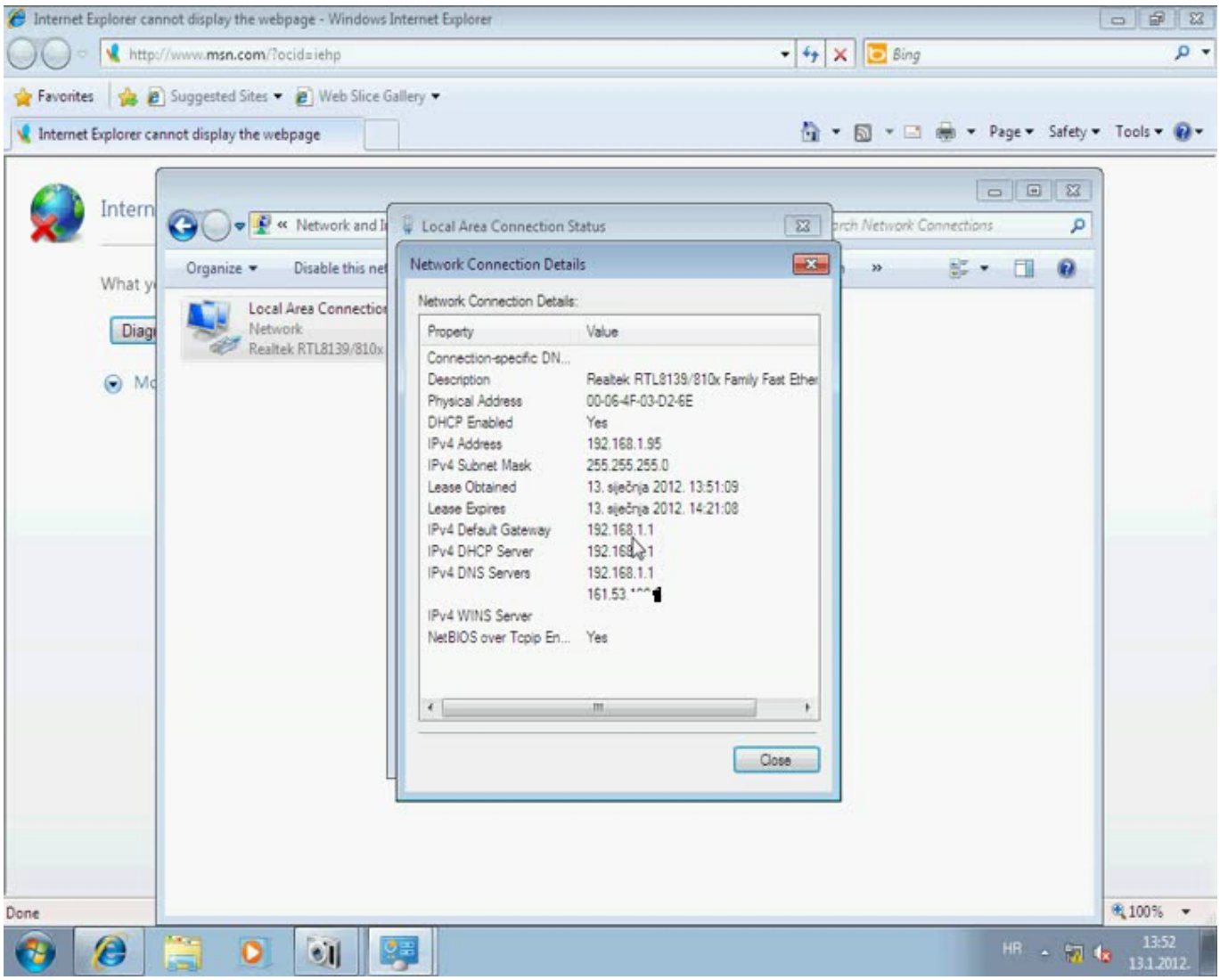
Windowsi 7 gube Internet konekciju

Nedavno sam rješavao zanimljiv problem: Windows 7 računala u lokalnoj mreži povremeno gube vezu prema Internetu, ali ne i prema LAN-u. Na Internetu ćete naći mnoštvo rasprava o toj temi, ali dosad još nitko nije našao zadovoljavajuće rješenje. Način na koji sam riješio problem nisam do sada susreo, niti je dokumentiran. Nastao je na temelju istraživanja slučaja unutar mreže moje ustanove. Vjerujem da se ovaj recept može uspješno primijeniti i drugdje.

Read english abstract **[1].**

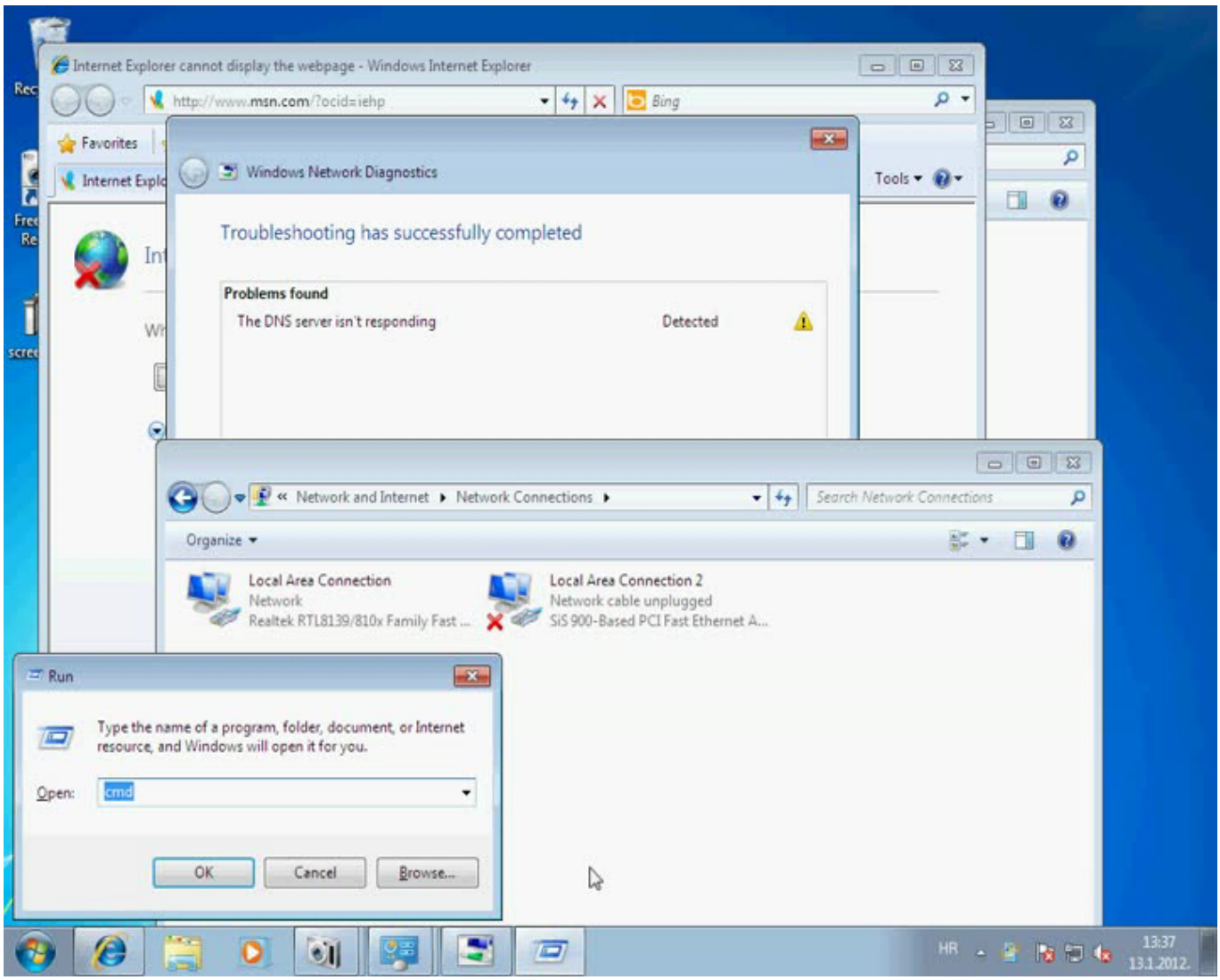
Na internetu se nalazi ogroman broj upita, komentara, primjera uspjelih i neuspjelih rješenja, vezanih za ovaj problem s kojim se, očigledno, susreću mnogi. Potražite ih, na primjer, na adresi answers.microsoft.com [2]

Windows 7 računala na mojoj ustanovi su klijenti Zentyala (Linux servera) koji im je gateway s DHCP i DNS servisom. Od njega svi klijenti dobiju lokalnu adresu, adresu gatewaya i DNS servera. Jedino Win7 klijenti povremeno gube Internet konekciju. Veza se obnavlja u gotovo pravilnim vremenskim intervalima, da bi se u periodima neaktivnosti opet izgubila i tako u nedogled. Na Linux i Windows XP klijentima takvih problema nema.



Ovdje nam ne pomaže mrežni indikator na kontrolnoj traci koji pokazuje status koji uglavnom ne odgovara onome što se tog časa događa sa vezom.

Dijagnostički alat iz "Network and sharing center" okriva problem: "The DNS server is not responding"



Pomoću komadnolinijskog retka sa Run-->cmd provjerimo postavke postavke mrežnog adaptera. Adapter je dobio mrežu adresu, gateway, DNS server, upravo vrijednosti koje treba dobiti DHCP-om. U postavkama se vide i 2 "pseudo" adapatera koji su uključeni u Windows Visti i Windows 7 za tuneliranje ipv6 kroz ipv4 protokol. Taj ćemo dio radi preglednosti ovdje preskočiti.

```
C:\Users\korisnik>ipconfig /all
Windows IP Configuration
Host Name . . . . . . . . . . . . : testni7
Primary Dns Suffix  . . . . . . . :
Node Type . . . . . . . . . . . . : Hybrid
IP Routing Enabled. . . . . . . . : No
 WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
Physical Address. . . . . . . . . : 00-06-4F-03-D2-6E
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.1.95(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : 18. sije?nja 2012. 9:52:05
Lease Expires . . . . . . . . . . : 18. sije?nja 2012. 10:22:05
Default Gateway . . . . . . . . . : 192.168.1.1
```

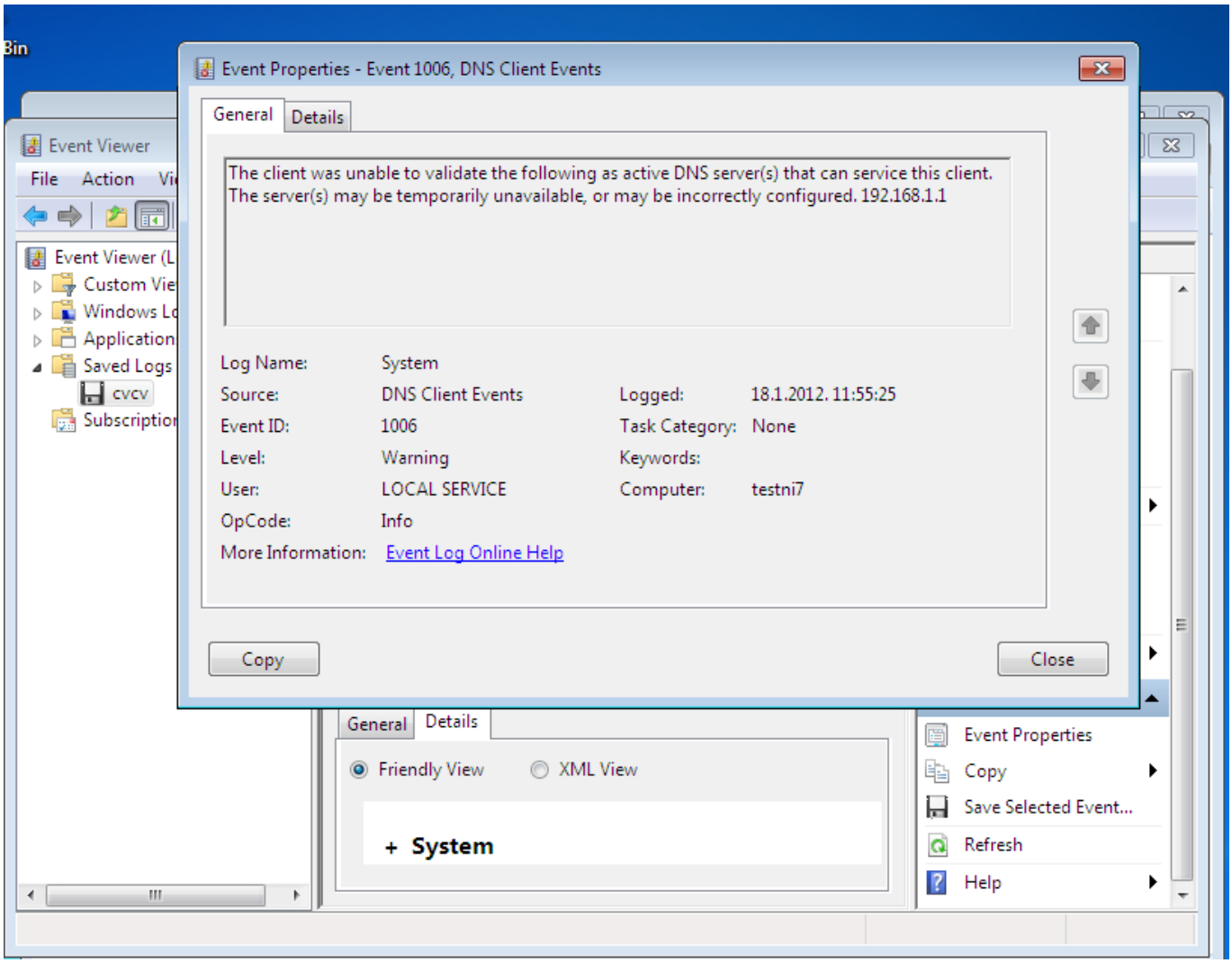
```
DHCP Server . . . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 192.168.1.1
```

Poslije isčitavanja tuđih iskustava na forumima i Microsoftovim "Pitanje-Odgovor" servisima, isprobao sam mnoge metode koje se tamo predlažu kao rješenje. Nabrojat ću samo neke: promjena DNS servera na Google i OpenDNS, pronalaženje i isključivanje pojedinih servisa, "powersave" opcije mrežnog adaptera, flushdns, ipconfig /renew, clean boot, isključivanja NETbios imena, reinstalacije drivera i cijelog OS-a. Zadnja dva nisam isprobao jer sam problem imao na više različitih računala sa različitim hardwareom. Sve je to bilo "tapkanje u mraku " koje je oduzimalo mnogo vremena, ali bez pravog rezultata.

Nakon svih tih "rekla-kazala" rješenja pribjegao sam analizi logova. To je dugotrajan i zamoran posao, jer u biti ne znate što tražite.

Na Windowsima se za to koristi "Event logs", do kojeg se dolazi kroz System and Security->Administrative tools->View event logs.

Pronašao sam zapis relevantan za moj slučaj:.



Kliknemo "details"

```
Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
```

```
  <Provider Name="Microsoft-Windows-DNS-Client" Guid="{1C95126E-7EEA-49A9-A3FE-
A378B03DDB4D}" />
  <EventID>1006</EventID>
  <Version>0</Version>
  <Level>3</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x4000000000000000</Keywords>
  <TimeCreated SystemTime="2012-01-18T10:55:25.484375000Z" />
  <EventRecordID>2124</EventRecordID>
  <Correlation />
  <Execution ProcessID="1028" ThreadID="1804" />
  <Channel>System</Channel>
  <Computer>testni7</Computer>
  <Security UserID="S-1-5-19" />
  </System>
- <EventData>
  <Data Name="AddressLength">16</Data>
  <Data Name="Address">02000000C0A80101000000000000000</Data>
  </EventData>
  </Event>
```

Jasno nam je samo da nam i dalje ništa nije jasno. Radi čega ne radi DNS servis koji je prijavljen na pravoj IP adresi? Pogotovo što svi ostali klijenti, osim Windowsa 7, s njim uredno komuniciraju?

Na Windows 7 klijentu istraživao sam dalje koristeći komandnolinijske probe *nslookup*, *ping* i *tracert*, koje su ponekad bile uspješne, ponekad nisu, ovisno o statusu veze.

```
C:\Users\korisnik>nslookup www.google.hr
DNS request timed out.
 timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.1

DNS request timed out.
 timeout was 2 seconds.

C:\Users\korisnik>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.

C:\Users\korisnik>tracert www.google.hr

Tracing route to www-cctld.l.google.com [209.85.147.94]
over a maximum of 30 hops:

 1    <1 ms     1 ms    <1 ms  ns.mojlan.com [192.168.1.1]
 2     1 ms    <1 ms     1 ms  161.53.x.x
 3    12 ms    11 ms    14 ms  CN-Srce-01-ES.core.carnet.hr [193.198.x.x]
 [...]
 16    49 ms    48 ms    49 ms  bru01m01-in-f94.1e100.net [209.85.147.94]
```

U gornjem primjeru Windows 7 klijent je između neuspješnog *pinga* i naredbe *tracert* uspio uspostaviti vezu.

Preostaje da se nekako "ulovi" trenutak kad dolazi do prekida i u log zapisuje poruka "DNS server is not responding". Ovog puta idem sa strane Zentyal servera koristeći *tcpdump*. Pratit ćemo sve upite i odgovore između Zentyal servera i Windows 7 klijenta.

Pokrenuo sam "tcpdump" na Zentyalu i analizirao log do trenutka kad veza proradi. Sa strane su moje bilješke.

192.168.1.95 Win7 klijent
192.168.1.1 Zentyal (Linux)server

```
#tcpdump -n -i eth0 | grep 192.168.1.95
10:48:53.687315 IP 192.168.1.1.67 > 192.168.1.95.68: BOOTP/DHCP, Reply, length 300
10:48:53.957659 IP 192.168.1.95 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:48:54.005982 IP 192.168.1.95.59964 > 239.255.255.250.3702: UDP, length 991
10:48:54.166762 IP 192.168.1.95 > 224.0.0.22: igmp v3 report, 1 group record(s)
 Multicast layer 2
10:48:54.214204 IP 192.168.1.95.59964 > 239.255.255.250.3702: UDP, length 991    WS-
Discovery (Web Services Dynamic Discovery)
10:49:00.917227 IP 192.168.1.95.60796 > 224.0.0.252.5355: UDP, length 22
 multicast na port 5355 LLMNR
10:49:01.026301 IP 192.168.1.95.60796 > 224.0.0.252.5355: UDP, length 22
10:49:03.870155 IP 192.168.1.95.59429 > 224.0.0.252.5355: UDP, length 22
10:49:03.979052 IP 192.168.1.95.59429 > 224.0.0.252.5355: UDP, length 22
10:49:13.260541 ARP, Request who-has 192.168.1.1 tell 192.168.1.95, length 46
10:49:21.307160 IP 192.168.1.95.57490 > 224.0.0.252.5355: UDP, length 24
  port 5355 Link-local Multicast Name Resolution
10:49:21.415989 IP 192.168.1.95.57490 > 224.0.0.252.5355: UDP, length 24
10:49:33.669797 ARP, Request who-has 192.168.1.1 tell 192.168.1.95, length 46
10:49:33.684077 IP 192.168.1.95 > 224.0.0.22: igmp v3 report, 1 group record(s)
   Multicast layer 2
10:49:33.684394 IP 192.168.1.95 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:49:33.703219 IP 192.168.1.95.59964 > 239.255.255.250.3702: UDP, length 991     WS-
Discovery (Web Services Dynamic Discovery)
10:49:33.807288 IP 192.168.1.95.59964 > 239.255.255.250.3702: UDP, length 991
10:49:34.165380 IP 192.168.1.95 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:50:04.633777 IP 192.168.1.95.54555 > 224.0.0.252.5355: UDP, length 24
 port 5355 Link-local Multicast Name Resolution
10:50:04.742561 IP 192.168.1.95.54555 > 224.0.0.252.5355: UDP, length 24
10:50:35.960834 IP 192.168.1.95.59311 > 224.0.0.252.5355: UDP, length 24
10:50:36.069659 IP 192.168.1.95.59311 > 224.0.0.252.5355: UDP, length 24
10:50:55.288529 IP 192.168.1.95.62633 > 224.0.0.252.5355: UDP, length 24
10:50:55.397291 IP 192.168.1.95.62633 > 224.0.0.252.5355: UDP, length 24
10:51:14.615775 IP 192.168.1.95.62967 > 224.0.0.252.5355: UDP, length 24
10:51:14.724887 IP 192.168.1.95.62967 > 224.0.0.252.5355: UDP, length 24
10:51:33.943243 IP 192.168.1.95.57613 > 224.0.0.252.5355: UDP, length 24
10:51:34.052112 IP 192.168.1.95.57613 > 224.0.0.252.5355: UDP, length 24
10:54:01.167028 ARP, Request who-has 192.168.1.1 tell 192.168.1.95, length 46
10:54:01.167148 IP 192.168.1.95.63168 > 192.168.1.1.53: 51659+ SRV? _VLMCS._TCP.mojla
n.com. (40)   Napokon DNS odgovara!
10:54:01.167389 IP 192.168.1.1.53 > 192.168.1.95.63168: 51659 NXDomain* 0/1/0 (90)  v
eza radi
10:54:06.164503 ARP, Request who-has 192.168.1.95 tell 192.168.1.1, length 28
10:54:06.164609 ARP, Reply 192.168.1.95 is-at 00:06:4f:03:d2:6e, length 46
10:55:25.650295 ARP, Request who-has 192.168.1.1 tell 192.168.1.95, length 46
10:55:25.650413 IP
192.168.1.95.57164 > 192.168.1.1.53: 60380+ A? www.mozilla.com [3]. (33)
```

Dump pokazuje da "čudni" visoki portovi 54555, 59311, 62633, 62633 sa 192.168.95 šalju multicast 224.0.0.252 na port 5355 .

Upotreba porta 5355 je rezervirana za LLMNR [4] (*Link Local Multicast Name Resolution*) protokol. Počeo se upotrebljavati na Windows Serveru 2008 i Visti. Koristi se za slučaj kada konvencionalni DNS upiti ne daju rezultate. Radi samo na lokalnom linku i ne može biti zamjena za DNS.

Zaključio sam da Windows 7 imaju, za razliku od XP-a, uključen ovaj protokol, te da možda upravo on stvara konfuziju u DNS upitima i odgovorima.

LLMNR na Windows 7 isključimo na slijedeći način:
Run->regedit

Lociramo se u :

HKLM/Software/Policies/Microsoft/WindowsNT/New->Key DNSClient
HKLM/Software/Policies/Microsoft/WindowsNT/DNSClient/

U New->DWORD nazvan "EnableMulticast" upišemo vrijednost 0.

Spremimo i izađemo iz registry editora. Nakon restarta pratimo aktivnosti pri uspostavljanju veze.

Kad ponovo pokrenemo *tcpdump* vidjet ćemo da više nema multicasta na port 5355, ali se veza i dalje ne uspostavlja i komunikacija stoji na upitu:

```
14:09:44.731758 ARP, Request who-has 192.168.1.1 tell 192.168.1.95, length 46
```

Nakon ovog su stvari jasnije: nije kriv LLMNR, iako je on bez Servera 2008 ovdje suvišan i samo stvara nepotreban mrežni promet. Problem je na razini ARP protokola, koji povremeno nije u stanju otkriti MAC adresu uređaja kojem je pridužena IP adresa 192.168.1.1. Radi toga ne može uspostaviti vezu s DNS servisom.

Izlistavamo arp tablicu našeg Windows 7 klijenta.

```
C:\Windows\system32>arp -a

Interface: 192.168.1.95 --- 0xb
Internet Address      Physical Address      Type
192.168.1.1              00:17:31:84:2c:44   dynamic
...
```

Na strani Linux servera pokrećemo *ifconfig* koji izlistava MAC adrese mrežnih adaptera.

```
ifconfig | grep HWaddr
eth0      Link encap:Ethernet  HWaddr 00:06:4f:03:d2:75
eth1      Link encap:Ethernet  HWaddr 00:17:31:84:2c:44
```

Zentyal server ima 2 ethernet adaptera, eth0 s adresom iz lokalne mreže, i eth1 s javnom adresom. Eto rješenja problema: iz nekog razloga, arp na Windows 7 uz IP adresu internog mrežnog sučelja veže MAC adresu javnog sučelja na serveru.

Rješenje je jednostavno: IP adresi 192.168.1.1 dodijelimo statičku MAC adresu ispravnog sučelja.

Run-->cmd

```
C:\Users\korisnik>netsh interface ipv4 add neighbors "Local Area Connection" 192.168.
1.1 00-06-4f-03-d2-75
```

Obratite pažnju na činjenicu da Windowsi neće prihvatiti dvotočku kao separator brojeva u MAC adresi, treba je zamijeniti crticama.

Ovakvo rješenje moglo bi izazvati probleme ako bi Windows 7 klijenta odnijeli izvan mreže ustanove i spojili ga, na primjer, na kućni ADSL router i koji koristi istu IP adresu, 192.168.1.1, ali mu je MAC adresa drugačija. Kod nas to nije problem jer se radi o desktop računalima koja su u sobama zaposlenika i koriste se isključivo na lokaciji ustanove. Za prijenosna računala se uvijek može koristiti bežična mreža preko eduroam infrastrukture koja nema ovakvih problema.

Naravno, očekujemo da se Microsoft izjasni radi čega implementacija ARP protokola na Windowsima 7 stvara probleme i da tu grešku ispravi. Uzgred budi rečeno, greška je tu još od 2008. godine i Viste, a Microsoft je upoznat s njom.

NAPOMENA:Za Windows 7 klijente koji koriste lokalizaciju na hrvatski jezik koristiti oblik naredbe.

```
C:\Users\korisnik>netsh interface ipv4 add neighbors "Lokalna veza" 192.168.1.1 00-06
-4f-03-d2-75
```

U suprotnom pri izvršavanju naredbe dobit ćete poruku "greška u sintaksi".

Ukoliko računalo,laptop odlazi sa vaše mreže postoji mogućnost da statički MAC unos radi problem ukoliko se
koristi ista lokalna IP adresa na drugoj mreži.U tom slučaju bi trebalo pobrisati sve unose slijedećom naredbom.

```
netsh interface ipv4 reset
```

Ukoliko se to seljenje dešava učestalo može se napraviti i skripta koju će korisnik sam moći po potrebi pokrenuti
ako npr. ima problem kod spajanja laptopa na kućni ADSL router koji koristi istu kombinaciju lokalne IP adrese.

uto, 2012-02-07 12:46 - Goran Šljivić**Vijesti:** Windows [5]
Kategorije: Mreža [6]
Vote: 5

Vaša ocjena: Nema Average: 5 (4 votes)

Source URL: https://sysportal.carnet.hr/node/931?page=0

Links
[1] https://sysportal.carnet.hr/node/932
[2] http://answers.microsoft.com/en-us/windows/forum/windows_7-networking/windows-7-loses-

internet-connection-but-not/0014801b-7e82-4bb6-a8e7-e8867eb3fcee
[3] http://www.mozilla.com/
[4] http://www.faqs.org/rfcs/rfc4795.html
[5] https://sysportal.carnet.hr/taxonomy/term/12
[6] https://sysportal.carnet.hr/taxonomy/term/29