

Отключение IPv6 в OpenWrt для Podkor

Устранение утечек трафика, сброса сессий нейросетей (ChatGPT / Gemini) и обхода VLESS-маршрутизации

Зачем отключать IPv6: В большинстве домашних конфигураций с Podkor туннелирование строится на базе IPv4. При активном IPv6 мобильные устройства (iOS, Android) и настольные браузеры по алгоритму *Happy Eyeballs* отдадут приоритет прямым IPv6-маршрутам домашнего провайдера в обход sing-box. Это приводит к деанонимизации узла, утечке DNS и сбросу сессий внешними защитными шлюзами.

Архитектура проблемы и механизм сбоя

1. Прямой обход прокси

Провайдер выдает динамический префикс IPv6. Запросы к доменам с AAAA-записями направляются напрямую в РФ-интернет минуя виртуальные интерфейсы Podkor.

2. Инвалидация сессий

Cloudflare и Google фиксируют несовпадение геолокаций: авторизационные токены идут через VLESS (IPv4), а фоновые WebSocket — через домашний IPv6.

Вариант 1. Пошаговая настройка в интерфейсе LuCI

1. Отключение служб раздачи IPv6 клиентам (LAN):

Перейдите в **Сеть (Network)** → **Интерфейсы (Interfaces)** → кнопка **Редактировать (Edit)** напротив интерфейса lan.

Откройте вкладку **Настройки DHCP-сервера** → вкладку **Настройки IPv6 (IPv6 Settings)**.

Установите значение «Отключено» (**Disabled**) для трех параметров:

- Служба Router Advertisement (*Router Advertisement-Service*)
- Служба DHCPv6 (*DHCPv6-Service*)
- NDP-прокси (*NDP-Proxy*)

Нажмите **Сохранить**.

2. Деактивация внешнего IPv6 WAN:

В общем списке интерфейсов найдите WAN6 (протокол *DHCPv6 client*).

Нажмите кнопку **Остановить (Stop)**, затем перейдите в свойства и выберите **Выключить (Disable)** либо полностью удалите интерфейс.

3. Очистка ULA-префикса (Локальный IPv6 пул):

В нижней части страницы **Сеть** → **Интерфейсы** найдите поле **IPv6 ULA-префикс (IPv6 ULA-Prefix)**.

Полностью удалите текстовое содержимое (оставьте поле абсолютно пустым).

4. Применение изменений:

Нажмите синюю кнопку **Сохранить и применить (Save & Apply)** в правом нижнем углу интерфейса.

Вариант 2. Экспресс-настройка через консоль (SSH)

Подключитесь к роутеру по SSH (например, `ssh root@192.168.1.1` или по внутреннему IP) и выполните команды пакетного отключения стека:

```
# 1. Деактивация раздачи IPv6 по локальной сети uci set dhcp.lan.dhcpv6='disabled' uci set
dhcp.lan.ra='disabled' uci set dhcp.lan.ndp='disabled' # 2. Очистка глобального уникального лока
льного префикса (ULA) uci set network.globals.ula_prefix='' # 3. Полное отключение внешнего интe
рфейса WAN6 uci set network.wan6.auto='0' 2>/dev/null uci set network.wan6.disabled='1' 2>/dev/n
ull # 4. Фиксация транзакций конфигуратора UCI uci commit dhcp uci commit network # 5. Остановка
демона odhcpd и перезапуск сетевой подсистемы /etc/init.d/odhcpd stop /etc/init.d/odhcpd disable
/etc/init.d/network restart /etc/init.d/dnsmasq restart
```

Методика валидации и тестирования

Точка проверки	Команда / Действие	Ожидаемый результат
Шлюз OpenWrt	В терминале роутера: <code>ifconfig br-lan</code>	<div>OK</div> Отсутствует глобальный <code>inet6 addr</code>
Рабочая станция	В терминале Windows: <code>ipconfig /all</code> или Linux <code>ip a</code>	<div>OK</div> IPv6-шлюз и DNS пусты
Мобильные клиенты	Переподключение Wi-Fi (или режим полета на 5 сек)	<div>OK</div> В свойствах сети только IPv4
Браузерная среда	Открыть сервис проверки: <code>https://test-ipv6.com</code>	<div>0/10</div> «IPv6 не обнаружен»

Дополнительная рекомендация для Podkop: Убедитесь, что в конфигурации каждого активного VLESS-подключения включена директива `domain_strategy: prefer_ipv4`, а в веб-интерфейсе активен чекбокс «Разрешение реальных IP-адресов» (Remote DNS resolving). Это исключит утечку DNS-пакетов при резолве зарубежных CDN.