Отключение протоколов NetBIOS, LLMNR и mDNS в Windows

winitpro.ru/index.php/2017/08/21/otklyuchenie-netbios-cherez-tcpip-i-llmnr-v-domene-s-pomoshhyu-gpo

Широковещательные протоколы **NetBIOS over TCP/IP, LLMNR** и **mDNS** (Multicast DNS) используются для разрешения имен в Windows сетях, в которых отсутствует (недоступен) DNS сервер (обычно это домашние или небольшие офисные/SOHO сети). В корпоративных сетях с DNS серверами, эти протоколы обычно не нужны. Более того, эти широковещательные протоколы легко могут использоваться злоумышленниками для реализации спуфинг, relay и MITM атак, позволяющих перехватить учетные данных пользователей в локальной подсети (в т.ч. можно получить хэши NTLM). Разберемся, как отключить протоколы LLMNR, NetBIOS и mDNS в доменной сети Windows вручную и через GPO.

Широковещательные протоколы LLMNR, NetBIOS и mDNS в Windows сетях

DNS является предпочтительным методом разрешения имен в Windows сетях. Если в сети отсутствуют DNS сервера, используются альтернативные разрешающие протоколы в следующем порядке:

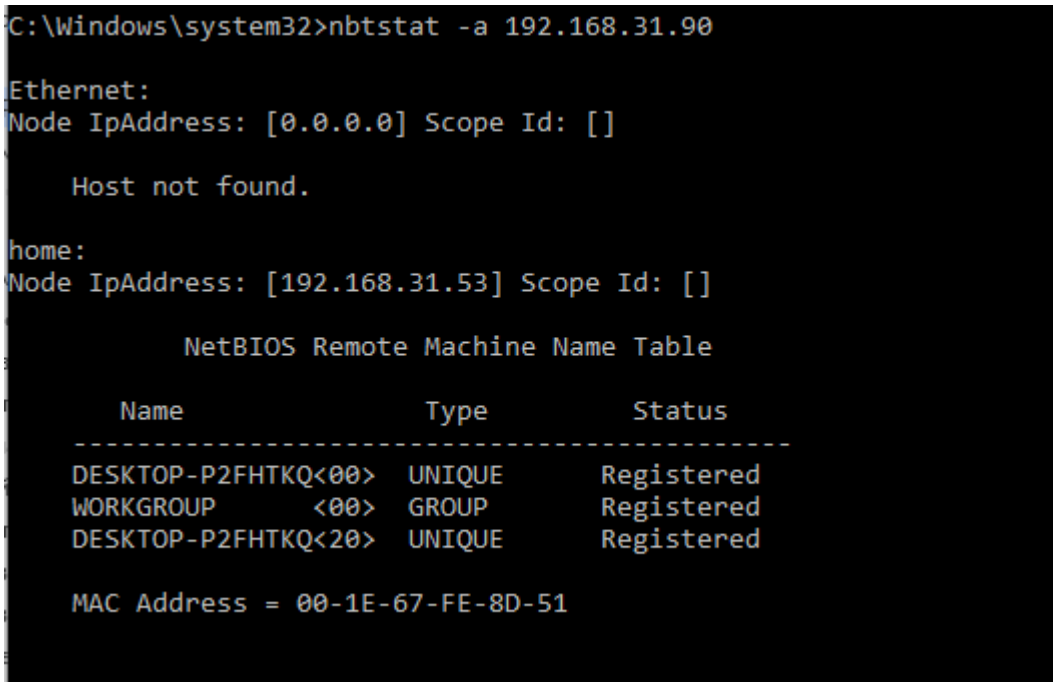
- **MulticastDNS (mDNS)**
- **Link-Local Multicast Name Resolution (LLMNR)**
- **NetBIOS (NBNS)**

Протокол LLMNR (механизм широковещательного разрешения имен) присутствует во всех версиях Windows, начиная с Vista и позволяет IPv6 и IPv4 клиентам разрешать имена соседних компьютеров без использования DNS сервера за счет широковещательных запросов в локальном сегменте сети L2. Этот протокол также автоматически используется при недоступности DNS (в рабочих группах Windows этот протокол используется для сетевого обнаружения/Network Discovery). Для передачи данных используется порт UDP/5355.

Протокол NetBIOS over TCP/IP или NBT-NS (UDP/137,138;TCP/139) – это широковещательный протокол, предшественник LLMNR, используется в локальной сети для публикации и поиска ресурсов. Поддержка NetBIOS over TCP/IP в Windows по умолчанию включена для всех интерфейсов.

В Windows можно вывести статистику протокола NetBIOS и текущих подключений TCP/IP по NBT с помощью команды nbtstat. Чтобы по IP адресу получить имя компьютера, выполните:

```
nbtstat -A 192.168.31.90
```



Утилита через NetBIOS обнаружила в локальной сети компьютер и вернула его имя. Можно получить из кэша NetBIOS все записи о соседних компьютерах в локальных сети:

```
nbtstat -c
```

В последних билдах Windows 11, NetBIOS будет использоваться только тогда, когдане получен ответ через mDNS или LLMNR.

Сетевой протокол **Multicast DNS (mDNS)** доступен начиная с версии Windows 10 1703 (в Windows Server с версии 2019). Позволяет разрешать имена хостов в IP-адреса в небольших локальных сетях без использования центрального DNS-сервера. Уникальность имен в пределах локальной сети обеспечивается присваиванием суффикса `.local` . Предполагалось, что mDNS должен полностью заменить устаревшие протоколы NetBIOS и LLMNR. Для разрешения имен используется многоадресная рассылка UDP пакетов на порт **5353**. mDNS также широко используется для автоматического обнаружения сетевых принтеров и других служб в локальной сети.

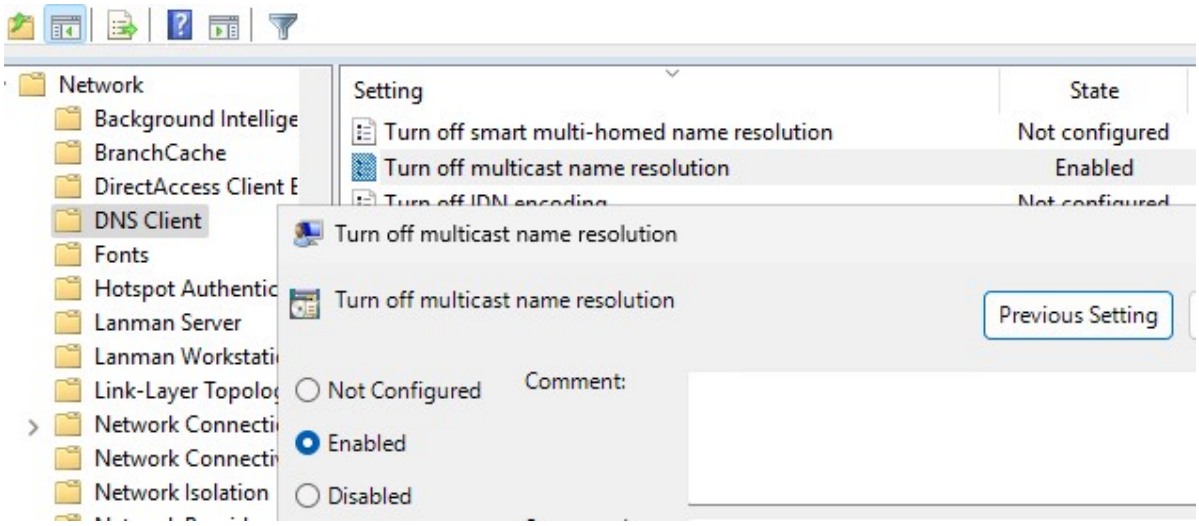
Протоколы **NetBIOS, LLMNR** и mDNS позволяют компьютерам в рабочей группе найти друг друга по именам при недоступности DNS сервера. В доменных сетях эти протоколы можно отключить.

Совет. Перед отключением протоколов NetBIOS, LLMNR и mDNS на всех компьютерах, проведите тестирование. Как правило, с отключением LLMNR обычно проблем нет, то отключение NetBIOS может парализовать работу устаревших систем.

Отключение протокола LLMNR с помощью GPO

В доменной среде широковещательные запросы LLMNR на компьютерах и серверах домена можно отключить с помощью групповой политики. Для этого:

1. В консоли `GPMC.msc` создайте новую или отредактируйте имеющуюся политику GPO, которую нужно применить ко всем рабочим станциям и серверам;
2. Перейдите в раздел **Computer Configuration -> Administrative Templates -> Network -> DNS Client;**
3. Включите политики **Turn off multicast name resolution** и **Turn off smart multi-homed name resolution**, изменив их значения на **Enabled**



4. Дождитесь обновления параметров GPO на клиентах или обновите их вручную командой `gpupdate /force` .

Можно отключить LLMNR в Windows, создав эти параметры в реестре с помощью PowerShell:

```
New-Item "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT" -Name DNSClient  -Force
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name EnableMultiCast -Value 0 -PropertyType DWORD -Force
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name DisableSmartNameResolution -Value 1 -PropertyType DWORD -Force
```

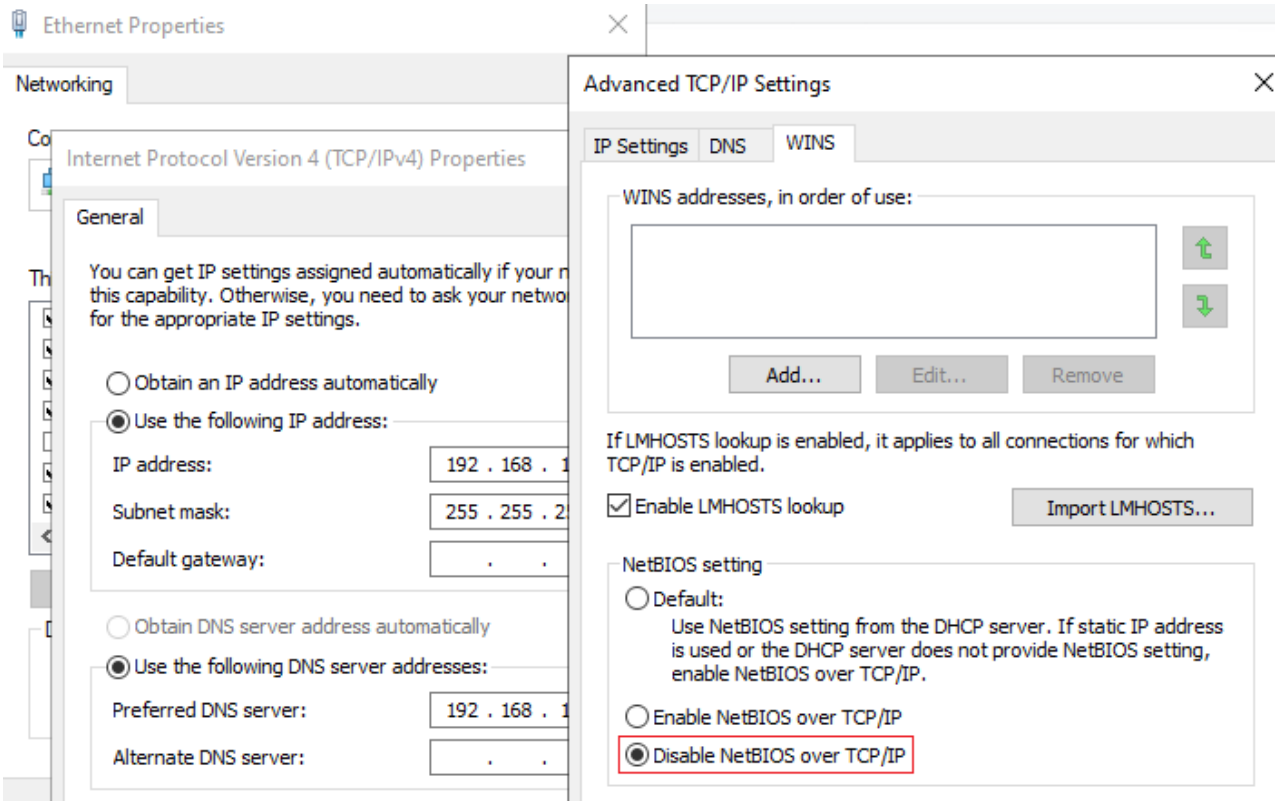
Отключение протокола NetBIOS over TCP/IP в Windows

Примечание.Протокол NetBIOS может использовать старыми версиями Windows и некоторыми не-Windows системами, поэтому отключение нужно сначала протестировать.

Отключить NetBIOS можно в настройках сетевого адаптера:

1. Откройте свойства сетевого подключения в панели `ncpa.cpl`
2. Выберите протокол **TCP/IPv4** и откройте его свойства;
3. Нажмите кнопку **Advanced**, затем перейдите на вкладку **WINS** и выберите опцию **Disable NetBIOS over TCP** (Отключить NetBIOS через TCP/IP);

4. Сохраните изменения.

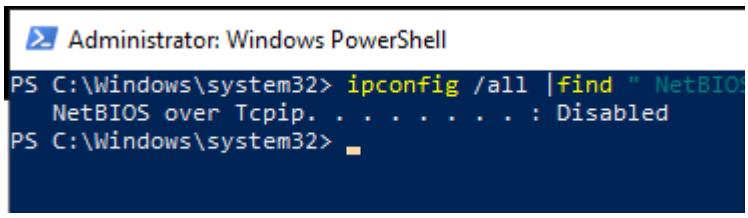


Если у вас на компьютере несколько сетевых интерфейсов (или отдельных VLAN), нужно будет отключить NetBIOS в свойствах каждого их них.

Проверьте статус NetBIOS over TCP/IP для сетевых адаптеров из командной строки:

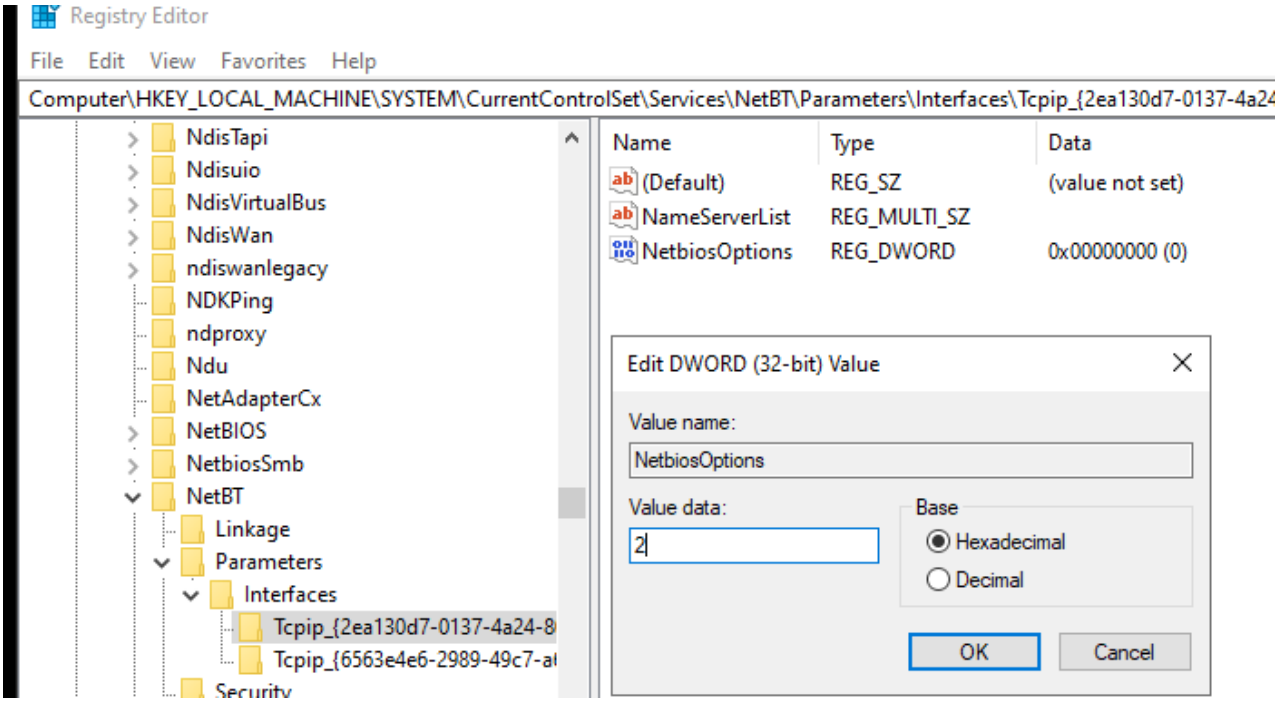
```
ipconfig /all |find "NetBIOS"
```

```
NetBIOS over Tcpip. . . . . : Disabled
```



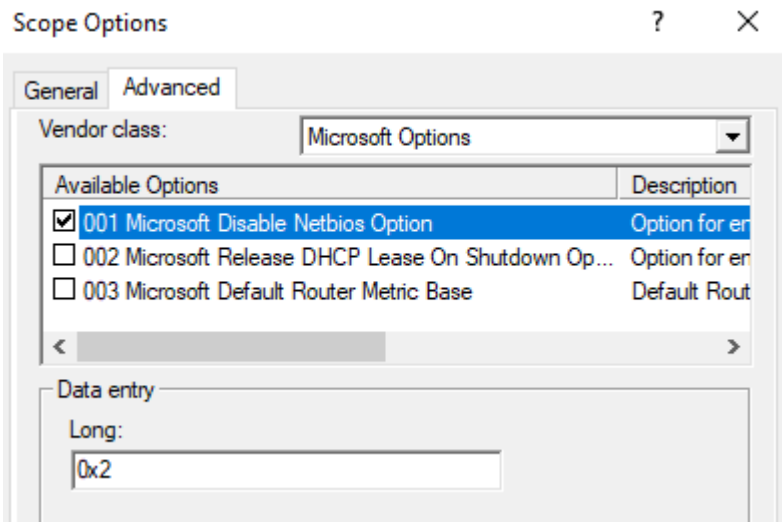
Можно отключить поддержку NetBIOS для конкретного сетевого адаптера через реестр. Для каждого сетевого адаптера компьютера есть отдельная ветка с его TCPIP_GUID внутри **HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces**.

Чтобы отключить NetBIOS для конкретного сетевого адаптера, нужно открыть его ветку и изменить значение параметра **NetbiosOptions** на **2** (по умолчанию значение – 0).



На клиентах домена, получающих IP адреса с DHCP сервера на Windows Server, вы можете отключить NetBIOS через отдельную DHCP опцию.

1. Для этого откройте консоль `dhcpmgmt.msc` и выберите настройки зоны Scope Option (или сервера – Server Options);
2. Перейдите на вкладку **Advanced**, в выпадающем списке Vendor class выберите **Microsoft Windows 2000 Options;**
3. Включите опцию **001 Microsoft Disable Netbios Option** и измените ее значение на **0x2.**



Как отключить NetBIOS через GPO?

В редакторе групповых политик или новых административных ADMX шаблонов GPO для Windows нет отдельного параметра, позволяющего отключить протокол NETBIOS over TCP/IP на компьютере. Чтобы отключить NETBIOS для всех адаптеров компьютера воспользуйтесь таким логон скриптом PowerShell.

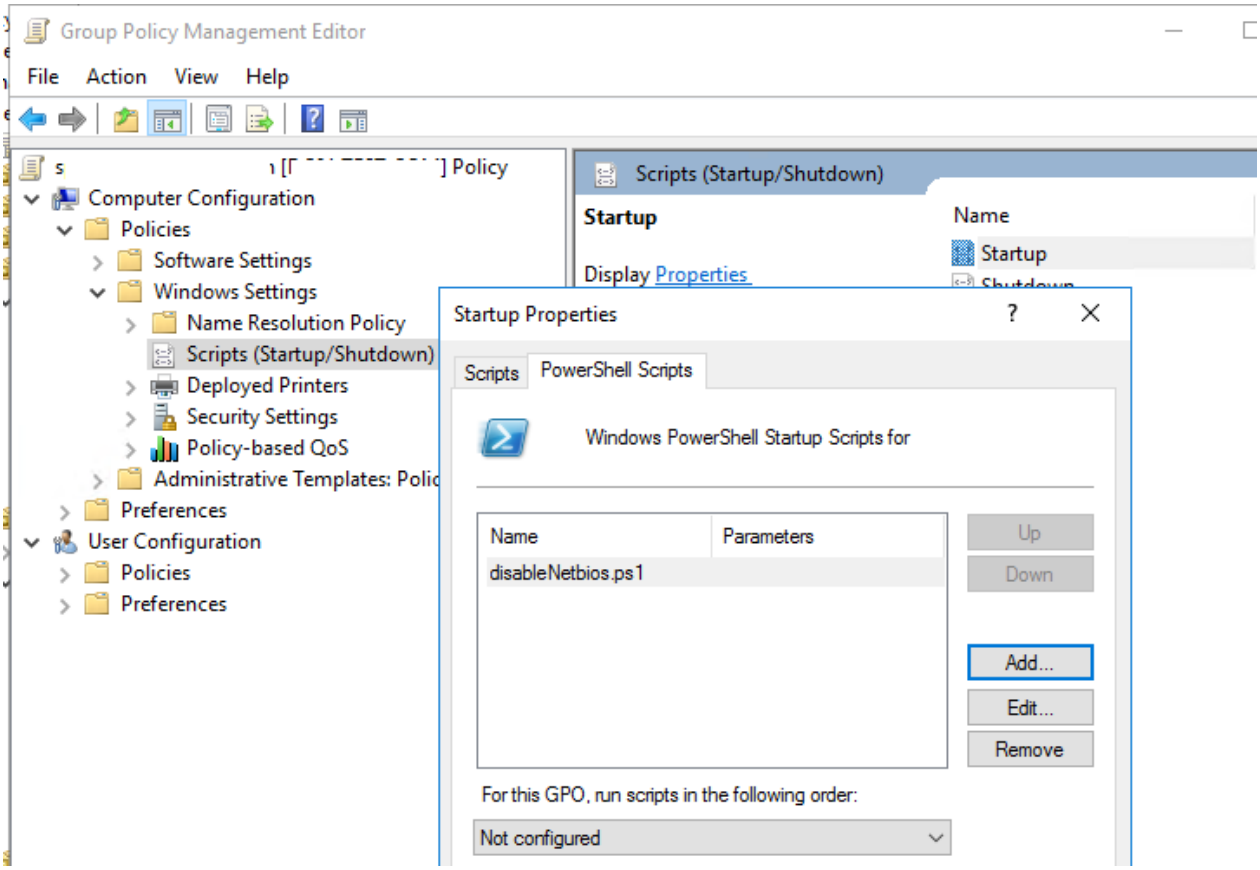
```
$regkey =
"HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
Get-ChildItem $regkey |foreach { Set-ItemProperty -Path
"$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}
```

Можно использовать более простой код с WMI запросом:

```
Get-WmiObject -Class Win32_NetworkAdapterConfiguration | %
{$_.SetTcpipNetbios(2)}
```

Сохраните этот код в файл disableNetbios.ps1, скопируйте его в каталог вашей GPO и запускайте на клиентах через **Computer Configuration -> Policies -> Windows Settings -> Scripts -> Startup -> PowerShell Scripts.**

Если на клиентах настройки политики выполнения PowerShell блокируют запуск этого скрипта, нужно подписать PS1 скрипт или запускать его в режиме -bypass.



Примечание. Для вступления изменений в силу, нужно отключить/включить сетевые адаптеры или перезагрузить компьютер.

Затем откройте командную строку и проверьте, что NetBIOS отключен для ваших сетевых адаптеров (кроме туннельных интерфейсов):

```
wmic nicconfig get caption,index,TcpipNetbiosOptions
```

```
PS C:\Windows\system32> wmic nicconfig get caption,index,TcpipNetbiosOptions
Caption                                  Index  TcpipNetbiosOptions
[00000000] Microsoft Kernel Debug Network Adapter  0
[00000001] Microsoft Hyper-V Network Adapter       1      2
[00000002] WAN Miniport (SSTP)                     2
[00000003] WAN Miniport (IKEv2)                    3
[00000004] WAN Miniport (L2TP)                     4
[00000005] WAN Miniport (PPTP)                     5
[00000006] WAN Miniport (PPPOE)                    6
```

Отключаем mDNS в Windows

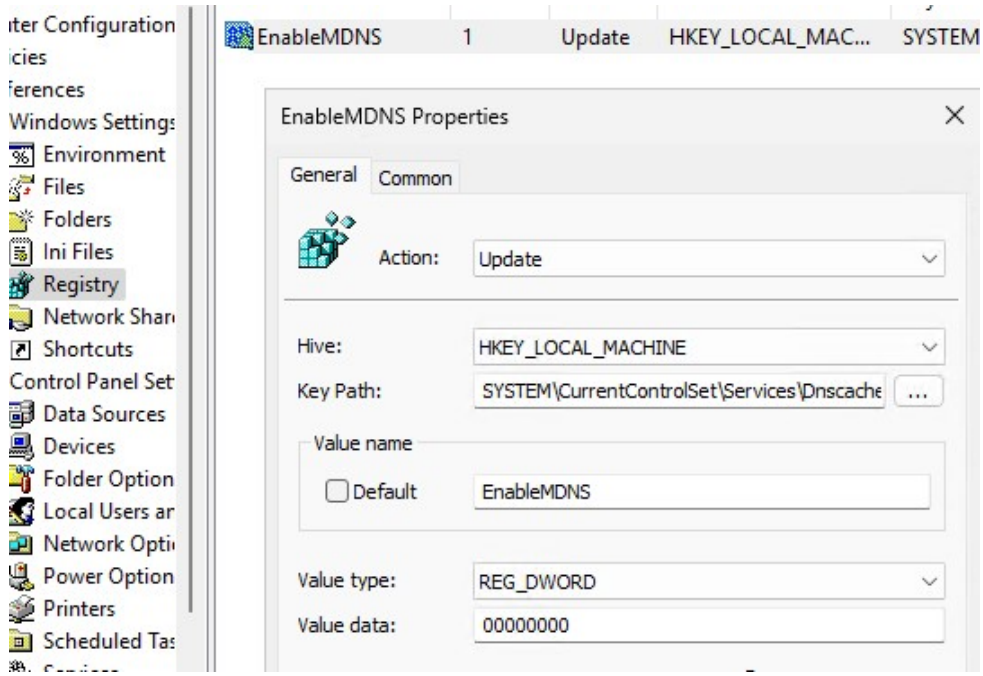
Для отключения протокола mDNS в Windows, нужно создать на компьютере параметр EnableMDNS со значением 0 в ветке реестра **HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters**.

Можно создать этот параметр командой:

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters" /v "EnableMDNS" /t REG_DWORD /d "0" /f
```

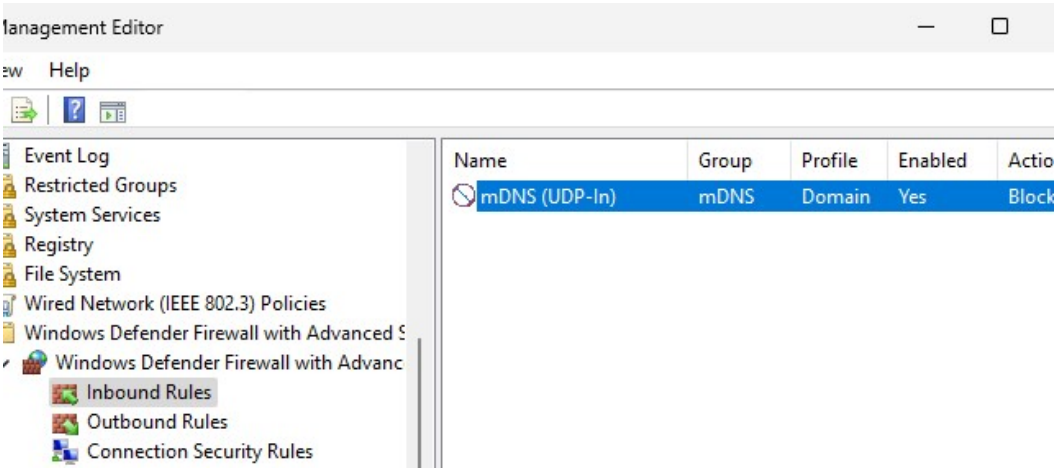
Либо применить параметр реестра через Group Policy Preferences (**Computer Configuration** > **Preferences** > **Windows Settings** > **Registry**)

- **Action**: Update
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path**: SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
- **Value name**: EnableMDNS
- **Value type**: DWORD
- **Value data**: 0



Также в GPO можно создать правило Windows Defender Firewall, которое будет блокировать входящий трафик mDNS на клиентах. Можно отключить правило **mDNS (UDP-In)** только для доменного профиля, чтобы ноутбуки пользователей при

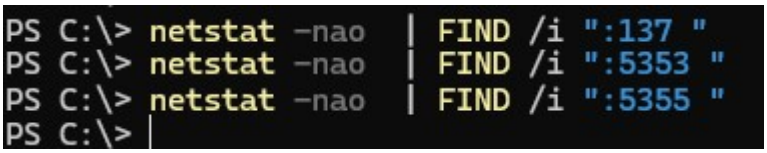
работе за пределами домена (офиса) могли обнаруживать в сети соседние устройства через mDNS.



При отключении mDNS у пользователей могут возникнуть проблемы с подключением к беспроводным дисплеям, проекторам через Miracast, а также некоторым принтерам.

Чтобы проверить, что на компьютере отключены NetBIOS, LLMNR и mDNS, выполните команды:

```
netstat -nao  | FIND /i ":137 "
netstat -nao  | FIND /i ":5353 "
netstat -nao  | FIND /i ":5355 "
```



Если эти протоколы разрешения имен отключены, команды не должны вернуть открытых портов.

Дополнительно в целях безопасности на компьютерах в корпоративной сети рекомендуется корректно настроить или совсем отключить протокол автонастройки прокси WPAD.