

DNS/DHCP Abfragen – Konsole und GUI

Autor: Moser Tobias

Datum: 20.11.2016

Typ: Information

Version: 1.0

INHALT

2	NSLookup.....	3
3	Grafische Tools.....	6
4	Aufgaben.....	7
5	DHCP Test Tools	8

2 NSLookup

Der Befehl **nslookup** kann unter Mac OS X, Windows und Unix verwendet werden, um IP-Adressen oder Domains eines bestimmten Computers mittels DNS herauszufinden. Der Name des Befehls bedeutet „Name Server look up“, was so viel heißt wie „beim Namens-Server nachschauen“. Als modernere Alternative zu nslookup hat sich zunehmend der Befehl dig etabliert, der unter Windows als Cygwin-Port verfügbar ist.

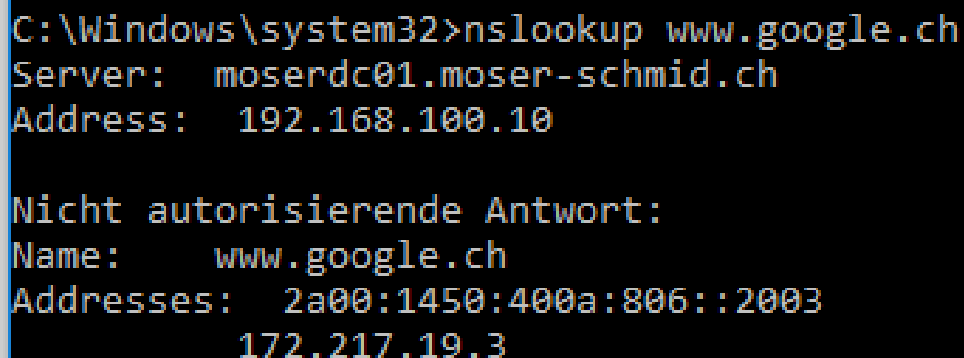
Mit dem Tool nslookup lässt sich der Domainname einer IP-Adresse bzw. die IP-Adresse eines Domainnamens ermitteln. Standardmäßig, im nicht interaktiven Modus, wird dazu der eingestellte DNS-Server zur Auflösung des Namens oder der IP-Adresse verwendet. Wenn ein anderer DNS-Server zur Auflösung verwendet werden soll, z. B. um diesen zu prüfen oder weil der eigene bestimmte Anfragen nicht unterstützt, muss dieser zusätzlich angegeben werden.

nslookup steht auf der Kommandozeile/Konsole als Befehl zur Verfügung.

Beispiel 1

Öffnen Sie auf dem Server eine DOSbox.

Geben Sie *nslookup* www.google.ch ein



```
C:\Windows\system32>nslookup www.google.ch
Server:  moserdc01.moser-schmid.ch
Address:  192.168.100.10

Nicht autorisierende Antwort:
Name:     www.google.ch
Addresses: 2a00:1450:400a:806::2003
          172.217.19.3
```

Als erstes sehen Sie den verwendeten DNS Server mit Name und IP Adresse.

Nach «nicht autorisierende Antwort» bekommen Sie für Ihre Anfrage nach www.google.ch die IP Adressen im Format v4 und v6.

Beispiel 2

Öffnen Sie auf dem Server eine DOSbox.

Geben Sie *nslookup -q=any google.ch* ein

```
C:\Windows\system32>nslookup -q=any google.ch
Server:  moserdc01.moser-schmid.ch
Address:  192.168.100.10

Nicht autorisierende Antwort:
google.ch      internet address = 172.217.18.99
google.ch      nameserver = ns4.google.com
google.ch      nameserver = ns1.google.com
google.ch      nameserver = ns2.google.com
google.ch      nameserver = ns3.google.com
google.ch      AAAA IPv6 address = 2a00:1450:400a:807::2003

ns4.google.com internet address = 216.239.38.10
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
```

Mit der Option *-q=any* weisen Sie den DNS Server an, dass er Ihnen alle Typen (A, NS usw.) zurückgeben soll.

Beispiel 3

Öffnen Sie auf dem Server eine DOSbox.

Geben Sie folgendes ein:

<i>Nslookup <enter></i>	<i>Wechsel in das Programm nslookup</i>
<i>Server 8.8.4.4 <enter></i>	<i>DNS Server auf 8.8.4.4 wechseln</i>
<i>Set type=any</i>	<i>Alle Einträge anzeigen (analog -q)</i>
<i>Google.ch</i>	<i>Angefragte Domain anzeigen</i>

```
C:\Windows\system32>nslookup
Standardserver:  moserdc01.moser-schmid.ch
Address:  192.168.100.10

> server 8.8.4.4
Standardserver:  google-public-dns-b.google.com
Address:  8.8.4.4

> set type=any
> google.ch
Server:  google-public-dns-b.google.com
Address:  8.8.4.4

Nicht autorisierende Antwort:
google.ch      internet address = 172.217.19.163
google.ch      AAAA IPv6 address = 2a00:1450:400a:806::2003
google.ch      text =

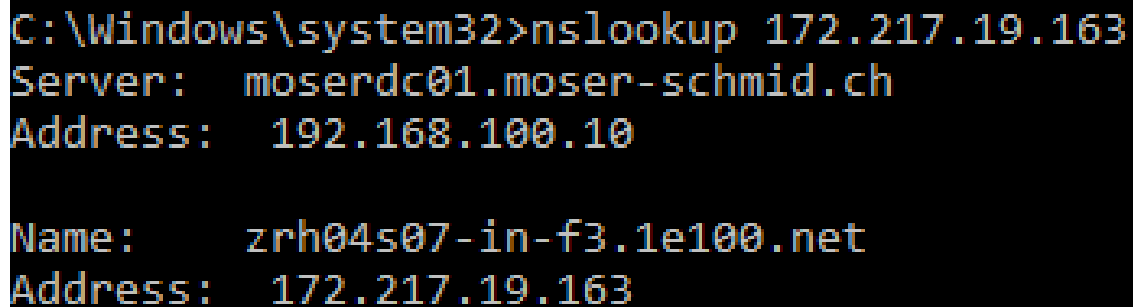
      "v=spf1 -all"
google.ch      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.ch      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.ch      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.ch      nameserver = ns4.google.com
google.ch      nameserver = ns2.google.com
google.ch      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.ch      MX preference = 10, mail exchanger = aspmx.l.google.com
google.ch      nameserver = ns3.google.com
google.ch      primary name server = ns4.google.com
                responsible mail addr = dns-admin.google.com
                serial  = 139721945
                refresh = 900 (15 mins)
                retry   = 900 (15 mins)
                expire  = 1800 (30 mins)
                default TTL = 60 (1 min)
google.ch      nameserver = ns1.google.com
>
```

Beispiel 4

Bis jetzt haben wir immer Namen in IP Adressen aufgelöst. Dieser Prozess nennt sich Forwardlookup Prozess. Die Anfrage kann aber auch in die andere Richtung gemacht werden. Wir fragen nun nach dem Namen der eingegebenen IP Adresse nach. Dieser Prozess wird reverse lookup genannt.

Öffnen Sie auf dem Server eine DOSbox.

Geben Sie *nslookup 172.217.19.163* ein



```
C:\Windows\system32>nslookup 172.217.19.163
Server:  moserdc01.moser-schmid.ch
Address:  192.168.100.10

Name:     zrh04s07-in-f3.1e100.net
Address:  172.217.19.163
```

3 Grafische Tools

Nun schauen Sie sich die folgenden Tools an.

Links:

<http://www.dnsstuff.com/tools>

<https://dnsquery.org/>

Ausprobieren Network Tools:

<\\10.0.22.26\\m123\\sw03\\tools\\>

Dnsdataview von Nirsoft

Und in Ihrem Windows 10 (mit Cisco Paket Tracer und Wireshark) befindet sich ein Tool namens Quest Free Network Tools.

Hier können Sie einmal das Tool whois query und DNS audit anschauen. Bei whois query unbedingt nur die Topleveldomain angeben.

4 Aufgaben

Versuchen Sie die untenstehenden Aufgaben zu lösen. Zeigen Sie zuerst einmal auf, wie sie vorgehen und danach das richtige Resultat.

Wie lautet der Domänenname von 91.198.174.192?

Wie lauten alle DNS Server von google.com?

Wie lauten die Mailserver von 20minuten.ch?

Wie lautet die IP Adresse von www.microsoft.com?

5 DHCP Test Tools

Sie finden auf dem NAS unter Tools zwei Tools, welche mit DHCP..... beginne.

Das erste Tool heisst dhcptest. Hiermit können Sie eine DHCPDiscover Nachricht erstellen und bekommen die ganzen Informationen zu Ihrem DNS.

```
Eingabeaufforderung - dhcptest-0.5-win64.exe
22.01.2016 07:35          962.872 dhcptest-0.5-win64.exe
                2 Datei(en),          1.367.352 Bytes
                2 Verzeichnis(se), 120.465.321.984 Bytes frei

C:\Temp>dhcptest-0.5-win64.exe
dhcptest v0.5 - Written by Vladimir Panteleev
https://github.com/CyberShadow/dhcptest
Run with --help for a list of command-line options.

Listening for DHCP replies on port 68.
Type "d" to broadcast a DHCP discover packet, or "help" for details.
d
Sending packet:
op=BOOTREQUEST chaddr=C7:D9:44:60:26:C5 hops=0 xid=78FB1AF1 secs=0 flags=8000
ciaddr=0.0.0.0 yiaddr=0.0.0.0 siaddr=0.0.0.0 giaddr=0.0.0.0 sname= file=
1 options:
 53 (DHCP Message Type): discover
Received packet from 192.168.178.1:67:
op=BOOTREPLY chaddr=C7:D9:44:60:26:C5 hops=0 xid=78FB1AF1 secs=0 flags=8000
ciaddr=0.0.0.0 yiaddr=192.168.178.200 siaddr=192.168.178.1 giaddr=0.0.0.0 sname= file=
11 options:
 53 (DHCP Message Type): offer
 54 (Server Identifier): 192.168.178.1
 51 (IP Address Lease Time): 864000 (1 week and 3 days)
 58 (Renewal (T1) Time Value): 432000 (5 days)
 59 (Rebinding (T2) Time Value): 756000 (1 week, 1 day, and 18 hours)
 1 (Subnet Mask): 255.255.255.0
 3 (Router Option): 192.168.178.1
 6 (Domain Name Server Option): 192.168.178.1
 15 (Domain Name): fritz.box
 28 (Broadcast Address Option): 192.168.178.255
 42 (Network Time Protocol Servers Option): C0 A8 B2 01
Received packet from 192.168.178.4:67:
op=BOOTREPLY chaddr=C7:D9:44:60:26:C5 hops=0 xid=78FB1AF1 secs=0 flags=8000
ciaddr=0.0.0.0 yiaddr=192.168.178.79 siaddr=192.168.178.4 giaddr=0.0.0.0 sname= file=
11 options:
 53 (DHCP Message Type): offer
 54 (Server Identifier): 192.168.178.4
 51 (IP Address Lease Time): 864000 (1 week and 3 days)
 58 (Renewal (T1) Time Value): 432000 (5 days)
 59 (Rebinding (T2) Time Value): 756000 (1 week, 1 day, and 18 hours)
 1 (Subnet Mask): 255.255.255.0
 3 (Router Option): 192.168.178.4
 6 (Domain Name Server Option): 192.168.178.4
 15 (Domain Name): fritz.box
 28 (Broadcast Address Option): 192.168.178.255
 42 (Network Time Protocol Servers Option): C0 A8 B2 04
Received packet from 192.168.178.1:67:
op=BOOTREPLY chaddr=C8:1E:E7:EB:7A:F7 hops=0 xid=446A035A secs=0 flags=8000
ciaddr=0.0.0.0 yiaddr=0.0.0.0 siaddr=192.168.178.1 giaddr=0.0.0.0 sname= file=
1 options:
 53 (DHCP Message Type): nak
Received packet from 192.168.178.1:67:
op=BOOTREPLY chaddr=C8:1E:E7:EB:7A:F7 hops=0 xid=446A035B secs=0 flags=8000
ciaddr=0.0.0.0 yiaddr=0.0.0.0 siaddr=192.168.178.1 giaddr=0.0.0.0 sname= file=
1 options:
 53 (DHCP Message Type): nak
```



```
C:\Temp>dhcptest-0.5-win64.exe --help
dhcptest v0.5 - Written by Vladimir Panteleev
https://github.com/CyberShadow/dhcptest
Run with --help for a list of command-line options.

Usage: dhcptest-0.5-win64.exe [OPTION]...

Options:
  --bind IP          Listen on the interface with the specified IP.
                     The default is to listen on all interfaces (0.0.0.0).
  --mac MAC          Specify a MAC address to use for the client hardware
                     address field (chaddr), in the format NN:NN:NN:NN:NN:NN
  --quiet            Suppress program output except for received data
                     and error messages
  --query            Instead of starting an interactive prompt, immediately send
                     a discover packet, wait for a result, print it and exit.
  --option N=STR     Add a string option with code N and content STR to the
                     request packet. E.g. to specify a Vendor Class Identifier:
                     --option "60=Initech Groupware"
                     You can specify hexadecimal or IPv4-formatted options using
                     --option "N[hex]=..." or --option "N[IP]=..."
  --request N        Uses DHCP option 55 ("Parameter Request List") to
                     explicitly request the specified option from the server.
                     Can be repeated several times to request multiple options.
  --print-only N     Print only the specified DHCP option.
                     It is assumed to be a text string.
  --timeout N        Wait N seconds for a reply, after which retry or exit.
                     Default is 10 seconds. Can be a fractional number.
  --tries N          Send N DHCP discover packets after each timeout interval.
                     Specify N=0 to retry indefinitely.
```

Wie lautet der DHCP von GIBZ?

```
C:\Temp>dhcpcheck

DHCPCheck
Copyright (c) by KS-Soft
Version 1.03
May, 2009
Web: www.ks-soft.net
EMail: support@ks-soft.net

Purpose: utility checks DHCP service on specified host

Usage: dhcpcheck.exe -host:<host_name> [-clientIP:<IP-address>] [-clientMAC:<MAC-address>] [-timeout:<timeout>] [-interfaceip:<IP-address>]

Parameters:
-host      : DHCP server name or IP address
-clientIP  : IP address to request (within the DHCP range)
-clientMAC : MAC address of the client's machine
             e.g: 00-13-20-70-B8-03 or 00:0c:6e:8c:d4:61
-timeout   : Communication timeout (msec), default: 5000 msec

Note: If "-clientIP:" parameter is not specified, dhcpcheck.exe sends the
DHCPINFORM packet to the server, otherwise it sends DHCPREQUEST packet in
order to request specified IP-address.

Examples:
dhcpcheck -host:localhost
dhcpcheck -host:10.10.1.1 -timeout:6000
dhcpcheck -host:10.10.1.1 -clientIP:10.10.1.55
dhcpcheck -host:10.10.1.1 -clientIP:10.10.1.55 -clientMAC:00-13-20-70-B8-03
dhcpcheck -host:10.10.1.1 -clientIP:10.10.1.55 -clientMAC:00:0c:6e:8c:d4:61 -timeout:8000

ScriptRes:Unknown:DHCP Server name or IP is required

C:\Temp>
```

Grafisches Tool mit DHCP Explorer.

