Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Сеть офиса до 50 РМ: VLAN, гостевой Wi-Fi, IP-план — наш стандарт

Как мы строим сегментацию на MikroTik RouterOS 7: bridge VLAN filtering, WPA3-Enterprise, defa…

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Плоская сеть 192.168.1.0/24, где ПК, сервер 1С, NAS, камеры и гостевые смартфоны видят друг друга, — норма в 8 из 10 офисов, которые мы принимаем на обслуживание. Один заражённый ноутбук получает L2-доступ ко всем ресурсам сразу: шифровальщик доходит до общих папок за минуты. Мы перестраиваем такую сеть в 5–7 изолированных VLAN с межсегментным файрволом без остановки офиса.

Почему это важно бизнесу

- Без сегментации зона поражения шифровальщика — вся сеть: простой офиса от 6 часов
- Гостевой Wi-Fi в общей сети = доступ посторонних устройств к 1С и файловым шарам
- Конфликты IP при удалёнке через VPN (192.168.1.0/24 дома и в офисе) — тикеты каждую неделю
- Логи доступа гостевого Wi-Fi обязаны храниться — без учёта сессий это риск для компании
- Недокументированная адресация: диагностика любой аварии начинается с археологии

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.x

RouterOS с bridge vlan-filtering=yes — один bridge на все порты, VLAN считает switch-чип

по докам help.mikrotik.com

5–7

VLAN по типам устройств: LAN, серверы, Wi-Fi-staff, VoIP, гости, камеры, management

наш стандарт

10.10.X.0/24

По /24 на VLAN из 10.0.0.0/8 — третий октет = VLAN ID, ноль конфликтов с домашними сетями

наш стандарт, RFC 1918

5 Мбит/с

Потолок на гостевого клиента через PCQ-очередь — один стриминг не съедает канал офиса

наш стандарт

1 ч

lease-time гостевого DHCP-пула против исчерпания адресов транзитными устройствами

наш стандарт

12 мес

Храним DHCP-leases и NAT-трансляции гостевой сети на внешнем syslog

требования законодательства РФ, наш syslog-шаблон

РЕАЛИЗАЦИЯ 1 ИЗ 3

Ядро: bridge VLAN filtering и default-deny

Что настраиваем

Роутер MikroTik RB5009 (RouterOS 7) + коммутаторы доступа, вся проводная сеть офиса

Как мы это делаем

1. В safe-mode собираем единый bridge, портам ставим pvid по роли; /interface bridge vlan — tagged на аплинки, untagged на access-порты
2. На access-портах включаем ingress-filtering=yes и frame-types=admit-only-untagged-and-priority-tagged — отсекаем VLAN hopping
3. Поднимаем /interface vlan на bridge (vlan10-lan…vlan99-mgmt), на каждом — /ip address .1/24 и свой DHCP-сервер со своим пулом
4. В /ip firewall filter chain=forward: точечные accept (LAN→1C tcp/1540-1591, LAN→NAS tcp/445), в конце drop 10.10.0.0/16→10.10.0.0/16
5. vlan-filtering=yes включаем последним шагом, уже сидя в management VLAN 99 — и только потом снимаем safe-mode

РЕЗУЛЬТАТ

Инцидент на рабочей станции остаётся внутри одного /24: до серверов долетают только явно разрешённые порты. Новое устройство в чужом сегменте не получает ничего — политика default-deny, а не default-allow.

КЛЮЧЕВОЙ НЮАНС

Порядок включения критичен: vlan-filtering до настройки management-доступа = локаут роутера. Мы всегда держим safe-mode и запасной access-порт в VLAN 99 до финальной проверки.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Wi-Fi: WPA3-Enterprise сотрудникам, изоляция гостям

Что настраиваем

Точки доступа MikroTik (пакет wifi-qcom, 802.11ax), два SSID на разных VLAN

Как мы это делаем

1. Два профиля /interface/wifi/configuration: staff и guest; в datapath каждого — vlan-id (30 и 50), трафик уходит тегированным в свой сегмент
2. Staff: security.authentication-types=wpa2-eap,wpa3-eap + aaa на RADIUS — User Manager v5 из RouterOS или Microsoft NPS при наличии AD (PEAP-MSCHAPv2)
3. Guest: WPA2/WPA3-PSK, в datapath client-isolation=yes — гостевые устройства не видят друг друга на L2
4. Гостям в chain=forward один accept в WAN и drop на 10.10.0.0/16; в chain=input режем доступ к самому роутеру кроме DHCP/DNS
5. Скорость гостей ограничиваем PCQ-очередью 5M/5M на 10.10.50.0/24; DHCP-leases и NAT шлём на syslog с хранением 12 месяцев

РЕЗУЛЬТАТ

Увольнение сотрудника = отключение учётки в AD, Wi-Fi гаснет сам — общий пароль не меняем и 30 человек не переподключаем. Гостевой сегмент закрывает требования: изоляция, лимит скорости, журналы сессий за год.

КЛЮЧЕВОЙ НЮАНС

В новом пакете wifi изоляция клиентов задаётся в datapath (client-isolation), а не галкой default-forwarding из старого wireless — при миграции точек на 802.11ax это проверяем первым делом.

РЕАЛИЗАЦИЯ 3 ИЗ 3

IP-план, DHCP static lease и документация

Что настраиваем

Адресный план всех VLAN + паспорт сети, передаваемый клиенту

Как мы это делаем

1. В каждом /24 фиксируем зоны: .1 шлюз, .2–.9 сетевое железо, .10–.49 серверы и статика, .50–.250 DHCP-пул, .251–.254 резерв
2. Принтеры, МФУ, камеры, СКУД сажаем на DHCP static lease по MAC (make-static) — адрес меняется в одной точке, не на каждой железке
3. Серверные адреса — вне DHCP-пула, руками, с записью в адресную таблицу в момент выдачи, а не «потом»
4. Паспорт сети: схема L1/L2 в draw.io, таблица IP/MAC/расположение, список VLAN с шлюзами; храним у клиента и у нас
5. После каждого изменения — /export file на роутере и выгрузка конфига в наше резервное хранилище

РЕЗУЛЬТАТ

Любой наш инженер (и админ клиента) за 5 минут понимает, что где стоит и куда подключено. Замена роутера по бэкапу конфига — час работы вместо дня реконструкции по памяти.

КЛЮЧЕВОЙ НЮАНС

Static lease на DHCP-сервере надёжнее статики на устройстве: при переносе принтера в другой VLAN правится одна строка на роутере. Документация короткая, но живая — протухшая таблица хуже её отсутствия.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **vlan-filtering включён до management VLAN**
  Мгновенный локаут роутера. Мы настраиваем всё в safe-mode, заводим VLAN 99 с адресом на bridge и включаем фильтрацию последним шагом.
- ✕ **frame-types=admit-all на access-портах**
  По умолчанию access-порт принимает и тегированные кадры — можно вбросить чужой VLAN-тег. Ставим frame-types=admit-only-untagged-and-priority-tagged +…
- ✕ **Гости отрезаны в forward, но не в input**
  Из гостевой сети остаётся доступ к Winbox/SSH самого роутера. Отдельно закрываем chain=input, оставляя гостям только DHCP и DNS.
- ✕ **Подсети 192.168.0.0/24 и 192.168.1.0/24**
  Совпадают с дефолтами домашних роутеров — VPN-клиенты ловят конфликт маршрутов. Берём только 10.10.X.0/24, X = VLAN ID.
- ✕ **Один DHCP на весь bridge**
  После сегментации клиенты получают адреса не своего сегмента. На каждый VLAN-интерфейс — свой /ip dhcp-server со своим пулом.
- ✕ **Статические IP прописаны на самих устройств…**
  Перенос принтера в другой VLAN превращается в обход по кабинетам. Используем DHCP static lease по MAC — правка в одной точке.
- ✕ **Сегментация есть, файрвола нет**
  RouterOS маршрутизирует между VLAN по умолчанию — «изоляция» иллюзорна. Всегда добавляем финальный drop inter-VLAN и точечные accept.
- ✕ **Общий WPA2-PSK для всех сотрудников**
  Пароль знают все, включая уволенных. Переводим staff-SSID на WPA2/WPA3-EAP с RADIUS (User Manager v5 или NPS + AD).

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Гостевой Wi-Fi в отдельном VLAN: только интернет, client-isolation, лимит скорости
- Серверы и NAS — в свой VLAN, доступ по списку портов, drop inter-VLAN в конце
- Адресация 10.10.X.0/24 вместо 192.168.0.0/24 и 192.168.1.0/24, план зон в каждом /24
- Актуальная таблица IP/MAC/VLAN и экспорт конфига после каждого изменения

НОРМАЛЬНО

- 5–7 VLAN по типам устройств: LAN, серверы, Wi-Fi, VoIP, гости, камеры, management
- Default-deny между всеми сегментами, ingress-filtering и frame-types на access-портах
- Static lease для принтеров, камер, СКУД; серверная статика вне DHCP-пула
- Syslog наружу: DHCP-leases и NAT гостевой сети с хранением 12 месяцев

ХОРОШО

- Staff Wi-Fi на WPA3-Enterprise: RADIUS (User Manager v5 / NPS + AD), учётки вместо P…
- Management VLAN 99: Winbox/SSH только из него, на остальных — drop в chain=input
- Мониторинг портов и линков (SNMP/Netwatch) с алертами в Telegram дежурному
- Паспорт сети L1/L2 + регламент изменений; бэкап конфига во внешнее хранилище

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Гость из гостевого Wi-Fi может открыть шару на NAS или веб-интерфейс камеры? (проверяли на практике, не по схем…
- [ ] Между VLAN стоит финальное правило drop, а разрешения — только точечные accept по портам?
- [ ] На access-портах включены ingress-filtering и frame-types против подмены VLAN-тега?
- [ ] Управление роутером и коммутаторами доступно только из management VLAN?
- [ ] Офисная адресация не пересекается с 192.168.0.0/24 и 192.168.1.0/24 домашних роутеров?
- [ ] Принтеры, камеры и СКУД закреплены static lease, а не статикой на устройствах?
- [ ] Сотрудники входят в Wi-Fi под личными учётками, а Wi-Fi уволенных гаснет вместе с учёткой AD?
- [ ] Логи DHCP и NAT гостевой сети пишутся на внешний syslog и хранятся 12 месяцев?
- [ ] Есть актуальная таблица IP/MAC/VLAN и свежий экспорт конфига роутера в бэкапе?
- [ ] Замену роутера можно выполнить по бэкапу конфига за час, без реконструкции по памяти?

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 текущей сети: карта устройств, найденные плоские сегменты и открытые порты, смета
- Проект и внедрение сегментации на MikroTik: VLAN, default-deny файрвол, миграция без простоя
- Гостевой и корпоративный Wi-Fi: изоляция, лимиты, WPA3-Enterprise с RADIUS под ваш AD
- IP-план и паспорт сети: схема, таблицы адресов, регламент изменений, бэкапы конфигов
- Дальнейшее сопровождение: мониторинг, журналы гостевых сессий, изменения по заявкам

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 Bridge VLAN Table, Bridging and Switching (help.mikrotik.com — ROS 7.x)

02 Layer2 misconfiguration (ingress-filtering, VLAN hopping) (help.mikrotik.com — ROS 7.x)

03 WiFi (wifi-qcom): configuration, security, datapath (help.mikrotik.com — ROS 7.x)

04 Enterprise wireless security with User Manager v5 (help.mikrotik.com — v5 / 7.x)

05 Network Policy Server: PEAP-MSCHAPv2 для Wi-Fi (learn.microsoft.com — WS2022)

06 RFC 1918 — Address Allocation for Private Internets (datatracker.ietf.org — 1996)

07 Шаблон IP-плана и паспорта сети ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.