Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DHCP в офисе до 50 рабочих мест: наша схема без простоев

Расчёт пула и lease, резервации по MAC, failover Windows Server, DHCP Snooping и мониторинг Za...

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Половина офиса утром без сети, принтер «теряет» IP, 1С не видит сервер по имени — почти всегда это DHCP: исчерпанный пул, чужой роутер с включённой раздачей адресов или устаревшие опции в забытом VLAN. Разбираем нашу схему выдачи адресов для офисов 10–50 РМ: расчёт пула, резервации, отказоустойчивость и мониторинг, при которых сеть не зависит от одного узла и человеческой памя…

Почему это важно бизнесу

- Исчерпанный пул бьёт выборочно: часть сотрудников без 1С и почты, а без инженера диагностика растягивается на часы
- Один принесённый роутер с включённым DHCP кладёт всю локалку: чужие шлюз и DNS останавливают 1С, печать и телефонию
- Слетевшая резервация принтера или кассы — регулярные простои бухгалтерии и точек продаж по 30–60 минут
- DHCP без бэкапа и реестра: после сбоя сервера резервации восстанавливают вручную день вместо 15 минут импортом

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

x4

IP-адресов закладываем на одно рабочее место: ПК, ноутбук, смартфон, периферия — пул считаем о...

наш стандарт

8 ч

lease time офисного сегмента: пул полностью обновляется за ночь, адреса не застревают за ушедш...

наш стандарт

1 час

MCLT в DHCP failover по умолчанию — максимум, на который партнёр продлевает lease без синхрони...

по докам Microsoft, WS2012+

50/50

режим Load Balance между двумя DHCP-серверами одной площадки — значение по умолчанию, его и де...

learn.microsoft.com

80%

порог PercentageInUse области, с которого Zabbix шлёт warning инженеру в Telegram (90% — high)

наш шаблон Zabbix

60 мин

интервал автобэкапа базы DHCP в %SystemRoot%\System32\dhcp\backup — локальный, поэтому дублиру...

learn.microsoft.com

РЕАЛИЗАЦИЯ 1 ИЗ 3

Область и резервации на Windows Server DHCP

Что настраиваем

Роль DHCP Server на выделенном member-сервере; офисы 20–50 PM с Active Directory

Как мы это делаем

1. Ставим роль Install-WindowsFeature DHCP -IncludeManagementTools и авторизуем сервер в AD через Add-DhcpServerInDC — неавторизованная служба адреса не выдаёт
2. Создаём область Add-DhcpServerv4Scope: размер пула = число устройств x2 (30 PM ≈ 60 устройств → пул 120 адресов), lease задаём -LeaseDuration 08:00:00
3. Опции области: 003 — шлюз, 006 — DNS строго контроллеры домена, 015 — имя AD-домена; включаем динамическое обновление DNS-зон с name protection
4. Add-DhcpServerv4Reservation для принтеров, МФУ, камер, VoIP и NAS; MAC — в формате с дефисами, после создания проверяем ipconfig /release + /renew на устройстве
5. Set-DhcpServerSetting -ConflictDetectionAttempts 2 — сервер проверяет адрес ping'ом перед выдачей и не конфликтует с забытой статикой

РЕЗУЛЬТАТ

Выдача адресов переживает рост офиса и «принесённые» устройства: пул с двукратным запасом не исчерпывается, ключевая периферия всегда на своих IP, короткие имена резолвятся во всех сегментах, а конфликты со старой статикой сервер отсекает сам ещё до выдачи адреса.

КЛЮЧЕВОЙ НЮАНС

Резервация с MAC в неверном формате (двоеточия или смешанные разделители вместо дефисов) молча игнорируется — поэтому каждую резервацию мы подтверждаем перевыдачей адреса на живом устройстве, а не «на глаз».

РЕАЛИЗАЦИЯ 2 ИЗ 3

Failover и барьер против rogue DHCP

Что настраиваем

Пара DHCP-серверов + управляемые коммутаторы доступа; все VLAN офиса

Как мы это делаем

1. Строим связь Add-DhcpServerv4Failover: Load Balance 50/50, MCLT 1 ч, -AutoStateTransition со -StateSwitchInterval 60 мин (по умолчанию авто-переход выключен), свой...
2. На коммутаторах включаем DHCP Snooping (ip dhcp snooping vlan 10,20), trust — только порт сервера и аплинки: посторонние DHCPOFFER отбрасываются на порту
3. В сегментах на MikroTik включаем /ip dhcp-server alert — роутер сам ловит чужие DHCP-ответы и пишет MAC нарушителя в лог
4. Роутеры и точки провайдеров вводим только в режиме Access Point с выключенным DHCP; их порты на коммутаторе остаются untrusted

РЕЗУЛЬТАТ

Отказ одного DHCP-сервера офис не замечает: партнёр продолжает выдачу в пределах MCLT и забирает область по switchover. Принесённый «роутер для гостевого Wi-Fi» больше не способен раздать свои адреса — его ответы гибнут на порту коммутатора, а не в переговорке у пользователей.

КЛЮЧЕВОЙ НЮАНС

Авторизация DHCP в AD останавливает только Windows-серверы — роутер-железку она не видит. Реальный барьер против rogue DHCP даёт именно snooping на уровне порта доступа, поэтому начинаем с него.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Мониторинг пула, аудит выдачи и восстановление

Что настраиваем

Zabbix + PowerShell на DHCP-хосте; клиенты на абонентском обслуживании

Как мы это делаем

1. Каждые 5 мин агент снимает Get-DhcpServerv4ScopeStatistics (PercentageInUse, Free) по всем областям; триггеры: warning с 80%, high с 90%
2. Раз в час контрольная машина шлёт тестовый DHCPDISCOVER: если OFFER приходит не с адреса нашего сервера — алерт в Telegram дежурному
3. Аудит выдачи: журналы DhcpSrvLog-*.log из %windir%\system32\dhcp перезаписываются по дням недели, поэтому копируем их на бэкап-узел и храним 30 дней
4. Еженедельно Export-DhcpServer -Leases в XML на бэкап-узел, конфиги Mikrotik/Keenetic — export в Git; восстановление отработано через Import-DhcpServer

РЕЗУЛЬТАТ

Исчерпание пула и появление чужого DHCP мы видим за часы до жалоб пользователей, а не после звонка «встала сеть». Полное восстановление сервера с областями, опциями и резервациями занимает 15 минут импортом XML вместо дня ручного восстановления по памяти.

КЛЮЧЕВОЙ НЮАНС

Штатный автобэкап DHCP каждые 60 минут пишется на тот же диск, что и база, — при гибели сервера он гибнет вместе с ней. Обязателен внешний Export-DhcpServer по расписанию.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Lease time 7 суток «по умолчанию»**
  Смартфоны и гости за неделю забивают пул втрое. Ставим 8–12 ч: пул обновляется за ночь, а нагрузка на сервер остаётся ничтожной
- ✕ **Rogue DHCP от провайдерского роутера**
  Монтажники включают роутер с активным DHCP — сеть получает чужие шлюз и DNS. Обходим DHCP Snooping'ом и регламентом ввода железа только через нас
- ✕ **Неверный формат MAC в резервации**
  Дефисы, двоеточия и точки в разных системах: невалидный MAC Windows игнорирует молча. Всегда проверяем резервацию перевыдачей адреса на устройстве
- ✕ **Статика на устройствах вместо резерваций**
  Статика на принтере рано или поздно конфликтует с пулом. Всё ключевое — только резервацией в DHCP, диапазон статики исключаем из пула явно
- ✕ **Забытый VLAN при смене DNS**
  DHCP настроен в 2–3 местах, при замене DC обновляют не все. Ведём реестр всех DHCP-точек клиента и проходим его чек-листом при каждом изменении
- ✕ **Два DHCP без согласования**
  «Подстраховочный» второй сервер без failover раздаёт конфликтующие адреса. Только штатный failover WS2012+ либо документированный split-scope
- ✕ **Надежда на AD-авторизацию против rogue**
  Rogue-защита AD останавливает лишь Windows-серверы, железки ей невидимы. Блокировку чужих OFFER делаем snooping'ом на коммутаторе
- ✕ **Бэкап DHCP только локальный**
  Автобэкап раз в 60 мин лежит на том же диске. Дублируем Export-DhcpServer в XML на внешний узел — иначе резервации восстанавливать вручную

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- DHCP в одной точке, пул = число устройств x2, lease time 8–12 ч
- Резервации по MAC для принтеров, камер, VoIP, NAS — без статики на устройствах
- Опции 003/006/015: шлюз, DNS = контроллеры домена, имя AD-домена
- ConflictDetectionAttempts = 2 и включённый автобэкап базы DHCP

НОРМАЛЬНО

- Перенос DHCP на Windows Server при наличии AD или от 25 рабочих мест
- DHCP Snooping на коммутаторах: trust только порт сервера и аплинки
- Zabbix-контроль PercentageInUse по областям, алерт с 80%
- Еженедельный Export-DhcpServer в XML вне сервера, конфиги роутеров — в Git

ХОРОШО

- DHCP failover Load Balance 50/50 на два сервера, MCLT 1 ч
- Часовой rogue-скан: тестовый DHCPDISCOVER, алерт на чужой OFFER
- Отдельные VLAN и области: офис / гости / камеры / VoIP со своими опциями
- Реестр всех DHCP-точек, обязательная актуализация при каждом изменении инфры

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Пул рассчитан из 4 IP на рабочее место и в пиковый день заполнен не выше 80%?
- [ ] Lease time 8–12 часов, а не 7 суток из заводских настроек роутера?
- [ ] Принтеры, камеры, VoIP и NAS получают адреса резервацией по MAC, а не статикой на устройстве?
- [ ] Опции 006/015 указывают на актуальные контроллеры домена во ВСЕХ VLAN, а не только в основном?
- [ ] На коммутаторах включён DHCP Snooping и trust задан только порту сервера?
- [ ] Есть второй DHCP-сервер в failover или документированный split-scope?
- [ ] База DHCP еженедельно выгружается Export-DhcpServer за пределы сервера?
- [ ] Заполнение пула мониторится и алертит инженера до исчерпания, а не после жалоб?
- [ ] Существует реестр всех точек, где работает DHCP (серверы, роутеры, VLAN)?
- [ ] Новое сетевое оборудование вводится в сеть только после проверки, что его DHCP выключен?

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

ЧТО МЫ ДЕЛАЕМ

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).

- Аудит DHCP/DNS офиса: пулы, lease, резервации, опции по всем VLAN — с письменным отчётом
- Перенос DHCP с роутера на Windows Server: область, резервации, failover за 1–2 часа работ
- Защита от rogue DHCP: DHCP Snooping на коммутаторах, регламент ввода оборудования
- Мониторинг Zabbix: заполнение пула, rogue-скан, алерты инженеру в Telegram
- Бэкап и документация: Export-DhcpServer по расписанию, реестр всех DHCP-точек клиента

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

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 DHCP Failover Settings / Failover Modes (Windows Server) (learn.microsoft.com — WS2012+)

02 Модуль PowerShell DhcpServer (Scope, Reservation, Failover, Export) (learn.microsoft.com — WS2025)

03 MikroTik RouterOS: IP / DHCP Server (alert, lease-time) (help.mikrotik.com — ROS 7.x)

04 Cisco IOS: конфигурация DHCP Snooping (cisco.com — IOS XE)

05 RFC 2132 — DHCP Options (3, 6, 15, 51) (rfc-editor.org — 1997)

06 Наш шаблон Zabbix: DHCP PercentageInUse + rogue-скан (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.