

# Tema 1

---

## Cerinte

Vi se da o captura de pachete **network.pcap** care poate fi deschisa folosind

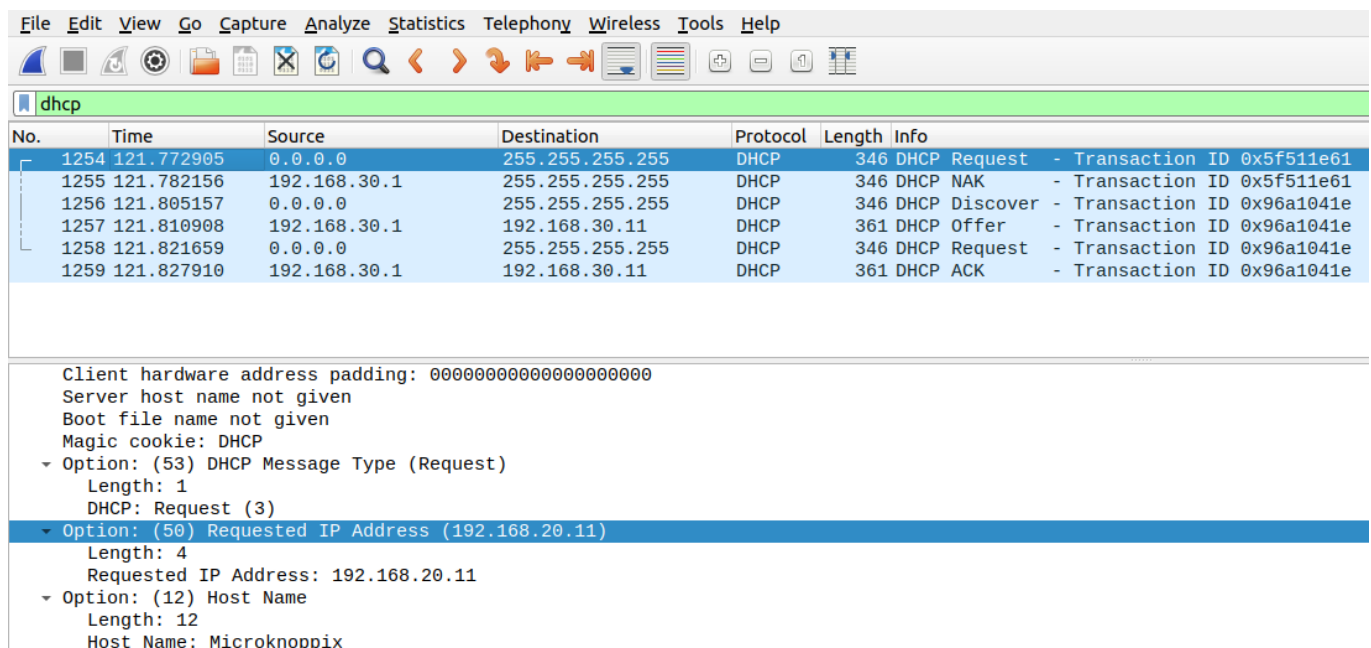
*Wireshark* (analizator de protocoale de retea). Aveți următoarele cerințe:

1. Care este adresa de IP ceruta de clientul DHCP?
2. Care este adrea de IPv6 a serverului de NTP?
3. Care este numele serverului autoritar (authoritative name server) pentru domeniul cautat?
4. Care este portul pentru protocolul CDP al host-ului CCNP-LAB-S2?
5. Ce versiune de IOS ruleaza pe host-ul CCNP-LAB-S2?
6. Cand a fost config-ul de NVRAM actualizat ultima data?

## Rezolvare 1.

R: 192.168.20.11

Filtram dupa DHCP



dhcph

No.	Time	Source	Destination	Protocol	Length	Info
1254	121.772905	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x5f511e61
1255	121.782156	192.168.30.1	255.255.255.255	DHCP	346	DHCP NAK - Transaction ID 0x5f511e61
1256	121.805157	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x96a1041e
1257	121.810908	192.168.30.1	192.168.30.11	DHCP	361	DHCP Offer - Transaction ID 0x96a1041e
1258	121.821659	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x96a1041e
1259	121.827910	192.168.30.1	192.168.30.11	DHCP	361	DHCP ACK - Transaction ID 0x96a1041e

Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
Option: (53) DHCP Message Type (Request)  
Length: 1  
DHCP: Request (3)  
Option: (50) Requested IP Address (192.168.20.11)  
Length: 4  
Requested IP Address: 192.168.20.11  
Option: (12) Host Name  
Length: 12  
Host Name: Microknoppix

Clientul a solicitat IP-ul 192.168.20.11 (Request 1254), fiind refuzat (NAK 1255).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
dhcp							
No.	Time	Source	Destination	Protocol	Length	Info	
1254	121.772905	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request	- Transaction ID 0x5f511e61
1255	121.782156	192.168.30.1	255.255.255.255	DHCP	346	DHCP NAK	- Transaction ID 0x5f511e61
1256	121.805157	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover	- Transaction ID 0x96a1041e
1257	121.810908	192.168.30.1	192.168.30.11	DHCP	361	DHCP Offer	- Transaction ID 0x96a1041e
1258	121.821659	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request	- Transaction ID 0x96a1041e
1259	121.827910	192.168.30.1	192.168.30.11	DHCP	361	DHCP ACK	- Transaction ID 0x96a1041e

Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
Length: 1
DHCP: Request (3)
Option: (54) DHCP Server Identifier (192.168.30.1)
Length: 4
DHCP Server Identifier: 192.168.30.1
Option: (50) Requested IP Address (192.168.30.11)
Length: 4
Requested IP Address: 192.168.30.11
Option: (12) Host Name
Length: 12
Host Name: Microknoppix

Clientul a trimis un mesaj de discover (Discover 1256), serverul i-a oferit IP-ul 192.168.30.1 (Offer 1257), clientul a solicitat IP-ul oferit (Request 1258), iar serverul a confirmat (ACK 1259).

## Rezolvare 2.

R: 2003:51:6012:110::dcf7:123

Filtram traficul NTP prin IPv6

No.	Time	Source	Destination	Protocol	Length	Info
2918	286.367467	2003:51:6012:121::10	2003:51:6012:110::dcf7:123	NTP	114	NTP Version 4, client
2919	286.368969	2003:51:6012:110::dcf7:123	2003:51:6012:121::10	NTP	114	NTP Version 4, server

<p>Frame 2919: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface unknown, id 0</p> <ul style="list-style-type: none"> <li>Ethernet II, Src: Cisco_9e:11:41 (00:14:09:9e:11:41), Dst: Cisco_ae:51:c1 (00:21:1b:ae:51:c1)</li> <li>802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 121</li> <li>Internet Protocol Version 6, Src: 2003:51:6012:110::dcf7:123, Dst: 2003:51:6012:121::10 <ul style="list-style-type: none"> <li>0110 .... = Version: 6</li> <li>.... 1011 1000 .... = Traffic Class: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)</li> <li>..... 1111 0100 1101 1010 1110 = Flow Label: 0xf4dae</li> </ul> </li> <li>Payload Length: 96</li> <li>Next Header: UDP (17)</li> <li>Hop Limit: 62</li> </ul> <p>Source: 2003:51:6012:110::dcf7:123</p> <p>Destination: 2003:51:6012:121::10</p> <ul style="list-style-type: none"> <li>User Datagram Protocol, Src Port: 123, Dst Port: 123</li> <li>Network Time Protocol (NTP Version 4, server)</li> </ul>	<pre> 0000  00 21 1b ae 31 c1 00 14 69 9e 11 41 81 00 00 79  !.1...i.A...y 0010  86 dd 6b 8f 4d ae 00 38 11 3e 20 03 00 51 60 12  .k.M..8-&gt;A..Q. 0020  01 10 00 00 00 00 dc f7 01 23 20 03 00 51 60 12  .....#..0.. 0030  01 21 00 00 00 00 00 00 00 10 00 7b 00 7b 00 38  .!.....{..8 0040  cf f0 24 01 0a ed 00 00 00 00 00 01 34 44 43    .\$......4DC 0050  46 61 dc 64 49 02 e1 7b 63 3e dc 64 4a 35 42 9e  Fa d!..c&gt; dJ5B 0060  5d 00 dc 64 4a 35 42 7d 52 08 dc 64 4a 35 42 93  j- dJ5B} R- dJ5B 0070  3c e1   &lt;. </pre>
--	--

Source IPv6 Address (ipv6.src), 16 bytes

Packets: 3893 - Displayed: 2 (0.1%)

Profile: Default

Putem observa din a doua interactiune client - server faptul ca adresa IPv6 a serverului este `2003:51:6012:110::dcf7:123`, transferul avand flag "NTP Version 4, server".

## Rezolvare 3.

R: `ns1.hans.hosteurope.de`

Filtram dupa DNS Response

No.	Time	Source	Destination	Protocol	Length	Info
3037	322.494205	2003:51:6012:120::a00:53	2003:51:6012:121::2	DNS	152	Standard query response 0x2aa5 A blog.webernetz.net A 5.35.226.136 NS ns1.hans.hosteurope.de NS ns2.hans.hos
243	21.050522	192.168.120.22	192.168.121.2	DNS	152	Standard query response 0xb4ca A blog.webernetz.net A 5.35.226.136 NS ns2.hans.hosteurope.de NS ns1.hans.hos
3507	321.054857	192.168.120.22	192.168.121.2	DNS	152	Standard query response 0xe597 A blog.webernetz.net A 5.35.226.136 NS ns2.hans.hosteurope.de NS ns1.hans.hos

<p>Data length: 4</p> <p>Address: 5.35.226.136</p> <ul style="list-style-type: none"> <li>Authoritative nameservers <ul style="list-style-type: none"> <li>webernetz.net: type NS, class IN, ns ns1.hans.hosteurope.de <ul style="list-style-type: none"> <li>Name: webernetz.net</li> <li>Type: NS (authoritative Name Server) (2)</li> <li>Class: IN (0x0001)</li> <li>Time to live: 184326 (1 day, 4 hours, 58 minutes, 46 seconds)</li> <li>Data length: 24</li> </ul> </li> <li>Name Server: ns1.hans.hosteurope.de</li> <li>webernetz.net: type NS, class IN, ns ns2.hans.hosteurope.de <ul style="list-style-type: none"> <li>Name: webernetz.net</li> <li>Type: NS (authoritative Name Server) (2)</li> <li>Class: IN (0x0001)</li> <li>Time to live: 184326 (1 day, 4 hours, 58 minutes, 46 seconds)</li> <li>Data length: 6</li> <li>Name Server: ns2.hans.hosteurope.de</li> </ul> </li> </ul> </li> </ul>	<pre> 0000  00 1e 7a 79 3f 11 00 14 69 9e 11 41 81 00 00 79  --zy?...i.A...y 0010  08 00 45 00 00 86 d5 5d 00 00 3e 11 34 a0 c0 a8  .E....]--&gt;4... 0020  78 16 c0 a8 79 02 00 35 dc 95 00 72 6e 96 2a a5  x...y..5...rn.* 0030  81 80 00 01 00 01 00 02 00 00 04 02 6c 6f 67 09  .....blog. 0040  77 65 62 65 72 6e 65 74 7a 03 6e 65 74 00 00 01  webernet z-net.. 0050  00 01 c0 0c 00 01 00 01 00 00 46 14 00 04 05 23  .....F...# 0060  e2 88 c0 11 00 02 00 01 00 01 97 86 00 18 83 0e  .....n 0070  73 31 04 08 61 6e 73 0a 68 6f 73 74 65 75 72 6f  s1.hans.hosteuro 0080  70 65 02 64 65 68 c0 11 00 02 00 01 00 01 97 86  pe.de]..... 0090  00 00 03 0e 73 32 c0 44  .....ns2.. </pre>
---	--

Name Server (dns.ns), 24 bytes

Packets: 3893 - Displayed: 4 (0.1%)

Profile: Default

Campul "Authoritative nameservers" contine numele serverelor autoritare:

- webernetz.net: type NS, class IN, ns ns2.hans.hosteurope.de,
- webernetz.net: type NS, class IN, ns ns1.hans.hosteurope.de.

## Rezolvare 4.

R: GigabitEthernet0/2

Filtram dupa CDP

No.	Time	Source	Destination	Protocol	Length	Info
133	11.088970	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
761	71.098782	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
1335	131.112111	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
1921	191.121684	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
2511	251.133254	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
3282	311.149194	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2

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  
Software Version  
Type: Software version (0x0005)  
Length: 276  
Software version: Cisco Internetwork Operating System Software  
Software version: IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)  
Software version: Technical Support: <http://www.cisco.com/techsupport>

Gasim informatiile despre port in campul "Port ID":

- Sent through Interface: **GigabitEthernet0/2.**

## Rezolvare 5.

R: 12.1(22)EA14

Filtram dupa CDP

No.	Time	Source	Destination	Protocol	Length	Info
133	11.088970	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernnetz.net Port ID: GigabitEthernet0/2
761	71.098782	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernnetz.net Port ID: GigabitEthernet0/2
1335	131.112111	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernnetz.net Port ID: GigabitEthernet0/2
1921	191.121684	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernnetz.net Port ID: GigabitEthernet0/2
2511	251.133254	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernnetz.net Port ID: GigabitEthernet0/2
3282	311.149194	Cisco_a1:5a:9a	CDP/VTP/DTP/PagP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernnetz.net Port ID: GigabitEthernet0/2

Port ID: GigabitEthernet0/2 Type: Port ID (0x0003) Length: 22 Sent through Interface: GigabitEthernet0/2 Capabilities Type: Capabilities (0x0004) Length: 8 Capabilities: 0x00000028 Software Version Type: Software version (0x0005) Length: 276 Software version: Cisco Internetwork Operating System Software <b>Software version: IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)</b> Software version: Technical Support: http://www.cisco.com/techsupport Software version: Copyright (c) 1986-2010 by cisco Systems, Inc. Software version: Compiled Tue 26-Oct-10 10:35 by nburra Platform: cisco WS-C2950G-24-EI
--

0090	6d 20 53 6f 66 74 77 61 72 65 20 0a 49 4f 53 20	m Software re dIOS
00a0	28 74 6d 29 20 43 32 39 35 30 20 53 6f 66 74 77	(tm) C29 50 Softw
00b0	61 72 65 20 28 43 32 39 35 30 2d 49 36 4b 32 4c	are (C29 50-I6K2L
00c0	32 51 34 2d 4d 29 2c 20 50 65 72 73 69 6f 6e 26	204-M), Version
00d0	31 32 2e 35 20 32 32 20 45 41 31 84 2c 20 52 45	12.1(22) EA14, RE
00e0	4c 45 41 53 45 20 53 4f 40 54 57 41 52 45 20 28	LEASE SOFTWARE (
00f0	66 63 31 29 0a 54 65 63 68 6e 69 63 61 6c 20 53	fc1).Tec hnical S
0100	75 70 70 6f 72 74 3a 20 68 74 74 70 3a 2f 2f 77	upport: http://w
0110	77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 74 65 63	ww.cisco .com/tec
0120	68 73 75 70 70 6f 72 74 0a 43 6f 70 79 72 69 67	hsupport .Copyrig
0130	68 74 20 28 63 29 20 31 39 38 36 2d 32 30 31 30	ht (c) 1 986-2010
0140	20 62 79 20 63 69 73 63 6f 20 53 79 73 74 65 6d	by cisc o System
0150	73 2c 20 49 6e 63 2e 0a 43 6f 6d 70 69 6c 65 64	s, Inc.. Compiled
0160	20 54 75 65 20 32 36 2d 4f 63 74 2d 31 39 20 31	Tue 26- Oct-10 1
0170	30 3a 33 35 20 62 79 20 6e 62 75 72 72 61 69 66	0:35 by nburra--

Gasim informatiile despre versiunea IOS in campul "Software Version":

- Software version: IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), **Version 12.1(22)EA14**, RELEASE SOFTWARE (fc1).

## Rezolvare 6.

R: 21:02:36 03/03/2017

Filtram packet bytes dupa NVRAM

(nu stiam prin ce protocoale se transmit date despre NVRAM config, asa ca am ales metoda aceasta, banuind ca voi gasi informatia in *packet bytes* - am vazut ca e de forma unui timestamp de [aici](#))

network.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 55

Packet bytes Narrow & Wide Case sensitive String nvrnm Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
3767	327.874041	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 0
3770	327.877414	192.168.110.10	192.168.121.2	TFTP	512	Data Packet, Block: 2
3771	327.877915	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 1
3772	327.879916	192.168.110.10	192.168.121.2	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	192.168.110.10	192.168.121.2	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	192.168.110.10	192.168.121.2	TFTP	562	Data Packet, Block: 4

Frame 3770: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface unknown, id 0

- 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 4, Src: 192.168.121.2, Dst: 192.168.110.10
- User Datagram Protocol, Src Port: 54445, Dst Port: 1556
- Trivial File Transfer Protocol
- Data (512 bytes)
  - Data: 0a210a21204c6173742063666e6096775726174696f6e20...
  - [Length: 512]

0000 00 14 69 9e 11 41 00 1e 7a 79 3f 11 81 00 00 79 . . i . A . . zy? . . . y

0010 08 00 45 00 02 20 00 01 00 00 ff 11 51 6e c0 a8 . E . . . . Qn .

0020 79 02 c0 a8 6e 0a d4 ad 06 14 02 0c 7b dc 00 03 y . n . . . . { . .

0030 00 01 0a 21 0a 21 20 4c 61 73 74 20 63 6f 6e 66 . . . . ! ! L ast conf

0040 69 67 75 72 61 74 69 6f 6e 20 63 68 61 6e 67 65 igratio n change

0050 20 61 74 20 32 30 3a 35 35 3a 34 35 20 55 54 43 at 20:5 5:45 UTC

0060 20 46 72 69 20 4d 61 72 20 33 20 32 30 31 37 20 Fri Mar 3 2017

0070 62 79 20 77 65 62 65 72 6a 6f 68 0a 21 20 4e 56 by weber joh! NV

0080 52 41 4d 20 63 6f 6e 66 69 67 20 6c 61 73 74 20 RAM conf ig last

0090 75 70 64 61 74 65 64 20 61 74 20 32 31 3a 30 32 updated at 21:02

00a0 3a 33 36 20 55 54 43 20 46 72 69 20 4d 61 72 20 :36 UTC Fri Mar

00b0 33 20 32 30 31 37 20 62 79 20 77 65 62 65 72 6a 3 2017 b y weberj

00c0 6f 68 0a 21 20 4e 56 52 41 4d 20 63 6f 6e 66 69 oh! NVR AM confi

00d0 67 20 6c 61 73 74 20 75 70 64 61 74 65 64 20 61 g last u pdated a

00e0 74 20 32 31 3a 30 32 3a 33 36 20 55 54 43 20 46 t 21:02: 36 UTC F

network.pcapng

Packets: 3893 - Displayed: 21 (0.5%)

Profile: Default

Wireshark - Follow UDP Stream (udp.stream eq 55) - network.pcapng

! Last configuration change at 20:55:45 UTC Fri Mar 3 2017 by weberjoh

! NVRAM config last updated at 21:02:36 UTC Fri Mar 3 2017 by weberjoh

! NVRAM config last updated at 21:02:36 UTC Fri Mar 3 2017 by weberjoh

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname CCNP-LAB-R2

!

boot-start-marker

boot-end-marker

!

!

enable secret 5 \$1\$Z.9j\$Nvobsx9NvJzqtRLQqR.9b0

!

11 client pkts, 10 server pkts, 20 turns.

Entire conversation (5.180 bytes)

Show and save data as ASCII Stream 55

Find:

Find Next

Filter Out This Stream Print Save as... Back Close

! NVRAM config last updated at **21:02:36 UTC Fri Mar 3 2017** by weberjoh.