# NetBIOS - informacje

**Położenie: c:\Windows\system32\drivers\etc\hosts, c:\Windows\system32\drivers\etc\lmhosts, c:\Windows\system32\DNS**



## Domeny a nazwy NetBIOS

System Windows rozwiązuje nazwy komputerów na ich numery IP w dwojaki sposób. Pierwszy z nich to obsługiwany centralnie statyczny serwer *DNS* (lub jego lokalna ograniczona wersja *Hosts*), który obsługuje nazwy zwane **domenami** (np. *raven.imagine*). Drugi to centralny dynamiczny *WINS* (lub jego statyczna ograniczona wersja *LmHosts*), który obsługuje nazwy zwane **NetBIOS** (np. *raven*) rozpoznawane tylko w ramach LAN.

## Serwer WINS

Gdy użytkownik używa *DHCP*, to *WINS* jest wręcz niezbędne. Serwer *WINS* działa na następującej zasadzie: klient w czasie startu przekazuje swoją nazwę *NetBIOS* oraz swój IP na serwer *WINS* (czyli unika rozgłaszania). Inni klienci korzystają z tej bazy danych.

## LmHosts

Teoretycznie, również plik *LmHosts* może być przechowywany centralnie na serwerze, a jego zawartość pobierana w czasie startu każdego klienta. Jak to zrobić? Oto niezbędne wpisy w pliku *c:\Windows\system32\drivers\etc\lmhosts*:

```
192.168.0.1     server              #PRE      #DOM:3bird
192.168.0.1     "3bird     /0x1b"   #PRE
#BEGIN_INCLUDE
#INCLUDE        \\server\netlogon\lmhosts_zdalny.txt
#END_INCLUDE
```

Komentarz: Pierwsza linia musi być zamieszczona, aby system wiedział, gdzie szukać wpisu ze sekcji *#INCLUDE* (nie działa podanie numeru IP zamiast nazwy *NetBIOS* serwera). Parametr *#PRE* wczytuje wpis do pamięci *cache*. Druga linia zawiera nazwę przeglądarki domeny, czyli PDC (wszystkich znaków w cudzysłowie ma być dokładnie 20, czyli nazwa domeny może mieć maksymalnie 15 znaków, a symbol **/** ma być dokładnie 16 znakiem). Aby wczytywany był plik ze serwera, w rejestrze *Windows* musi istnieć zapis:
*\HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares* ---> dodać: ***netlogon***
Ilość ładowanych do pamięci wpisów określa klucz:
*\HKLM\System\CurrentControlSet\Services\NetBT\Parameters\MaxPreload*
Na końcu pliku *LmHosts* należy dodać 4 wiersze odstępu, a sam plik musi mieć prawo odczytu przez wszystkich i nie może być zapisany w *Unicode*. Umieszczane tam nazwy hostów i domen muszą mieć nie więcej niż 15 znaków (dłuższe są skracane).

Niestety, wczytywanie pliku *LmHosts* ze serwera **nie działa** w praktyce (przynajmniej nie w *Windows XP HE*). Można łatwo się o tym przekonać wydając na koncie administratora polecenie:
**nbtstat -c** (wypisuje cache'owaną tablicę z *LmHosts*)
Plik ten można za to wczytać "ręcznie" wydając polecenie:
**nbtstat -R**
Wydaje się, że przyczyna może tkwić w tym, że przy starcie, system próbuje odczytać zdalny plik *LmHosts* zanim uruchomiony na dobre zostanie interfejs sieciowy i zanim nawiązana zostanie łączność ze serwerem. Rozwiązaniem nie jest jednak utworzenie skryptu, który wydawałby polecenie **nbtstat -R** z pewnym opóźnieniem (i umieszczenie go w *\HKLM...\Run*), gdyż polecenie to może być zrealizowane tylko na koncie administratora (tylko on ma prawo do wydawania tego polecenia), gdy użytkownik zaloguje się na konto z ograniczeniami, polecenie **nbtstat -R** umieszczone w skrypcie, nie zostanie wykonane.

## Kolejność rozwiązywania nazw

Twórcy *Windows* twierdzą, że kolejność przeszukiwania serwisów w celu rozwiązania nazw na numer IP, jest następująca:

| ***NetBIOS*** | ***Host Name Resolution*** |
|---|---|
| 1. *Name cache.* | 1. *Local cache.* |
| 2. *WINS.* | 2. *Hosts.* |
| 3. *Broadcast.* | 3. *DNS.* |
| 4. *LmHosts.* | 4. *WINS.* |
| 5. *Hosts.* | 5. *Broadcast.* |
| 6. *DNS.* | 6. *LmHosts.* |

Tyle teoria. Praktyka jednak zdaje się być inna i to często niezależnie od wybranych/używanych usług. W szczególności, w drugim przypadku zdaje się nie działać *Local cache* oraz *Broadcast*, a jeśli komputer nie jest podłączony do sieci, to próba odpytania *DNS* (i braku odpowiedzi) przedłuża całą procedurę do 15 sekund (zanim dojdzie do *LmHosts* czy do *cachowanego LmHosts*). Wydaje się, że użytkownik nie może w żaden sposób zmienić tej kolejności.

## Blokowanie stron www

Jakie pierwszy parametr musi koniecznie być numer IP (nie są akceptowane nazwy domen). Po wpisaniu nazwy domeny, przeglądarka zostanie przekierowana na podany numer IP:
127.0.0.1 www.strona.pl
127.0.0.1 www.inna.strona.pl
Aby zablokować zmianę zawartości pliku przez innych użytkowników systemu, wydajemy polecenie:
C:\> **cacls** *C:\windows\system32\drivers\etc***hosts** /E /G Wszyscy:N
C:\> **cacls** *C:\windows\system32\drivers\etc***hosts** /E /G root:F

## Narzędzia diagnostyczne

**arp -a** – wykaz IP i MAC w sieci lokalnej
**arp -d** - czyszczenie tablicy zebranych adresów MAC
**hostname** – podaje nazwę *NetBIOS* naszej maszyny
**ipconfig** – ip, maska i brama naszej maszyny
**ipconfig /displaydns** - wykaz ostatnio używanych adresów DNS przetrzymywanych w pamięci *cache*
**ipconfig /flushdns** - czyści cache z adresów DNS
**nbstart** – wykaz *NetBIOS over TCP/IP*
**netstat** – statystyki TCP/IP
**netstat -r** - tablica routingu
**nslookup** - podaje numer IP na podstawie wpisanej domeny
**ping** – wysyłanie pakietów *echo*
**ping 192.168.0.255** – wykaz IP w sieci lokalnej (pingowanie na *broadcast*)
**route** – wykaz tras naszych pakietów
**tracert** – dokładny wykaz trasy do wybranej maszyny

## NetBIOS na Linuksie

Na serwerze *Samba* w systemie *Linux* odpowiada za kolejność przeszukiwań następujący wpis:
*name resolve order = hosts wins lmhosts bcast*
przy czym tutaj wyrażenie "*hosts*" może oznaczać plik */etc/hosts*, *DNS* lub *NIS* (zależy to od ustawień w plikach */etc/host.conf*, */etc/nsswitch.conf*, */etc/resolv.conf*).
Aby linuksowa Samba stała się serwerem *WINS* należy umieścić wpis:
*wins support = yes*
Aby sprawdzić tablicę cache'owanych nazw *LmHosts* (Linux także może być klientem *LmHosts*) należy wydać polecenie:

# **nmblookup**

*Ostatnia aktualizacja: 2 maja 2021.*