Динамическая конфигурация устройств. DHCPv4. Адресация IPv6, DHCPv6 и протоколы SLAAC, EUI-64.

1. Протокол DHCP

Всем устройствам, которые обмениваются сообщениями через сеть Интернет, необходимы уникальные IP-адреса. Эти адреса могут назначаться в статическом или динамическом режиме. В статическом режиме адреса вручную назначает администратор при конфигурировании устройства. ***Рекомендуется назначать статические IP-адреса на маршрутизаторы, серверы, сетевые принтеры*** и другие устройства, адреса которых меняется редко. В то же время, адреса рабочих станций могут изменяться достаточно часто. Некоторые пользователи в Интернет выходят эпизодически, поэтому им нужны IP-адреса не постоянно.

Протокол динамического конфигурирования узлов (Dynamic Host Configuration Protocol – ***DHCP***) позволяет автоматизировать процесс назначения IP-адресов рабочим станциям из диапазона, предоставленного администратору провайдером. Динамическое назначение адресов протоколом DHCP производится по запросу клиента на определенный промежуток времени, для продления которого пользователь должен периодически обращаться к серверу. При освобождении IP-адресов они возвращаются DHCP-серверу, который перераспределяет их. При повторном запросе клиента, освободившего IP-адрес, сервер пытается назначить ранее использовавшийся адрес. Помимо IP-адреса протокол DHCP предоставляет пользователю еще целый ряд параметров (маску подсети, шлюз по умолчанию, IP-адрес сервера DNS и др.)

Для работы протокол использует клиент-серверную архитектуру и работает поверх протокола UDP:

- Порт 67 – DHCP-сервер
- Порт 68 – DCHP-клиент

DHCPv4 является версией протокола, которая поддерживает работу с адресацией IPv4.

Процесс получения информации от DHCP-сервера происходит в четыре этапа, как представлено на рисунке 1.

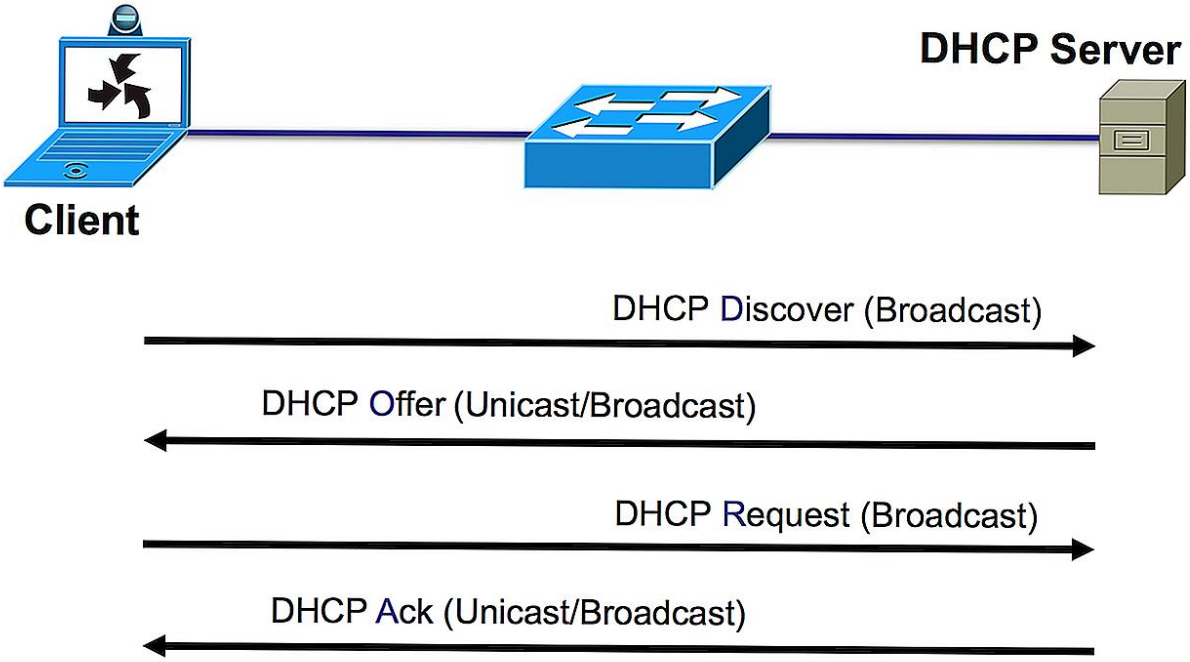

Рисунок 1 – Процесс получения адресной информации через DHCPv4

Изначально клиент находится в состоянии инициализации (***INIT***) и не имеет своего IP-адреса. Он отправляет широковещательное сообщение ***DCHP Discover*** на все устройства в локальной сети (***устройство указывает IP-адрес назначения – 255.255.255.255 и MAC-адресом – FF:FF:FF:FF:FF:FF***).

В случае, если DHCP-сервер находится в той же сети, что и устройство, он получит сообщение DCHP Discover. Если сервера нет, то это сообщение получит ***DHCP Relay Agent*** и перешлет его серверу. В случае отсутствия последнего, клиент не получит IP-адрес.

DHCP-сервер отвечает на поиск предложением, он сообщает IP, который может подойти клиенту. IP выделяются из области (***SCOPE***) доступных адресов, которая задается администратором.

DHCP выделяет доступные IP-адреса из области на определенный промежуток времени (может быть задан администратором), поэтому нет гарантии, что при следующем подключении у данного клиента останется

прежний IP. Но есть возможность назначить какому-либо клиенту определенный IP навсегда. К примеру, забронировать 192.168.0.10 за компьютером системного администратора. Такое сохранение IP для отдельных клиентов называют резервацией (***reservation***).

DHCP Offer содержит IP из доступной области, который предлагается клиенту отправкой широковещательного (broadcast) или прямого (unicast) сообщения. При этом, поскольку нужный клиент пока не имеет IP, для отправки прямого сообщения он идентифицируется по MAC-адресу, который был указан в качестве источника в сообщении DCHP Discover.

В случае, если несколько DHCP-серверов отвечают DHCP-клиенту сообщением ***DHCP Offer***, клиент принимает только первое полученное сообщение. Затем клиент передает сообщение ***DHCP Request***. Этим сообщением он принимает предлагаемый адрес и уведомляет DHCP-сервер об этом. Широковещательное сообщение почти полностью дублирует DHCP Discover, но содержит в себе уникальный IP, выделенный сервером. Таким образом, клиент сообщает всем доступным DHCP-серверам о получении конкретного адреса, а сервера помечают IP как занятый.

Сервер получает от клиента ***DHCP Request*** и окончательно подтверждает передачу IP-адреса клиенту сообщением ***DHCP ACK***. Это broadcast или unicast сообщение утверждает не только владельца IP, но и срок, в течение которого клиент может использовать этот адрес. DHCP-клиент отправляет Gratuitous ARP, чтобы убедиться в уникальности полученного IP-адреса.

Кроме DORA – четырех сообщений для получения адреса – DHCP использует и другие.

DHCP NAK. Нередко в источниках можно встретить написание DHCPNACK, что является неправильным, так как RFC 2131 регламентирует именно NAK. DHCPNAK отправляется сервером вместо окончательного подтверждения. Такой отказ может быть отправлен клиенту, если аренда запрашиваемого IP истекла или клиент перешел в новую подсеть.

DHCP Release. Клиент отправляет это сообщение, чтобы уведомить сервер об освобождении занимаемого IP. Иными словами, это досрочное окончание аренды.

DHCP Inform. Этим сообщением клиент запрашивает у сервера локальные настройки. Отправляется, когда клиент уже получил IP, но для правильной работы ему требуется конфигурация сети. Сервер информирует клиента ответным сообщением с указанием всех запрошенных опций.

DHCP-сервер может назначать IP-адреса одним из трех основных способов.

Статическое распределение (static allocation). Почти как ввод адреса на каждом компьютере вручную. Отличие в том, что системный администратор задает нужные соответствия IP для MAC-адресов клиентов на самом DHCP-сервере. IP останется за клиентом, даже если тот выйдет из сети, отключится, перейдет в новую сеть и т.п.

Автоматическое распределение (automatic allocation). Сервер закрепляет IP из области за каждым клиентом навсегда. Срок аренды не ограничен.

Динамическое распределение (dynamic allocation). DHCP-сервер назначает адрес из области на определенное время, называемое сроком аренды. Такой подход полезен, если число доступных IP ограничено. IP назначается каждому клиенту при подключении к сети и возвращается в область, как только клиент его освобождает. В таком случае IP может отличаться при каждом подключении, но обычно назначается прежний.

Когда DHCP-сервер выделяет IP из области, он оставляет запись о том, что этот адрес зарезервирован за клиентом с указанием срока действия IP. Этот срок действия называется срок аренды (lease time). ***Срок аренды по умолчанию выставлен на 24 часа***, но может доходить до нескольких дней, недель или даже месяцев. Период задается в настройках самого сервера. При необходимости, можно закрепить адрес за определенным устройством.

2. Адресация IPv6

В настоящее время наблюдается дефицит адресов в связи с ростом числа пользователей Интернета, бурным развитием сетей мобильной связи, предоставляющих услуги передачи данных, использованием сетевых технологий для управления технологическими процессами и бытовой техникой. 32 двоичных разряда адреса версии IPv4 обеспечивают примерно 4 миллиарда адресов. В Северной Америке уже использованы все общественные адреса версии IPv4. Для снижения остроты дефицита в локальных сетях используются частные адреса, разработаны ***трансляторы NAT и PAT***, используются маски переменной длины и адресация на основе префикса. Однако эти меры лишь предоставляли отсрочку полного истощения адресов версии IPv4.

Кардинальным решением данной проблемы является разработка и внедрение адресации версии ***IPv6***. Версия IPv6 использует ***для адресации 128 двоичных разрядов***, что обеспечивает адресацию 3,4 10^{38} объектов, вместо 32 разрядов версии IPv4, обеспечивающей адресацию 4,3 10^{9} объектов. Со временем версия IPv6 заменит IPv4 в качестве основного сетевого протокола Internet Protocol.

Адреса версии IPv6 представлены в виде ***8 блоков по 16 двоичных разрядов,*** которые записываются в шестнадцатеричной системе, т.е. каждый блок представлен в виде четырех шестнадцатеричных чисел. Блоки разделяются двоеточием. Ниже приведен пример адреса версии IPv6:

2af9:0000:7ee5:d947:0009:01c5:6b9f:00c4.

Для облегчения чтения впереди стоящие нули могут быть пропущены. При этом вышеприведенный адрес может быть записан в виде:

2af9:0:7ee5:d947:9:1c5:6b9f:c4.

Если в адресе имеется длинная последовательность нулей, например,

2af9:0:7ee5:0:0:0:6b9f:c4,

то запись можно сократить путем использования двух двоеточий подряд

2af9:0:7ee5::6b9f:c4.

Два двоеточия подряд в адресе могут быть использованы только один раз. Таким образом, адрес 2af9:0:0:0:0:0:0f:c4 может быть представлен 2af9::c4.

Младшие разряды адреса нижнего уровня иерархии (идентификатор интерфейса) используется для задания номера узла, а старшие разряды – для задания ***префикса адреса*** (номера сети), как представлено на рис.X.

Префикс адреса (64 бита)		Идентификатор интерфейса (64 бита)	
127	64	63	0

Рисунок 2 – Уровни иерархии адреса IPv6

Причем старшие разряды адреса образуют несколько полей. Формат адреса IPv6 приведен ниже на рис. 3.

Наименование поля	FP	TLA	Резерв	NLA	SLA	Идентификатор интерфейса
Длина поля (бит)	3	13	8	24	16	64

Рисунок 3 – Формат адреса IPv6

Идентификатор интерфейса задает адрес узла (интерфейса) в определенной сети. Длина идентификатора интерфейса составляет 64 младших бита адреса (четыре младших блока из четырех шестнадцатеричных чисел). Это позволяет в поле идентификатора интерфейса размещать адреса конечных узлов различных сетевых технологий, например, физический ***MAC-адрес длиной 48 бит***. При этом идентификаторы интерфейса могут быть динамически получены из адреса Уровня 2. Поэтому отпадает необходимость в протоколе ARP, который связывает IP-адреса и соответствующие MAC-адреса, что ускоряет процесс продвижения пакета через маршрутизатор. В этом поле могут также задаваться адреса других

протоколов, например, ATM-адреса, номера телефонов международной и междугородной связи, номера мобильных телефонов, а также адреса IPv4.

Поле префикса формата (***FP – Format Prefix***) версии IPv6 имеет размер 3 бита и значение в двоичном коде 001. Поэтому адреса версии IPv6 будут начинаться либо с шестнадцатеричной цифры 2 (0010), либо 3 (0011).

Поле агрегирования верхнего уровня (***TLA – Top-Level Aggregation***) задает адреса сетей пяти основных регистратров Европы, Азии, Северной Америки, Южной Америки, Африки (ARIN, RIPE, APNIC, LACNIC, AfriNIC). 13 разрядов этого поля позволяет адресовать 8196 сетей. Поле префикса формата FP и поле агрегирования верхнего уровня TLA составляют 16 старших бит адреса IPv6, они выделяются и управляются организацией IANA и пятью основными регистраторами адресов. Для возможности расширения этого поля в будущем зарезервировано еще 8 разрядов. С учетом префикса формата (001) первая сеть IPv6 будет иметь номер 2001.

Поле агрегирования следующего уровня (NLA – Next-Level Aggregation) адресует сети мелких и средних провайдеров. 24 разряда этого поля позволяют адресовать примерно 16 миллионов сетей.

Поле местного уровня (***SLA – Site-Level Aggregation***) используется для адресации подсетей пользователя. Таким образом, в распоряжении сетевого администратора имеется 16 двоичных разрядов, что позволяет организации адресовать до 65 535 отдельных подсетей.

Кроме формата (рис.3) для описания адреса IPv6 используется также формат (рис.4), где 48 старших бита адреса образуют префикс сайта (***Site Prefix***), из которых 32 старших – образуют префикс провайдера (ISP Prefix).

Так как в поле идентификатора интерфейса могут задаваться адреса IPv4, то обеспечивается совместимость IPv4 и IPv6. Для преобразования адреса IPv6 в адрес IPv4 разработан подтип адреса, в котором 4 младших байта содержат адрес предыдущей версии IPv4, а старшие 12 байт – содержат нули. При преобразовании адреса IPv4 в адрес IPv6 младшие 4 байта

содержат адрес версии IPv4, байты 5 и 6 содержат единицы, а старшие 10 байт содержат нули.

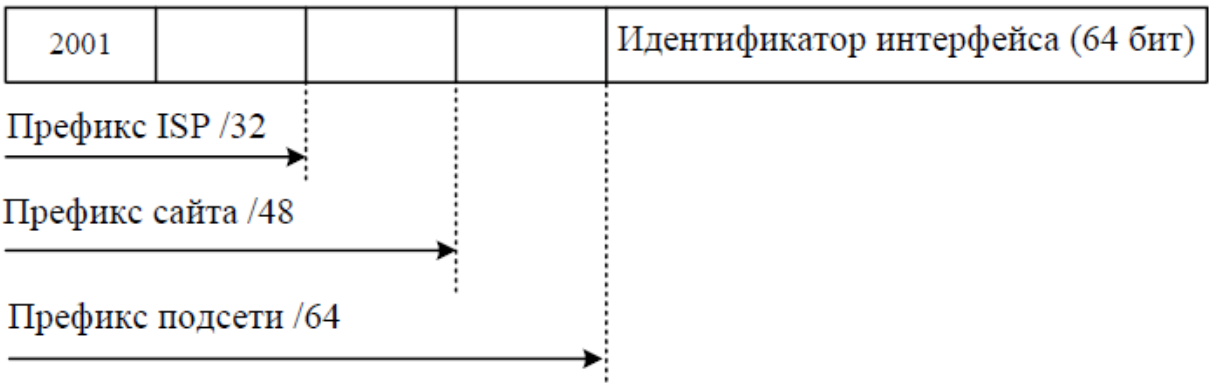

Рисунок 4 – Префиксы формата адреса IPv6

На период перехода от IPv4 к IPv6 разработано несколько механизмов. Например, механизм двойного стека, когда устройства поддерживают оба протокола, причем, IPv6, является привилегированным. То есть, на интерфейсах устройств конфигурируется **два стека протоколов**. Устройство с двойным стеком определяет, какой стек использовать, базируясь на адресе назначения пакета, отдавая предпочтение IPv6, когда это возможно.

Классификация IPv6-адресов

В IPv6 не существует широковещательных (broadcast) адресов, их функции выполняют многоадресные (multicast) адреса.

Адреса IPv6 делятся на следующие типы:

Unicast-адреса: предназначены для идентификации интерфейса узла, работающего под управлением IP-протокола шестой версии.

Multicast-адреса: предназначены для отправки пакетов на несколько адресов (в шестой версии протокола является заменой широковещательного (broadcast) адреса).

Anycast-адреса: назначается сразу нескольким устройствам, при этом пакет, отправляемый на anycast-адрес, получает узел, являющийся ближайшим из имеющих данный адрес.

Unicast-адреса, в свою очередь, также делятся на типы:

Global: публичный адрес (является аналогом публичного адреса в протоколе четвёртой версии). К таким адресам в интернете можно проложить полноценный маршрут. Он – уникален, и может настраиваться как статически, так и присваиваться провайдером динамически.

Unique Local: это – аналог частного адреса в IPv4. Такие адреса не предназначены для маршрутизации в глобальном протоколе шестой версии.

Link Local: канальные (локальные) адреса, автоматически назначаемые самим хостом. Пакеты, имеющие канальный адрес источника или конечного узла, не могут маршрутизироваться в глобальном интернете и используются только в пределах того канала, в котором созданы. К этим адресам не предъявляется требование уникальности, они могут быть одними и теми же в каждой из сетей. Канальные адреса используются, например, при проведении процедуры обнаружения соседей, примерно так же, как это делает ARP в IPv4. Эти адреса находятся в диапазоне fe80::/10, то есть, первый гекстет имеет значения от fe80 до febf.

3. DHCPv6

DHCPv6 – это версия протокола DHCP для работы с **IPv6**. Этот протокол назначает как IPv6 адреса, так и другие параметры настройки сети, такие, как адрес DNS или доменное имя. DHCPv6 сервер также может обеспечить сервис DHCPv6 без состояния отслеживания (SLAAC), при котором клиенту могут быть назначены параметры конфигурации, такие как адрес DNS-сервера и доменное имя без назначения IPv6-адреса.

В протоколе DHCPv6 предусмотрены три объекта: ***клиент, Relay и сервер***. Протокол DHCPv6 ***основан на протоколе UDP***. Клиент DHCPv6 отправляет сообщения запроса конфигурации DHCP-серверу или DHCP-Relay на порт **UDP 547**, в ответ сервер или Relay DHCPv6 отправляют сообщения на порт **UDP 546**. Клиент DHCPv6 отправляет сообщения ***Solicit и Request*** DHCP-серверу или Relay на **multicast-адрес - ff02::1:2.**

Существует несколько режимов его работы:

DHCPv6 Stateful Autoconfiguration: сервер присваивает IPv6-адреса и другие сетевые параметры.

DHCPv6 Stateless Autoconfiguration: хосты генерируют IPv6-адреса при помощи SLAAC, а DHCPv6-сервер назначает прочие сетевые параметры (но не IPv6-адреса).

Такой режим позволяет DHCPv6-серверу назначать дополнительные сетевые параметры (но не IPv6-адреса) устройствам, у которых уже есть адрес.

DHCPv6-клиент отправляет multicast-сообщение Information-request с опцией Option Request. Данная опция содержит запрашиваемые клиентом параметры. Сервер отвечает клиенту unicast-сообщением Reply, содержащим запрошенные параметры.

DHCPv6 Prefix Delegation (PD) Autoconfiguration: используется для распределения префиксов нижестоящим устройствам в сетях с развитой иерархией. Нижестоящие устройства могут объявлять полученные префиксы в сообщениях RA.

К ***DHCPv6 Stateful Autoconfiguration*** относится настройка, приведенная на рисунке 5.

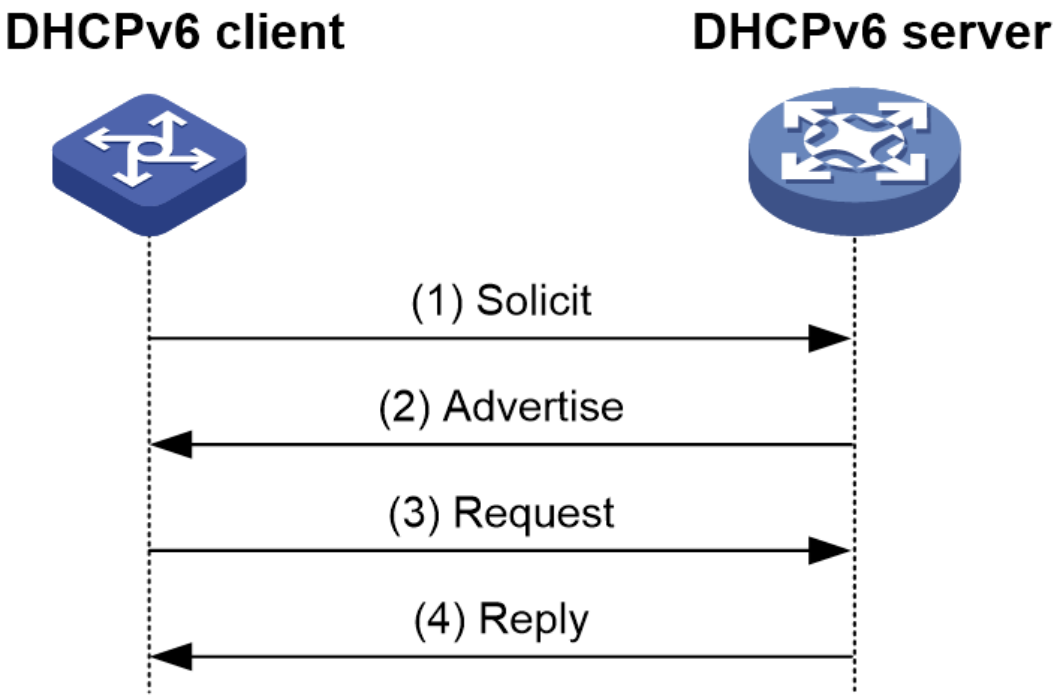

Рисунок 5 – Процесс получения адресной информации через DHCPv6

Когда DHCPv6 клиент пытается запросить IPv6 адрес и другую конфигурацию, сначала клиент должен найти DHCPv6-сервер, а только после этого запросить конфигурацию.

В момент обнаружения сервера, DHCP клиент пытается найти DHCPv6 сервер, рассылая ***DHCP Solicit*** сообщения, содержащее собственный идентификатор DUID, на **multicast** -адрес FF02::1:2.

Каждый DHCPv6-сервер, получивший ***DHCP Solicit***, ответит клиенту сообщением ***DHCP Advertise***, которое содержит идентификатор DUID сервера и его приоритет.

Возможно, что клиент получить несколько сообщений ***DHCP Advertise***. В этом случае клиент должен выбрать один сервер и ответить ему сообщение ***DHCP Request***, чтобы запросить предложенный им адрес.

Выбранный DHCPv6-сервер подтверждает клиенту IPv6 адрес и другие параметры в сообщении ***DHCP Reply***.

Если DHCPv6 сервер и DHCPv6 клиент не находятся в одной сети, сервер не сможет получить multicast-пакеты от клиента и ответить ему. Для пересылки таких пакетов используется ***DHCPv6-Relay***, функции которого реализованы на коммутаторе. Когда DHCPv6-relay получает сообщение от DHCPv6 клиента, он инкапсулирует его в пакет ***Relay-forward*** и доставляет следующему ***DHCPv6-Relay*** или серверу.

4. SLAAC

Динамическая настройка IPv6-адреса может происходить с помощью протокола DHCPv6, если DHCP-сервер недоступен, то существует возможность получения адреса с помощью ***IPv6 Stateless Address Autoconfiguration (SLAAC)***.

SLAAC – это служба без отслеживания состояния, не отслеживает состояние адреса. Это означает не существует сервера, который хранит информацию о сетевых адресах, чтобы знать, какие адреса IPv6

используются, а какие из них доступны. В основе SLAAC лежит протокол ICMPv6 RA. Он аналогичен протоколу ICMPv4, но при этом имеет дополнительный функционал. SLAAC использует ICMPv6-сообщения запроса маршрутизатора и объявления маршрутизатора, чтобы предоставить информацию об адресации и другую информацию о конфигурации, обычно предоставляемую DHCP-серверами. Хост устанавливает свой IPv6-адрес на основе информации, отправляемой в RA, эти сообщения отправляются каждые 200 секунд.

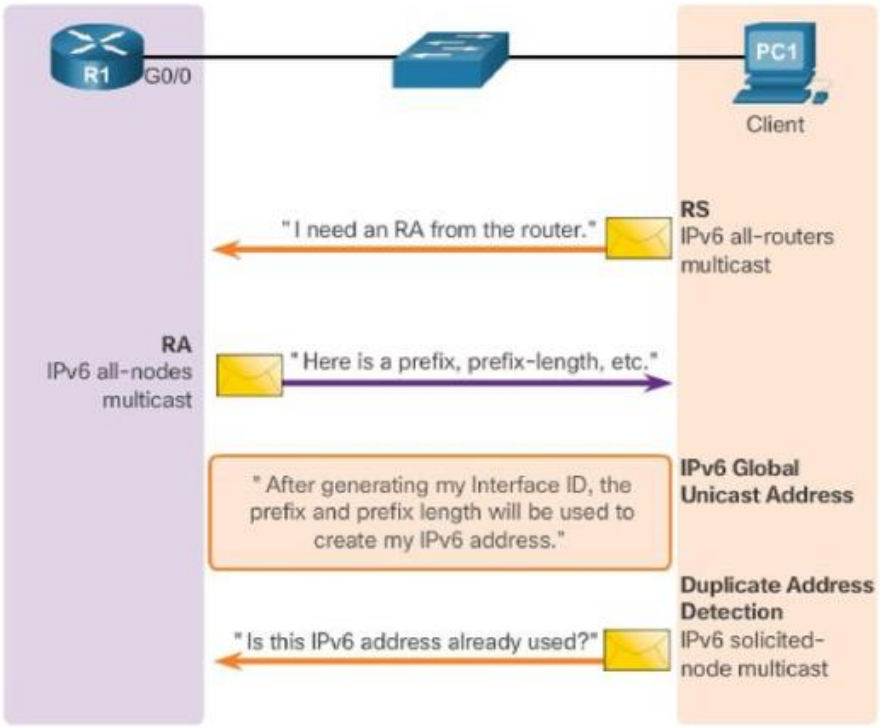

Рисунок 6 – Процесс работы SLAAC

Процесс работы SLAAC описывается следующим образом. Устройство отправляет сообщение RS, запрашивая у маршрутизаторов информацию о сети. Маршрутизаторы отвечают с помощью RA, указывая префикс сети и другую информацию (длину префикса и флаги). Хост использует полученный префикс сети и генерирует уникальный идентификатор интерфейса для создания полного IPv6-адреса. Для этого может быть использован алгоритм EUI-64. Далее хост убеждается, что такой адрес является уникальным при помощи DAD (Duplicate Address Detection).

Устройство отправляет NS (Neighbor Solicitation) для проверки, не используется ли этот адрес в сети. Если сообщение не приходит в ответ, то адрес считается уникальным и его использование разрешено, но если было получено ответное сообщение, то хост должен сгенерировать другой адрес.

5. EUI-64

EUI-64 (Extended Unique Identifier-64) — это метод генерации уникальных 64-битных идентификаторов, используемых в IPv6 для автоматической настройки адресов. EUI-64 основывается на MAC-адресе устройства и используется для создания уникальных IPv6-адресов для узлов в сети. Однако MAC-адрес содержит 48 бит, а идентификатор интерфейса – 64 бит. Не хватает бит для однозначной конвертации.

Процесс формирования идентификатора интерфейса EUI-64 из MAC-адреса состоит из следующих шагов:

1. Разделение MAC-адреса на две части: 48-битный MAC-адрес делится на две части: первая часть содержит первые 24 бита (идентификатор производителя), а вторая часть — последние 24 бита (идентификатор устройства).
2. Добавление разделителя FFFE: В середину между этими частями вставляются 16 бит (2 байта) со значением FFFE. Это делается для расширения MAC-адреса до 64 бит.
3. Инвертирование 7-ого бита: В стандартном MAC-адресе 7-й бит отвечает за уникальность и глобальность адреса. Этот бит инвертируется. Если 7-й бит был равен 0 (локальный адрес), он становится 1 (глобальный адрес), и наоборот.

В результате получается 64-битный идентификатор. Далее в начало добавляется сетевой префикс IPv6.

Пример формирования IPv6-адреса с помощью алгоритма EUI-64.

1. Существует MAC-адрес: 00-1A-2B-3C-4D-5E.

2. Разделим его на две части и получим: 00-1A-2B – идентификатор производителя и 3C-4D-5E – идентификатор устройства. Вставим между ними FFFE. В результате получим 00-1A-2B-FFFE-3C-4D-5E.

3. Инвертируем 7-й бит и получаем: 02-1A-2B-FFFE-3C-4D-5E.

4. После соединяем с префиксом сети 2001:0db8:85a3::/64. После всех преобразований получается адрес 2001:0db8:85a3:021A:2BFF:FE3C:4D5E

Контрольные вопросы:

1. Какие порты использует протокол DHCP?
2. Какие поля входят в кадр IPv6?
3. Какие сообщения рассылаются в процессе работы протокола DHCP?
4. Какие дополнительные параметры предоставляет DHCP-клиенту помимо IP-адреса?
5. Какие типы адресов существуют в IPv6?
6. В чем различие динамической настройки по DHCPv6 от настройки с помощью SLAAC?
7. Как происходит процесс получения IPv6 адреса с помощью SLAAC?
8. Опишите процесс работы EUI-64 при формировании IPv6-адреса?
9. Какие устройства обычно используют статические IP-адреса, и почему?