# **NSSWITCH, DNS-Кеш, сетевые адаптеры, Форвардинг.**

### **Порядок источников имен NSSWITCH.**

Перед доступом к сайту компьютеру необходимо узнать его IP. Обычно для этого используется запрос к DNS серверу, который веб-браузер или операционная система выполняют автоматически, без действий пользователя.

В операционных системах ****Windows****и ****Linux****имеется файл ****hosts****, в котором можно установить IP адреса для любых имён — хостов и доменных имён. По умолчанию операционные системы работают так:

• *если запрашиваемое имя присутствует в файле hosts, то его IP берётся из этого файла и запрос к DNS серверу не делается*

• *если в файле hosts имя хоста не найдено, то выполняется запрос к DNS серверу*

В операционной системе Linux можно поменять приоритет источников для получения IP адреса или вовсе отключить некоторые из них. Для этого используется файл ****«/etc/nsswitch.conf».****

Файл ****«/etc/nsswitch.conf»****— это «****Name Service Switch configuration file****», то есть конфигурационный файл переключения служб имён.

Строка, которая отвечает за преобразование имён хостов начинается на «hosts».

Должна выглядеть так.

*hosts: files dns*

В старых или более новых системах она может быть такой.

hosts: files mymachines myhostname resolve [!UNAVAIL=return] dns

• *hosts — это указание на службу, для которой предназначена строка.*

• *files означает файл, относящийся к этой службе. У каждой службы в системе свой файл, в данном случае имеется ввиду «/etc/hosts».*

• *mymachines — судя по названию, означает имя машины.*

• *myhostname - hostname, логично.*

• *resolve — это системная служба резолва.*

• *Строка [!UNAVAIL=return] означает, что если предыдущая служба недоступна, то немедленно будет возвращён результат без запроса в следующем источнике.*

Файлы других служб.

*aliases /etc/aliases*

*ethers /etc/ethers*

*group /etc/group*

*hosts /etc/hosts*

*initgroups /etc/group*

*netgroup /etc/netgroup*

*networks /etc/networks*

*passwd /etc/passwd*

*protocols /etc/protocols*

*publickey /etc/publickey*

*rpc /etc/rpc*

*services /etc/services*

*shadow /etc/shadow*

Чтобы отключить файл «****/etc/hosts****» просто уберите слово «****files****».

Чтобы сделать приоретет dns выше файла «****/etc/hosts****» поставте это слово перед словом «****files****».

### **DNS-Кеш.**

Иногда вам может понадобится очистить кеш dns. Например, вам в организации для вашего выделенного белого ip адреса предоставлен доступ к какой-нибудь базе данных. И частенько бывает что у кого-нибудь что-нибудь не грузится, или возникают проблемы с dns-сервером.

Обычно очистка ****dns****-кеша помогает временно решить проблему. Чтобы постоянно не чистить кеш ****dns****стоит внести в файл «****hosts****» вашей системы сопоставление доменного имени и ip-адреса этой базы данных.

В ****Linux-е**** очистить ****кеш-dns**** немного сложнее, чем в ****Windows-е****.

Сначала необходимо определить кто занимается кешированием.

Например посмотрим на ****systemd-resolved****. Он бывает гораздо удобнее, чем встроеный резолвер в ****Network Manager****.

*$ sudo systemd-resolve —statistics*

Команда вернет ошибку, если резолвер не используется.

Если всё-таки используется для его очистки и перезапуска можно воспользоваться следующими командами.

*$ sudo systemd-resolve —flush-caches*

*$ sudo systemctl enable systemd-resolved.service*

Не забудьте про службу кеширования запросов службы имён «****nscd****».

*$ systemctl restart nscd*

*$ nscd -K; nscd*

Для её установки и настройки в ****Debian****.

*$ sudo apt install nscd*

*$ sudo service nscd restart*

*$ sudo ncsd -g*

*$ sudo strings /var/cache/nscd/hosts*

В ****Archlinux****она есть только в ****«****[AUR](https://vk.com/away.php?to=https%3A%2F%2Faur.archlinux.org%2Fpackages%2Funscd&cc_key=)****»****.

При использовании «****Network Manager****», его банально необходимо перезапустить.

*$ sudo service networking restart*

*# или*

*$ sudo systemctl restart NetworkManager*

### **Управление сетевыми адаптерами из CMD/PowerShell.**

Вообще у меня 2 заготовленых «****bat-файла****» с подсказками команд в кодировке «****ANSI****» и кончанием строк «****CRLF****» для коректного отображения русского языка. Один для ****Win-7**** и младше, другой для ****Win-10****. Оба запускают нужную мне оболочку и я могу проконтролировать сетевые соединения, сначала наличие или отсутствие тырнета и в каком месте: «****ping ya.ru****», «****nslookup ya.ru****», «****arp -a****», а затем и сами адаптеры, чтобы не искать в каждой системе где их можно ****включить****или ****выключить****.

Естественно запускаю файлы от имени Администратора по ****ПКМ****.

Файл «****network-cmd.bat****».

*@echo off*

*chcp 1251 >nul*

*echo.*

*echo "ipconfig /flushdns"*

*echo "ipconfig /registerdns"*

*echo 'ipconfig /release "Подключение по локальной сети"'*

*echo 'ipconfig /renew "Подключение по локальной сети"'*

*echo "ipconfig /all"*

*echo "ipconfig /displaydns"*

*echo.*

*echo "netsh interface show interface"*

*echo 'netsh interface set interface "Подключение по локальной сети" disable'*

*echo 'netsh interface set interface "Подключение по локальной сети" enable'*

*echo 'netsh interface set interface name="Подключение по локальной сети" admin=DISABLED'*

*echo 'netsh interface set interface name="Подключение по локальной сети" admin=ENABLED'*

*echo.*

*cmd.exe*

Файл «****network-powershell.bat****».

*@echo off*

*chcp 1251 >nul*

*echo.*

*echo "ipconfig /flushdns"*

*echo "ipconfig /registerdns"*

*echo 'ipconfig /release "Ethernet"'*

*echo 'ipconfig /renew "Ethernet"'*

*echo "ipconfig /all"*

*echo "ipconfig /displaydns"*

*echo.*

*echo "Get-NetAdapter | format-list"*

*echo 'Disable-NetAdapter -Name "Ethernet" -Confirm:$false'*

*echo 'Enable-NetAdapter -Name "Ethernet" -Confirm:$false'*

*echo.*

*powershell.exe*

Тут всё очевидно. Просто копируйте нужную команду и вставляйте в ваш CMD.

### **Форвардинг.**

Форвардинг (или перенаправление) – это процесс переадресации запросов на другой хост, порт или сеть. Поскольку этот процесс изменяет назначение передаваемого пакета, он считается операцией NAT.

В Linux-е для постоянного форвардинга по ipv4 необходимо раскоментировать строку в файле «****/etc/sysctl.conf****».

*$ sudo nano /etc/sysctl.conf*

*net.ipv4.ip\_forward = 1*

Для применения изменений без перезагрузки.

*sudo sysctl -p*

А теперь самое интересное.

****Как тоже самое сделать в Windows-е ???****

Для этого необходимо в редакторе реестра по пути «****HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters****» в параметре «****IPEnableRouter****» изменить шестнадцатеричное значение с ****0**** на ****1****.

Можно тоже самое сделать это с помощью «****reg-файла****», например, «****Net-Forwarding.reg****».

*Windows Registry Editor Version 5.00*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters]*

*"IPEnableRouter"=dword:00000001*

При необходимости убрать пере-направление, просто поменяйте последнюю единичку на нолик.

Ну а сегодня на этом всё. Надеюсь я хоть немного вас заинтересовал.

Спасибо за внимание. Всем Удачи, до новых встреч, Пока-Пока!