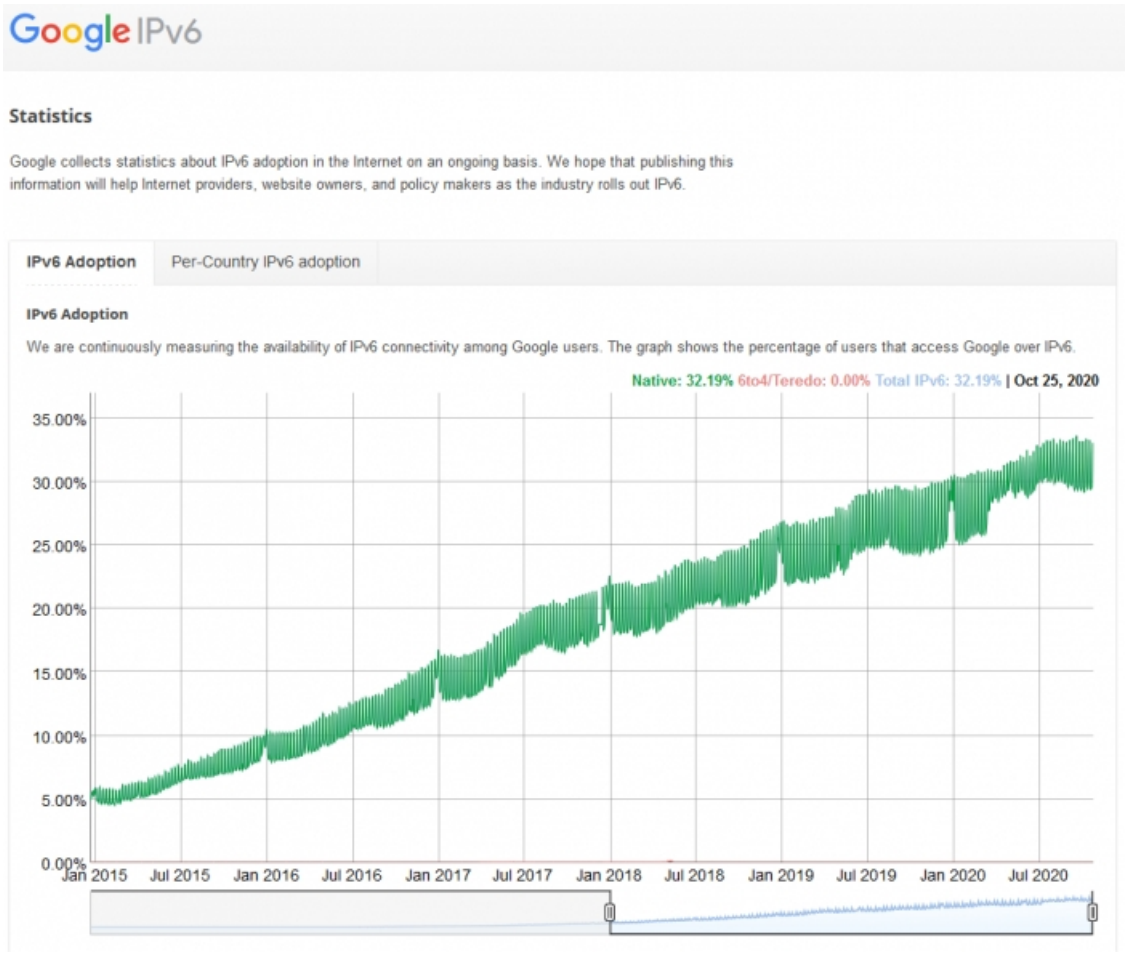
IPv6 на коммутаторах доступа SNR

Введение

Сегодня мы решили затронуть тему настройки IPv6 на коммутаторах доступа SNR. Не станем писать банальностей, вроде "IPv4-адреса заканчиваются", но вспомним Республику Беларусь, где уже около года действует закон об обязательном предоставлении абонентам IPv6-адресов. Обратимся к статистике Google, которая фиксирует рост доли IPv6 в мировом сетевом трафике с 5,5% в январе 2015 до 32% в октябре 2020. Согласитесь, не взрывной, но уверенный рост. Предоставление IPv6-адресов также может стать конкурентным преимуществом для операторов связи, это можно использовать в целях маркетинга.



Статистика Google по использованию IPv6 в мировом сетевом трафике

Краткий обзор IPv6

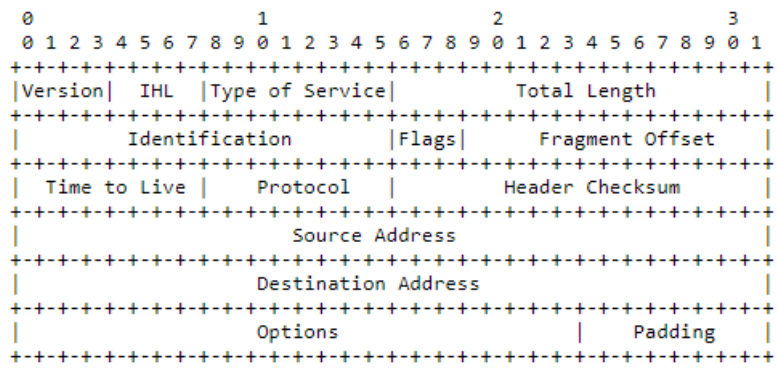
Протокол сетевого уровня IPv6 (RFC 8200) решает не только проблему нехватки классических IP-адресов. Многие механизмы в нем пересмотрены, что-то оптимизировали, от чего-то отказались. Увеличение длины IP-адреса с 32 до 128 бит - пожалуй, наименьшее из изменений.

Ключевые отличия от IPv4

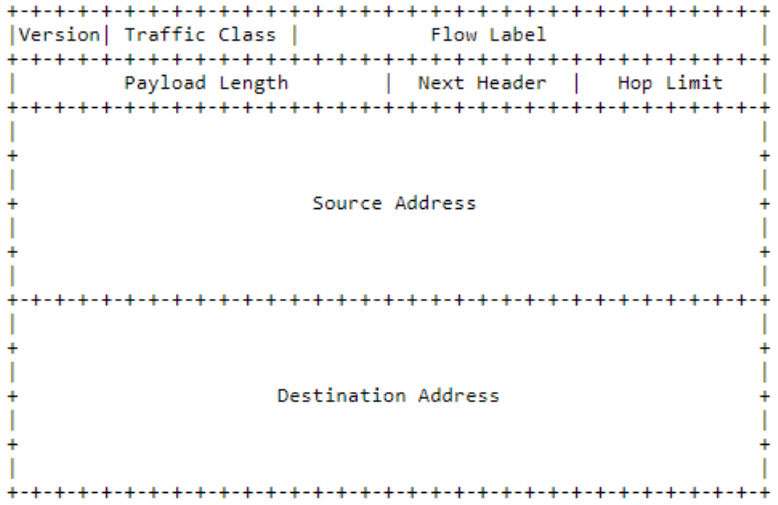
- Полностью переработан заголовок IP-пакета.
- Полный отказ от бродкаста в пользу мультикаста.
- Отказ от классов сетей.
- На смену протоколу ARP пришел Neighbor Discovery Protocol (NDP).
- Добавлен механизм SLAAC, позволяющий получить уникальный, глобально маршрутизируемый IPv6-адрес без использования какого-либо DHCP-сервера.
- Добавлен механизм Prefix Delegation, позволяющий CPE анонсировать префикс оператора связи, а IPv6-хосту генерировать себе на его основе адрес.
- В силу количества IPv6-адресов NAT становится не нужен.
- Введены новые типы сетевых адресов.
- Вместо маски подсети используется только длина префикса.

Заголовок IPv6

Сравним заголовки IPv4 и IPv6-пакетов, используя картинки прямо из RFC:



Заголовок пакета IPv4

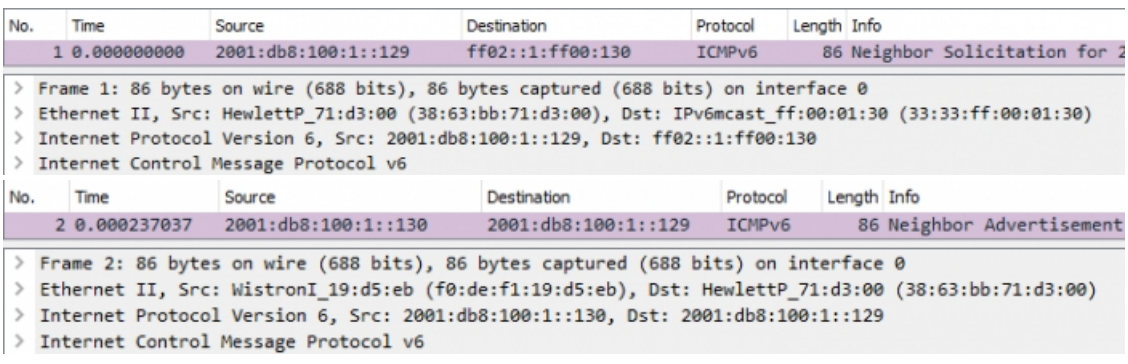


Заголовок пакета IPv6

Можно заметить, что в новой версии протокола заголовок заметно упростился за счет использования меньшего количества полей. Разработчики посчитали, что на современном оборудовании часть из них просто не нужна. Например, нет смысла считать контрольную сумму, если это уже сделано на канальном уровне и будет сделано на транспортном. Т.к. IPv6-заголовок имеет фиксированную длину 40 байт, то и в поле IHL (Internet Header Length) больше нет смысла и т.д. Добавлено совершенно новое поле ‘IPv6 Flow Label’, служащее для упрощения маршрутизации пакетов одного потока (RFC 6437).

Neighbor Discovery Protocol вместо ARP

В IPv6 произошел полный отказ от протокола ARP, его функции взял на себя NDP. Он, в свою очередь, является частью протокола ICMPv6. Для определения MAC-адреса хоста протокол ARP использует ARP-Request и ARP-Reply сообщения, рассылаемые бродкастом. Подобным образом действует NDP через Neighbor Solicitation (NS) и Neighbor Advertisement сообщения, но делает это мультикастом. Давайте рассмотрим этот процесс подробнее в анализаторе трафика Wireshark:



ПК1 посылает в сеть мультикастовое NS-сообщение с вопросом "какой MAC-адрес у хоста 2001:db8:100::130"? ПК2 получает его, понимает, что сообщение предназначено для него. Далее формирует NA-сообщение с ответом и отвечает юникастом на IPv6-адрес отправителя. Но как этот процесс достигается, если не использовать широковещательный запрос? Существует зарезервированный IPv6 мультикастовый адрес ff02::1, который "слушают" все IPv6-хосты, но чем тогда это будет отличаться от broadcast? Ничем. Для NS-сообщений, в качестве адреса назначения, используется специальный мультикастовый адрес, который рассчитывается на основе искомого IPv6-адреса. Такой адрес начинается с ff02::1:ff00:0/104, последние 24 бита формируются из последних 24 битов искомого адреса. Например, если мы в NS-сообщении спрашиваем "кто имеет IPv6-адрес 2001:db8:100::130?", то в качестве адреса назначения будет использоваться ff02::1:ff00:130, это называется solicited-node multicast address. В свою очередь хост с адресом 2001:db8:100::130 "слушает" мультикаст-группу ff02::1:ff00:130. Такой метод допускает теоретическую ситуацию, когда несколько хостов будут "слушать" одинаковую группу и получать NS-сообщения им не предназначенные. Но это все равно намного более оптимальный алгоритм, чем broadcast. Сам же этот solicited-node multicast address на канальном уровне привязывается к мультикастовому MAC-адресу 33:33:ff:00:01:30, где ff:00:01:30 - последние 32 бита solicited-node адреса.

Типы IPv6 адресов

Если в IPv4 было, условно говоря, два типа юникастовых IP-адресов - внешние и внутренние, то в IPv6 их три:

- Global Unicast Address - аналог внешнего IPv4-адреса;
- Link-Local Unicast Address - совершенно новый тип служебных IP-адресов, служащих для взаимодействия протоколов;
- Unique Local Addresses - аналог внутреннего IPv4-адреса.

Рассмотрим подробнее Link-Local Unicast Address. Такие адреса всегда начинаются на fe80, остальная часть генерируется автоматически, обычно на основе MAC-адреса. Должны быть уникальными только в пределах одной канальной среды, т.к. не маршрутизируются. Любой IPv6-хост в сети обязан иметь Link-Local Unicast адрес. Используется для обмена некоторыми типами сообщений в таких протоколах, как ICMPv6, DHCPv6, OSPFv3 и т.д. Является next-hop адресом для протоколов динамической маршрутизации и используется для указания шлюза по умолчанию для хостов.

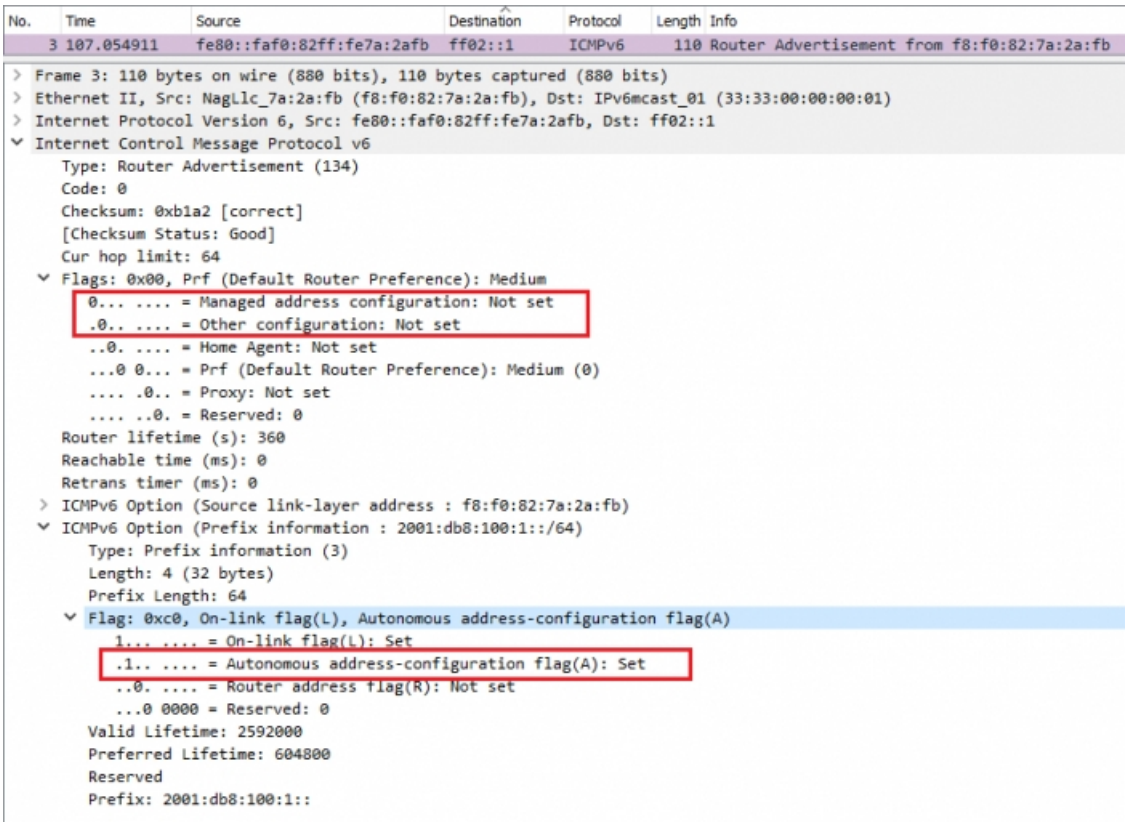
Методы динамической конфигурации IPv6-адреса

Протокол DHCP также подвергся серьезной переработке в его IPv6-версии. Теперь есть три способа автоматически получить сетевой адрес:

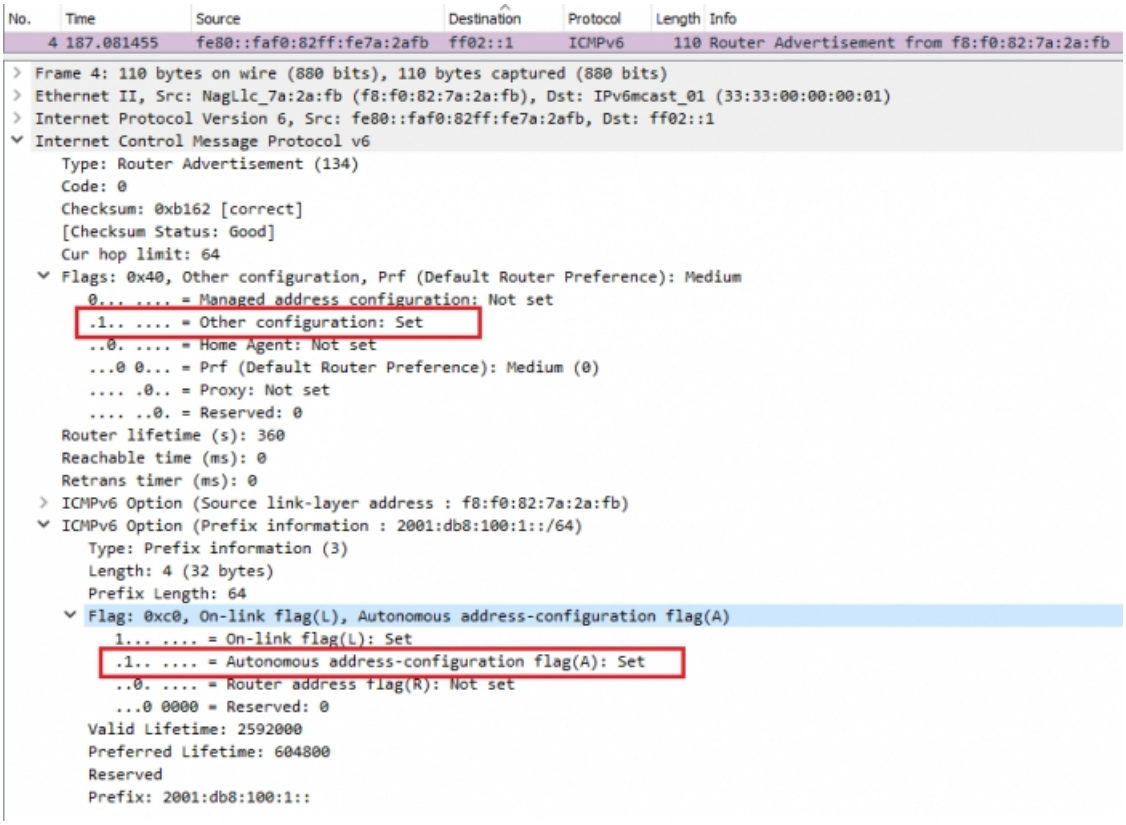
- Stateless Address Autoconfiguration (SLAAC).
- Stateless DHCPv6.
- Stateful DHCPv6.

Если раньше этот процесс всегда происходил только между клиентом и сервером, то теперь появляется третий необходимый участник - маршрутизатор. Он периодически рассылает по сети ICMPv6-RA (Router Advertisement)-сообщения или отвечает ими на ICMPv6-RS (Router Solicitation)-сообщения. Главными для нас являются значения полей A Flag, O Flag и M Flag, которые могут быть 0 или 1. Именно на этой основе хост-клиент принимает решение, какой тип динамического IPv6-адреса ему использовать.

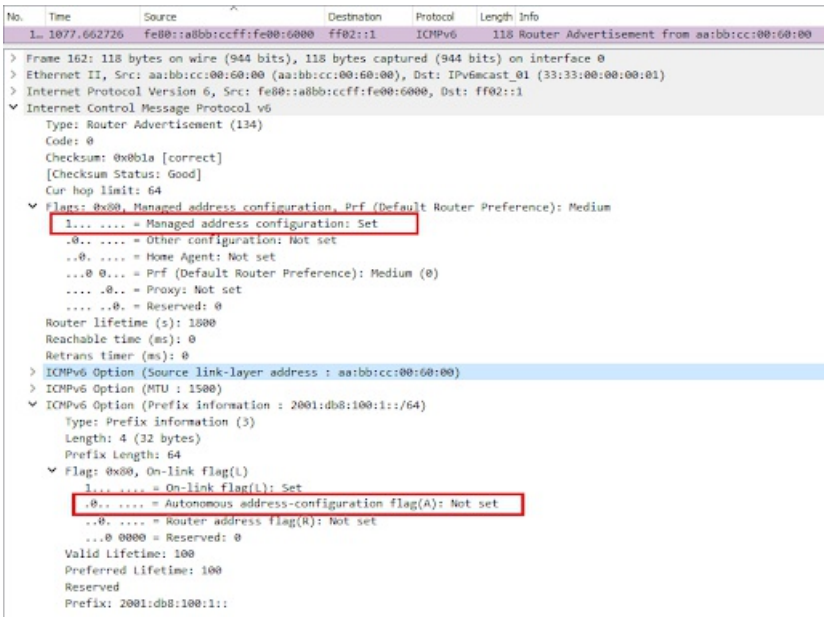
SLAAC. Получая RA-сообщение с активным A-флагом, клиент сам формирует себе IPv6-адрес. Первые 64 бита берутся из поля "Prefix information" остальные формируются либо методом EUI-64, либо случайным образом. Заметьте, что DHCPv6-сервер тут вообще не используется.



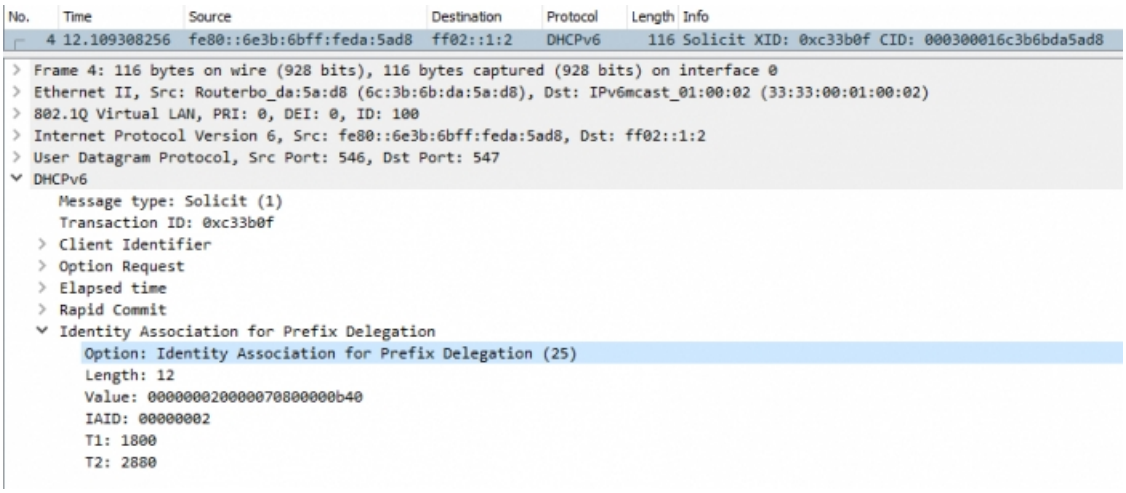
Stateless DHCPv6. Минус метода SLAAC в том, что мы имеем только свой IPv6-адрес и адрес шлюза по умолчанию. Но если мы хотим автоматически получать и информацию о DNS серверах и другую информацию? Тогда в RA-сообщениях, помимо A-флага, также будет активным O-флаг. Получая такое сообщение хост также будет формировать свой IPv6-адрес сам, но еще обратится по специальному мультикастовому адресу ff02:1:2 к ближайшему DHCPv6-серверу за дополнительными реквизитами.

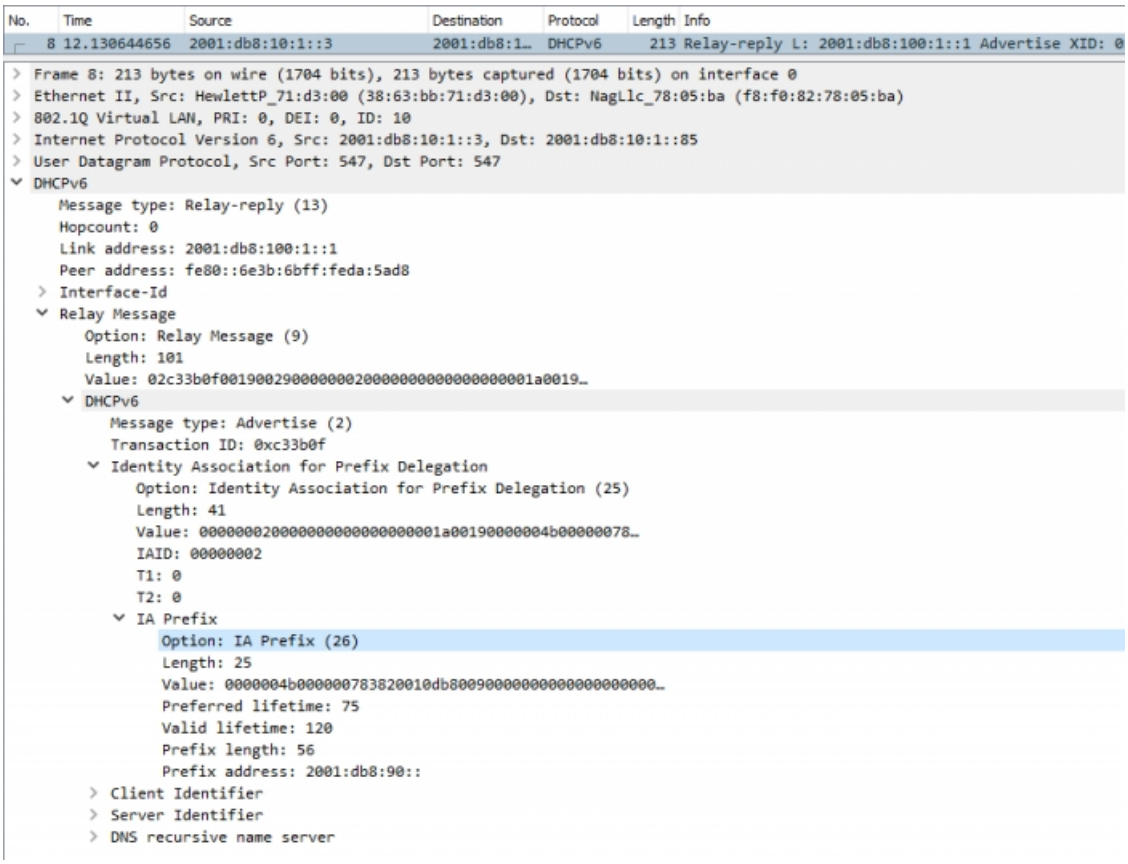


Stateful DHCPv6. Это, по-сути, классический метод получения IPv6-адреса динамическим способом, к которому мы привыкли в IPv4. Сервер выделяет адреса из пулов, может ориентироваться при этом на опции 18 (interface-id), 37 (remote-id) и 38 (subscriber-id). Чтобы использовать Stateful DHCPv6, мы должны анонсировать в RA-сообщениях только M-флаг.



Prefix Delegation. При данном методе мы имеем дело с двумя маршрутизаторами. Абонентский (CPE) является запрашивающим и отправляет DHCPv6 Solicit-сообщение делегирующему. Последний отправляет ответ в виде делегированного префикса. Обычно его длина /56, это является рекомендацией RFC 6177. CPE сам добавляет к префиксу недостающие 8 бит и в Advertise-сообщении анонсирует стандартный /64 префикс. Рассмотрим этот процесс в Wireshark. Запрашивающий маршрутизатор отправляет делегирующему DHCPv6 Solicit-сообщение с опцией 25, которая сигнализирует о желании использовать Prefix Delegation. Сервер отвечает Advertise-сообщением с опцией 26, где содержится делегируемый префикс с его длиной. При этом CPE, в зависимости от настроек, анонсирует либо A, либо A+O флаги. Следовательно, клиент генерирует себе IPv6-адрес сам, на основе префикса.





Основные настройки IPv6 на коммутаторах SNR

Разобравшись с теорией, можно переходить к практике. Рассмотрим базовые настройки IPv6 на коммутаторах доступа SNR.

Хочется отметить, что все управляемые коммутаторы SNR, от FastEthernet моделей, таких как SNR-S2985G-24TC, до гигабитных коммутаторов с 10Г аплинками (SNR-S2989G-24TX), поддерживают одинаковый функционал и имеют одинаковые настройки в части IPv6.

Назначить IPv6-адрес управления

Назначить адрес L3-интерфейсу можно несколькими методами. Полностью указать его с длиной префикса, использовать метод EUI-64 или использовать DHCPv6-клиент. Последний способ требует предварительно внесения в конфигурацию строки ‘service dhcpv6’. Рассмотрим все три способа на трех VLAN-интерфейсах:

```
Switch(config)#service dhcpv6
Switch(config)#int vlan1
Switch(config-if-vlan1)#ipv6 address 2001:db8:100:1::1/64
Switch(config-if-vlan1)#int vlan2
Switch(config-if-vlan2)#ipv6 address 2001:db8:100:2::/64 eui-64
Switch(config-if-vlan1)#int vlan3
Switch(config-if-vlan2)#ipv6 dhcp-client enable
```

Проверим результат:

```
Switch#sh ipv6 interface brief
Vlan1                                   [up]
    2001:db8:100:1::1/64
    fe80::faf0:82ff:fe78:5ba/64
Vlan2                                   [up]
    2001:db8:100:2:faf0:82ff:fe78:5ba/64
    fe80::faf0:82ff:fe78:5ba/64
Vlan3                                   [up]
    2001:db8:100:3::100/64
    fe80::faf0:82ff:fe78:5ba/64
Loopback                                [up]
    ::1/128
```

Задать статическую IPv6 neighbor-запись

Полностью аналогично статической ARP-записи и производится из-под VLAN-интерфейса.

```
Switch(config)#int vlan1
Switch(config-if-vlan1)#ipv6 neighbor 2001:db8:100:1::10 f0-de-f1-19-d5-eb interface e1/0/2
```

Проверим результат:

```
Switch#sh ipv6 neighbors
IPv6 neighbour unicast items: 4, valid: 3, matched: 3, incomplete: 0, delayed: 0, manage items: 0
IPv6 Address                    Hardware Addr       Interface     Port              State       Age-time(sec)
2001:db8:100:1::3               38-63-bb-71-d3-00   Vlan1         Ethernet1/0/8     reachable   1168
2001:db8:100:1::10              f0-de-f1-19-d5-eb   Vlan1         Ethernet1/0/2     permanent
fe80::f1ed:8839:4a8:13fc        38-63-bb-71-d3-00   Vlan1         Ethernet1/0/8     reachable   1192
```

Настроить DHCPv6 Relay

```
Switch(config)#service dhcpv6
Switch(config)#int vlan10
Switch(config-if-vlan10)#ipv6 dhcp relay destination 2001:db8:100:1::1
```

Security RA и его использование

Если RA-сообщения будет посылать IPv6-хост злоумышленника, то может выйти так, что клиентский ПК будет использовать его link-local адрес, как шлюз по умолчанию. Также злоумышленник может анонсировать неверный IPv6-префикс и его длину. Защититься от этого поможет функционал Security RA. Включим настройку глобально и запретим на абонентских портах RA-сообщения:

```
Switch(config)#ipv6 security-ra enable
Switch(config)#int e1/0/1-24
Switch(config-if-port-range)#ipv6 security-ra enable
```

Такие сообщения теперь могут приходить только с аплинков e1/0/25-28. Проверим конфигурацию Security RA:

```
Switch#sh ipv6 security-ra
IPv6 security RA information:
Global IPv6 Security RA State: enabled
Ethernet1/0/1
IPv6 Security RA State: Yes
Ethernet1/0/2
IPv6 Security RA State: Yes
...
```

Важно отметить, что механизмы защиты Security RA и SAVI являются взаимоисключающими.

SAVI и DHCPv6 Snooping

SAVI (Source Address Validation Improvement) включает в себя ND Snooping, DHCPv6 Snooping и RA Snooping. Он позволяет защищаться от нелегитимных DHCPv6-серверов и источников RA-сообщений с помощью знакомых нам доверенных портов. Выдаваемые IPv6-адреса и префиксы, привязываются к MAC-адресам и портам в биндинг-таблице. Мы также можем ограничить максимальное количество адресов на порт. Присутствует возможность создавать статические SAVI-записи, с указанием IP-адреса, MAC-адреса и номера интерфейса.

Прежде, чем использовать IPv6-адрес, устройство должно задействовать механизм Duplicate Address Detection (DAD). На специальный мультикастовый адрес посылается ICMPv6-NS сообщение с проверкой, не занят ли кем-то еще в сети этот адрес. Если никто не ответил положительно, то адрес свободен. Настройка savi ipv6 имеет три опции и работает с DAD-NS и DHCPv6-сообщениями. ‘DHCP-ONLY’ отслеживает DHCPv6-пакеты, а DAD NS-пакеты только с link-local адресом. ‘SLAAC-ONLY’ отслеживает DAD NS-пакеты со всеми типами адресов. DHCP-SLAAC отслеживает все DHCPv6 и DAD NS-пакеты.

Настройка savi check binding имеет два режима. Simple mode удаляет записи из таблицы, когда порт находится в состоянии DOWN, а время аренды IPv6-адреса истекло. Probe mode дополнительно посылает NS-пакет перед этим для дополнительной проверки состояния клиента. Если NA-пакет не получен в ответ, запись удаляется.

Включим SAVI, аналог IPv6 source guard, на порту e1/0/3 и ограничим максимальное количество привязанных IPv6-адресов на нем 10 штуками. Заносить в биндинг таблицу будем как адреса сформированные dhcp-методом, так и slaac. Порт e1/0/25 назначим доверенным для DHCPv6 и RA-сообщений.

```
Switch(config)#savi enable
Switch(config)#savi ipv6 dhcp-slaac enable
Switch(config)#savi check binding probe mode
Switch(config)#ipv6 dhcp snooping vlan 10

Switch(config)#int e1/0/3
Switch(config-if-ethernet1/0/3)#switchport access vlan 10
Switch(config-if-ethernet1/0/3)#savi ipv6 check source ip-address mac-address
Switch(config-if-ethernet1/0/3)#savi ipv6 binding num 10

Switch(config)#int e1/0/25
Switch(config-if-ethernet1/0/25)#switchport mode trunk
Switch(config-if-ethernet1/0/25)#ipv6 nd snooping trust
Switch(config-if-ethernet1/0/25)#ipv6 dhcp snooping trust
```

Проверим результат:

```
Switch#sh savi ipv6 check source binding

Static binding count: 0
Dynamic binding count: 4
Binding count: 4

MAC               IP                                VLAN Port          Type    State       Expires
------------------------------------------------------------------------------------------------------------------------------------------------
6c-3b-6b-da-5a-d8  fe80::6e3b:6bff:feda:5ad8          100  Ethernet1/0/1   slaac   BOUND     14383
6c-3b-6b-da-5a-d8  2001:db8:90::/56                  100  Ethernet1/0/1   dhcp    BOUND     106
b8-27-eb-ea-05-e1  fe80::ba27:ebff:feea:5e1          250  Ethernet1/0/2   slaac   BOUND     14380
b8-27-eb-ea-05-e1  2001:db8:250:1::130                250  Ethernet1/0/2   dhcp    BOUND     115
------------------------------------------------------------------------------------------------------------------------------------------------
```

CPS (Control Packet Snooping)

CPS работает совместно с SAVI и анализирует IPv6-пакеты на предмет префикса. Если он не соответствует тому, что задан в CPS, выдаваемый DHCPv6-сервером адрес не попадет в SAVI биндинг-таблицу. Рассмотрим порядок его настройки. Пропишем разрешенный префикс для global-unicast адреса, а затем префикс fe80::/64 под который будут подпадать все link-local адреса:

```
Switch(config)#ipv6 cps prefix 2001:db8:100:1::/64 vlan 100
Switch(config)#ipv6 cps prefix fe80::/64 vlan 100
Switch(config)#ipv6 cps prefix check enable
```

Теперь если DHCPv6-сервер во VLAN 100 отдаст на DHCP-SOLICIT-запрос адрес с отличным от 2001:db8:100:1::/64 префиксом, такой адрес не попадет в SAVI биндинг-таблицу.

ND Security

ND Security позволяет влиять на автоматическое изучение neighbor-записей и контролировать их, является полным аналогом ARP Security. Три рассматриваемые далее команды можно применять как глобально, так и из-под VLAN-интерфейса. Тогда они будут применяться только в этом VLAN. Рассмотрим пример использования ND Security. На данный момент имеем в neighbor-таблице две записи, связанные с тестовым ПК1.

```
Switch#sh ipv6 neighbors
IPv6 neighbour unicast items: 3, valid: 2, matched: 2, incomplete: 0, delayed: 0, manage items: 0
IPv6 Address                  Hardware Addr        Interface      Port              State         Age-time(sec)
2001:db8:100:1::3             38-63-bb-71-d3-00    Vlan1          Ethernet1/0/1     reachable     1136
fe80::f1ed:8839:4a8:13fc      38-63-bb-71-d3-00    Vlan1          Ethernet1/0/1     reachable     1150

IPv6 neighbour table: 2 entries
```

Теперь рассмотрим команду ‘ipv6 nd-security updateprotect’. Как понятно из названия, она блокирует обновление MAC-адресов в neighbor-записях. Если после ее применения изменить MAC-адрес на тестовом ПК, то его запись в neighbor-таблице не обновится.

На данный момент обе записи в таблице динамические. Сконвертируем их в статические командой ‘ipv6 nd-security convert’. Записи стали статическими и попали в конфигурацию:

```
Switch(config)#ipv6 nd-security convert
Switch(config)#sh ipv6 neighbors
IPv6 neighbour unicast items: 3, valid: 2, matched: 2, incomplete: 0, delayed: 0, manage items: 0
IPv6 Address                            Hardware Addr   Interface       Port                State       Age-time(sec)
2001:db8:100:1::3                       38-63-bb-71-d3-00     Vlan1       Ethernet1/0/1       permanent
fe80::f1ed:8839:4a8:13fc                  38-63-bb-71-d3-00     Vlan1       Ethernet1/0/1       permanent

IPv6 neighbour table: 2 entries

Switch(config)#sh run int vlan1
!
interface Vlan1
 ipv6 address 2001:db8:100:1::1/64
 ipv6 neighbor fe80::f2de:f1ff:fe19:d5eb f0-de-f1-19-d5-eb interface Ethernet1/0/2
 ipv6 neighbor 2001:db8:100:1::4 f0-de-f1-19-d5-eb interface Ethernet1/0/2
!
```

Наконец, запретим автоматическое изучение новых neighbor-записей командой ipv6 nd-security learnprotect‘. ’

Заключение

Подводя итог, можно сказать, что мы поговорили про основные особенности IPv6, принцип работы и посмотрели на самые яркие отличия от IPv4. Рассмотрели типы адресов и все способы их выдачи. На этом мы, надеюсь, не заканчиваем знакомиться с протоколом IP шестой версии. Если статья вызовет достаточный интерес, то можно ждать продолжения - рассказ про работу с опциями 18 (interface-id), 37 (remote-id) и 38 (subscriber-id). А также детальное рассмотрение DHCPv6-снупинга и релея на коммутаторах доступа SNR.
По всем вопросам вы можете обратиться к вашему менеджеру. Напоминаем, что у нас есть Telegram-канал, а также подробная база знаний.