



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DHCP на Windows Server: пошаговый первичный деплой

Как мы разворачиваем роль с нуля: IP-план, relay, первая область, опции 003/006/015 и приёмка

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Раздача адресов живёт на роутере или L3-коммутаторе: аренды без учёта, принтеры и кассы меняют IP, резервирований нет, DNS-записи клиентов не обновляются. Итог — «1С не печатает», «сетевая папка недоступна», разбор каждого инцидента вручную. Мы переносим адресацию на роль DHCP Server в Windows Server, привязываем её к AD и DNS и делаем адресный план управляемым артефактом.

Почему это важно бизнесу

- Простой печати и обмена с 1С из-за смены IP у принтера и сервера — часы работы бухгалтерии и склада
- Конфликты адресов и APIPA 169.254.0.0/16 парализуют рабочее место целиком, а не отдельный сервис
- Без журнала аренд невозможно ни расследовать инцидент, ни посчитать реальное число устройств в сети
- Адресация на роутере умирает вместе с роутером: замена железа = переконфигурация всей сети вручную
- Чужой DHCP от принесённого сотрудником роутера раздаёт неверный шлюз всему офису



Ключевые параметры реализации

8 суток

Аренда офисной области; renew в T1 = 50%, rebind в T2 = 87,5% срока
RFC 2131, раздел 4.4.5

UDP 67/68

Порты DHCP-обмена; для будущей failover-пары дополнительно TCP 647 между узлами
RFC 2131; DHCP failover (MS)

0...5

ConflictDetectionAttempts: дефолт 0, на миграции ставим 1, после приёмки возвращаем 0
Set-DhcpServerSetting, WS2025

60 мин

Дефолт BackupInterval dhcp.mdb; CleanupInterval задаём 120 мин
Set-DhcpServerDatabase
Set-DhcpServerDatabase WS2025

.2-.99

Блок статики в /24, который выводим из пула exclusion-диапазоном: шлюзы, МФУ, серверы
Стандарт адресации ITfresh

Роль 12

Ветка ServerManager\Roles\12: ConfigurationState=2 снимает алерт post-install
Deploy DHCP with PowerShell



Подготовка: IP-план, статика и relay на L3

Что настраиваем

Периметр и ядро сети: L3-коммутатор или маршрутизатор, будущий DHCP-узел в домене, до 5 клиентских VLAN офиса до 50 РМ

Как мы это делаем

- 1 Фиксируем IP-план в таблице: VLAN, префикс, шлюз, блок статика .2-.99, пул .100-.240, резерв .241-.254; исключения задаём до активации
- 2 Статика узла: New-NetIPAddress -IPAddress 10.10.10.20 -PrefixLength 24 -DefaultGateway 10.10.10.1 и Set-DnsClientServerAddress на IP контроллеров
- 3 Вводим в домен ДО установки роли и сверяем время с PDC-эмулятором (w32tm /query /status): рассинхрон ломает Kerberos и авторизацию
- 4 На L3 прописываем ip helper-address на адрес DHCP-узла в каждом клиентском VLAN и гасим встроенный пул коммутатора или роутера
- 5 Проверяем, что DHCPDISCOVER доходит: giaddr в запросе равен адресу SVI нужного VLAN, иначе сервер выберет чужую область

РЕЗУЛЬТАТ

Область выбирается по giaddr правильно с первой попытки, статика и пул не пересекаются, а «двойной DHCP» исключён ещё до установки роли. План адресации становится документом, по которому потом собираются резервирования и мониторинг.

КЛЮЧЕВОЙ НЮАНС

Статический IPv4 и DNS на контроллеры домена задаём до установки роли: узел с адресом по DHCP теряет привязку области, а без корректного DNS не идёт регистрация записей клиентов.



Установка роли и пост-развёртывание

Что настраиваем

Узел *dhcp01* в домене: роль *DHCP Server*, *security*-группы, авторизация в AD, серверные настройки *DDNS* и базы

Как мы это делаем

- 1 `Install-WindowsFeature DHCP -IncludeManagementTools`, затем `netsh dhcp add securitygroups` (группы *DHCP Administrators/Users*) и `Restart-Service dhcpserver`
- 2 Авторизация в AD: `Add-DhcpServerInDC -DnsName dhcp01.corp.local -IPAddress 10.10.10.20`, контроль — `Get-DhcpServerInDC`; без записи аренды не выдаются
- 3 Снимаем ложный алерт *Server Manager*: `Set-ItemProperty registry::HKLM\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name ConfigurationState -Value 2`
- 4 `Set-DhcpServerv4DnsSetting -DynamicUpdates Always -DeleteDnsRRonLeaseExpiry $true -NameProtection $true`; учётка *DDNS* — `Set-DhcpServerDnsCredential`
- 5 `Set-DhcpServerDatabase -BackupInterval 60 -CleanupInterval 120` (минуты) и `Set-DhcpServerAuditLog -Enable $true -MinMBDiskSpace 20`

РЕЗУЛЬТАТ

Роль поднимается одним воспроизводимым скриптом за 10–15 минут, служба легально работает в домене, *DNS*-записи клиентов создаются и удаляются вместе с арендой, а база сама бэкапится и чистится по расписанию.

КЛЮЧЕВОЙ НЮАНС

Отдельная учётка *DDNS* обязательна, если *DHCP* стоит на контроллере домена или узлов несколько: иначе записи принадлежат серверу и «чужой» узел их не перезапишет. В бэкап *dhcp.mdb* креды не входят.



Первая область, опции 003/006/015 и приёмка

Что настраиваем

Область Office 10.10.10.0/24 на dhcp01: пул, исключения, опции, резервирования и проверка на клиенте

Как мы это делаем

- 1 Add-DhcpServerv4Scope -Name Office -StartRange 10.10.10.100 -EndRange 10.10.10.240 -SubnetMask 255.255.255.0 -LeaseDuration 8.00:00:00 -State InActive
- 2 Add-DhcpServerv4ExclusionRange -ScopelId 10.10.10.0 -StartRange 10.10.10.2 -EndRange 10.10.10.99 — статика инфраструктуры выводится из пула
- 3 Опции области: Set-DhcpServerv4OptionValue -ScopelId 10.10.10.0 -Router (003) -DnsServer (006) -DnsDomain (015); NTP — OptionId 42, PXE — 66 и 67
- 4 Резервирования: Add-DhcpServerv4Reservation -ScopelId 10.10.10.0 -IPAddress 10.10.10.31 -ClientId 00-23-AC-F4-11-02 -Description с моделью МФУ
- 5 Активируем: Set-DhcpServerv4Scope -ScopelId 10.10.10.0 -State Active; приёмка — ipconfig /renew, Get-DhcpServerv4Lease, Get-DhcpServerv4FreeIpAddress

РЕЗУЛЬТАТ

Клиент получает адрес, шлюз, DNS и суффикс за один цикл DISCOVER-OFFER-REQUEST-ACK; принтеры и МФУ сидят на постоянных адресах; занятость пула видна по PercentageInUse из Get-DhcpServerv4ScopeStatistics, а не на глаз.

КЛЮЧЕВОЙ НЮАНС

Область создаём в состоянии InActive и активируем последней, уже с исключениями и опциями: активная область с непроверенным пулом успевает раздать неверный шлюз всему сегменту.



Подводные камни

✗ Роль стоит, но не авторизована в AD

Служба стартует и молчит, клиенты уходят в APIPA 169.254.x.x. Проверяем Get-DhcpServerInDC и добавляем узел через Add-DhcpServerInDC.

✗ Пул пересекается со статикой

Исключения задали после активации — конфликты разошлись. Порядок: InActive, ExclusionRange, затем Set-DhcpServerv4Scope -State Active.

✗ Забыт ip helper-address в VLAN

Broadcast не покидает подсеть, область не выбирается. Relay указываем на IP DHCP-узла в каждом клиентском VLAN, проверяем giaddr в запросе.

✗ Двойной DHCP: роутер плюс сервер

Старый пул на роутере или L3 не выключили — часть клиентов получает чужой шлюз. Гасим встроенный DHCP в тот же час, что активируем область.

✗ Клиенты не регистрируются в DNS

Не включён DynamicUpdates и нет учётки DDNS. Ставим Set-DhcpServerv4DnsSetting -DynamicUpdates Always и Set-DhcpServerDnsCredential.

✗ Аренда 8 суток в гостевой сети

Пул выдается устройствами, которые ушли вчера. Гостевому и Wi-Fi-сегменту — своя область с -LeaseDuration 0.04:00:00, а не общий пул.

✗ Старая аренда живёт после миграции

Клиент держит адрес прежнего пула до T1 — половины срока аренды. На приёмке делаем ipconfig /release + /renew, оборудование — рестарт порта.

✗ Нет бэкапа базы dhcp.mdb

Каталог %SystemRoot%\System32\dhcp\backup никто не выгружает. Задаём BackupInterval и еженедельный Export-DhcpServer -File ... -Leases.

Как правильно

МИНИМУМ

- Статический IP, членство в домене и синхронное время до установки роли
- Авторизация в AD и проверка Get-DhcpServerInDC перед активацией области
- Одна область на подсеть с исключением блока статики и опциями 003/006/015
- Встроенный DHCP на роутере и коммутаторах выключен полностью

НОРМАЛЬНО

- Развёртывание скриптом PowerShell, сохранённым в репозитории конфигураций
- ip helper-address на всех клиентских VLAN, giaddr проверен трассировкой
- DDNS с отдельной учёткой, NameProtection и DeleteDnsRRonLeaseExpiry \$true
- Резервирования по MAC для МФУ, касс, ТСД и сетевого оборудования

ХОРОШО

- Разные области и сроки аренды для офиса, Wi-Fi, гостей и VoIP
- PercentageInUse из Get-DhcpServerv4ScopeStatistics: порог 85%
- Аудит-лог DhcpSrvLog-*.log из System32\dhcp собирается в SIEM
- Вторая нода и failover-пара как следующий шаг после приёмки

Чек-лист самопроверки

- | | |
|---|--|
| ☐ Есть ли утверждённый IP-план: VLAN, префиксы, шлюзы, границы статика и DHCP-пула? | ☐ Исключения заданы до активации области, статика и пул нигде не пересекаются? |
| ☐ У DHCP-сервера статический IPv4 и DNS на контроллеры домена, DHCP на его NIC выключен? | ☐ Опции 003, 006 и 015 заданы на уровне области, а не только сервера? |
| ☐ Сервер введён в домен и авторизован: Get-DhcpServerInDC возвращает его имя и адрес? | ☐ Срок аренды выбран под сегмент: офис — 8 суток, Wi-Fi и гости — 2-8 часов? |
| ☐ В каждом клиентском VLAN прописан ip helper-address на адрес DHCP-узла? | ☐ Приёмка пройдена: ipconfig /renew на клиенте и Get-DhcpServerv4Lease на сервере? |
| ☐ Встроенная раздача адресов на роутере и L3-коммутаторах отключена полностью? | ☐ Настроены резервирования по MAC для принтеров, МФУ, касс и сетевого оборудования? |

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Проектируем IP-план и сегментацию VLAN, согласуем границы статики, пула и резерва
- Разворачиваем роль DHCP Server скриптом: авторизация в AD, DDNS, аудит, бэкап базы
- Настраиваем relay на коммутаторах и переносим раздачу с роутера без простоя офиса
- Собираем области и резервирования, проводим приёмку на клиентах и фиксируем в паспорте сети
- Подключаем мониторинг занятости пула и сопровождаем адресацию дальше по SLA

15+

лет в ИТ-поддержке

50

рабочих мест — наш профиль

МТС

дата-центр, Москва



КОНТАКТЫ

Обсудить вашу задачу

Сайт **itfresh.ru**

Телефон **+7 903 729-62-41**

Telegram **@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.



itfresh.ru



Техническая база

- 01** Deploy DHCP Using Windows PowerShell (learn.microsoft.com — 2025)
- 02** Install and configure DHCP Server on Windows Server (learn.microsoft.com — 2025)
- 03** Add-DhcpServerv4Scope, Add-DhcpServerv4ExclusionRange (learn.microsoft.com — WS2025)
- 04** Set-DhcpServerv4OptionValue, Add-DhcpServerv4Reservation (learn.microsoft.com — WS2025)
- 05** Set-DhcpServerv4DnsSetting, Set-DhcpServerDnsCredential (learn.microsoft.com — WS2025)
- 06** Set-DhcpServerDatabase, Set-DhcpServerAuditLog (learn.microsoft.com — WS2025)
- 07** RFC 2131: Dynamic Host Configuration Protocol (rfc-editor.org — 1997)
- 08** RFC 2132: DHCP Options and BOOTP Vendor Extensions (rfc-editor.org — 1997)

