HYPACK
a xylem brand

Sounding Better!

Finding an Unknown IP Address

By Cristhian Bemudez

During some integrations, I have seen a couple of problems some users usually have. When you are trying to connect some network devices and you use certain protocols, such as TCP and Modbus, you need to configure your PC in the same subnet in order to make both devices in the network visible; however, what happens when you do not know the IP address of the device you are going to integrate with HYPACK®? In some cases, you can use the device software to check or change the address, but it is not always possible.

Recently, I was helping a user configure an OPC server that uses the information that came from a PLC (programmable logic controller). The PLC was configured around 15 years ago and they did not have the software to verify the configuration, so I had to look for a way to find the IP address.

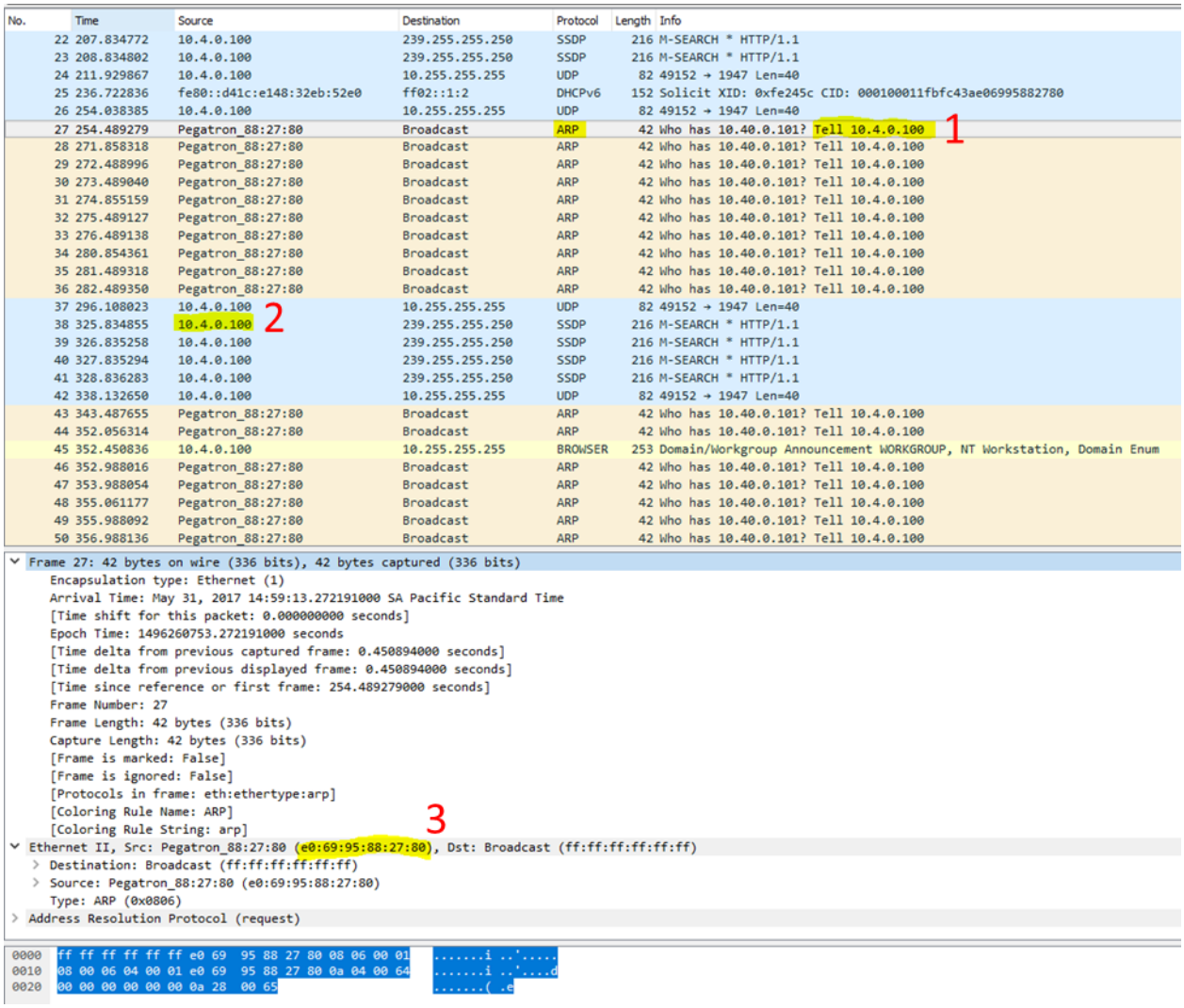
When you connect the network cable, most of the devices exchange messages to determine who is connected to the physical medium; thus, we can use Wireshark to analyze the packets exchanged.

In this example, I tested two devices that had a static IP address configured, one of those is the PLC that I mentioned before.

In the following screenshot, it is possible to see several messages that help us to determine the IP address of the PLC:

1. The PLC sent an ARP protocol message where you can see the IP address. This protocol uses the physical addresses (MAC) to map them with the IP addresses.
2. Some devices also send specific messages where you can see the source IP we are looking for.
3. Every network interface has a MAC address; this is a 6-digit, hexadecimal number that is usually printed on a label. This can help to determine which device sent the package.

FIGURE 1. Capture of the PLC Device.



In the following example, once I connected the cable, the messages my computer received are very clear. In my computer, I did not configure any IP address, but once the cable is plugged in, both devices started to exchange messages.

The IP address we were looking for was 192.168.15.20 and it was possible to see it because the device sent several multicast and broadcast packets.

Not all the devices send this kind of message; I have tested a couple that might not have all implemented protocols to meet the neighbors in the network.

FIGURE 2. *No IP Configured in the PC.*

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0
2	0.004182	fe80::496e:9a9:2214…	ff02::1:2	DHCPv6	157	Solicit XID: 0xf53c40 CID: 0001
3	0.020472	Panasoni_e3:39:0e	LLDP_Multicast	LLDP	58	NoS = 70:58:12:e3:39:0e TTL = 3
4	0.267790	Panasoni_e3:39:0e	Broadcast	ARP	42	Who has 169.254.48.248? Tell 0.0
5	0.267920	::	ff02::1:ff14:30f8	ICMPv6	78	Neighbor Solicitation for fe80:
6	0.267989	fe80::496e:9a9:2214…	ff02::2	ICMPv6	62	Router Solicitation
7	0.268069	fe80::496e:9a9:2214…	ff02::16	ICMPv6	90	Multicast Listener Report Messag
8	0.764523	fe80::496e:9a9:2214…	ff02::16	ICMPv6	90	Multicast Listener Report Messag
9	0.953818	192.168.15.20	224.0.0.251	MDNS	512	Standard query response 0x001f P
10	0.954254	192.168.15.20	224.0.0.113	ALLJOY…	78	VERSION 0 WHOHAS
11	0.954256	192.168.15.20	192.168.15.255	ALLJOY…	78	VERSION 0 WHOHAS
12	0.954258	192.168.15.20	224.0.0.113	ALLJOY…	78	VERSION 1 WHOHAS
13	0.954258	192.168.15.20	192.168.15.255	ALLJOY…	78	VERSION 1 WHOHAS
14	0.954913	192.168.15.20	224.0.0.251	MDNS	288	Standard query 0x0021 PTR _alljo
15	0.966242	192.168.15.20	224.0.0.22	IGMPv3	62	Membership Report / Join group 2
16	1.005609	fe80::496e:9a9:2214…	ff02::1:2	DHCPv6	157	Solicit XID: 0xf53c40 CID: 0001
17	1.026515	Panasoni_e3:39:0e	LLDP_Multicast	LLDP	58	NoS = 70:58:12:e3:39:0e TTL = 3
18	1.054241	192.168.15.20	224.0.0.251	MDNS	512	Standard query response 0x001f P
19	1.054504	192.168.15.20	224.0.0.251	MDNS	288	Standard query 0x0021 PTR _alljo
20	1.081668	192.168.15.20	192.168.15.255	SSDP	309	NOTIFY * HTTP/1.1
21	1.081992	192.168.15.20	192.168.15.255	SSDP	318	NOTIFY * HTTP/1.1
22	1.081993	192.168.15.20	192.168.15.255	SSDP	365	NOTIFY * HTTP/1.1
23	1.081994	192.168.15.20	192.168.15.255	SSDP	363	NOTIFY * HTTP/1.1
24	1.082170	192.168.15.20	192.168.15.255	SSDP	375	NOTIFY * HTTP/1.1
25	1.082255	192.168.15.20	192.168.15.255	SSDP	373	NOTIFY * HTTP/1.1
26	1.082334	192.168.15.20	192.168.15.255	SSDP	309	NOTIFY * HTTP/1.1
27	1.082417	192.168.15.20	192.168.15.255	SSDP	318	NOTIFY * HTTP/1.1
28	1.082518	192.168.15.20	192.168.15.255	SSDP	365	NOTIFY * HTTP/1.1
29	1.082613	192.168.15.20	192.168.15.255	SSDP	363	NOTIFY * HTTP/1.1
30	1.082721	192.168.15.20	192.168.15.255	SSDP	375	NOTIFY * HTTP/1.1
31	1.082809	192.168.15.20	192.168.15.255	SSDP	373	NOTIFY * HTTP/1.1
32	1.096329	192.168.15.20	224.0.0.22	IGMPv3	70	Membership Report / Join group 2
33	1.101419	192.168.15.20	192.168.15.255	SSDP	375	NOTIFY * HTTP/1.1
34	1.152458	192.168.15.20	192.168.15.255	SSDP	384	NOTIFY * HTTP/1.1
35	1.155208	192.168.15.20	224.0.0.251	MDNS	512	Standard query response 0x001f P
36	1.155477	192.168.15.20	224.0.0.251	MDNS	288	Standard query 0x0021 PTR _alljo
37	1.193052	192.168.15.20	224.0.0.113	ALLJOY…	161	VERSION 0 ISAT
38	1.193063	192.168.15.20	192.168.15.255	ALLJOY…	161	VERSION 0 ISAT
39	1.193954	192.168.15.20	224.0.0.113	ALLJOY…	187	VERSION 1 ISAT

```
> Frame 11: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: LgElectr_08:19:5c (3c:cd:93:08:19:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.15.20, Dst: 192.168.15.255
> User Datagram Protocol, Src Port: 9956, Dst Port: 9956
```

```
0000  ff ff ff ff ff ff 3c cd  93 08 19 5c 08 00 45 00   ......<. ...\..E.
0010  00 40 03 b4 40 00 40 11  96 95 c0 a8 0f 14 c0 a8   .@..@.@. ........
0020  0f ff 26 e4 26 e4 00 2c  c5 29 00 01 00 78 8d 02   ..&.&.., .)...x..
0030  0c 3a 31 47 5a 73 34 68  76 6f 2e 32 2a 10 6f 72   .:1GZs4h vo.2*.or
0040  67 2e 61 6c 6c 6a 6f 79  6e 2e 73 6c 2e 2a         g.alljoy n.sl.*
```