

**Министерство образования Республики Беларусь
Учреждение образования
Гомельский государственный университет им. Ф. Скорины**

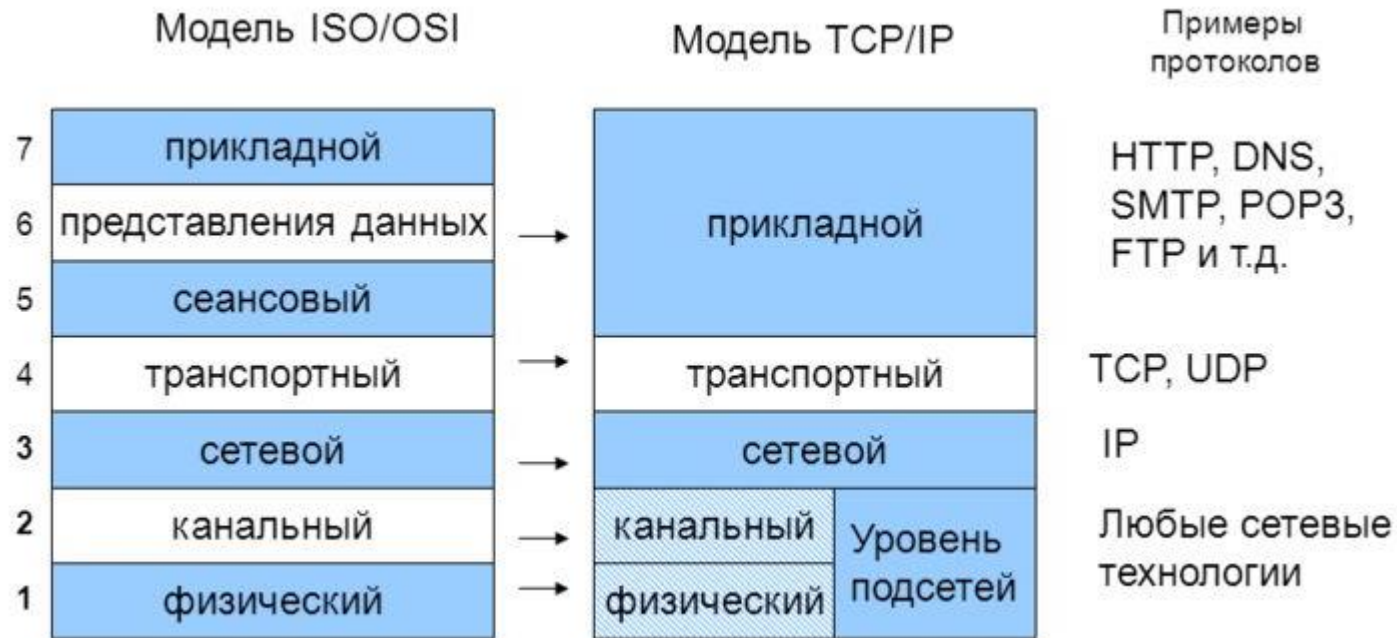
Физический факультет

«Компьютерные сети и Web-дизайн»

Лекция – IP-адресация

Лектор – ст. преподаватель Грищенко В.В.

Адресация в небольших сетях



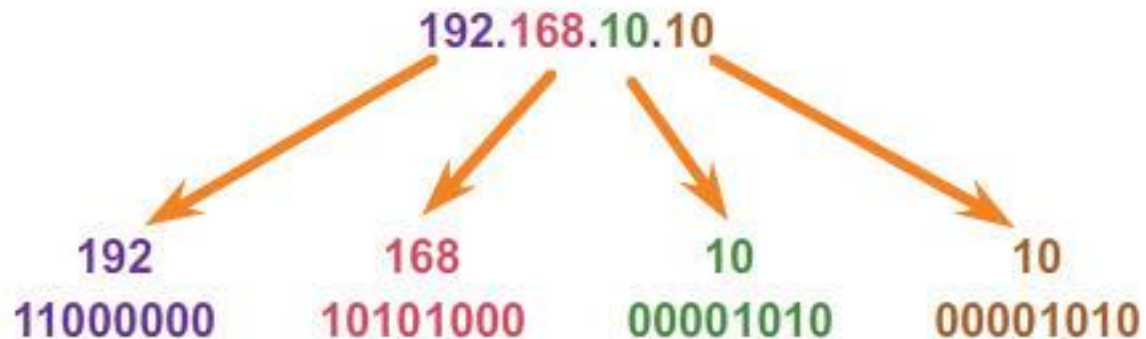
Адресация в небольших сетях

- Схему IP-адресации необходимо планировать, документировать и обслуживать с учётом типа устройств, получающих адрес.
- Примеры устройств, которые будут включены в проект IP-сети:
 - оконечные пользовательские устройства;
 - серверы и периферийные устройства;
 - узлы с доступом через Интернет;
 - промежуточные устройства.
- Спланированные схемы IP-адресации позволяют администратору:
 - отслеживать устройства и устранять неполадки;
 - контролировать доступ к ресурсам.

Структура IPv4-адреса

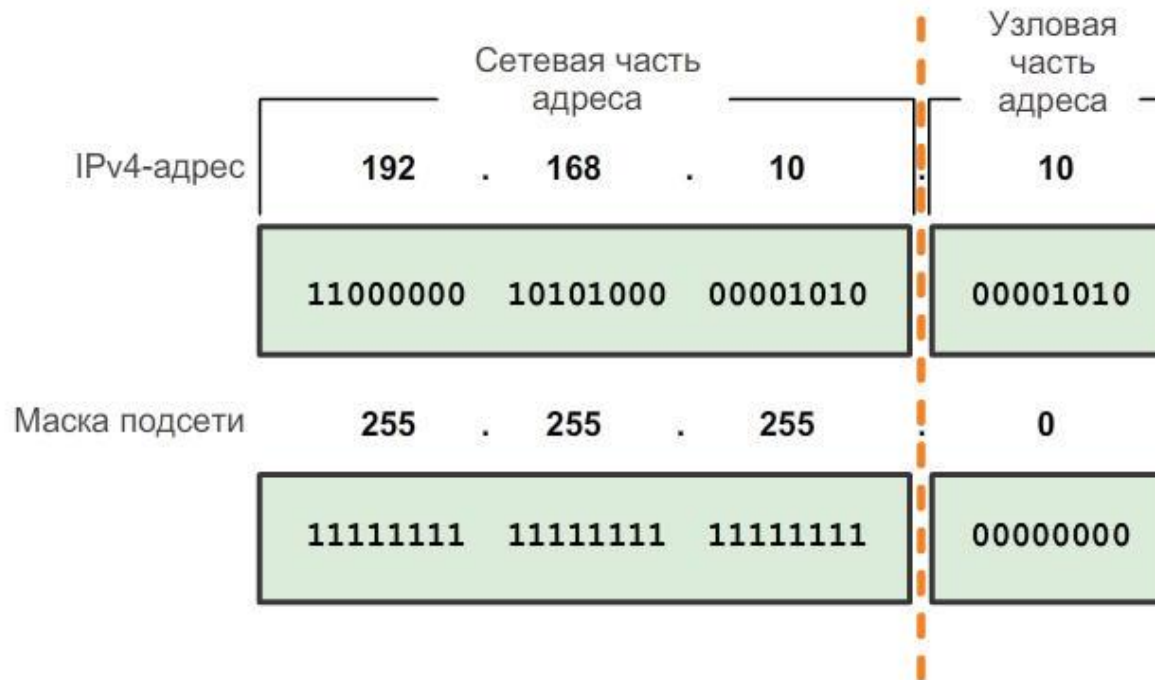
Преобразование десятичных чисел в двоичные

Преобразование десятичных чисел в двоичные



Маска подсети IPv4

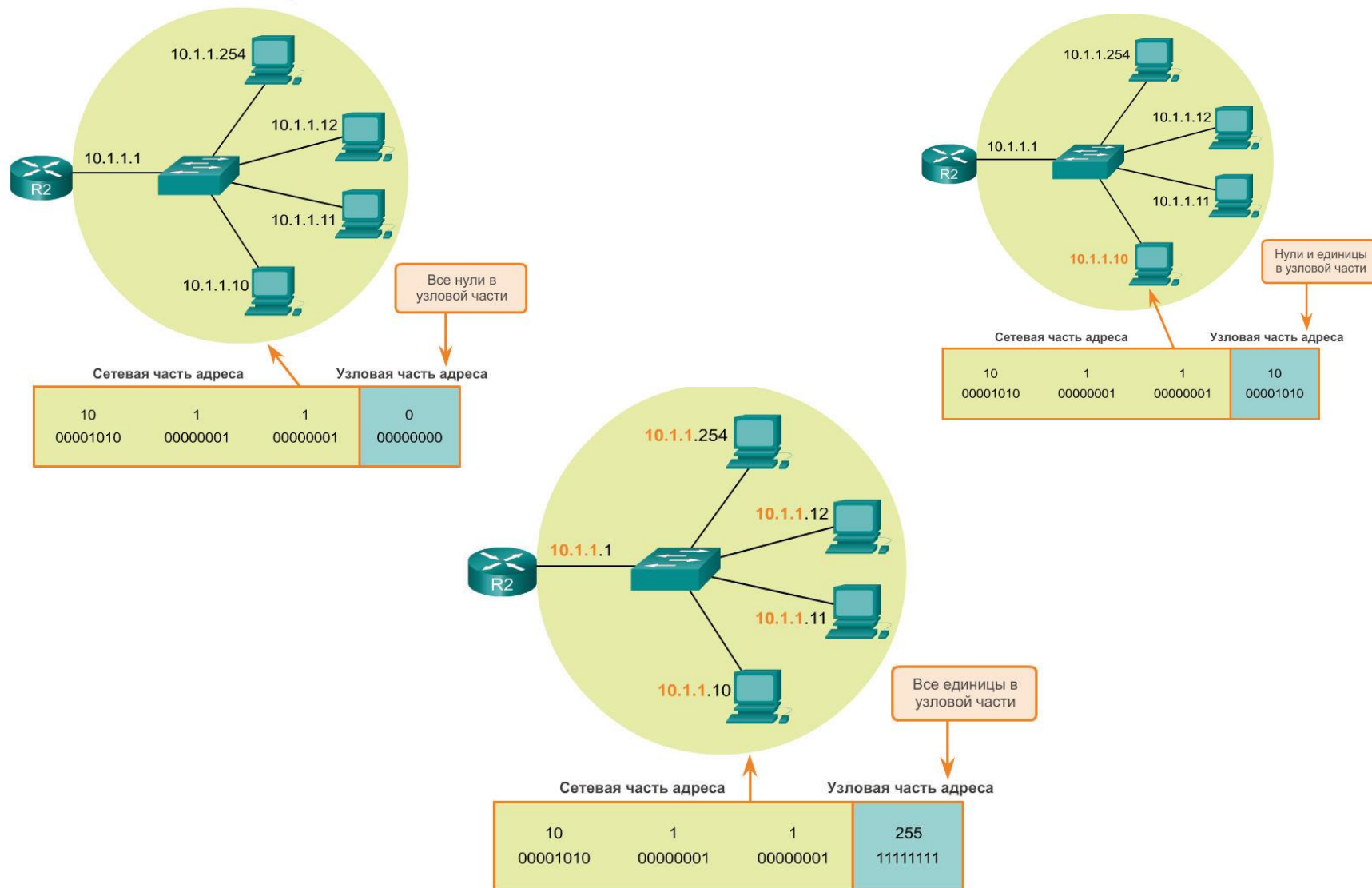
Сетевая и узловая части IPv4-адреса



- Для определения частей сети и узла в адресе устройства используют отдельный 32-битный шаблон — маску подсети.
- Маска подсети не содержит сетевой и хостовой части конкретного IPv4-адреса, но показывает, как эти части выделить для данного IPv4-адреса.

Маска подсети IPv4

Сетевой адрес, адрес узла и адрес широковещательной рассылки IPv4

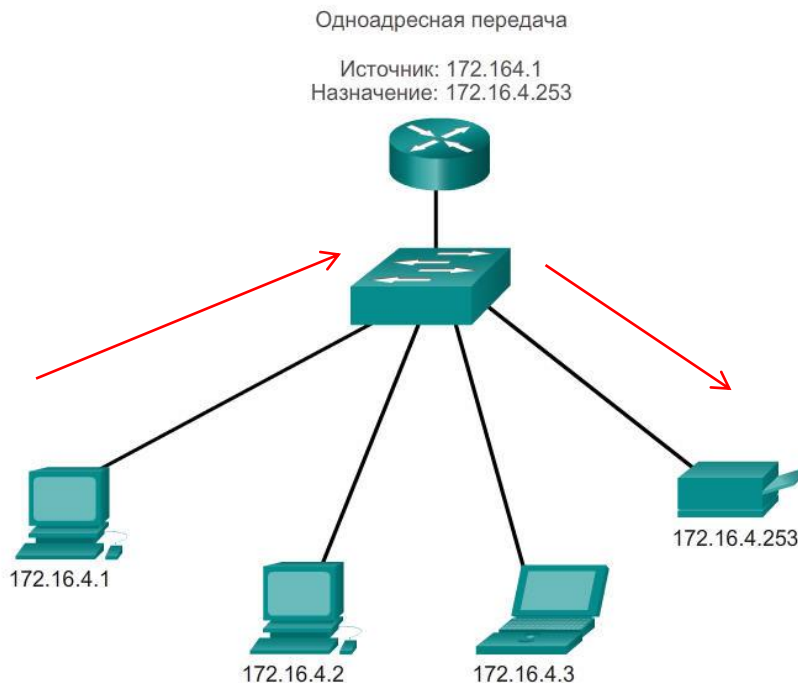


Одноадресная передача, широковещательная и многоадресная рассылка IPv4

Одноадресная передача

В IPv4-сети узлы могут обмениваться данными одним из следующих трёх способов.

- 1. Одноадресная передача** — процедура отправки пакета с одного узла на отдельный узел.



Одноадресная передача, широковещательная и многоадресная рассылка IPv4

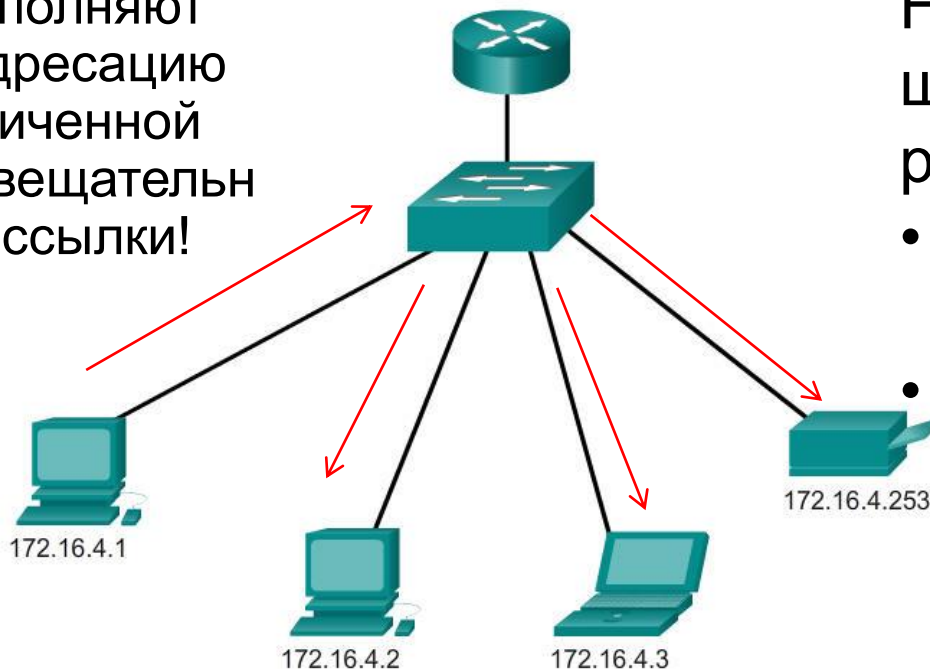
Широковещательная передача

2. Широковещательная передача — процедура отправки пакета с одного узла на все узлы сети

Ограниченная широковещательная рассылка

Источник: 172.164.1
Назначение: 255.255.255.255

Маршрутизаторы не выполняют переадресацию ограниченной широковещательной рассылки!



Направленная широковещательная рассылка

- Назначение 172.16.4.255
- Узлы в сети 172.16.4.0/24

Многоадресная передача

- **Многоадресная передача** — процедура отправки пакета с одного узла на группу выбранных узлов (могут находиться в различных сетях)
- Снижает поток трафика
- Зарезервировано для адресации групп многоадресной передачи, диапазон 224.0.0.0 – 239.255.255.255.
- Локальный адрес канала: диапазон 224.0.0.0—224.0.0.255 (например, данные маршрутизации, которыми обмениваются протоколы маршрутизации)
- Адреса глобальной области: диапазон 224.0.1.0—238.255.255.255 (например, адрес 224.0.1.1 зарезервирован для протокола сетевого времени)

Публичные и частные IPv4-адреса

Блоки частных адресов

- Узлы, которым не требуется доступ к сети Интернет, могут использовать частные адреса
- 10.0.0.0–10.255.255.255 (10.0.0.0/8)
- 172.16.0.0–172.31.255.255 (172.16.0.0/12)
- 192.168.0.0–192.168.255.255 (192.168.0.0/16)

Адреса в общем пространстве адресов

- Не маршрутизируются глобально
- Предназначены только для использования в сетях поставщиков услуг
- Блок адресов: 100.64.0.0/10

Специальное использование IPv4-адресов

- **Сетевые адреса и адреса широковещательной рассылки:** в пределах каждой сети узлам не назначаются первый и последний адреса
- **Интерфейс «обратной петли»:** 127.0.0.1 представляет собой специальный адрес, используемый узлами для направления трафика на эти узлы (адреса в диапазоне 127.0.0.0 – 127.255.255.255 зарезервированы)
- **Локальный адрес канала:** адреса в диапазоне 169.254.0.0–169.254.255.255 (169.254.0.0/16) можно автоматически назначать локальному узлу
- **Адреса TEST-NET:** в диапазоне 192.0.2.0—192.0.2.255 (192.0.2.0/24) отложены для образовательных и обучающих целей и используются в документации и примерах сетей
- **Экспериментальные адреса:** в диапазоне 240.0.0.0—255.255.255.254 зарезервированы

Представление IPv6-адреса

- Имеют длину 128 битов и записываются как строка шестнадцатеричных значений
- В рамках протокола IPv6 4 бита представляют одно шестнадцатеричное число, 32 шестнадцатеричных значения составляют адрес IPv6

2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200

FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF

- Для обозначения сегмента из 16 битов или четырёх шестнадцатеричных чисел используется хекстет.
- Может записываться символами в нижнем или верхнем регистре

Правило 1. Пропуск начальных нулей

- Первое правило, которое позволяет уменьшить объём обозначений в IPv6-адресах — это возможность пропуска всех начальных нулей во всех 16-битных разделах хекстета.
- 01AB можно представить как 1AB
- 09F0 можно представить как 9F0
- 0A00 можно представить как A00

Предпочтительно	2001:0DB8:0000:1111:0000:0000:0000:0200
Без ведущих нулей	2001: DB8: 0:1111: 0: 0: 0: 200

Правило 2. Исключение всех нулевых сегментов

- Двойное двоеточие (::) может заменять все единичные, непрерывные строки из одного или нескольких 16-битных сегментов (хекстетов), которые состоят только из нулей
- Двойное двоеточие (::) можно использовать в одном адресе только один раз; в противном случае адрес будет неоднозначным
- Это называется *сжатым форматом*
- Неверный адрес: 2001:0DB8::ABCD::1234

Правило 2. Исключение всех нулевых сегментов

■ Примеры

№1

Предпочтительно	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Без ведущих нулей	2001: DB8: 0: 0:ABCD: 0: 0: 100
Сжатый	2001:DB8::ABCD:0:0:100
или	
Сжатый	2001:DB8:0:0:ABCD::100

Может использоваться только символ ::

№2

Предпочтительно	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Без ведущих нулей	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Сжатый	FE80::123:4567:89AB:CDEF

Типы IPv6-адресов

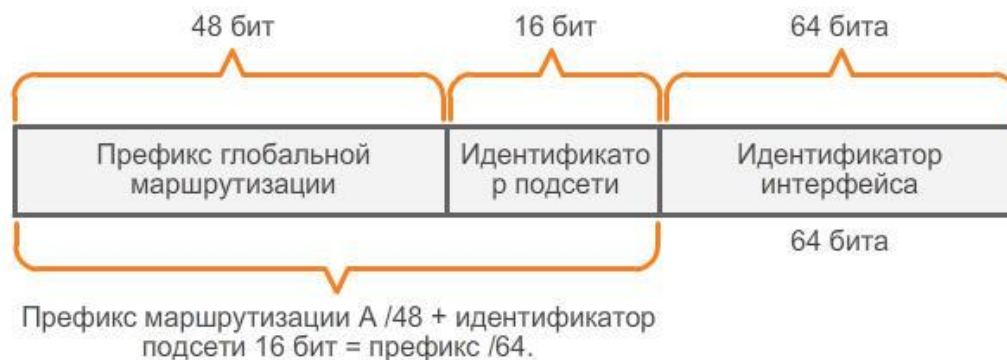
Длина IPv6-префикса

- IPv6 не использует для маски подсети десятичное представление с разделительными точками
- Длина префикса обозначает сетевую часть IPv6-адреса, используя следующий формат:
 - IPv6-адрес/длина префикса
 - Длина префикса может указываться в диапазоне от 0 до 128
 - Стандартная длина префикса — /64



Структура глобального IPv6-адреса одноадресной передачи

- Глобальный индивидуальный адрес состоит из трёх частей.



- **Глобальный префикс маршрутизации:** префикс или сетевая часть адреса, назначенного поставщиком (например интернет-провайдером) клиенту или сайту. Региональные интернет-регистраторы назначают клиентам глобальный префикс маршрутизации /48
- 2001:0DB8:ACAD::/48 имеет префикс, означающий, что первые 48 бит (2001:0DB8:ACAD) представляют собой префикс или сетевую часть

Типы IPv6-адресов

Типы IPv6-адресов

Существует три типа IPv6-адресов:

- **одноадресной передачи;**
- **многоадресной рассылки;**
- **адрес любого хоста из группы.**

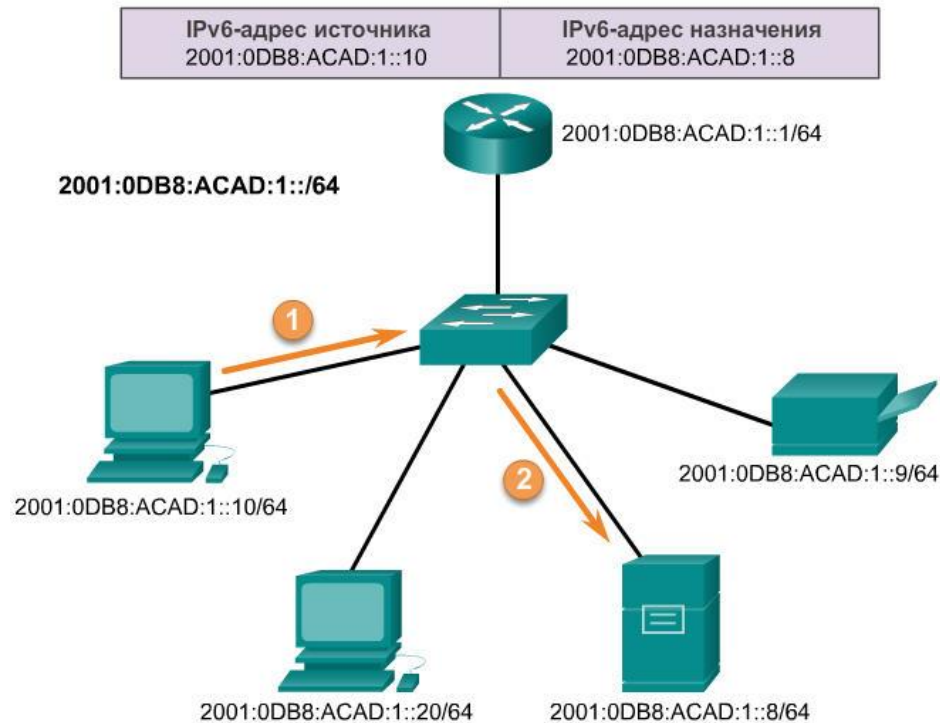
Примечание. Протокол IPv6 не содержит адресов широковещательной рассылки.

Типы IPv6-адресов

Индивидуальные IPv6-адреса

■ Одноадресная передача

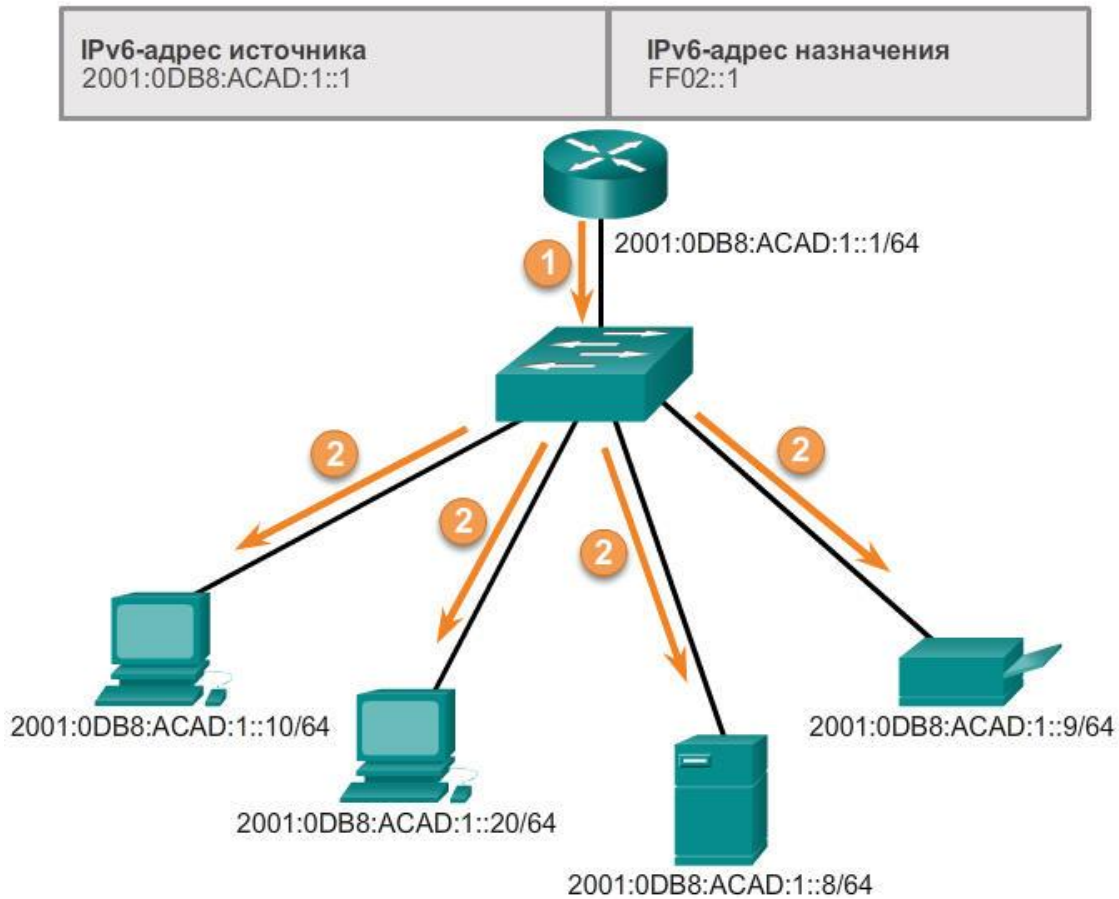
- Служит уникальным идентификатором интерфейса устройства, которое использует протокол IPv6.
- Пакет, отправленный на индивидуальный адрес, будет получен интерфейсом, которому назначен этот адрес.



Типы IPv6-адресов

Назначаемые IPv6-адреса многоадресной рассылки

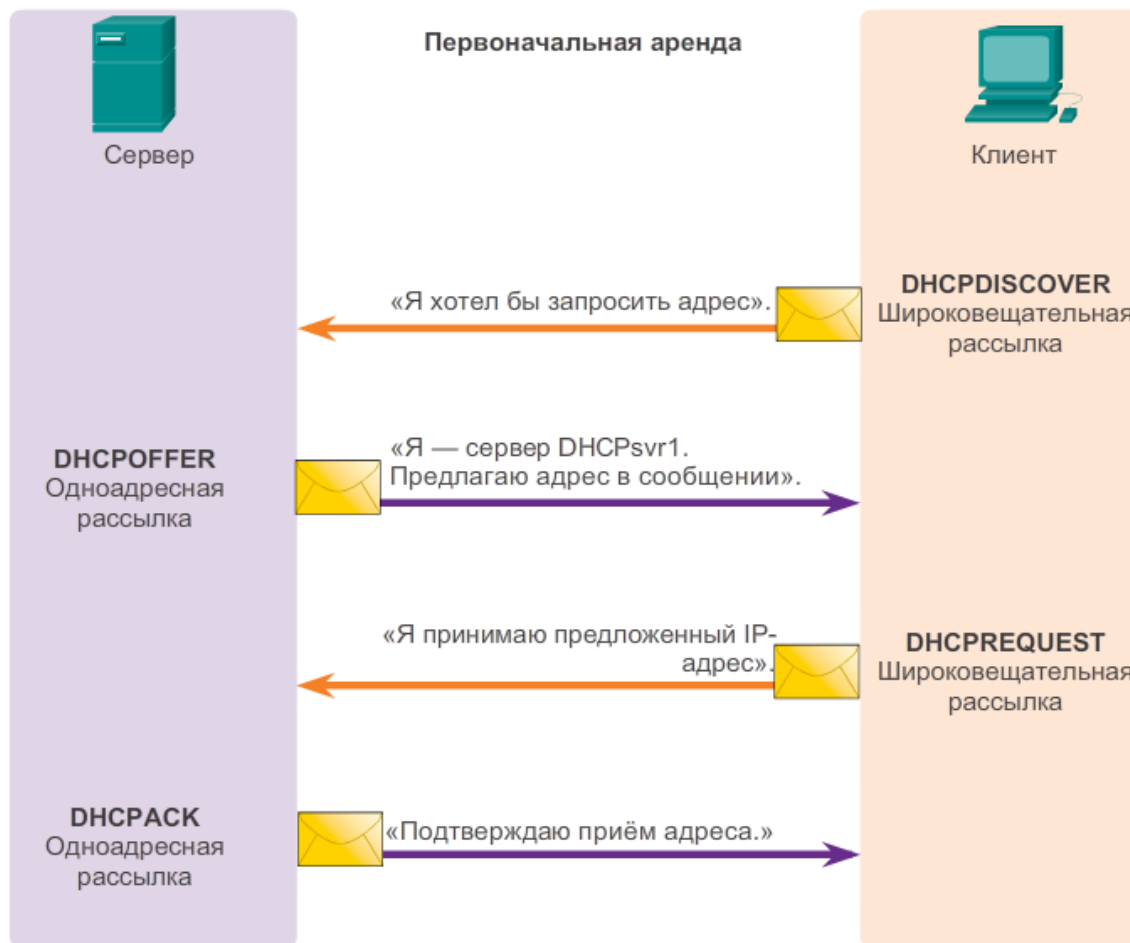
Многоадресная передача IPv6 для всех узлов



Принцип работы протокола DHCPv4

Общие сведения о протоколе DHCPv4

Операция DHCPv4



Принцип работы протокола DHCPv4

Формат сообщений DHCPv4

Формат сообщений DHCPv4

8	16	24	32
Код операции (OP) (1)	Тип оборудования (1)	Длина физического адреса (1)	Переходы (1)
Идентификатор транзакции			
Секунды — 2 байта		Флаги — 2 байта	
IP-адрес клиента (CIADDR) — 4 байта			
Ваш IP-адрес (YIADDR) — 4 байта			
IP-адрес сервера (SIADDR) — 4 байта			
IP-адрес шлюза (GIADDR) — 4 байта			
Физический адрес клиента (CHADDR) — 16 байт			
Имя сервера (SNAME) — 64 байта			
Имя файла загрузки — 128 байт			
Параметры DHCP — размер не задан			

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.

Принцип работы протокола DHCPv4

Проверка сервера DHCPv4

```
C:\WINDOWS\system32\cmd.exe

WINS Proxy Enabled .....: No

Ethernet Adapter Local Area Connection

Connection-specific DNS Suffix.: example.com ←
Description .....: SiS 900 PCI Fast Ethernet
Adapter
Physical Address.....: 00-E0-18-5B-DD-35
Dhcp Enabled .....: Yes
Autoconfiguration Enabled.....: Yes
IP Address .....: 192.168.10.10 ←
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1 ←
DHCP Server .....: 192.168.10.1
Lease Obtained.....: Monday, May 27, 2013 1:06:22PM

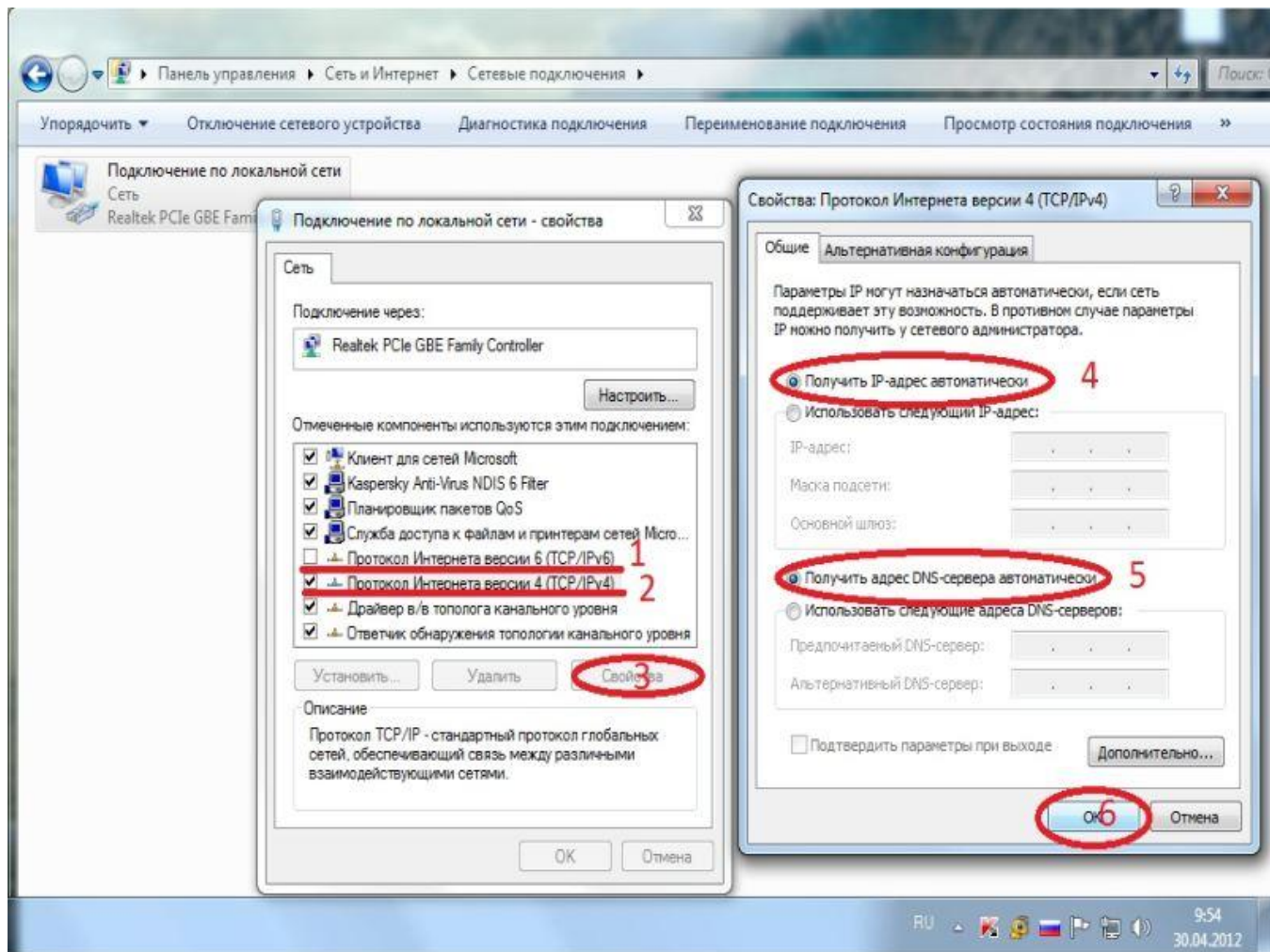
Lease Expires .....: Tuesday, May 28, 2013 1:06:22PM

DNS Servers . . . . .: 192.168.11.5 ←

C:\Documents and settings\SpanPC>
```

Принцип работы протокола DHCPv4

Настройка DHCPv4 в Windows 7



Автоматическая настройка адреса без отслеживания состояния (SLAAC)

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

Автоматическая настройка ICMPv6-адреса без отслеживания состояния



Всем маршрутизаторам, на адрес IPv6 многоадресной рассылки

Запрос маршрутизатора (сообщение RS)
«Мне нужно объявление маршрутизатора (сообщение RA) от маршрутизатора».

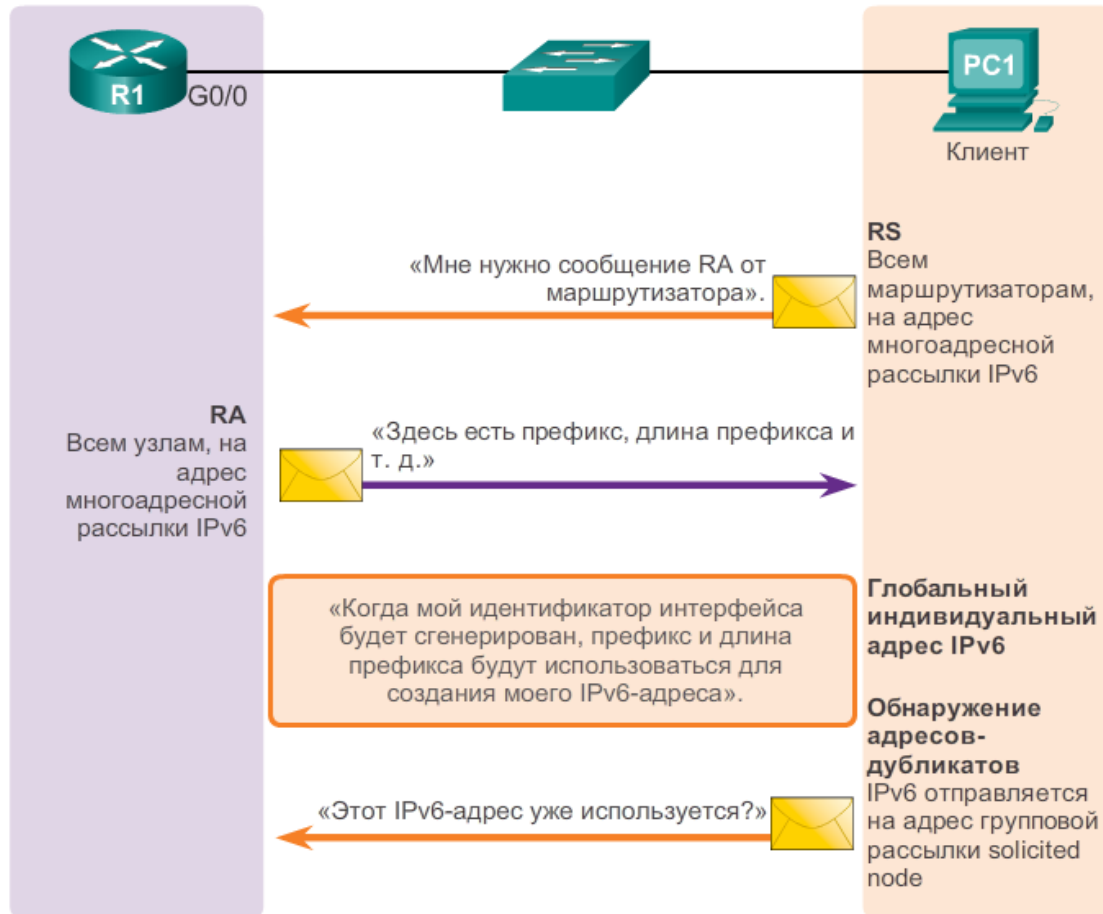
Объявление маршрутизатора (сообщение RA)
«Здесь указаны ваш префикс, длина префикса и другая информация».

Всем узлам, на адрес IPv6 многоадресной рассылки

SLAAC и DHCPv6

Принцип работы SLAAC

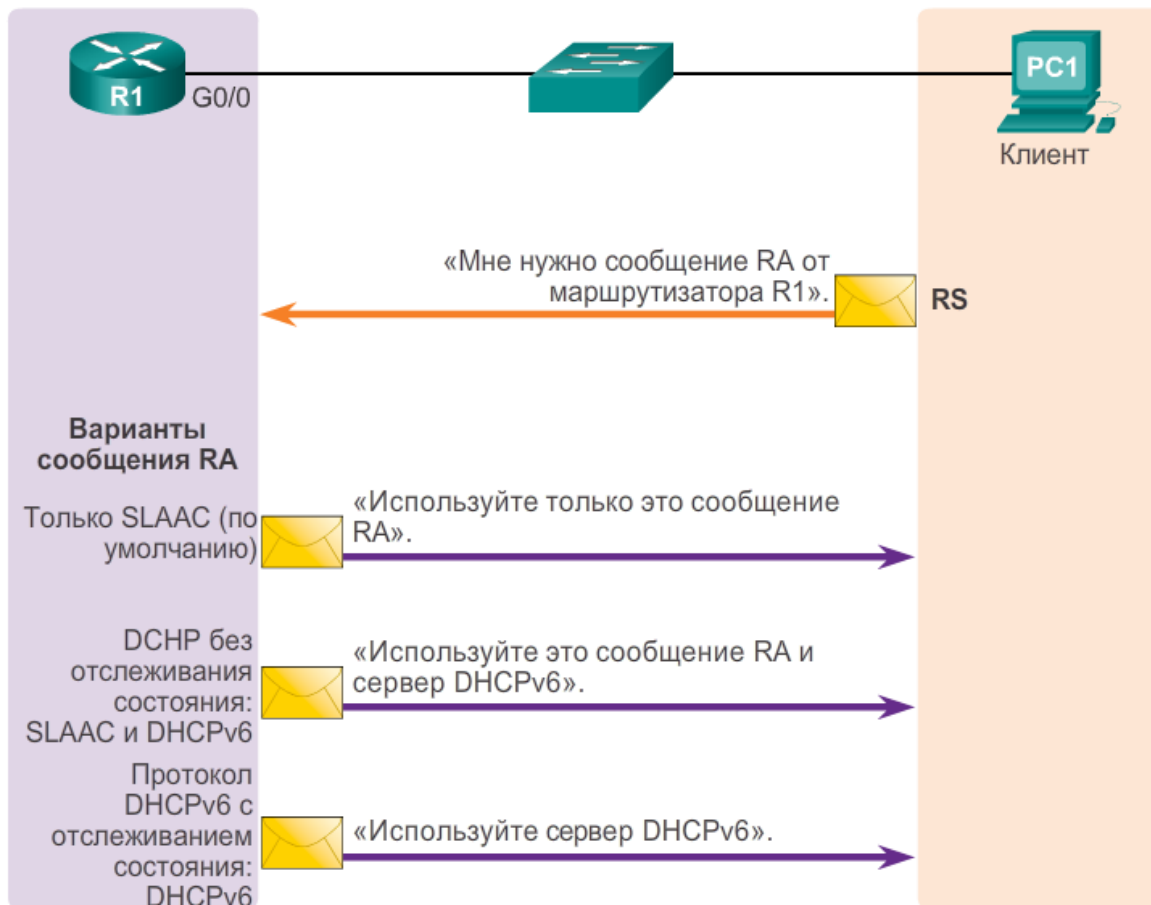
Клиент выполняет обнаружение адресов-дубликатов



SLAAC и DHCPv6

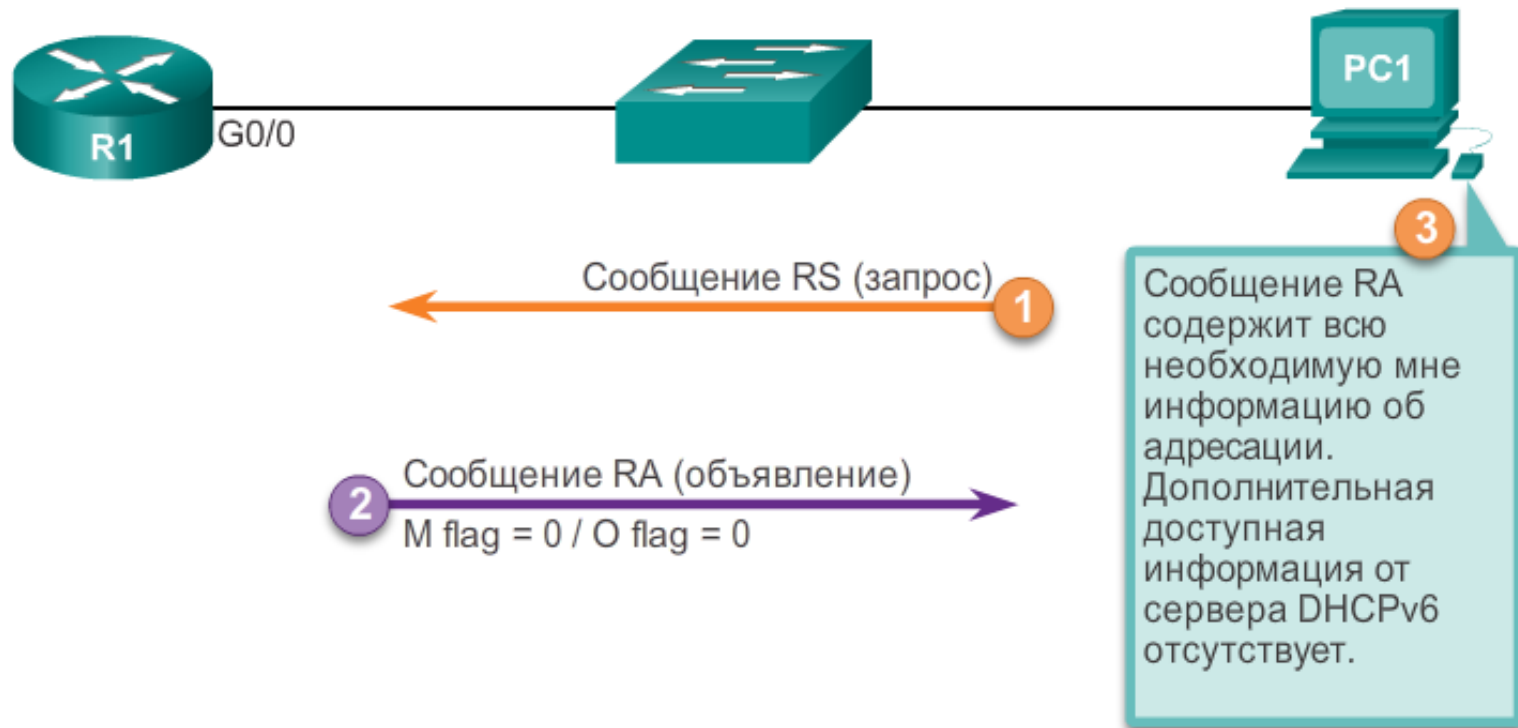
SLAAC и DHCPv6

SLAAC и DHCPv6



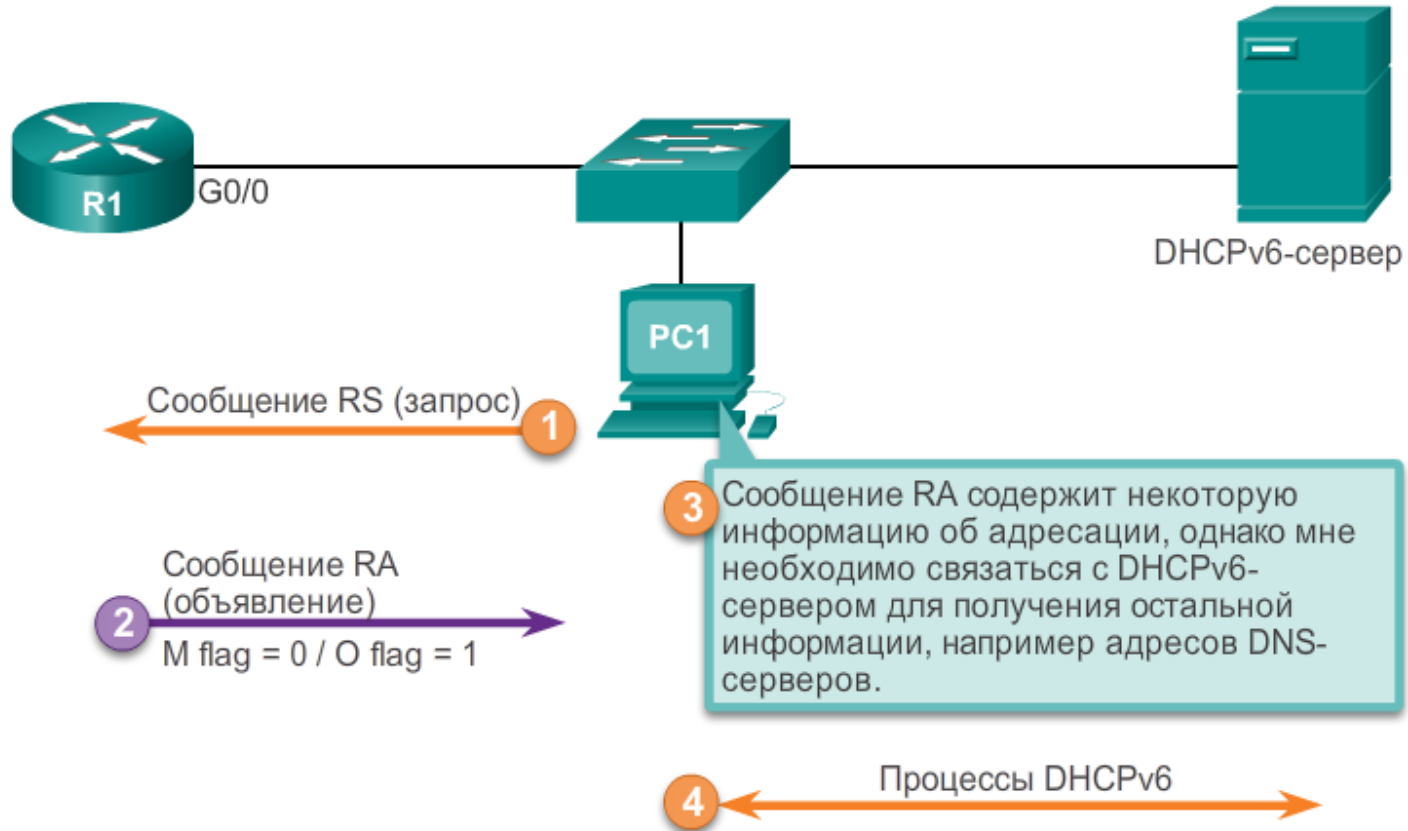
SLAAC и DHCPv6

Опция SLAAC



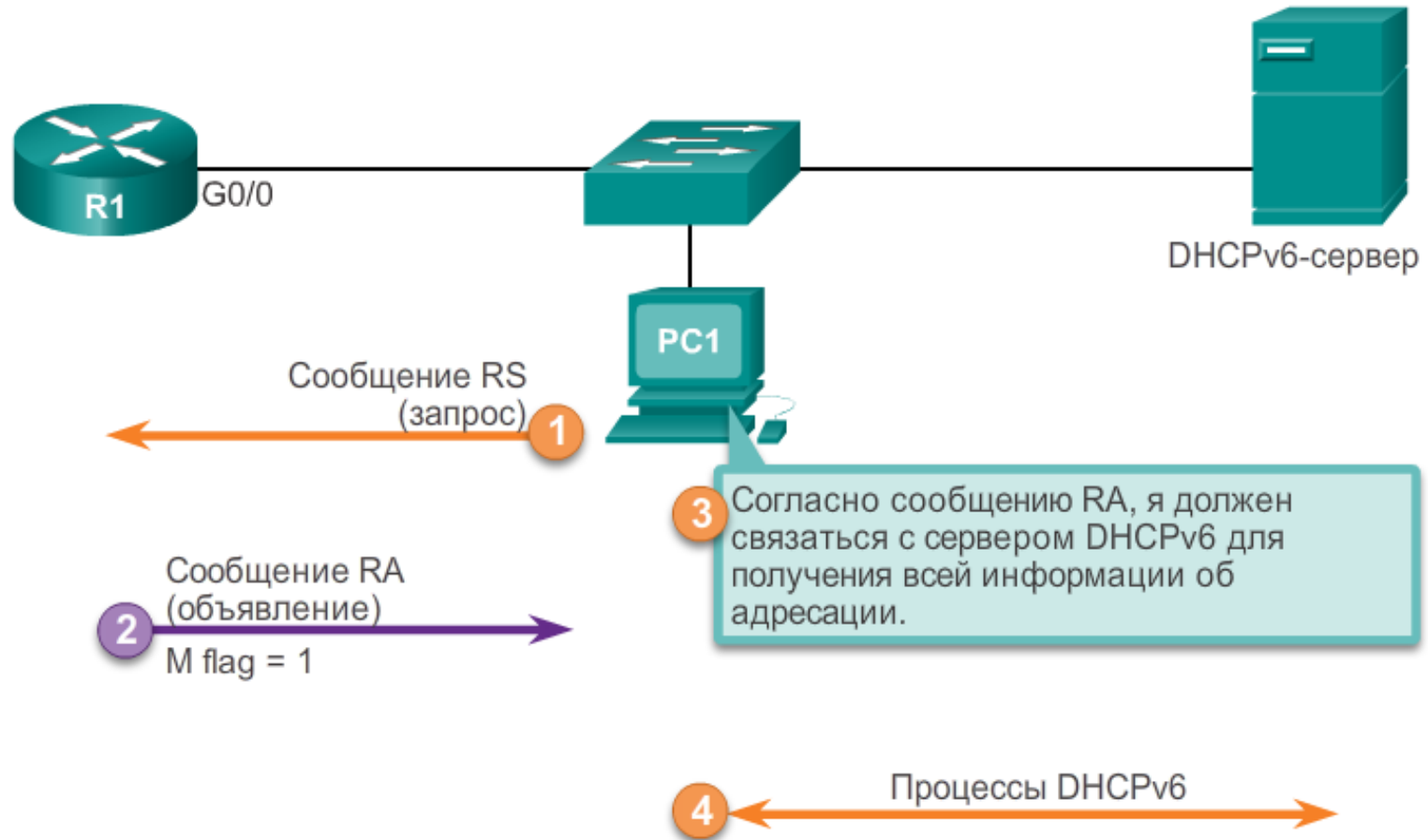
SLAAC и DHCPv6

Опция DHCP без отслеживания состояния



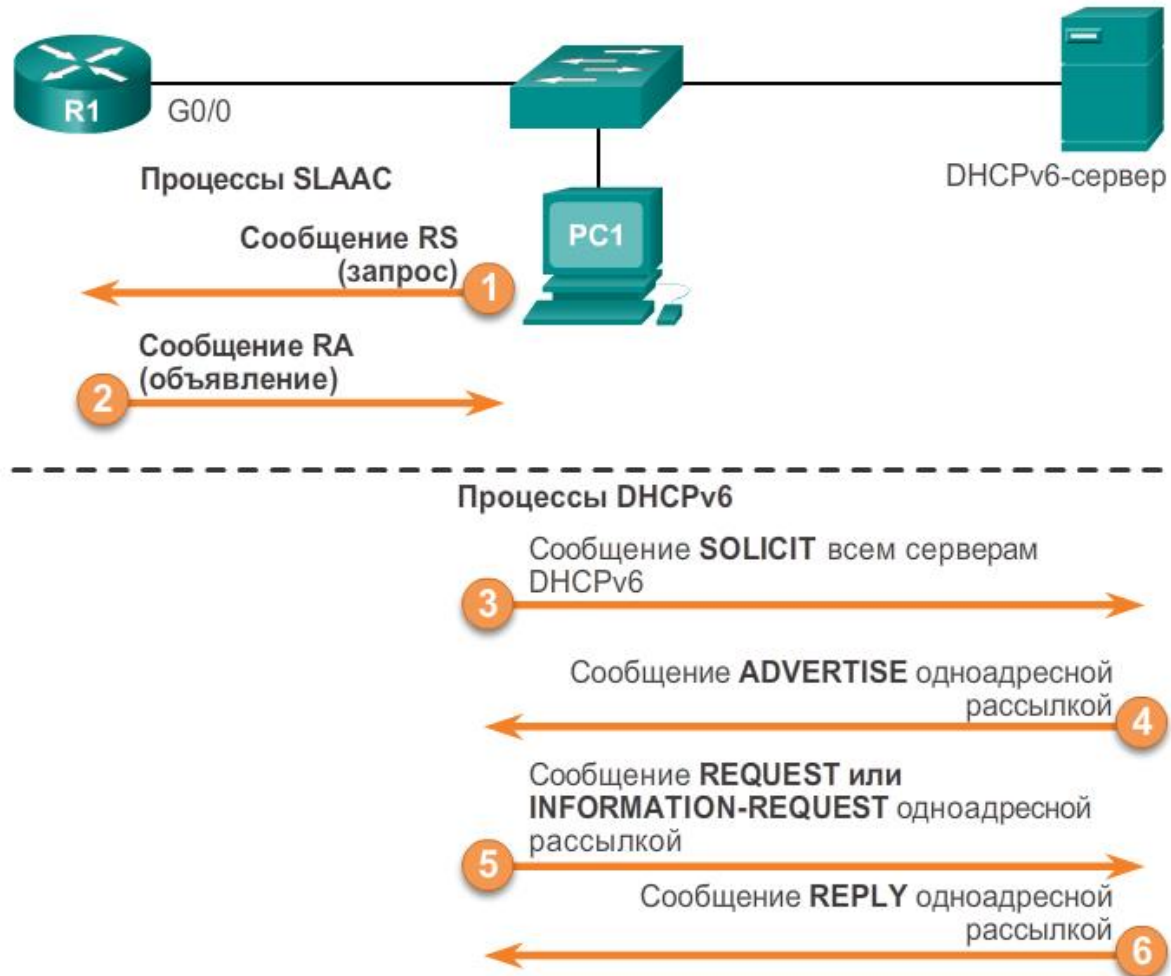
SLAAC и DHCPv6

Функция DHCP с сохранением состояния



SLAAC и DHCPv6

Операции протокола DHCPv6



Индивидуальные IPv6-адреса

Процесс EUI-64 или сгенерированный в произвольном порядке

Процесс EUI-64

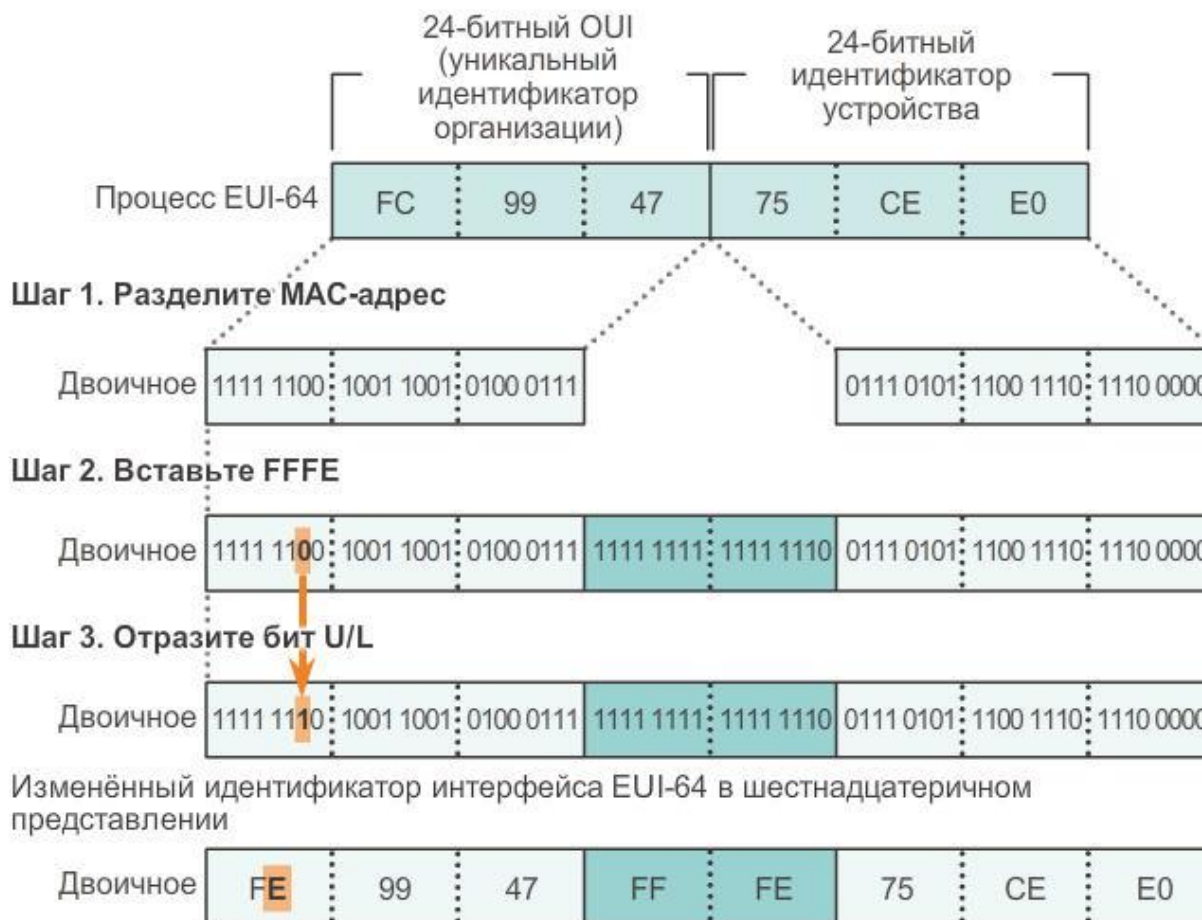
- процесс использует 48-битный MAC-адрес Ethernet и выполняет вставку 16 бит в средней части 46-битного MAC -адреса с целью создания 64-битного идентификатора интерфейса
- преимущество заключается в том, что можно использовать MAC-адрес Ethernet, чтобы определить легко отслеживаемый интерфейс

идентификатор интерфейса EUI-64 представлен двоичным представлением и состоит из трёх частей:

- 24-битный идентификатор производителя оборудования (OUI) на основе MAC-адреса клиента, но при этом седьмой бит (бит «Универсально/локально») отображается в обратном порядке (ноль становится единицей)
- вставленное 16-битное значение FFFE
- 24-битный идентификатор устройства на основе MAC-адреса клиента

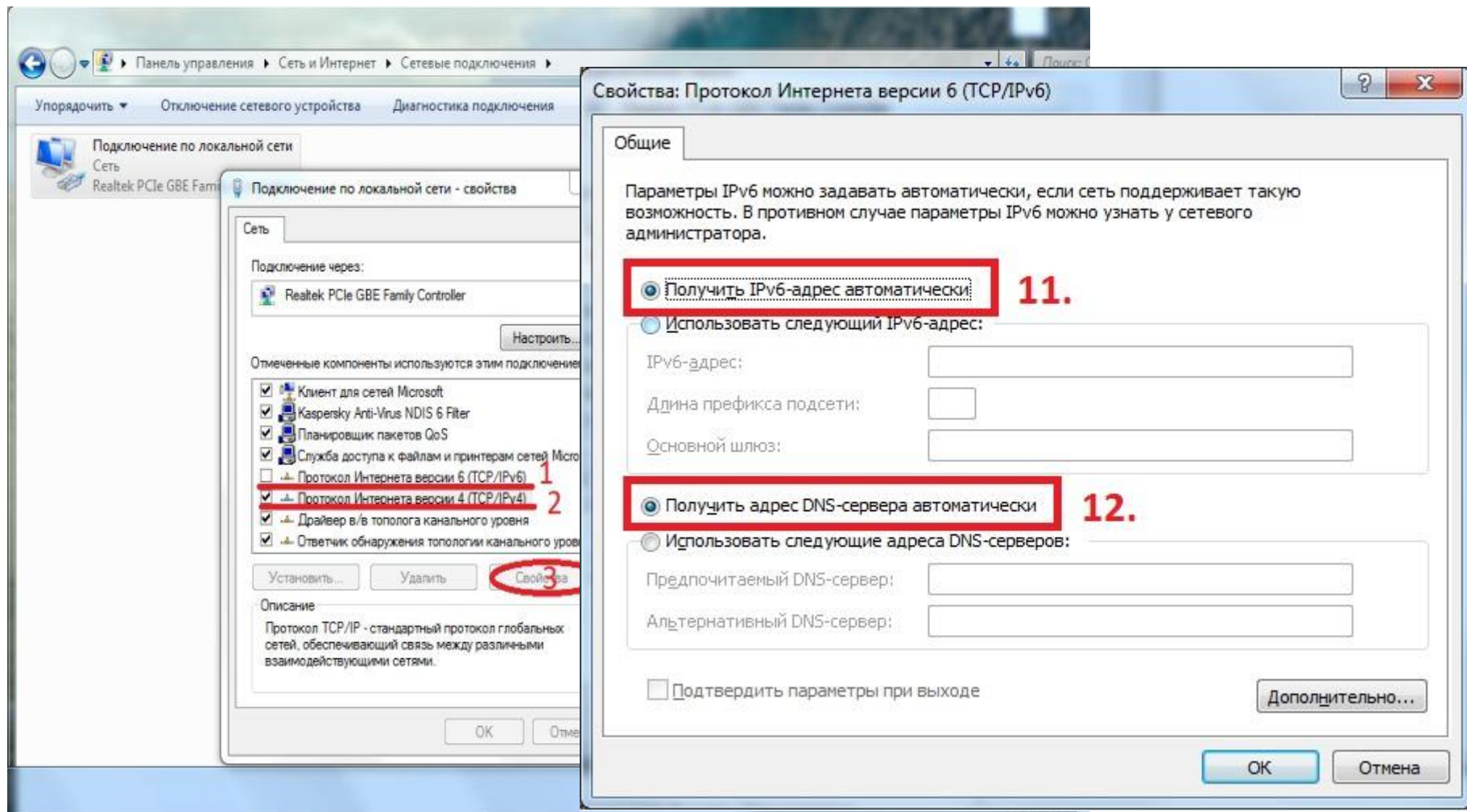
Процесс EUI-64 или сгенерированный в произвольном порядке

Процесс расширенного уникального идентификатора EUI-64 (процесс EUI-64)



Принцип работы протокола DHCPv6

Настройка DHCPv6 в Windows 7



Тестирование и проверка

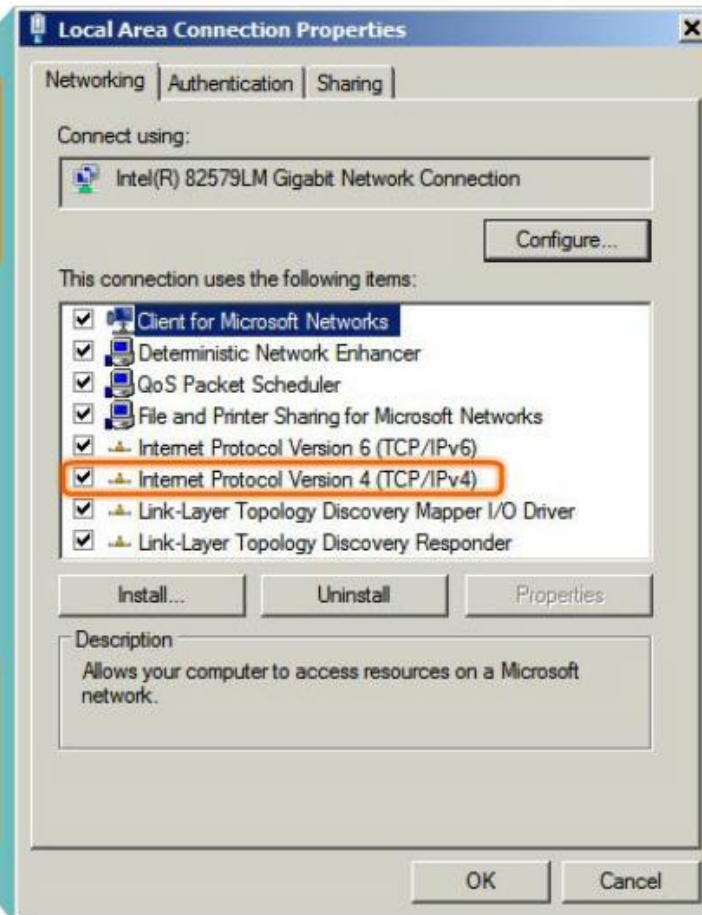
Ping: тестирование локального стека

Проверка локального TCP/IP-стека

Отправление эхо-запроса на локальный узел подтверждает, что протокол TCP/IP установлен и работает на локальном узле.

```
C:\>ping 127.0.0.1
```

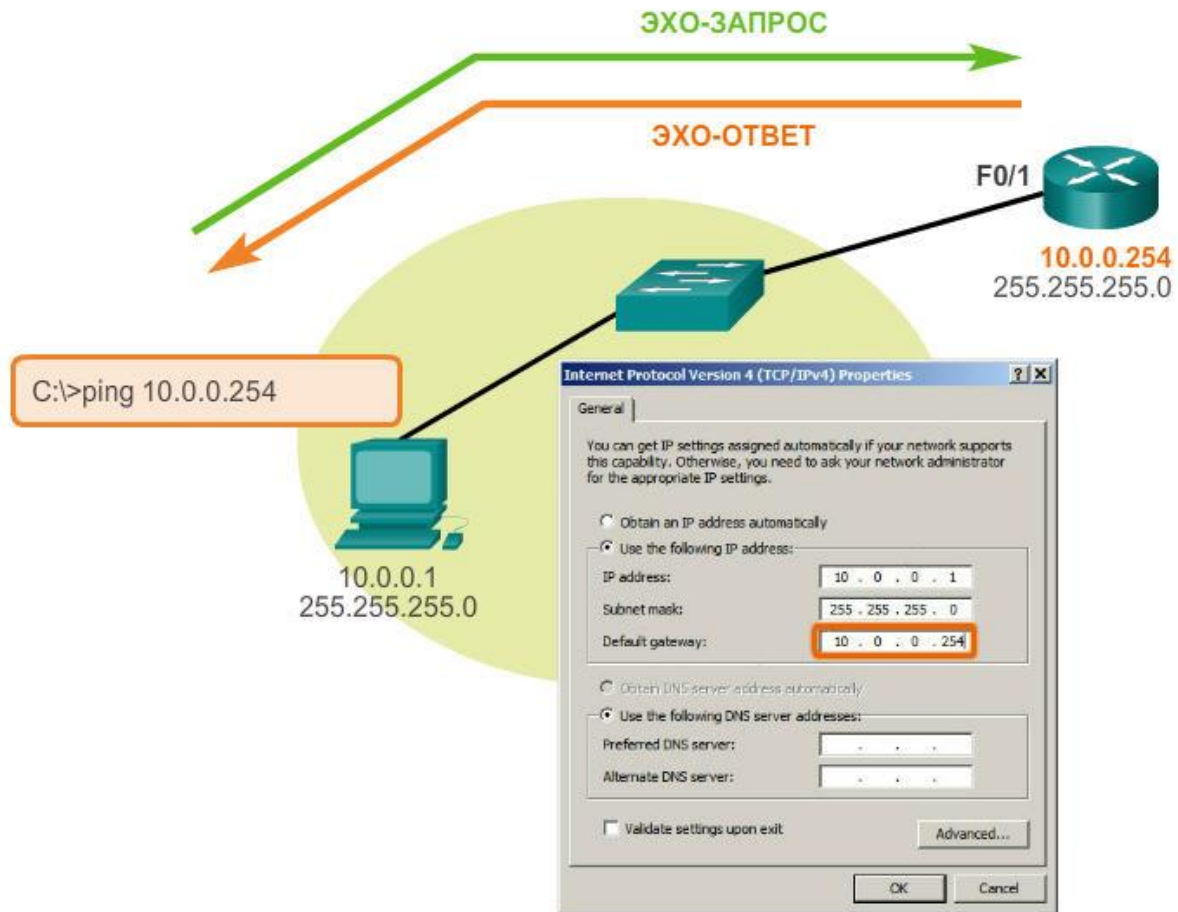
Отправка эхо-запроса по IP-адресу **127.0.0.1** приведёт к тому, что устройство выполнит эхо-тестирование в отношении самого себя.



Тестирование и проверка

Ping: проверка подключения к локальной сети (LAN)

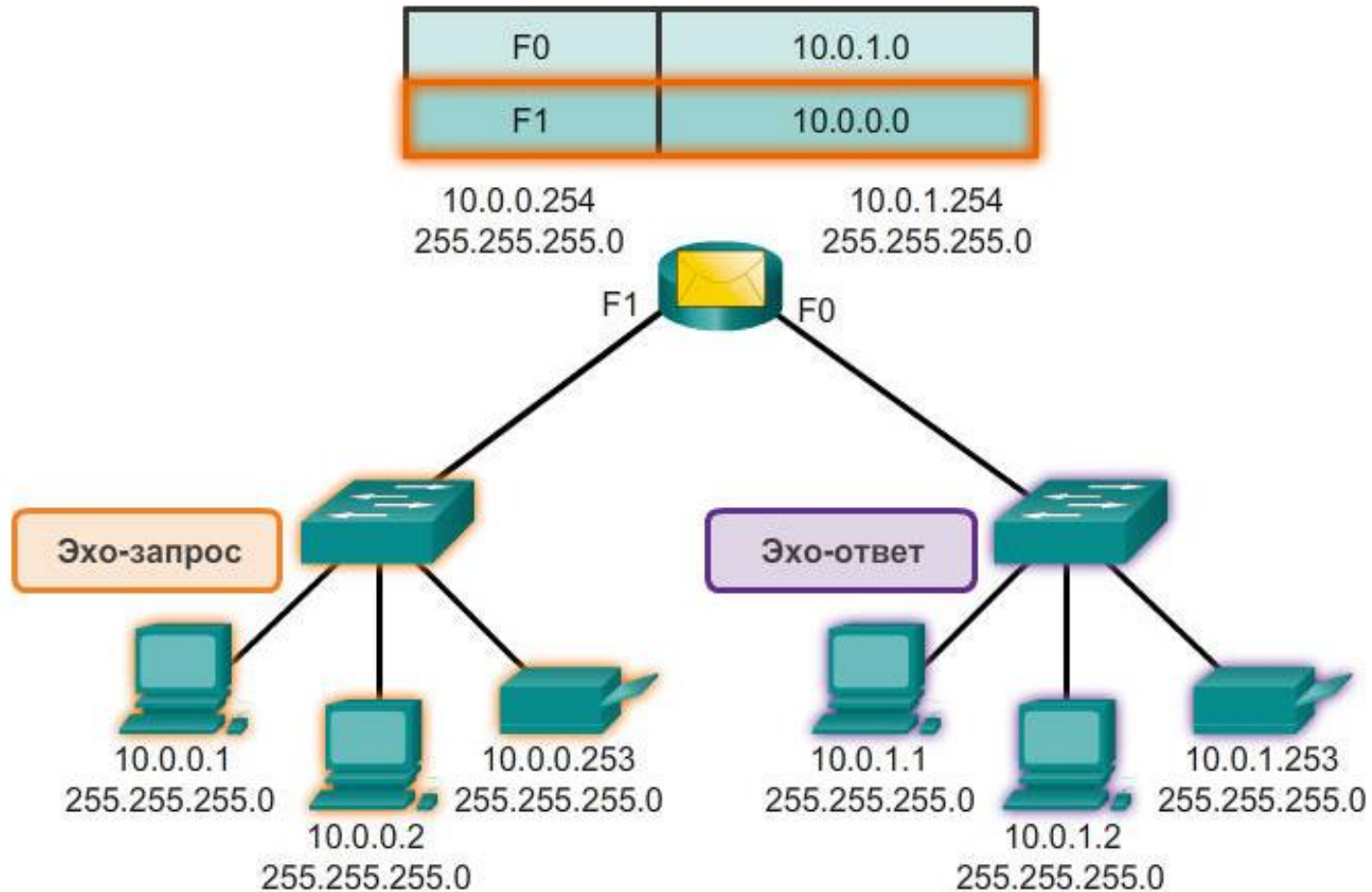
Проверка IPv4-соединения к локальной сети



Тестирование и проверка

Ping: проверка подключения к удалённой сети

Проверка соединения с удалённой локальной сетью
Эхо-запрос на удалённый узел



Traceroute: тестирование пути

Traceroute (tracert)

- Создаёт список переходов, успешно выполненных на пути
- Предоставляет важные сведения о проверке и устранении неполадок
- Если данные достигают места назначения, команда трассировки создаёт список интерфейсов для каждого маршрутизатора на пути между узлами
- Если при передаче данных произошёл сбой на любом из переходов на пути, то адрес последнего маршрутизатора, от которого получен отклик трассировки, может указывать место, где имеется проблема или ограничения, налагаемые системой безопасности
- Предоставляет время прохождения сигнала туда и обратно для каждого перехода на пути и сообщает, когда переход не отправляет отклик

Базовый уровень сети

Выполнение единой проверки

FEB 8, 2013 08:14:43

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:  
  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
  
Ping statistics for 10.66.254.159:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

MAR 17, 2013 14:41:06

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:  
  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
  
Ping statistics for 10.66.254.159:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

Перехват эхо-запроса маршрутизатора: сохранение в текстовый файл



В сеансе работы с терминалом выполните следующие действия:

1. Иницилируйте процесс захвата текста.
2. Выполните команду **ping** <ip address> .
3. Остановите процесс захвата текста.
4. Сохраните текстовый файл.