq=1 Ack=3477 Win=31856 Len=0 TSval=26846195 TSecr=323783
7	0.009617	131.151.32.21	131.151.32.129	X11	1518	Event: ConfigureNotify, Expose, ConfigureNotify, Expose, ConfigureNotify, ConfigureN...
8	0.009662	131.151.32.21	131.151.32.129	X11	638	Event: ConfigureNotifyEvent: ConfigureNotify, Expose, ConfigureNotify, ConfigureNoti...
9	0.009802	131.151.32.129	131.151.32.21	TCP	70	1162 → 6000 [ACK] Seq=3757 Ack=1449 Win=27472 Len=0 TSval=323784 TSecr=26846195

> Frame 1: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)

✓ Ethernet II, Src: AniCommu_40:ef:24 (00:40:05:40:ef:24), Dst: 3com_9f:b1:f3 (00:60:08:9f:b1:f3)

> Destination: 3com_9f:b1:f3 (00:60:08:9f:b1:f3)

> Source: AniCommu_40:ef:24 (00:40:05:40:ef:24)

Type: 802.1Q Virtual LAN (0x8100)

✓ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 32

000. = Priority: Best Effort (default) (0)

...0 = DEI: Ineligible

.... 0000 0010 0000 = ID: 32

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 131.151.32.129, Dst: 131.151.32.21

> Transmission Control Protocol, Src Port: 1162, Dst Port: 6000, Seq: 1, Ack: 1, Len: 1448

```
0000 00 60 08 9f b1 f3 00 40 05 40 ef 24 81 00 00 20  ..@..@.$...
0010 08 00 45 00 05 dc 3b 32 40 00 40 06 b2 25 83 97  ..E...;2 @..%..
0020 20 81 83 97 20 15 04 8a 17 70 4e 14 d0 a9 4d 3d  ... ..pN...M=
0030 54 b9 80 18 70 f8 10 b8 00 00 01 01 08 0a 00 04  T...p...
0040 f0 c7 01 99 a3 c5 36 00 02 00 be 00 c0 00 36 00  ....6...6..
0050 02 00 bc 00 c0 00 0c 00 05 00 50 00 c0 00 0c 00  ....P...
0060 00 00 0b 00 00 00 00 fc 00 00 00 c0 05 00 50 00  ....P...
0070 c0 00 03 00 00 00 02 00 00 00 0e 00 00 00 3d 00  ....=...
0080 04 00 38 00 c0 00 00 00 f2 ff 00 00 00 00 0c 00  ..8.....
```

Packets: 395 · Displayed: 395 (100.0%) Profile: Default

18:35 2/6/2020

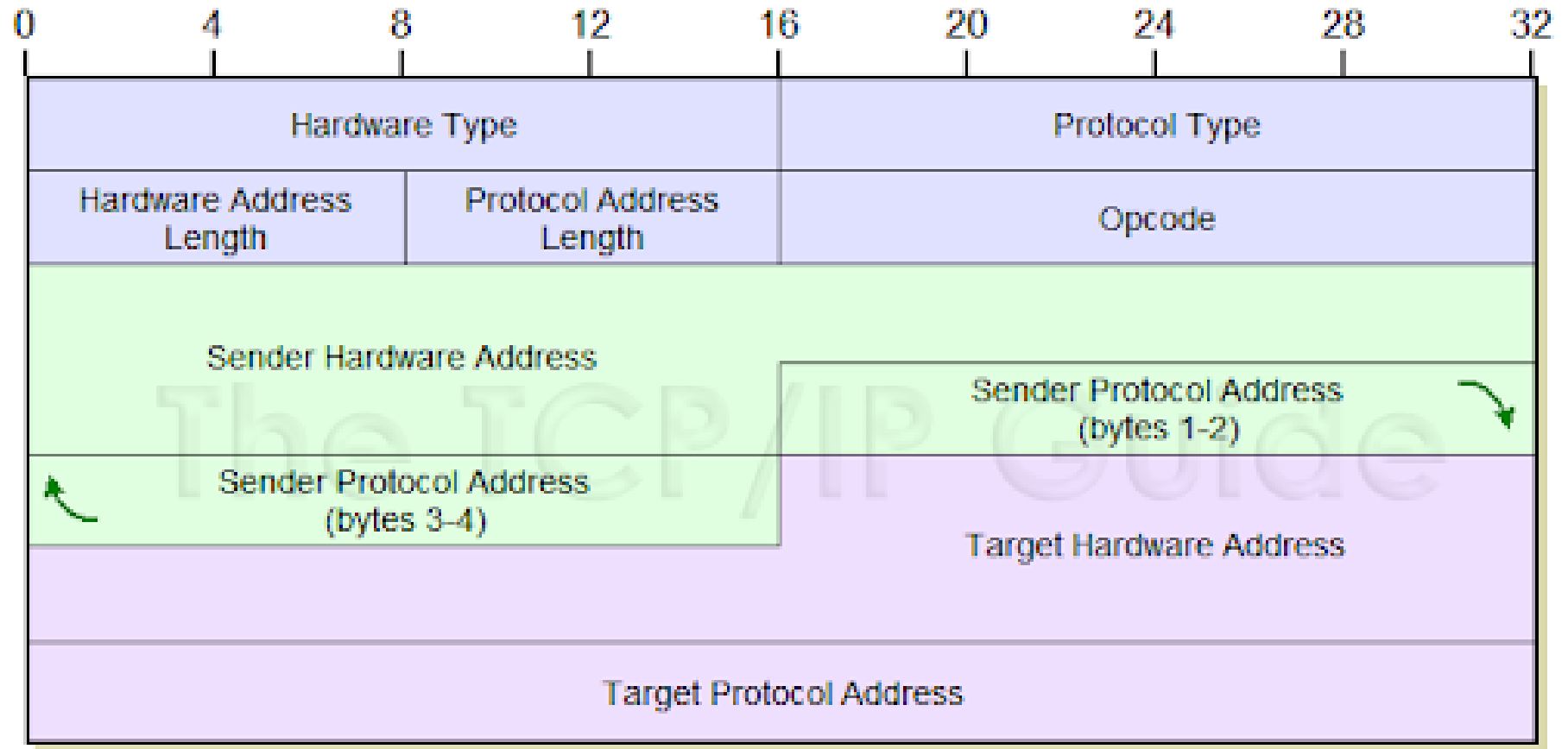
Análisis de tráfico ARP


- Realice las siguientes tareas en el intérprete de comandos y capture una o más tramas auxiliándose con el analizador de protocolos: Observe el estado de la memoria caché de ARP en su PC.
- ***C:\>WINDOWS>arp -a***
Borre la memoria caché de ARP en su PC.
- ***C:\>WINDOWS>arp -d <dirección IP>***

Análisis de tráfico ARP

- 1) Inicie una captura con el Analizador y haga PING a otra PC de la misma LAN o al Gateway de su red. Detenga la captura.**
- 2) Responda:**
 - a. ¿Cuántas PDU intervienen en la resolución ARP?**
 - b. Describa la secuencia de tramas involucradas, justificando todas las direcciones MAC e IP que aparecen**
 - c. ¿Cuál es el estado actual de la memoria caché de ARP?**
 - d. Volver a ejecutar el comando Ping a la misma máquina y observar la secuencia de tramas ARP. ¿Aparecen las mismas tramas ARP? ¿Por qué?**
 - e. ¿Qué formato tiene una PDU ARP?**
- 3) Abra una página en Internet. Capture el tráfico involucrado y responda las mismas preguntas que en el ejercicio anterior.**

Análisis de tráfico ARP



 *Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
9	0.364216	52:d4:f6:7e:03...	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.26
22	9.947726	HuaweiTe_22:0d...	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.16
54	20.041374	Kaonmedi_67:b5...	WistronI_3d:26:b4	ARP	60	Who has 192.168.0.21? Tell 192.168.0.1
55	20.041408	WistronI_3d:26...	Kaonmedi_67:b5:db	ARP	42	192.168.0.21 is at 20:6a:8a:3d:26:b4
80	33.885791	WistronI_3d:26...	Kaonmedi_67:b5:db	ARP	42	Who has 192.168.0.1? Tell 192.168.0.21
81	33.886251	Kaonmedi_67:b5...	WistronI_3d:26:b4	ARP	60	192.168.0.1 is at 90:f8:91:67:b5:db

```
> Frame 54: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0
```

```
> Ethernet II, Src: Kaonmedi 67:b5:db (90:f8:91:67:b5:db), Dst: WistronI 3d:26:b4 (20:6a:8a:3d:26:b4)
```

- ▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

```
Hardware size: 6
```

Protocol size: 4

Opcode: request (1)

Sender MAC address: Kaonmedi 67:b5:db (90:f8:91:67:b5:db)

Sender IP address: 192.168.0.1

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.0.21

0000	20 6a 8a 3d 26 b4 90 f8	91 67 b5 db 08 06 00 01	j = & g
0010	08 00 06 04 00 01 90 f8	91 67 b5 db c0 a8 00 01 g
0020	00 00 00 00 00 00 c0 a8	00 15 00 00 00 00 00 00
0030	00 00 00 00 00 00 00 00	00 00 00 00

 Address Resolution Protocol: Protocol

Packets: 481 · Displayed: 29 (6.0%) · Dropped: 0 (0.0%)

Profile: Default

 Escribe aquí para buscar



^



P

45
1020

2

18:45
2/6/2020



ARP Replay

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
9	0.364216	52:d4:f6:7e:03...	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.26
22	9.947726	HuaweiTe_22:0d...	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.16
54	20.041374	Kaonmedi_67:b5...	WistronI_3d:26:b4	ARP	60	Who has 192.168.0.21? Tell 192.168.0.1
55	20.041408	WistronI_3d:26...	Kaonmedi_67:b5:db	ARP	42	192.168.0.21 is at 20:6a:8a:3d:26:b4
80	33.885791	WistronI_3d:26...	Kaonmedi_67:b5:db	ARP	42	Who has 192.168.0.1? Tell 192.168.0.21
81	33.886251	Kaonmedi_67:b5...	WistronI_3d:26:b4	ARP	60	192.168.0.1 is at 90:f8:91:67:b5:db

> Frame 55: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0

> Ethernet II, Src: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4)

Sender IP address: 192.168.0.21

Target MAC address: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

Target IP address: 192.168.0.1

0000 90 f8 91 67 b5 db 20 6a 8a 3d 26 b4 08 06 00 01 ...g..j -=&.....

0010 08 00 06 04 00 02 20 6a 8a 3d 26 b4 c0 a8 00 15j -=&.....

0020 90 f8 91 67 b5 db c0 a8 00 01 ...g.....

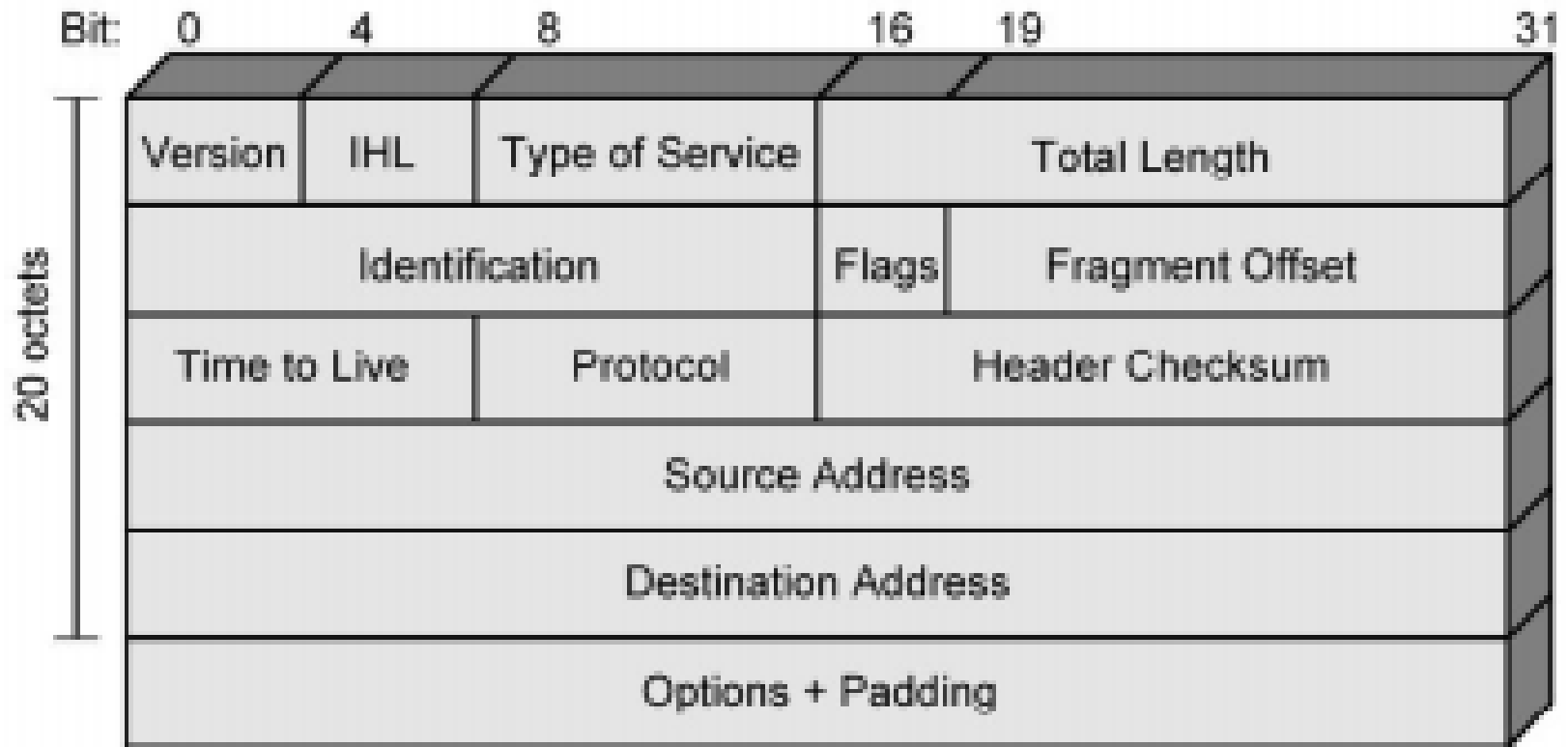
Address Resolution Protocol: Protocol

Packets: 481 · Displayed: 29 (6.0%) · Dropped: 0 (0.0%)

Profile: Default

18:46 2/6/2020

Análisis del tráfico IP e ICMP



Encabezamiento IP

Versión: (4 bits) (siempre vale lo mismo (0100)).

Long de la Cabecera: (4 bits) (en palabras de 32 bits). Su valor mínimo es de 5 a 15

Tipo de Servicio: (8 bits) - Indica una serie de parámetros sobre la calidad de servicio - Estos 8 bits se agrupan de la siguiente manera. Los 5 bits de menos peso son independientes e indican características del servicio y los 3 bits restantes están relacionados con la precedencia de los mensajes,

Longitud Total: (16 bits) - Tamaño total, en octetos, del datagrama, incluyendo el tamaño de la cabecera y el de los datos. En caso de fragmentación este campo contendrá el tamaño del fragmento, no el del datagrama original.

Identificador: (16 bits) Identificador único del datagrama. Se utilizará, en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El originador del datagrama debe asegurar un valor único para la pareja origen-destino y el tipo de protocolo durante el tiempo que el datagrama pueda estar activo en la red.

Encabezamiento IP

Indicadores (flags): (3 bits) - Actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes:

bit 0: Reservado; debe ser 0

bit 1: 0 = Divisible, 1 = No Divisible

bit 2: 0 = Últ Fragmento, 1 = Fragmento Intermedio (le siguen más fragmentos)

La indicación de que un paquete que es indivisible debe ser tenida en cuenta bajo cualquier circunstancia. Si el paquete necesitara ser fragmentado, no se enviará.

Posición de Fragmento: (13 bits) - En paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.

Tiempo de Vida (TTL): (8 bits) - Indica el máximo número de routers que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en, como mínimo, un direccionador. Cuando llegue a ser 0, el paquete no será reenviado.

Protocolo: (8 bits) - Indica el protocolo de siguiente nivel utilizado en la parte de datos del datagrama.

Encabezamiento IP

Suma de Control de Cabecera: (16 bits) - Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida)

Dirección IP de origen: 32 bits

Dirección IP de destino: 32 bits

Opciones: Variable. Puede contener un número indeterminado de opciones, que tendrán dos posibles formatos: Formato de opciones simple y Formato de opciones compuesto

Relleno: Variable - Utilizado para asegurar que el tamaño, en bits, de la cabecera es un múltiplo de 32. El valor usado es el 0.

Análisis de encabezamiento IP

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ping

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.21	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1525/62725, ttl=128 (reply in 2)
2	0.001272	192.168.0.1	192.168.0.21	ICMP	74	Echo (ping) reply id=0x0001, seq=1525/62725, ttl=64 (request in 1)
3	1.011839	192.168.0.21	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1526/62981, ttl=128 (reply in 4)
4	1.012842	192.168.0.1	192.168.0.21	ICMP	74	Echo (ping) reply id=0x0001, seq=1526/62981, ttl=64 (request in 3)
5	2.022703	192.168.0.21	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1527/63237, ttl=128 (reply in 6)
6	2.023132	192.168.0.1	192.168.0.21	ICMP	74	Echo (ping) reply id=0x0001, seq=1527/63237, ttl=64 (request in 5)

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0

> Ethernet II, Src: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

> Internet Protocol Version 4, Src: 192.168.0.21, Dst: 192.168.0.1

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0xc31f (49951)
- > Flags: 0x0000
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0xf63a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.21
- Destination: 192.168.0.1

> Internet Control Message Protocol

0000 90 f8 91 67 b5 db 20 6a 8a 3d 26 b4 08 00 45 00 ...g..j.=&...E.

0010 00 3c c3 1f 00 00 80 01 f6 3a c0 a8 00 15 c0 a8 .<.....:.....

0020 00 01 08 00 47 66 00 01 05 f5 61 62 63 64 65 66Gf.. .abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Ethernet (eth), 14 byte(s)

Packets: 20 · Displayed: 20 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Escribe aquí para buscar

Análisis de encabezamiento ICMP

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Contents Depend on Type and Code (variable)		

Tipos y códigos de los mensajes ICMP:

- 0 y 8: Eco de solicitud y de respuesta (PING)
- 3: Destino no alcanzable (Se genera cuando un datagrama no encuentra la dirección IP destino)
- El campo Código brinda información adicional sobre las causas por las cuales no se llega a destino:
- Los valores que toma son:
 - 0: Red inalcanzable. 1: Host inalcanzable. 2: Protocolo inalcanzable. 3: Puerto inalcanzable. 4: Fragmentación requerida y bit de no fragmentar puesto a 1 en el datagrama origen. 5: Falla en la ruta. 6: Red desconocida. 7: Host desconocido. 8: Host origen aislado. 9: Acceso a la red administrativamente prohibido. 10: Acceso al Host administrativamente prohibido. 11: Red inalcanzable por tipo de servicio. 12: Host inalcanzable por tipo de servicio.
- 4: Fuente agotada: Buffer lleno
- 11: Tiempo de vida excedido: El campo TTL llegó a 0.
- 5: Se requiere redireccionamiento: Existe una ruta mejor.
- 12: Problemas con el parámetro: Error semántico o sintáctico en el encabezamiento IP.
- 13 y 14: Solicitud y respuesta de marcador de tiempo
- 15 y 16: Solicitud y respuesta de información
- 17 y 18: Solicitud y respuesta de máscara de dirección

Análisis de ICMP (PING)

Wireshark interface showing ICMP (PING) analysis.

Filter: icmp

No.	Time	Source	Destination	Protocol	Length	Info
20	3.598463	192.168.0.21	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1570/8710, ttl=128 (reply in 21)
21	3.599405	192.168.0.1	192.168.0.21	ICMP	74	Echo (ping) reply id=0x0001, seq=1570/8710, ttl=64 (request in 20)
31	4.605412	192.168.0.21	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1571/8966, ttl=128 (reply in 32)
32	4.605909	192.168.0.1	192.168.0.21	ICMP	74	Echo (ping) reply id=0x0001, seq=1571/8966, ttl=64 (request in 31)
34	5.616382	192.168.0.21	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1572/9222, ttl=128 (reply in 35)
35	5.617568	192.168.0.1	192.168.0.21	ICMP	74	Echo (ping) reply id=0x0001, seq=1572/9222, ttl=64 (request in 34)

Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0

Ethernet II, Src: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

Internet Protocol Version 4, Src: 192.168.0.21, Dst: 192.168.0.1

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4739 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence number (BE): 1570 (0x0622)
- Sequence number (LE): 8710 (0x2206)
- [\[Response frame: 21\]](#)

Data (32 bytes)

```
0000  90 f8 91 67 b5 db 20 6a 8a 3d 26 b4 08 00 45 00  ...g..j.=&...E.
0010  00 3c db 04 00 00 80 01 de 55 c0 a8 00 15 c0 a8  .<.....U.....
0020  00 01 08 00 47 39 00 01 06 22 61 62 63 64 65 66  ....G9.. "abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
```

Internet Control Message Protocol: Protocol

Packets: 40 · Displayed: 8 (20.0%) · Dropped: 0 (0.0%)

Profile: Default

21:13 2/6/2020

Análisis de ICMP (PING 200)

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
8	1.552796	192.168.0.21	192.168.0.1	ICMP	242	Echo (ping) request id=0x0001, seq=1574/9734, ttl=128 (reply in 9)
9	1.553828	192.168.0.1	192.168.0.21	ICMP	242	Echo (ping) reply id=0x0001, seq=1574/9734, ttl=64 (request in 8)
14	2.563275	192.168.0.21	192.168.0.1	ICMP	242	Echo (ping) request id=0x0001, seq=1575/9990, ttl=128 (reply in 15)
15	2.563644	192.168.0.1	192.168.0.21	ICMP	242	Echo (ping) reply id=0x0001, seq=1575/9990, ttl=64 (request in 14)
18	3.573661	192.168.0.21	192.168.0.1	ICMP	242	Echo (ping) request id=0x0001, seq=1576/10246, ttl=128 (reply in 19)
19	3.574754	192.168.0.1	192.168.0.21	ICMP	242	Echo (ping) reply id=0x0001, seq=1576/10246, ttl=64 (request in 18)

> Frame 8: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0

> Ethernet II, Src: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

> Internet Protocol Version 4, Src: 192.168.0.21, Dst: 192.168.0.1

▼ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xb796 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 1574 (0x0626)

Sequence number (LE): 9734 (0x2606)

[\[Response frame: 9\]](#)

> Data (200 bytes)

```
0000 90 f8 91 67 b5 db 20 6a 8a 3d 26 b4 08 00 45 00  ...g.. j -=&...E-
0010 00 e4 db 32 00 00 80 01 dd 7f c0 a8 00 15 c0 a8  ...2....
0020 00 01 08 00 b7 96 00 01 06 26 61 62 63 64 65 66  ....-&abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f  wabcdefg hijklmno
```

wireshark_Ethernet_20200602211628_a15712.pcapng

Packets: 25 · Displayed: 8 (32.0%)

Profile: Default

21:16 2/6/2020

Análisis de ICMP (PING 1499)

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
5	1.908071	192.168.0.21	192.168.0.1	ICMP	61	Echo (ping) request id=0x0001, seq=1578/10758, ttl=128 (reply in 7)
7	1.911131	192.168.0.1	192.168.0.21	ICMP	61	Echo (ping) reply id=0x0001, seq=1578/10758, ttl=64 (request in 5)
9	2.919098	192.168.0.21	192.168.0.1	ICMP	61	Echo (ping) request id=0x0001, seq=1579/11014, ttl=128 (reply in 11)
11	2.920451	192.168.0.1	192.168.0.21	ICMP	61	Echo (ping) reply id=0x0001, seq=1579/11014, ttl=64 (request in 9)
13	3.926203	192.168.0.21	192.168.0.1	ICMP	61	Echo (ping) request id=0x0001, seq=1580/11270, ttl=128 (reply in 15)
15	3.928015	192.168.0.1	192.168.0.21	ICMP	61	Echo (ping) reply id=0x0001, seq=1580/11270, ttl=64 (request in 13)

> Frame 5: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0

> Ethernet II, Src: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

> Internet Protocol Version 4, Src: 192.168.0.21, Dst: 192.168.0.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 47

Identification: 0xdb4a (56138)

> Flags: 0x00b9

Fragment offset: 1480

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0xdd63 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.21

Destination: 192.168.0.1

> [2 IPv4 Fragments (1507 bytes): #4(1480), #5(27)]

> Internet Control Message Protocol

0000 90 f8 91 67 b5 db 20 6a 8a 3d 26 b4 08 00 45 00 ...g.. j .=&...E.

0010 00 2f db 4a 00 b9 80 01 dd 63 c0 a8 00 15 c0 a8 ./J.... c.....

0020 00 01 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e ..abcdef ghijklmn

Frame (61 bytes) Reassembled IPv4 (1507 bytes)

wireshark_Ethernet_20200602211802_a06992.pcapng

Packets: 32 · Displayed: 8 (25.0%) · Dropped: 0 (0.0%) Profile: Default

21:19 2/6/2020

Análisis de ICMP (PING 2000)

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000006	192.168.0.11	192.168.0.1	ICMP	562	Echo (ping) request id=0x0001, seq=1821/7431, ttl=128 (reply in 4)
4	0.018326	192.168.0.1	192.168.0.11	ICMP	562	Echo (ping) reply id=0x0001, seq=1821/7431, ttl=64 (request in 2)
59	1.005591	192.168.0.11	192.168.0.1	ICMP	562	Echo (ping) request id=0x0001, seq=1822/7687, ttl=128 (reply in 71)
71	1.041393	192.168.0.1	192.168.0.11	ICMP	562	Echo (ping) reply id=0x0001, seq=1822/7687, ttl=64 (request in 59)
357	2.017670	192.168.0.11	192.168.0.1	ICMP	562	Echo (ping) request id=0x0001, seq=1823/7943, ttl=128 (reply in 359)
359	2.039496	192.168.0.1	192.168.0.11	ICMP	562	Echo (ping) reply id=0x0001, seq=1823/7943, ttl=64 (request in 357)

> Frame 2: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{8C4C8BC3-5ABA-4444-A748-C338292C8679}, id 0

> Ethernet II, Src: HonHaiPr_76:20:23 (ec:55:f9:76:20:23), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

> Internet Protocol Version 4, Src: 192.168.0.11, Dst: 192.168.0.1

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 548
- Identification: 0xfed5 (65237)
- > Flags: 0x00b9
- Fragment offset: 1480
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0xb7ed [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.11
- Destination: 192.168.0.1
- > [2 IPv4 Fragments (2008 bytes): #1(1480), #2(528)]

> Internet Control Message Protocol

0000 90 f8 91 67 b5 db ec 55 f9 76 20 23 08 00 45 00 ...g...U·v#..E·

0010 02 24 fe d5 00 b9 80 01 b7 ed c0 a8 00 0b c0 a8 ·\$......

0020 00 01 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e ··abcdef ghijklmn

Frame (562 bytes) Reassembled IPv4 (2008 bytes)

Internet Control Message Protocol: Protocol

Packets: 1071 · Displayed: 8 (0.7%) · Dropped: 0 (0.0%) Profile: Default

Escribe aquí para buscar

18:44 3/6/2020

Análisis de ICMP (PING 1472)

icmp 1472.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.21	192.168.0.1	ICMP	1514	Echo (ping) request id=0x0001, seq=1586/12806, ttl=128 (reply in 2)
2	0.001140	192.168.0.1	192.168.0.21	ICMP	1514	Echo (ping) reply id=0x0001, seq=1586/12806, ttl=64 (request in 1)
4	1.005677	192.168.0.21	192.168.0.1	ICMP	1514	Echo (ping) request id=0x0001, seq=1587/13062, ttl=128 (reply in 5)
5	1.006811	192.168.0.1	192.168.0.21	ICMP	1514	Echo (ping) reply id=0x0001, seq=1587/13062, ttl=64 (request in 4)
6	2.018537	192.168.0.21	192.168.0.1	ICMP	1514	Echo (ping) request id=0x0001, seq=1588/13318, ttl=128 (reply in 7)
7	2.019277	192.168.0.1	192.168.0.21	ICMP	1514	Echo (ping) reply id=0x0001, seq=1588/13318, ttl=64 (request in 6)

> Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0

> Ethernet II, Src: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

> Internet Protocol Version 4, Src: 192.168.0.21, Dst: 192.168.0.1

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 1500
- Identification: 0xdb7e (56190)
- > Flags: 0x0000
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0xd83b [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.21
- Destination: 192.168.0.1

> Internet Control Message Protocol

0010 05 dc db 7e 00 00 80 01 d8 3b c0 a8 00 15 c0 a8
0020 00 01 08 00 3a 15 00 01 06 32 61 62 63 64 65 66 ..:..2abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f wabcdefg hijklmno

Fragment offset (13 bits) (p.frag_offset), 2 byte(s)

Packets: 17 · Displayed: 8 (47.1%) Profile: Default

Escribe aquí para buscar

21:22 2/6/2020

Análisis de ICMP (PING 1473)

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
12	1.628989	192.168.0.21	192.168.0.1	ICMP	35	Echo (ping) request id=0x0001, seq=1590/13830, ttl=128 (reply in 14)
14	1.631410	192.168.0.1	192.168.0.21	ICMP	60	Echo (ping) reply id=0x0001, seq=1590/13830, ttl=64 (request in 12)
20	2.640198	192.168.0.21	192.168.0.1	ICMP	35	Echo (ping) request id=0x0001, seq=1591/14086, ttl=128 (reply in 22)
22	2.642183	192.168.0.1	192.168.0.21	ICMP	60	Echo (ping) reply id=0x0001, seq=1591/14086, ttl=64 (request in 20)
25	3.646270	192.168.0.21	192.168.0.1	ICMP	35	Echo (ping) request id=0x0001, seq=1592/14342, ttl=128 (reply in 27)
27	3.648572	192.168.0.1	192.168.0.21	ICMP	60	Echo (ping) reply id=0x0001, seq=1592/14342, ttl=64 (request in 25)

> Frame 12: 35 bytes on wire (280 bits), 35 bytes captured (280 bits) on interface \Device\NPF_{C77D6DD3-E861-4536-825D-0B54ABAEF310}, id 0

> Ethernet II, Src: WistronI_3d:26:b4 (20:6a:8a:3d:26:b4), Dst: Kaonmedi_67:b5:db (90:f8:91:67:b5:db)

> Internet Protocol Version 4, Src: 192.168.0.21, Dst: 192.168.0.1

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 21
- Identification: 0xdb90 (56208)
- > Flags: 0x00b9
- Fragment offset: 1480
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0xdd37 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.21
- Destination: 192.168.0.1
- > [2 IPv4 Fragments (1481 bytes): #11(1480), #12(1)]

> Internet Control Message Protocol

```
0000  90 f8 91 67 b5 db 20 6a 8a 3d 26 b4 08 00 45 00  ...g..j -=&...E-
0010  00 15 db 90 00 b9 80 01 dd 37 c0 a8 00 15 c0 a8  .....7.....
0020  00 01 61  ..a
```

Frame (35 bytes) Reassembled IPv4 (1481 bytes)

wireshark_Ethernet_20200602212308_a13860.pcapng

Packets: 34 · Displayed: 8 (23.5%) Profile: Default

21:23 2/6/2020



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

FIN