Using Wireshark to Capture Network Traffic

When troubleshooting an issue in an HDA installation, you may be required to capture the network traffic at the jobsite to help determine the cause of an issue. To do this, we will use the Wireshark application.

1. Install Wireshark on a PC that is on the **same local network** as the HDA system.

Windows 64-bit install package Windows 32-bit install package iOS Mac install package

2. Open Wireshark:

In Windows, **right-click** the Wireshark icon and **"Run as Administrator"**

	7		
		Open	
Wire		Move to OneDrive	
		Open file location	
	•	Run as administrator	
W	S	Share with Skype	
llestadi		Troubleshoot compatibility	
Using		Pin to Start	
		7-Zip	>
		CRC SHA	>

3. Pick **a PC adapter** to use for the network capture.

Typically, the interface showing the most network activity will be the interface to choose.

In this example, a PC is connected to the router using wired Ethernet.

In the below picture, the "Ethernet" interface is showing the most network activity, as signified by the line graph of network traffic next to the text "Ethernet"

📕 Tł	ne Wires	shark Net	twork	Analyzer							
File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help	
		0	010	XC	9 🗢 🖻) 😤 T	& 📑 🔳	\oplus Θ (R. III.		
Ap	oply a di	splay filte	r <(Ctrl-/>							
				Welo	ome to Wi	reshark					
				Capt	ure						
				using	this filter:	Enter a	capture filter				
					Local Area	Connecti	on* 10				
					Local Area	Connecti	on* 9				
					Local Area	Connecti	on* 8			-	
				- e	Bluetooth	Network (Connection 2				
					Ethernet			m	~~~~~	л	
					Local Area	Connecti	on* 2			-	
					Local Area	Connecti	on* 1			-	
					Wi-Fi						
					Adapter fo	or loopbac	k traffic captur	e /	Л.	L	
				۲	USBPcap1						

In this case you would double-click on the "Ethernet" line item to begin capturing network traffic.

If possible, used wired Ethernet to capture network traffic.

4. **Windows**: if you view the following **error** window when opening Wireshark:

🔼 The	e Wireshark Network Analyzer							
<u>F</u> ile	🗖 Wireshark	_		×	ools	<u>H</u> el		
Eilter	ter The NPF driver isn't running. You may have trouble capturing or listing interfaces.							
Ī	Don't show this me			ula	r Ne			
Capture								
□ Interface List								

Run C prompt as "Administrator" on the local PC. (Right-click on the C-Prompt application)

0/	T Open
	G Run as administrator
	部 Pin to Start
ed by Atlassian JIRA	>6 Oripin from taskbar B Properties a problem
パ Unpin from taskt	par
🖾 🗓 🖬 🖬 🔤 🖉	a ② 🖬 🧏 國 💁 👘 ② ヘ 🎬 11:24 AM Thursday 専 空 切》 7/1/2021

Type in "net start npf" after the "system32" prompt, as shown below.

Time	Source	Destination	1
5.483736	192.168.1.15	235.0.1.10	-
5.50 Administrator: C 5.81	ommand Prompt	225 122 0 1	
5.90Microsoft Windo 5.91(c) 2020 Micros 5.94	ows [Version 10.0.19041.746] soft Corporation. All rights r	eserved.	
5.97C:\WINDOWS\syst	em32≻net start npf		
6.15The Npcap Packe 6.18 6.19 6.32	et Driver (NPF) service was st	arted successfully.	
C:\WINDOWS\syst	:em32>		
: a4 1, S trol			

5. Wireshark will **begin capturing network packets**. Let the Wireshark Capture **run for 4-5 minutes.**

	🙇 Capturing from Ethernet											
File	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help											
	<u>/ = 1</u> 🐵 🗈 🗙 🖻 9, (=) 🕸 🗿 🞍 🚍 🔍 9, (9, 9, 9)											
	Apply a display filter <ctrl-></ctrl->											
No.	Time	Source	Destination	Protocol	Length	Info						
	1666 13.713949	192.168.1.164	52.96.170.82	TLSv1.2	408	Application Data						
	1667 13.719192	Universa_46:00:2b	Spanning-tree-(for-bridges	MRP-MVRP	60	Multiple VLAN Registration Protocol						
	1668 13.719619	Universa_46:00:2b	LLDP_Multicast	MRP-MSRP	60	Multiple Stream Reservation Protocol						
	1669 13.741448	192.168.1.33	235.0.1.10	UDP	147	50398 → 5600 Len=105						
	1670 13.749202	192.168.1.39	255.255.255.255	UDP	60	52862 → 61510 Len=15						
	1671 13.762917	Universa_46:00:1e	Spanning-tree-(for-bridges	MRP-MVRP	60	Multiple VLAN Registration Protocol						
	1672 13.763362	Universa_46:00:1e	LLDP_Multicast	MRP-MSRP	60	Multiple Stream Reservation Protocol						
	1673 13.763362	Universa_46:00:1e	LLDP_Multicast	PTPv2	64	Sync Message						
	1674 13.764988	Universa_46:00:1e	LLDP_Multicast	PTPv2	90	Follow_Up Message						
	1675 13.777503	52.96.170.82	192.168.1.164	TLSv1.2	689	Application Data						
	1676 13.779058	192.168.1.164	52.96.170.82	TLSv1.2	405	Application Data						
	1677 13.838264	52.96.170.82	192.168.1.164	TLSv1.2	683	Application Data						
	1678 13.839735	192.168.1.164	52.96.170.82	TLSv1.2	412	Application Data						
	1679 13.886432	Universa_46:00:1e	LLDP_Multicast	PTPv2	64	Sync Message						

> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{46B0279D-1FCA-4201-83A9-6F6257D57C07}, id 0 > Ethernet II, Src: Universa_46:00:1e (00:1f:b8:46:00:1e), Dst: LLDP_Multicast (01:80:c2:00:00:0e)

> Precision Time Protocol (IEEE1588)

```
        0000
        01
        80
        c2
        00
        00
        0e
        00
        16
        b8
        46
        00
        1e
        88
        f7
        10
        02

        0010
        00
        2c
        00
        00
        02
        08
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
        00
```

6. After capturing network traffic for 4-5 minutes, use **Capture** drop-down menu to select **Stop** (as shown below)

	Capturing from Ethernet										
Fi	le Edit	View Go	Cap	oture Analyze Sta	tistics Telep	oho ny	Wireless Tools Help				
	(🔳 🙋	0	۲	Options	Ctrl+K		0.0.0				
	Apply a	display filter <		Start	Ctrl+E	H					
No		Time		Stop	Ctrl+E	Destin	ation	Protocol	Length		Info
	16061	132.35829	2	Restart	Ctrl+R	LLDP	Multicast	PTPv2		64	Sync Message
	16062	132.35996		Capture Filters		LLDP	Multicast	PTPv2		90	Follow_Up Message
	16063	132.37185				Spann	ning-tree-(for-bridges	MRP-MVRP		60	Multiple VLAN Registration Protocol
	16064	132.37230		Kefresh Interfaces	FD	LLDP.	Multicast	MRP-MSRP		60	Multiple Stream Reservation Protocc
	16065	132.38035	_	192 168 1 69		2:9.2	255.255.250	SSDP		260	NOTIFY * HTTP/1.1
	16066	132.380923		192.168.1.69		239.2	255.255.250	SSDP		266	NOTIFY * HTTP/1.1
	16067	132.380923		192.168.1.69		239.2	255.255.250	SSDP		319	NOTIFY * HTTP/1.1
	16068	132.380923		192.168.1.69		239.2	255.255.250	SSDP		260	NOTIFY * HTTP/1.1
	16069	132.380923		192.168.1.69		239.2	255.255.250	SSDP		266	NOTIFY * HTTP/1.1
	16070	132.380923		192.168.1.69		239.2	255.255.250	SSDP		319	NOTIFY * HTTP/1.1
	16071	132.380923		192.168.1.69		239.2	255.255.250	SSDP		260	NOTIFY * HTTP/1.1
	16072	132.380923		192.168.1.69		239.2	255.255.250	SSDP		266	NOTIFY * HTTP/1.1
	16073	132.381449		192.168.1.69		239.2	255.255.250	SSDP		319	NOTIFY * HTTP/1.1
	16074	132.396134		Universa 42:00:5	a	IEEE:	1722 01:00:00	IEEE1722-1		82	AVDECC Discovery Protocol

> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{46B0279D-1FCA-4201-83A9-6F6257D57C07}, id 0

> Ethernet II, Src: Universa_46:00:1e (00:1f:b8:46:00:1e), Dst: LLDP_Multicast (01:80:c2:00:00:0e)

> Precision Time Protocol (IEEE1588)

7. Select File and then Save As...

Set an appropriate name for the network capture file.

🚄 *Ether	net											
<u>F</u> ile <u>E</u> d	t <u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	Statistic	: Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp						
<u>О</u> ре	n		(Ctrl+O	E 👔	🕹 🚍 📃 Q. Q. Q. 🎹						
Оре	n <u>R</u> ecent				•							
<u>M</u> er	ge					Destination						
<u>I</u> mp	ort from H	lex Du	mp		е	Spanning-tree-(for-bridges						
<u>C</u> los	e		(Ctrl+W	е	LLDP_Multicast						
						235.0.1.10						
<u>S</u> ave	1		(Ctrl+S	e	LLDP_Multicast						
Save	Δς		(Ctrl+Shift+S	s e	LLDP_Multicast						
	<u></u>				þ	Spanning-tree-(for-bridges…						
File	Set				► P	LLDP_Multicast						
						235.0.1.10						
Expo	ort Specifi	ed Pac	kets		e	LLDP_Multicast						
Exp	ort Packet	Dissec	tions		▶ ^e	LLDP_Multicast						
	Event Deskt Dates Chi					LLDP_Multicast						
Exp	оп Раскет	Bytes.		tri+Shitt+	* e	LLDP_Multicast						
Expo	ort PDUs to	o File			e	LLDP_Multicast						
Expo	ort TLS Ses	sion K	eys		P	Spanning-tree-(for-bridges						



When saving the file, save as file type .pcap -



8. Reach out to URC Technical Support to submit this log for evaluation.