haneWIN DNS Server
Version 2.0

Copyright 2002-2019, Herbert Hanewinkel, Neuried

Updated: Feb 2019

Overview

The software implements a DNS Server for all Windows NT platforms.
The server can run as Primary or Backup DNS server and supports dynamic DNS updates based on RFC 2136.
The server operates as a so called "**recursive DNS forwarder**" with caching. Requests for non local domains are answered from the cache or forwarded to external nameservers.
Name resolution for hosts or complete domains can be blocked by the server with entries in a block list. (e.g. to suppress ads or tracking)
For external forwarding the server supports **DNS over TLS** (RFC 7858) and DNS Transport over TCP (RFC7766) with translation of client requests and replies between UDP and TCP. TLS uses the Microsoft TLS implementation and is available on Windows 7 and higher versions.

As an optional additional feature the service could be used to remove or set the default gateway of the computer by a non-privileged user. Removing the default gateway is an easy way to disconnect from the internet without disconnecting your computer from your LAN/WLAN.

The DNS Server is implemented as service for Windows 200x/XP/VISTA/7/8/10. A Control Panel Applet provides interactive access to the service.
The DNS Server is also available as portable Windows application.

The software is implemented as 32- and 64 Bit versions.

Installation

Requirements

Windows 200x/XP/VISTA/7/8/10 configured for TCP/IP.

Installation of the DNS Server service

1. Install the software by running the setup.
2. Enable the DNS server in firewall for incoming requests. An example is given in file firewall.bat.

Setup of DNS Server portable application

1. Extract the dns folder from zip archive, start the application. .
2. Enable the DNS server in firewall for incoming requests. An example is given in file firewall.bat.

If a **hosts** file exists on the compuer it is loaded as a starting point for a DNS configuration. Local domain and computer name are extracted from the Windows settings. You need administrator privileges to setup a configuration. Use the **Add Entry** menu entry to add further names to the database. For automated update of entries of the service a command line tool **DNSCMD.EXE** is provided.

Users Guide

The Info Box at startup is displayed only for the unregistered version.

Running the DNS server as a Service

The server is installed as a service for Windows 200x/XP/VISTA/7/8/10. The service is configured and monitored by the Control Panel Applet DNS Server. You need administrator privileges to change the configuration.

The start menu entries to install/remove the service execute the following commands:

1. The DNS Server service is installed with the command:
```
DNS4NT -install
```

and automatically started on Windows startup. The installed service can be started and stopped manually through the service control panel.

2. The command
   ```
   DNS4NT -remove
   ```
   stops and removes the DNS server service.

Menus

File

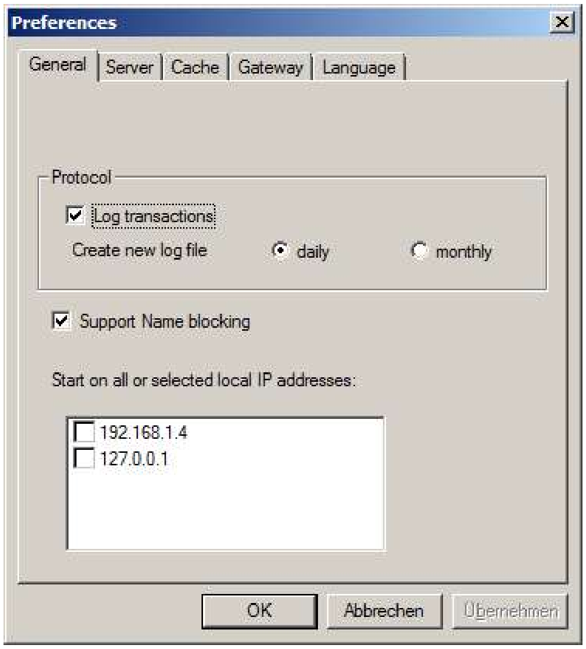
Statistics
shows DNS server usage statistics.

Exit
terminates the program

Options

Preferences

General



Protocol

☑ Log transactions

Create new log file ● daily ○ monthly

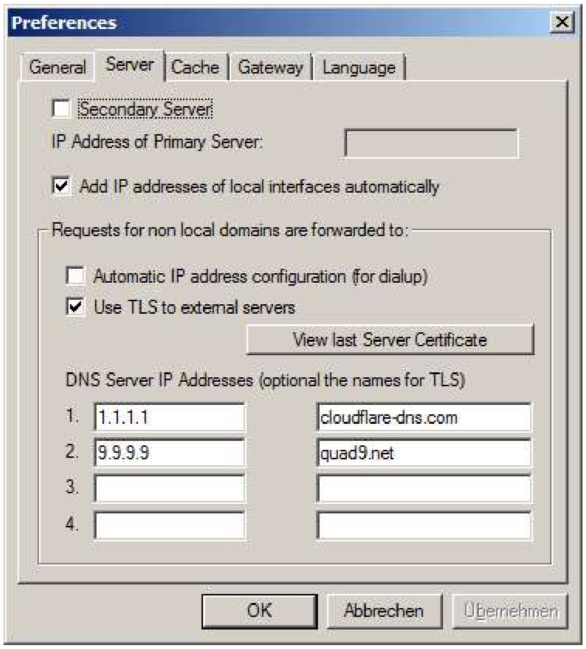
☑ Support Name blocking

Start on all or selected local IP addresses:

□ 192.168.1.4
□ 127.0.0.1

- Log transactions: Enables transaction and error log in a file. A new file can be created daily or once per month.
- Support name blocking: Enable a configurable blacklist of domains to reduce ad's and tracking
- Interfaces: By default the server is started on all local interfaces. If the server should run on selected local interfaces only, specify a comma separated list of up to 8 local interface ip addresses.

Server



☐ Secondary Server

IP Address of Primary Server:

☑ Add IP addresses of local interfaces automatically

Requests for non local domains are forwarded to:

☐ Automatic IP address configuration (for dialup)

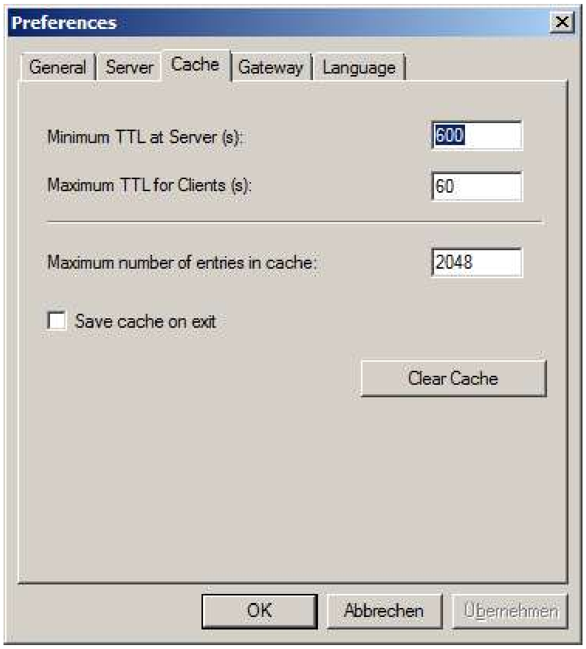
☑ Use TLS to external servers

DNS Server IP Addresses (optional the names for TLS)

1.	1.1.1.1	cloudflare-dns.com
2.	9.9.9.9	quad9.net
3.		
4.		

- for a Backup Name server the IP address of the Primary Name server must be specified. Requests for non local names, names that can not resolved locally, are forwarded to the addresses specified as external name server addresses.
- Local IP addresses could be added to the server database automatically.
- For dialup connections the server can configure the assigned external DNS server IP addresses.
- DNS over TLS could be selected for security.
  The configured server is expected to run on port 853. The software uses the Microsoft TLS implementation, depending on the OS TLS 1.2 may need an update of the implementation. DNS over TLS was tested with a collection of servers. Independant of the Windows OS it failed with google.dns (8.8.8.8 and 8.8.4.4). It works fine with quad9.net, cloudflare-dns.com and others.
- The certificate of the last TLS handshake with a server could be displayed. If the server name is specifed, the name is checked against the CN name of the certificate. Without the name any server name is accepted.

Cache



Minimum TTL at Server (s): 600

Maximum TTL for Clients (s): 60

Maximum number of entries in cache: 2048

☐ Save cache on exit

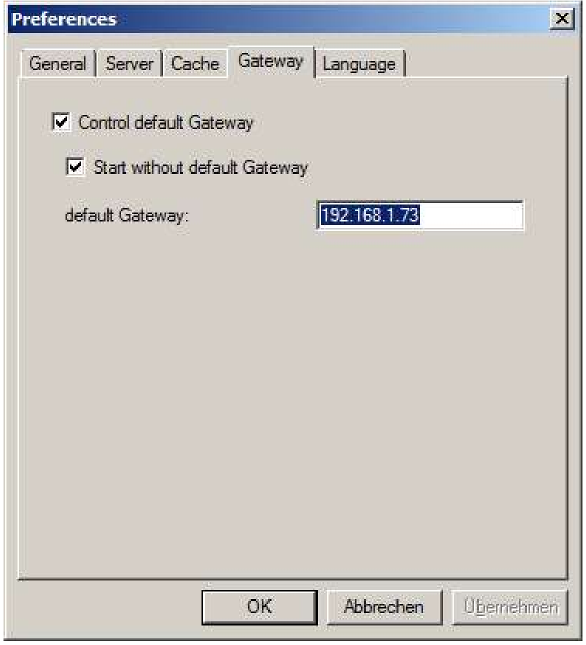
The current implementation of the server caches A, NS CNAME, and MX records. The software can modify the TTL values (valid through value of an entry) of DNS entries to improve network use and cache performance. Without any TTL entries the original values received are untouched.

- By specifying a **Minimal Server TTL** the valid through time of received entries is increased for entries with a smaller TTL value. The entries will remain longer in the cache and therefore improve operation, but the entry may be invalid. It makes sense for entries with a very low TTL e.g. 10 seconds. Increasing such TTL's to 300 seconds greatly enhances performance.

- By specifying a **Maximum Client TTL** caching of entries by clients can be reduced or avoided in favour of central caching in the DNS Server.
- The maximum number of cached entries is configurable. Least used entries are dropped from the cache is the maximum is exceeded.
- Save cache on exit writes cached information to a file CACHE.DMP. If available CACHE.DMP is used to initialize the cache on next restart of the server.
- Using the **Clear cache** button all cache entries are removed.

Gateway

This is a feature independent from DNS.



☑ Control default Gateway

☑ Start without default Gateway

default Gateway: 192.168.1.73

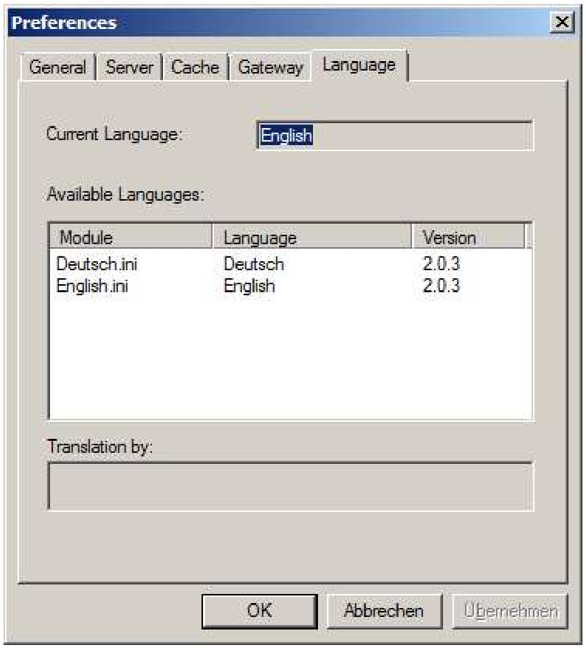
To temporary disconnect from Internet normally one can disconnect WLAN or deactivate the LAN connection. But this disconnects also from local network. Disconnecting from Internet without disconnectiong from local network could be achieved by removing the default gateway, but removing or setting the default gateway requires administrator rights on Windows.

- Activating the option allows a standard user to remove or set a predefined default gateway.
- To control the default gateway either right click on the tray icon and select the Set/Remove ... command or enter on a command line:
  dnscmd -gateway (removes the default gateway)
  dnscmd gateway (restores the default gateway)
-

To start a computer disconnected and connect manually to the Internet:

- For DHCP assigned IP addresses check the second option.
- For computers with fixed IP addresses the default gateway could be left empty in the TCP/IP configuration and configured here.

Language



Current Language: English

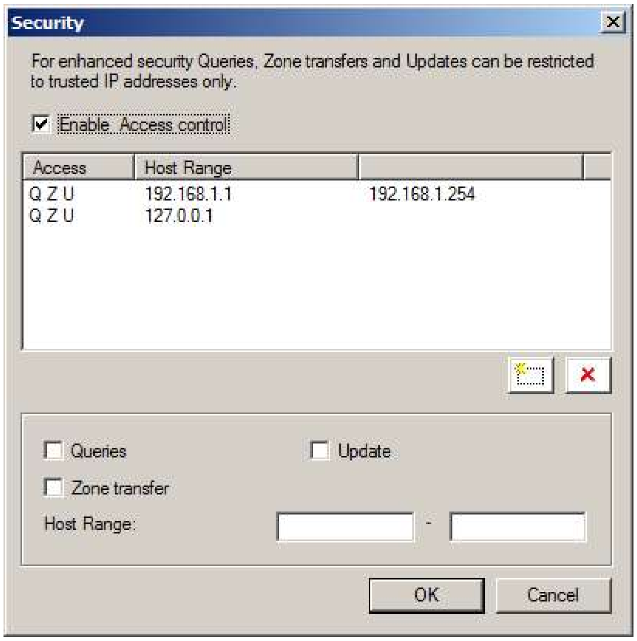
Available Languages:

Module	Language	Version
Deutsch.ini	Deutsch	2.0.3
English.ini	English	2.0.3

Translation by:

selects an user interface language.

Security



For enhanced security Queries, Zone transfers and Updates can be restricted to trusted IP addresses only.

☑ Enable Access control

Access	Host Range	
Q Z U	192.168.1.1	192.168.1.254
Q Z U	127.0.0.1	

☐ Queries ☐ Update

☐ Zone transfer

Host Range: -

Access can be granted by IP address for queries, zonetransfers, and updates.

- **Queries** are all types of queries to resolve a name.
- A **Zonetransfer** is used by a backup name server to update the database from the primary server.
- **Updates** are sent by DHCP Servers or DHCP clients to autmatically register an new name in the name server database. Updates must be sent to a primary name server only.

If you enable access control you need normally to include 127.0.0.1 to the addresses or the DNS client of the computer will not be able to contact the server.

Local Domain

general configuration settings for the local domain. The Database version is increased after a modification of the database automatically.

Add Entry

to add new Address, Nameserver or MX(Mail) records. To remove an entry use the context menu that will appear after clicking with the right mouse button on an entry.

Block Name

Name resolution for a host or domain can be blocked by adding an entry to the block list. The server returns IP address 127.0.0.1 for blocked names. Block names are stored in a file "domains.blk". For the entries pattern matching with wildcards is supported.

Additional names can be loaded from an external file in hosts format. The file must be named "hosts.blk" in the software installation folder. It is recommended for large files, because the entries are sorted on load for fast access at run time.

View

Database
displays the contents of the database.
Cache
displays the current contents of the cache including remaining live time of an entry.
Blocked Names
displays blocked names and a counter of blocked access.

Help

Contents
starts a HTML browser displaying the manual.
Register
prompts for the license key and your name, company. Check the Info menu to find out if the license information was accepted.
Show License
displays the conditions for using this software.
Info
displays program version information.

Support

The latest version is available on www.hanewin.net. Please mail comments, questions, problems to mail@hanewin.net.