

# Wireshark- OSI- Physical & Data-link Layers

BAT-221: BAS Networking



This material is based upon work supported by the National Science Foundation Advanced Technical Education grant program, A New Technician Training Program for Advanced Building Technologies, DUE-2000190.

The opinions, findings, and conclusions or recommendations expressed are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Wireshark - OSI - Physical & Data-link Layers© 2023 by Wake Technical Community College is licensed under CC BY-NC-SA 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/4.0/ Name:

Section:

# Wireshark- OSI- Physical & Data-link Layers

# <u>Synopsis</u>

In this lab, we are going to use Wireshark to analyze the two lowest layers of the OSI model: Physical and Data-link layer.

# **OBJECTIVES**

Upon completion of this activity the student will be able to:

- Capture and analyze network traffic using Wireshark.
- Analyze the OSI Physical layer in Wireshark.
- Understand the fields that make up a frame in the OSI Data-link layer.
- Analyze the OSI Data-link layer in Wireshark.

# PARTS AND EQUIPMENT

• Networked laptop

# **SOFTWARE**

• <u>Wireshark</u> [https://www.wireshark.org/]

## REFERENCES

- <u>What is a MAC Address: How to Find and Identify</u> [https://whatismyipaddress.com/macaddress]
- <u>OSI Model</u> [http://www.practicalnetworking.net/series/packet-traveling/osi-model/]
- <u>What is the Internet Control Message Protocol (ICMP)?</u> [https://www.fortinet.com/resources/cyberglossary/internet-control-message-protocol-ICMP]

# MANUALS

• <u>Network Communications for Buildings</u> [https://www.ccontrols.com/pdf/NCB2015.pdf]

## BACKGROUND

The MAC address is a 48-bit (6 byte) network address. The MAC address is used to uniquely identify devices on a network.

A MAC address is hardcoded onto the network adaptor by the manufacturer. The manufacturer makes sure the address is unique.

The MAC address will appear be written using hexadecimal numbers and will usually appear in the following formats:

- A0-51-0B-29-C9-4E
- A0:51:0B:29:C9:4E

The MAC address is used for source and destination address at the Data-link layer.

## PROCEDURES

## **Part 1: Network configuration**

We need to get the IPv4 address and MAC address of the network adaptor that we are going to be capturing traffic on.

#### 1.1 - Laptop configuration

An ipconfig will give us the IPv4 address but we also want to know the MAC address on the network adaptor, so we are going to run it without the /all switch.

Run an "ipconfig /all" to get the IPv4 address and the MAC address:



What is the MAC (Physical) address of our network interface?

What is the IPv4 address of our network interface?

What is the IPv4 address of the Default Gateway?

#### 1.2 - Default gateway

To reach outside out LAN, we go through the Default Gateway. While we have the IPv4 address of the Default Gateway, we need to get the MAC address of Default Gateway. We have already gotten the IPv4 address of the Default Gateway from our network interface.

#### ARP

ARP is a protocol that maps an IP address to a MAC (Physical) address.

We can use the dos "arp" command to get the translation between the two.

Run the arp command with the -a switch with the IPv4 address of the Default Gateway.

Wake Tech BAT Lab	4 of 23	Last updated:
https://www.waketech.edu/pro	ograms-courses/credit/building-automation	8/28/2023

What is the IPv4 address of the Default Gateway from our network interface?\_\_\_\_\_

C:\WINDOWS\system32\cmd.exe		_	×
C:\Users≻arp -a 10.1.200.1			î
Interface: 10.1.201.72 0x19 Internet Address Physical Address 10.1.200.1 a0-b4-39-ce-9e-02	Type dynamic		
C:\Users>			
			~

What is the MAC address of the Default Gateway?\_\_\_\_\_

1.3 - Summarize

Summarize the MAC and IPv4 address for our interface network as well as the Default Gateway.

 Network Interface MAC address?

 Network Interface IPv4 address?

 Default Gateway MAC address?

 Default Gateway IPv4 address?

# Part 2: Wireshark

## 2.1 - Wireshark Capture

Start Wireshark and it should start capturing network traffic once you have selected the network interface.

🙍 Capturing from Wi-Fi															_	۵	I	$\times$
File Edit View Go Capture Analyze Statistics Telephony Wireless	Tools H	Help																
◢ ■ ◢ ◎   🗈 🗙 🖻 🔍 ⇔ ⇒ 🕾 🗿 🖢 🚍 🔍 Q, Q, Q	Q. 🎹																	
Apply a display filter <ctrl-></ctrl->																		· ] +
No. Time Delta Source	Destinatio	on		Prot	ocol				Le	ength	Info							^
120 07:36:19.042916 0.204028 10.1.201.67	239.25	5.255.	250	SSD	P					179	M-S	EAR	CH	* H	TTP	/1.1	L	
121 07:36:19.145747 0.102831 10.1.175.46	224.0.	0.251		MDN	IS					254	Sta	nda	ird	que	ry	resp	ons	se
122 07:36:19.676508 0.530761 10.1.201.72	23.62.	32.5		TCP	•					55	[TC	PK	eep	-A1	ive	] 63	3844	1 →
123 07:36:19.676895 0.000387 10.1.201.72	44.236	5.123.1	31	TCP	•					567	630	67	→ 1	.514	[P	SH,	ACK	(]
124 07:36:19.688488 0.011593 23.62.32.5	10.1.2	201.72		TCP	•					66	[TC	PK	eep	-A1	ive	AC	(] 2	443
125 07:36:19.761408 0.072920 10.1.201.105	224.0.	0.251		MDN	IS					81	Sta	nda	ird	que	ry	0x0(	900	AN
126 07:36:19.761408 0.000000 10.1.201.105	224.0.	0.251		MDN	IS					119	Sta	nda	ind	que	ry	resp	ons	se
	224.0.	0.252								110	Sta	nda	ira	que	ry	oxa:	9/3 / EN	AN
	10.1.2	207.200		NDN	IS IC					110	Reg	ist	rat	ion		SMI		
	239 25	5 255	250	SCD	15					216	M-S	EVB	пас Сн	топ * н		/1 1		100
131 07:36:19 761408 0.000000 10.1.201.31	10 1 2	07 255	250	NRN	IS IS					110	Reg	ict	rat	ion	NB	SWI	1- EN	NG-
132 07:36:19.843685 0.082277 44.236.123.131	10.1.2	201.72		TCP	,					56	151	4 →	63	067	ΓA	СК ]	Sec	a=1
	101111									20					1	]	200	<u> </u>
		0000	_	54	01	20	0		_	1.4	20		0	0.2	00	00	45	
> Frame 1: 100 bytes on wire (800 bits), 100 byte	s capt	0000	a0	51	00	29	c9	4e	a0 74	04	39	ce	9e	02	08	00	45	00
Ethernet II, Src: Cisco_ce:9e:02 (a0:04:39:ce:9	e:02),	0010	-00	56	CC 01	49	40	00	/1	40	ат	ст	34	72	85	ca 42	ba i	10
Transmission Control Protocol Sps Ponts 443 D	s, Dst	0020	69	48	£.	DD	T5	37	9C	40	64	62	ec	C2	е6 00	43	50	18
Transmission Control Protocol, SPC Port. 445, D	SUFOI	0030	08	00	TC	ea	00	70	1/ 2£	22	63	- 7	29	00	1-	00 E L	00	40
r mansport Layer Security		0040	00	00	58 01-	21	58	70	2T	22	DD	a/	ae 4-	89 4.£	1a	20	00	29
		0050	55	4T	90	ба	61	ze	99	аŏ	сс	10	4e	17	9т	20	9a .	33
		0060	еЗ	95	10	<b>c</b> 1												
<	>	<																>
● ℤ Wi-Fi: <live capture="" in="" progress=""></live>						Pa	acket	s: 132	Disp	played	: 132	(100.0	)%)			Pro	file: [	Default

## 2.2 - Ping traffic

The network frames that we are going to be examining are ICMP packets. We are going to generate ICMP requests by using the dos "ping" command.

The dos "ping" command by default generates four ICMP requests.

Open a command prompt window and ping <u>www.waketech.edu</u>.

GSE C:\WINDOWS\system32\cmd.exe	-	×
C:\Users>ping www.waketech.edu		î
Pinging www.waketech.edu [172.28.1.77] with 32 bytes of data: Reply from 172.28.1.77: bytes=32 time=2ms TTL=60 Reply from 172.28.1.77: bytes=32 time=2ms TTL=60 Reply from 172.28.1.77: bytes=32 time=2ms TTL=60 Reply from 172.28.1.77: bytes=32 time=2ms TTL=60		
Ping statistics for 172.28.1.77: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 2ms, Average = 2ms		
C:\Users>		

## 2.3 - Stop Capture

Wireshark should have captured the network traffic that we want to examine. There is no need for Wireshark to continue to capture packets.

You can stop capturing network traffic by one of the following ways:

- 1. Toolbar: Click "Stop capturing packets" icon
- 2. Menu: Capture  $\rightarrow$  Stop
- 3. Shortcut: CTRL+E

Capturing from Wi-Fi

Image: Compute Analyze Statistics Telephony Wireless Tools Help           No.         Time         Deta         Source         Destination         Protocol         Length         Info         Image: Compute State         Image: Compute State <th></th> <th>Capturing fr</th> <th>om Wi-Fi</th> <th></th> <th>-</th> <th>٥</th> <th>p</th> <th><math>\times</math></th>		Capturing fr	om Wi-Fi																								-	٥	p	$\times$
No.         Unite         Deta         Source         Destination         Protocol         Length         Info         Image: Constraint of the standard of the	File	Edit Vi	ew Go	Captu	ire Ana	lyze	Statistics	s Te	lepho	ny	Wireless	; Tool	s H	lelp																
No.         Time         Deta         Source         Destination         Protocol         Length         Info         ^           1701         07:37:21.716540         0.000000         10.1.201.105         224.0.0.251         MDNS         81         Standard query         0x0000         AN           1702         07:37:21.716540         0.000000         10.1.201.105         224.0.0.251         MDNS         81         Standard query         0x9000         AN           1704         07:37:21.716540         0.000000         10.1.201.105         124.0.0.251         MDNS         110         Registration NB         SMM-ENC-           1706         07:37:21.815716         0.000000         10.1.201.105         10.1.207.255         NBNS         110         Registration NB         SMM-ENC-           1706         07:37:21.815716         0.000000         10.1.201.252         10.1.207.255         NBNS         110         Registration NB         SMM-ENC-           1708         07:37:21.815716         0.000000         10.1.201.72         192.168.3.200         SNMS         92         Name query NB         MAKEGOU           1709         07:37:21.823549         0.007674         10.1.201.72         192.168.3.200         SNMP         83         get-request 1.3		🔳 🔬 🍺	010		9 9	⇔ ⇔	🗟 👔	Ŷ			€, €,	Q 🔢	¢.																	
No.         Time         Deta         Source         Destination         Protocol         Length         Info         A           1761         07:37:21.716540         0.009158         10.1.201.105         224.0.0.251         MDNS         81         Standard query 0x0000         AN           1702         07:37:21.716540         0.000000         10.1.201.105         224.0.0.251         MDNS         119         Standard query 0x576 AN           1704         07:37:21.716540         0.000000         10.1.201.105         10.1.207.255         NBNS         110         Registration NB SWM-ENG-           1706         07:37:21.815716         0.000000         10.1.201.105         10.1.207.255         NBNS         110         Registration NB SWM-ENG-           1706         07:37:21.815716         0.000000         10.1.200.252         10.1.207.255         NBNS         92         Name query NB WORKGROUP           1709         07:37:21.815716         0.0000259         10.1.207.255         NBNS         92         Name query NB WORKGROUP           1709         07:37:21.815716         0.0000259         10.1.207.255         NBNS         92         Name query NB WAKETECH(1           1709         07:37:21.823649         0.000259         10.1.201.72         192:168.3.2002		Ar Stop apt	uring pac	kets 1-/	/>																								-	·] +
1701 07:37:21.716540 0.009158 10.1.201.105       224.0.0.251       MDNS       81 Standard query 0x0000 AN         1702 07:37:21.716540 0.000000 10.1.201.105       224.0.0.251       MDNS       119 Standard query response         1703 07:37:21.716540 0.000000 10.1.201.105       224.0.0.252       LLMNR       75 Standard query 0x576 AN         1704 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB SWM-ENG-         1706 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WAKETECH:         1709 07:37:21.815716 0.000000 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.000001 10.1.201.72       192.168.3.202       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:22.176131 0.258361 10.1.201.72       22.112.127.43       TLSV1.2       248 Application Data         *	No.		Time			Delta		Sour	ce			Dest	inatio	'n		Prot	ocol				L	ength	Info							^
1702 07:37:21.716540 0.000000 10.1.201.105       224.0.0.251       MDNS       119 Standard query response         1703 07:37:21.716540 0.000000 10.1.201.105       224.0.0.252       LLMNR       75 Standard query %xf576 AN         1704 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB SWM-ENG-         1706 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB WM-ENG-         1706 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1709 07:37:21.823649 0.000259 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.094121 10.1.174.188       224.0.0.251       MDNS       553 Standard query response         1712 07:37:21.917770 0.094000 10.1.200.223       239.255.255.250       SDP       217 M-SEARCH * HTTP/1.1         1713 07:37:22.176131 0.258361 10.1.201.72       52.1127.43       TLSv1.2       248 Application Data       V         *       *       *       *       *       *       *       *       *       *	1701 07:37:21.716540 0.009158 10.1.201.105 224.0.0.251 MDNS 81 Standard query 0x6														0x0(	900	AN													
1703 07:37:21.716540 0.000000 10.1.201.105       224.0.0.252       LLMNR       75 Standard query 0xf576 AN         1704 07:37:21.815716 0.00000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB SWM-ENG-         1706 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB SWM-ENG-         1706 07:37:21.815716 0.000000 10.1.201.205       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1709 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1709 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1709 07:37:21.815716 0.000000 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1710 07:37:21.917770 0.004025 10.1.201.72       192.168.3.202       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.004000 10.1.200.223       239.255.255.250 SSDP       217 M-SEARCH * HTTP/1.1       1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSY1.2       248 Application Data       V         >       Frame 1:		1702	07:37	:21.7	16540	0.00	90000	10.	1.2	01.	105	224	.0.	0.251		MDN	IS					119	Sta	nda	ard	que	ry	resp	pon	se
1704 07:37:21.815716 0.090900 10.1.201.105       10.1.207.255       NBNS       110 Registration NB SWM-ENG- 1706 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB SWM-ENG- 1706 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB SWM-ENG- 1706 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1709 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1709 07:37:21.815716 0.000000 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1710 07:37:21.8233649 0.000259 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.094121 10.1.174.188       224.0.0.251       MDNS       553 Standard query response         1712 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data          *       *       *       *       *       *         > Frame 1: 100 bytes on wire (800 bits), 100 bytes capt       0000       a0 51 0b 29 c9 4e a0 b4 39 ce 9e 02 08 000 45 00       *       *       *       *         > Internet Protocol Version 4, Src: 52.114.133.205, Dst       0010       005 6c c49 40 00 71 06 af cf 34 72 85 cd 08 01       *       *       *       *       *		1703	07:37	:21.7	16540	0.00	90000	10.	1.2	01.	105	224	.0.	0.252		LLM	INR					75	Sta	nda	ard	que	ry	0xf	576	AN
1705 07:37:21.815716 0.000000 10.1.201.105       10.1.207.255       NBNS       110 Registration NB WORKGROU         1706 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1709 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1710 07:37:21.823390 0.007674 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.094121 10.1.174       192.168.3.202       SNMP       83 get-request 1.3.6.1.2.1.         1712 07:37:21.917770 0.094020 10.1.200.223       239.255.255.250       SSDP       217 M-SEARCH * HTTP/1.1         1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data             0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00         > Frame 1: 100 bytes on wire (800 bits), 100 bytes capt       0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00       0010       00 56 cc 49 40 00 71 06 af cf 34 72 85 cd 0a 01       0020       c9 48 01 bb f5 37 0c 40       64 62 ce cc 2e 64 35 0		1704	07:37	:21.8	815716	0.09	99176	10.	1.2	01.	105	10.	1.2	07.255		NBN	IS					110	Reg	ist	rat	ion	NB	SWI	4-EI	VG-
1706 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       110 Registration NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.823300 0.007674 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1710 07:37:21.823649 0.000259 10.1.201.72       192.168.3.202       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.094121 10.1.174.188       224.0.0.251       MDNS       553 Standard query response         1712 07:37:21.917770 0.000000 10.1.200.223       239.255.255.250 SSDP       217 M-SEARCH * HTTP/1.1         1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data             0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00         > Ethernet II, Src: Cisco_ce:9e:02 (a0:b4:39:ce:9e:02),       0010       005 6c c4 94 00 07 10 6 af cf 34 72 85 cd 0a 01       0010         > Internet Protocol Version 4, Src: 52.114.133.205, Dst       0020 c9 48 01 bb f5 37 0c 40 64 62 ec c2 e6 43 50 18       0030 08 06 ce a0 00 017 03 03 00 29 00 00 00 00 00       0030 08 06 ce a0 00 017 03 03 00 29 00 00 00 00 00       0030 08 06 ce a0 00 017 03 03 00 29 00 00 00 00		1705	07:37	:21.8	815716	0.00	90000	10.	1.2	01.	105	10.	1.2	07.255		NBN	IS					110	Reg	ist	rat	ion	NB	SWI	4-EI	VG-
1707 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WORKGROUP         1708 07:37:21.815716 0.000000 10.1.200.252       10.1.207.255       NBNS       92 Name query NB WAKETECH         1709 07:37:21.823300 0.007674 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1710 07:37:21.823649 0.000259 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.094121 10.1.174.188       224.0.0.251       MDNS       553 Standard query response         1712 07:37:21.917770 0.090000 10.1.200.223       239.255.255.250 SSDP       217 M-SEARCH * HTTP/1.1         1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data          Frame 1: 100 bytes on wire (800 bits), 100 bytes capt       0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00         > Ethernet II, Src: Cisco_ce:9e:02 (a0:b4:39:ce:9e:02),       0010       00 56 cc 49 40 00 71 06 af cf 34 72 85 cd 0a 01         > Mother Protocol Version 4, Src: 52.114.133.205, Dst       0020       c9 48 01 bb f5 37 0c 40 64 62 ec c2 e6 43 50 18       0030       08 00 fc ea 00 00 17 03 03 00 29 00 00 00 00 00       0040       0040 00 08 327 38 70 2f 22 bb a7 de 89 1a 5b 0b d9       0050 55 4f 9b 6a 61 2e 99 a8 cc 10 4e 1f 9f 20 9a 33       0060       e3 95 1c c1		1706	07:37	:21.8	815716	0.00	00000	10.	1.2	01.	105	10.	1.2	07.255		NBN	IS					110	Reg	ist	rat	ion	NB	WOF	RKG	ROU
1708 07:37:21.813716 0.000000 10.1.200.222       10.1.207.252       10.1.207.255       NBNS       92 Name query NB WakeFECH(1         1709 07:37:21.823390 0.0007674 10.1.201.72       192.168.3.200       SNMP       83 get-request 1.3.6.1.2.1.         1710 07:37:21.823649 0.000259 10.1.201.72       192.168.3.202       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.094121 10.1.174.188       224.0.0.251       MDNS       553 Standard query response         1712 07:37:21.917770 0.094000 10.1.200.223       239.255.250 SSDP       217 M-SEARCH * HTTP/1.1       1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data                   > Frame 1: 100 bytes on wire (800 bits), 100 bytes capt       0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00          > Internet Protocol Version 4, Src: 52.114.133.205, Dst       0010       00 56 cc 49 40 00 71 06 af cf 34 72 85 cd 0a 01          > Transmission Control Protocol, Src Port: 443, Dst Por         0030 08 00 fc ea 00 00 17 03 03 00 29 00 00 00 00          > Mono 40 00 03 82 7 38 70 2f 22       bb a7 de 89 1a 5b 0b d9              > Transport Layer Security <td></td> <td>1707</td> <td>07:37</td> <td>:21.8</td> <td>815716</td> <td>0.00</td> <td>00000</td> <td>10.</td> <td>1.2</td> <td>00.</td> <td>252</td> <td>10.</td> <td>1.2</td> <td>07.255</td> <td></td> <td>NBN</td> <td>IS IS</td> <td></td> <td></td> <td></td> <td></td> <td>92</td> <td>Nam</td> <td>ie d</td> <td>quer</td> <td>y N</td> <td>BW</td> <td>ORK</td> <td>GRO</td> <td>JP&lt;</td>		1707	07:37	:21.8	815716	0.00	00000	10.	1.2	00.	252	10.	1.2	07.255		NBN	IS IS					92	Nam	ie d	quer	y N	BW	ORK	GRO	JP<
1769 07:37:21.823549 0.0074 16:1.201.72       192.168.3.200       SNMP       35 get-request 1.3.6.1.2.1.         1710 07:37:21.823649 0.000259 10.1.201.72       192.168.3.202       SNMP       83 get-request 1.3.6.1.2.1.         1711 07:37:21.917770 0.0004121 10.1.174.188       224.0.0.251       MDNS       553 Standard query response         1712 07:37:22.176131 0.258361 10.1.200.223       239.255.255.250 SSDP       217 M-SEARCH * HTTP/1.1         1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data		1708	07:37	:21.8	315/16	0.00	00000	10.	1.2	00. 01	252	10.	1.2	07.255	0	NRI	IS ID					92	Nan	ie d	luer	yN -∸	8 W.	AKE	I ECI	4<1
1710 07:37:21.917770 0.094121 10.1.174.188       224.00.0.251       MDNS       553 Standard query response         1711 07:37:21.917770 0.000000 10.1.200.223       239.255.255 .250 SSDP       217 M-SEARCH * HTTP/1.1         1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data         >       Frame 1: 100 bytes on wire (800 bits), 100 bytes capt       0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00         >       Ethernet II, Src: Cisco_ce:9e:02 (a0:b4:39:ce:9e:02),       0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00         >       Internet Protocol Version 4, Src: 52.114.133.205, Dst       0000       a0 51 0b 53 70 c40       64 62 ec c2 e6 43 50 18         >       Transmission Control Protocol, Src Port: 443, Dst Por       0030       08 00 fc ea 00 00 17 03 03 00 29 00 00 00 00       00         >       Transport Layer Security       0000       55 4f 9b 6a 61 2e 99 a8       cc 10 4e 1f 9f 20 9a 33       0660       e3 95 1c c1		1709	07:37	.21.0	222290	0.00	2/6/4	10.	1.2	01. 01	72	192	1.10	0.5.20	9 2	SINP						00	get	-re	eque	st c+	1.2	.0	1.2	1
1711 07.37:21.917770 0.000000 10.1.200.223       239.255.255.250 SSDP       217 M-SEARCH * HTTP/1.1         1712 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data                 > Frame 1: 100 bytes on wire (800 bits), 100 bytes capt       0000       a0 51 0b 29 c9 4e a0 b4 39 ce 9e 02 08 00 45 00          > Ethernet II, Src: Cisco_ce:9e:02 (a0:b4:39:ce:9e:02),       0010       005 6c cc 49 40 00 71 06 af cf 34 72 85 cd 0a 01          > Internet Protocol Version 4, Src: 52.114.133.205, Dst       0020       c9 48 01 bb f5 37 0c 40 64 62 ec c2 e6 43 50 18          > Transmission Control Protocol, Src Port: 443, Dst Por       0030       08 00 fc ea 00 00 17 03 03 00 29 00 00 00 00          > Transport Layer Security       0040       00 38 27 38 70 2f 22 bb a7 de 89 1a 5b 0b d9           0050       55 4f 9b 6a 61 2e 99 a8 cc 10 4e 1f 9f 20 9a 33             0060       e3 95 1c c1		1710	07.37	· 21.0	17770	0.00	3/121	10.	1 1	74	188	224	0	0.2.20	Z	MDN	IF IS					553	sec sta	nda	eque and	auo	1.J	.0	1.2	
1713 07:37:22.176131 0.258361 10.1.201.72       52.112.127.43       TLSv1.2       248 Application Data                >       Frame 1: 100 bytes on wire (800 bits), 100 bytes capt       0000       a0 51 0b 29 c9 4e a0 b4 39 ce 9e 02 08 00 45 00         >       Ethernet II, Src: Cisco_ce:9e:02 (a0:b4:39:ce:9e:02),       0010       00 56 cc 49 40 00 71 06 af cf 34 72 85 cd 0a 01         >       Internet Protocol Version 4, Src: 52.114.133.205, Dst       0020       c9 48 01 bb f5 37 0c 40 64 62 ec c2 e6 43 50 18         >       Transmission Control Protocol, Src Port: 443, Dst Por       0030       08 00 fc ea 00 00 17 03 03 00 29 00 00 00 00         >       Transport Layer Security        0050       55 4f 9b 6a 61 2e 99 a8 cc 10 4e 1f 9f 20 9a 33         0060       e3 95 1c c1		1712	07:37	:21.9	17770	0.00	20000	10.	1.2	00.	223	239	. 25	5.255.	250	SSE	)P					217	M-S	FΔR	ксн	чис * Н	'у ТТР	/1.1	1	
<pre>&lt;</pre>		1713	07:37	:22.1	76131	0.25	58361	10.	1.2	01.	72	52.	112	.127.4	3	TLS	5v1.	.2				248	App	lic	ati	on	Dat	a		
Frame 1: 100 bytes on wire (800 bits), 100 bytes capt Ethernet II, Src: Cisco_ce:9e:02 (a0:b4:39:ce:9e:02), Internet Protocol Version 4, Src: 52.114.133.205, Dst Transmission Control Protocol, Src Port: 443, Dst Por Transport Layer Security          0000       a0 51 0b 29 c9 4e a0 b4       39 ce 9e 02 08 00 45 00         0010       00 56 cc 49 40 00 71 06       af cf 34 72 85 cd 0a 01         0020       c9 48 01 bb f5 37 0c 40       64 62 ec c2 e6 43 50 18         0030       08 00 fc ea 00 00 17 03       03 00 29 00 00 00 00         0040       00 00 38 27 38 70 2f 22       bb a7 de 89 1a 5b 0b d9         0050       55 4f 9b 6a 61 2e 99 a8       cc 10 4e 1f 9f 20 9a 33         0060       e3 95 1c c1	<																													> <sup>×</sup>
<pre>&gt; Ethernet II, Src: Cisco_ce:9e:02 (a0:b4:39:ce:9e:02), &gt; Internet Protocol Version 4, Src: 52.114.133.205, Dst &gt; Transmission Control Protocol, Src Port: 443, Dst Por &gt; Transport Layer Security</pre> 0010 00 56 cc 49 40 00 71 06 af cf 34 72 85 cd 0a 01 0020 09 48 01 bb f5 37 0c 40 64 62 ec c2 e6 43 50 18 0030 08 00 fc ea 00 00 17 03 03 00 29 00 00 00 00 00 0040 00 03 8 27 38 70 2f 22 bb a7 de 89 1a 5b 0b d9 0050 55 4f 9b 6a 61 2e 99 a8 cc 10 4e 1f 9f 20 9a 33 0060 e3 95 1c c1	>	Enamo 1	· 100	hyte	- on w	ino	(800	hit	·c)	10	a hyt	os ca	ant	0000	a0	51	Øh	29	<u>6</u> 9	40	a0	h4	39	CP	96	02	08	99	45	99
<ul> <li>&gt; Internet Protocol Version 4, Src: 52.114.133.205, Dst</li> <li>&gt; Transmission Control Protocol, Src Port: 443, Dst Por</li> <li>&gt; Transport Layer Security</li> <li>0020</li> <li>c9 48 01 bb f5 37 0c 40 64 62 ec c2 e6 43 50 18</li> <li>0030</li> <li>0040</li> <li>0040</li> <li>0040</li> <li>0050</li> <li>55 4f 9b 6a 61 2e 99 a8 cc 10 4e 1f 9f 20 9a 33</li> <li>e3 95 1c c1</li> </ul>	Ś	Ftherne	+ TT.	Src:	Cisco	ce:	9e:02	) (a	.∍/, i0:b/	4:3	9:ce:	9e:00	2).	0010	00	56	сс	49	40	00	71	06	af	cf	34	72	85	cd	0a	01
> Transmission Control Protocol, Src Port: 443, Dst Por > Transport Layer Security          0030       08 00 fc ea 00 00 17 03 03 00 29 00 00 00 00 00 0040       00 8 00 fc ea 00 00 17 03 03 00 29 00 00 00 00 00 0040       00 00 38 27 38 70 2f 22 bb a7 de 89 1a 5b 0b d9 055 4f 9b 6a 61 2e 99 a8 cc 10 4e 1f 9f 20 9a 33 0060	>	Interne	t Prot	ocol	Versi		. Sro	c: 5	2.1	14.	133.2	05. E	Dst	0020	c9	48	01	bb	f5	37	0c	40	64	62	ec	c2	e6	43	50	18
> Transport Layer Security       0040     00 40     00 40     38 27 38 70 2f 22     bb a7 de 89 1a 5b 0b d9       0050     55 4f 9b 6a 61 2e 99 a8     cc 10 4e 1f 9f 20 9a 33       0060     89 1c c1	>	Transmi	ssion	Cont	rol Pr	otoc	ol, 9	Src	Por	t:	443,	Dst F	Por	0030	08	00	fc	ea	00	00	17	03	03	00	29	00	00	00	00	00
0050 55 4f 9b 6a 61 2e 99 a8 cc 10 4e 1f 9f 20 9a 33 0060 e3 95 1c c1	>	Transpo	rt Lay	er Se	ecurit	y	1				1			0040	00	00	38	27	38	70	2f	22	bb	a7	de	89	1a	5b	Øb	d9
0060 e3 95 1c c1														0050	55	4f	9b	6a	61	2e	99	a8	cc	10	4e	1f	9f	20	9a	33
														0060	e3	95	1c	c1												
	<												>	<														11 -		>

## 2.4 - Filter ICMP requests

Even though we were only capturing network traffic for a small period of time, Wireshark would have captured hundreds if not thousands of packets. We want to limit packets to just show the ICMP requests and replies.

1. In the filter window type "ICMP" and hit Enter.

▲ *Wi-Fi File Edit View Go Capture Analyze Statistics Telephony Wireless	s Tools H	lelp											-	٥		×
	Q. III															
( icmp														X -	1.	] +
No. Time Delta Source	Destinatio	'n	F	Protocol				Leng	th Inf	o						
237 07:44:46.709979 0.000000 10.1.201.72	172.28	.1.77	]	ICMP				7	4 E c	ho	(pi	ng)	req	uest	i	d=0×
238 07:44:46.712328 0.002349 172.28.1.77	10.1.2	01.72	]	ICMP				7	'4 Ec	ho	(pi	ng)	rep	ly	i	d=0x
274 07:44:47.726548 1.014220 10.1.201.72	172.28	.1.77	]	ICMP				7	'4 Ec	ho	(pi	ng)	req	uest	i	d=0x
275 07:44:47.729931 0.003383 172.28.1.77	10.1.2	01.72	]	ICMP				7	'4 Ec	ho	(pi	ng)	rep	ly	i	d=0x
312 07:44:48.742718 1.012787 10.1.201.72	172.28	.1.77	]	ICMP				7	'4 Ec	ho	(pi	ng)	req	uest	i	d=0x
313 07:44:48.745126 0.002408 172.28.1.77	10.1.2	01.72	]	ICMP				7	'4 Ec	ho	(pi	ng)	rep	ly	i	d=0x
340 07:44:49.759847 1.014721 10.1.201.72	172.28	.1.77	]	ICMP				7	4 Ec	ho	(pi	ng)	req	uest	i	d=0x
- 341 07:44:49.762519 0.002672 172.28.1.77	10.1.2	01.72	]	ICMP				7	'4 Ec	ho	(pi	ng)	rep	ly	i	d=0x
< >																
<																>
> Frame 237: 74 bytes on wire (592 bits), 74 byt	es capt	0000	a0 I	b4 39	ce	9e	02 a	0 51	. 01	b 29	9 c9	4e	<b>0</b> 8	00 4	5 0	90
<pre>&gt; Ethernet II, Src: IntelCor_29:c9:4e (a0:51:0b:</pre>	29:c9:4	0010	00	3c 42	e0	00	00 E	0 01	. 7	7 20	e 0a	01	c9	48 a	ic 1	lc
> Internet Protocol Version 4, Src: 10.1.201.72,	Dst: 1	0020	01 4	4d 08	00	4d	4e 6	0 01	. 00	ð Ød	61	62	63	64 6	5 6	56
> Internet Control Message Protocol		0030	67	68 69	6a	6b	6c 6	id 6e	e 61	f 70	9 71	72	73	74 7	57	76
		0040	77	61 62	63	64	65 6	6 67	68	8 69	9					
C	>	5														>

You should see 8 packets in the Packet List pane. The 8 packets represent the 4 ICMP requests and a reply back for each request.

## 2.5 - Wireshark Configuration

We want to see the Packet Diagram in our view, so we need to set some preferences. The Packet Diagram shows a physical layout of the packet and makes looking at the frames easier.

Open the preferences by one of the following means:

- Menu: Edit  $\rightarrow$  Preferences...
- Shortcut: Ctrl+Shift+P

We want to change the layout of the Wireshark panes and we want to see the Packet Diagram in Pane 3. Make sure to save your preferences.



📕 *Wi	i-Fi								- I	J X
File	Edit View Go Capture	Analyze Statistics	s Telephony Wireless	Tools Help						
	1 🖉 🛞 📙 🔚 🔀 🖻	९ 🗢 🔿 🗟 🛉	: 👲 📃 🔳 🔍 Q (	R. 🎹						
📕 icm	ıp								×	
No.	Time	Delta	Source	Destination	Protocol	Length	Info			
	237 07:44:46.70	9979 0.000000	10.1.201.72	172.28.1.77	ICMP	74	Echo	(ping)	reques	st id=0x
	238 07:44:46.71	2328 0.002349	172.28.1.77	10.1.201.72	ICMP	74	Echo	(ping)	reply	id=0x
	274 07:44:47.72	6548 1.014220	10.1.201.72	172.28.1.77	ICMP	74	Echo	(ping)	reques	st id=0x
	275 07:44:47.72	9931 0.003383	172.28.1.77	10.1.201.72	ICMP	74	Echo	(ping)	reply	id=0x
	312 07:44:48.74	2718 1.012787	10.1.201.72	172.28.1.77	ICMP	74	Echo	(ping)	reques	st id=0x
	313 07:44:48.74	5126 0.002408	172.28.1.77	10.1.201.72	ICMP	74	Echo	(ping)	reply	id=0x
	340 07:44:49.75	9847 1.014721	10.1.201.72	172.28.1.77	ICMP	74	Echo	(ping)	reques	st id=0x
L	341 07:44:49.76	2519 0.002672	172.28.1.77	10.1.201.72	ICMP	74	Echo	(ping)	reply	id=0×
<										>
> Fr > Et > In	ame 237: 74 bytes hernet II, Src: 1 ternet Protocol \	s on wire (592 IntelCor_29:c9 /ersion 4, Sro	2 bits), 74 byte 9:4e (a0:51:0b:2 c: 10.1.201.72,	s Ethernet 9 0 1 1			15 16	1 1		
> In	ternet Control Me	essage Protoco	51			De		on		
						5	Source			
					Туре					
				Internet Proto	col Version 4					
							15 16			
<			:	Version	Header Le Differer	tiated Services Fie	ld Í		To	tal Lenrr≚
0 7	Wi-Fi				Packets:	454 · Displayed: 8	(1.8%) • [	Dropped: 0	(0.0%)    P	rofile: Default

Your screen should look like this now:

## Packet List

The top pane is the Packet List and shows all the packets that have been filtered. If you select a packet, then the panes below change to show that packet's information.

#### Packet Details

The bottom left pane is the Packet Details and shows the OSI model of the packet selected in the Packet List.

You can expand each level in the Packet Details to see more information.

## Packet Diagram

The bottom right pane is the Packet Diagram and shows the frame in a physical diagram that makes looking at the data easier. It shows the packet selected in the Packet List.

Right-click the Packet Diagram and Select "Show Field Values" so the field values will be shown in the Packet Diagram pane.

# Part 3: OSI – Physical layer

The Physical layer is the first layer of the OSI Model. It includes anything physically needed to send data from one location to another.

There are many possible mediums for the data to travel over and some examples are:

- Category cable
- Fiber
- Wireless

The network adapters of the Physical layer handles encoding the data into a format necessary to transfer the data based upon the medium. For Category cable, the data is encoded and transferred using voltages while fiber would utilize light. Radio waves are part of the Physical layer for Wireless.

The Physical layer includes but is not limited to:

- Network adaptors
- Medium
  - Copper and voltages for Category cables
  - Antennas and radio waves for Wi-Fi
- Hardware

Are the network adaptors considered part of the Physical layer?\_\_\_\_\_

For Category cables, how is the data represented over the wire?

Are radio waves considered part of the Physical layer?\_\_\_\_\_

If we are discussing speech from one person to another, name three items that would be considered part of the Physical layer?\_\_\_\_\_

## Part 4: Wireshark – Physical layer

We are going to examine the Physical layer in Wireshark.

Select the first packet in the Packet List. The first item in the Packet Details window represents the Physical layer of the OSI model.

Expand the Physical layer.

<b>/</b> * <b>\</b>	Vi-Fi					-	ð	×
File	Edit View Go Capture	Analyze Statistics Telephony Wir	reless Tools Help					
		₹ ← → ≌ ↑ <u>↓</u> ⊒ ⊒ ♥						
ic	mp						$\times$	• +
No.	Time	Delta Source	Destination	Protocol	Length Info			
►	237 07:44:46.709979	0.000000 10.1.201.72	172.28.1.77	ICMP	74 Echo (p	ing) request	id=0x0	001, s
-	238 07:44:46.712328	0.002349 172.28.1.77	10.1.201.72	ICMP	74 Echo (p:	ing) reply	id=0x0	001, s
	274 07:44:47.726548	1.014220 10.1.201.72	172.28.1.77	ICMP	74 Echo (p:	ing) request	id=0x0	001, s
	275 07:44:47.729931	0.003383 172.28.1.77	10.1.201.72	ICMP	74 Echo (p:	ing) reply	id=0x0	001, s
	312 07:44:48.742718	1.012787 10.1.201.72	172.28.1.77	ICMP	74 Echo (p:	ing) request	id=0x0	001, s
	313 07:44:48.745126	0.002408 172.28.1.77	10.1.201.72	ICMP	74 Echo (p:	ing) reply	id=0x0	001, s
	340 07:44:49.759847	1.014721 10.1.201.72	172.28.1.77	ICMP	74 Echo (p:	ing) request	id=0x0	001, s
L	341 07:44:49.762519	0.002672 172.28.1.77	10.1.201.72	ICMP	74 Echo (p:	ing) reply	id=0x0	001, s
<								>
V F	came 237 74 bytes on wir	e (592 bits) 74 bytes cant	Ethernet					•
	Section number: 1	()))))))))		1	h6			
5	Interface id: 0 (\Device	NPE {E137E075-D30C-450E-B	FIIII					
	Encansulation type: Ethe	ernet (1)		Desti	nation			
	Arrival Time: Aug 23, 20	23 07:44:46.709979000 Fast		a0:b4:39:ce:9e:02	�@ <b>�</b> @X@X@H@			
	[Time shift for this nat	ket: 0.00000000 seconds]					_	
	Enoch Time: 1692791086.	709979000 seconds						
	[Time delta from previo	is captured frame: 0.148969						
	[Time delta from previo	us displayed frame: 0.00000			-			
	[Time since reference of	first frame: 6.604997000	-0.51		urce			
	Frame Number: 237		10:01	00:29:09:480 <b>0</b> 00 <b>0000000000000000000000000000000</b>		.mp II		
	Frame Length: 74 bytes	(592 bits)		Type				
	Capture Length: 74 bytes	s (592 bits)	IPv4					
	[Frame is marked: False]	]						
	[Frame is ignored: False	•]	Internet Protocol Version	- 4				
	[Protocols in frame: et	h:ethertype:ip:icmp:data]	h	I	16		al	
	[Coloring Rule Name: IC	1P]	ř <del>i i i i i i i</del>					
	[Coloring Rule String: :	icmp    icmpv6]	Version Header Len.	Differentiated Services Field	Total Ler	ngth		
> E	thernet II, Src: IntelCor	_29:c9:4e (a0:51:0b:29:c9:4	400 0000 20000000	0x0000 🔶 00000 00	6000 0000 0	100000		
> 1	nternet Protocol Version 4	4, Src: 10.1.201.72, Dst: 1					_	
> 1	nternet Control Message P	rotocol	Iden	tification	Flags Fragn	nent Offset		
			0x42e0 (1712		0.000			
			Time to Live	Protocol	Header Chr	acksum		
					0х772епп пп			
					000000000000000000000000000000000000000			
<		>		Courses	Addross			~
$\bigcirc$	Frame (frame), 74 bytes			Packets: 4	54 · Displayed: 8 (1.8%) · Dr	opped: 0 (0.0%)	Profile:	Default

The Packet Diagrams pane is the bottom right pane. The Physical layer is not represented in the Packet Diagram pane and the top entry here represents the Data-link layer.

How many bytes are in this frame?\_\_\_\_\_

How many bits are in this frame?\_\_\_\_\_

There are 8 bits per byte. Does the number of bytes correspond to the number of bits in this frame?\_\_\_\_\_\_

What date & time did this frame arrive at?\_\_\_\_\_

Expand the "Interface id" and what is the Interface description?\_\_\_\_\_

Does the interface description match the network connection listed in "ncpa.cpl" that you are capturing traffic on for Wireshark?

In the Physical layer, do you see a MAC address field or an IPv4 address field?

In the Physical layer, why do you see or not see a MAC address field or an IPv4 address field?

## Part 5: OSI – Data Link layer

The Data-Link layer is the second layer in the OSI model. The Data-link layer is responsible for the node-to-node delivery. It delivers the data from a source node to the destination node and just moves data to the next hop.

The addressing for the Data-link layer is the MAC (media access control) or Physical address. While we may refer to devices by their IP address, the network utilizes the MAC address for its addressing at this layer.

The Data-link layer can only transmit to a node in the same LAN.

5.1 - MAC address

What is MAC an abbreviation for?

Is the MAC address the same as the Physical address?

How many bytes is a MAC address?\_\_\_\_\_

#### 5.2 - Ethernet II DIX frame



Answer the questions in this Part with help from the Network Communications for Buildings manual.

Using the manual, look at the Ethernet Frames section under Shared Ethernet to answer the following questions.

#### Ethernet II fields

Looking at the Ethernet II DIX Frame, answer the following questions:

What field is the first 64 bits (8 bytes)?\_\_\_\_\_

What field is the next 48 bits (6 bytes)?\_\_\_\_\_

What field is the next 48 bits (6 bytes)?\_\_\_\_\_

What field is the next 16 bits (2 bytes)?\_\_\_\_\_

Wake Tech BAT Lab14 of 23https://www.waketech.edu/programs-courses/credit/building-automation

Last updated: 8/28/2023

What field is the next field?
What field exists after the Data field?
<i>Preamble field</i> When calculating the size of the frame is the Preamble field considered part of the Ethernet frame?
Destination field Is the Destination field a MAC address or IPv4 address?
How many bits is the Destination field?
What is the purpose of the Destination field?
Does the Destination field represent the next hop or the final destination?
Is the Destination field a node in the same LAN?
Source field Is the Source field a MAC address or IPv4 address?
How many bits is the Source field?
What is the purpose of the Source?
Data Type field Does the Data-link layer guarantee delivery of data?
If delivery of data is guaranteed who would do that?
What is the purpose of the Type field?
Data field What is the minimum size of the Data field?
What is the maximum size of the Data field?
What is a runt packet?

## Frame Check Sequence field

The Frame Check Sequence is sometimes abbreviated to FCS.

What is the purpose of the FRC field?\_\_\_\_\_

How does the destination node utilize the FRC field?

What is considered a successful transmission according to the FRC field?\_\_\_\_\_

At this layer, if the destination calculates the FRC and the calculated FRC does not match the FRC field sent in the frame, is the source node informed?

# Part 6: Wireshark – Data-link layer – ICMP request

We are going to look at an Ethernet frame in Wireshark.

Close the expanded Physical layer in the Packet Details pane to hide the Physical layer details.

The second item in the Packet Details represents the second layer of the OSI model. Expand the second item in the Packet Details list to show the frame in the Packet Diagram pane.

## 6.1 - ICMP request

Make sure you are still looking at the first packet in the Packet List as this is an ICMP request. In an ICMP request, your laptop is sending a request to <u>www.waketech.edu</u>. With the request, your laptop is the source.

The Data-link layer just handles node-to-node traffic.

For any traffic to travel outside your LAN, the traffic will go through the Default Gateway, so the Default Gateway is where this ICMP request is going to. While there are many more hops before the packet gets to the final destination; we are only capturing the traffic to and from our network interface. With the ICMP request, the Default Gateway is the destination because the final destination is outside our LAN.

## Destination field

Click on the Destination field in the Packet Details and you should see the Destination field will be highlighted in the Packet Diagram in the right pane.

	*Wi-Fi							-	đ	×
File	e Edit View Go Capture Ar	alyze Statistics	Telephony W	Vireless Tools Help						
	🔳 🖉 💽 📙 🛅 🗙 🖸 🤇	🗢 🔿 😤 🛉	<u>↓</u> _   =   €	B. O. O. 🎹						
	icmp								$\times \rightarrow$	• +
No.	Time	Delta	Source	Destination	Protocol	Length	Info			
	237 07:44:46.709979	0.000000	10.1.201.72	172.28.1.77	ICMP	74	Echo (ping)	request	id=0x0	001, s
-	238 07:44:46.712328	0.002349	172.28.1.77	10.1.201.72	ICMP	74	Echo (ping)	reply	id=0x0	001, s
	274 07:44:47.726548	1.014220	10.1.201.72	172.28.1.77	ICMP	74	Echo (ping)	request	id=0x0	001, s
	275 07:44:47.729931	0.003383	172.28.1.77	10.1.201.72	ICMP	74	Echo (ping)	reply	id=0x0	001, s
	312 07:44:48.742718	1.012787	10.1.201.72	172.28.1.77	ICMP	74	Echo (ping)	request	id=0x0	001, s
	313 07:44:48.745126	0.002408	172.28.1.77	10.1.201.72	ICMP	74	Echo (ping)	reply	id=0x0	001, s
	340 07:44:49.759847	1.014721	10.1.201.72	172.28.1.77	ICMP	74	Echo (ping)	request	id=0x0	001, s
	341 07:44:49.762519	0.002672	1/2.28.1.//	10.1.201.72	ICMP	/4	Echo (ping)	reply	1d=0x0	001, s
<										>
>	Frame 237: 74 bytes on wire	(592 bits), 7	4 bytes capt	Ethernet						~
$\sim$	Ethernet II, Src: IntelCor_2	9:c9:4e (a0:5	1:0b:29:c9:4	6	1	16			31	
	> Destination: Cisco_ce:9e:0	02 (a0:b4:39:	ce:9e:02)							
	<pre>&gt; Source: IntelCor_29:c9:4e</pre>	(a0:51:0b:29	:c9:4e)		Desti	nation	_			
	Type: IPv4 (0x0800)				a0:b4:39:ce:9e:02	• • • • • • • • • • • • • • • • • • •	œ			
>	Internet Protocol Version 4,	Src: 10.1.20	1.72, Dst: 1							
>	Internet Control Message Pro	tocol								
					So	urce				
					a0:51:0b:29:c9:	4e 0000 00				
				ID-4	lype					
				IPV4						
				Internet Protocol Version	4					
				P	1 1 1 1 1 1 1 1	16			31	
				Mania a Mania Ian	Differentiated Convine Field		Tetal I an oth			
				400 0000 20v@A@	0v0000 A DDADD DD	6	Iotal Length	חו		
				400 0000		, °				
				Ident	ification	Flags	Fragment (	Offset		
				0x42e0 (1712	))	0x000	000 000			
						<u>├</u>			+	
				Time to Live	Protocol	F	leader Checksu	m		
				12800 0000 00	ICMPe00 0000 00	0x7	72e00 0000			
<			>			Address				~
0	Z Destination Hardware Address	(eth.dst), 6 byte	;		Packets: 4	54 · Displayed: 8	(1.8%) · Dropped	: 0 (0.0%)	Profile:	Default

What is the Destination (MAC address only) of the Ethernet frame?\_\_\_\_\_

What is the MAC address of your Default Gateway?\_\_\_\_\_

Is the Destination of the Ethernet frame the same as the Default Gateway?\_\_\_\_\_

If you answered No, troubleshoot the issue.

The Destination field is how many bytes?\_\_\_\_\_

The Destination address of the Ethernet frame should match the MAC address of the Default Gateway.

## *Source field*

Click on the Source field in the Packet Details and you should see the Source field will be highlighted in the Packet Diagram in the right pane.

	*Wi-Fi								-	đ	×
File	e Edit View Go Capture	Analyze Statistics	Telephony V	Vireless Tools He	elp						
	🔳 🖉 🛞 📙 🔚 🔀 🖸 🖉	९ 🗢 🗢 🕾 👔		R. Q. Q. 🎹							
	icmp									$\times \rightarrow$	<b>•</b> +
No	Time	Delta	Source	Destination	n	Protocol	Length	Info			
_►	237 07:44:46.709979	0.000000	10.1.201.72	172.28.1	.77	ICMP	74	Echo (pin	g) request	id=0x0	001, s
-	238 07:44:46.712328	0.002349	172.28.1.77	10.1.201	.72	ICMP	74	Echo (pin	g) reply	id=0x0	001, s
	274 07:44:47.726548	1.014220	10.1.201.72	172.28.1	.77	ICMP	74	Echo (pin	g) request	id=0x0	001, s
	275 07:44:47.729931	0.003383	172.28.1.77	10.1.201	.72	ICMP	74	Echo (pin	g) reply	id=0x0	001, s
	312 07:44:48.742718	1.012787	10.1.201.72	172.28.1	.77	ICMP	74	Echo (pin	g) request	1d=0x0	001, s
	313 07:44:48.745126	0.002408	1/2.20.1.//	10.1.201	.72	TCMP	74	Echo (pin	g) reply	10=0x0	001, S
	341 07:44:49.759647	0.0014721	172 28 1 77	1/2.20.1	72	TCMP	74	Echo (pin	<ol> <li>request</li> <li>reply</li> </ol>	id-0x6	001, 5
_	541 07.44.45.702515	0.002072	1/2.20.1.//	10.1.201	.72	TCHE	/4	CCHO (pin	5) герту	10-070	001, 3
<											>
>	Frame 237: 74 bytes on wir	e (592 bits), 7	4 bytes capt	Ethernet							^
~	Ethernet II, Src: IntelCor	_29:c9:4e (a0:5	1:0b:29:c9:4	°		15	16			31	
	> Destination: Cisco_ce:96	e:02 (a0:b4:39:	ce:9e:02)			Desti	nation				
	<pre>&gt; Source: IntelCor_29:c9:4 Type: TPu4 (0x0800)</pre>	4e (a0:51:0D:29	:c9:4e)			a0:b4:39:ce:9e:0	02 0000 00				
5	Internet Protocol Version	4. Spc: 10.1.20	1.72. Dst: 1								
Ś	Internet Control Message P	rotocol									
	5										
						Sou	- urce				
						a0:51:0b:29:c9:4	4e 0000 00				
							1				
					Ту	/pe					
					IPv400						
							_				
				Internet Proto	col Version	4					
				° I I I		15	16			31	
				Version	Header Len	Differentiated Services Field		Total Lengt	h		
				400 00¢0	2000 00�	0x0000 0000 00	6	5000 0000	] 00		
								-		_	
					Identif 42-0 (17120)	fication	Flags	Fragmer	nt Offset		
					4260 (17120)						
				Timet	to Live	Protocol	1	Header Check	sum		
				12800	0000 00	CMP00 0000 00	0x7	72e00 00	00 00		
<			>			-					~
	Source Hardware Address (	eth.src) 6 bytes				Packets: 4	Addrocc 54 - Displayed: 8	(1.8%) · Drop	ped: 0 (0.0%)	Profile	Default
0		constant of the officer				- detects -	s. s.spidycaro	(inclusive prop	p = 20. 0 (01070)	onnea	e ci d'ant

What is the Source (MAC address only) of the Ethernet frame?\_\_\_\_\_

What is MAC address of your network interface from Part 1?\_\_\_\_\_

Is the Source of the Ethernet frame the same as your network interface?

➢ If you answered No, troubleshoot the issue.

The Source field is how many bytes?\_\_\_\_\_

The Source address of the Ethernet frame should match the MAC address of your network interface. This shows that your network interface is sending the data.

#### Type field

What is the Type field of the Ethernet frame?\_\_\_\_\_

## Preamble field

Do you see the Preamble field?

Why do you see or not see the Preamble field?

#### FCS field

Do you see the FCS field?\_\_\_\_\_

Why do you see or not see the FCS field?\_\_\_\_\_

#### IP Address

In the Data-link layer, is the IPv4 address referenced?\_\_\_\_\_

In the Data-link layer, why do you see or not see an IPv4 address?\_\_\_\_\_

# Part 7: Wireshark – Data-link layer – ICMP reply

## 7.1 - ICMP reply

Select the second packet in the Packet List pane is the reply to the first packet which was a request.

We want to look at the ICMP reply which is the response to our request. Now this implies the packet is going to our laptop. With the ICMP request, our network interface was the source; however, with the ICMP reply out network interface is the destination.

#### Destination field

Click on the Destination field in the Packet Details.



What is the Destination (MAC address only) of the Ethernet frame?\_\_\_\_\_

What is MAC address of your network interface?

Is the Destination of the Ethernet frame the same as your network interface?\_

➢ If you answered No, troubleshoot the issue.

Since this is the ICMP reply, the Destination address of the Ethernet frame should match the MAC address of your network interface.

#### *Source field*

Click on the Source field in the Packet Details.

Eil	*Wi-Fi Edit View Go Capture An	nalvze Statistics Telenhony Wireless	Tools Help		-	- 0 ×
			<ul> <li>Interp</li> <li>Interp</li> </ul>			
			<b>~</b> Ⅲ			
No	lime	Delta Source	Destination	Protocol	Length Info	
7*	237 07:44:46.709979	0.000000 10.1.201.72	1/2.28.1.//	ICMP	74 Echo (ping) reque	st 1d=0x0001, s
4-	236 07:44:46.712328	0.002349 1/2.28.1.//	10.1.201.72	TCMP	74 Echo (ping) reply	1d=0x0001, s
	274 07:44:47.720340	0.003383 172 28 1 77	1/2.20.1.//	TCMP	74 Echo (ping) reque	id=0x00001, 5
	312 07:44:47.725551	1 010787 10 1 201 72	172 28 1 77	TCMP	74 Echo (ping) repu	id=0x0001, 5
	313 07:44:48 745126	0 002408 172 28 1 77	10 1 201 72	TCMP	74 Echo (ping) requi	id=0x0001, 3
	340 07:44:40.745120	1 014721 10 1 201 72	172 28 1 77	TCMP	74 Echo (ping) requi	st id=0x0001, s
IL.	341 07:44:49.762519	0.002672 172.28.1.77	10.1.201.72	TCMP	74 Echo (ping) reply	id=0x0001, s
	512 07111101702515	01002072 17212011777	10111201172	2011	, ceno (ping) (cpi	14 0.0001, 5
<						>
>	Frame 238: 74 bytes on wire	(592 bits), 74 bytes capt	Ethernet			^
$\sim$	Ethernet II, Src: Cisco_ce:9	e:02 (a0:b4:39:ce:9e:02),	0 1 1 1 1 1 1 1	15	16	31
	<pre>&gt; Destination: IntelCor_29:</pre>	c9:4e (a0:51:0b:29:c9:4e)		Dectiv	nation	
	> Source: Cisco_ce:9e:02 (additional content of the second cont	0:b4:39:ce:9e:02)		a0:51:0b:20:c0:4		
	Type: IPv4 (0x0800)			00.51100.25105.		
>	Internet Protocol Version 4,	Src: 172.28.1.77, Dst: 1				
>	Internet Control Message Pro	otocol				
					1	
				Sou	urce	
				a0:b4:39:ce:9e:0	02 000 00	
			т			
			ID://f (//9/05)TL F	ne non no		
			1PV4I (40495)U L			
			Internet Protocol Version	4		
				15		31
			Version Header Len	Differentiated Services Field	Total Length	
			4p@∲@∲ 20 000	0x0000 0000 0000 00	6000 0000 00	
			ldentif	ication	Flags Fragment Offset	
			0xbd6f (48495)□	0000 0000 00	0x0_10	
			-			
			lime to Live	Protocol	Header Checksum	
				CMP100000630000000000	0x409100 0000 00	
<		>		Source	Addross	×
C	Source Hardware Address (eth	n.src), 6 bytes		Packets: 45	54 · Displayed: 8 (1.8%) · Dropped: 0 (0.0	%) Profile: Default

What is the Source (MAC address only) of the Ethernet frame?\_\_\_\_\_

What is MAC address of your network interface from Part 1?\_\_\_\_\_

Is the Source of the Ethernet frame the same as the Default Gateway?

➢ If you answered No, troubleshoot the issue.

Since this is an ICMP reply, the Source address of the Ethernet frame should match the MAC address of the Default Gateway. This shows that your network interface is sending the data.

## Part 8: Summary

How many bits is a MAC address?\_\_\_\_\_

How many bytes is a MAC address?\_\_\_\_\_

Last updated: 8/28/2023

Does the OSI Physical layer reference an address?

In the OSI Data-link layer, what types of addresses are used?\_\_\_\_\_

In detail, explain why the source address of the ICMP request is the destination of the ICMP reply?\_\_\_\_\_

In detail, explain why the destination address of the ICMP request is the source of the ICMP reply?\_\_\_\_\_