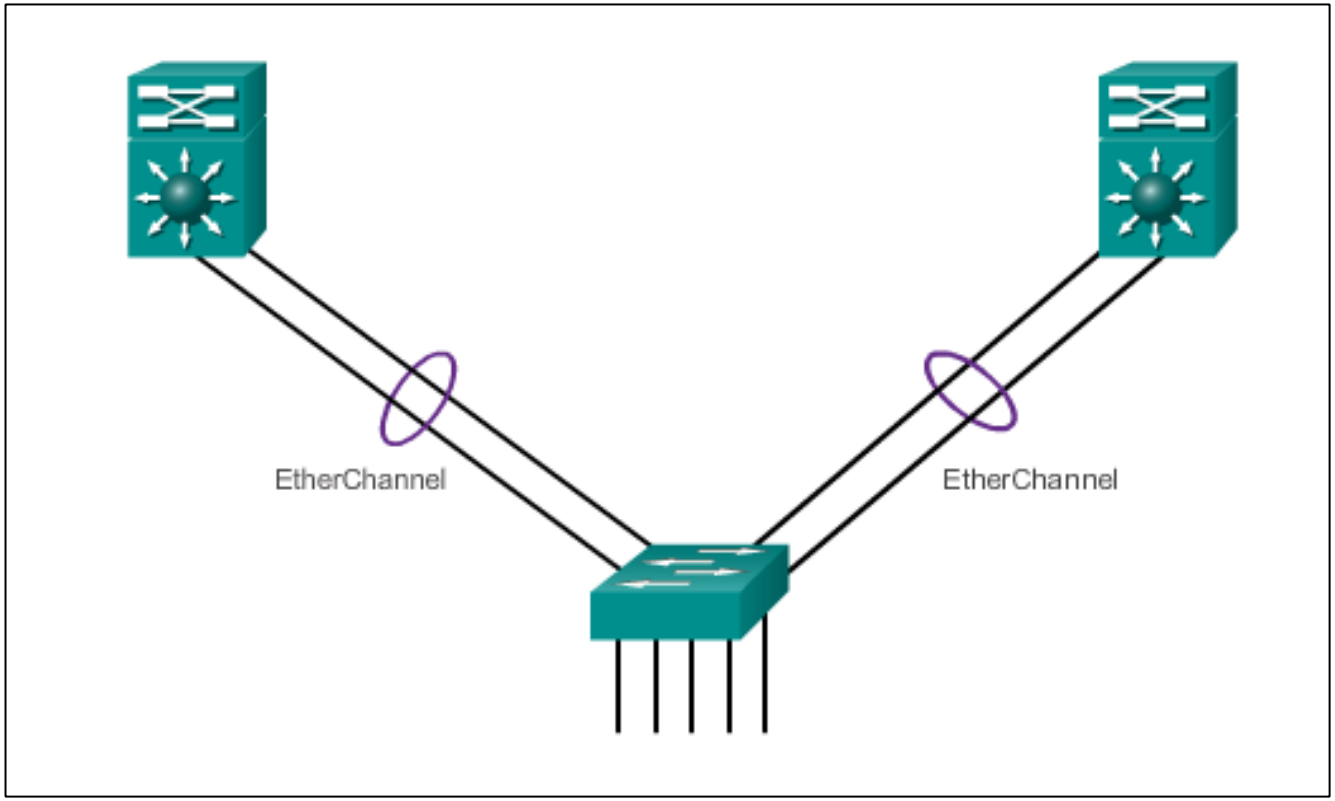
МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ | НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Агрегирование каналов

Коммутация, маршрутизация и беспроводная связь

Введение в агрегирование каналов

- Технология EtherChannel разработана компанией Cisco **для объединения нескольких портов** Fast Ethernet или Gigabit Ethernet **в один логический канал.**
- При настройке EtherChannel создаётся **виртуальный интерфейс**, который называется **агрегированный канал** (port channel). **Физические интерфейсы объединяются в интерфейс агрегированного канала.**



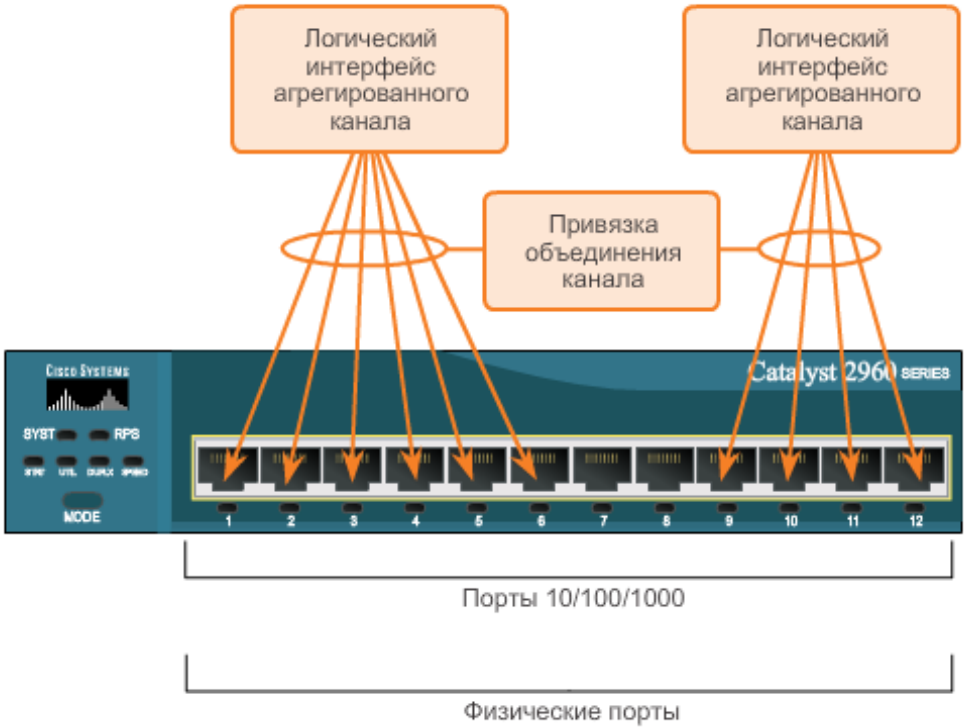
Агрегирование каналов

Преимущества EtherChannel

- **Большинство задач конфигурации выполняется на интерфейсе EtherChannel, а не на отдельных портах.** Это обеспечивает согласованную конфигурацию на всех каналах.
- EtherChannel **использует существующие порты коммутатора**. Для обеспечения более высокой пропускной способности не требуется дорогостоящая замена канала на более быстрый.
- Между каналами, которые являются частью одного и того же EtherChannel, происходит **распределение нагрузки**.
- EtherChannel создает объединение, которое рассматривается, как **один логический канал**. Если существует только один канал EtherChannel, **все физические каналы в EtherChannel активны**, поскольку STP видит только один (логический) канал.
- EtherChannel предоставляет **функции избыточности**, поскольку общий канал считается одним логическим соединением. EtherChannel **продолжает работать даже в том случае, если общая пропускная способность снижается из-за потери соединения в пределах EtherChannel.**

Ограничения реализации

- EtherChannel можно реализовать путем объединения нескольких физических портов в один или несколько логических каналов EtherChannel.
- **Типы интерфейсов нельзя смешивать.**
- EtherChannel предоставляет **полнодуплексную полосу пропускания до 800 Мбит/с** (Fast EtherChannel) **или 8 Гбит/с** (Gigabit EtherChannel) между двумя коммутаторами или между коммутатором и узлом.
- В настоящее время все каналы EtherChannel могут содержать **до восьми совместимо настроенных Ethernet-портов.**



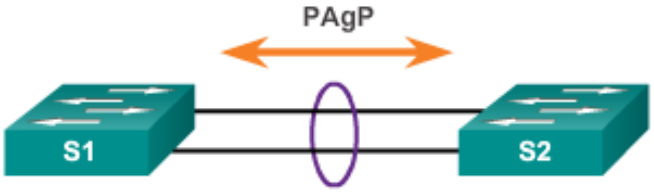
Принцип работы EtherChannel

Протокол агрегирования портов PAgP

Etherchannel можно образовать путем согласования с использованием одного из двух протоколов, PAgP или LACP. Данные протоколы позволяют портам со сходными характеристиками **образовывать каналы путем динамического согласования со смежными коммутаторами**.

Режимы PAgP:

- **On (Вкл):** участник канала без согласования (без протокола).
- **Desirable (Рекомендуемый):** активно запрашивает возможность и готовность к участию другой стороны.
- **Auto (Автоматический):** пассивно ожидает действий другой стороны.



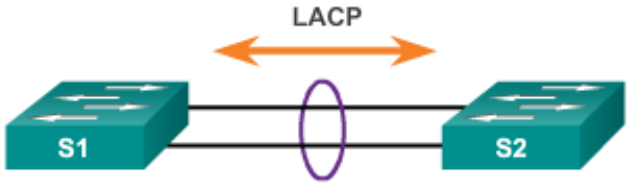
S1	S2	Формирование канала
Вкл	Вкл	Да
Автоматический/Рекомендуемый	Рекомендуемый	Да
Вкл/Автоматический/Рекомендуемый	Конфигурация не задана	Нет
Вкл	Рекомендуемый	Нет
Автоматический/Вкл	Автоматический	Нет

Протокол агрегирования портов LACP

LACP определяется стандартом IEEE (802.3ad), который обеспечивает возможность объединения нескольких физических портов для создания единого логического канала. LACP обеспечивает возможность согласования коммутатором автоматического объединения путем отправки соседу пакетов LACP. Он выполняет функцию, сходную с функциями PAgP для Cisco EtherChannel. Поскольку протокол LACP относится к стандарту IEEE, его можно использовать **для упрощения работы с каналами EtherChannel в неоднородных средах.** На устройствах Cisco поддерживаются оба протокола.

Режимы LACP:

- **On (Вкл):** участник канала без согласования (без протокола).
- **Active (Активный):** активно запрашивает возможность и готовность к участию другой стороны.
- **Passive (Пассивный):** пассивно ожидает действий другой стороны.



S1	S2	Формирование канала
Вкл	Вкл	Да
Активный/Пассивный	Активный	Да
Вкл/Активный/Пассивный	Конфигурация не задана	Нет
Вкл	Активный	Нет
Пассивный/Вкл	Пассивный	Нет

Настройка EtherChannel

Инструкция по настройке

При настройке EtherChannel рекомендуется соблюдать следующие инструкции и ограничения:

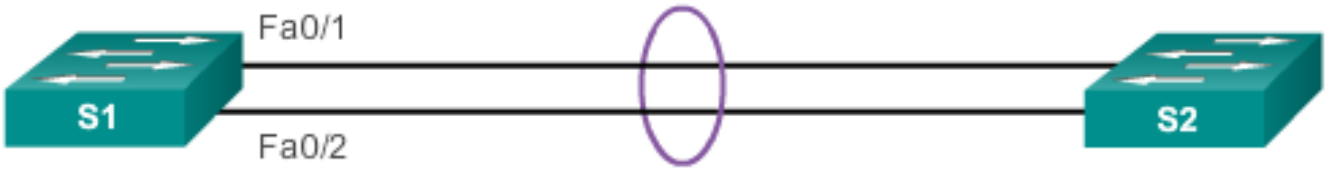
- **Поддержка EtherChannel.** Все интерфейсы Ethernet на всех модулях должны поддерживать EtherChannel; при этом не требуется, чтобы эти интерфейсы были физически смежными или находились на одном модуле.
- **Скорость и дуплексный режим.** Настройте ***все интерфейсы*** в EtherChannel для работы ***на одной скорости и в одном дуплексном режиме.***
- **Сопоставление сетей VLAN.** ***Все интерфейсы*** в объединении EtherChannel должны быть ***назначены в один VLAN или настроены в качестве транкового канала.***
- **Диапазон сетей VLAN.** EtherChannel поддерживает одинаковые разрешённые диапазоны сетей VLAN на всех интерфейсах в транковом канале EtherChannel. Если разрешённый диапазон сетей VLAN не совпадает, интерфейсы не смогут создать EtherChannel даже при выборе **auto** или **desirable** режимов.

Настройка интерфейсов

Настройка EtherChannel с использованием LACP

```
S1(config)# interface range FastEthernet0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```

Создает EtherChannel и настраивает транковый канал.



Настройка EtherChannel с использованием LACP проходит в два этапа.
Шаг 1. Укажите интерфейсы, составляющие группу EtherChannel, используя команду режима глобальной конфигурации **interface range** *interface*. Ключевое слово **range** позволяет выбрать несколько интерфейсов и настроить их одновременно. Рекомендуется сперва отключить эти интерфейсы, чтобы избежать активности в канале из-за неполной конфигурации.
Шаг 2. Создайте интерфейс агрегированного канала с помощью команды **channel-group** *identifier* **mode active** режима конфигурации диапазона интерфейса. Идентификатор задает номер группы каналов. Ключевые слова **mode active** определяют его как конфигурацию EtherChannel LACP.

Проверка EtherChannel

- **`show interface Port-channel`** – отображается общий статус интерфейса агрегированного канала.
- **`show etherchannel summary`** – отображается по одной строке данных на каждый канал.
- **`show etherchannel port-channel`** – отображаются сведения о конкретном интерфейсе агрегированного канала.
- **`show interfaces etherchannel`** – просмотреть данные о роли физического интерфейса в работе EtherChannel.

МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ | НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Основные понятия FHRP

Коммутация, маршрутизация и беспроводная связь

Протокол резервирования первого перехода (FHRP)

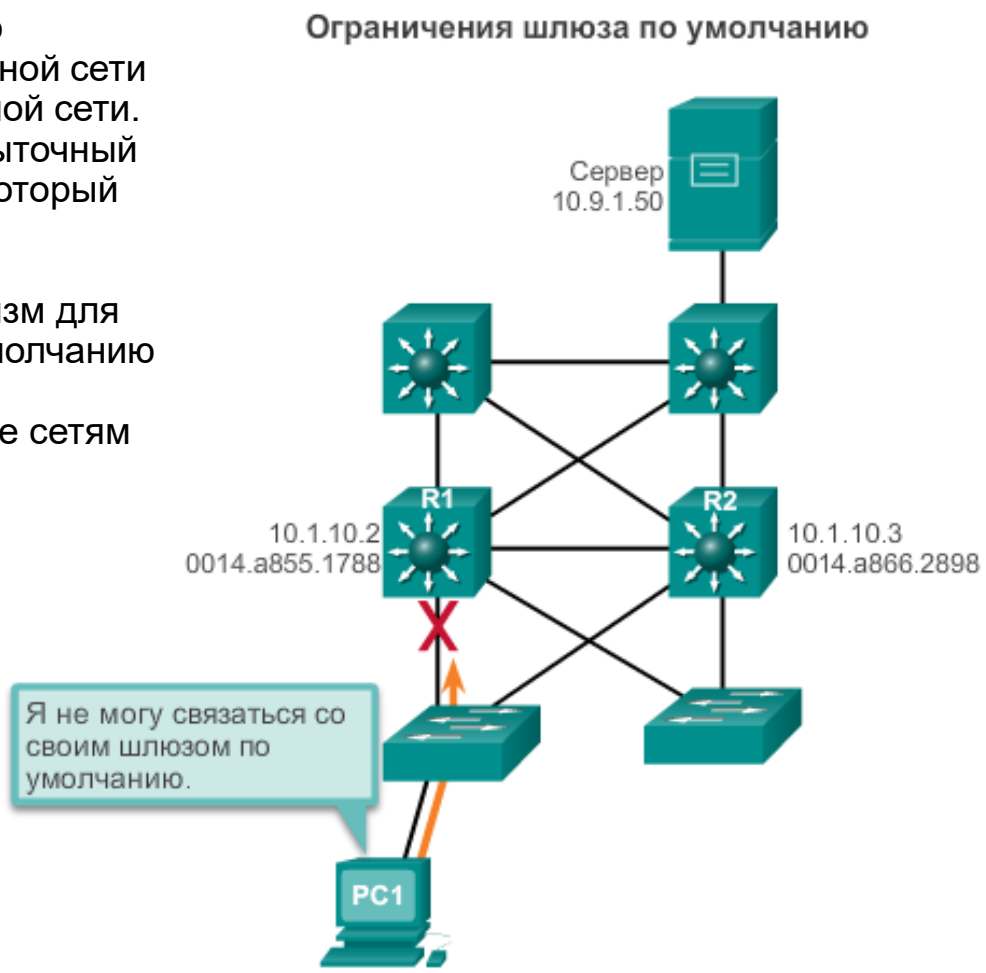
Ограничение шлюза по умолчанию

Конечные устройства, как правило, настраиваются с одним IPv4-адресом для шлюза по умолчанию.

- Если интерфейс маршрутизатора шлюза по умолчанию выходит из строя, хосты локальной сети теряют подключение за пределами локальной сети.
- Это происходит, даже если существует избыточный маршрутизатор или коммутатор уровня 3, который может служить шлюзом по умолчанию.

First hop redundancy protocols (FHRPs) - механизм для предоставления альтернативных шлюзов по умолчанию в коммутируемых сетях, где два или более маршрутизаторов подключены к одним и тем же сетям VLAN.

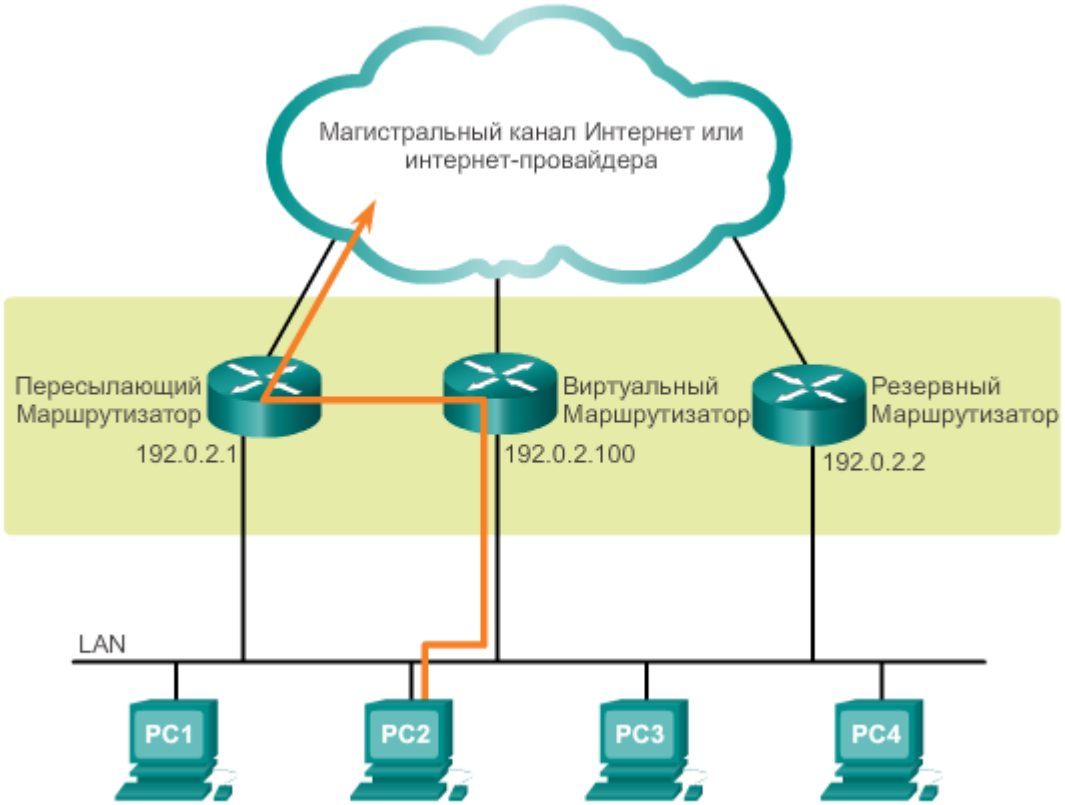
R1 отвечает за маршрутизацию пакетов от PC1. В случае недоступности R1 протоколы маршрутизации выполняют динамическое схождение. Теперь R2 маршрутизирует пакеты из внешних сетей, которые должны были пройти через R1. Тем не менее, трафик из внутренней сети, связанный с R1, включая трафик с рабочих станций, серверов и принтеров, для которых R1 настроен в качестве шлюза по умолчанию, ***до сих пор отправляется на R1 и сбрасывается.***



Протокол резервирования первого перехода (FHRP)

Избыточность маршрутизаторов

- Одним из способов для устранения единой точки отказа на шлюзе по умолчанию является **реализация виртуального маршрутизатора.**
- Несколько маршрутизаторов настраиваются для совместной работы, что создает иллюзию одного маршрутизатора на узлах сети LAN.
- При совместном использовании IP-адреса и MAC-адреса двух или более маршрутизаторов они могут работать, как один виртуальный маршрутизатор.
- Способность сети динамически восстанавливаться после сбоя устройства, выполняющего функцию шлюза по умолчанию, называется **избыточностью на первом хопе**.



Избыточность маршрутизаторов

В случае сбоя активного маршрутизатора протокол резервирования переводит резервный маршрутизатор на новые функции активного маршрутизатора. В случае сбоя активного маршрутизатора происходит следующее:

1. Резервный маршрутизатор перестает видеть сообщения приветствия от пересылающего маршрутизатора.
2. Резервный маршрутизатор принимает роль передающего маршрутизатора.
3. Поскольку новый пересылающий маршрутизатор использует как IP-адрес, так и MAC-адрес виртуального маршрутизатора, конечные устройства не замечают перебоев в обслуживании.

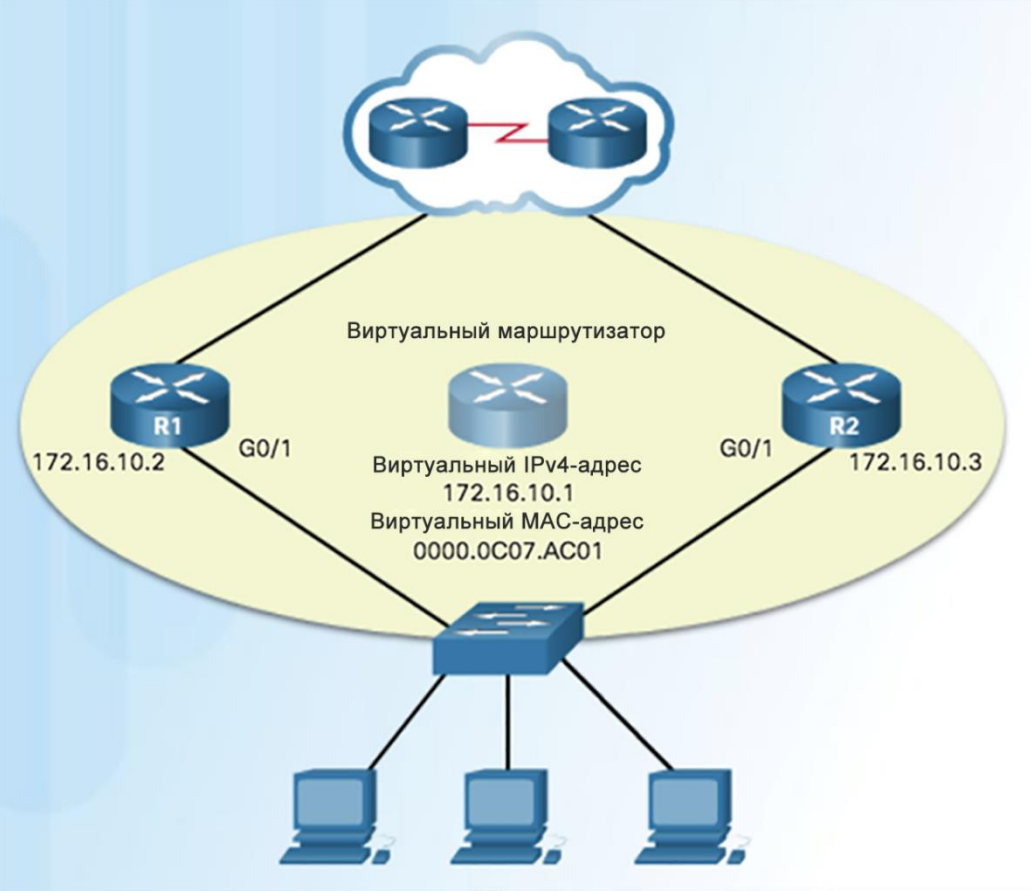
Протоколы резервирования первого перехода

- **Протокол резервирования (Hot Standby Router Protocol, HSRP).** HSRP используется группой маршрутизаторов для выбора активного и резервного устройств.
- **Протокол резервирования виртуального маршрутизатора (VRRPv2)**. Принадлежащий компании протокол, динамически назначающий функцию одному или нескольким VRRP-маршрутизаторам в локальной сети IPv4.
  - Один маршрутизатор выбирается в качестве основного виртуального маршрутизатора, а другие маршрутизаторы выступают в роли резервных на случай отказа основного виртуального маршрутизатора.
- **VRRPv3** — возможность поддержки IPv4 и IPv6.
- **Протокол распределения нагрузки для шлюзов (GLBP).** Принадлежащий компании Cisco протокол FHRP, который обеспечивает защиту трафика данных от неисправного маршрутизатора или сети, обеспечивая при этом **распределение нагрузки** по группе резервных маршрутизаторов.
- **GLBP для IPv6.** Принадлежащий компании Cisco протокол FHRP имеет такие же функции, как протокол GLBP.

Протоколы резервирования первого перехода

✓ Функция HSRP определяет группу маршрутизаторов, состоящую из активного и резервного маршрутизаторов.
✓ Виртуальные IP- и MAC-адреса используются совместно двумя маршрутизаторами.
✓ Для проверки состояния HSRP используется команда **show standby**.
✓ Функция HSRP принадлежит компании Cisco.
✓ Протокол резервирования виртуального маршрутизатора VRRP является стандартным протоколом.

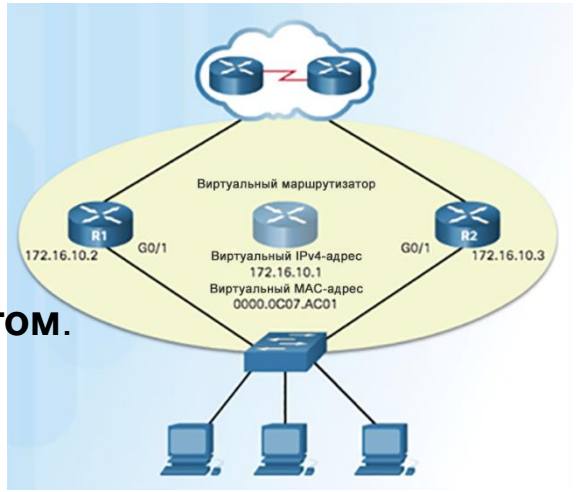
Обзор протокола HSRP



- Протокол HSRP выбирает один из маршрутизаторов в качестве активного маршрутизатора и шлюза по умолчанию.
- Другой маршрутизатор становится резервным.
- В случае сбоя активного маршрутизатора роль активного маршрутизатора и шлюза по умолчанию переходит к резервному маршрутизатору.
- Узлы настроены с одним ВИРТУАЛЬНЫМ адресом шлюза по умолчанию, который распознается и активным и резервным маршрутизатором.

Приоритет и приоритетное вытеснение HSRP

- Роль активных и резервных маршрутизаторов определяется процессом выбора.
- **По умолчанию** в качестве **активного** выбирается маршрутизатор с **максимальным** в численном отношении адресом **IPv4**.
- Выбор HSRP следует определять с помощью приоритета, при этом не нужно использовать самый высокий адрес.
- Приоритет HSRP
  - Используется для определения активного маршрутизатора.
  - Приоритет HSRP по умолчанию — 100.
  - Приоритет задается в диапазоне от 0 до 255, а **активным** становится маршрутизатор **с самым высоким приоритетом**.
  - Используйте команду **standby priority interface**.
- Приоритетное вытеснение HSRP
  - Приоритетное вытеснение — это способность маршрутизатора HSRP запускать процесс повторного выбора.
  - Для запуска нового процесса выбора HSRP необходимо включить механизм приоритетного вытеснения с помощью команды **standby preempt interface.**
  - Маршрутизатор, появившийся в сети с более высоким приоритетом, становится активным маршрутизатором.



Принципы работы протокола HSRP

Состояния и таймеры HSRP

Состояние	Определение
Initial	Это состояние возникает при изменении конфигурации или в том случае, когда интерфейс впервые становится доступным.
Learn	Маршрутизатор не определил виртуальный IP-адрес и пока не получил сообщения приветствия от активного маршрутизатора. В этом состоянии маршрутизатор ожидает получения сообщения приветствия от активного маршрутизатора.
Listen	Маршрутизатору известен виртуальный IP-адрес, но маршрутизатор не является ни активным, ни резервным маршрутизатором. Он прослушивает сообщения приветствия от этих маршрутизаторов.
Speak	Маршрутизатор отправляет периодические сообщения приветствия и активно участвует в процессе выбора активного и/или резервного маршрутизатора.
Standby	Маршрутизатор является кандидатом на роль следующего активного маршрутизатора и периодически отправляет сообщения приветствия.
Active	В настоящее время маршрутизатор пересылает пакеты, отправленные на виртуальный MAC-адрес группы. Маршрутизатор периодически отправляет сообщения приветствия.

- По умолчанию активные и резервные маршрутизаторы HSRP отправляют пакеты приветствия на групповой адрес группы HSRP каждые 3 секунды (таймер приветствия). Резервный маршрутизатор станет активным, если он не получает сообщения приветствия от активного маршрутизатора в течение 10 секунд (таймер удержания).
- Эти настройки таймера можно уменьшить, чтобы ускорить переключение при отказе или приоритетное вытеснение. Однако чтобы избежать повышения нагрузки на ЦП и ненужных изменений резервного состояния, не устанавливайте таймер приветствия менее, чем на 1 секунду, а таймер удержания — менее, чем на 4 секунды.

Настройка HSRP

Команды настройки HSRP

Команда	Определение
`Router(config-if)# standby version 2`	Задает использование HSRP версии 2. По умолчанию используется HSRP версии 1.
`Router(config-if)# standby [group-number] ip-address`	Задает виртуальный IP-адрес HSRP, который будет использоваться для заданной группы. Если группа не задана, то виртуальный IP-адрес назначается группе 0.
`Router(config-if)# standby [group-number] priority [priority-value]`	Задает для нужного активного маршрутизатора более высокий приоритет, чем приоритет по умолчанию (100). Находится в диапазоне от 0 до 255. Если приоритеты не заданы или приоритеты равны, то преимущество имеет маршрутизатор с наивысшим IP-адресом.
`Router(config-if)# standby [group-number] preempt`	Задает на данном маршрутизаторе приоритетное вытеснение активного в настоящий момент маршрутизатора.


```
R1(config)# interface g0/1
R1(config-if)# ip address 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
R2(config)# interface g0/1
R2(config-if)# ip address 172.16.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 172.16.10.1
R2(config-if)# no shutdown
```

Настройка HSRP

Проверка HSRP

Активный маршрутизатор HSRP имеет следующие характеристики:

- Отвечает на ARP-запросы шлюза по умолчанию, отправляя MAC-адрес виртуального маршрутизатора.
- Выполняет активную пересылку пакетов для виртуального маршрутизатора.
- Отправляет сообщения приветствия.
- Содержит данные IP-адреса виртуального маршрутизатора.

Резервный маршрутизатор HSRP имеет следующие характеристики:

- Прослушивает периодические сообщения приветствия.
- Выполняет активную пересылку пакетов, если данные не поступают с активного маршрутизатора.

Для проверки состояния HSRP используется команда **show standby**.

```
Router# show standby
Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
  Gratuitous ARP 14 sent, next in 7.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
       Down Interface Ethernet0/2, pri 15
       Down Interface Ethernet0/3
Group name is "HSRP1" (cfgd)
Follow by groups:
Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.666)
Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec
```

Сбой в работе протокола HSRP

Большинство проблем возникает во время одной из следующих операций HSRP:

- Сбой выбора активного маршрутизатора, который управляет виртуальным IP-адресом для группы
- Сбой отслеживания активного маршрутизатора на резервном маршрутизаторе
- Сбой определения момента, когда управление виртуальным IP-адресом для группы должно быть передано другому маршрутизатору
- Сбой настройки виртуального IP-адреса в качестве шлюза по умолчанию на оконечных устройствах

Распространенные неполадки конфигурации HSRP

Команды отладки также можно использовать для обнаружения следующих распространенных проблем конфигурации:

- Маршрутизаторы HSRP подключены к разным сетевым сегментам. Это может быть вызвано проблемой физического уровня, но также может быть ошибкой конфигурации вложенного интерфейса VLAN.
- Для маршрутизаторов HSRP настроены адреса IPv4 из разных подсетей. Пакеты приветствия HSRP являются локальными. Они не маршрутизируются за пределы сетевого сегмента. Таким образом, если на активном маршрутизаторе случится сбой, резервный маршрутизатор не будет об этом знать.
- Для маршрутизаторов HSRP настроены разные виртуальные адреса IPv4. Виртуальный IPv4-адрес является шлюзом по умолчанию для конечных устройств.
- Для маршрутизаторов HSRP настроены разные номера группы HSRP. Это приведет к тому, что каждый маршрутизатор будет принимать роль активного маршрутизатора.
- Оконечные устройства настроены с использованием неправильного адреса шлюза по умолчанию. Хотя это и не связано непосредственно с протоколом HSRP, однако задание на сервере DHCP одного из реальных IP-адресов маршрутизатора HSRP будет означать, что оконечные устройства смогут подключаться к удаленным сетям, только если этот маршрутизатор HSRP активен.

МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ | НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Протокол DHCP. SLAAC и DHCP.

Коммутация, маршрутизация и беспроводная связь

Введение

Протокол динамической конфигурации узла (DHCP) — это сетевой протокол, обеспечивающий автоматическую IP-адресацию и другую информацию для клиента:

- IP-адрес.
- Маска подсети (IPv4) или длина префикса (IPv6).
- Адрес шлюза по умолчанию.
- Адрес DNS-сервера.

Общие сведения о протоколе DHCPv4

DHCPv4 использует три разных метода присвоения адреса:

Распределение вручную — администратор присваивает устройству-клиенту предварительно выделенный IPv4-адрес, в то время как DHCPv4 только передаёт IPv4-адрес к устройству.

Автоматическое распределение — DHCPv4 автоматически присваивает устройству постоянный ***статический*** IPv4-адрес, выбирая его из пула доступных адресов. Аренда не требуется.

Динамическое распределение — DHCPv4 динамически присваивает или выдаёт в аренду IPv4-адрес из пула адресов на ограниченный период времени по выбору сервера или до тех пор, пока у клиента есть необходимость в адресе. Наиболее распространённый метод.

Общие сведения о протоколе DHCPv4

Широковещательная рассылка сообщения обнаружения всех доступных серверов DHCP (**DHCPDISCOVER**) со своего MAC-адреса

Сервер DHCP отвечает **одноадресным сообщением** с предложением DHCP (**DHCPOFFER**), которое разрешает клиенту арендовать адрес. Сообщение с предложением содержит назначаемые IP-адрес и маску подсети, IP-адрес DNS-сервера и IP-адрес шлюза по умолчанию, срок аренды. Сервер DHCP создает запись ARP, состоящей из MAC-адреса запрашивающего клиента и выданного клиенту IPv4-адреса.

Клиент DHCP

Клиент может получить несколько сообщений DHCPOFFER, если в локальной сети есть несколько серверов DHCP. Поэтому клиент должен выбрать один из серверов, для чего он отправляет сообщение **широковещательной рассылкой** с запросом DHCP (**DHCPREQUEST**), в котором указывается конкретный сервер и предложение аренды, которое принимает клиент, и косвенное сообщение отклонения для всех других серверов, которые могли предоставить клиенту предложение привязки к предложенным сервером параметрам. Сообщение DHCPREQUEST используется как для первоначальной аренды адреса, так и для её продления.

Сервер DHCP

Сервер проверяет, не используется ли выдаваемый в аренду IP-адрес с помощью отправки эхо-запроса по протоколу ICMP на этот адрес. После этого сервер создаёт новую запись ARP для клиентской аренды.
Если запрашиваемый IP-адрес по-прежнему доступен, сервер возвращает **одноадресное сообщение** с подтверждением DHCP (**DHCPACK**). Если предложение больше не действительно, сервер отвечает одноадресным сообщением с отрицательным подтверждением DHCP (**DHCPNAK**).

Принцип работы протокола DHCPv4

Формат сообщений DHCPv4

8	16	24	32
Код операции (1) Общий тип сообщения: 1 – сообщение-запрос; 2 — сообщение-ответ.	**Тип оборудования (1)** Тип аппаратного оборудования: 1 — Ethernet, 15 — Frame Relay, 20 — последовательный канал и т.д. Эти же коды используются в сообщениях ARP.	**Длина физического адреса (1)**	**Переходы (1)** Управление процессом пересылки сообщений. Устанавливается клиентом на 0 перед отправкой сообщения-запроса.
Идентификатор транзакции (4) - используется клиентом для согласования запроса с ответами от DHCPv4-серверов.			
Секунды (2) – количество секунд с момента, когда клиент начал пытаться получить или продлить аренду. Используется DHCPv4-серверами для расстановки приоритетности ответов, в случае нескольких клиентских запросов.	**Флаги (2)** - применяются клиентом, который не знает своего IPv4-адреса при отправлении запроса. Используется только один из 16 бит. Значение 1 в этом поле сообщает DHCPv4-серверу или агенту-ретранслятору, принимающему запрос, что ответ должен быть послан в форме широковещательной рассылки.		
IP-адрес клиента (4) – используется клиентом при обновлении адреса по истечении срока аренды для продления аренды. Клиент подставляет собственный IPv4-адрес в это поле только в случае, если у него есть действующий IPv4-адрес, совпадающий с ранее назначенным; в противном случае значение поля устанавливается на 0.			
Ваш IP-адрес (4) – используется сервером для присвоения нового IPv4-адреса клиенту.			
IP-адрес сервера (4) – применяется сервером для распознавания адреса сервера, который клиент должен использовать для следующего шага в процессе самонастройки. Этот сервер может являться (или не являться) сервером, посылающим ответ. Сервер, посылающий ответ, всегда включает собственный IPv4-адрес в отдельное поле - опцию Идентификатор сервера DHCPv4.			
IP-адрес шлюза (4) – Использование адреса шлюза упрощает передачу DHCPv4- запросов и ответов между клиентом и сервером, которые находятся в разных подсетях или сетях.			
Физический адрес клиента (16) – MAC-адрес клиента			
Имя сервера (64) – необязательно для заполнения, используется сервером, отправляющим сообщения DHCPOFFER или DHCPACK. Именем сервера может быть простой текстовый псевдоним или доменное имя DNS-сервера.			
Имя файла загрузки (128) – используется клиентом для запроса файла загрузки в сообщении DHCPDISCOVER и сервером в сообщении DHCPOFFER для точного задания директории файла загрузки и имени файла.			
Параметры DHCP (размер не задан) – опции DHCP, а также некоторые параметры, необходимые для основных операций протокола DHCP. Длина этого поля меняется. Поле может использоваться как клиентом, так и сервером.			

Сообщения обнаружения и предложения DHCPv4

Кадр Ethernet	IP	UDP	DHCPDISCOVER
DST MAC: FF:FF:FF:FF:FF:FF SRC MAC: MAC A	IP SRC: 0.0.0.0 IP DST: 255.255.255.255	UDP 67	CIADDR: 0.0.0.0 GIADDR: 0.0.0.0 Маска: 0.0.0.0 CHADDR: MAC A

MAC: адрес управления доступом к среде передачи данных
CIADDR: IP-адрес клиента
GIADDR: IP-адрес шлюза
CHADDR: аппаратный адрес клиента

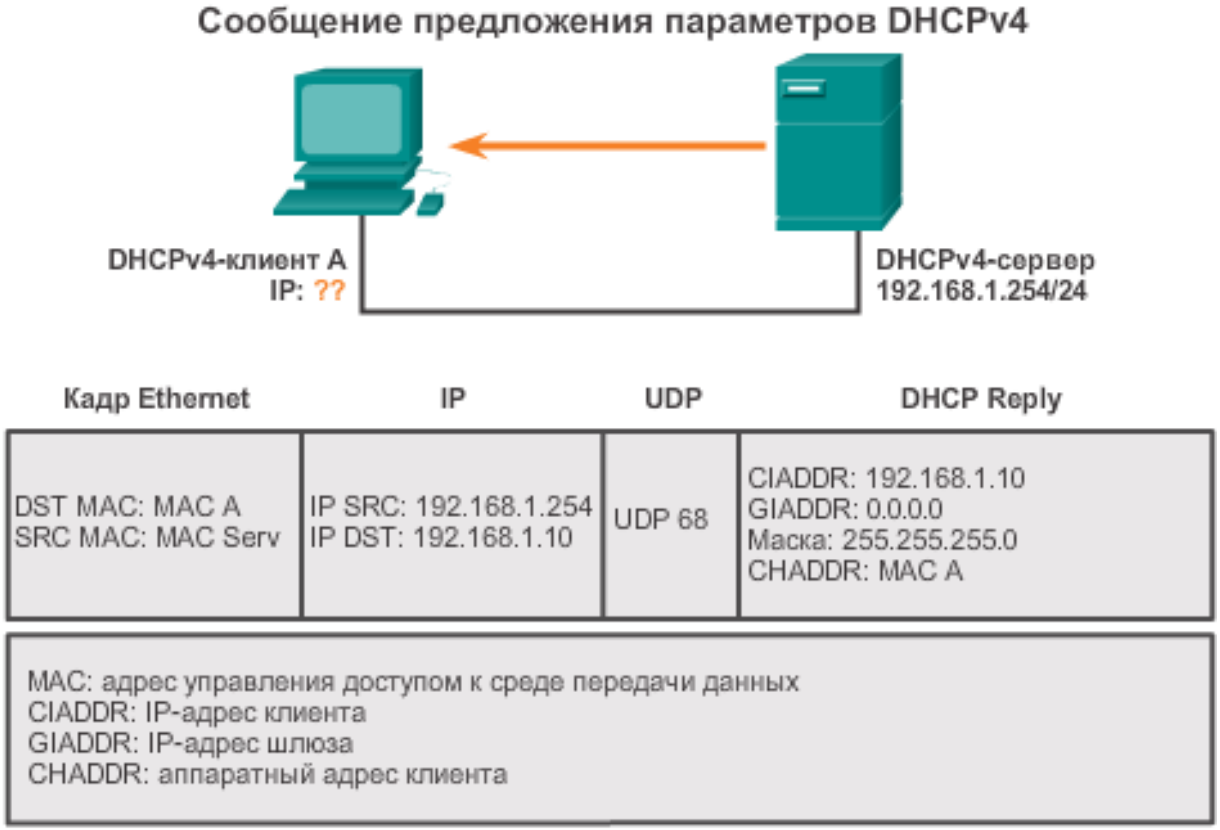
DHCP-клиент посылает направленную широковещательную IP-рассылку с DHCPDISCOVER-пакетом. В этом примере DHCP-сервер находится в том же сегменте и принимает этот запрос. Сервер отмечает, что поле GIADDR пустое, таким образом, клиент находится в том же сегменте. Сервер также отмечает физический адрес клиента в пакете запроса.

Сообщение **DHCPDISCOVER** представляет собой широковещательную рассылку IPv4 (IPv4-адрес назначения 255.255.255.255).

Поскольку у клиента ещё нет настроенного IPv4-адреса, используется IPv4-адрес источника — 0.0.0.0.

IPv4-адрес клиента (CIADDR), адрес основного шлюза (GIADDR) и маска подсети в сообщении DHCPDISCOVER соответствуют используемому адресу 0.0.0.0.

Сообщения обнаружения и предложения DHCPv4



DHCPv4-сервер отвечает на сообщение DHCPDISCOVER сообщением **DHCPOFFER**. Это сообщение содержит предварительные настройки для клиента: IPv4-адрес клиента, предложенный сервером, маску подсети, срок аренды и IPv4-адрес DHCPv4-сервера, от которого исходит предложение.

Сообщение DHCPOFFER может быть также настроено для содержания дополнительных данных, таких как время обновления аренды и адрес DNS-сервера.

Сервер DHCP отвечает на сообщение DHCPDISCOVER, высылая значения IP-адреса (CIADDR) и маски подсети. Используя физический адреса устройства-клиента (CHADDR), сервер создаёт и отправляет кадр запрашивающему клиенту.

Для завершения процесса клиент и сервер отправляют сообщения подтверждения.

Конфигурация сервера DHCPv4. Проверка.

- Маршрутизатор Cisco под управлением ОС Cisco IOS можно настроить в качестве DHCPv4-сервера. Для настройки протокола DHCP:

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

1. Исключите административно назначенные адреса из пула.
2. Задайте имя пула DHCP.
3. Определите диапазон адресов и маску подсети.
4. Назначьте шлюз по умолчанию.
5. Дополнительные элементы, которые можно включить в пул — сервер DNS, имя домена.

- Команды проверки DHCP

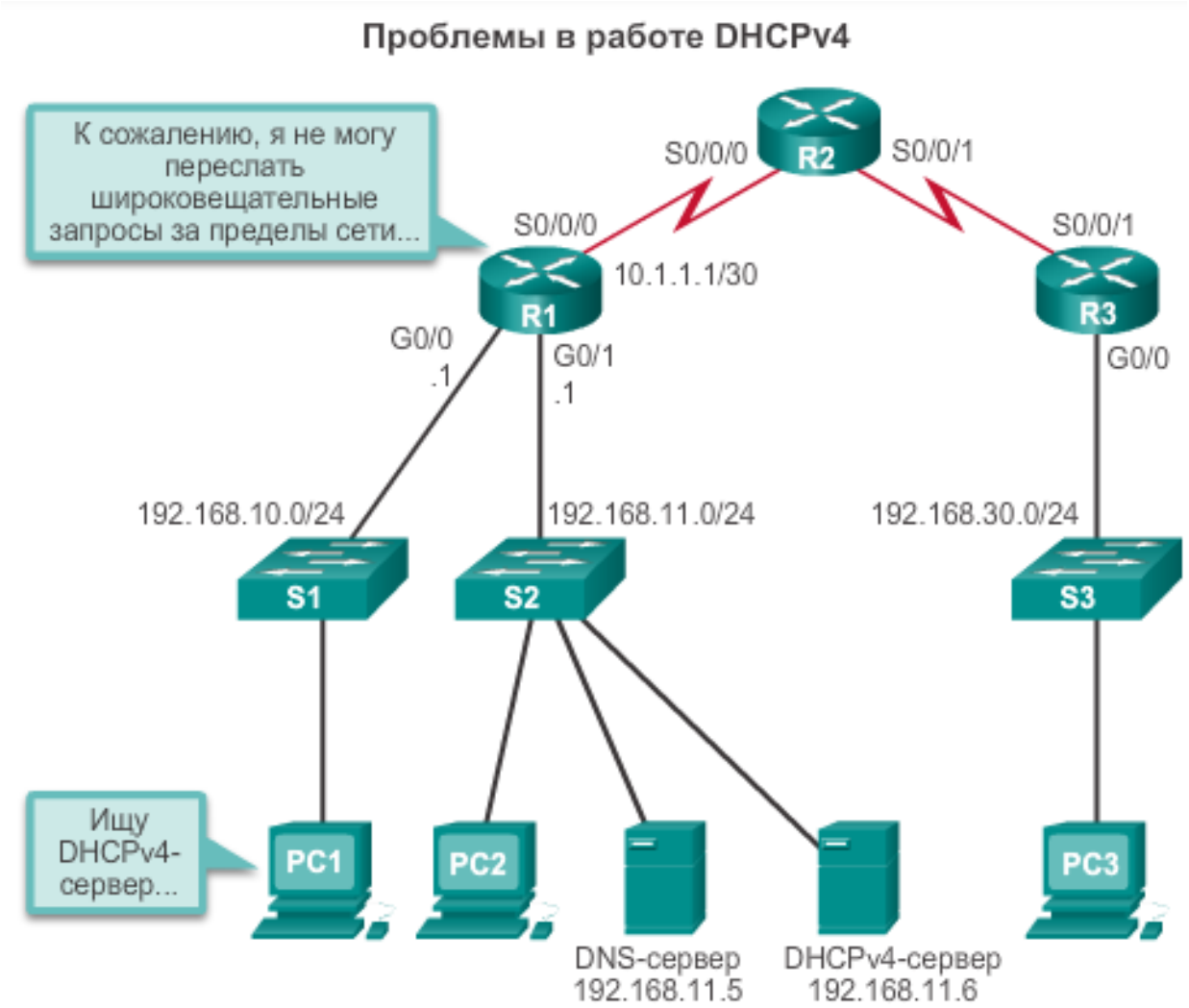
  show running-config | section dhcp

  show ip dhcp binding

  show ip dhcp server statistics

- Для отключения dhcp выполните команду **no service dhcp.**

Ретрансляция DHCPv4



В этом сценарии маршрутизатор R1 не настроен в качестве DHCPv4-сервера и не отправляет сообщения широковещательной рассылки, поскольку DHCPv4-сервер расположен в другой сети, PC1 не может получить IP-адрес через DHCP.

Для этого необходимо R1 сконфигурировать как **агент DHCPv4-ретрансляции** и назначить интерфейсу G0/0 **вспомогательный адрес** DHCPv4-сервера 192.168.11.6.

Ретрансляция DHCPv4

Использование **вспомогательного IP-адреса (ip helper address)** позволяет маршрутизатору пересылать сообщения широковещательной рассылки DHCPv4 на сервер DHCPv4. Выполняет функцию агента-ретранслятора.

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<Output omitted>
```

Когда маршрутизатор R1 сконфигурирован как агент DHCPv4-ретрансляции, он принимает широковещательные запросы, а затем отправляет эти запросы как одноадресную рассылку на IPv4-адрес 192.168.11.6. Команда **show ip interface** применяется для проверки конфигурации.

Конфигурация маршрутизатора в качестве DHCPv4-клиента


```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  <Output omitted>
```

В некоторых случаях маршрутизаторы Cisco **в небольших или домашних офисах** (SOHO) и филиалах должны быть настроены **в качестве DHCPv4-клиентов** аналогично настройке клиентских компьютеров. Используемый метод зависит от интернет-провайдера. В простейшей конфигурации для соединения с кабельным или DSL-модемом используется Ethernet-интерфейс. *Для настройки Ethernet-интерфейса в качестве DHCP-клиента* используйте команду режима настройки интерфейса **ip address dhcp**.

Поиск и устранение неполадок в работе протокола DHCPv4

Задачи поиска и устранения неполадок

Поиск и устранение неполадок. Задача 1. Разрешение конфликтов IPv4-адресов

У клиента, подключённого к сети, может **истечь срок аренды** IPv4-адреса. Если клиент не возобновит аренду, DHCPv4-сервер может переназначить этот IPv4-адрес другому клиенту. После перезагрузки клиент запросит IPv4-адрес. Если DHCPv4-сервер не даст ответ достаточно быстро, клиент будет использовать IPv4-адрес, использовавшийся в последний раз. Возникает ситуация, когда **два клиента используют один IPv4-адрес**, создавая **конфликт**.

Команда **show ip dhcp conflict** отображает все конфликты адресов, зарегистрированные DHCPv4-сервером. Для обнаружения клиента сервером используется команда **ping**. Для обнаружения конфликта клиент использует протокол разрешения адресов (ARP). **При обнаружении конфликта адрес удаляется из пула и не присваивается до устранения конфликта администратором.**

Выходные данные отображают IP-адреса, конфликтующие с сервером DHCP. В данных указан метод обнаружения (detection method) и время обнаружения (detection time) конфликтующих IP-адресов, предложенных сервером DHCP.

```
R1# show ip dhcp conflict
IP address       Detection Method      Detection time
192.168.10.32    Ping                   Feb 16 2013 12:28 PM
192.168.10.64    Gratuitous ARP         Feb 23 2013 08:12 AM
```

Поиск и устранение неполадок в работе протокола DHCPv4

Задачи поиска и устранения неполадок

Поиск и устранение неполадок. Задача 2. Проверка физического соединения

Для начала необходимо применить команду **show interfaces** *interface*, чтобы убедиться, что **интерфейс маршрутизатора**, действующий **в качестве основного шлюза для клиента, функционирует.** Если статус интерфейса отличается от статуса up, трафик (включая запросы DHCP-клиента) не проходит через порт.

Поиск и устранение неполадок. Задача 3. Проверка связности с использованием статического IP-адреса

При проведении работ по поиску и устранению неполадок любой неисправности DHCPv4, **необходимо проверить связность (доступ к сетевым ресурсам) путём настройки статической IPv4-адресации на клиентской рабочей станции.** Если рабочей станции не удаётся получить доступ к сетевым ресурсам, несмотря на наличие статически настроенного IPv4-адреса, DHCPv4 не является источником проблемы. В этом случае необходимо провести проверку сетевого подключения.

Поиск и устранение неполадок в работе протокола DHCPv4

Задачи поиска и устранения неполадок

Поиск и устранение неполадок. Задача 4. Проверка настройки порта коммутатора

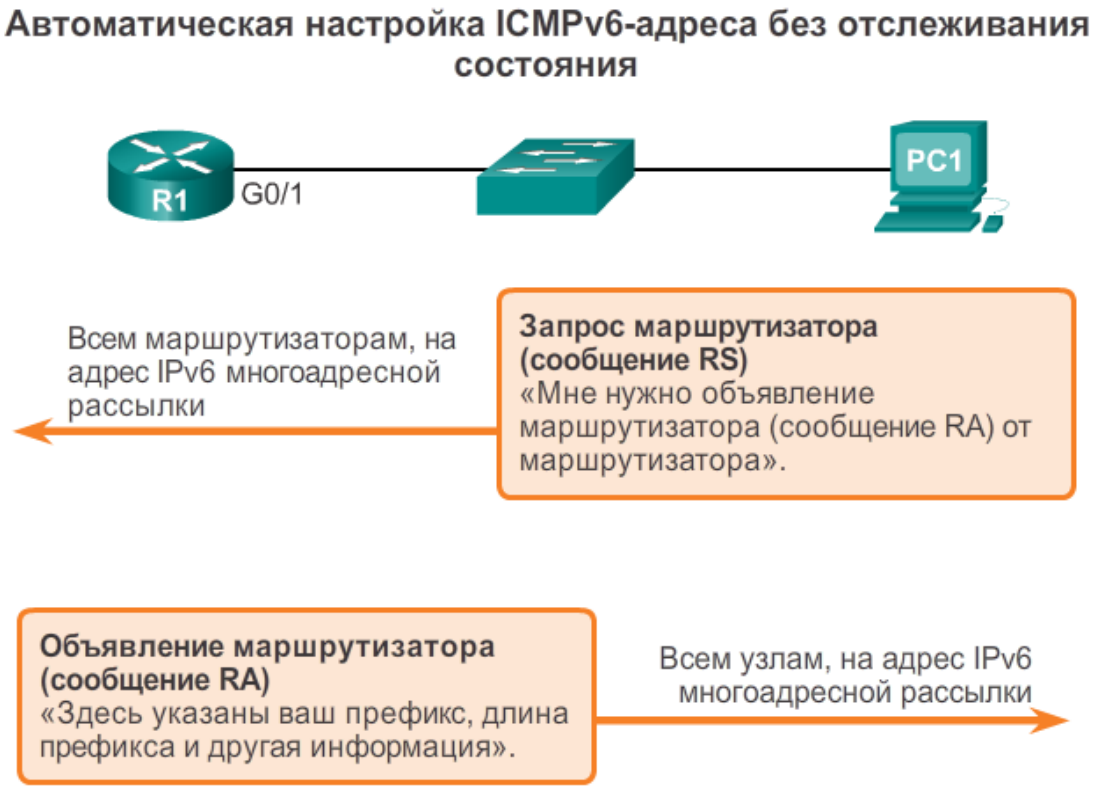
В случае если DHCPv4-клиент не может получить IPv4-адрес от DHCPv4-сервера при загрузке, стоит попробовать получить IPv4-адрес от DHCPv4-сервера, **вручную отправив DHCPv4-запрос с устройства-клиента**.
Примечание. Если между клиентом и DHCPv4-сервером есть **коммутатор**, и клиент не может получить настройки DHCP, причиной могут служить **неполадки в настройке порта коммутатора**. Причиной могут быть проблемы, связанные с созданием транковых и логических каналов, а также с протоколами STP и RSTP. Решением наиболее часто возникающих проблем DHCPv4-клиента при первоначальной установке коммутатора Cisco может стать настройка расширения PortFast и пограничного порта.

Поиск и устранение неполадок. Задача 5. Диагностика работы протокола DHCPv4 в той же подсети или VLAN

Важно различать, **правильно ли функционирует DHCPv4 в качестве DHCPv4-сервера, когда клиент находится в той же подсети или VLAN**. В случае если протокол DHCPv4 работает корректно при условии, что клиент находится в той же подсети или VLAN, **проблема** может заключаться **в агенте DHCP-ретрансляции**. Если неполадки сохраняются даже при проверке работы DHCPv4 в той же подсети или VLAN в качестве DHCPv4-сервера, проблема обычно заключается в DHCPv4-сервере.

Автоматическая настройка адреса без отслеживания состояния (SLAAC) для IPv6

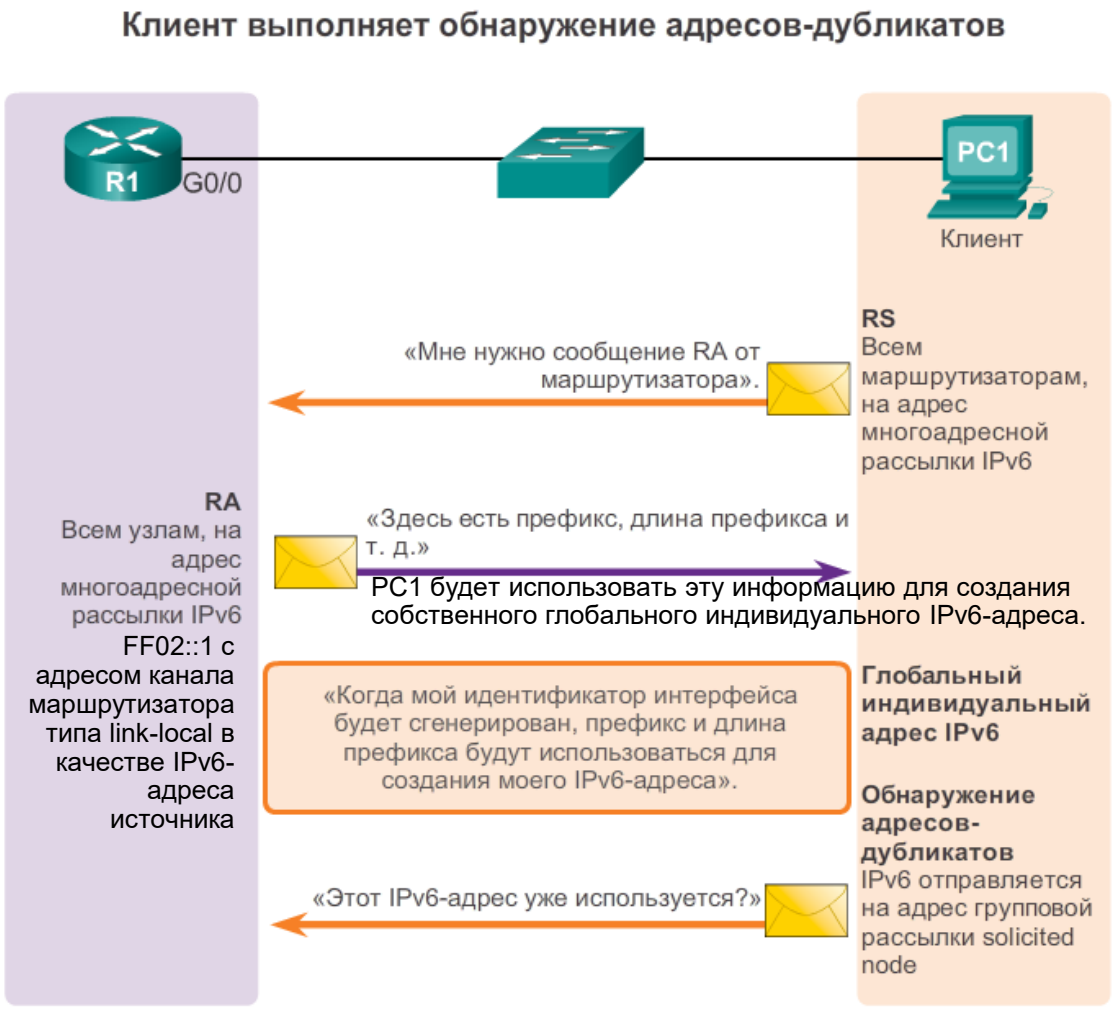
Автоматическая настройка адреса без отслеживания состояния (SLAAC) — это способ получения устройством глобального IPv6-адреса одноадресной рассылки без использования DHCPv6-сервера.



Существует два метода, с помощью которых глобальные индивидуальные IPv6-адреса могут быть присвоены динамически:

- Автоматическая настройка адреса без отслеживания состояния (SLAAC),
- Протокол динамической конфигурации сетевого узла (DHCP) для IPv6 (DHCPv6 с отслеживанием состояния)

Принцип работы SLAAC



PC1 имеет теперь 64-разрядный префикс сети, но требует 64-битный идентификатор интерфейса (IID) для создания глобального индивидуального адреса.

Существует два способа создания для PC1 собственного уникального ID:

EUI-64 — при помощи процесса EUI-64 PC1 создаёт IID, используя свой 48-битный MAC-адрес.

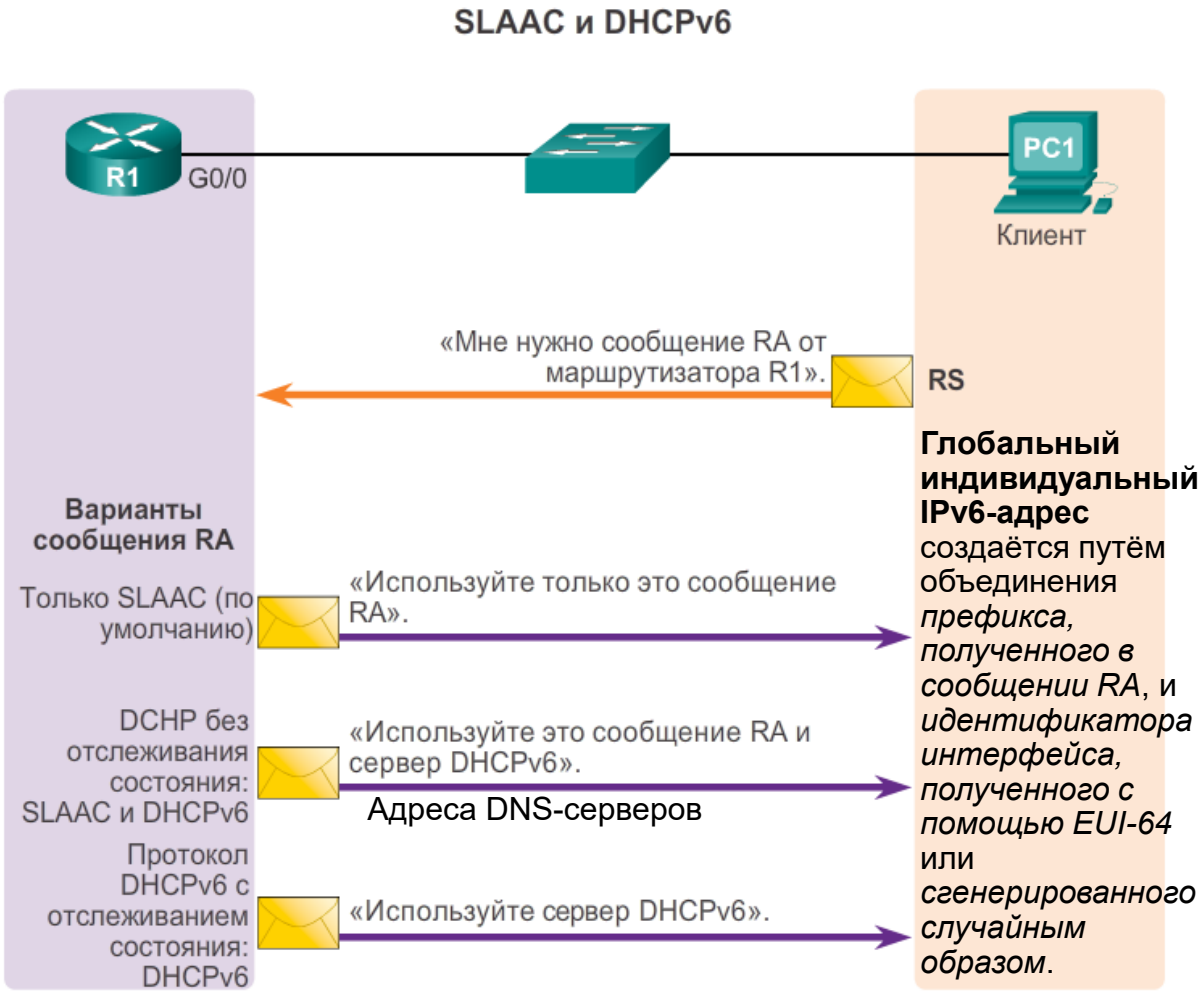
Генерация случайным образом — 64-битный IID может быть случайным числом, сгенерированным операционной системой клиента.

SLAAC и DHCPv6

Настроен ли клиент на автоматическое получение информации об IPv6-адресации с использованием SLAAC, DHCPv6 или сочетанием обоих вариантов, *зависит от настроек, содержащихся в сообщении RA*.

ICMPv6 сообщения RA содержат два флага, обозначающих, какой из вариантов должен быть использован клиентом: *флаг управляемой конфигурации адресов **(M)*** и *флаг другой конфигурации **(O)***. Различные сочетания флагов M и O, сообщения RA выбирают один из трёх вариантов адресации устройства IPv6:

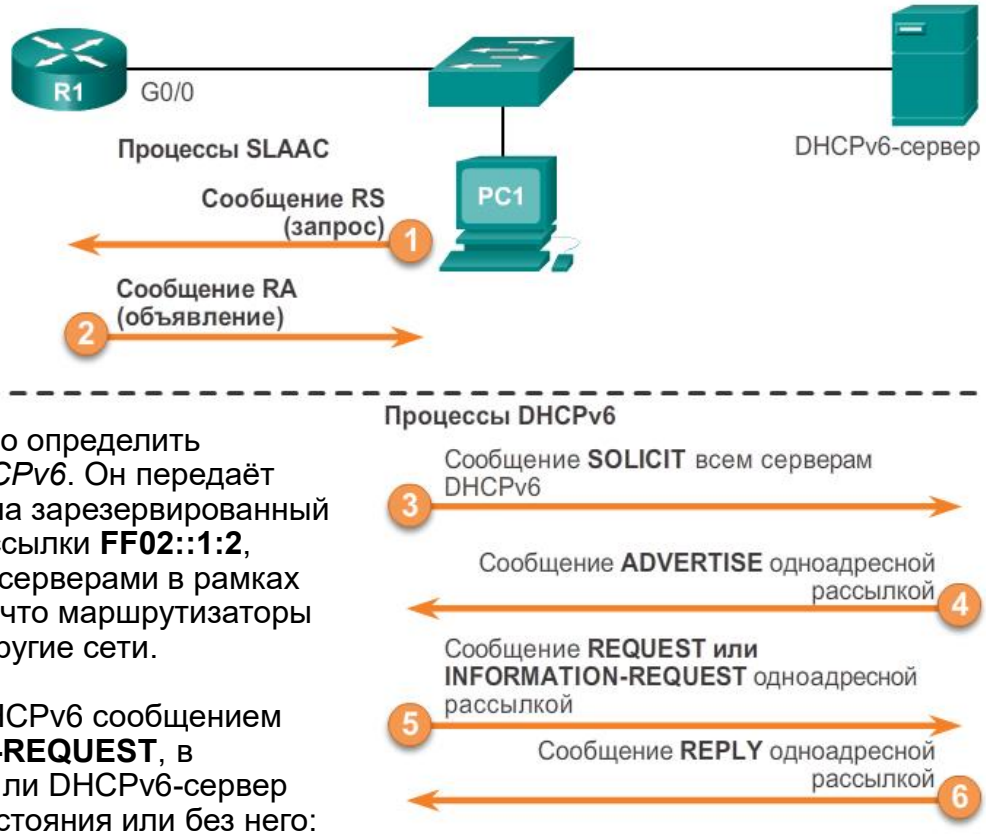
- **M=0, O=0: *SLAAC*** (только объявление маршрутизатора);
- **M=0, O=1: *протокол DHCPv6 без отслеживания состояния*** (объявления маршрутизатора и DHCPv6);
- **M=1: *протокол DHCPv6 с отслеживанием состояния*** (только DHCPv6).



Операции протокола DHCPv6

1-2. Работа DHCPv6 начинается с сообщения **RA**, отправленного от маршрутизатора по протоколу ICMPv6. Сообщение RA может отправляться периодически или в ответ на запрос устройства **RS**. Если вариант работы DHCPv6 указан в сообщении RA, устройство начинает передачу информации по схеме клиент-сервер с использованием DHCPv6.

Сообщения протокола DHCPv6 посылаются через протокол UDP: порт 546 – от сервера к клиенту, порт 547 – от клиента к серверу.



4. Один или несколько серверов DHCPv6 отвечают DHCPv6-сообщением **ADVERTISE**, которое сообщает DHCPv6-клиенту, что *сервер доступен* для предоставления службы DHCPv6.

3. DHCPv6-клиенту необходимо определить *местоположение сервера DHCPv6*. Он передаёт сообщение DHCPv6 **SOLICIT** на зарезервированный IPv6-адрес многоадресной рассылки **FF02::1:2**, используемый всеми DHCPv6 серверами в рамках канала link-local, это означает, что маршрутизаторы не направляют сообщения в другие сети.

6. Сервер отправляет клиенту DHCPv6 сообщение **REPLY**, содержащее запрашиваемую в сообщении REQUEST или INFORMATION-REQUEST информацию.

5. Клиент отвечает серверу DHCPv6 сообщением **REQUEST** или **INFORMATION-REQUEST**, в зависимости от того, является ли DHCPv6-сервер сервером с отслеживанием состояния или без него:

DHCPv6-клиент без отслеживания состояния — клиент отправляет DHCPv6 сообщение **INFORMATION-REQUEST** серверу DHCPv6, запрашивая *только параметры конфигурации*, *например, адрес DNS-сервера*. Клиент создаёт собственный IPv6-адрес при помощи префикса из сообщения RA и самогенерируемого идентификатора интерфейса.
DHCPv6-клиент с отслеживанием состояния — клиент отправляет DHCPv6 сообщение **REQUEST** серверу для получения *IPv6-адреса и всех остальных параметров конфигурации от сервера*.

Конфигурация маршрутизатора в качестве DHCPv6-сервера без отслеживания состояния

Настройка DHCPv6-сервера без отслеживания состояния на маршрутизаторе

Шаг 1. Активация маршрутизации IPv6

```
Router(config)# ipv6 unicast-routing
```

необходима для отправки сообщений RA по протоколу ICMPv6

Шаг 2. Настройка DHCPv6-пула

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6)#
```

создаёт пул с именем pool-name и переводит маршрутизатор в режим конфигурации DHCPv6

С помощью функции SLAAC клиент принимает информацию, необходимую для создания глобального индивидуального IPv6-адреса, информацию о шлюзе по умолчанию. При этом сервер DHCPv6 без отслеживания состояния можно настроить для предоставления информации, которая могла не быть включена в сообщение RA, например, адреса DNS-сервера и доменного имени.

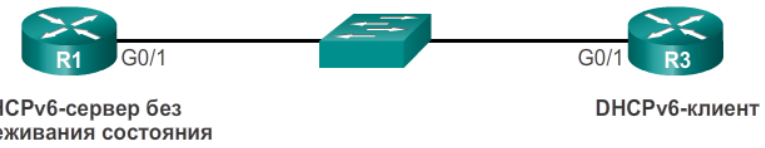
Шаг 3. Настройка параметров пула

```
Router(config-dhcpv6)# dns-server dns-server-address
Router(config-dhcpv6)# domain-name domain-name
```

Шаг 4. Настройка DHCPv6-интерфейса

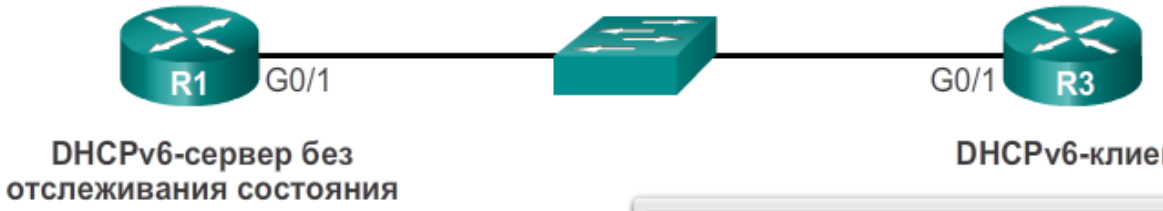
```
Router(config)# interface type number
Router(config-if)# ipv6 dhcp server pool-name
Router(config-if)# ipv6 nd other-config-flag
```

Команда интерфейса **ipv6 dhcp server** *pool-name* привязывает созданный DHCPv6-пул к интерфейсу. Маршрутизатор отвечает на DHCPv6-запросы на этом интерфейсе информацией, содержащейся в пуле. Значение флага O необходимо изменить с 0 на 1, используя команду интерфейса **ipv6 nd other-config-flag**. Сообщения RA, отправленные на этот интерфейс, указывают, что дополнительная информация доступна на **DHCPv6-сервере без отслеживания состояния**.



DHCPv6 без отслеживания состояния

Конфигурация маршрутизатора в качестве DHCPv6-клиента без отслеживания состояния




```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#
```

- Команда **ipv6 enable** используется ввиду того, что маршрутизатор ещё не имеет глобального индивидуального адреса.
- Команда **ipv6 address autoconfig** включает автоматическую настройку IPv6-адресации с использованием SLAAC.
- Проверка DHCP-клиента без отслеживания состояния с помощью следующих команд:
  - **show IPv6 interface**
  - **debug ipv6 dhcp detail**

Конфигурация маршрутизатора в качестве DHCPv6-сервера с отслеживанием состояния

Настройка DHCPv6-маршрутизатора с отслеживанием состояния

Шаг 1. Активация маршрутизации IPv6

```
Router(config)# ipv6 unicast-routing
```

необходима для отправки сообщений RA по протоколу ICMPv6

Шаг 2. Настройка DHCPv6-пула

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6)#
```

создаёт пул с именем pool-name и переводит маршрутизатор в режим конфигурации DHCPv6

Шаг 3. Настройка параметров пула

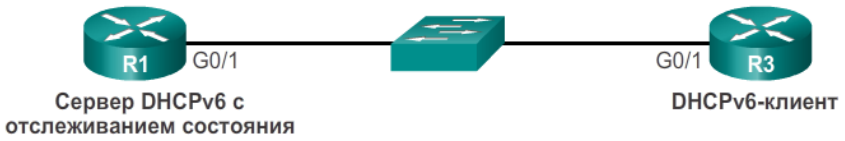
```
Router(config-dhcpv6)# address prefix/length [lifetime
                       {valid-lifetime preferred-lifetime
                       | infinite}]
Router(config-dhcpv6)# dns-server dns-server-address
Router(config-dhcpv6)# domain-name domain-name
```

Команда **address prefix** используется для обозначения адресного пула, из которого сервер будет выделять адреса. Параметр **lifetime** указывает действительное и предпочтительное время аренды в секундах.
Другая информация, предоставленная DHCPv6-сервером с отслеживанием состояния, обычно включает адрес DNS-сервера и доменное имя.

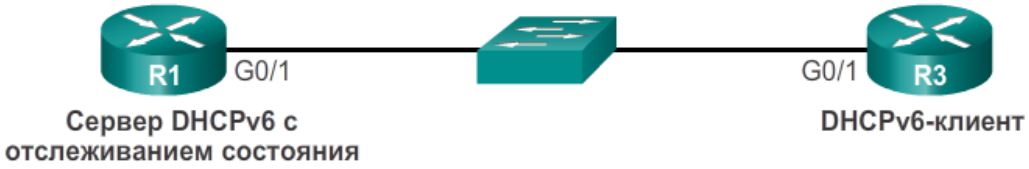
Шаг 4. Настройка DHCPv6-интерфейса

```
Router(config)# interface type number
Router(config-if)# ipv6 dhcp server pool-name
Router(config-if)# ipv6 nd managed-config-flag
```

Команда интерфейса **ipv6 dhcp server** *pool-name* привязывает созданный DHCPv6-пул к интерфейсу. Маршрутизатор отвечает на DHCPv6-запросы на этом интерфейсе информацией, содержащейся в пуле. Значение флага M необходимо изменить с 0 на 1 с помощью команды интерфейса **ipv6 nd managed-config-flag**. Установленное значение говорит устройству не использовать SLAAC, а получить настройки IPv6-адресации и все параметры конфигурации от **DHCPv6-сервера с отслеживанием состояния**.



Конфигурация маршрутизатора в качестве DHCPv6-клиента с отслеживанием состояния




```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
R3(config-if)#
```

Команда **ipv6 enable** позволяет маршрутизатору получить адрес link-local, чтобы отправлять сообщения RS.

Команда режима конфигурации интерфейса **ipv6 address dhcp** разрешает маршрутизатору выполнять функцию DHCPv6-клиента на данном интерфейсе.

Проверка DHCPv6-сервера с отслеживанием состояния при помощи:

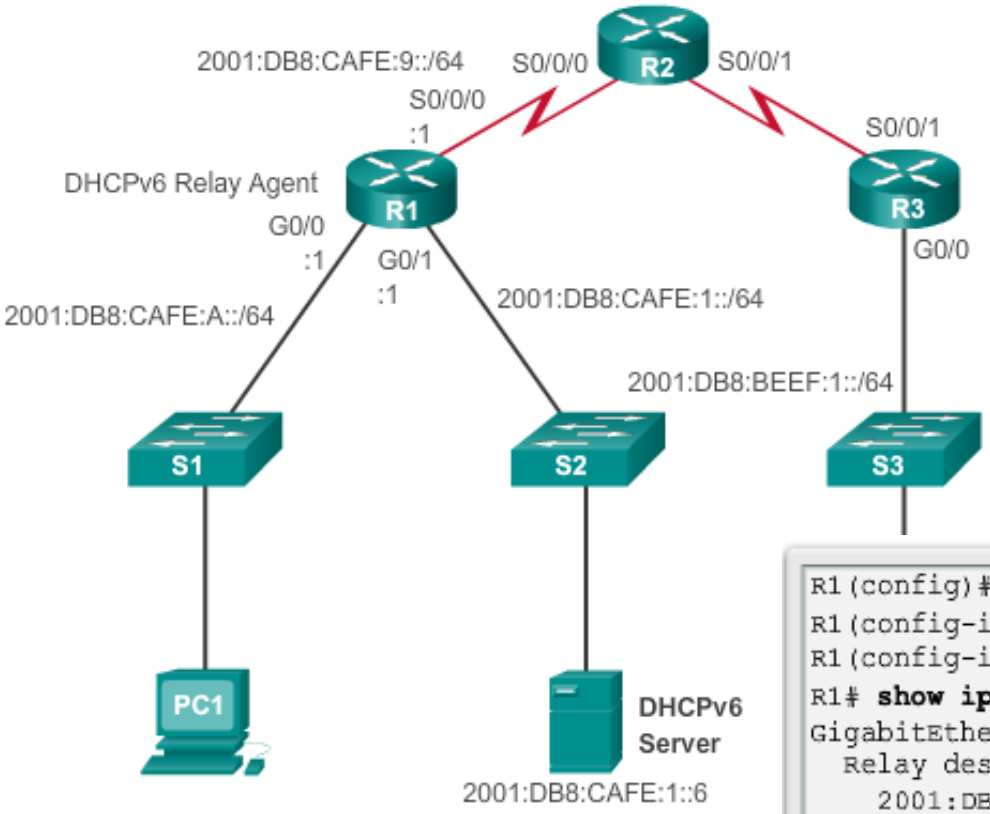
show ipv6 dhcp pool

show ipv6 dhcp binding

Проверка DHCPv6-клиента с отслеживанием состояния при помощи:

show ipv6 interface

Конфигурация маршрутизатора в качестве агента ретрансляции DHCPv6 с отслеживанием состояния



Агент DHCPv6-ретрансляции настроен с помощью команды **ipv6 dhcp relay destination** на интерфейсе, соответствующем DHCPv6-клиенту, с использованием адреса DHCPv6-сервера в качестве адреса назначения.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
R1#
```