

Протокол IPv6

будущее уже наступило

Who am I?

Алексей Чобан

- Опыт работы с сетями – 12 лет
- Опыт работы с Mikrotik – 11 лет
- Сертифицирован Mikrotik, Cisco



– системный интегратор
(Mikrotik, Cisco, Juniper, VoIP, Billing, IPTV)

Содержание



- Проблема исчерпания адресов IPv4. Методы решения.
- Описание протокола IPv6. Сравнение с IPv4.
- Формат адреса IPv6. Типы адресов IPv6.
- SLAAC, DHCPv6, статическая адресация
- DNS
- Проблемы IPv6
- Поддержка IPv6 в Mikrotik RouterOS
- Настройка туннеля 6to4
- Настройка Firewall, DNS
- Neighbor Discovery
- Домашнее задание
- Литература

Иерархия управления IP-адресами

IANA – Internet Assigned Numbers Authority
(Глобальное управление адресным пространством)



RIR – Regional Internet Registry
(ARIN, RIPE NCC, APNIC, LACNIC, AfriNIC)

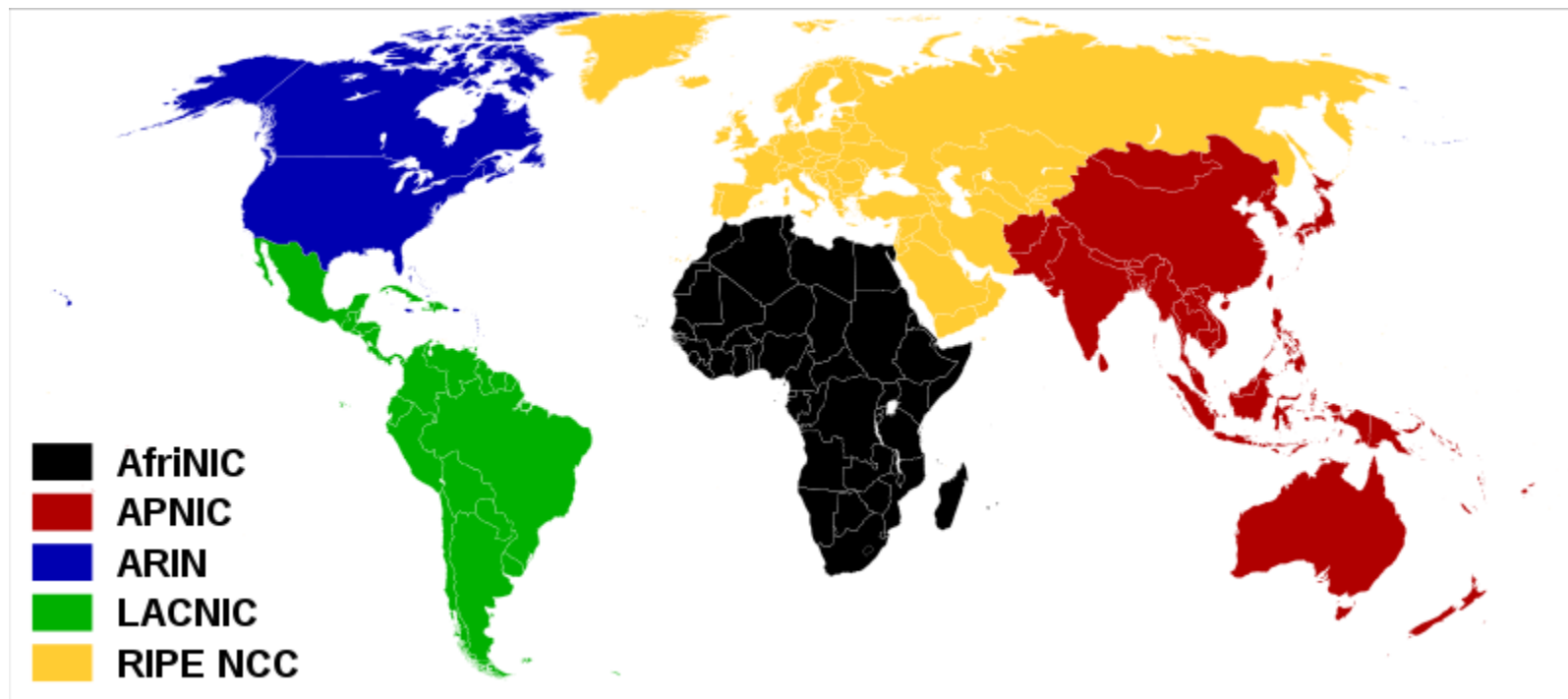


LIR – Local Internet Registry
(Провайдеры Интернет, IT-компании)



End-users – конечные пользователи
(Компании, физические лица)

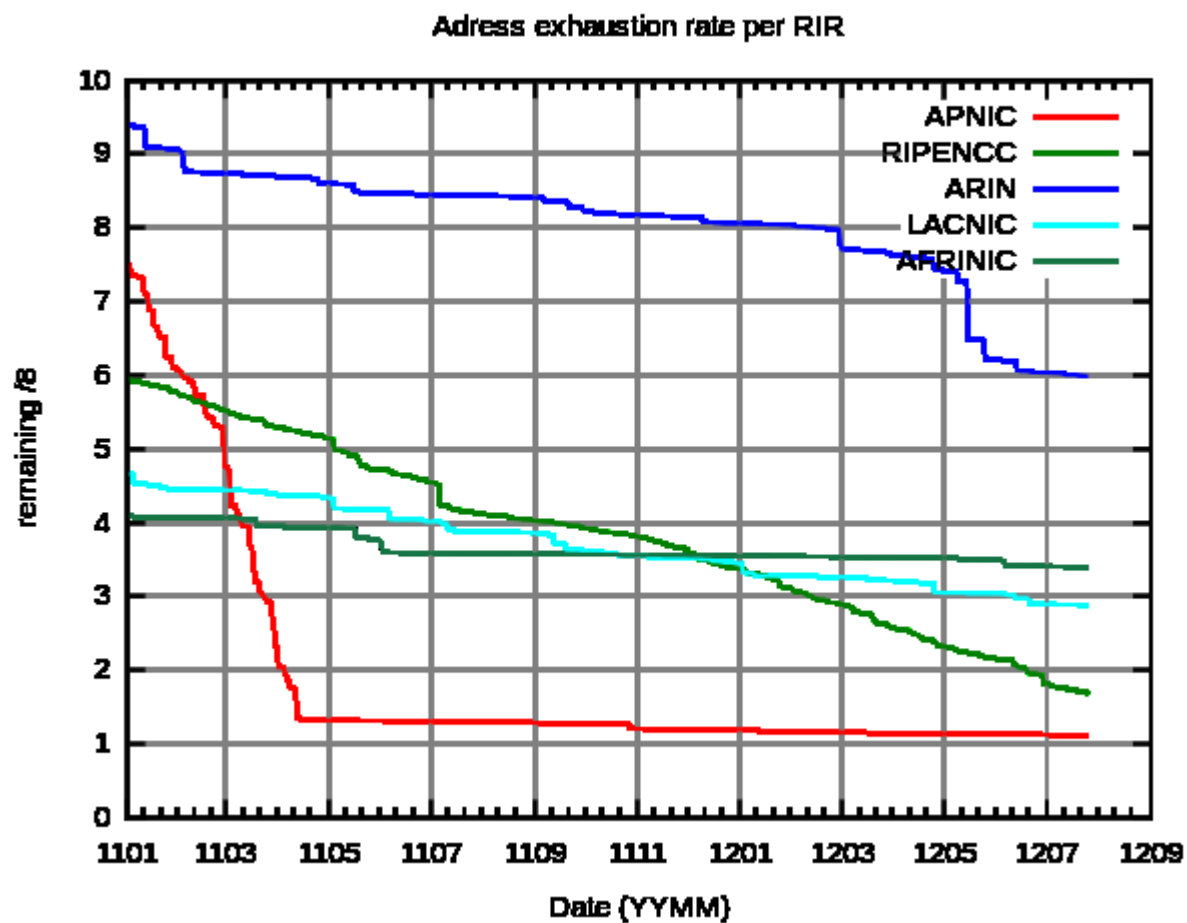
Зоны ответственности RIR



Ситуация с IPv4 сегодня

- Всего – $2^{32} = 4294967296$ адреса IPv4
- IANA – свободных адресов нет
- APNIC – ~1 блок /8
- RIPE NCC – ~1 блок /8
- ARIN – ~3 блока /8
- LACNIC – ~2 блока /8
- AfriNIC – ~3 блока /8
- Полное исчерпание в 2013-2014 годах
- APNIC, RIPE NCC, ARIN – в первой половине 2013

Исчерпание блоков у RIR



Методы экономии IPv4

- CIDR – Classless Inter Domain Routing -
уход от классов A,B,C
- NAT – Network Address Translation -
сокрытие частных адресов
- CGN – Carrier Grade NAT -
NAT44 на уровне ISP
- Таблетки от жадности для LIR и End-users -
строгий контроль расходования адресов

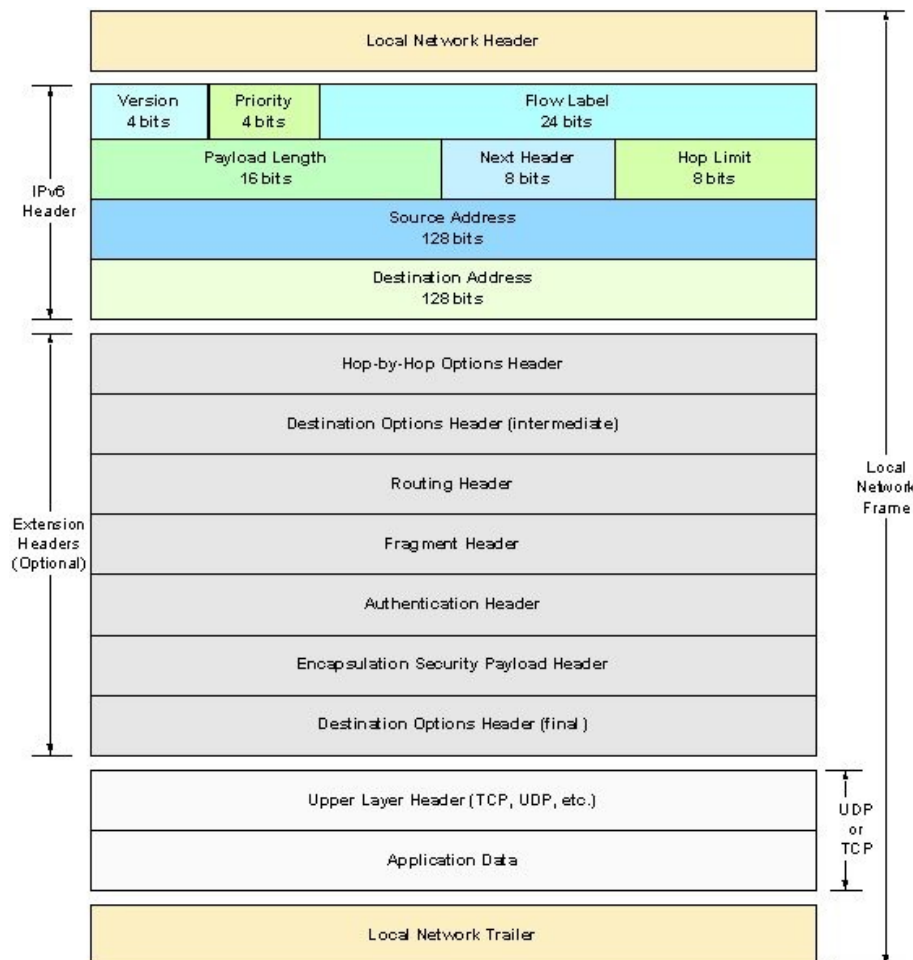
Пространство IPv4 ВСЕ РАВНО ИСЧЕРПАНО
IPv4 не выдается

IPv6 – конец света отменяется

- Длина адреса – 128 бит
- Общее кол-во адресов – 2^{128} = мноооооооого
- Встроенный IPSEC
- Встроенный QoS
- Можно использовать совместно с IPv4 – Dual Stack
- Оптимизирован формат пакета (нет checksum, нет fragmentation, label, etc)
- Авто-настройка адресов на хостах (SLAAC)
- Джамбограммы – размер пакета до 4-х гигабайт
- Уже поддерживается практически всеми сетевыми вендорами и операционными системами

Форматы пакетов

IPv6 vs IPv4



Byte 1	Byte 2	Byte 3	Byte 4
Ver=4	IHL=5	Type of Service	Total Length=472
Identification=111			Flag=0
Time=123		Protocol=6	Header Checksum
Source Address			
Destination Address			
Options			
Data			
Data			
Data			

Сравнение IPv4 и IPv6

Критерий	IPv4	IPv6
Кол-во бит	32	128
Кол-во адресов	2^{32}	2^{128} (в 10^{29} раз больше)
Единица адресации на пользователя	Хост /32	Сеть /64 ($1,8 \cdot 10^{19}$ хостов)
NAT	Есть	Нет необходимости
Настройка адресов на хостах	Static, DHCP	SLAAC, DHCPv6, Static
Формат записи	176.113.48.46	2a00:1450:4017:801::1003

Формат адреса IPv6

- Двоичное представление:

```
0010101000000000 0001010001010000 0100000000010111 0000100000000000  
0000000000000000 0000000000000000 0000000000000000 0001000000000010
```

- Шестнадцатеричное представление:

2a00:1450:4017:0800:0000:0000:0000:1002

- Шестнадцатеричное сокращенное представление:

2a00:1450:4017:800::1002

Важно: сокращать можно только одну группу нулей, иначе возникнет неопределенность в количестве нулей в адресе

- Маска подсети указывается только в сокращенном виде:

2a00:1450:4017:800::1002/64

- Использование в URL:

http://[2a00:1450:4017:800::1010]:8080/

Типы адресов IPv6

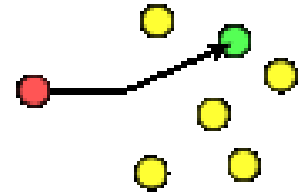
- Unicast
- Anycast
- Multicast

- Нет Broadcast => нет ARP
Функции протокола ARP заменены multicast-рассылкой при помощи протокола ICMPv6
(Stateless Address Autoconfiguration, Neighbor Discovery)

Unicast-адреса

- Global addresses

- Маршрутизируются в Интернете
- В данный момент используется блок 2000::/3
- Остальные зарезервированы для будущего использования



- Link-Local addresses

- Адресация в локальной сети
- Префикс FE80::/10 (чаще всего FE80::<EUI-64>/64)
- Аналог 169.254.0.0/16 в IPv4
- Маршрутизатор не перенаправляет трафик от этих адресов в другие сегменты
- Используется в SLAAC, Neighbor Discovery

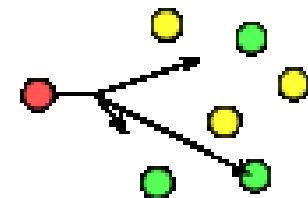
Unicast-адреса (продолж.)

- Unique-Local addresses
 - Префикс FC00::/64, FD00::/64
 - Аналог 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 (RFC1918)
 - На практике не используются
- Special purpose addresses
 - Unspecified address - ::/128 – аналог 0.0.0.0
 - Loopback address – ::1/128 – аналог 127.0.0.1
- Compatibility addresses
 - Инкапсуляция IPv6 в IPv4 или наоборот в гибридных сетях

Anycast и Multicast адреса

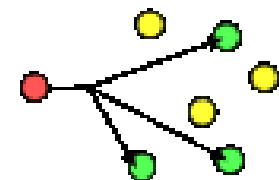
- Anycast addresses

- Неотличимы по виду от Unicast
- Используются для адресации множества хостов(интерфейсов)
- Пакет доставляется до ближайшего согласно маршрутной метрике интерфейса
- Используются в CDN



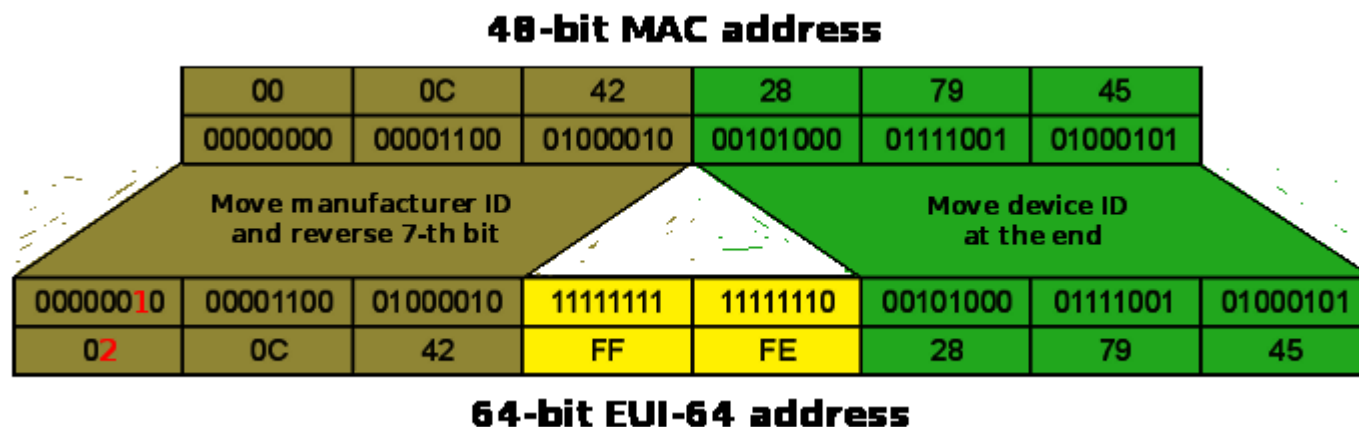
- Multicast addresses

- Префикс FF:: (FF02::5, FF02::6 – OSPF)
- Адресуют группу хостов (интерфейсов)
- Пакеты доставляются до всех хостов в multicast-группе
- Замена Broadcast (Neighbor Discovery, Stateless Address Autoconf.)



Идентификатор интерфейса, EUI-64

- Максимальный префикс подсети - /64 =>
 - младшие 64 бита – хостовая часть адреса (идентификатор интерфейса)
 - 2^{64} вариантов
- Методы определения хостовой части
 - EUI-64 – Extended Unique Identifier
 - Случайным образом – для безопасности, по умолчанию в Windows
 - Вручную



Stateless Address Autoconfiguration (SLAAC)

- Очень простой метод авто-настройки адресов IPv6
 - Аналог APIPA – 169.254.0.0/16 в IPv4
 - Работает только с префиксом /64
 - Нет Broadcast (ARP), поэтому используется Multicast
 - Похож на OSPF
 - RADVD
 - ICMPv6
1. При включении хост присваивает себе link-local адрес (FE80::/64 или FE80::/64) = > LAN работает
 2. Если обнаружен конфликт IP – интерфейс отключается
 3. Хост начинает рассылать ICMPv6 “Router Solicitation”
 4. Маршрутизатор с настроенным анонсом глобального префикса рассылает ICMPv6 “Router Advertisement” всем хостам по Multicast и ответы на “Router Solicitation” по Unicast
 5. RA содержит информацию о глобальном префиксе, default gw, DNS, MTU, Lifetime, etc
 6. Хост присваивает себе глобальный адрес на основе префикса в сочетании с EUI-64 или random

DHCPv6, Статическая адресация

DHCPv6

- Рекомендуется использовать для большего контроля сети
- Позволяет передать доп. опции (bootfile,NTP,DNS)
- Больше подходит для ISP и Enterprise
- Работает с любым префиксом (с некоторыми ограничениями)

Static

- Ручная настройка адреса на интерфейсе
- Работает с любым префиксом
- Используется в не-multicast средах

DNS в IPv6

Прямые зоны (Forward zones)

- Используются записи типа AAAA
- В зонах DNS можно сочетать IPv4 (A) и IPv6 (AAAA) адреса

```
time<--><-----><----->A<----->212.56.198.26  
ipv6.time<-----><----->AAAA<-->2a00:1450:4017:800::1002
```

Обратные зоны (Reverse zones)

- Записи создаются в домене ip6.arpa (in-addr.arpa в IPv4)
- **Полный** адрес записывается в обратном направлении
2a00:1450:4017:0800:0000:0000:0000:1002 ->
2.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.7.1.0.4.0.5.4.1.0.0.a.2.ip6.arpa.

```
$ORIGIN 0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.7.1.0.4.0.5.4.1.0.0.a.2.ip6.arpa.  
2.0.0.0><-----><----->IN PTR ipv6.time.it-lab.md.
```

Проблемы IPv6

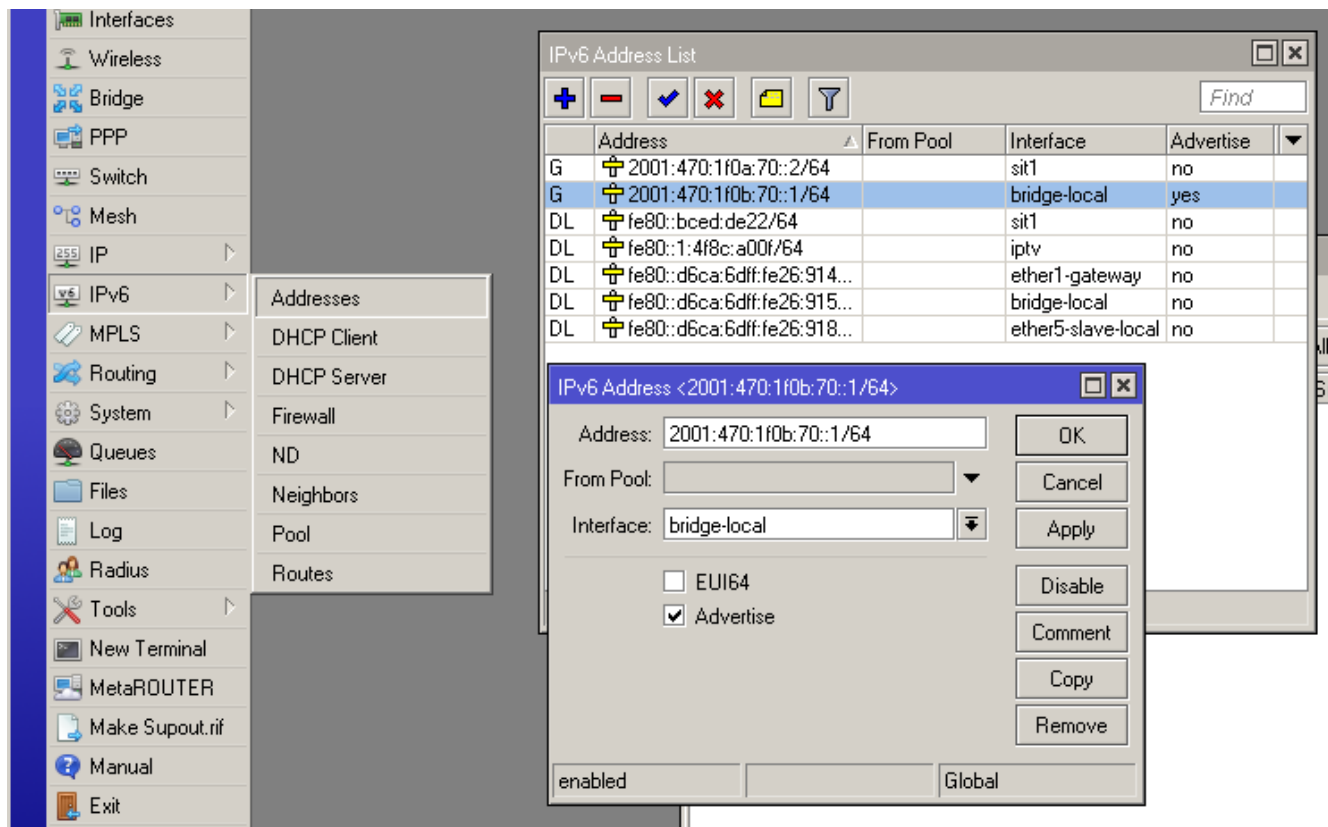
- Не запомнишь свой домашний (офисный, и т.д.) IP
- Сложно работать с адресами => утилиты для работы с IPv6:
 - http://www.gestioip.net/cgi-bin/subnet_calculator.cgi
- **Отсутствует NAT => обязательно firewall**
- «Чужие» маршрутизаторы с RA, DHCPv6 в сети => контроль на коммутаторах
- Стыковка IPv4 и IPv6 => Dual Stack, CGN NAT64 (поддержка в RouterOS?), 6rd, 6to4
- Сложный troubleshooting, так как нет четкого разделения функций протоколов по уровням OSI => используйте IPv4
- Не все вендоры оборудования и ОС поддерживают IPv6 (либо только частично)
- Низкий уровень подготовки IT-специалистов по IPv6
- Сложно организовать миграцию в крупных сетях (ISP, Enterprise) из-за разнородного оборудования и пересечения зон ответственности

IPv6 в Mikrotik RouterOS

- Установите пакет ipv6
- Полноценная поддержка: SLAAC, ND, EUI-64, Firewall, DNS, DHCPv6, OSPFv3, BGP
- Все настройки в меню /ipv6
- Режимы подключения к глобальному IPv6:
 - native IPv6 – прямое подключение к сети IPv6.
просите у своего ISP для тестирования или продакшна
 - tunneled IPv6, 6to4 – подключение через туннельных брокеров поверх IPv4.
подходит для подготовки и тестирования работы IPv6 у вас

Link-local и статические адреса

- Advertise включает RA
- L – link-local, D – dynamic, G – global



Настройка туннеля 6to4

- Рекомендуется tunnelbroker.net:

- много узлов по миру
- бесплатно
- очень быстро и просто
- префикс /64 или /48

Tunnel Details

IPv6 Tunnel

Example Configurations

Advanced

Tunnel ID: 185920

Creation Date:

Description:

Delete Tunnel

Dec 1, 2012

IPv6 Tunnel Endpoints

Server IPv4 Address:

Server IPv6 Address:

Client IPv4 Address:

Client IPv6 Address:

216.66.80.30

2001:470:1f0a:70::1/64

188.237.222.34

2001:470:1f0a:70::2/64

Available DNS Resolvers

Anycasted IPv6 Caching Nameserver:

Anycasted IPv4 Caching Nameserver:

2001:470:20::2

74.82.42.42

Routed IPv6 Prefixes

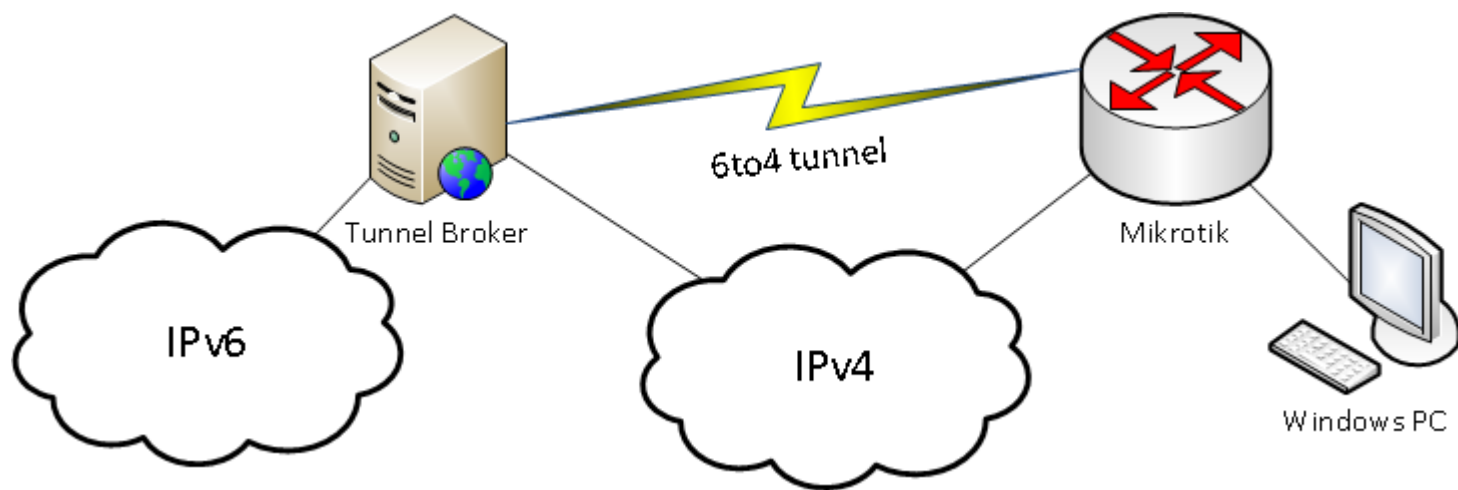
Routed /64:

Routed /48:

2001:470:1f0b:70::/64

2001:470:708a::/48 **[X]**

Схема стенда



Настройка туннеля 6to4 (продолж.)

- Добавляем туннель 6to4:
`/interface 6to4 add comment="IPv6 tunnel" local-address=188.237.222.34 mtu=1280
name=sit1 remote-address= 216.66.80.90`
- Прописываем пиринговый IPv6-адрес и маршрут по-умолчанию:
`/ipv6 address add address=2001:470:1f0a:70::2/64 advertise=no eui-64=no
interface=sit1
/ipv6 route add dst-address=::/0 gateway=2001:470:1f0a:70::1`
- Прописываем выданный IPv6-префикс на внутреннем интерфейсе:
`/ipv6 address add address=2001:470:1f0b:70::1/64 advertise=yes eui-64=no
interface=bridge-local`
- Проверяем наличие глобального IPv6-адреса на хостах внутри сети:
 - Windows – `ipconfig /all`
 - *nix - `ifconfig`
- Обратите внимание, что Link-local адрес на хосте сохраняется.
Default gw является Link-local адрес маршрутизатора, а не Global

Firewall, DNS в IPv6

- Настройка firewall идентична IPv4, поддерживаются address-list, mangle(только для QoS, нет policy routing):

```
/ipv6 firewall address-list
```

```
add address=2001:470:1f0b:70::2/128 disabled=no list=MyHost
```

```
/ipv6 firewall filter
```

```
add action=accept chain=forward disabled=no dst-address-list=MyHost dst-port=80  
protocol=tcp src-address=::/0
```

```
add action=accept chain=forward disabled=no dst-address-list=MyHost dst-port=53  
protocol=udp
```

```
add action=accept chain=forward disabled=no dst-address-list=MyHost dst-port=53  
protocol=tcp
```

- DNS-сервер полноценно поддерживает IPv6:

```
/ip dns set servers=2001:470:1f0b:70::2 allow-remote-requests=yes
```

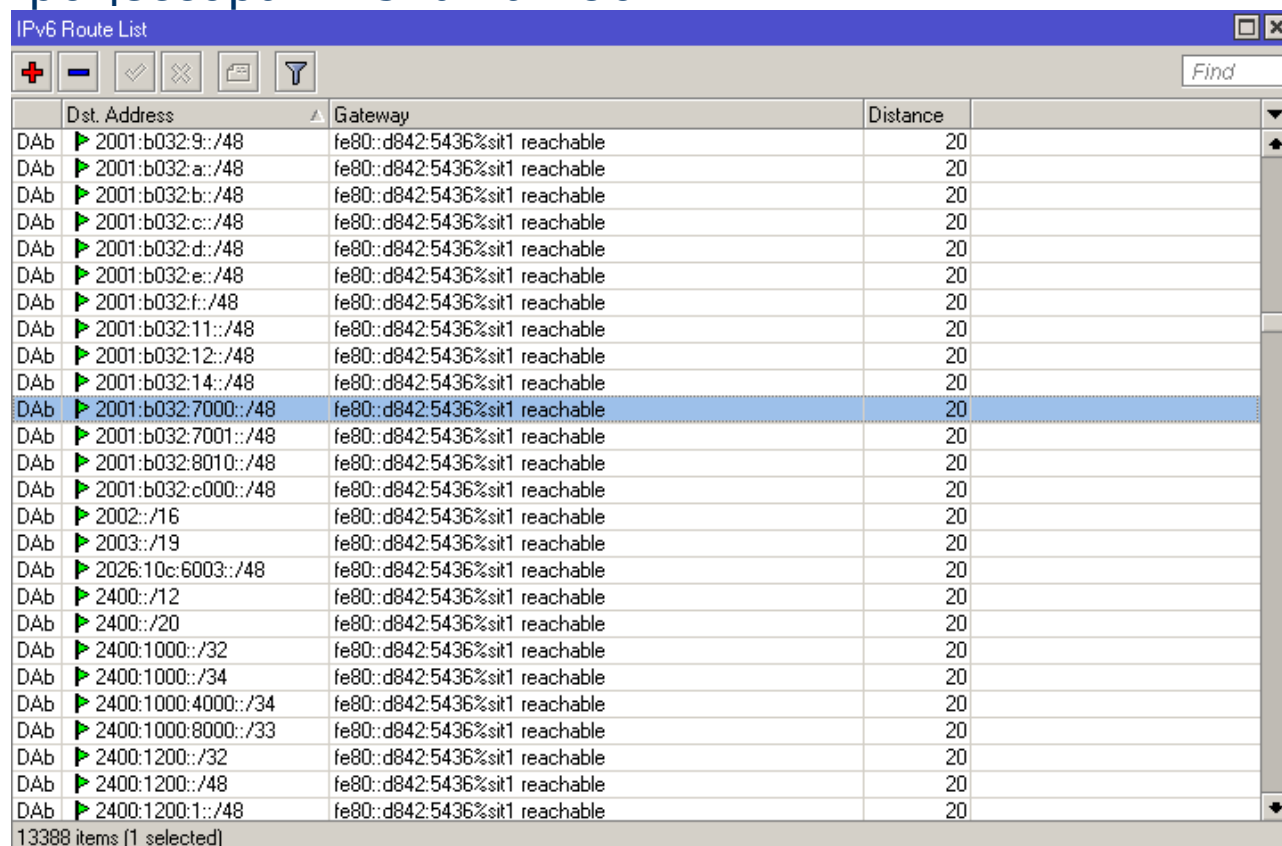
Neighbor Discovery

- Нет ARP
 - RouterOS использует RADVD для обнаружения соседей
 - С помощью RA сообщений протокола ICMPv6 хостам анонсируются Global prefix, DNS, default gw
 - Управление анонсами RA:
 - /ipv6 nd set ...
 - Просмотр хостов-соседей:
 - /ipv6 neighbor print
- Flags: R - router
- ```
0 address=2001:470:1f0b:70:1ab:2458:e911:2a5d interface=bridge-local
mac-address=E0:B9:A5:9E:63:C5 status="stale"
```

The screenshot shows the 'ND <bridge-local>' configuration window in RouterOS. The interface is set to 'bridge-local'. The RA Interval is 200-600, RA Delay is 3, and RA Lifetime is 1800. The MTU, Reachable Time, and Retransmit Interval are set to their default values. The Hop Limit is also set to its default. The 'Advertise MAC Address' and 'Advertise DNS' checkboxes are checked, while 'Managed Address Configuration' and 'Other Configuration' are unchecked. The window includes buttons for OK, Cancel, Apply, Disable, Copy, and Remove. At the bottom, there are status indicators for 'enabled' and 'default'.

# BGP6 в Mikrotik

- Full BGP на Mikrotik – 13388 префиксов
- Загрузка процессора 2-3% на x86



| Dst. Address              | Gateway                        | Distance |
|---------------------------|--------------------------------|----------|
| DAb ▶ 2001:b032:9::/48    | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:a::/48    | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:b::/48    | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:c::/48    | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:d::/48    | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:e::/48    | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:f::/48    | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:11::/48   | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:12::/48   | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:14::/48   | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:7000::/48 | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:7001::/48 | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:8010::/48 | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2001:b032:c000::/48 | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2002::/16           | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2003::/19           | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2026:10c:6003::/48  | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400::/12           | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400::/20           | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400:1000::/32      | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400:1000::/34      | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400:1000:4000::/34 | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400:1000:8000::/33 | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400:1200::/32      | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400:1200::/48      | fe80::d842:5436%sit1 reachable | 20       |
| DAb ▶ 2400:1200:1::/48    | fe80::d842:5436%sit1 reachable | 20       |

13388 items (1 selected)

# Домашнее задание

- Читайте материал по IPv6
- Тестируйте в своей сети IPv6 через туннельного брокера или своего ISP
- Делайте апгрейд оборудования и софта для полной поддержки IPv6
- Обучайте IT-специалистов
- Создавайте план внедрения IPv6
- Если Вы – ISP, предыдущие пункты выполнять каждый день.  
(DHCPv6, 6rd, CGN NAT64, Dual Stack)

# Литература

- Google.com
- <http://ru.wikipedia.org/wiki/IPv6>
- <http://wiki.mikrotik.com/wiki/Manual:IPv6/Address>
- <http://ru.wikipedia.org/wiki/ICMPv6>
- [http://www.gestioip.net/cgi-bin/subnet\\_calculator.cgi](http://www.gestioip.net/cgi-bin/subnet_calculator.cgi)
- <http://tunnelbroker.net>
- [http://en.wikipedia.org/wiki/List of IPv6 tunnel brokers](http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers)

**Алексей Чобан**

**ac@it-lab.md**

**http://www.it-lab.md**

**+373 69999975**