Информационные сети

Преображенский Юрий Петрович,
начальник службы информатизации и менеджмента качества,
кандидат технических наук, доцент

- I -

Сети в общем

Структурированные кабельные системы

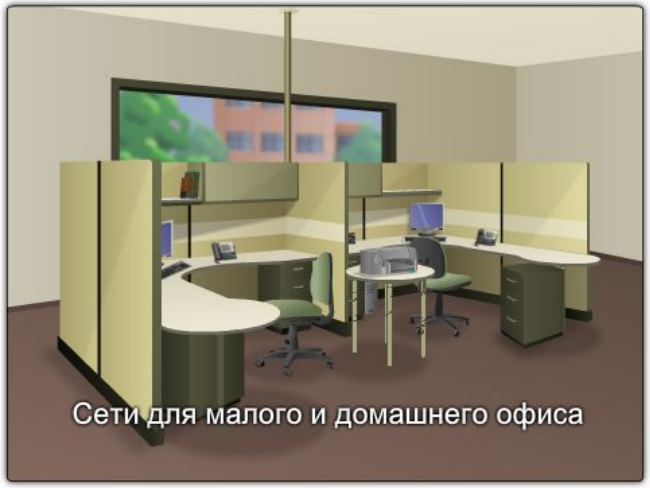
Сеть - совокупность программных, аппаратных и коммуникационных средств, обеспечивающих эффективное распределение вычислительных ресурсов

- локальные сети (LAN, Local Area Network);
- глобальные сети (WAN, Wide Area Network);
- городские сети (MAN, Metropolitan Area Network).
- персональные сети (PAN, Personal Area Network)

Современная сеть предоставляет несколько видов телекоммуникационных услуг

Сети различаются размером и принципами установления связи

PAN
LAN



LAN

MAN

WAN

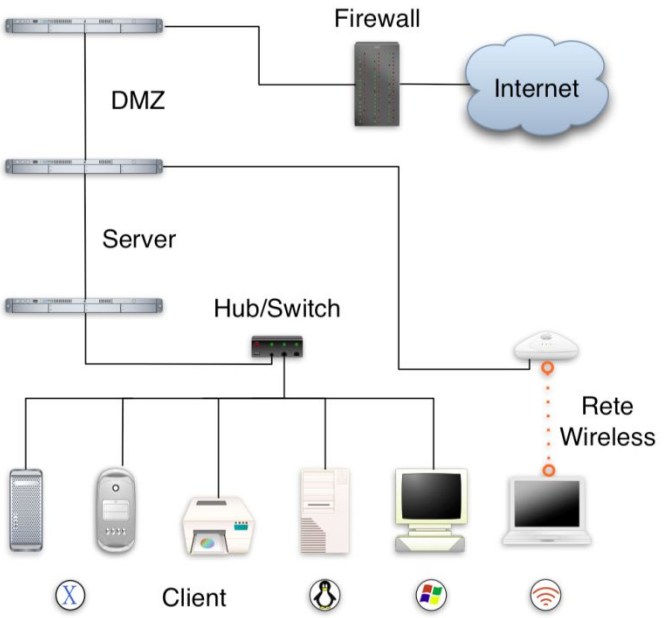
* SOHO-сети = Small or Home Office

WAN

Глобальные сети ориентированы на соединение — до начала передачи данных между абонентами устанавливается соединение (сеанс).

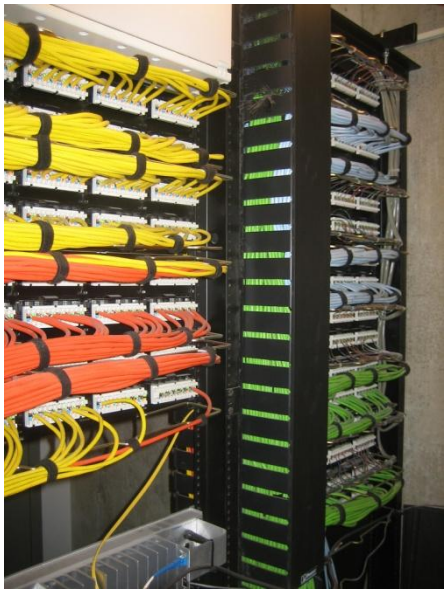
LAN

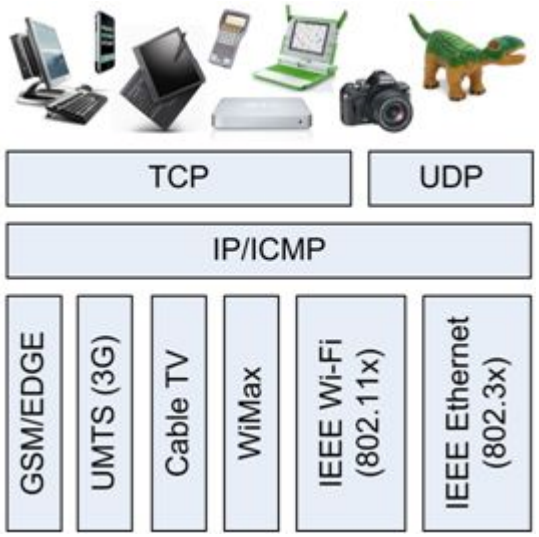
В локальных сетях используются методы, не требующие предварительной установки соединения, — пакет с данными посылается без подтверждения готовности по



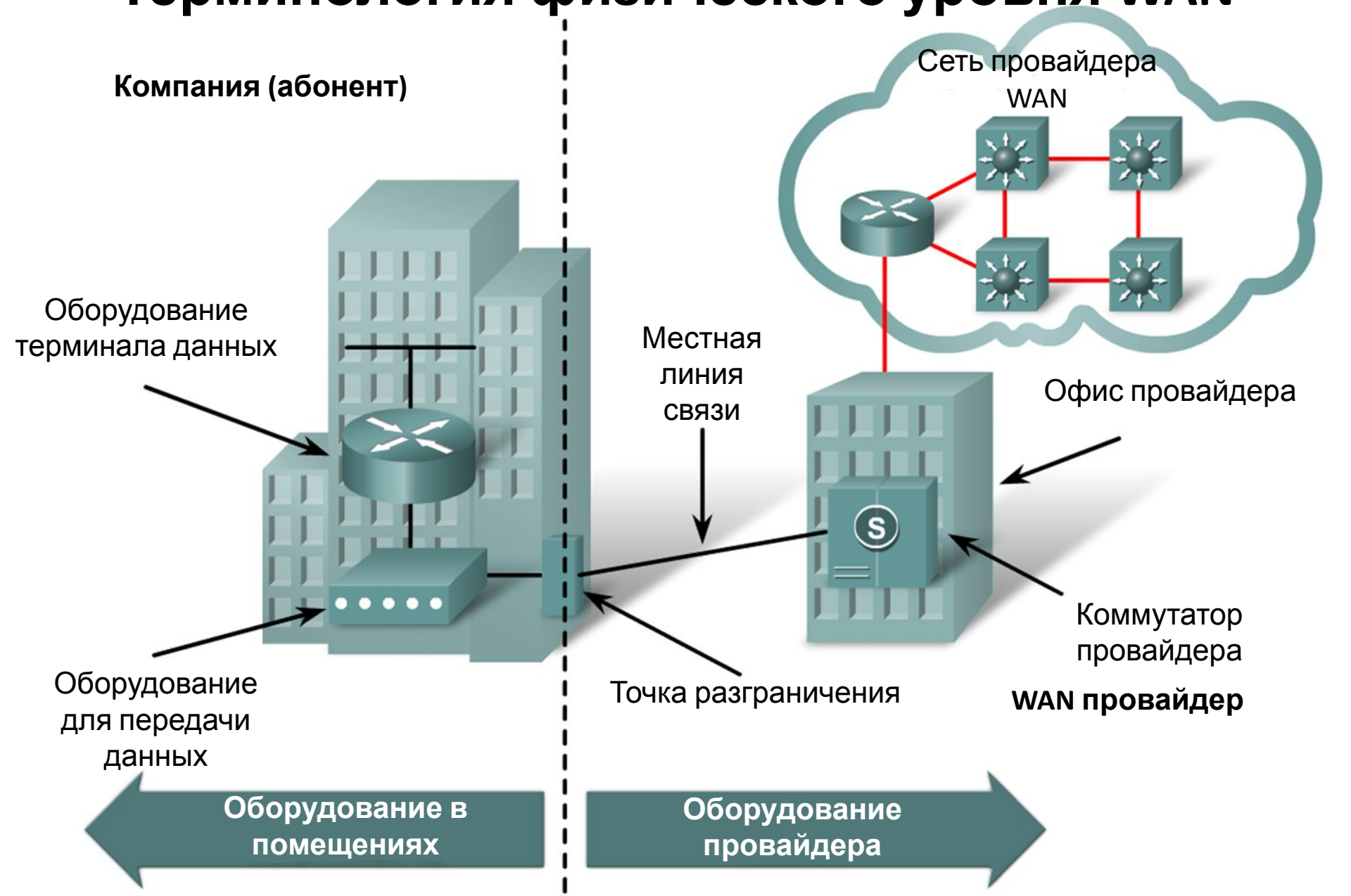
Уровни сетевой инфраструктуры

- кабельная система и средства коммуникаций
- активное сетевое оборудование
- сетевые протоколы
- сетевые службы
- сетевые приложения

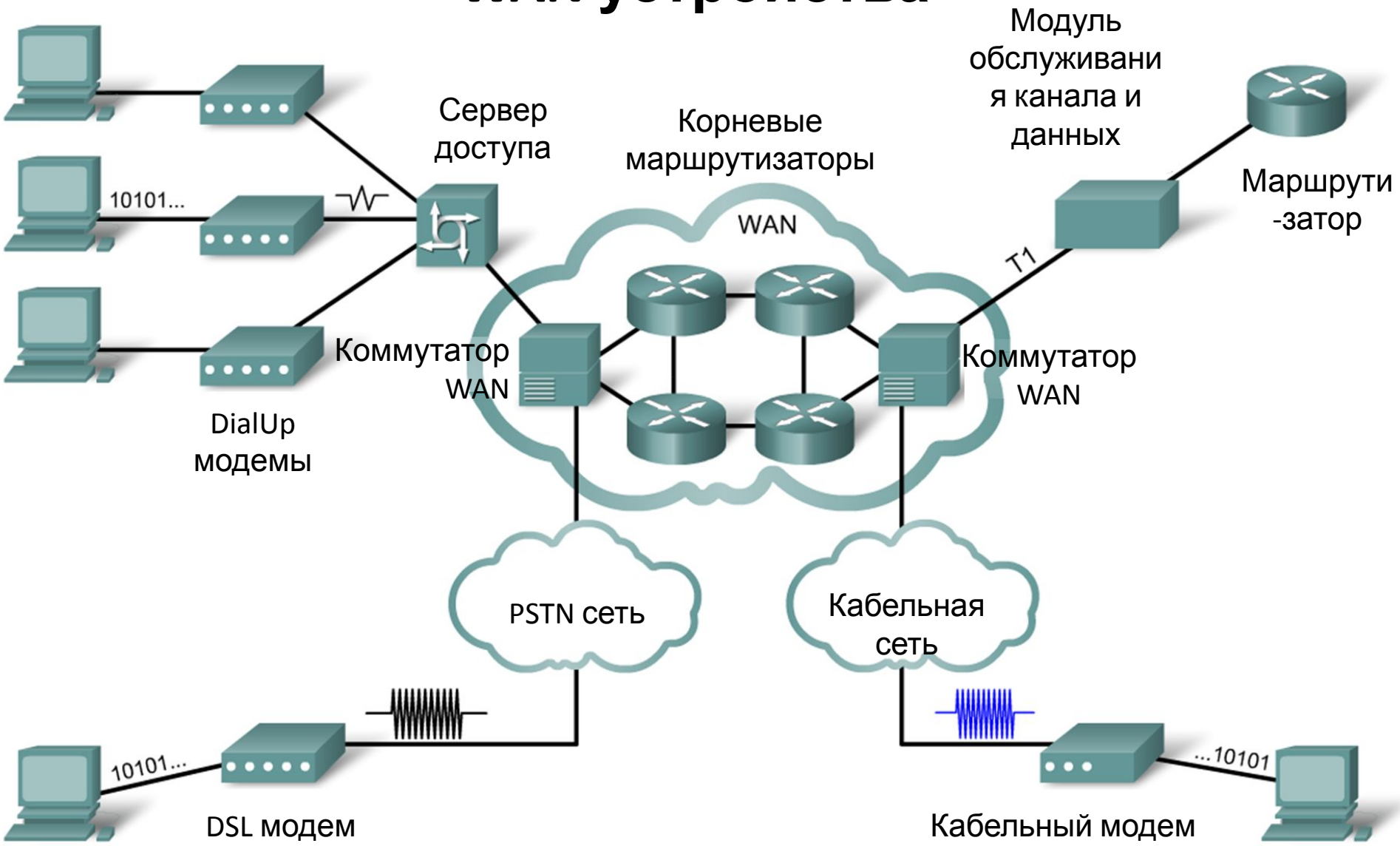




Терминология физического уровня WAN



WAN устройства



Службы базового набора сетевых служб корпоративной сети

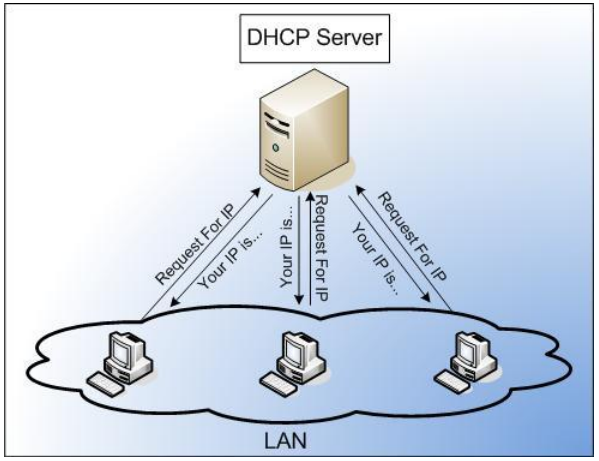
1.службы сетевой инфраструктуры DNS, DHCP, WINS;

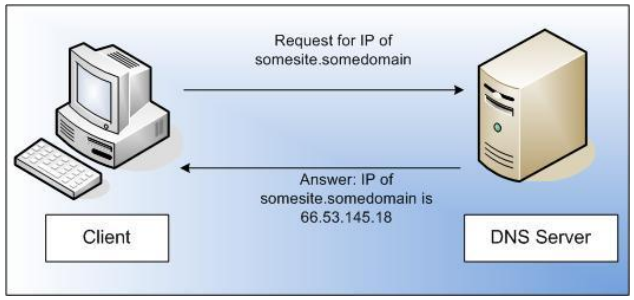
2.службы файлов и печати

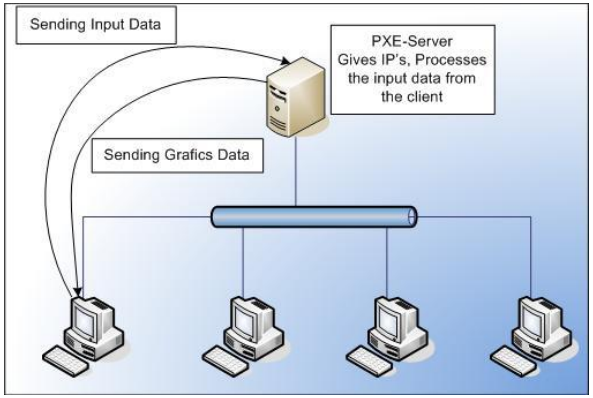
3.службы каталогов (Novell NDS, MS AD)

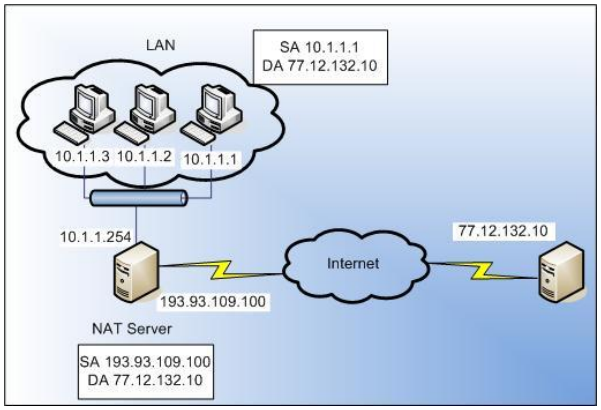
4. службы обмена сообщениями

5. службы доступа к базам данных







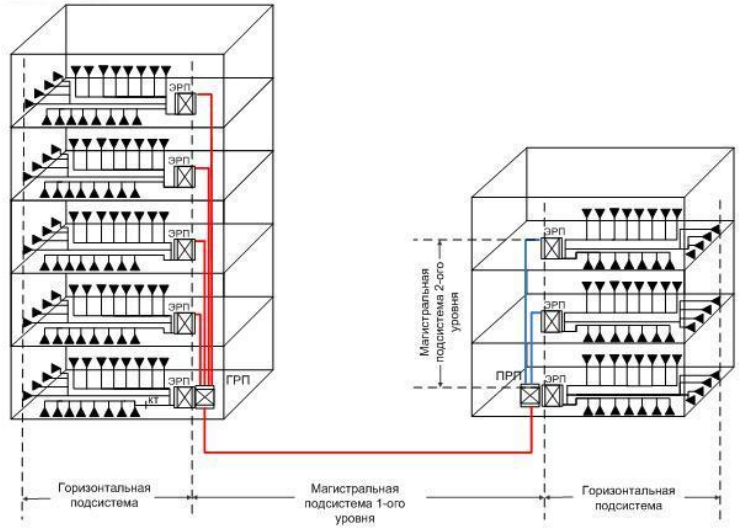


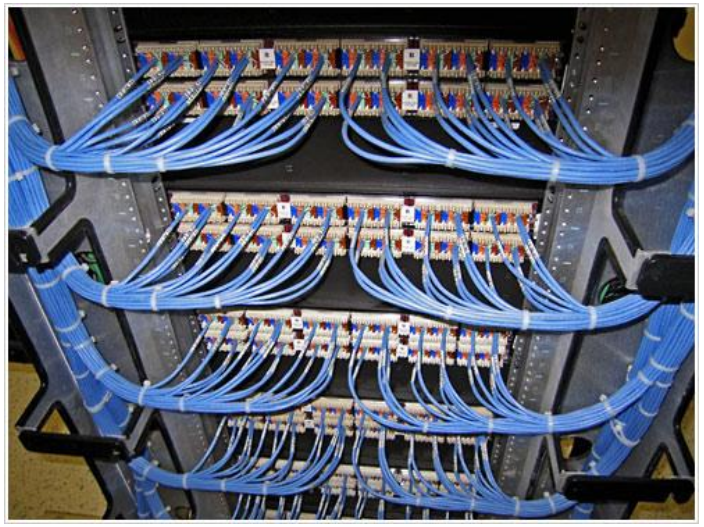
Задачи сетевого администрирования в распределенной корпоративной сети

1. Планирование сети.
2. Установка и настройка сетевых узлов (устройств активного сетевого оборудования, персональных компьютеров, серверов, средств коммуникаций).
3. Установка и настройка сетевых протоколов.
4. Установка и настройка сетевых служб.
   - установка и настройка служб сетевой инфраструктуры (службы DNS, DHCP, WINS, службы маршрутизации, удаленного доступа и виртуальных частных сетей - VPN);
   - установка и настройка служб файлов и печати, которые в настоящее время составляют значительную часть всех сетевых служб;
   - администрирование служб каталогов (Novell NDS, Microsoft Active Directory), составляющих основу корпоративной системы безопасности и управления доступом к сетевым ресурсам;
   - администрирование служб обмена сообщениями (системы электронной почты);
   - администрирование служб доступа к базам данных.
5. Поиск неисправностей.
6. Поиск узких мест сети и повышения эффективности работы сети.
7. Мониторинг сетевых узлов.
8. Мониторинг сетевого трафика.
9. Обеспечение защиты данных.

Структурированной кабельной системой (СКС) называется кабельная система:

- имеющая стандартизованную структуру и топологию,
- использующая стандартизованные элементы (кабели, разъемы, коммутационные устройства и т.п.),
- обеспечивающая стандартизованные параметры (скорость передачи данных, затухание и проч.),
- управляемая (администрируемая) стандартизованным образом.





Преимущества СКС

- универсальность: одна кабельная система обслуживает все необходимые в здании системы: телефонную, ЛВС, пожарную, охранную и др.
- высокую адаптивную способность к изменениям внешних условий («гибкость»), действительно, без изменений в пространстве, без перекладки кабелей СКС легко приспосабливается:
  - к изменениям организационной структуры предприятия (организация новых и ликвидация старых подразделений);
  - к передислокации сотрудников и подразделений;
  - к смене типов оборудования и, следовательно, к смене его поставщиков, а независимость от конкретных поставщиков всегда полезна.
- небольшую численность и моноспециализированность обслуживающего СКС персонала (не нужны отдельные специалисты по проводке для пожарных, охранных, телефонных и других систем - нужен лишь администратор СКС);
- высокую экономичность по критерию "затраты - эффективность". С определенного момента затраты на поддержание ИКС значительно превышают аналогичные для СКС. При реальном сроке окупаемости СКС в 3...5 лет "цена владения" ею оказывается существенно меньшей, чем для ИКС.

Стандарт СКС обеспечивает…

- **пользователей** - независимой от применений универсальной кабельной системой и открытым рынком ее компонент;
- **пользователей** - гибкой кабельной схемой, так что модификации ее легки и экономичны;
- **строителей-профессионалов** - руководством, позволяющим приспособить здание к кабелям еще до того, как станут известны специфические требования;
- **стандартизаторов** в промышленности и применениях - кабельной системой, которая поддерживает выпускаемые изделия и обеспечивает основу для разработки будущих изделий.

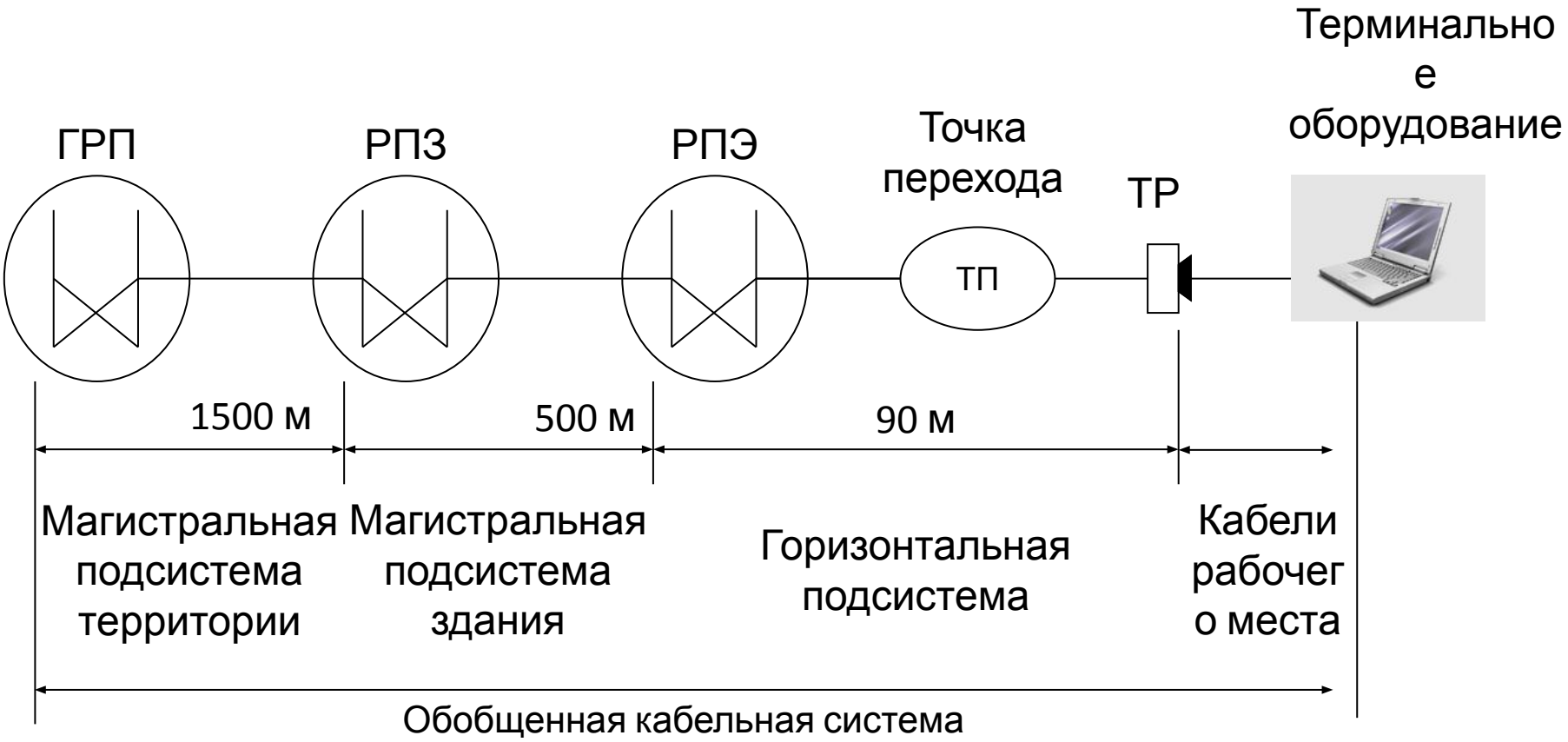
Стандарт оптимален для участков, имеющих географический размах до 3000 м, офисную площадь - до 1 000 000 кв.м и "население" - от 50 до 50 000 чел.

Функциональные элементы обобщенной кабельной системы

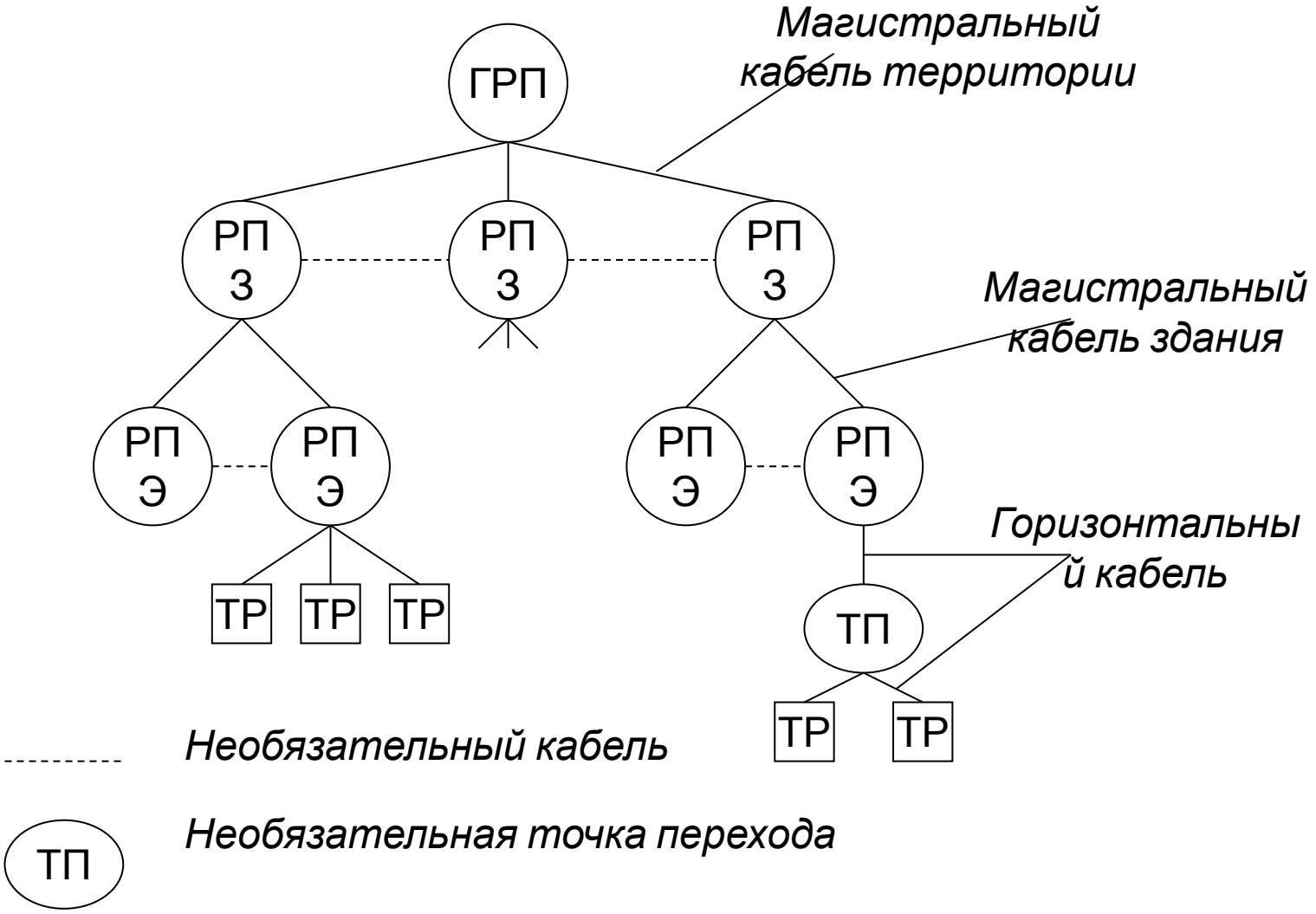
- Главный Распределительный Пункт (ГРП)
- Магистральный кабель территории
- Распределительный Пункт Здания (РПЗ)
- Магистральный кабель здания
- Распределительный Пункт Этажа (РПЭ)
- Горизонтальный кабель
- Точка перехода (ТП)
- Телекоммуникационный Разъем (ТР)

Обобщенная кабельная подсистема состоит из трех кабельных подсистем:

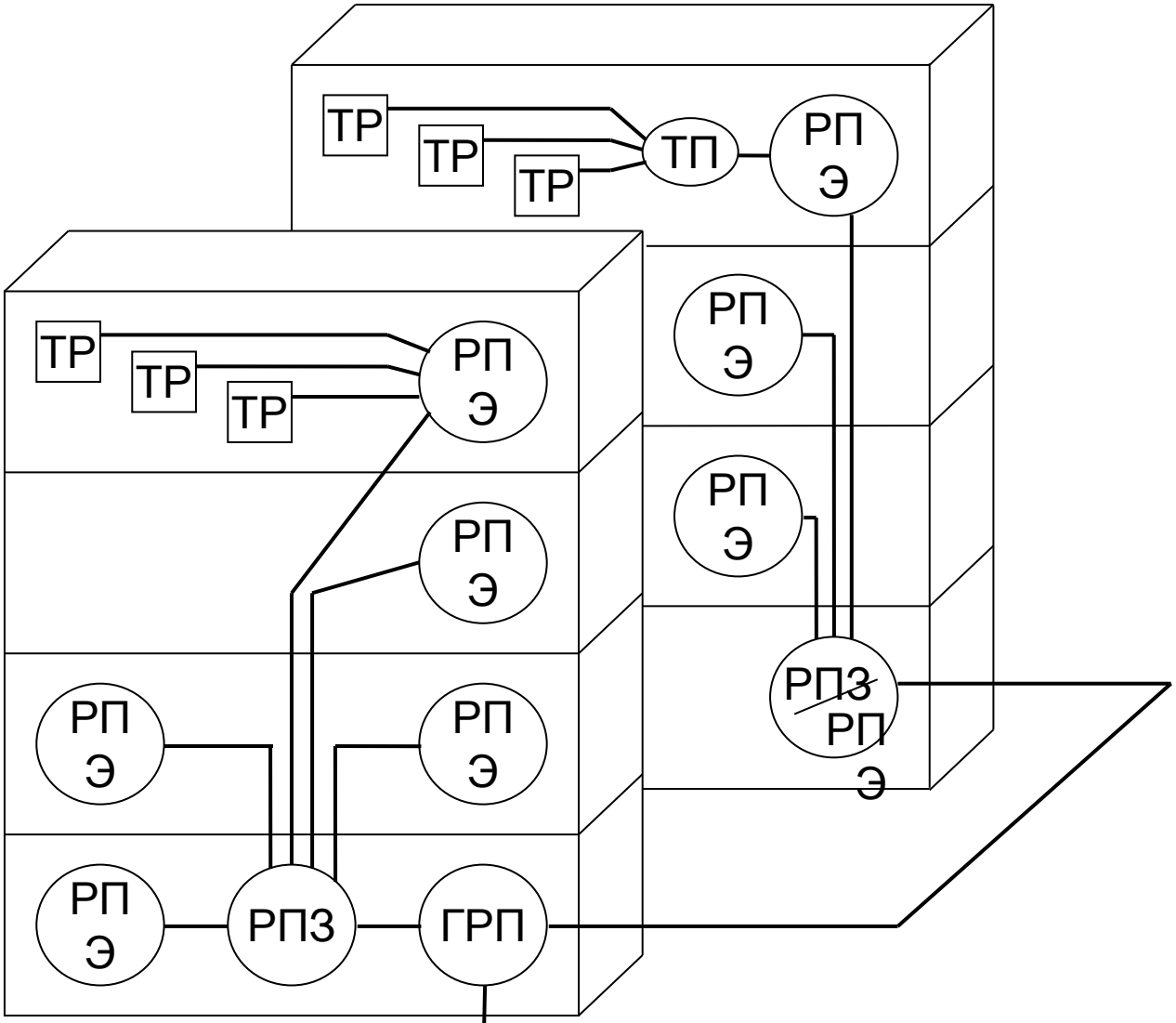
- Магистральная подсистема территории
- Магистральная подсистема здания
- Горизонтальная подсистема



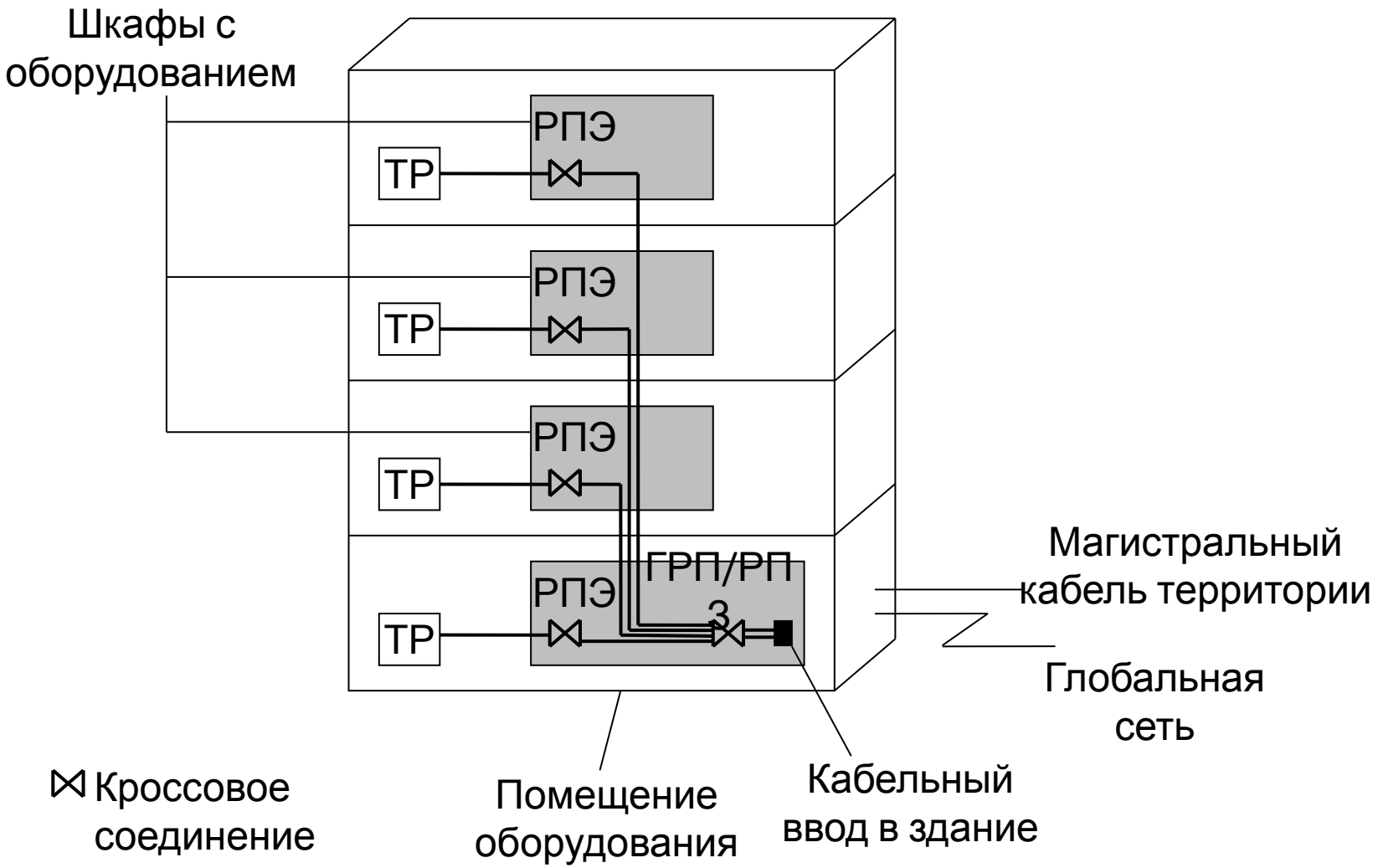
Обобщенная кабельная система



Иерархическая форма представления кабельной системы



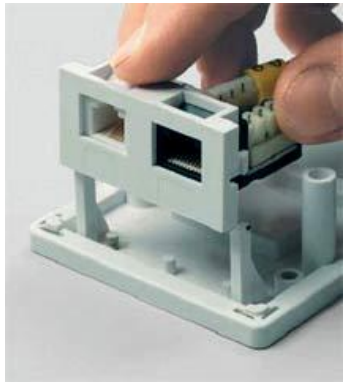
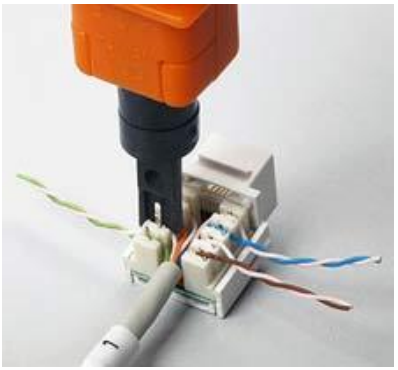
Функции распределительных пунктов



Размещение распределительных пунктов

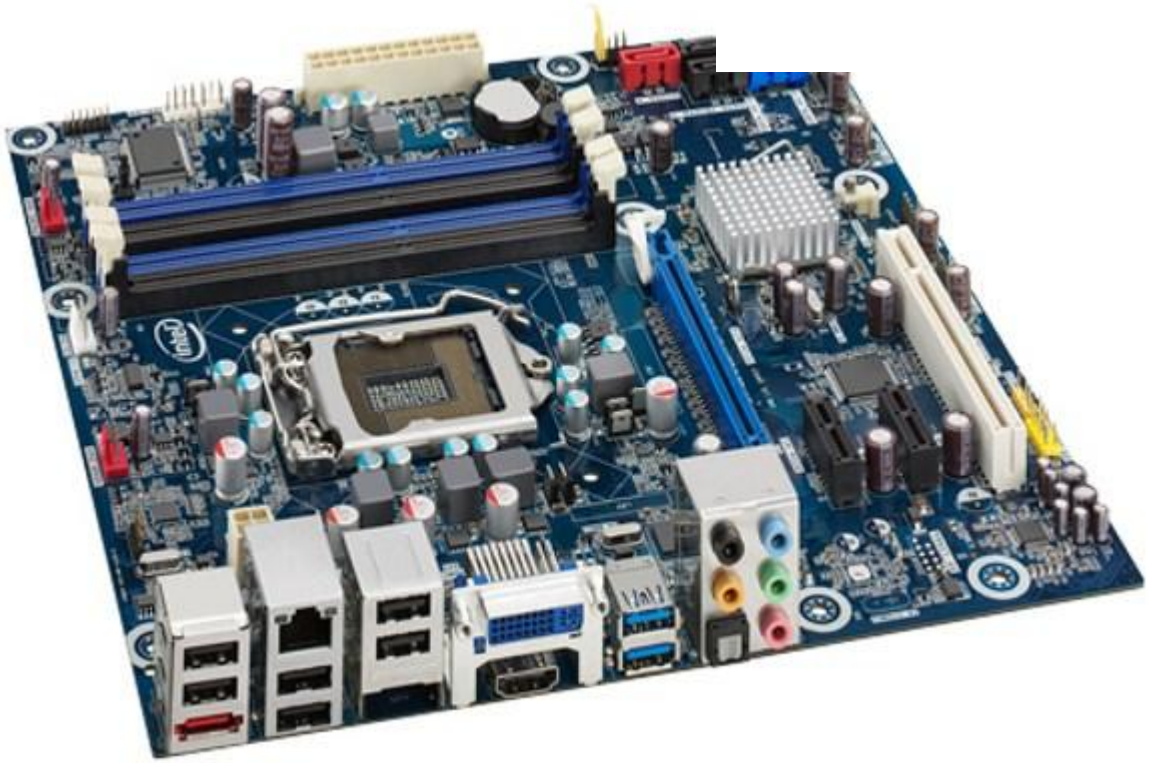
Оборудование и инструментарий, используемые при развертывании СКС

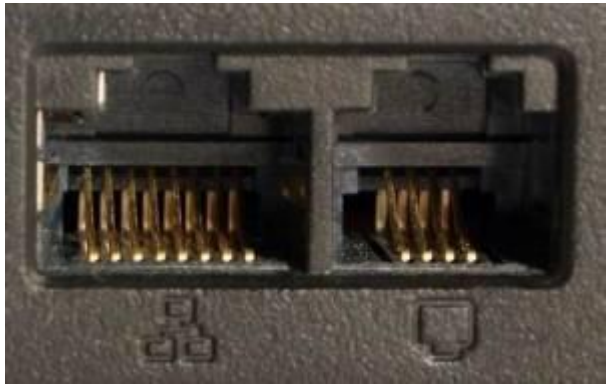


Извращения, кривые руки и тяжёлые наркотики несовместимы с СКС !

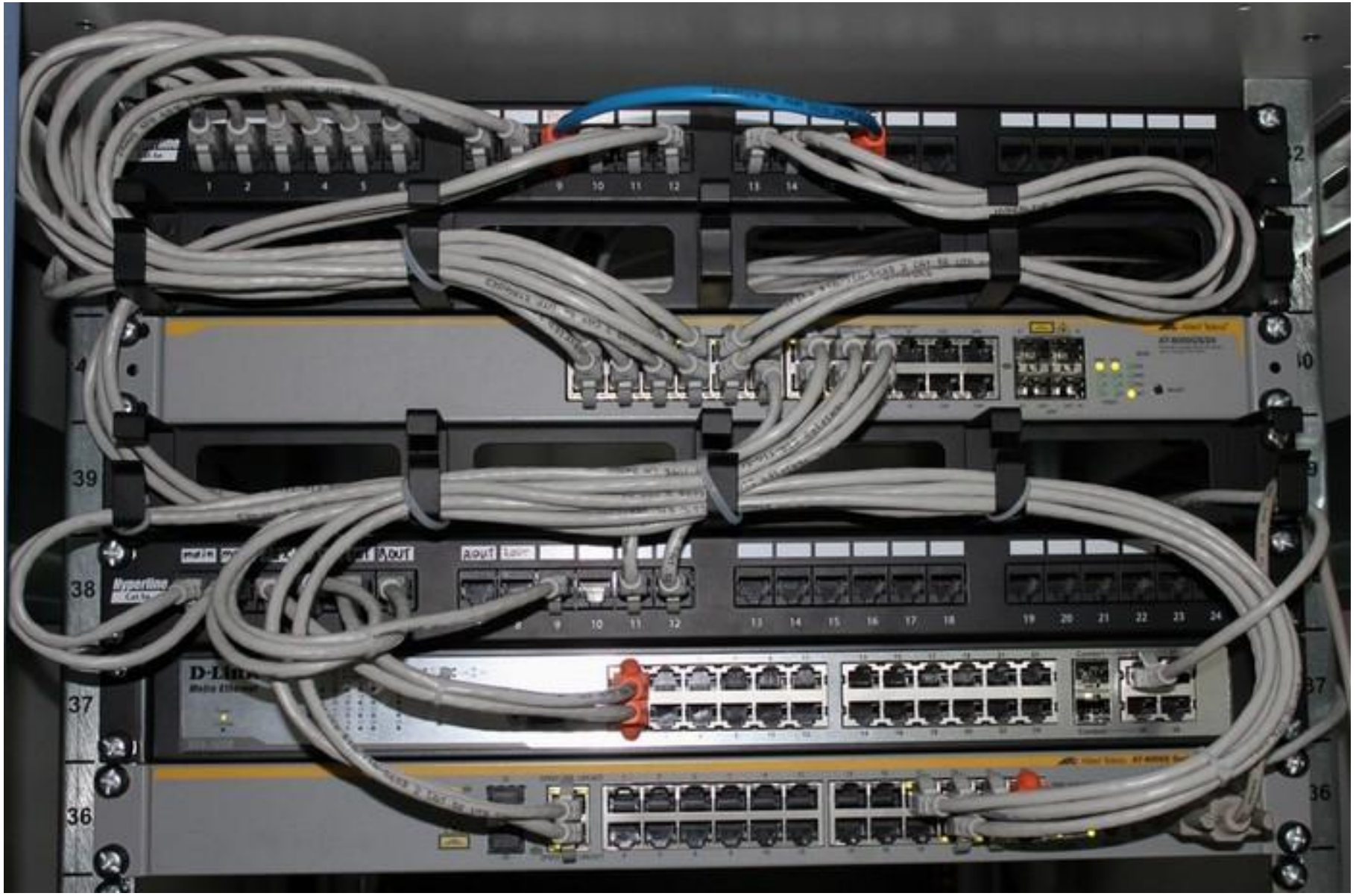
Сетевые карты



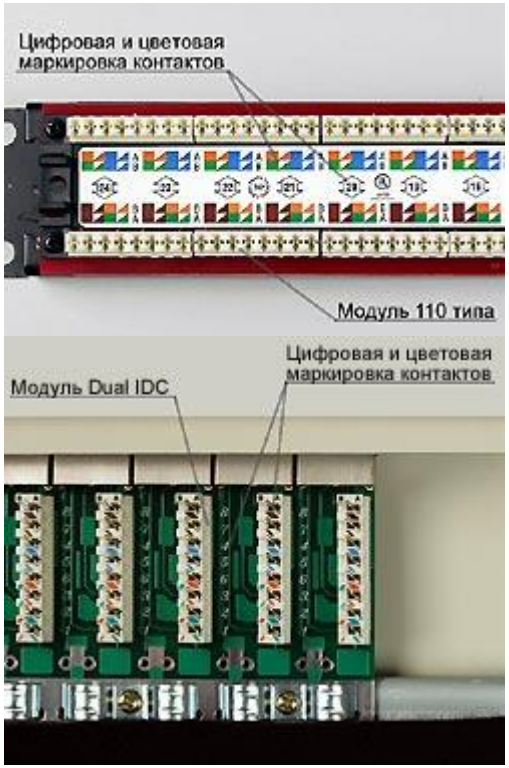


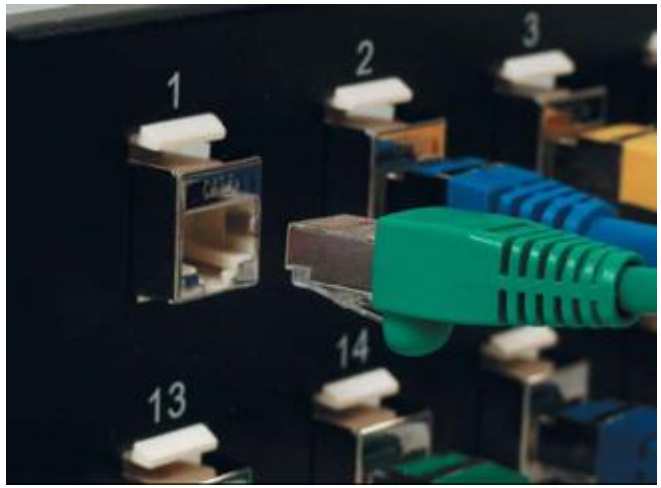
Патч-панели и сетевые розетки

Патч-панель в стойке

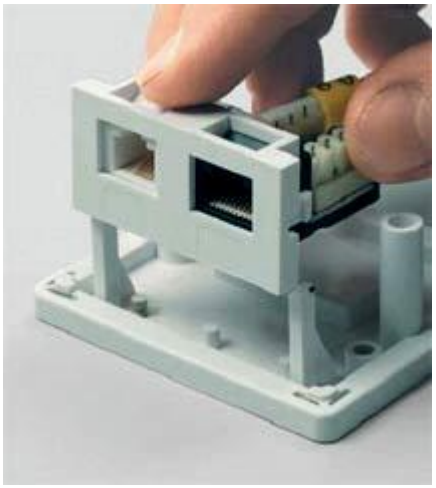


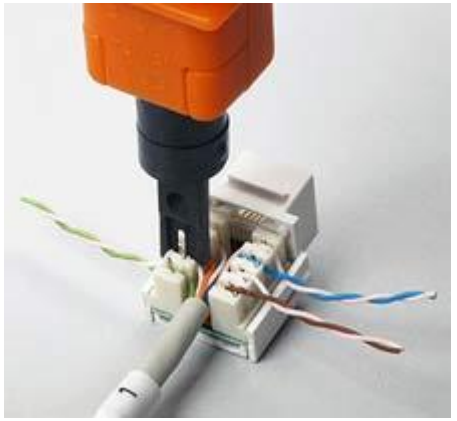
Патч-панель, интимные подробности





Разновидности розеток и модулей

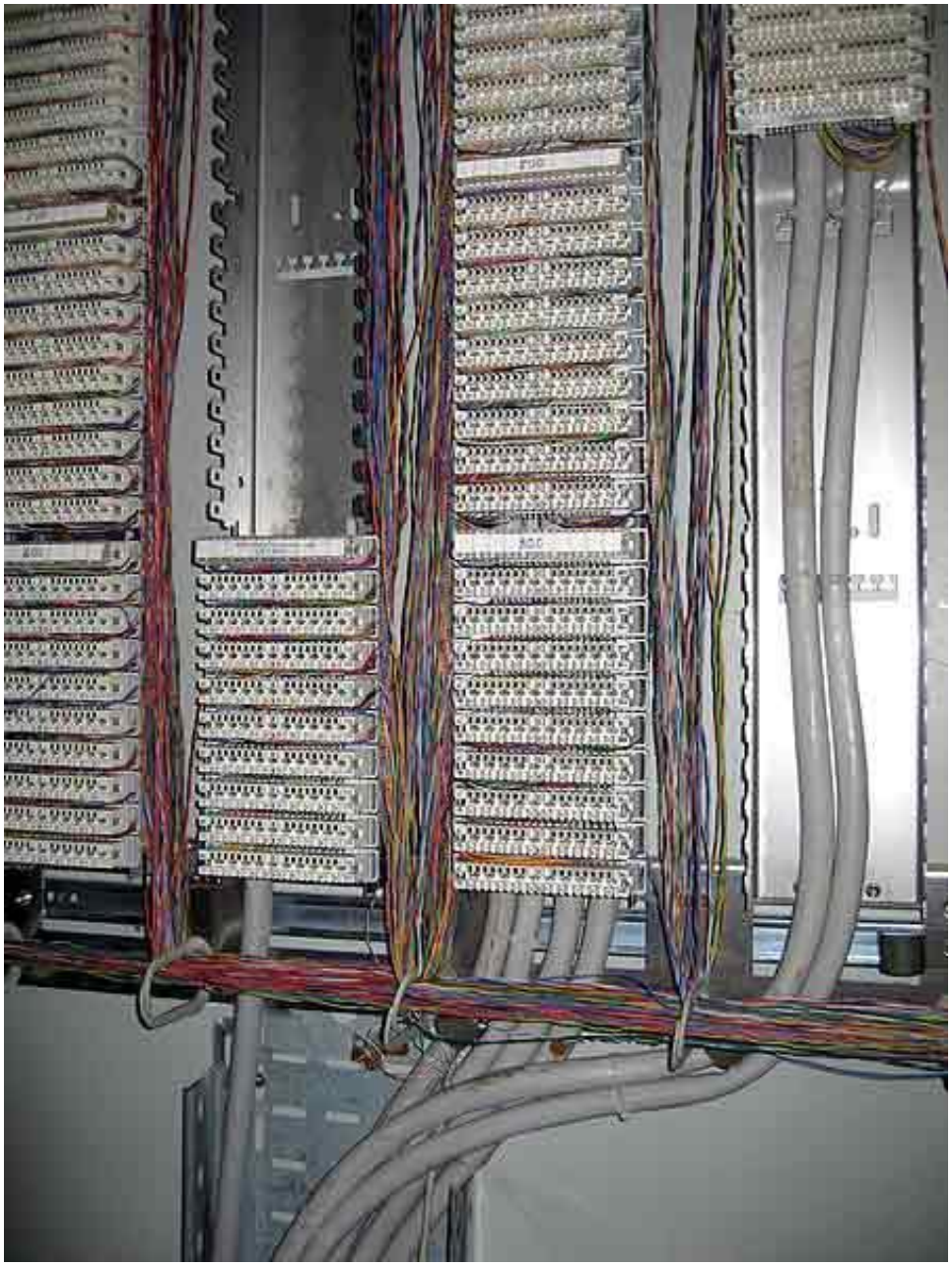


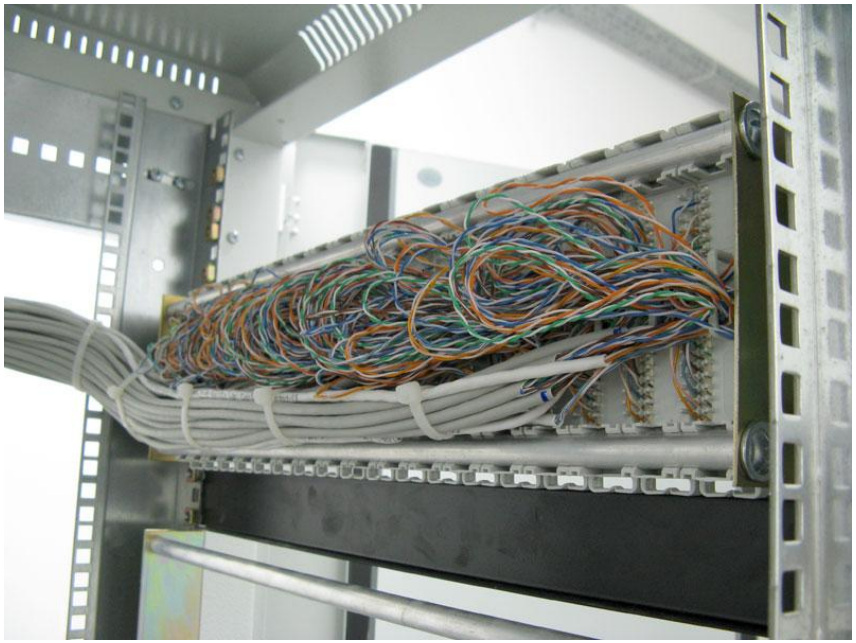


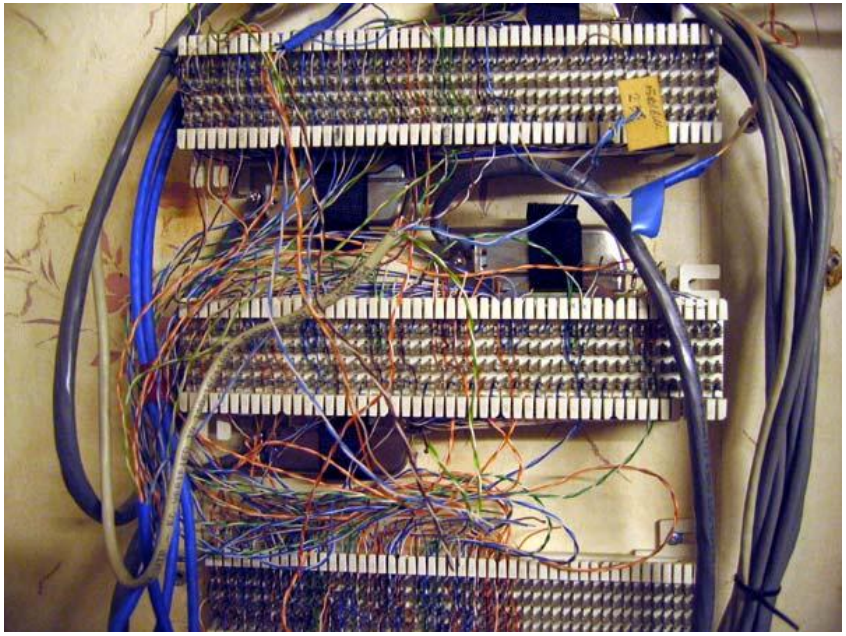
Кросс – это не о спорте, это о сети

КРОСС - **к**онтрольно **р**аспределительное **о**борудование **с**редств **с**вязи. **Кросс**, **кроссовый узел** — помещение или пространство, отведенное под коммутацию телекоммуникационных проводов

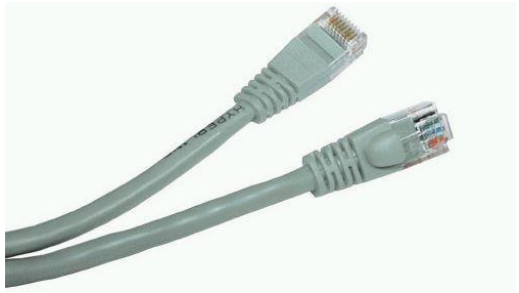
Кросс. Проводной ад.

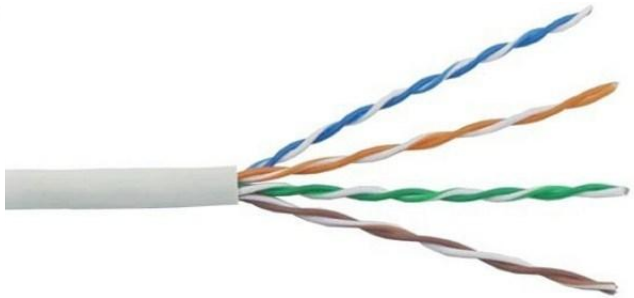




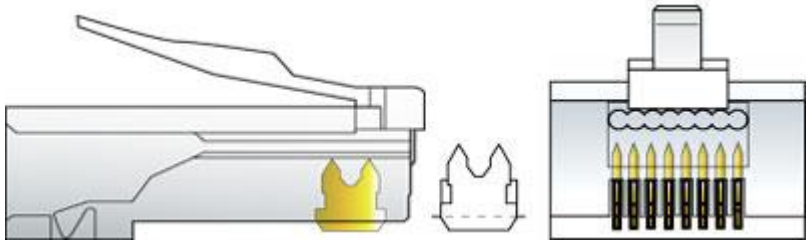


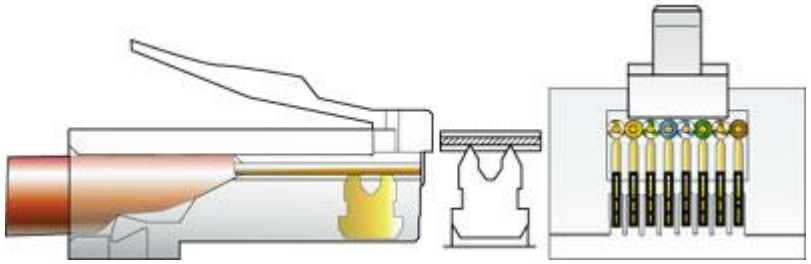
Проводные вопросы и прочие мелочи



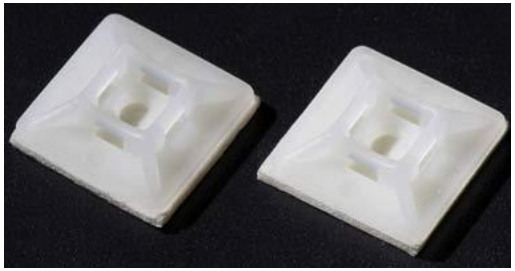


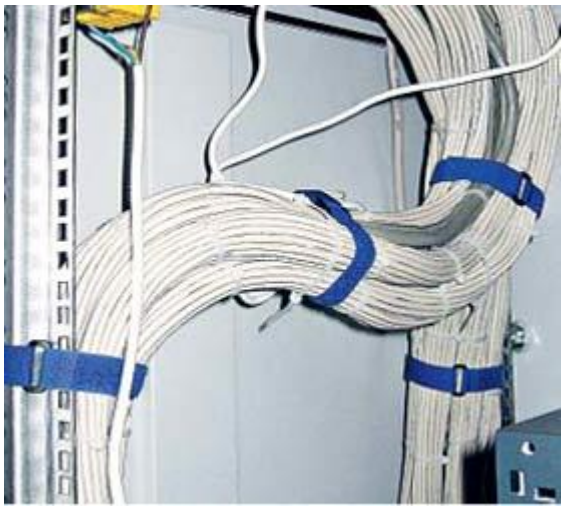
Коннекторы бывают разные…





Кабельные рюшечки…





Стойки и шкафы

Основа всего – болт и квадратная гайка!

Ну и кабельные организаторы…

Неуправляемые коммутаторы

Управляемые коммутаторы

Беспроводные сетевые карты

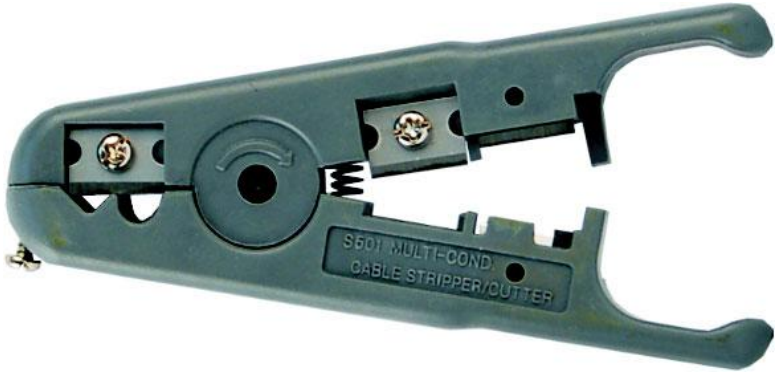
Беспроводные точки доступа

Инструменты

Crimper, Кримпер, «Обжимка»

Инструменты

Устройство для заделки кабеля (Кроссовочный нож)



Устройство для снятия оболочки и обрезки кабеля

Инструменты

Кабель-тестеры

Инструменты

Тон-генератор // Аппарат частотного поиска

Инструменты

Набор инструментов

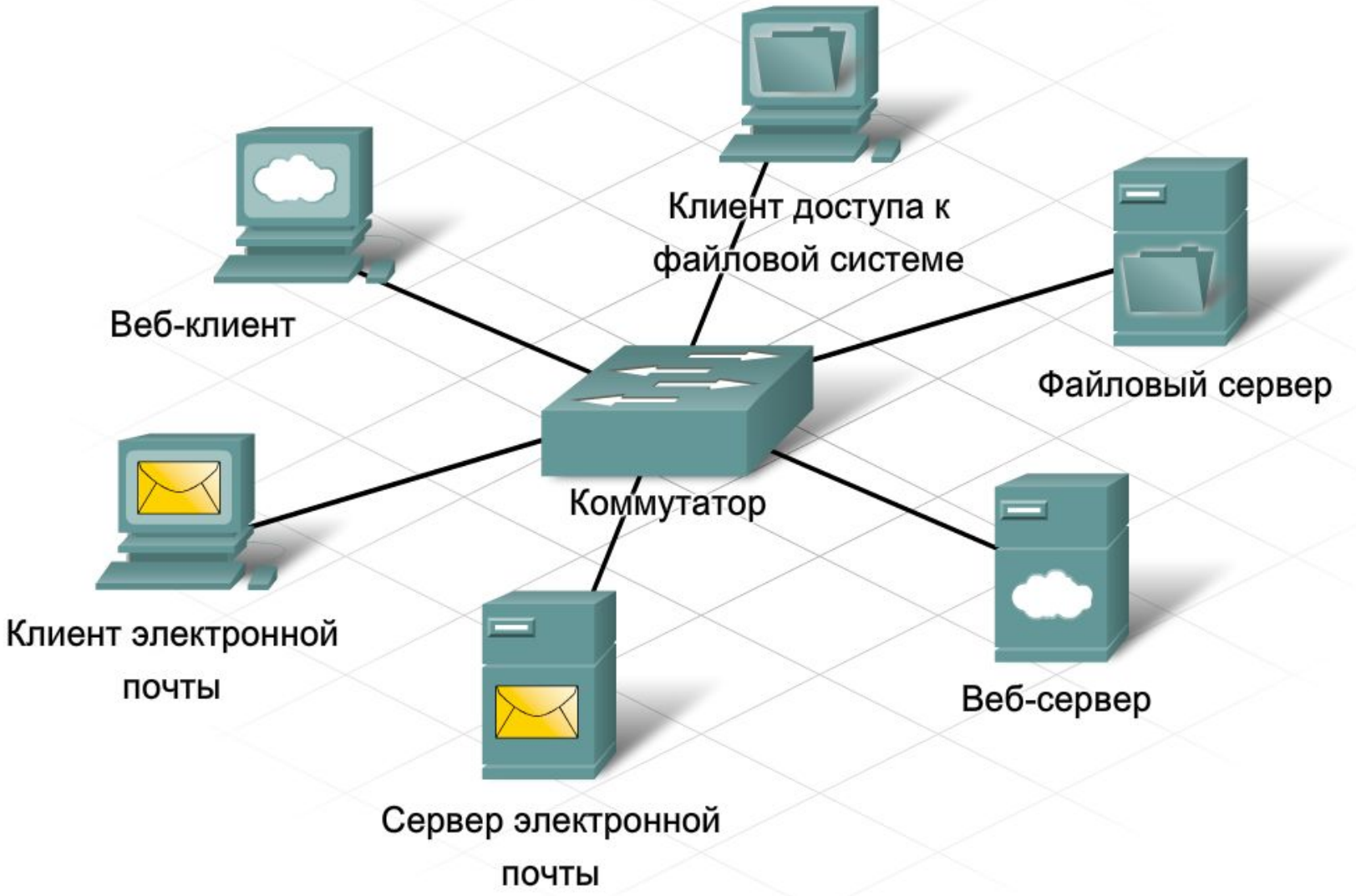
- II -

Сети для домашних пользователей и малых предприятий

(SOHO-сети)

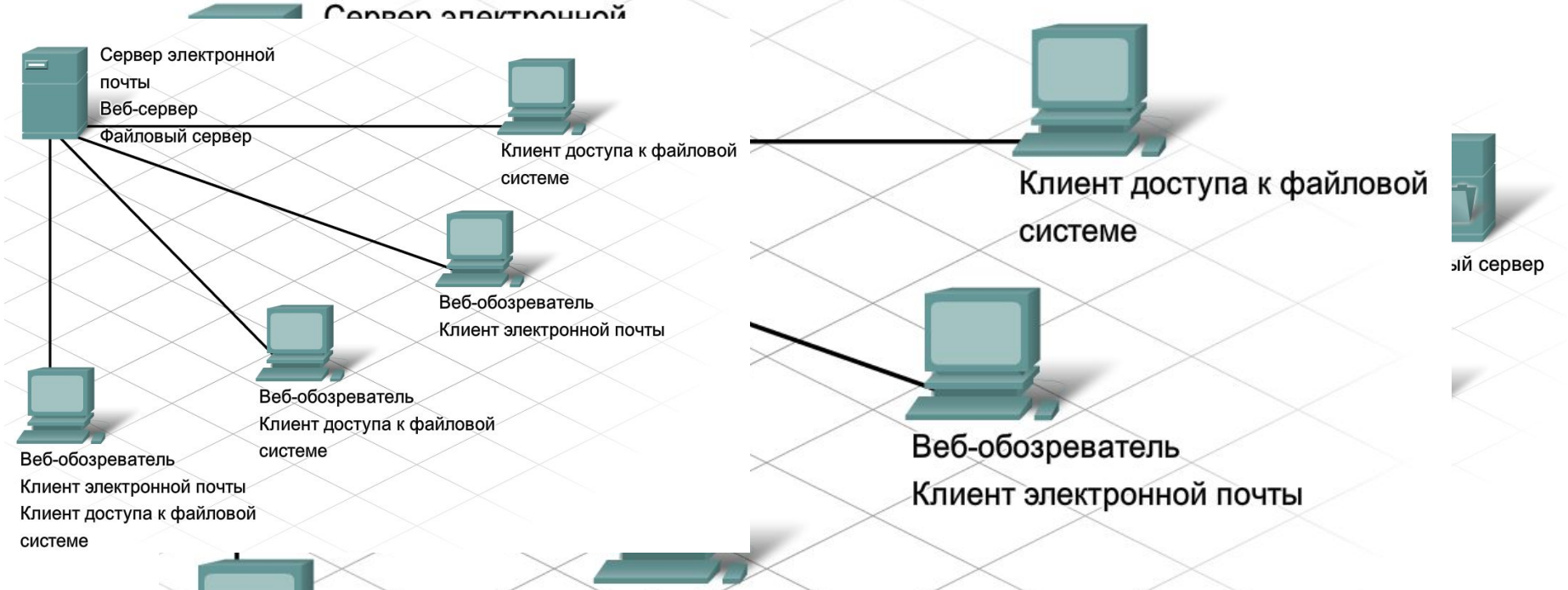
Основные компоненты сети

В компьютерной сети компьютеры выполняют различные роли



Роль компьютера в общем НЕ ИМЕЕТ отношения к топологии сети!

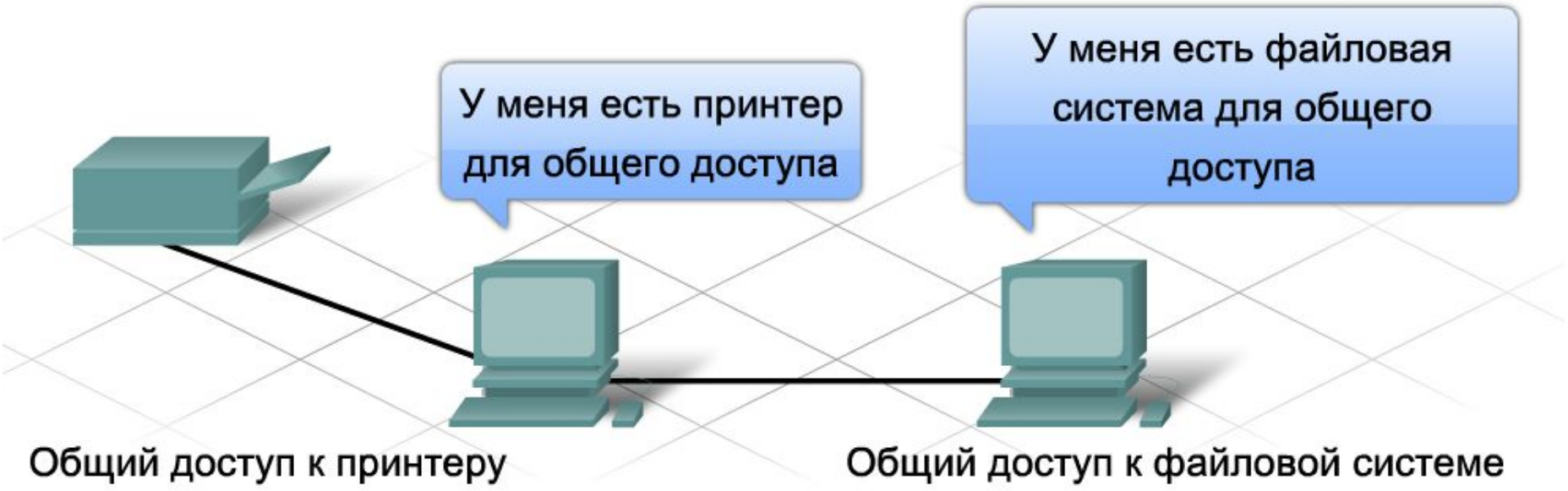
В компьютерной сети компьютеры выполняют различные роли



Не следует путать архитектуру (структуру) сети и топологию сети! Архитектура – это логическое объединение ее компонентов/устройств, а топология – это физический способ соединения устройств сети

Роль компьютера в общем НЕ ИМЕЕТ отношения к топологии сети!

Одноранговая сеть



Обычно клиентское и серверное программное обеспечение запускается на разных компьютерах, но эти роли может играть и один компьютер. В небольших корпоративных и домашних сетях многие компьютеры работают и как серверы, и как клиенты. Такие сети называются **одноранговыми**.

Одноранговая сеть

Преимущества организации одноранговой сети:

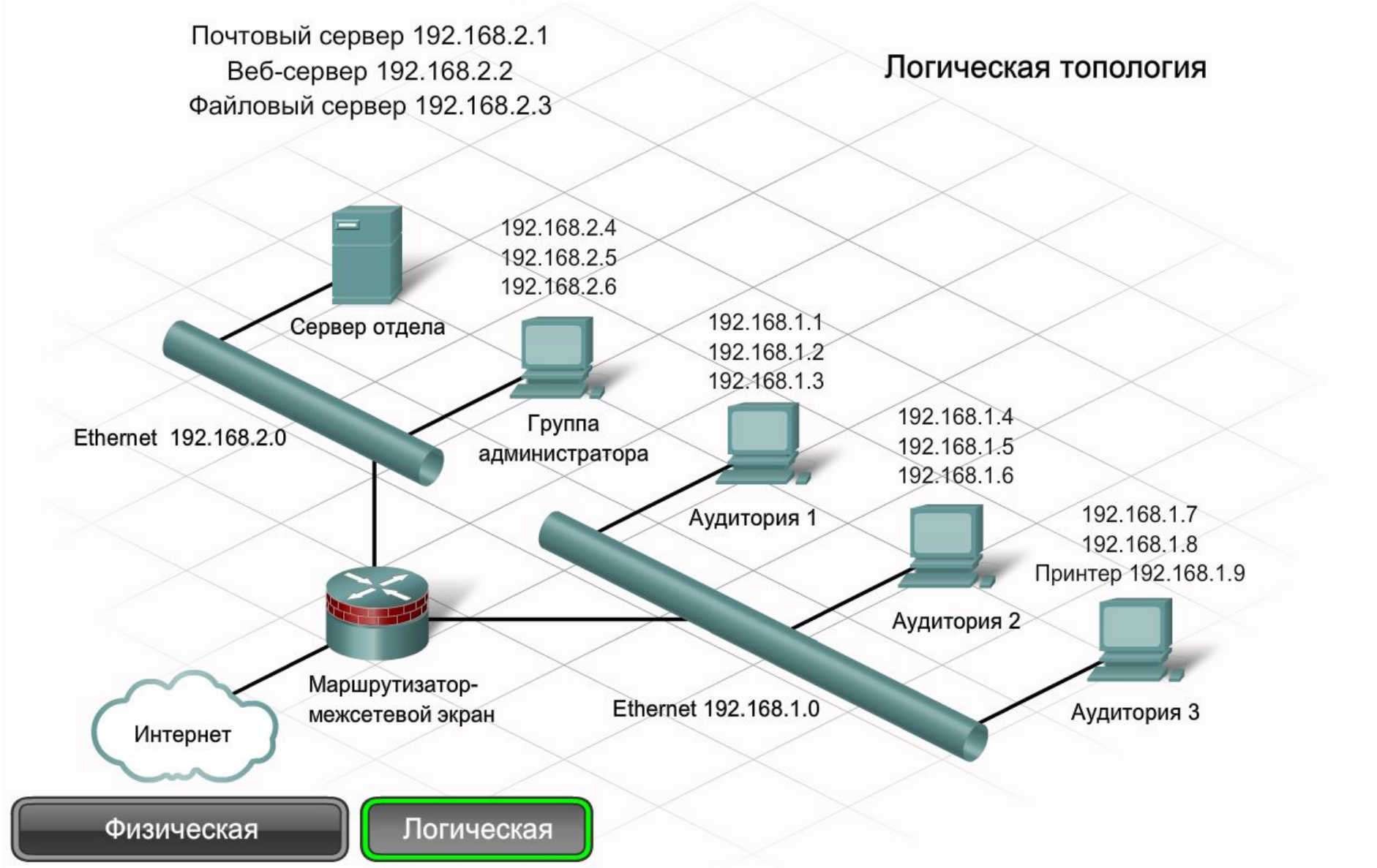
- ✔ простота развертывания;
- ✔ низкая сложность;
- ✔ более низкая стоимость, т.к. сетевые устройства и выделенные серверы могут не понадобиться;
- ✔ возможность использования для выполнения простых задач, например, передачи файлов и предоставления общего доступа к принтерам.

Недостатки организации одноранговой сети:

- ✔ отсутствие централизованного администрирования;
- ✔ низкий уровень безопасности;
- ✔ невозможность масштабирования;
- ✔ все устройства могут выполнять роль и клиентов, и серверов, что может снизить их производительность.

Топологии сетей

Топологии сетей

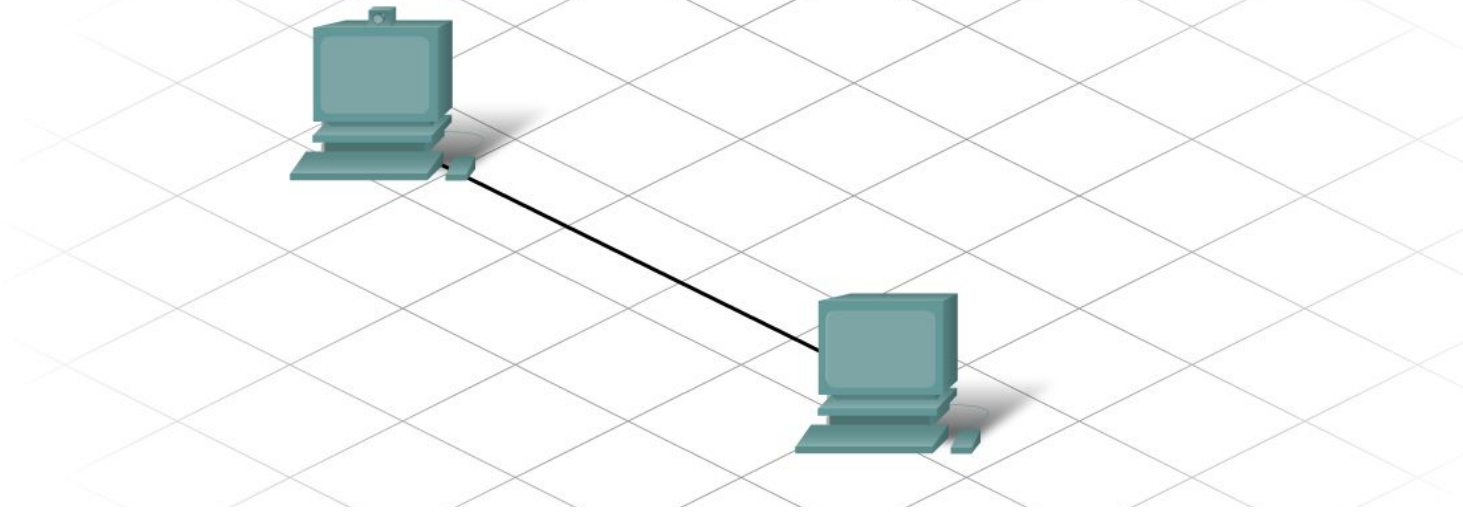


Протоколы. Правила обмена данными

Выбор **протоколов** зависит от характеристик источника, канала и адресата сообщения. Правила общения с помощью одного средства связи, например, телефона, не обязательно совпадают с правилами другого средства связи, например, почты.

Современная сеть предоставляет несколько видов телекоммуникационных услуг

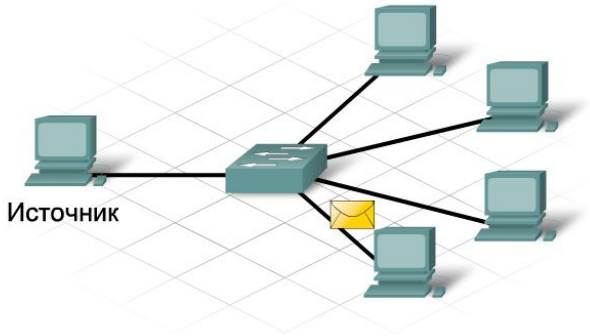
Кодировка данных при обмене между узлами должна соответствовать среде связи. Узел-отправитель преобразует передаваемое по сети сообщение в биты. Каждый бит кодируется набором звуков, световых волн или электрических импульсов, в зависимости от типа сети. Узел назначения принимает и декодирует сигналы и интерпретирует сообщение.



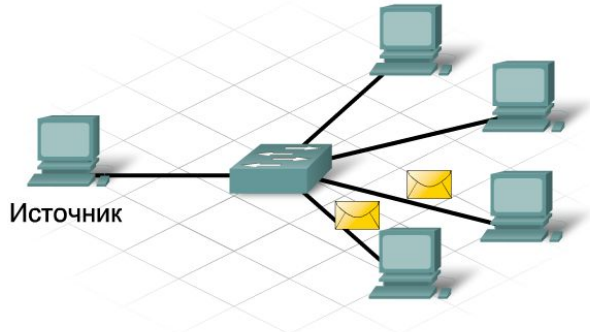
Процесс декапсуляции данных

Методы рассылки сообщений

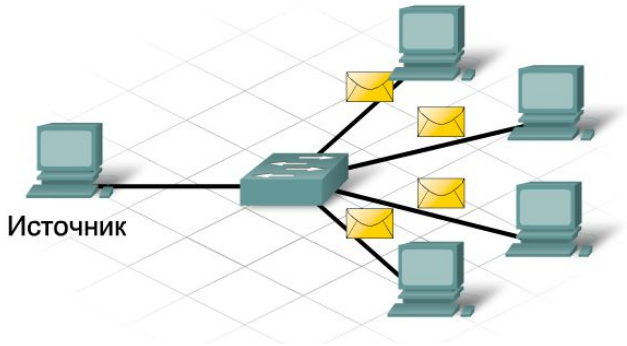
Метод рассылки "**один к одному**" называется одноадресным (**unicast**). Это означает, что у сообщения есть только один адресат.



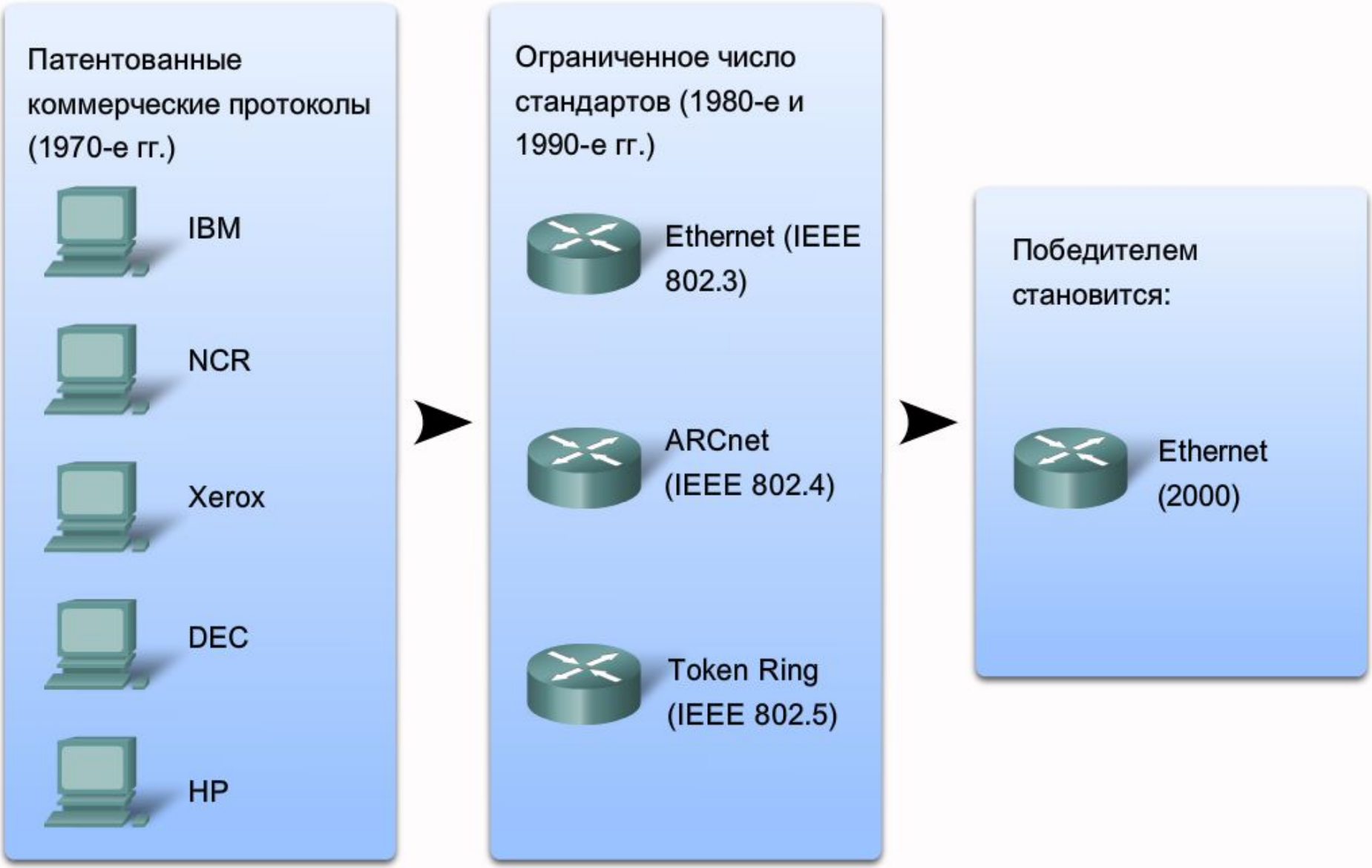
Если узел рассылает сообщения методом "**один ко многим**", это многоадресная рассылка (**multicast**). Многоадресная рассылка предусматривает одновременную отправку одного и того же сообщения группе узлов.



Если всем сетевым узлам необходимо получить сообщение в одно и то же время, используется широковещательная рассылка (**broadcast**). Это метод рассылки сообщений "**один ко всем**". Кроме того, для узлов предусмотрены правила рассылки сообщений с подтверждением и



Протоколы. Стандартизация протоколов



Протоколы. Стандартизация протоколов

С момента создания Ethernet в 1973 г. стандарты усовершенствовались, следуя за появлением более быстрых и гибких версий технологии. Способность стандарта Ethernet к развитию - одна из основных причин его популярности. Для каждой версии сети Ethernet есть свой стандарт. Например, **802.3 100BASE-T** -это стандарт **100**-мегабитной сети Ethernet с использованием **кабеля с витой парой**. Название стандарта расшифровывается следующим образом:

100 — это скорость в мегабитах в секунду;

BASE — это монополосная передача;

T - тип кабеля, в данном случае, витая пара.

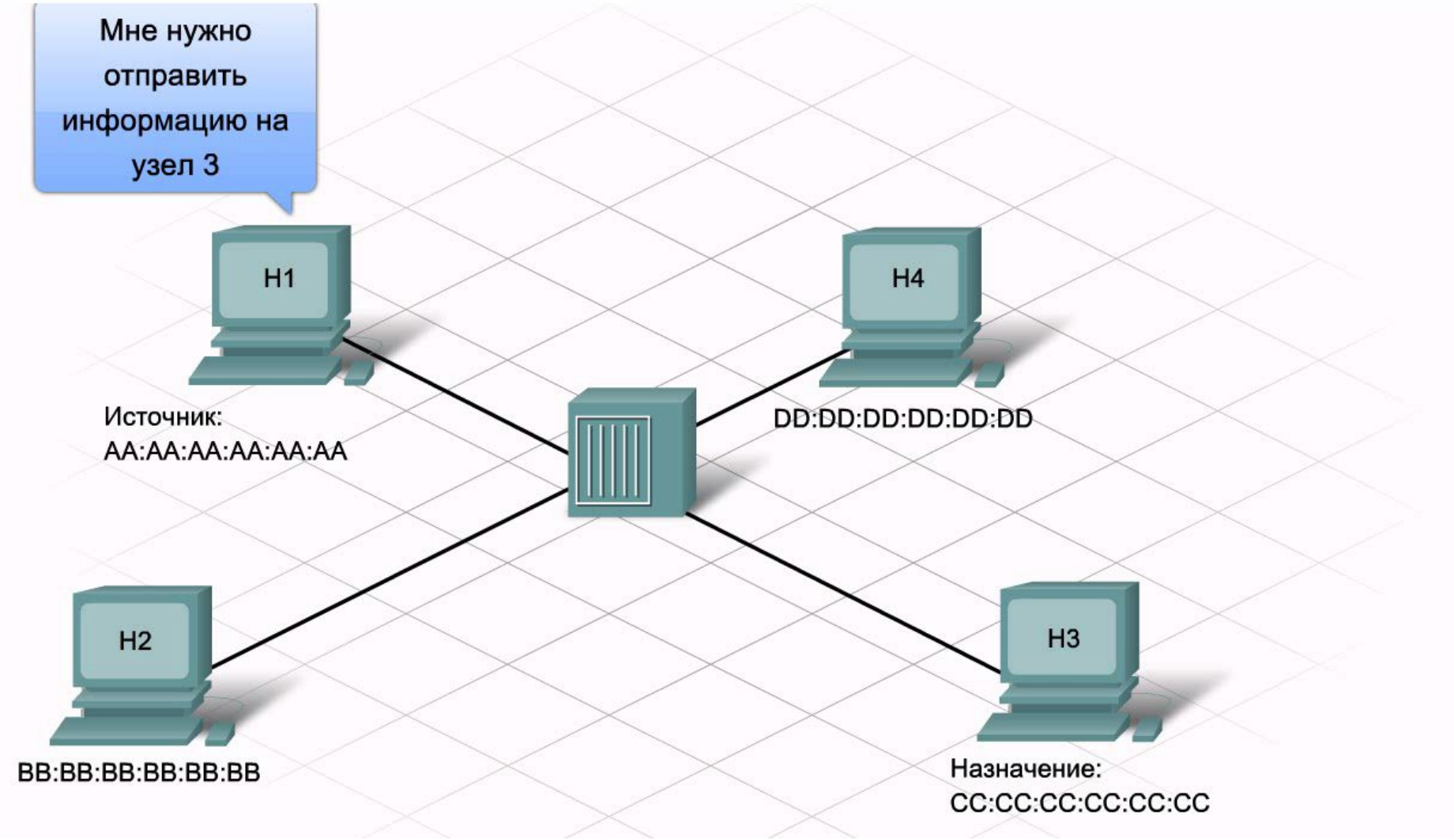
Институт инженеров по электротехнике и электронике, или IEEE (произносится как "ай-три и"), занимается сетевыми стандартами, включая Ethernet и стандарты беспроводных сетей. Комитеты IEEE отвечают за утверждение и обновление стандартов подключения, требований к среде передачи и протоколам связи. Каждому технологическому стандарту присваивается номер, соответствующий номеру ответственного за утверждение и обновление комитета. Стандартами Ethernet занимается комитет 802.3.

Физическая адресация

В процессе изготовления всем сетевым интерфейсам Ethernet даются физические адреса. Он называется **адресом управления доступом к среде** (**MAC-адресом**). MAC-адрес идентифицирует каждый узел источника и каждый узел назначения в сети.

Когда подключенный к Ethernet узел включается в обмен данными, он рассылает кадры со своим MAC-адресом в качестве источника и MAC-адресом предполагаемого получателя. Все принимающие узлы декодируют кадр и считывают MAC-адрес назначения. Если он соответствует настроенному MAC-адресу сетевой интерфейсной платы, она обрабатывает и сохраняет сообщение. Если MAC-адрес назначения не соответствует MAC-адресу узла, сетевой адаптер игнорирует сообщение.

Физическая адресация



Обмен данными в Ethernet

Стандартные протоколы Ethernet определяют многие аспекты сетевого обмена данными, включая формат и размер кадра, синхронизацию и кодировку.

Поля кадра стандарта IEEE 802.3 Ethernet

Байты	Имя поля
7	Преамбула
1	Разделитель начала кадра
6	MAC-адрес назначения
6	MAC-адрес источника
2	Поле "Длина/тип"
46 - 1500	Инкапсулированные данные
4	Контрольная последовательность кадра (контрольная сумма пакета CRC)

Максимальный размер кадров Ethernet, начиная с поля MAC-адреса назначения до контрольной последовательности кадра, составляет **1518 байт**, **минимальный — 64 байта**. Не входящие в этот диапазон кадры принимающие узлы не обрабатывают. Помимо форматов, размеров и синхронизации кадра стандарты Ethernet определяют кодирование бит кадра при передаче по каналу.

Логическая адресация

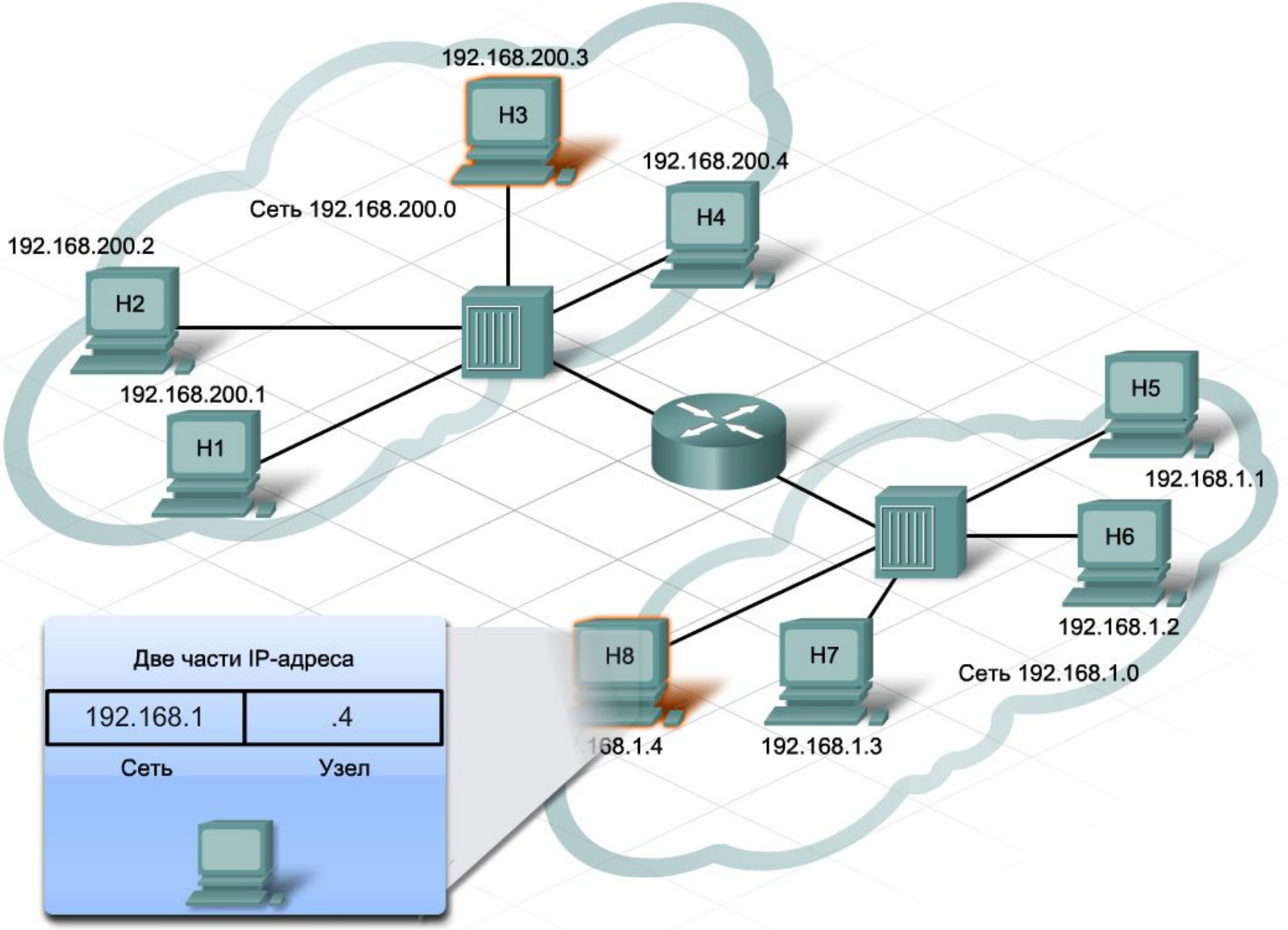
Как правило, имя человека не меняется. Адрес же зависит от местожительства и может измениться. MAC-адрес узла не меняется, физически присвоен сетевому адаптеру и известен как физический адрес. Он остается неизменным, независимо от расположения узла в сети.

IP-адрес похож на адрес места жительства человека. Он называется **логическим адресом**, поскольку присваивается логически, в зависимости от местонахождения узла. IP-адрес, или сетевой адрес, присваивает узлу сетевой администратор на основе характеристик локальной сети.

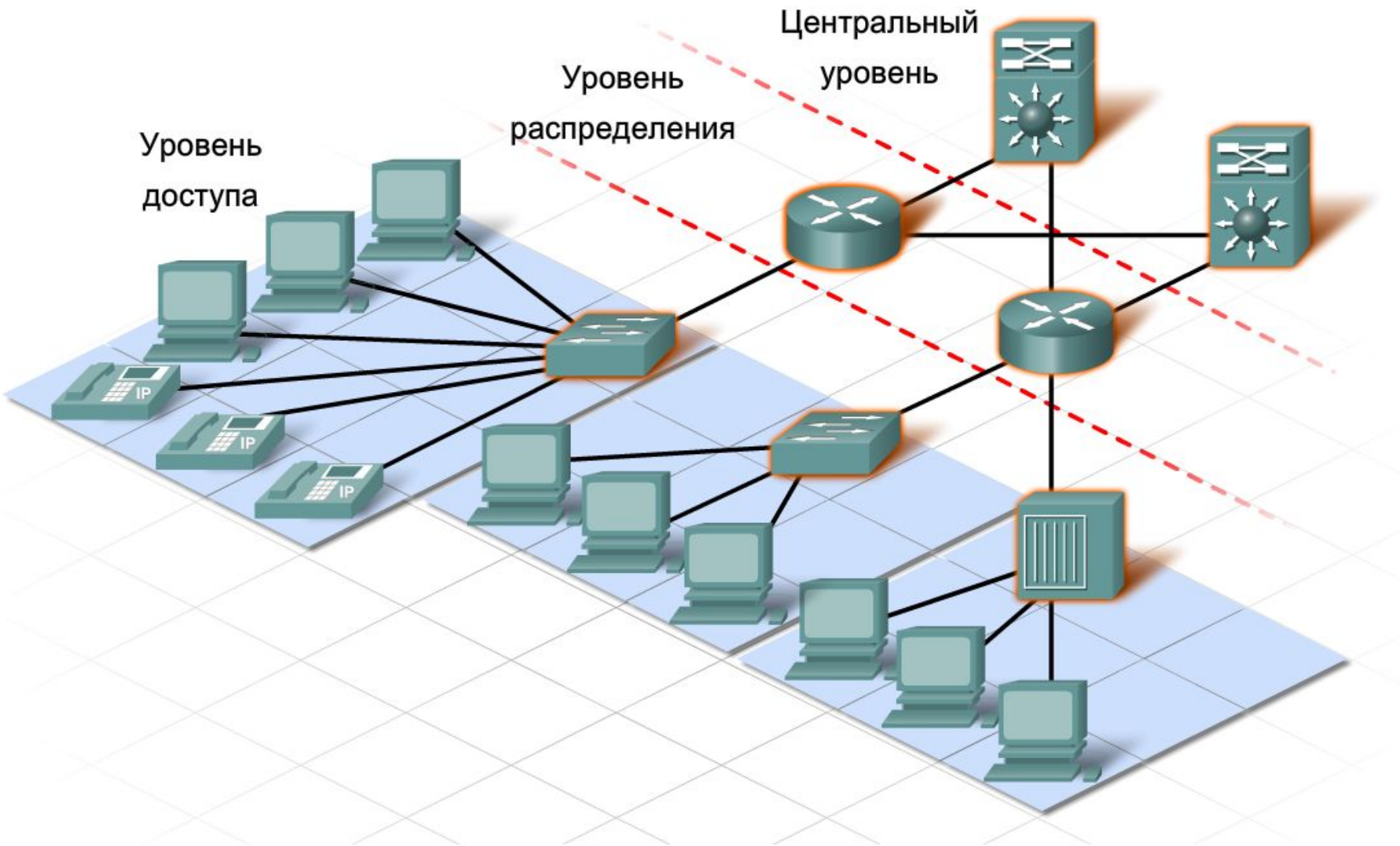
IP-адреса состоят из двух частей. Одна из них является идентификатором локальной сети. Сетевая часть IP-адреса общая у всех узлов в одной локальной сети. Вторая часть IP-адреса является идентификатором конкретного узла. Относящаяся к узлу часть IP-адреса в одной локальной сети не повторяется.

Физический MAC-адрес и логический IP-адрес необходимы компьютеру для обмена данными в иерархической сети точно так же, как для отправки письма необходимо имя и адрес человека.

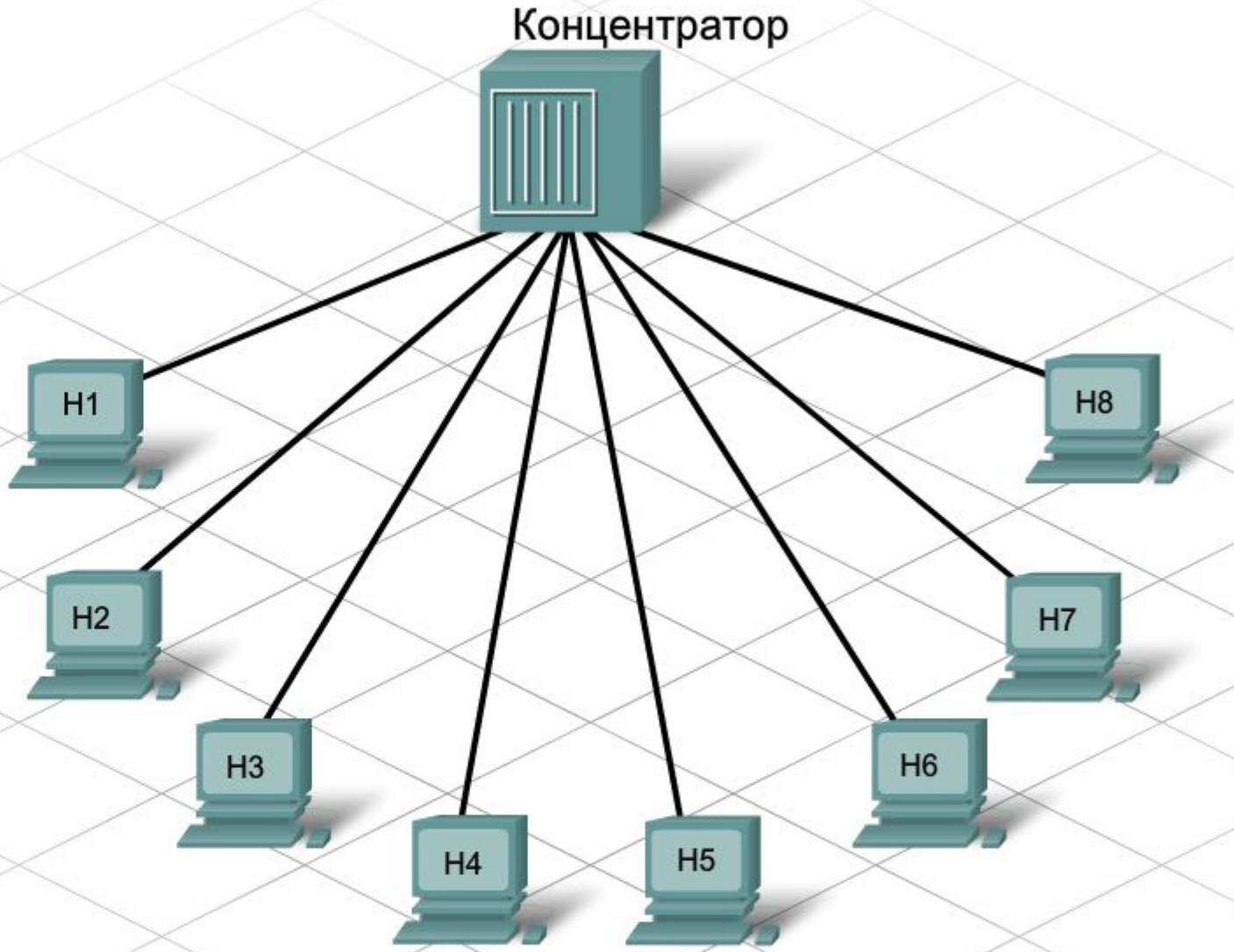
Логическая адресация



Уровни и устройства доступа и распределения



Уровень доступа. Концентраторы



выведены из эксплуатации.

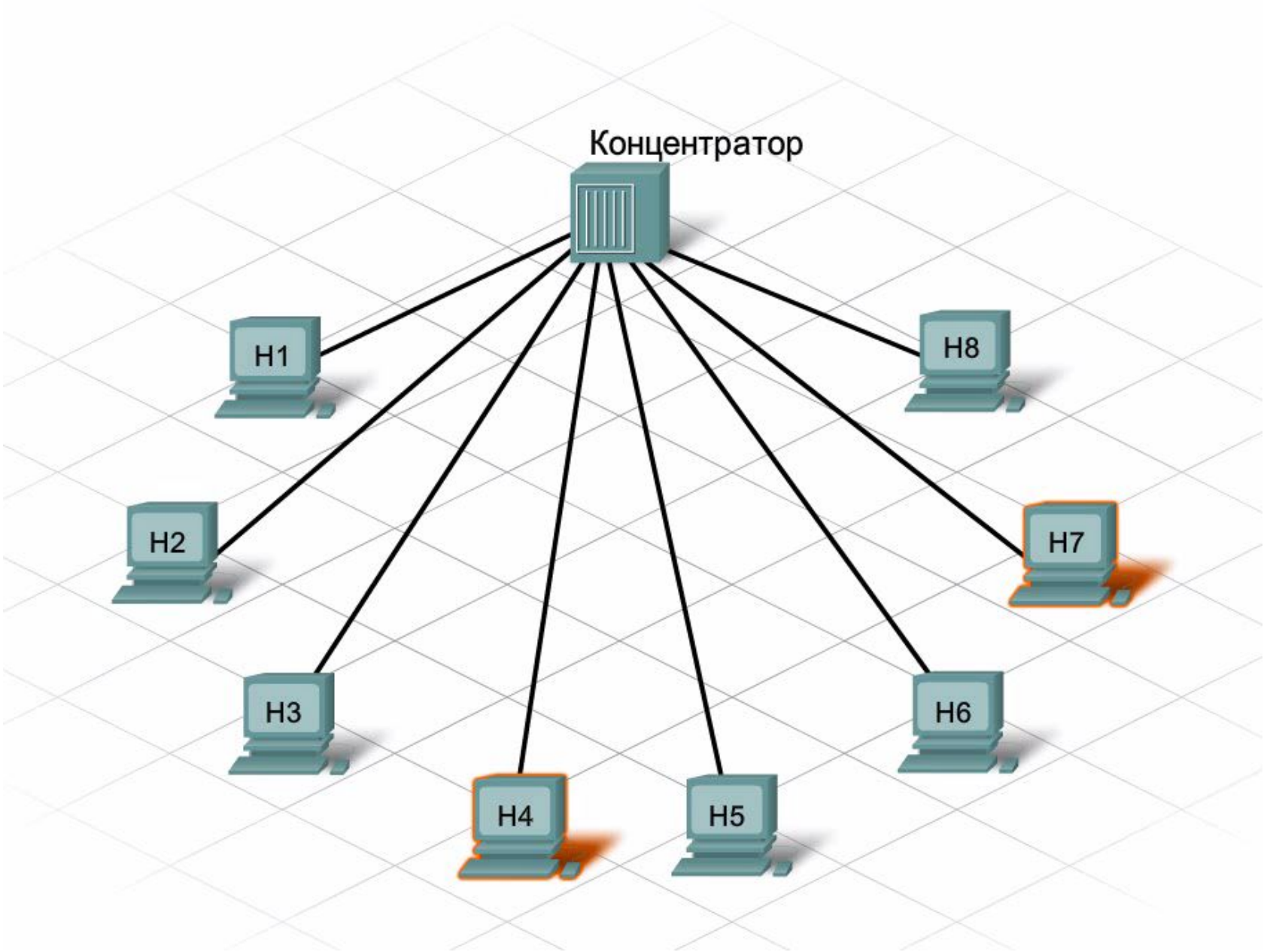
Коллизия. Домен коллизий

Через концентратор Ethernet можно одновременно отправлять только одно сообщение. Возможно, два или более узла, подключенные к одному концентратору, попытаются одновременно отправить сообщение. При этом происходит столкновение электронных сигналов, из которых состоит сообщение.

Столкнувшиеся сообщения искажаются. Узлы не смогут их прочесть. Поскольку концентратор не декодирует сообщение, он не обнаруживает, что оно искажено, и повторяет его всем портам. Область сети, в которой узел может получить искаженное при столкновении сообщение, называется **доменом коллизий**.

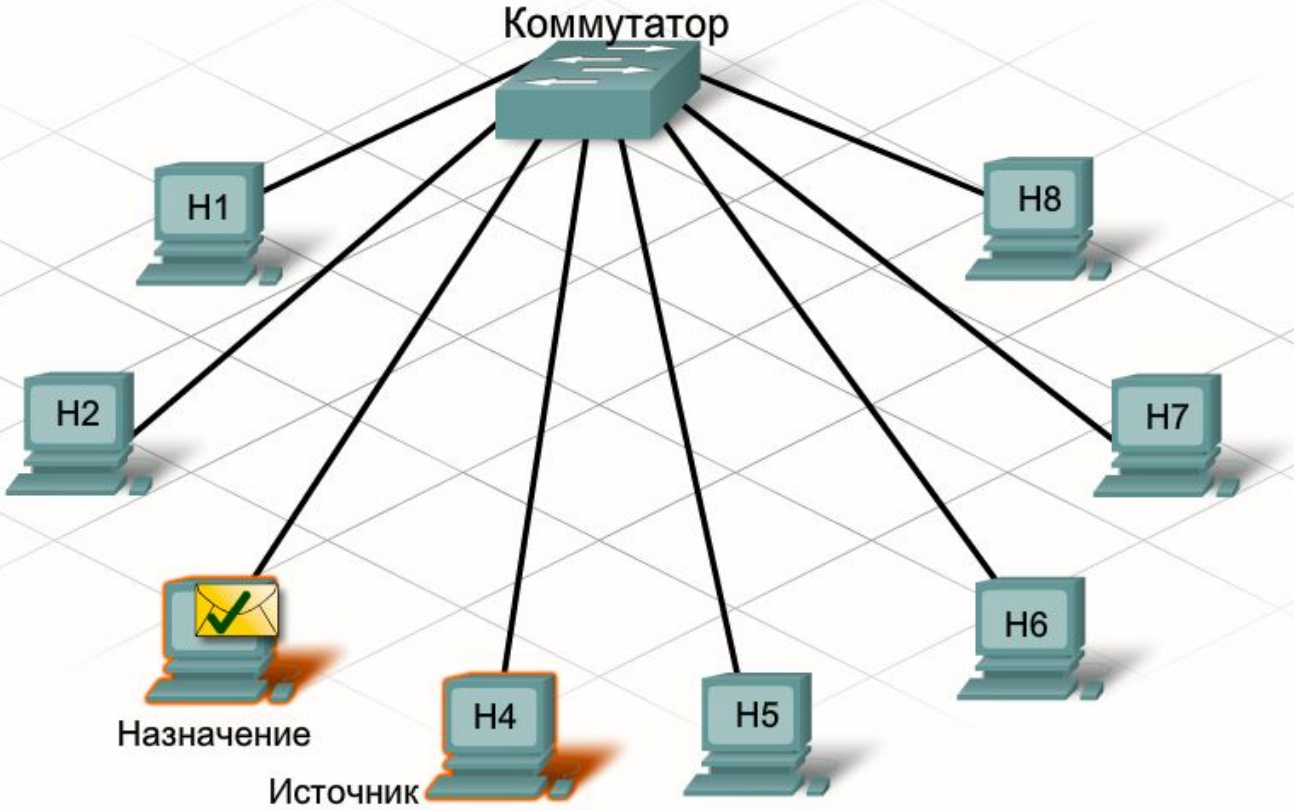
Внутри этого домена узел, получивший искаженное сообщение, обнаруживает, что произошла **коллизия**. Каждый отправляющий узел какое-то время ждет и затем пытается снова отправить или переправить сообщение. По мере того, как количество подключенных к концентратору узлов растет, растет и вероятность столкновения. Чем больше столкновений, тем больше будет повторов. При этом сеть перегружается, и скорость

Коллизия. Домен коллизий



Уровень доступа. Коммутаторы

Таблица MAC-адресов			
fa0/1	fa0/2	fa0/3	fa0/4
206d.8c01.0000	206d.8c01.1111	206d.8c01.2222	206d.8c01.3333
fa0/5	fa0/6	fa0/7	fa0/8
206d.8c01.4444	206d.8c01.5555	206d.8c01.6666	206d.8c01.7777



устанавливать несколько соединений одновременно без

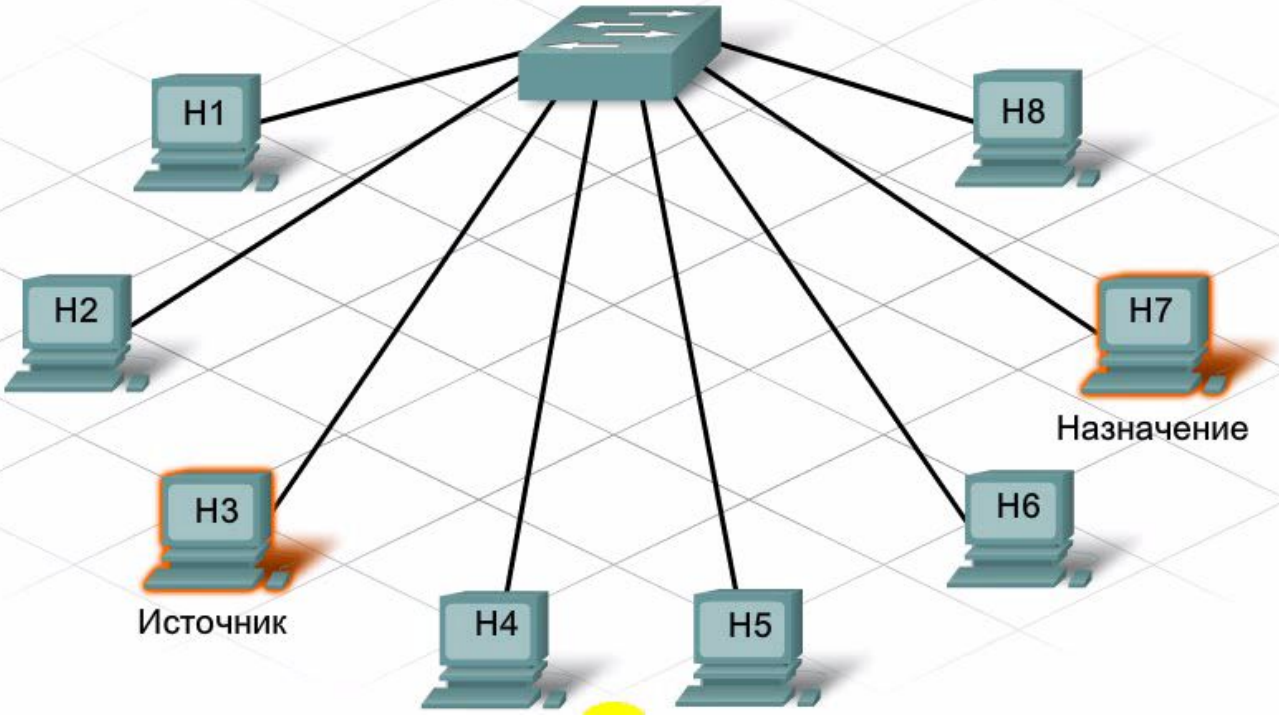
Коммутаторы. Обработка нового узла

Что происходит в том случае, если коммутатор получает кадр, адресованный новому узлу, которого еще нет в таблице MAC-адресов? Если MAC-адреса назначения нет в таблице, коммутатор не может создать отдельный канал, поскольку не имеет соответствующей информации. Если коммутатор не может определить, где расположен узел назначения, он передает сообщение всем подключенным узлам, используя процесс, который называется **массовой рассылкой (broadcast, броадкастом)**. Каждый узел сравнивает MAC-адрес назначения сообщения со своим MAC-адресом, но только тот узел, которому оно адресовано, обрабатывает сообщение и отвечает на него.

Коммутатор строит таблицу MAC-адресов, проверяя MAC-адрес источника в каждом кадре, который проходит между узлами. Когда новый узел отправляет сообщение или отвечает на сообщение из массовой рассылки, коммутатор немедленно выясняет его адрес и порт, к которому он подключен. Таблица динамически обновляется каждый раз, как коммутатор считывает новый MAC-адрес источника. Таким образом он быстро узнает адреса всех

Коммутаторы. Обработка нового узла

Таблица MAC-адресов			
fa0/1	fa0/2	fa0/3	fa0/4
260d.8c01.0000	260d.8c01.1111	260d.8c01.2222	260d.8c01.3333
fa0/5	fa0/6	fa0/7	fa0/8
260d.8c01.4444	260d.8c01.5555		260d.8c01.7777

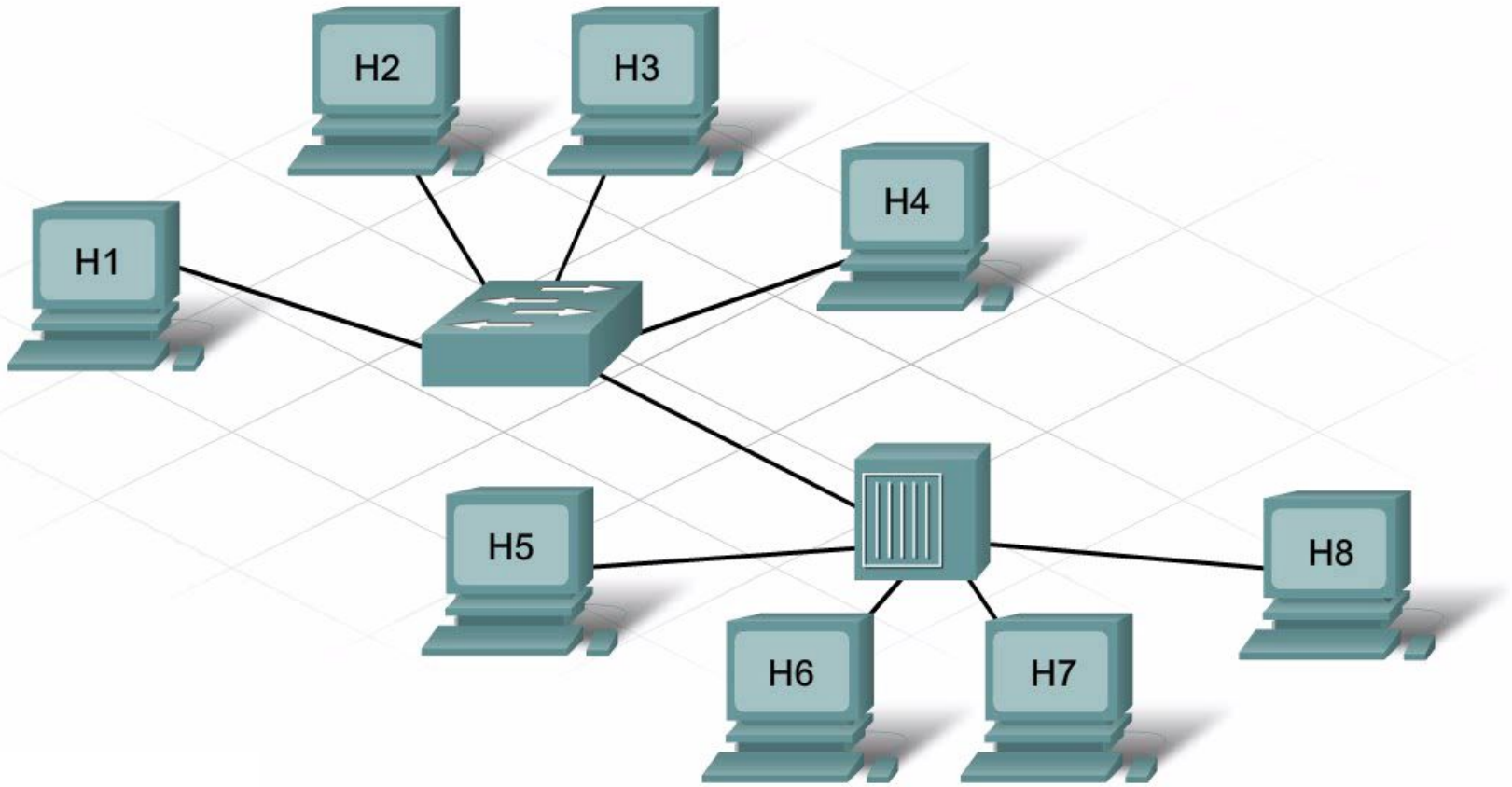


Широковещательная рассылка сообщений

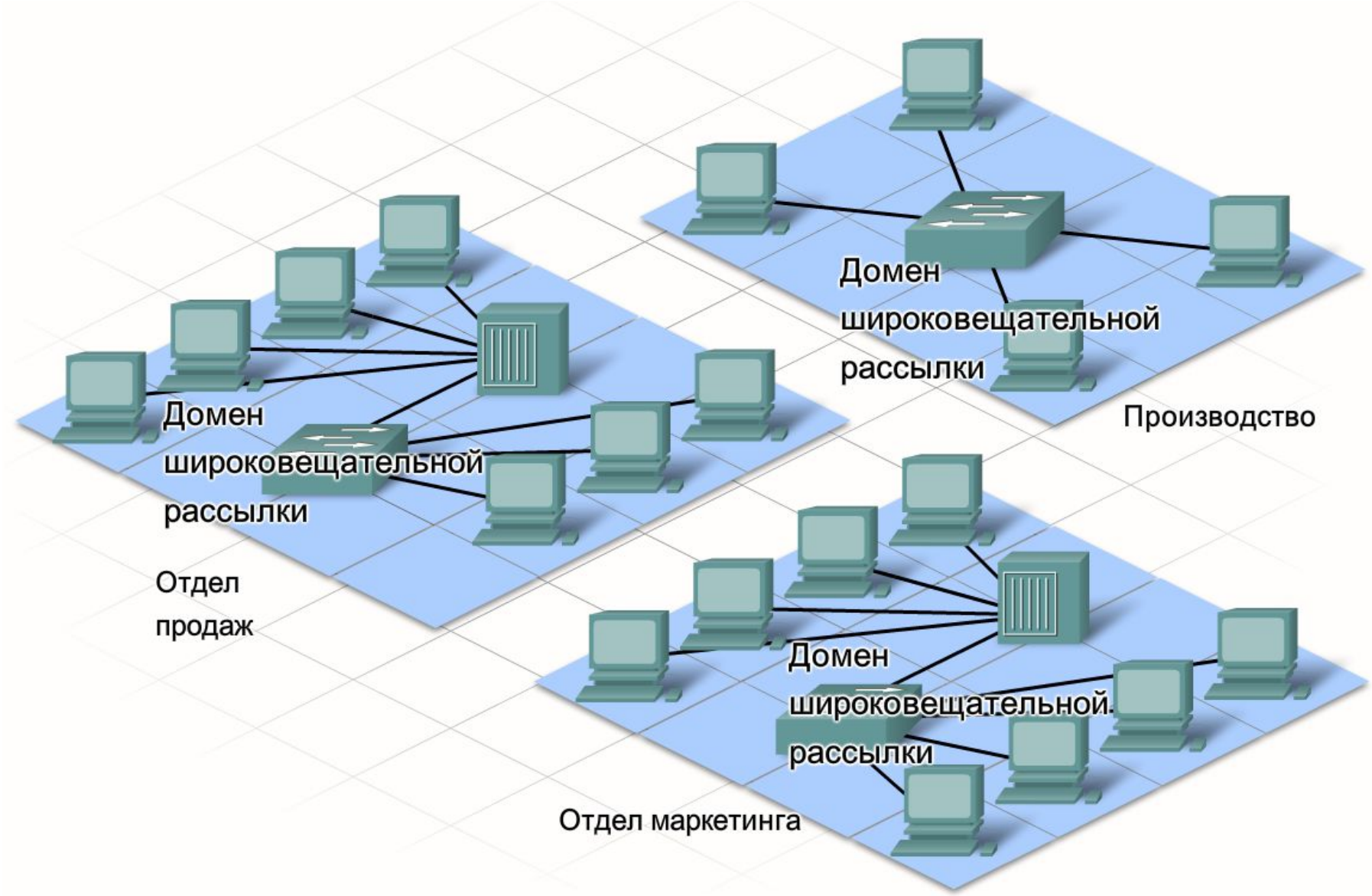
Если узлы подключаются через коммутатор или концентратор, образуется единая локальная сеть. В локальной сети одному узлу часто приходится одновременно рассылать сообщения всем остальным узлам. Для этого используется так называемая **широковещательная (broadcast) рассылка сообщений**. Широковещательные рассылки нужны в том случае, если узлам нужно найти информацию, не зная точно, на каком узле она находится, или если узлу нужно своевременно предоставить информацию всем остальным узлам в той же сети.

Для этого сообщения широковещательной рассылки отправляются на уникальный MAC-адрес, который опознают все узлы. В действительности MAC-адрес широковещательной рассылки представляет собой 48-битный адрес, в который входят все остальные адреса. Из-за своей длины MAC-адрес обычно представляется в шестнадцатеричном формате. Шестнадцатеричный MAC-адрес широковещательной рассылки выглядит как **FF:FF:FF:FF:FF:FF**. Каждое F соответствует четырем другим знакам двоичного адреса

Широковещательная рассылка сообщений



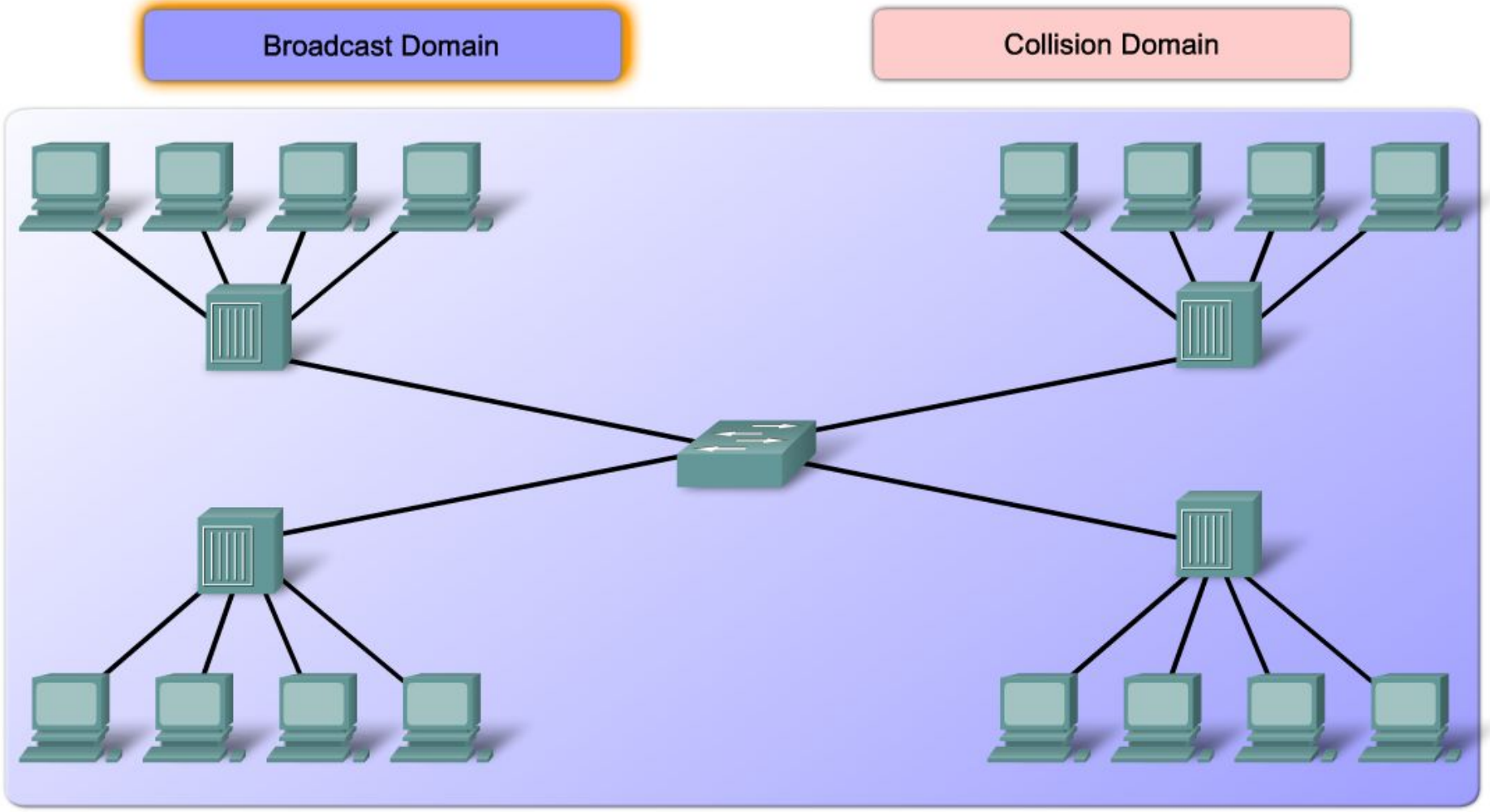
Домен широковещательной рассылки



рассылки, на несколько сетей.

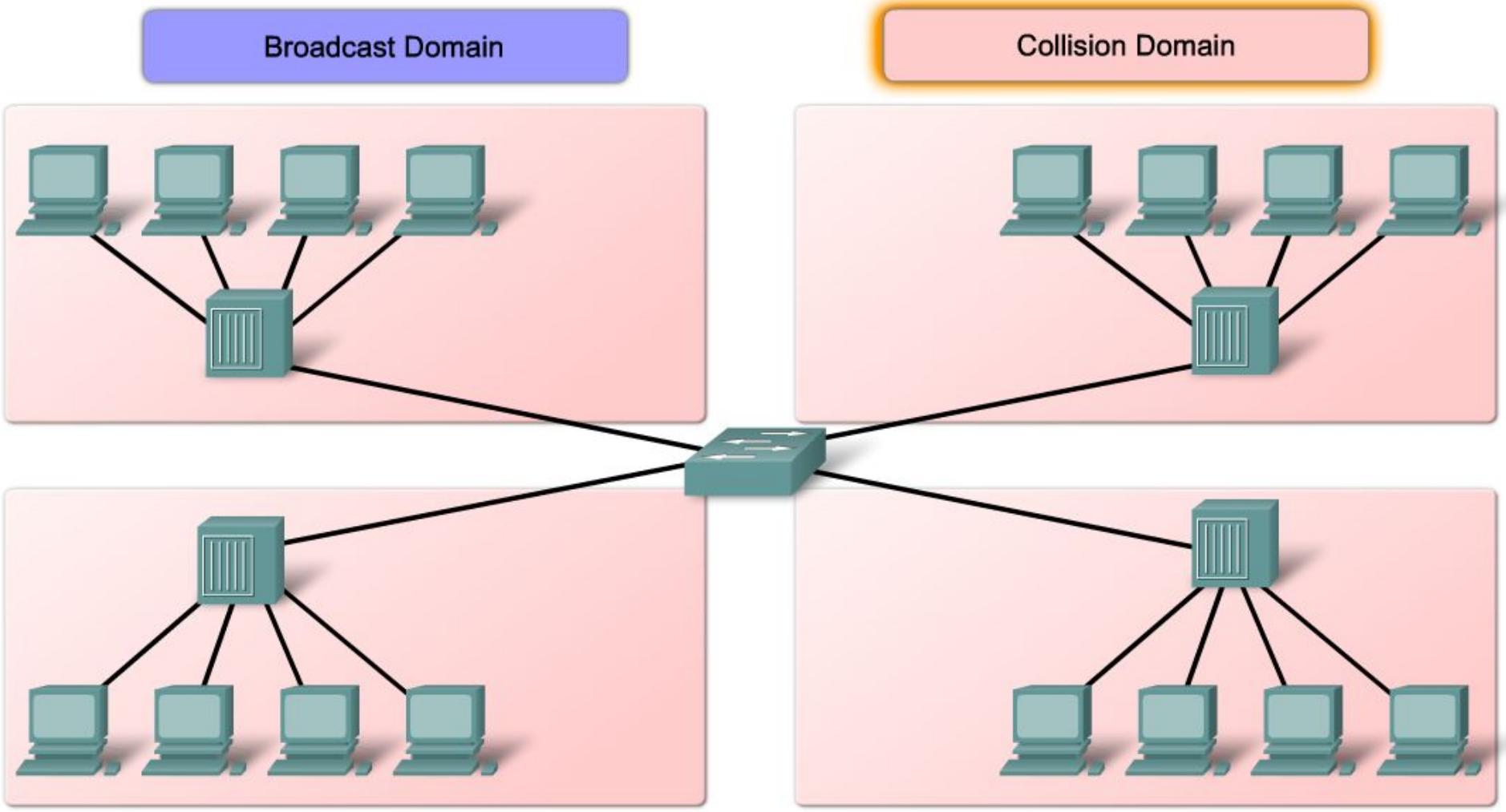
Широковещательный домен

Домен коллизий



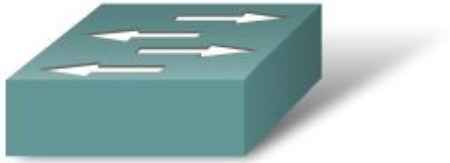
Широковещательный домен

Домен коллизий



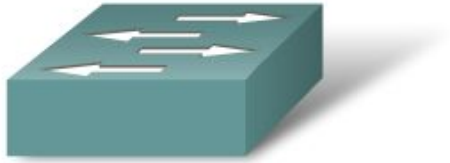
Способы пересылки коммутаторами пакетов в сети

С промежуточным хранением



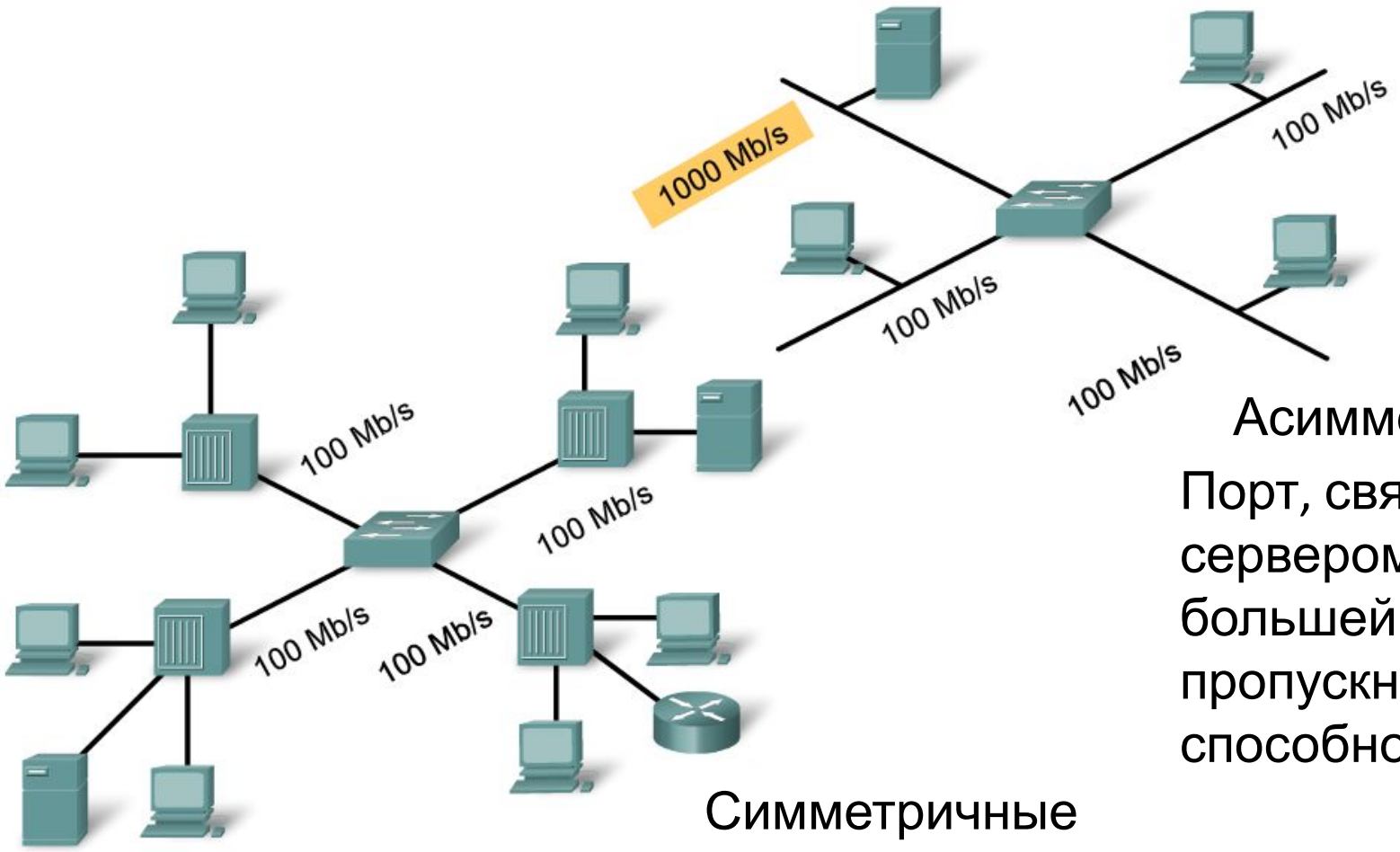
Коммутатор с промежуточным хранением получает пакет, вычисляет контрольную сумму и проверяет длину. Если в контрольной сумме и длине пакета нет ошибок, коммутатор смотрит на адрес назначения, который определяет исходящий интерфейс, после чего пакет отправляется через нужный порт

Сквозной



Сквозной коммутатор отправляет пакет до того, как он будет полностью получен. Как минимум, должен быть прочитан адрес получателя, прежде чем пакет будет отправлен

Симметричные и асимметричные коммутаторы



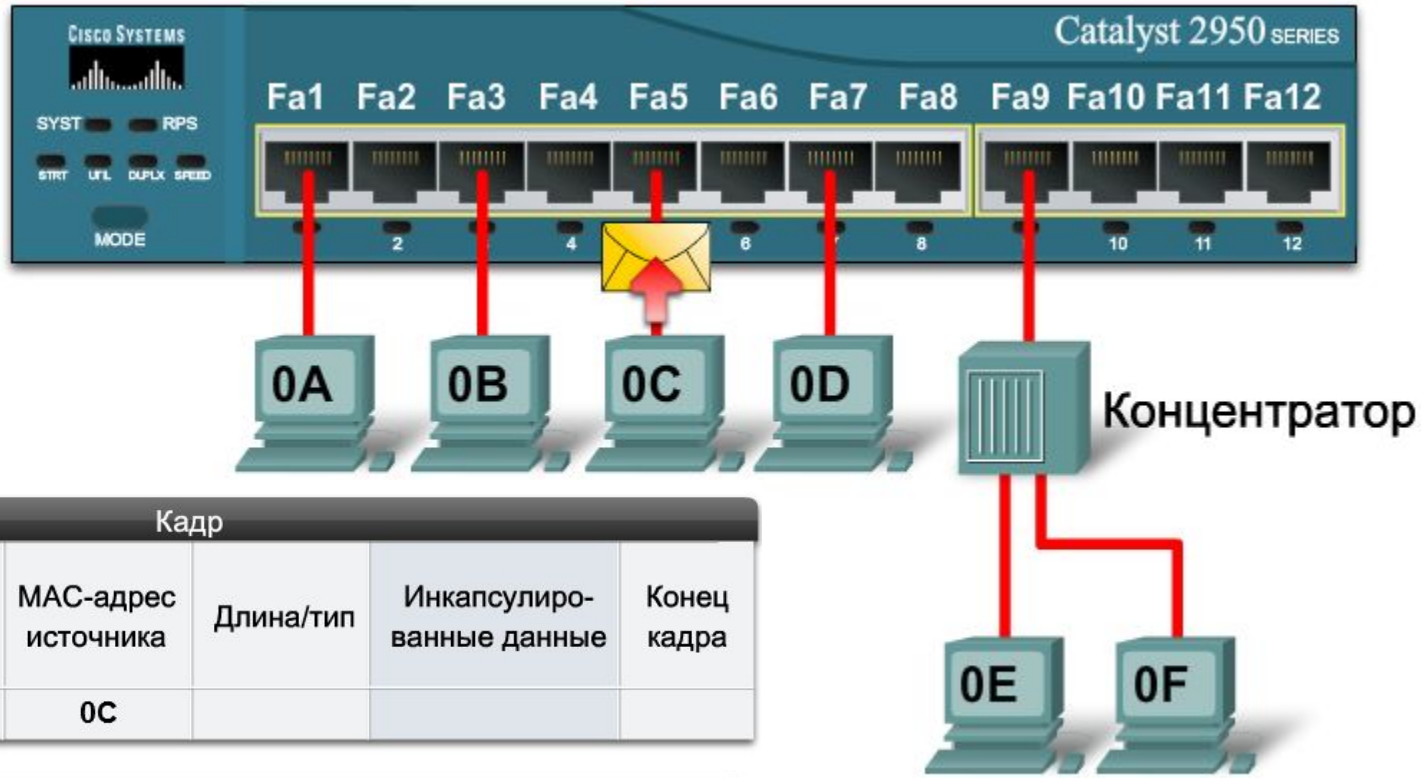
Асимметричные

Порт, связанный с сервером, обладает большей пропускной способностью

Симметричные

Все порты обладают одинаковой пропускной способностью

Проверка понимания

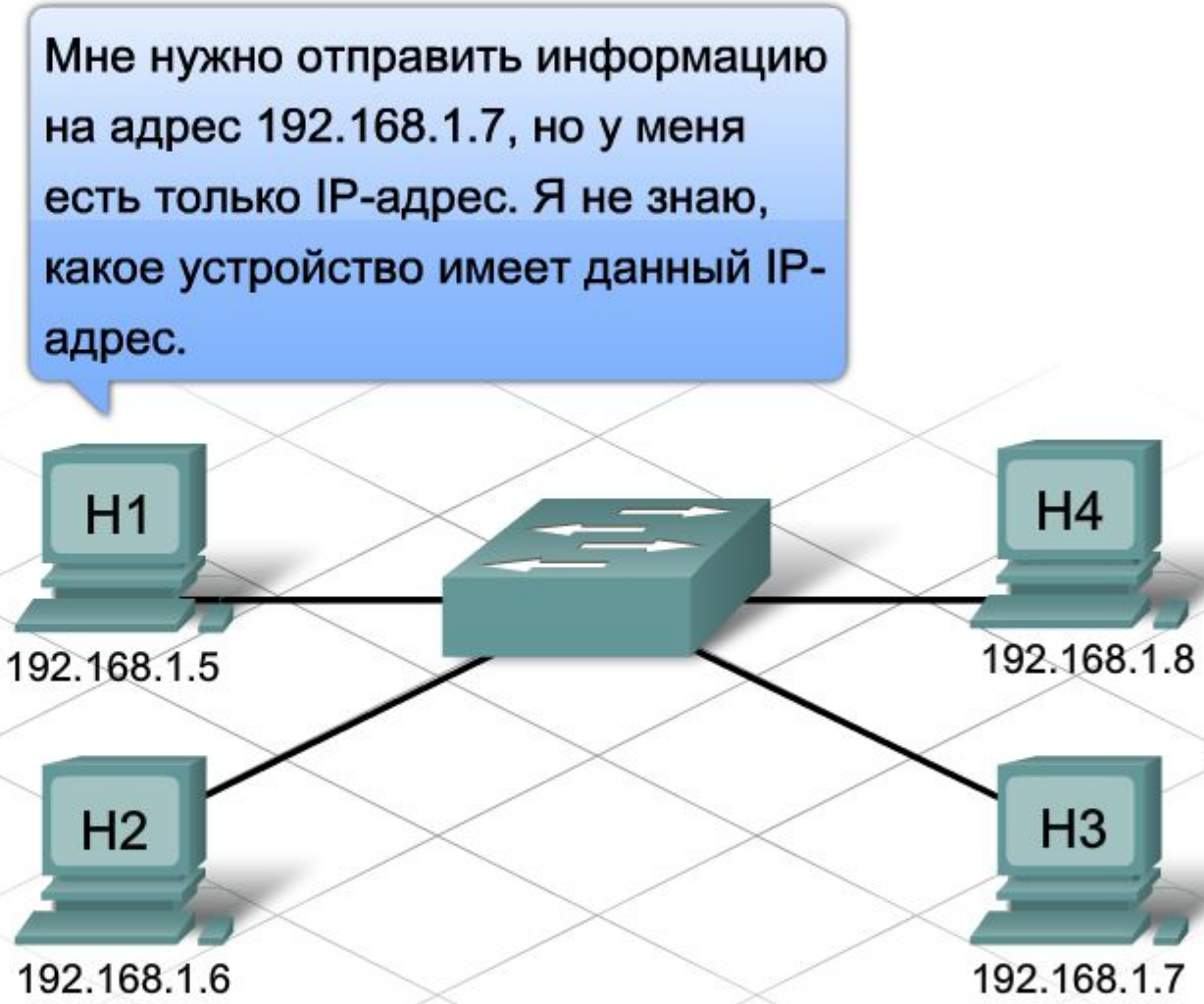


Кадр					
Преамбула	MAC-адрес назначения	MAC-адрес источника	Длина/тип	Инкапсулиро-ванные данные	Конец кадра
	0D	0C			

Таблица MAC-адресов					
Fa1	Fa2	Fa3	Fa4	Fa5	Fa6
				0C	
Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
		0F			

Куда и как коммутатор перешлет кадр?

Протокол ARP (Address Resolution Protocol)



Протокол ARP (Address Resolution Protocol)

При наличии IP-адреса узла ARP определяет и сохраняет MAC-адрес узла в локальной сети в три этапа.

1. Отправляющий узел создает и отправляет кадр по MAC-адресу широковещательной рассылки. В кадре находится сообщение с IP-адресом узла назначения.
2. Каждый сетевой узел получает этот кадр и сравнивает IP-адрес из сообщения со своим. Узел с соответствующим IP-адресом посылает отправителю свой MAC-адрес.
3. Узел-отправитель получает сообщение и сохраняет MAC-адрес и IP-адрес в таблице ARP.

Когда MAC-адрес назначения оказывается в таблице ARP отправителя, появляется возможность отправлять кадры напрямую, минуя запрос ARP.

Уровень распределения. Маршрутизаторы

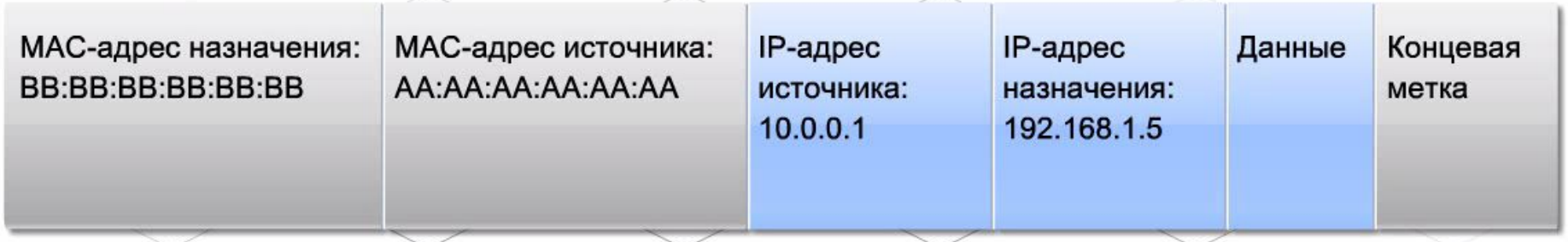
Маршрутизатор (router) - это сетевое устройство, связывающее локальные сети. На уровне распределения маршрутизаторы направляют трафик и выполняют другие важные для эффективной работы сети функции. В отличие от коммутаторов, которые декодируют только кадр с MAC-адресом, маршрутизаторы декодируют пакет, находящийся внутри кадра.

В пакете содержатся IP-адреса источника и назначения и данные пересылаемого сообщения. Маршрутизатор считывает сетевую часть IP-адреса назначения и с ее помощью определяет, по какой из подключенных сетей лучше всего переслать сообщение адресату.

Если сетевая часть IP-адресов источника и назначения не совпадает, для пересылки сообщения необходимо использовать маршрутизатор. Если узел, находящийся в сети 1.1.1.0, должен отправить сообщение узлу в сети 5.5.5.0, оно переправляется маршрутизатору. Он получает сообщение, распаковывает и считывает IP-адрес назначения. Затем он определяет, куда переправить сообщение. Затем маршрутизатор снова

Уровень распределения. Маршрутизаторы

IP-пакет, инкапсулированный в кадре Ethernet



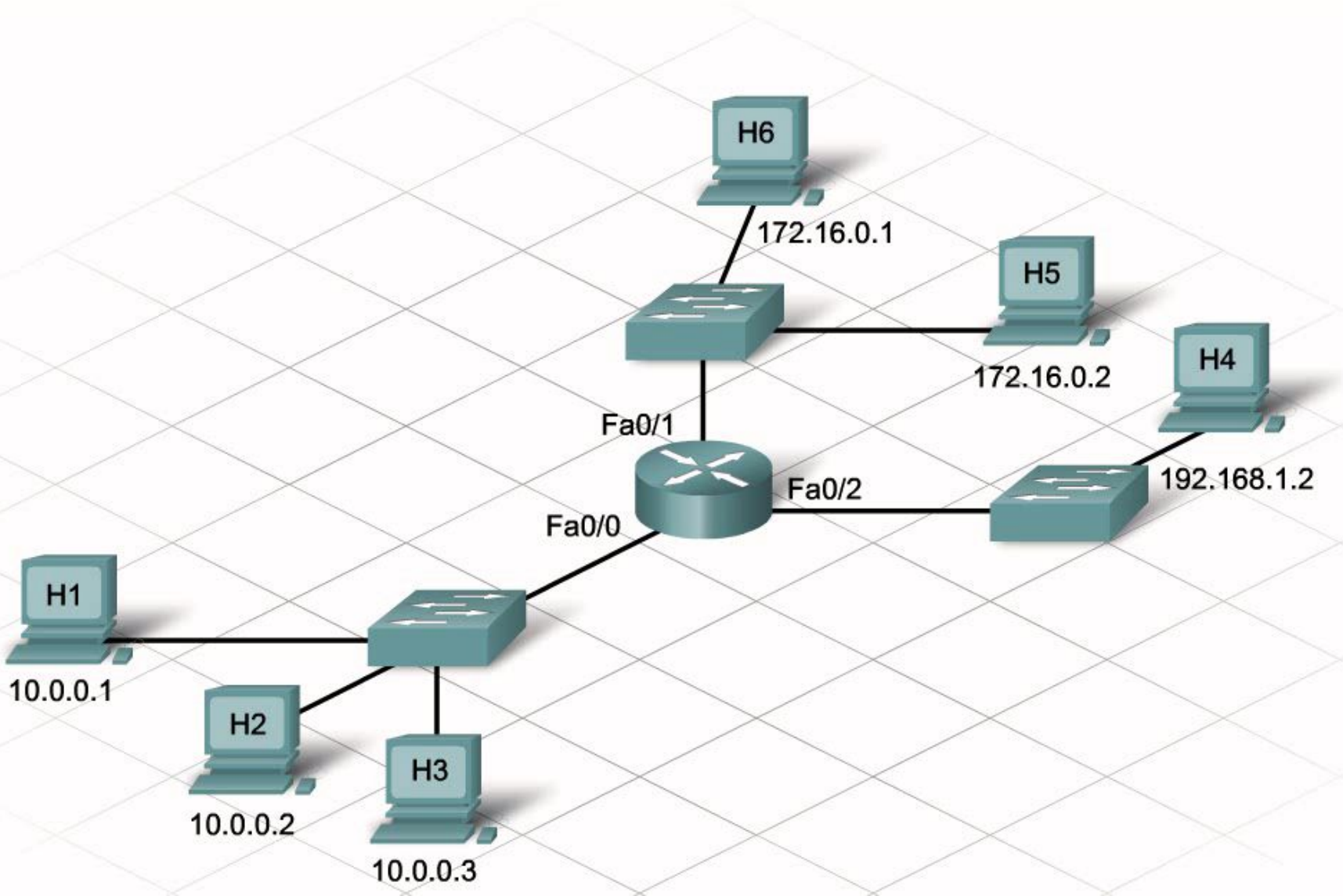
Принципы работы маршрутизатора

Каждый **порт** (**интерфейс**) маршрутизатора связан со своей локальной сетью. У каждого маршрутизатора есть таблица локально подключенных сетей и их интерфейсов. Кроме того, в этих таблицах маршрутизации бывает информация о маршрутах, или путях для подключения к другим локально подключенным удаленным сетям.

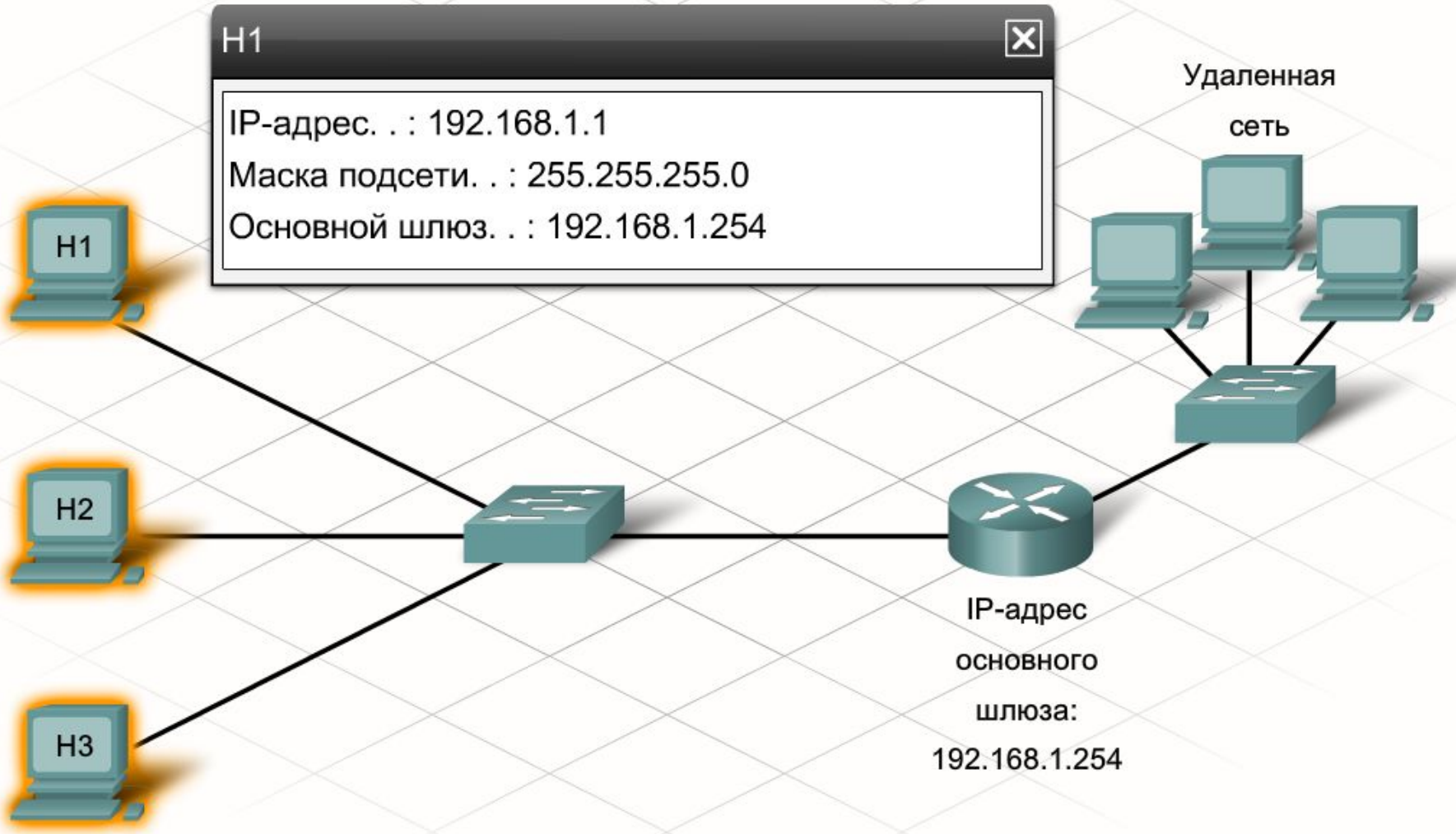
Получив кадр, маршрутизатор декодирует его и получает пакет с IP-адресом назначения. Этот адрес он сравнивает с данными всех сетей из таблицы маршрутизации. Если адрес сети назначения есть в таблице, маршрутизатор инкапсулирует пакет в новый кадр и отправляет. Этот новый кадр направляется в сеть назначения через интерфейс, относящийся к выбранному пути. Процесс перенаправления пакетов в сеть назначения называется маршрутизацией.

Интерфейсы маршрутизатора не пересылают сообщения, направленные на IP-адрес широковещательной рассылки локальной сети. Поэтому рассылки локальной сети не попадают в другие сети через маршрутизатор.

Принципы работы маршрутизатора



Основной шлюз (Default gateway)



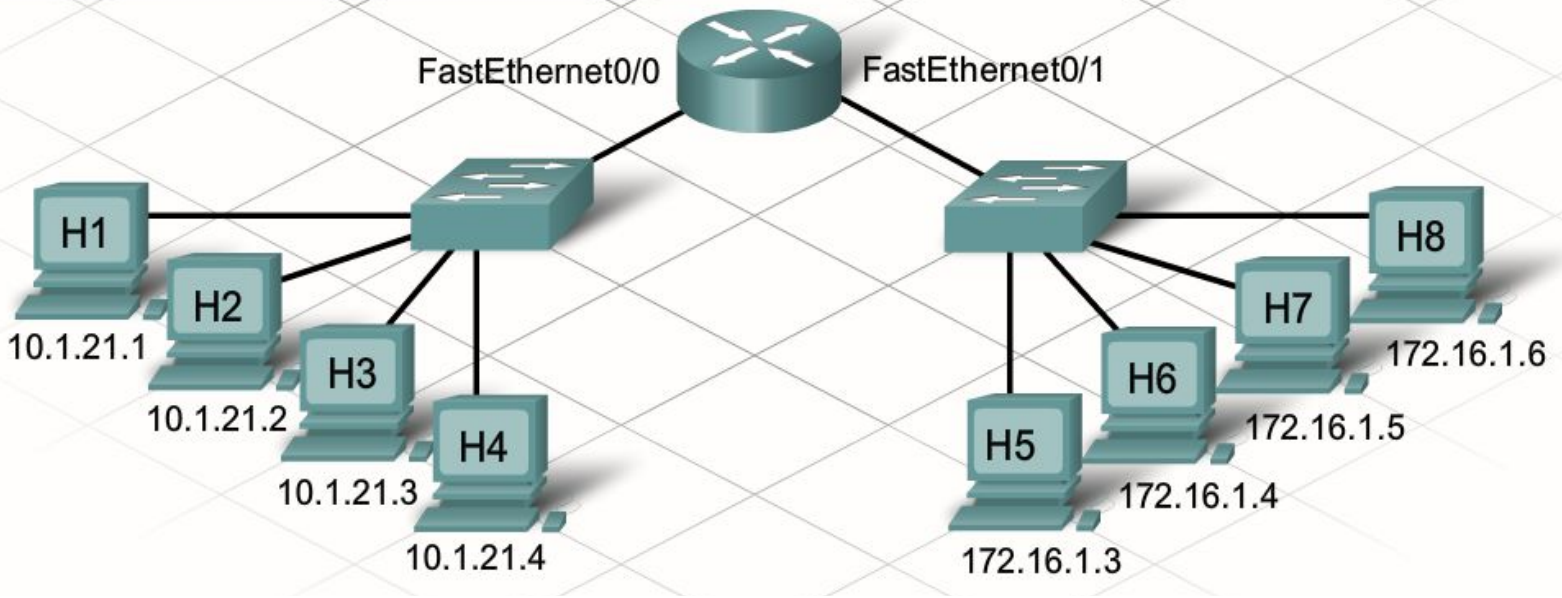
Таблицы в памяти маршрутизаторов

ARP-таблица

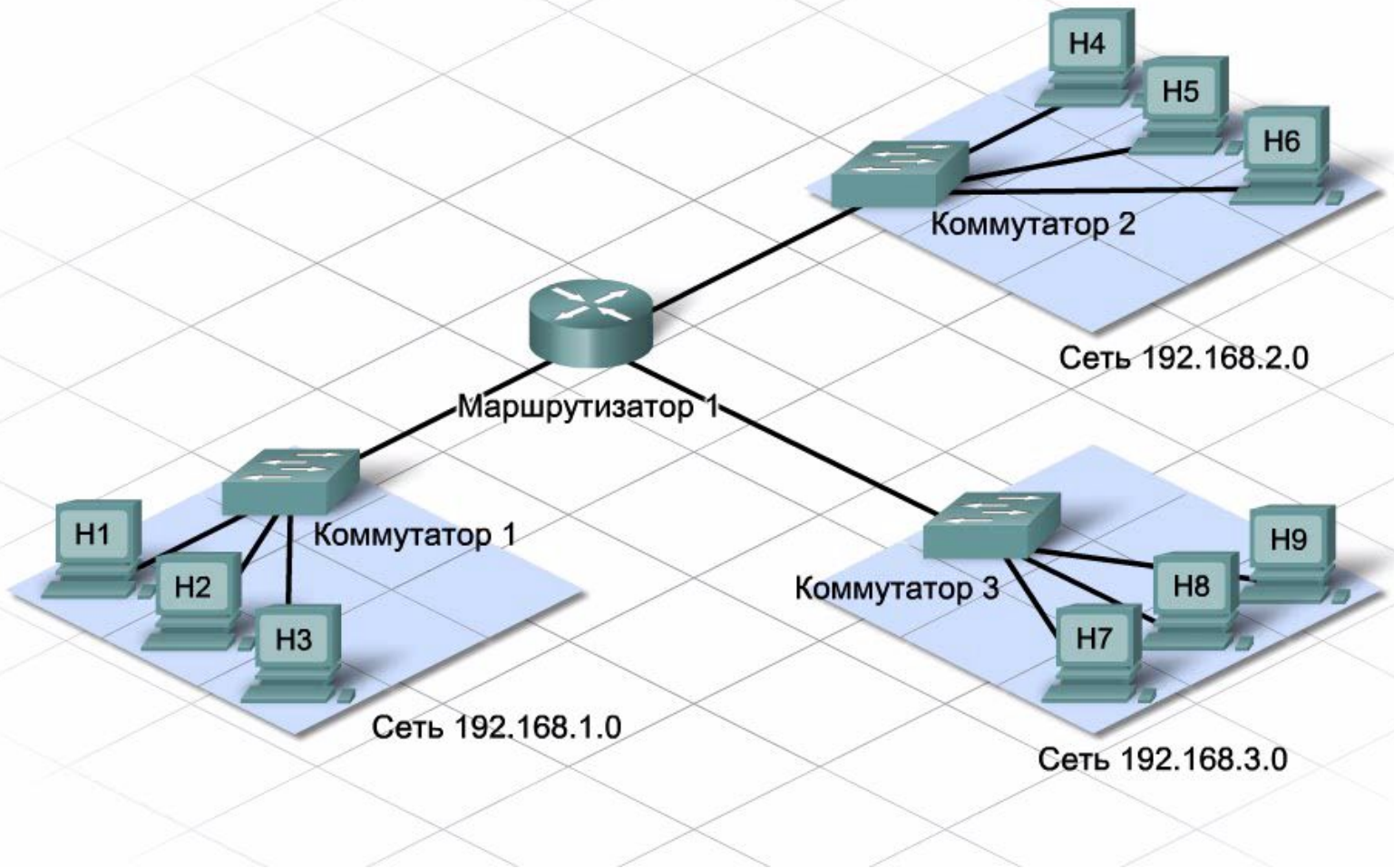
Адрес	Аппаратный адрес	Интерфейс
10.1.21.1	0002.a5ec.c7f9	FastEthernet0/0
10.1.21.2	0012.3fec.fb0d	FastEthernet0/0
10.1.21.3	0014.220e.dac5	FastEthernet0/0
10.1.21.4	00c0.9f4b.8b76	FastEthernet0/0
172.16.1.3	0ac3.a56c.d7f5	FastEthernet0/1
172.16.1.4	0a2f.4fed.dd0d	FastEthernet0/1
172.16.1.5	0b03.3002.ea2d	FastEthernet0/1
172.16.1.6	0d00.a94b.8caa	FastEthernet0/1

Таблица маршрутизации

Тип	Сеть	Порт
C	10.0.0.0/8	FastEthernet0/0
C	172.16.0.0/16	FastEthernet0/1



Межсетевая маршрутизация



Проверка понимания

Таблица маршрутизации

Тип	Сеть	Порт	IP-адрес следующего перехода (hop)	Метрика
C	**192.168.3.0/2**	Ethernet1/1	---	**0/0**
C	**172.16.1.0/24**	Ethernet1/2	---	**0/0**
C	**10.5.5.0/24**	Ethernet1/3	---	**0/0**

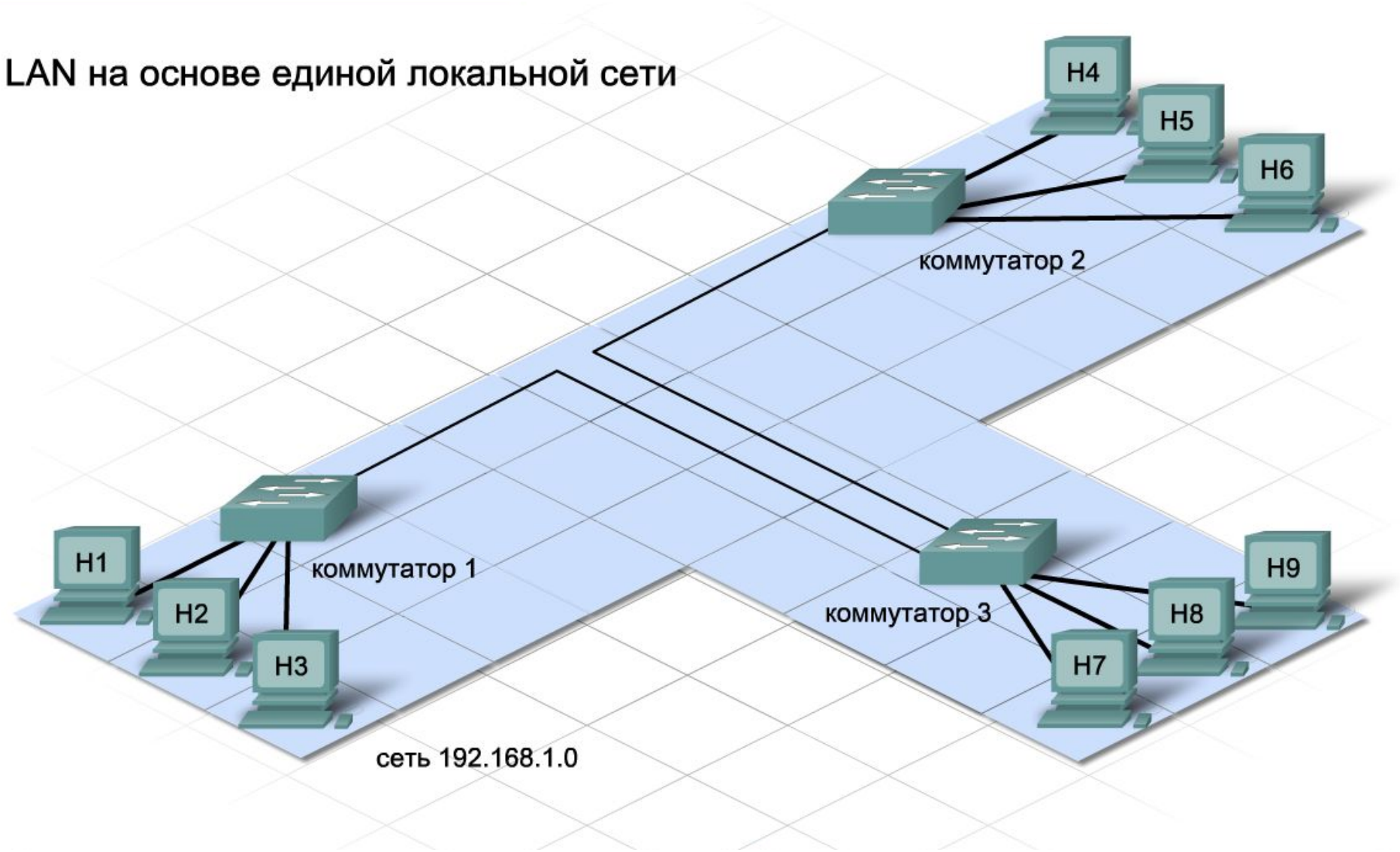
Кадр

	Метка начала	IP-адрес назначения 172.16.1.2	IP-адрес источника 10.5.5.8	Инкапсулированные данные	

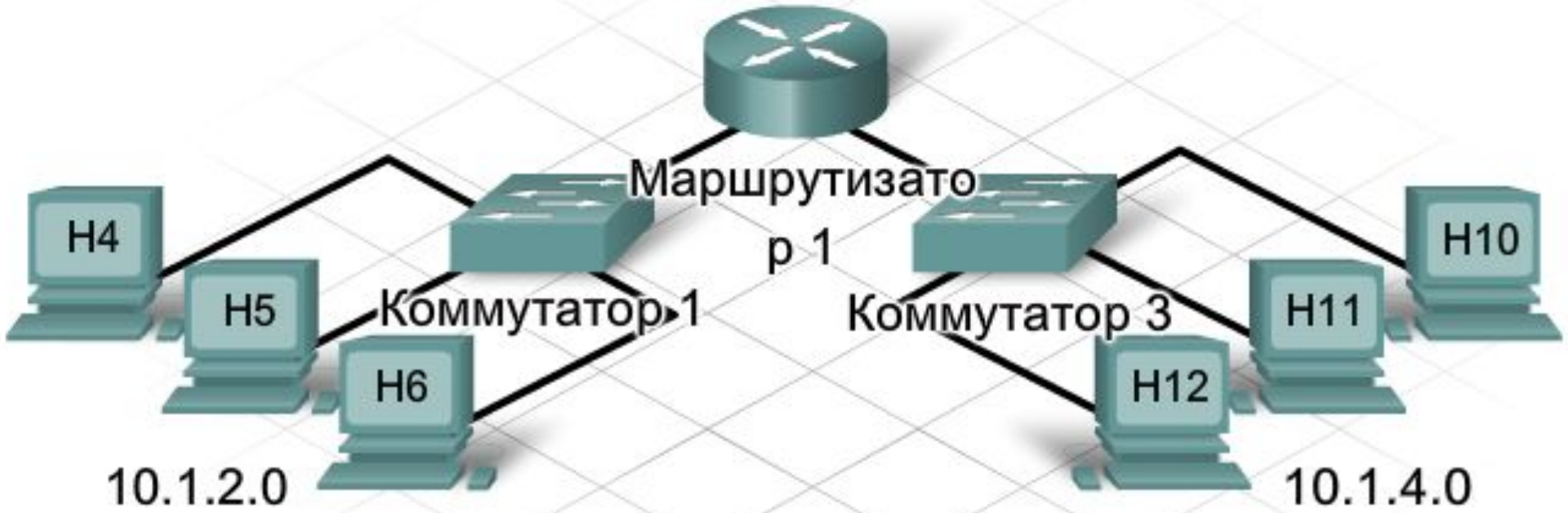
1. Укажите адрес основного шлюза, используемого для пересылки данного пакета маршрутизатору

2. На какой интерфейс маршрутизатор перешлет пакет после его получения?

Уровень распределения. Сегментация

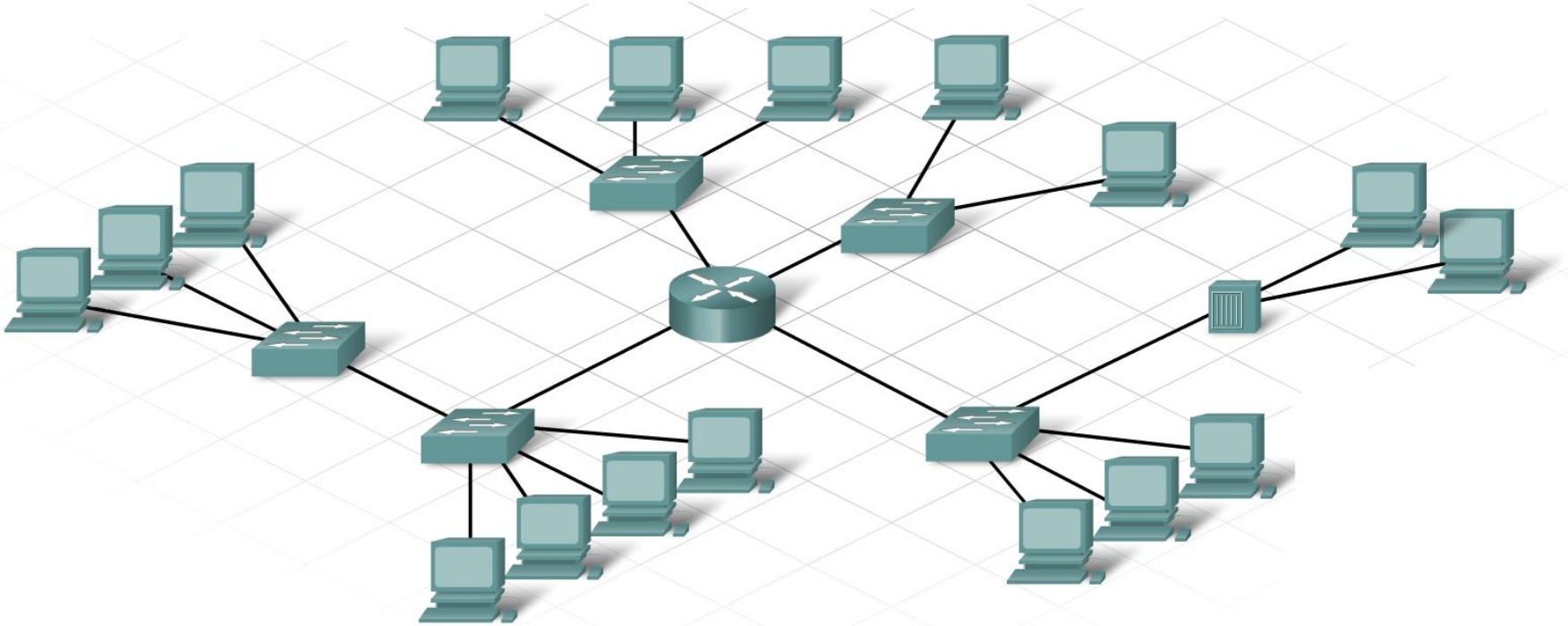


Преимущества и недостатки сегментации



усложняют конфигурацию сети и в некоторых случаях создают

Проверка понимания



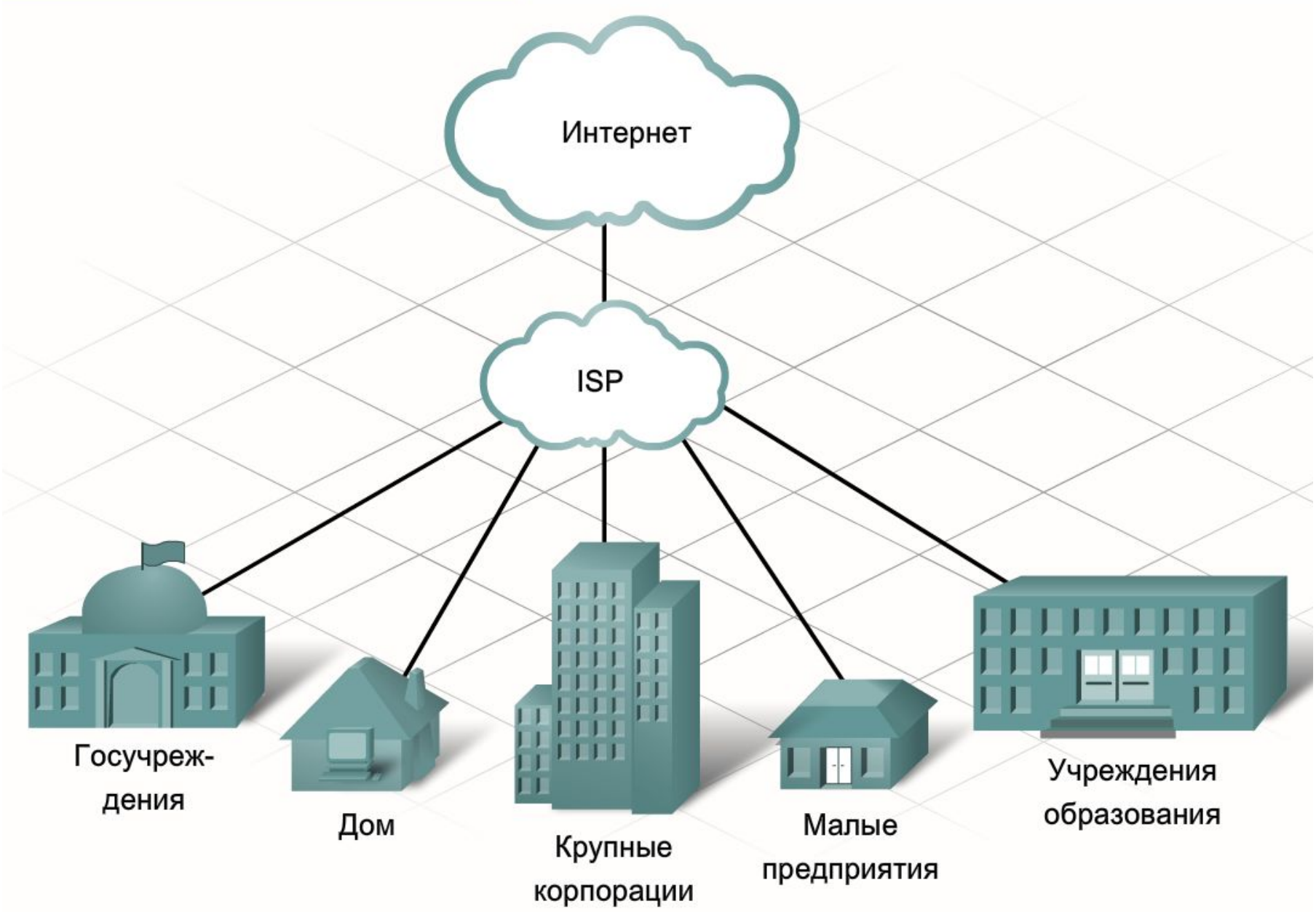
Сколько локальных сетей вы здесь видите?

- III -

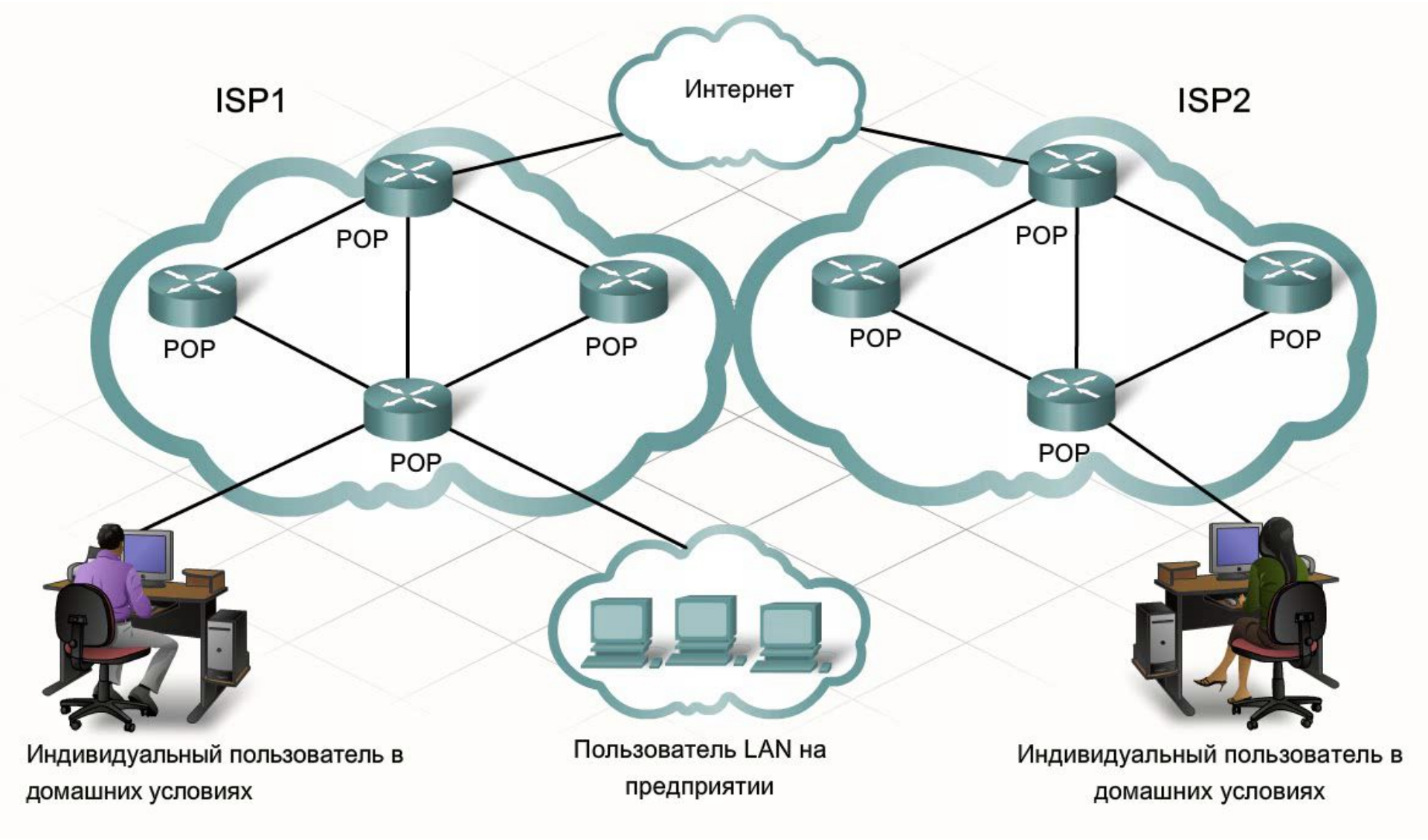
WAN-подключения

Кабели – среда передачи

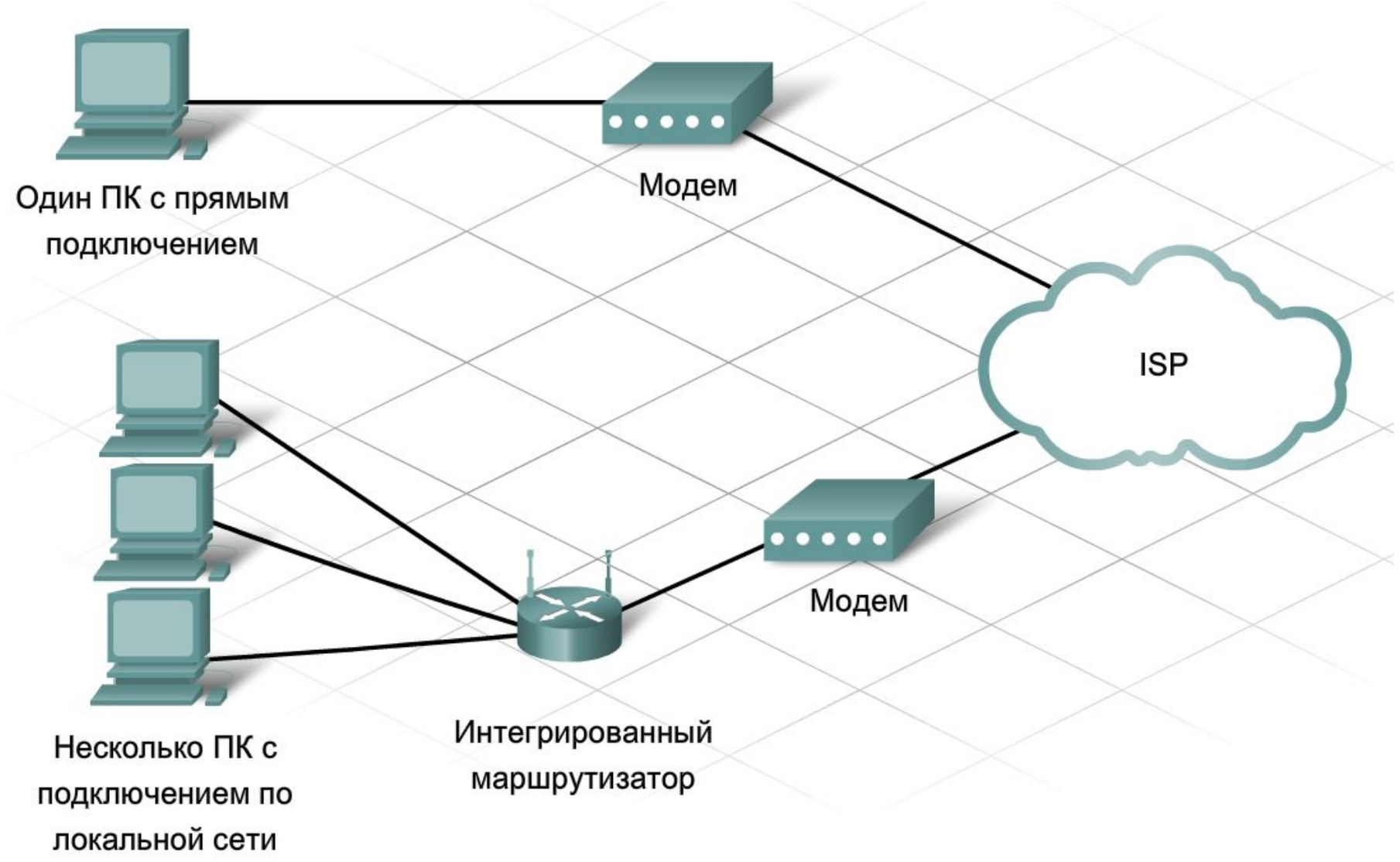
Провайдеры услуг сети Интернет



Взаимосвязь провайдеров услуг Интернет



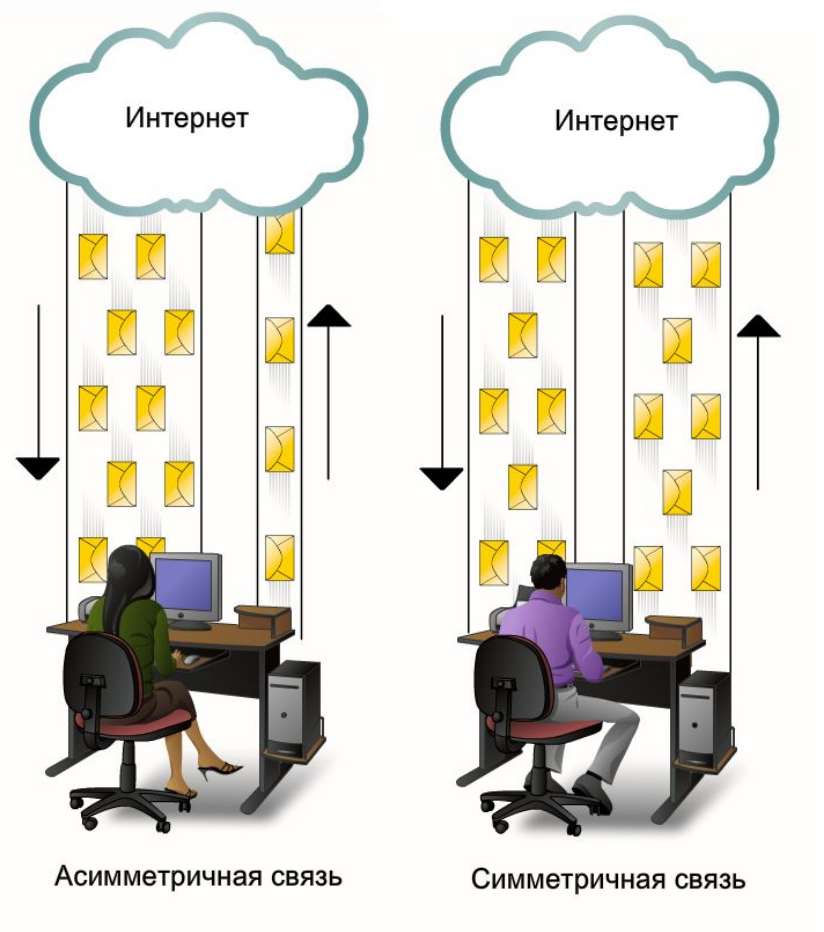
Варианты подключения к ISP



Уровни обслуживания ISP

Уровни обслуживания ISP

При передаче данные либо выгружаются в Интернет (**upload**), либо загружаются из Интернета (**download**). Если скорость загрузки отличается от скорости выгрузки, связь называется **асимметричной**. Если скорость одинаковая в обоих случаях, она называется **симметричной**.

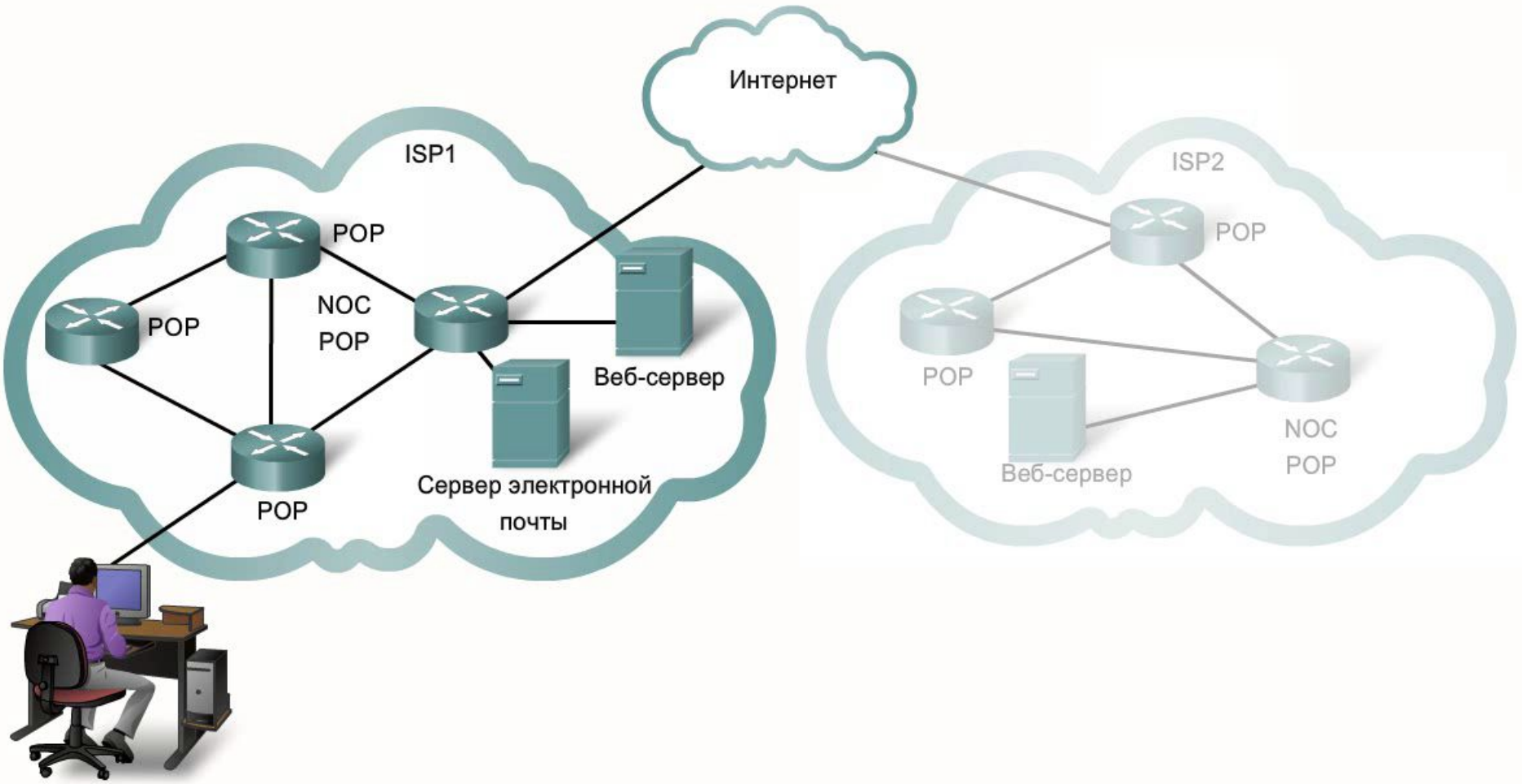


Уровни обслуживания ISP

В Интернете используются только уникальные IP-адреса. Существуют организации, которые контролируют распределение IP-адресов и не допускают дублирования. Поставщики услуг Интернета получают блоки IP-адресов от локального, национального или **регионального интернет-регистратора** (**RIR, Region Internet Registrator**). Поставщик услуг Интернета распоряжается этими адресами и предоставляет их конечным пользователям.

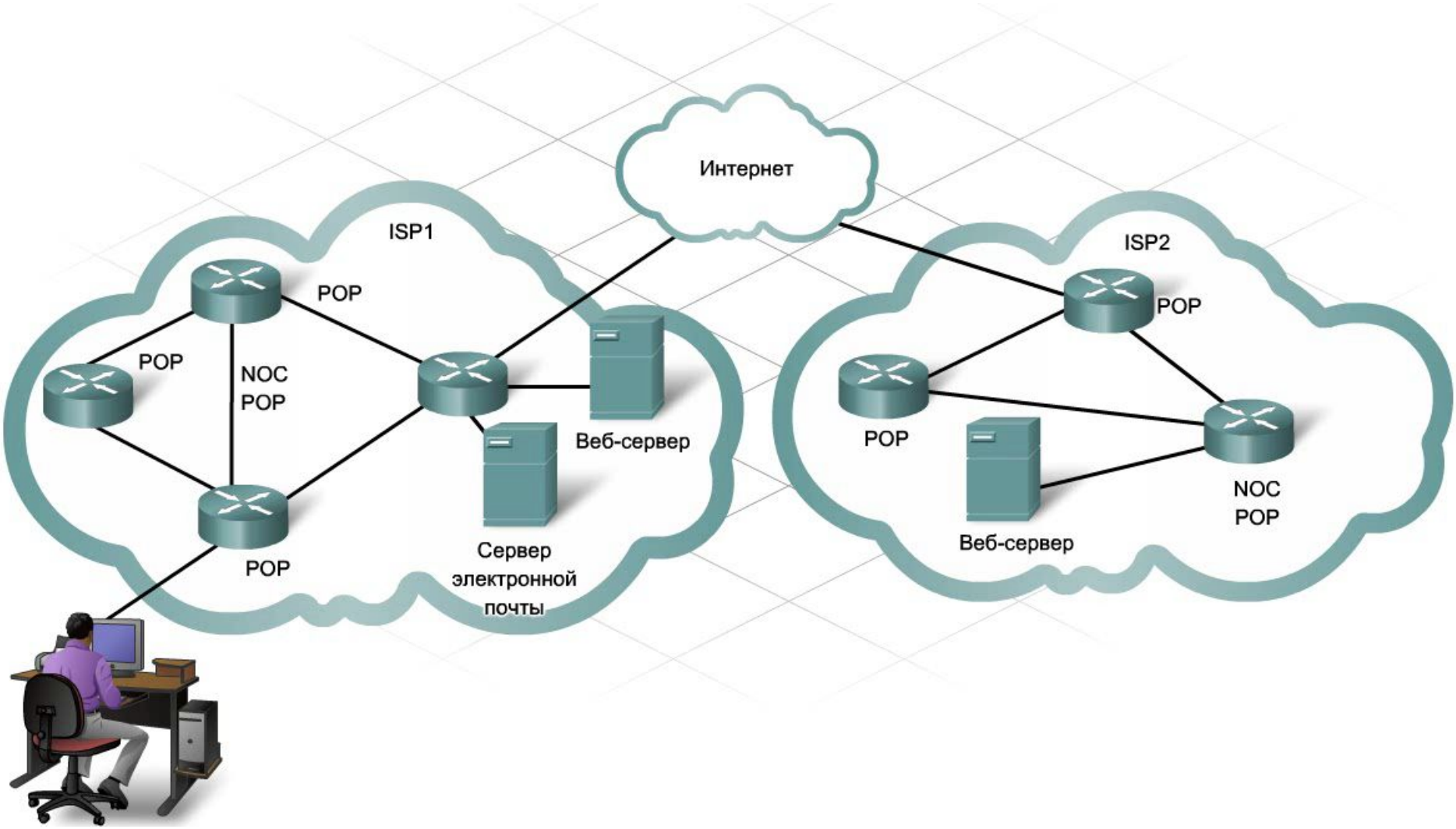
IP-конфигурацию домашних и корпоративных компьютеров определяют поставщики услуг Интернета. Обычно это происходит автоматически, когда пользователь подключается к поставщику услуг Интернета и получает доступ в Интернет.

Обработка пакетов оборудованием ISP

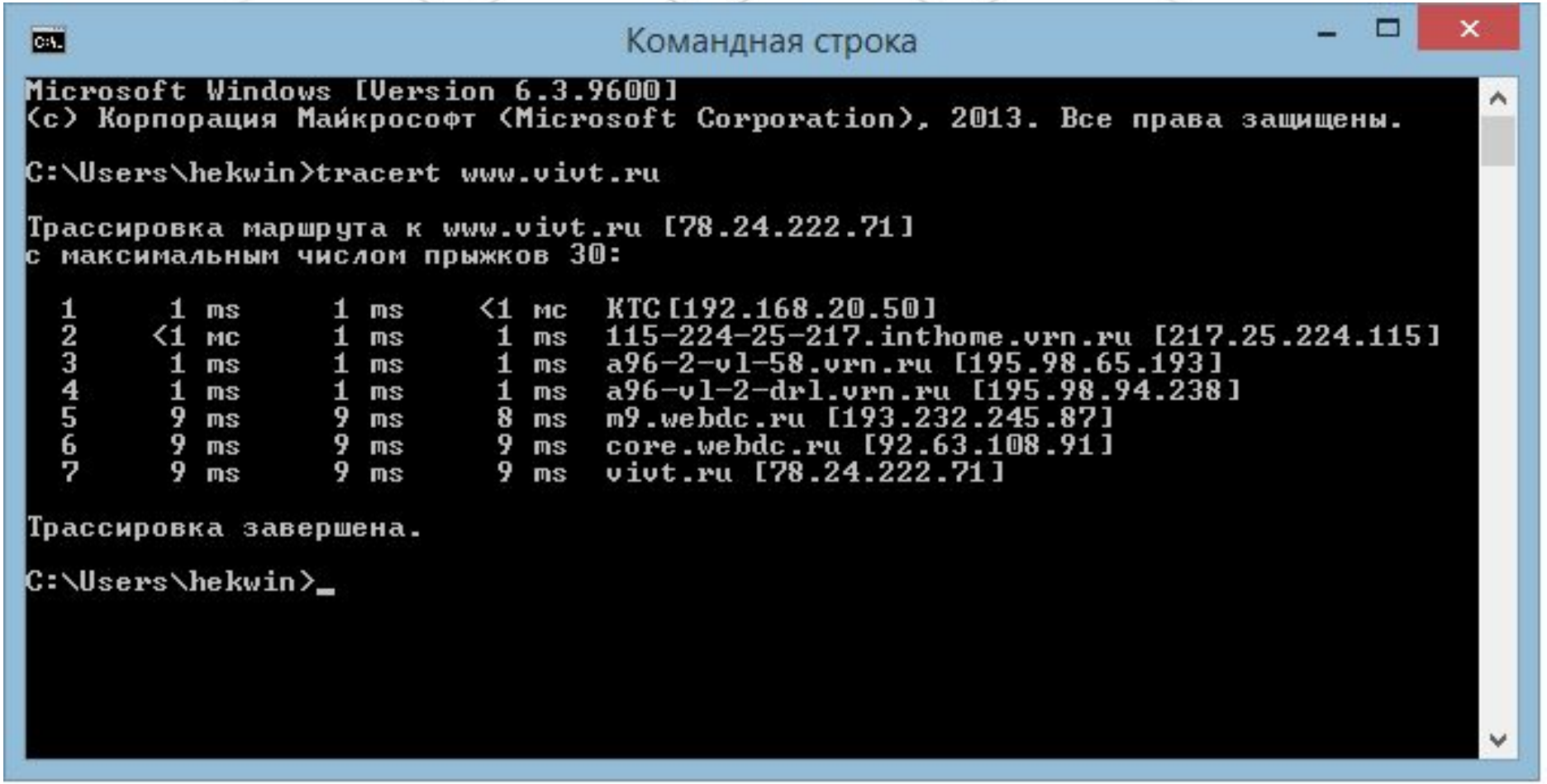


Интернета.

Обработка пакетов оборудованием ISP

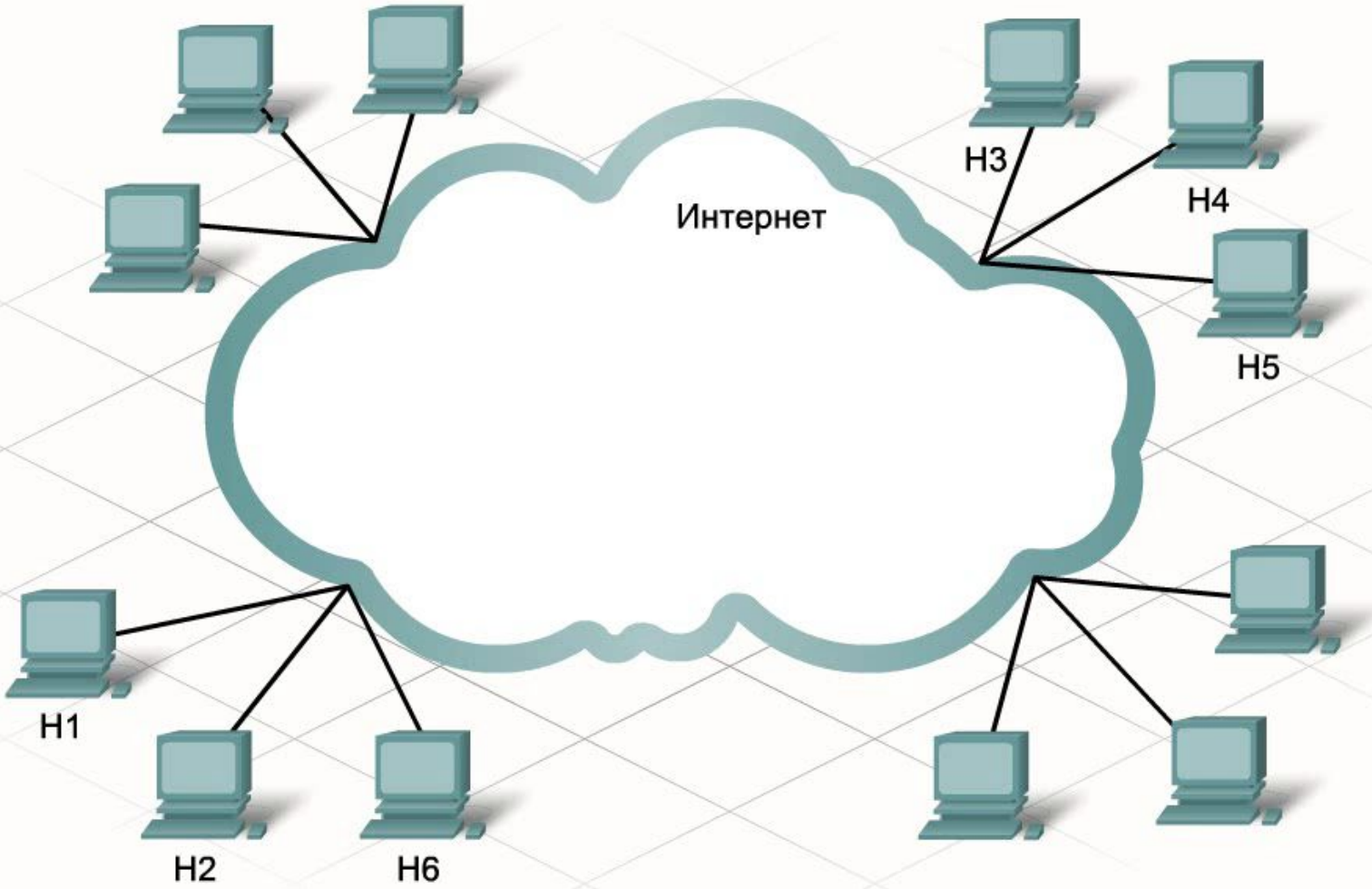


Передача пакетов в Интернет



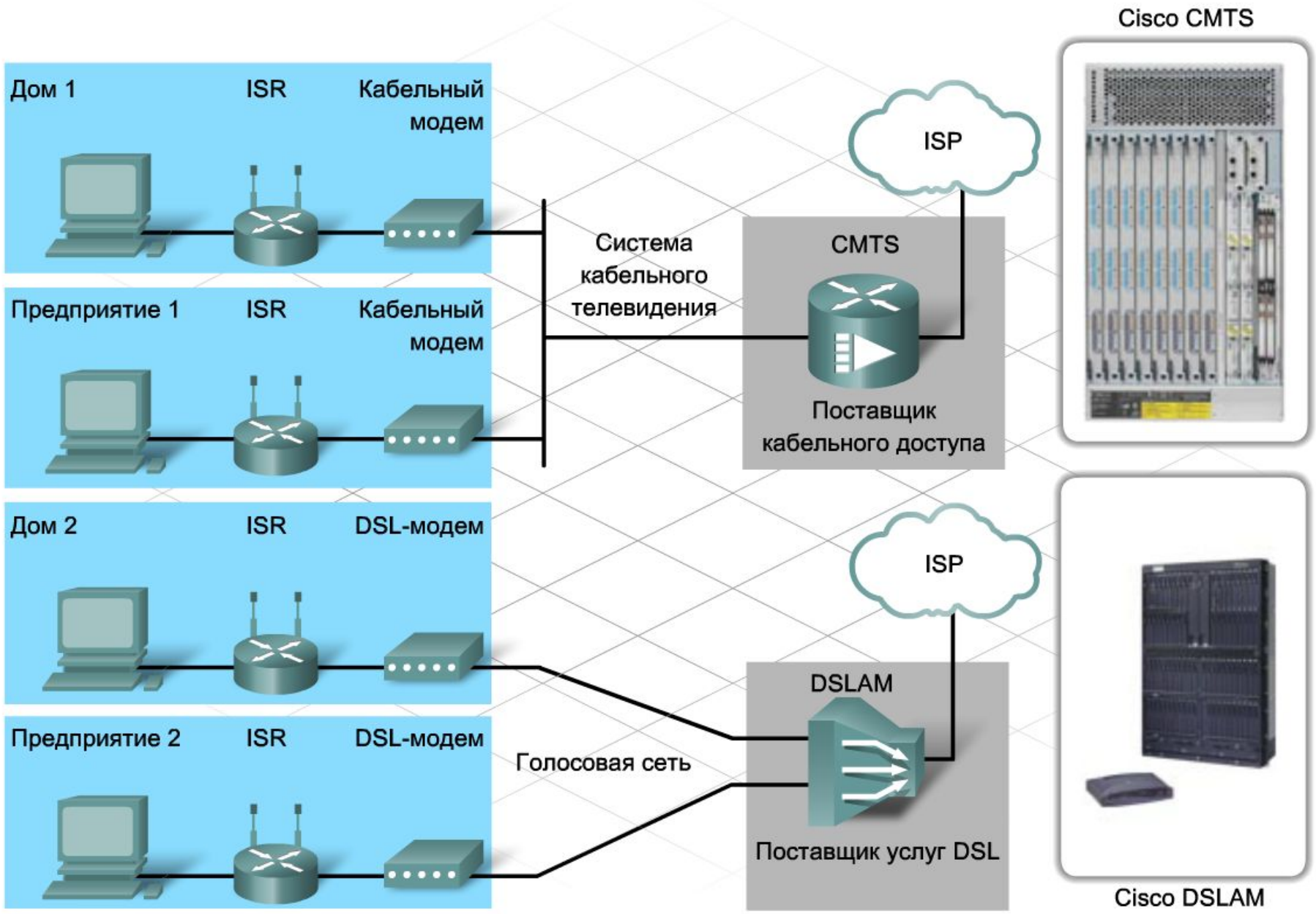
2. PARIS (209.165.202.129) 8 msec 8 msec 8 msec
3. ROME (209.165.200.225) 8 msec 8 msec 4 msec

Интернет – как облако



между ними находится много взаимосвязанных устройств.

Устройства в Интернет-облаке



Физическая среда подключения

Витая пара (Twisted Pair, TP)
В современной технологии Ethernet для подключения устройств чаще всего используется тип кабеля с медными проводниками, который называется витой парой. Поскольку Ethernet является основой большинства локальных сетей, витая пара - наиболее распространенный тип сетевого кабеля.

Коаксиальный кабель (Coaxial cable)
Обычно коаксиальные кабели изготавливают из меди или алюминия. Они применяются в кабельном телевидении. Кроме того, таким кабелем соединяются различные компоненты систем спутниковой связи.

Оптоволоконный кабель (Fiber optic cable)
Оптоволоконные кабели изготавливаются из стекла или пластика. У них очень высокая пропускная способность, позволяющая передавать большие объемы данных. Оптоволоконные кабели используются в магистральных сетях, на крупных предприятиях и больших информационных центрах. Кроме того, их активно применяют телефонные компании

Витая пара

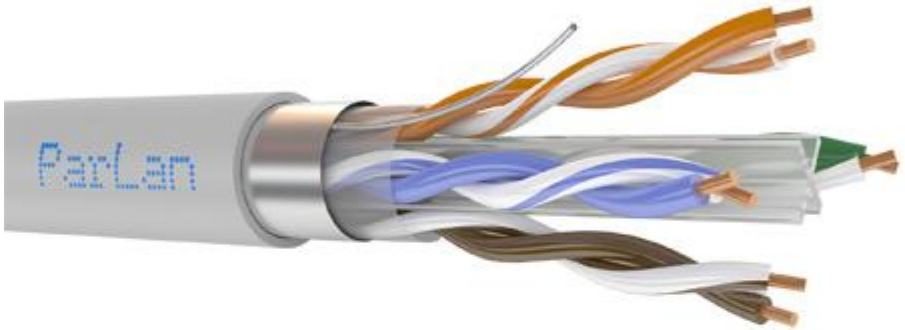
на каждые 2,5 см, поэтому их устойчивость выше.

Витая пара

Категория	Полоса частот, МГц	Обозначение	Применение
CAT3	16	10BASE-T, 100BASE-T4 Ethernet	4-парный кабель, используется при построении телефонных и локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных до 10 Мбит/с или 100 Мбит/с по технологии100BASE-T4 на расстоянии не дальше 100 метров.
CAT5	100	100BASE-TX Ethernet (LAN, ATM,CDDI)	4-парный кабель, использовался при построении локальных сетей 100BASE-TX и для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар.
CAT5e	125	1000Base-T	4-парный кабель, усовершенствованная категория 5 (уточненные/улучшенные спецификации). Скорость передач данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар. Кабель категории 5e является самым распространённым и используется для построения компьютерных сетей. Иногда встречается двухпарный кабель категории 5e. Преимущества данного кабеля в более низкой себестоимости и меньшей толщине.

Витая пара

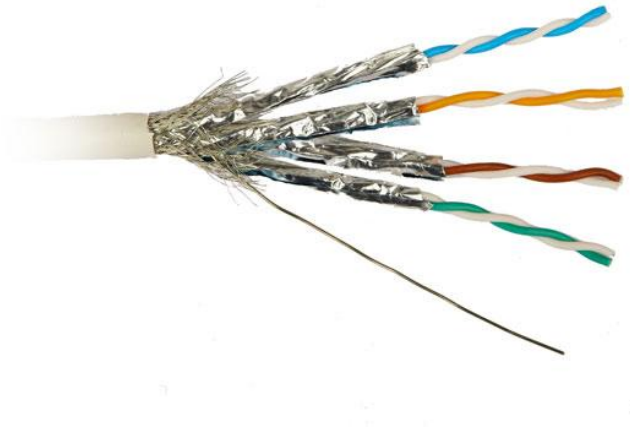
Категория	Полоса частот, МГц	Обозначение	Применение
CAT6	250	Fast Ethernet, Gigabit Ethernet (10GBASE-T Ethernet)	применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 55 м.
CAT6a	500	Gigabit Ethernet (10GBASE-T Ethernet)	применяется в сетях Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 100 метров.

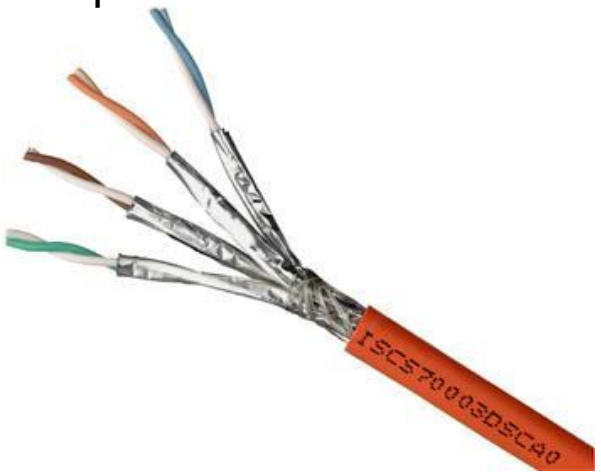


Витая пара

Категория	Полоса частот, МГц	Обозначение	Применение
CAT7	600	Gigabit Ethernet (10GBASE-T Ethernet)	спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, скорость передачи данных до 10 Гбит/с. Кабель этой категории имеет общий экран и экраны вокруг каждой пары. Седьмая категория, строго говоря, не UTP, а S/FTP (Screened Fully Shielded Twisted Pair).
CAT7a	до 1200	Gigabit Ethernet (40GbE, 100GbE)	разработана для передачи данных на скоростях до 40 Гбит/с на расстояние до 50 м и до 100 Гбит/с на расстояние до 15 м.

*Иногда F расшифровывают как Foiled - фольгированная





Коаксиальный кабель

Как и витая пара, коаксиальный кабель передает данные в виде электрических сигналов. Экранирование у него лучше, чем у UTP, отношение сигнала к шуму ниже и данных передается больше. Такими кабелями часто подключают телевизоры к источнику сигнала (телевизионный выход, спутниковое телевидение или обычная антенна). Кроме того, они используются в NOC, для подключения оконечной системы линии кабельного модема (CMTS) и некоторых высокоскоростных интерфейсов.

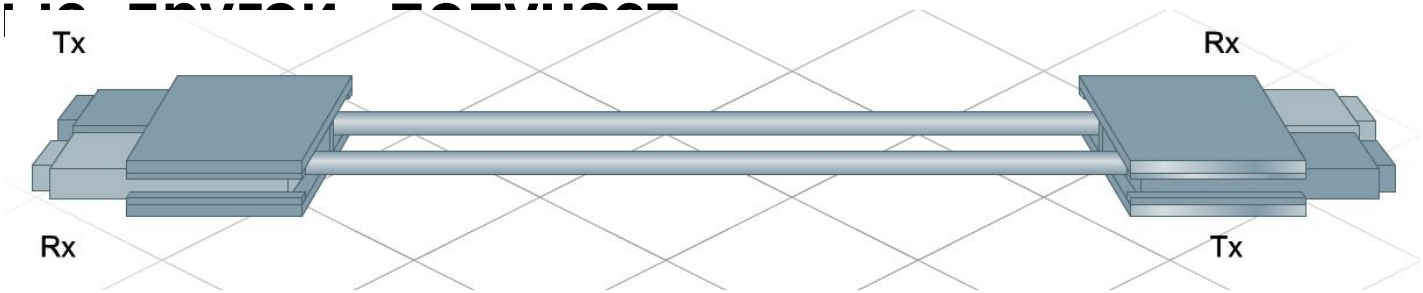
Хотя коаксиальный кабель и улучшает характеристики передачи данных, в локальных сетях вместо него используется витая пара. Отчасти дело в том, что по сравнению с UTP этот кабель сложнее в установке, дороже и хуже поддается ремонту.

Оптоволоконный кабель

В отличие от ВП и коаксиального кабеля, оптоволоконный передает данные в виде импульсов света. Оптоволоконные кабели обычно не используются в домах и на малых предприятиях, но широко распространены в крупных организациях и информационных центрах.

Оптоволоконный кабель изготавливается из стекла или пластика, не проводящего электричество. Соответственно, он устойчив к ЭМП и подходит для мест, где помехи представляют собой серьезную проблему.

В любой оптоволоконной сети фактически присутствует два кабеля. Один из них передает данн



Оптоволоконный кабель

Существует два вида оптоволоконных кабелей: многомодовый и одномодовый.

Многомодовый кабель

Из двух видов оптоволоконных кабелей многомодовый дешевле и шире распространен. Обычно импульсы света подает светодиод, или **светоизлучающий диод (СИД, light-emitting diode, LED)**. Кабель называется **многомодовым**, поскольку по нему одновременно проходит несколько лучей света, передающих данные. Каждый луч проходит через сердечник кабеля по своему пути. Обычно многомодовые кабели используются в кабелепроводах длиной до 2000 метров. По мере совершенствования технологий это расстояние постоянно увеличивается.

Оптоволоконный кабель

Существует два вида оптоволоконных кабелей: многомодовый и одномодовый.

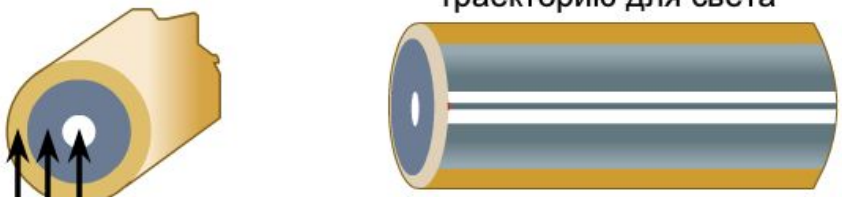
Одномодовый кабель

Конструкция одномодового оптоволоконного кабеля такова, что луч проходит через волокно **только одним путем**. Источником света для таких кабелей является светодиодный **лазер**, который значительно дороже обычных СИД. Благодаря интенсивности лазера достигается большая скорость и дальность передачи данных. Одномодовые кабели передают данные примерно на 3000 метров. Они используются в магистральных кабелепроводах, в том числе для соединения различных NOC. По мере совершенствования технологий это расстояние также постоянно увеличивается.

Оптоволоконный кабель

Одномодовый кабель

Создает прямую траекторию для света



Стеклянный сердечник = 9 микрон

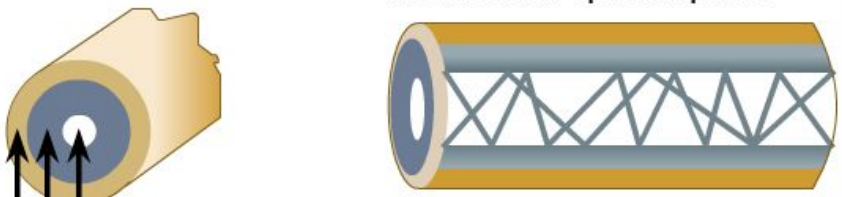
Плакировка стекла, 125 микрон в диаметре

Полимерное покрытие

- Небольшой сердечник
- Низкий уровень рассеивания
- Предназначен для больших расстояний
- Источники света - лазеры
- Широко используется в магистральных соединениях комплекса зданий (длина - несколько тысяч метров)

Многомодовый кабель

Позволяет свету проходить по нескольким траекториям



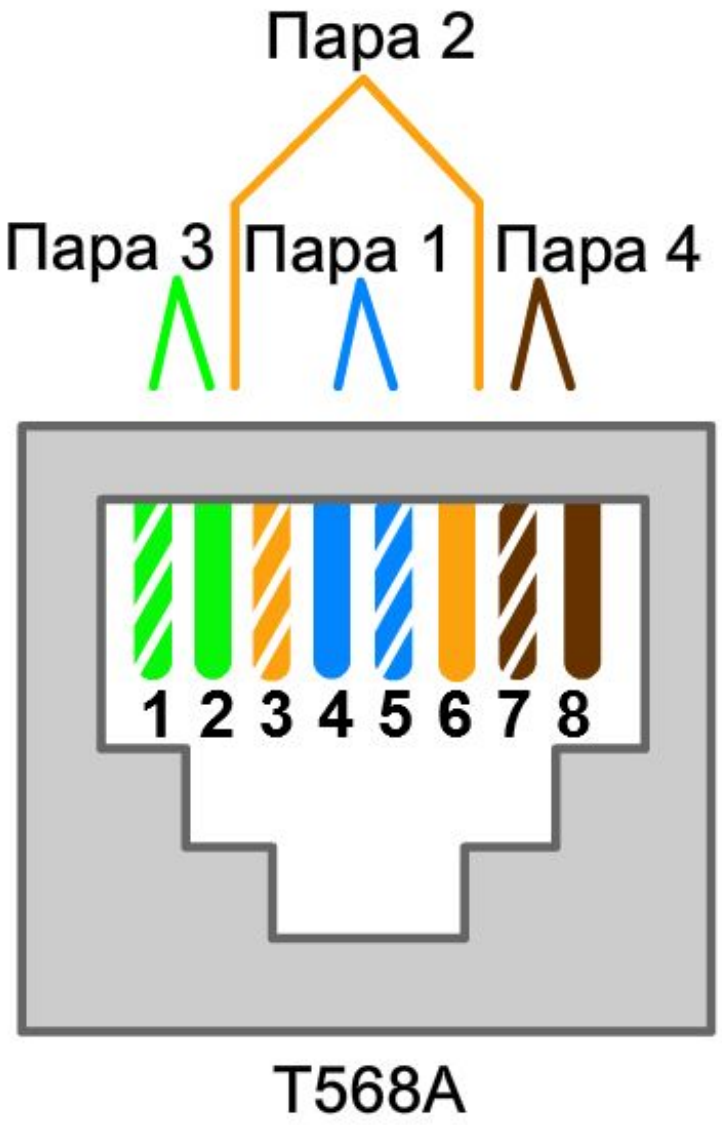
Стеклянный сердечник = 50/62,5 микрон

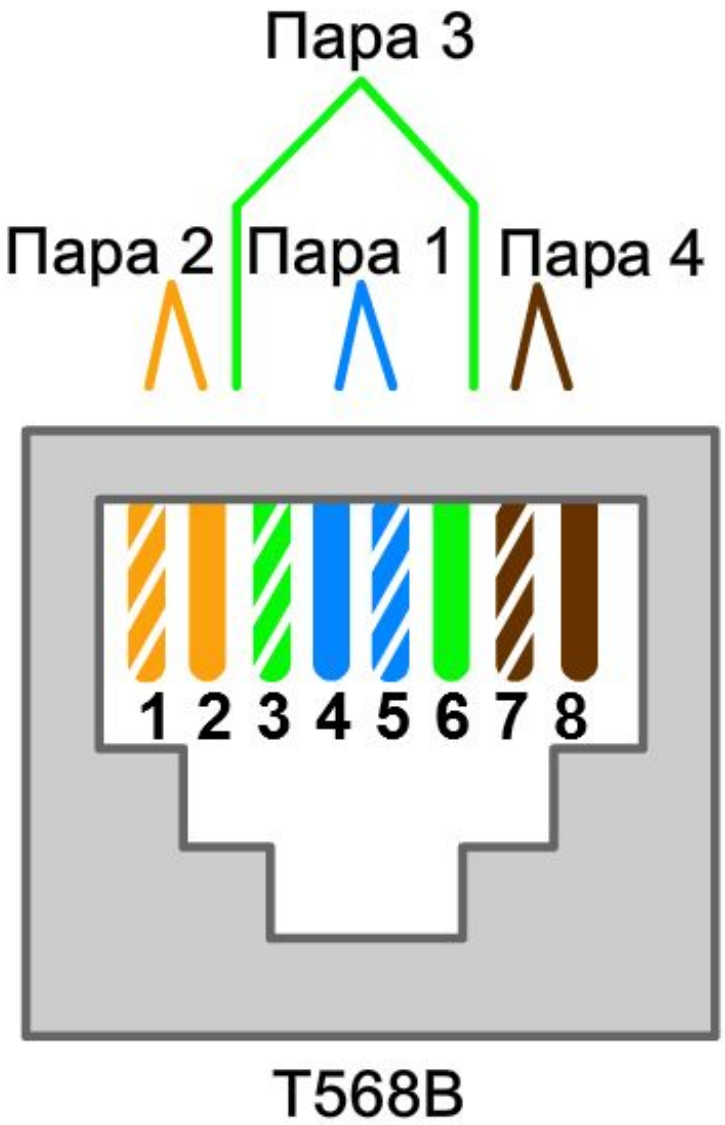
Плакировка стекла, 125 микрон в диаметре

Покрытие

- Сердечник больше, чем у одномодовых кабелей
- Более высокий коэффициент рассеивания (и значит, возможна потеря сигнала)
- Предназначен для больших (но меньших, чем для одномодового) расстояний
- Источники света - СИД
- Широко используется в сетях LAN или сетях комплекса зданий (длина - несколько сотен метров)

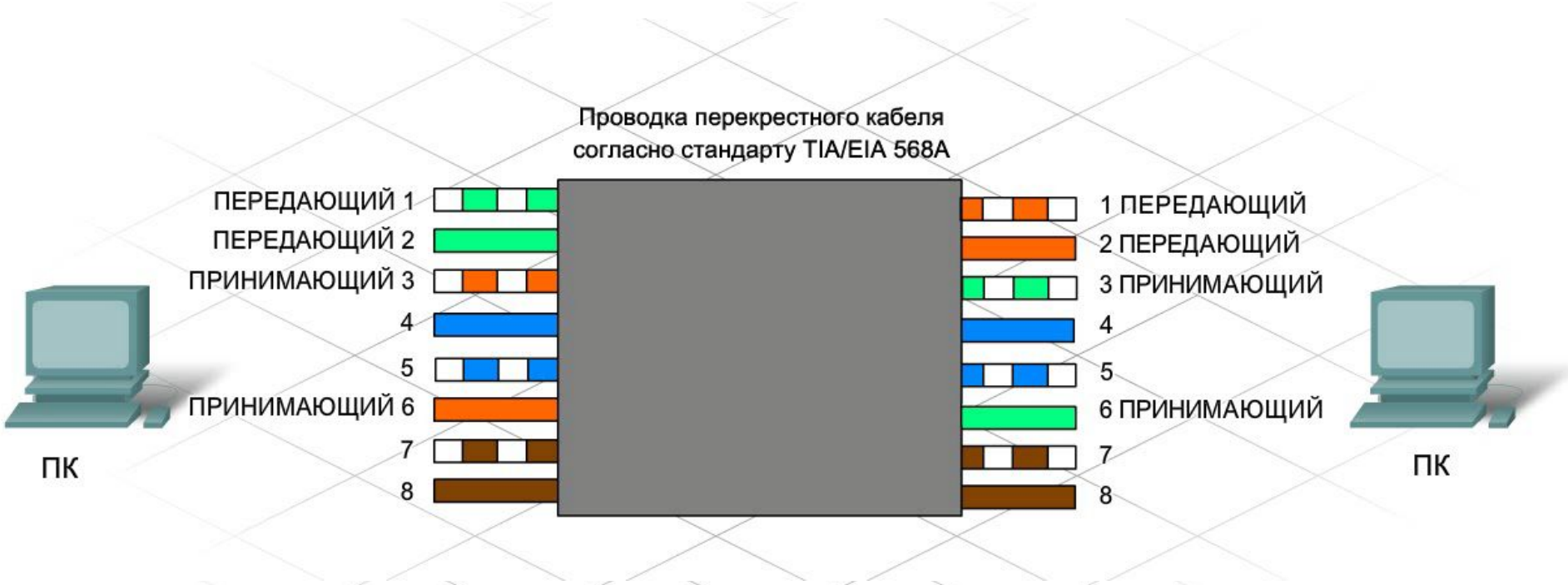
Вернемся к UTP





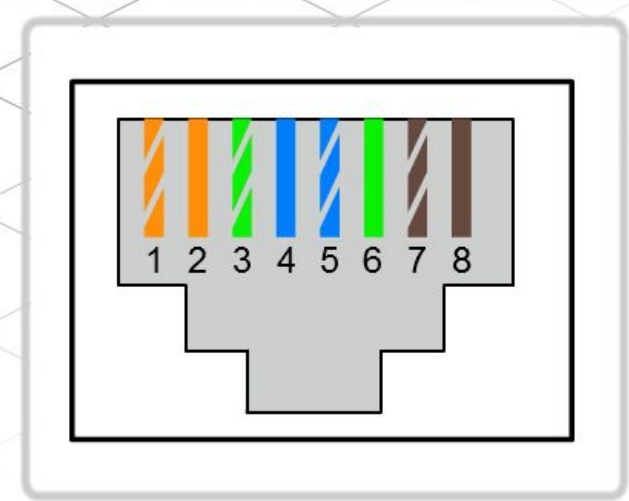
Вернемся к UTP

По схемам T568A и T568B можно создать два типа кабелей: прямой или перекрестный кабель. Эти два типа кабелей встречаются в информационных центрах.

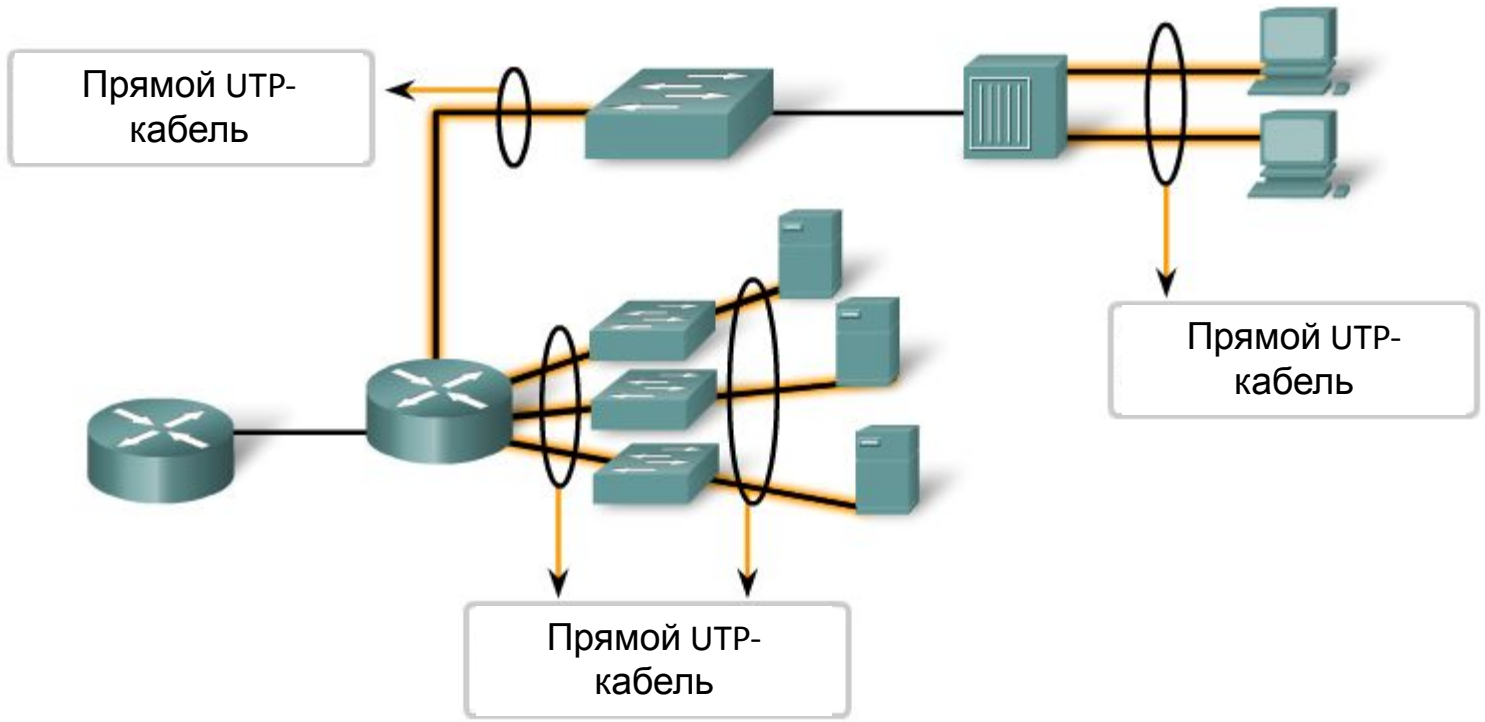


кабеля для соединения двух устройств зависит от того, какие пары проводов используются для передачи и приема данных.

Вернемся к UTP

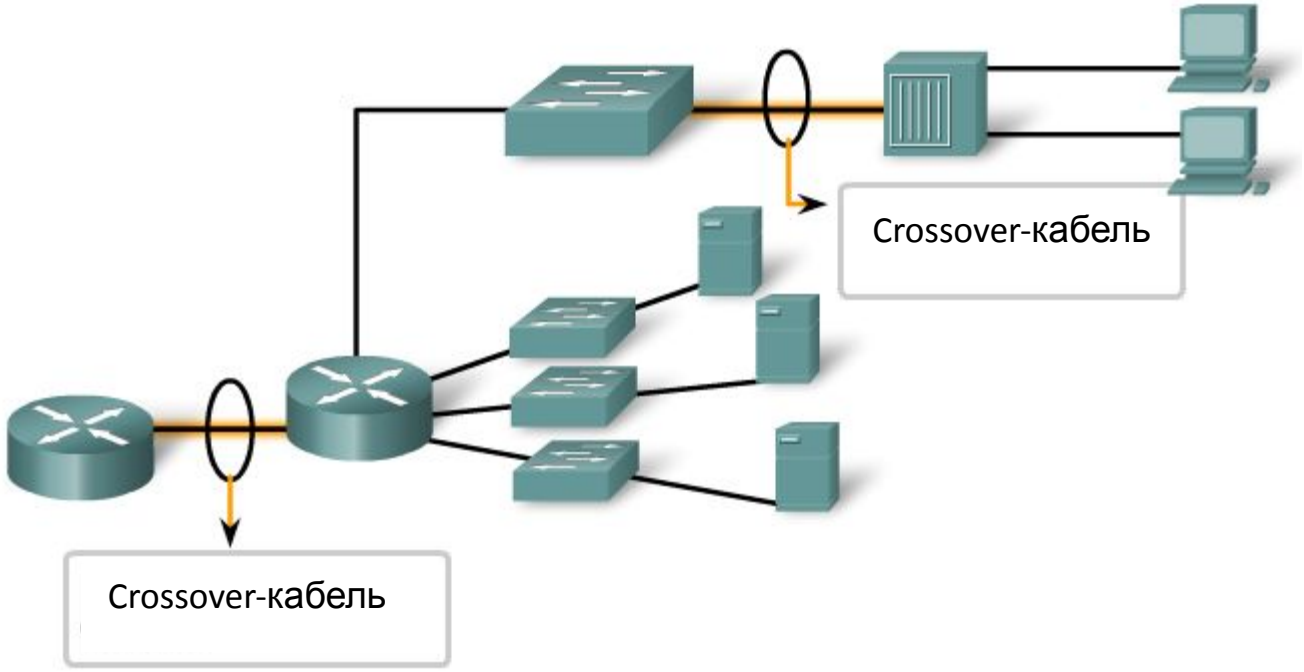


Соединение сетевых устройств



* Негласное правило: устройства разных уровней сетевой модели соединяются прямым кабелем

Соединение сетевых устройств



* Негласное правило: устройства одного уровня сетевой модели соединяются кроссоверным кабелем

Оптимальные методы прокладки кабелей

1. Важно, чтобы типы кабелей и компонентов сети соответствовали обязательным стандартам.

2. В стандартах указана максимальная длина кабелей различных типов. Обязательно учитывайте ограничения по длине, относящиеся к установленным кабелям.

3. UTP, как и любой другой кабель с медными проводниками, подвержен воздействию ЭМП. Важно, чтобы он проходил вдали от источников помех, например, высоковольтных кабелей и флуоресцентных ламп. Возможными источниками помех являются телевизоры, компьютерные мониторы и микроволновые печи. Иногда кабели передачи данных приходится прокладывать по кабельным каналам, чтобы защититься от ЭМП и РЧП.

4. Неправильное подключение и использование низкокачественных кабелей и разъемов может снизить пропускную способность кабеля. Обязательно следуйте правилам подключения и проверяйте правильность выполнения работы.

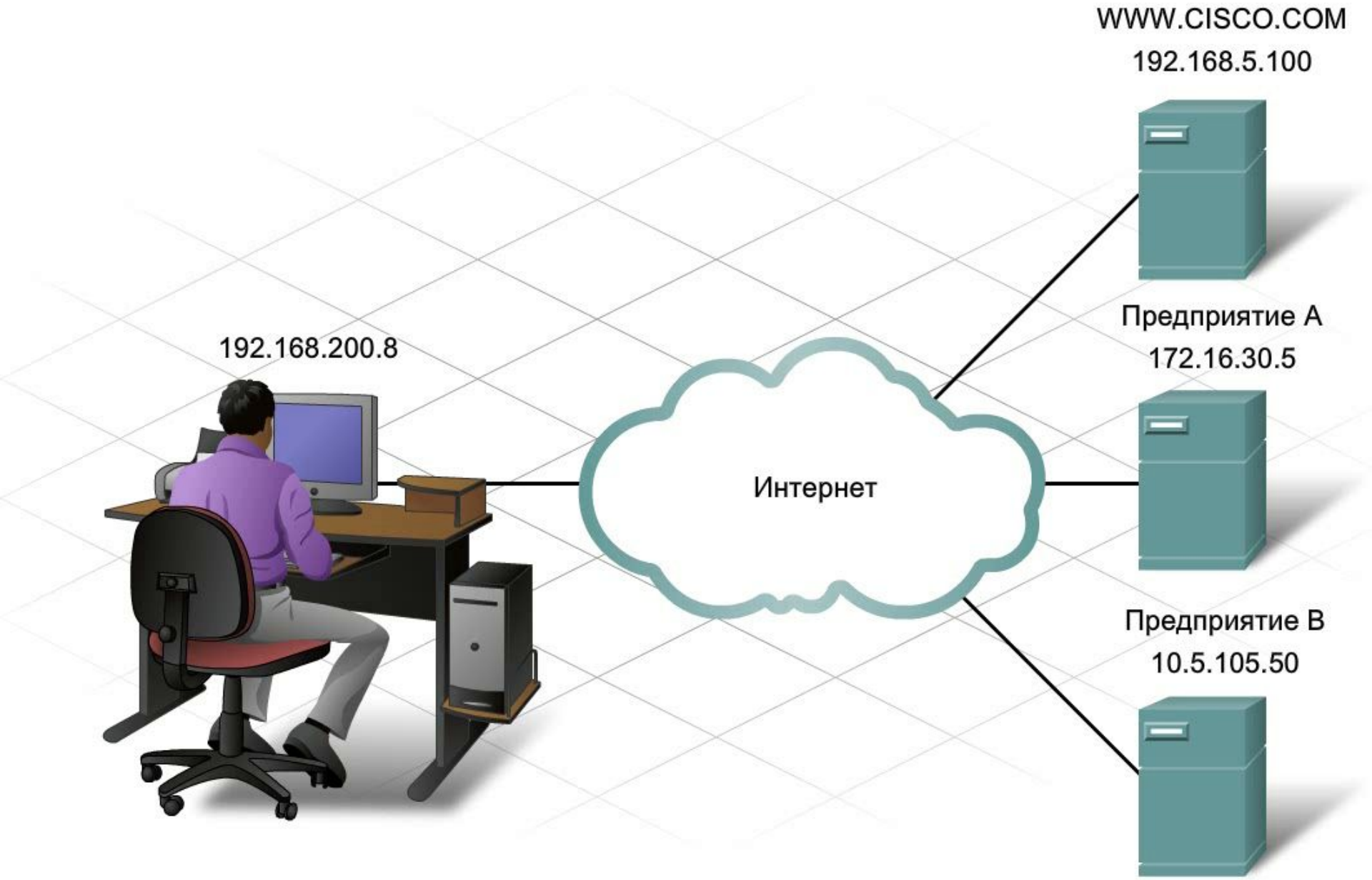
5. Проверьте все кабели и убедитесь в правильности подключения и работоспособности.

6. В процессе монтажа помечайте все кабели и записывайте их положение в сетевую документацию.

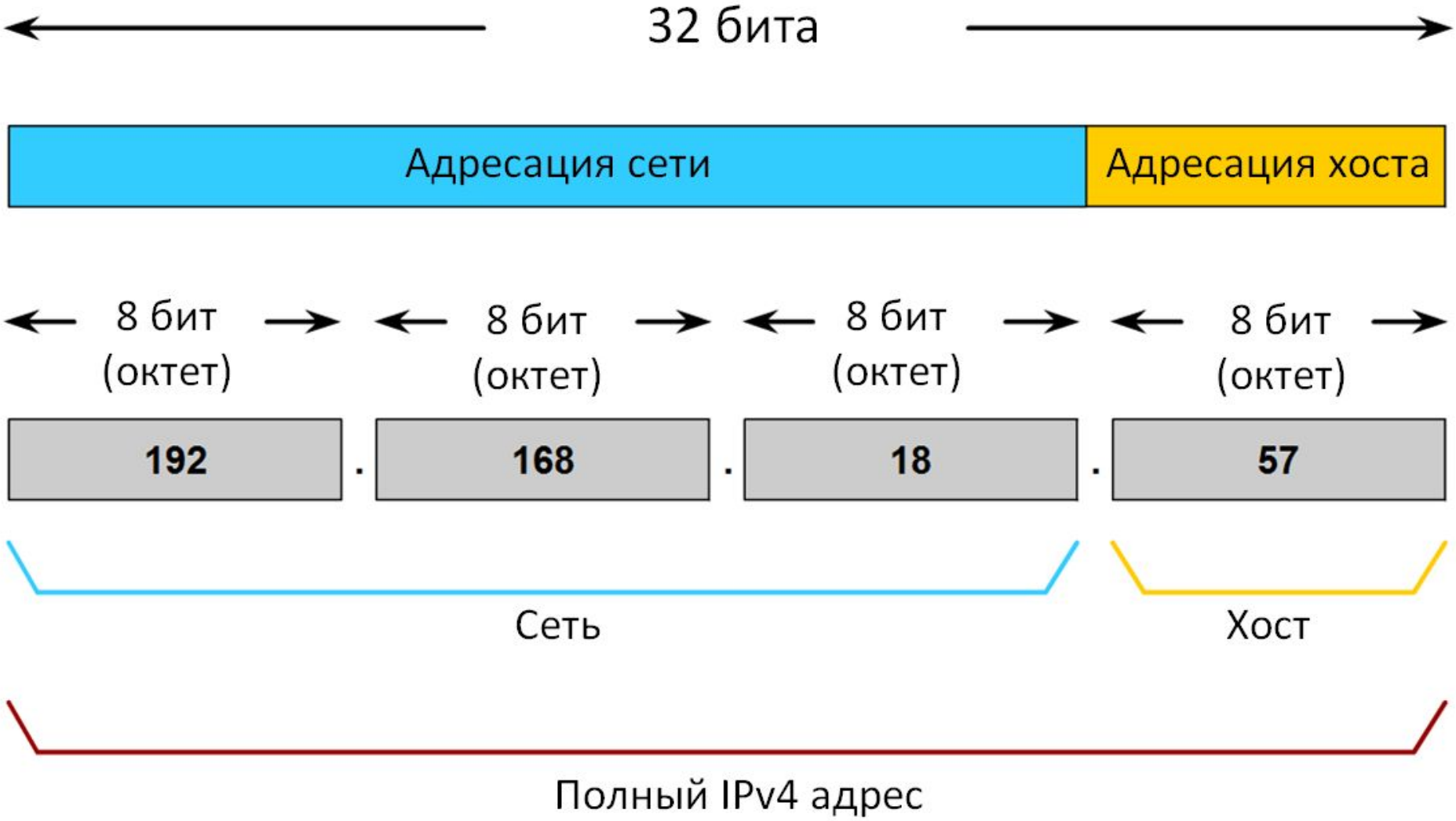
- IV -

IPv4 - адресация

Задачи IP-адресации



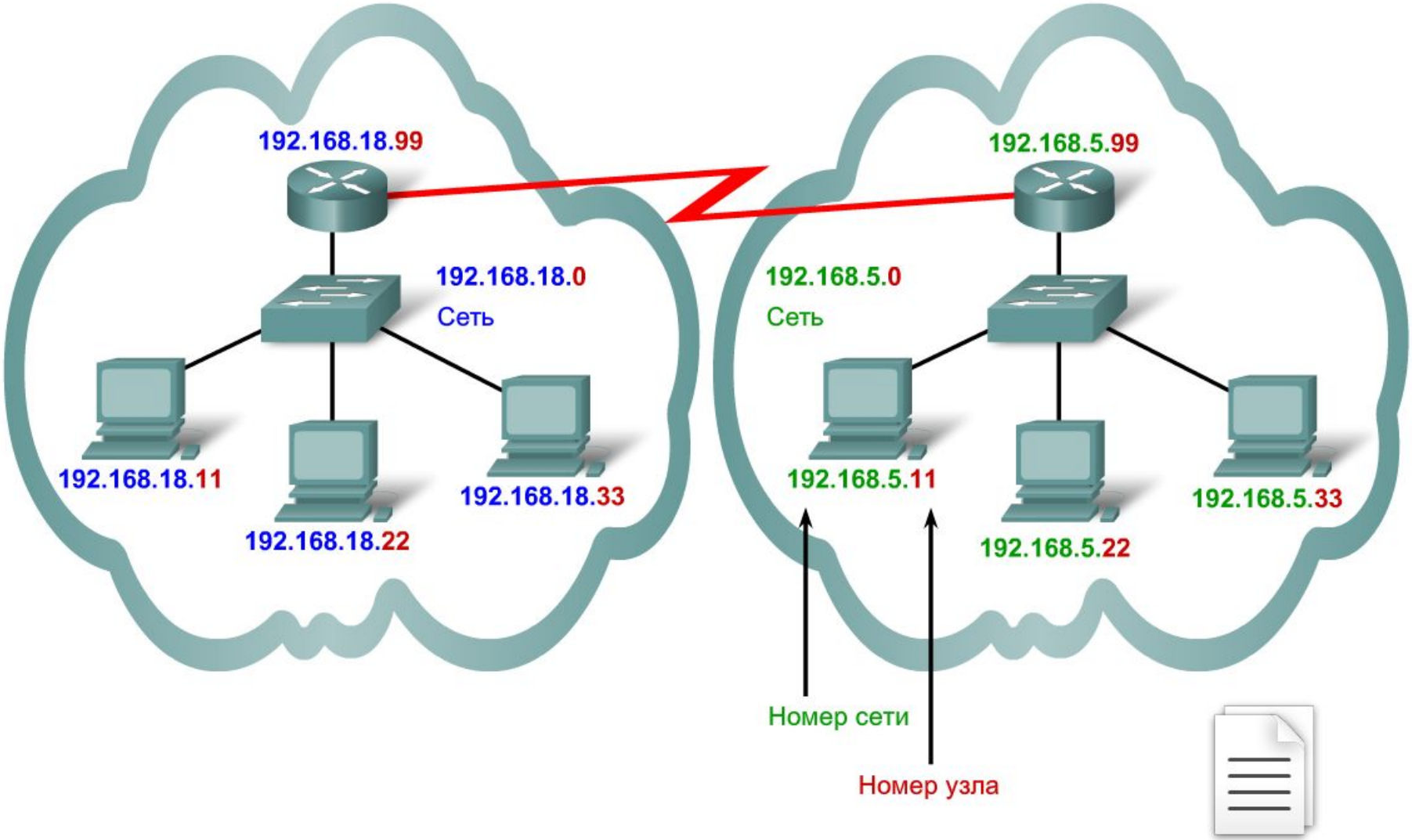
IP - адресация



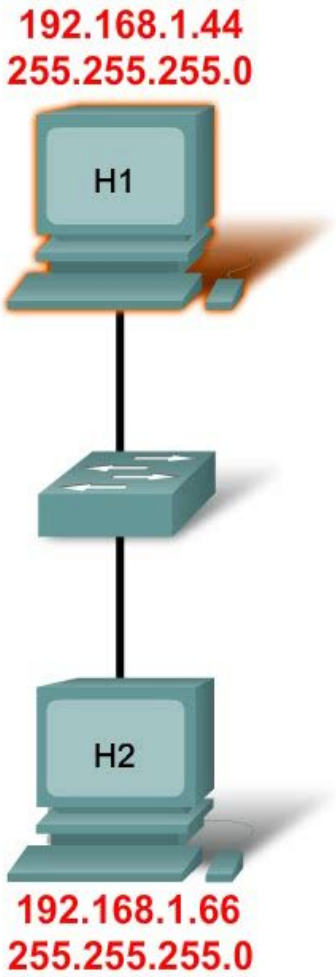
Структура IP-адреса

Таким образом, значение каждого из четырех октетов находится в диапазоне от 0 до 255

Части IP-адреса



Взаимодействие IP-адреса и маски подсети



пакет на интерфейс локального маршрутизатора для отправки в другую сеть.

Классы IP-адресов

Класс	Диапазон значений 1 октета	Биты первого октета	Части адресов сети (N) и хоста (H)	Маска подсети по умолчанию	Число подсетей и хостов
A	1-127	00000000 – 01111111	N.H.H.H	255.0.0.0	128 сетей (2^7) 16777214 хостов в сети(2^{24}-2)
B	128-191	10000000 – 10111111	N.N.H.H	255.255.0.0	16 384 сетей (2^{14}) 65 534 хостов в сети (2^{16} - 2)
C	192-223	11000000 – 11011111	N.N.N.H	255.255.255.0	2 097 150 сетей (2^{21}) 254 хоста в сети (2^8 - 2)
D	224-239	11100000 – 11101111	Мультикастовая адресация		
E	240-255	11110000 – 11111111	Экспериментальная адресация		

Адрес 127.0.0.1 – «локальная петля», локальный IP-адрес по-умолчанию

Использование маски подсети на примере двоичной арифметики

Адрес хоста	192	168	1	1
Маска подсети	255	255	255	0
Адрес хоста	**11000000**	**10101000**	**00000001**	**00000001**
	AND	AND	AND	AND
Маска подсети	**11111111**	**11111111**	**11111111**	**00000000**
Адрес подсети	**=11000000**	**=10101000**	**=00000001**	**=00000000**

24 бита

2^8=256 адресов

.0 – подсеть

.255 – широковещательный

остается 254 адреса

/24 означает использование 24 бит маски подсети для определения адреса подсети

Использование маски подсети на примере двоичной арифметики

Адрес хоста	192	168	1	129
Маска подсети	255	255	255	128
Адрес хоста	**11000000**	**10101000**	**00000001**	**10000001**
	AND	AND	AND	AND
Маска подсети	**11111111**	**11111111**	**11111111**	**10000000**
Адрес подсети	**=11000000**	**=10101000**	**=00000001**	**=10000000**

25 бит

/25 означает использование 25 бит маски подсети для определения адреса подсети

2^7=128 адресов

.128 – подсеть

.255 – широковещательный

остается 126 адресов

.0 .127 и .128 … .255

подсеть широковещательный подсеть широковещательный

256/128 = 2 диапазона адресов по 128 адресов в каждом

Использование маски подсети на примере двоичной арифметики

Адрес хоста	192	168	1	253
Маска подсети	255	255	255	252
Адрес хоста	**11000000**	**10101000**	**00000001**	**11111101**
	AND	AND	AND	AND
Маска подсети	**11111111**	**11111111**	**11111111**	**11111100**
Адрес подсети	**=11000000**	**=10101000**	**=00000001**	**=11111100**

30 бит

/30 означает использование 30 бит маски подсети для определения адреса подсети

.0....3|.4....7|.8....11|.12....15|.16....19|.....|.248....251|.252....255

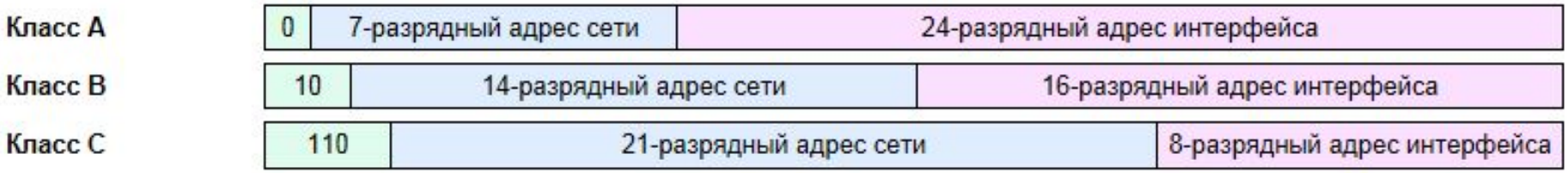
256/4 = 64 диапазона адресов по 4 адреса в каждом

2^2=4 адреса

.252 – подсеть

.255 – широковещательный

остается 2 адреса



Классы IP-адресов

Класс	Первые биты	Число байт для № сети	Число байт для № узла	Число сетей	Число узлов
A	0	1	3	128 (-2)	16 777 216 (-2)
B	10	2	2	16 384	65 536 (-2)
C	110	3	1	2 097 152	256 (-2)

Нумерация IP-сетей

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети
A	0	1.0.0.0	126.0.0.0
B	10	128.0.0.0	191.255.0.0
C	110	192.0.0.0	223.255.255.0

192.0.2.32/27.

Октеты IP-адреса	192								0								2								32							
Биты IP-адреса	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0
Биты маски подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
Октеты маски подсети	255								255								255								224							

172.16.0.1/12.

Октеты IP-адреса	172								16								0								1							
Биты IP-адреса	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Биты маски подсети	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Октеты маски подсети	255								240								0								0							

Возможные маски

IP/маска	До последнего IP в подсети	Маска	Количество адресов	Класс
a.b.c.d/**32**	+0.0.0.0	255.255.255.255	1	1/256 C
a.b.c.d/**31**	+0.0.0.1	255.255.255.254	2	1/128 C
a.b.c.d/**30**	+0.0.0.3	255.255.255.252	4	1/64 C
a.b.c.d/**29**	+0.0.0.7	255.255.255.248	8	1/32 C
a.b.c.d/**28**	+0.0.0.15	255.255.255.240	16	1/16 C
a.b.c.d/**27**	+0.0.0.31	255.255.255.224	32	1/8 C
a.b.c.d/**26**	+0.0.0.63	255.255.255.192	64	1/4 C
a.b.c.d/**25**	+0.0.0.127	255.255.255.128	128	1/2 C
a.b.c.0/**24**	+0.0.0.255	255.255.255.000	256	1 C

Возможные маски

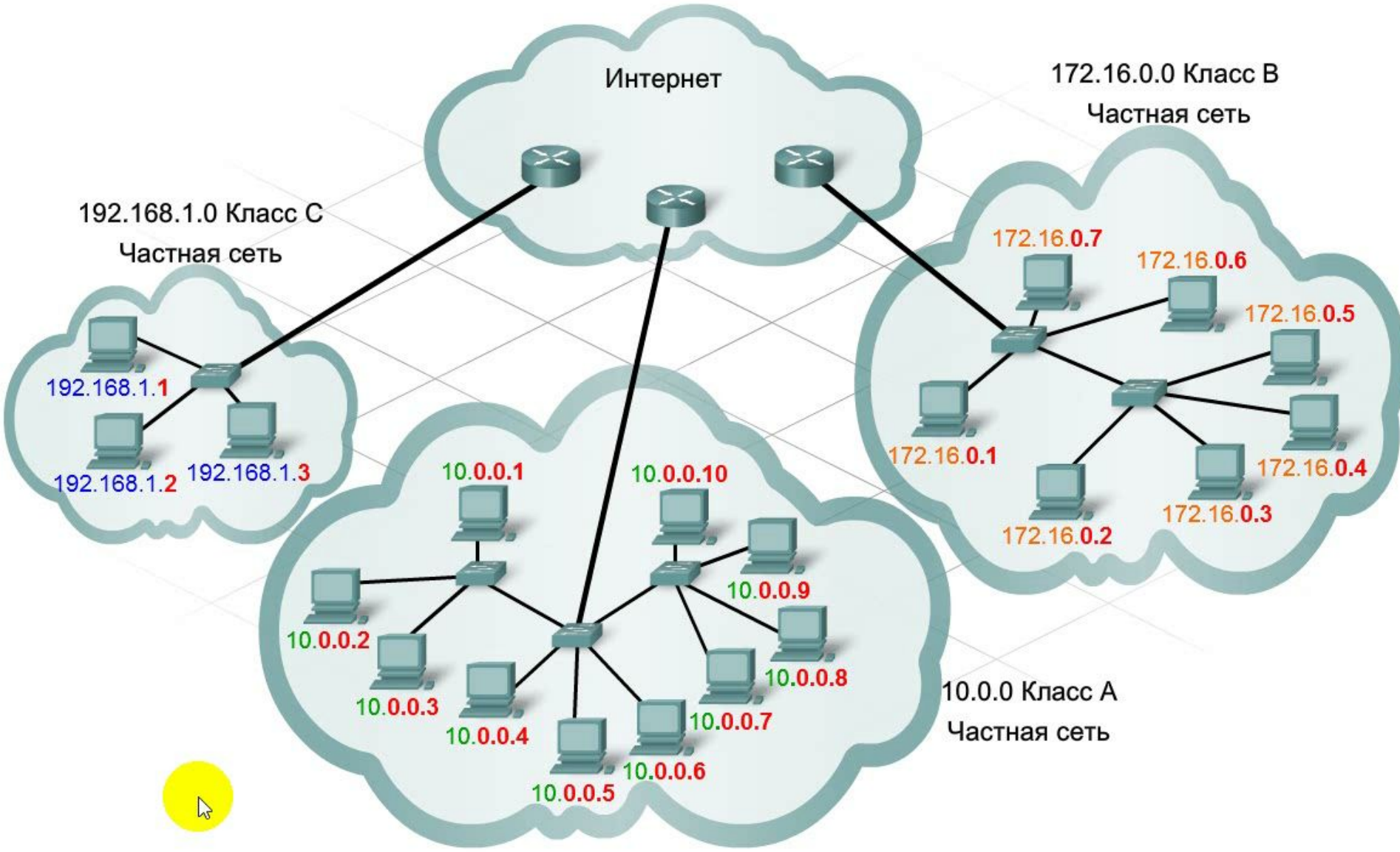
IP/маска	До последнего IP в подсети	Маска	Количество адресов	Класс
a.b.c.0/**23**	+0.0.1.255	255.255.254.000	512	2 C
a.b.c.0/**22**	+0.0.3.255	255.255.252.000	1024	4 C
a.b.c.0/**21**	+0.0.7.255	255.255.248.000	2048	8 C
a.b.c.0/**20**	+0.0.15.255	255.255.240.000	4096	16 C
a.b.c.0/**19**	+0.0.31.255	255.255.224.000	8192	32 C
a.b.c.0/**18**	+0.0.63.255	255.255.192.000	16 384	64 C
a.b.c.0/**17**	+0.0.127.255	255.255.128.000	32 768	128 C
a.b.0.0/**16**	+0.0.255.255	255.255.000.000	65 536	256 C = 1 B

Публичные и частные IP-адреса

В соответствии со стандартом RFC 1918 для общения внутри организаций было зарезервировано несколько диапазонов адресов класса A, B и C. Как видно из таблицы, в диапазон частных адресов входит одна сеть класса A, 16 сетей класса B и 256 сетей класса C. Таким образом, сетевые администраторы получили определенную степень свободы в плане предоставления внутренних адресов.

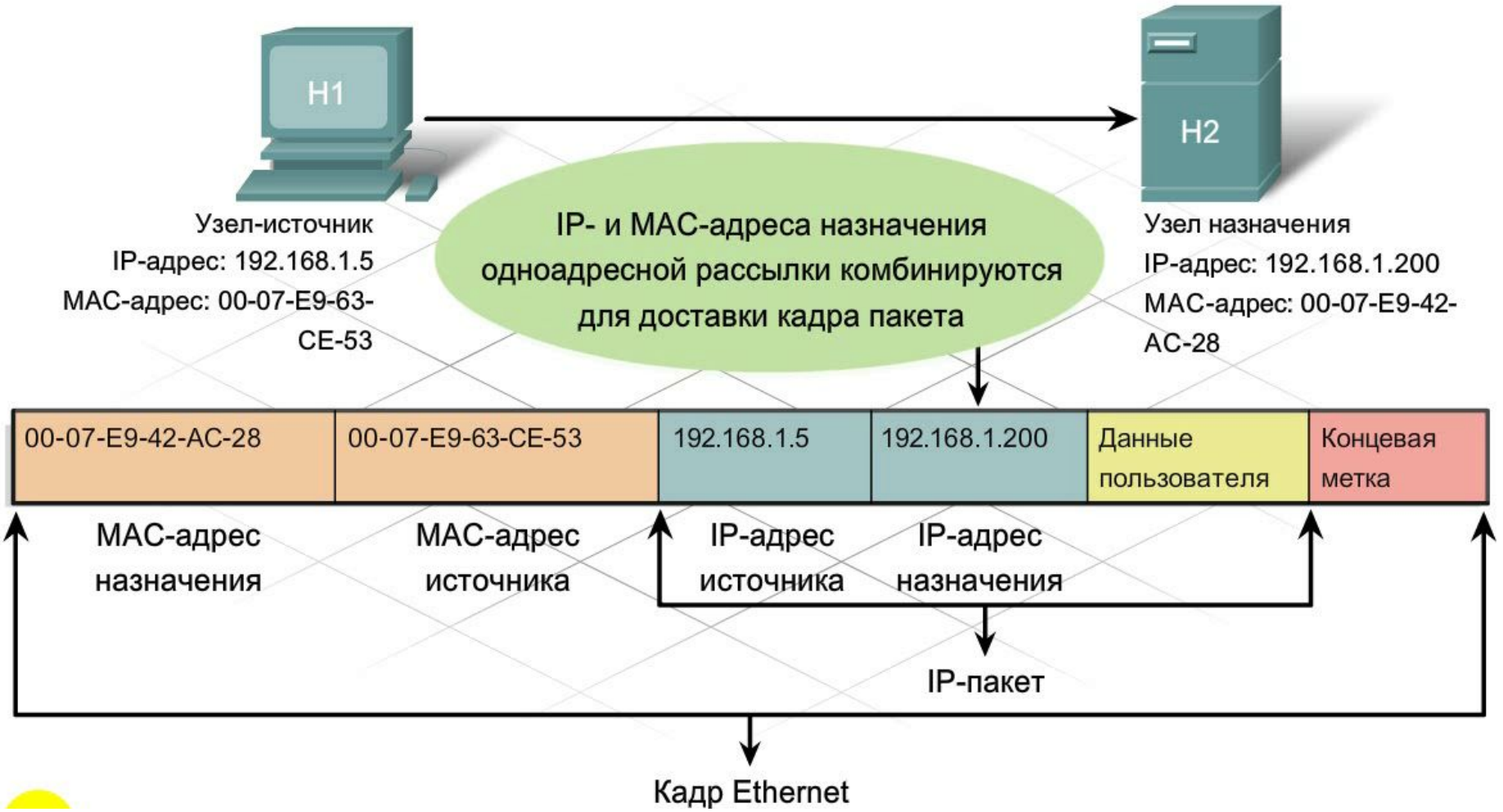
Класс адреса	Число зарезервированных сетевых адресов	Сетевые адреса
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

Публичные и частные IP-адреса

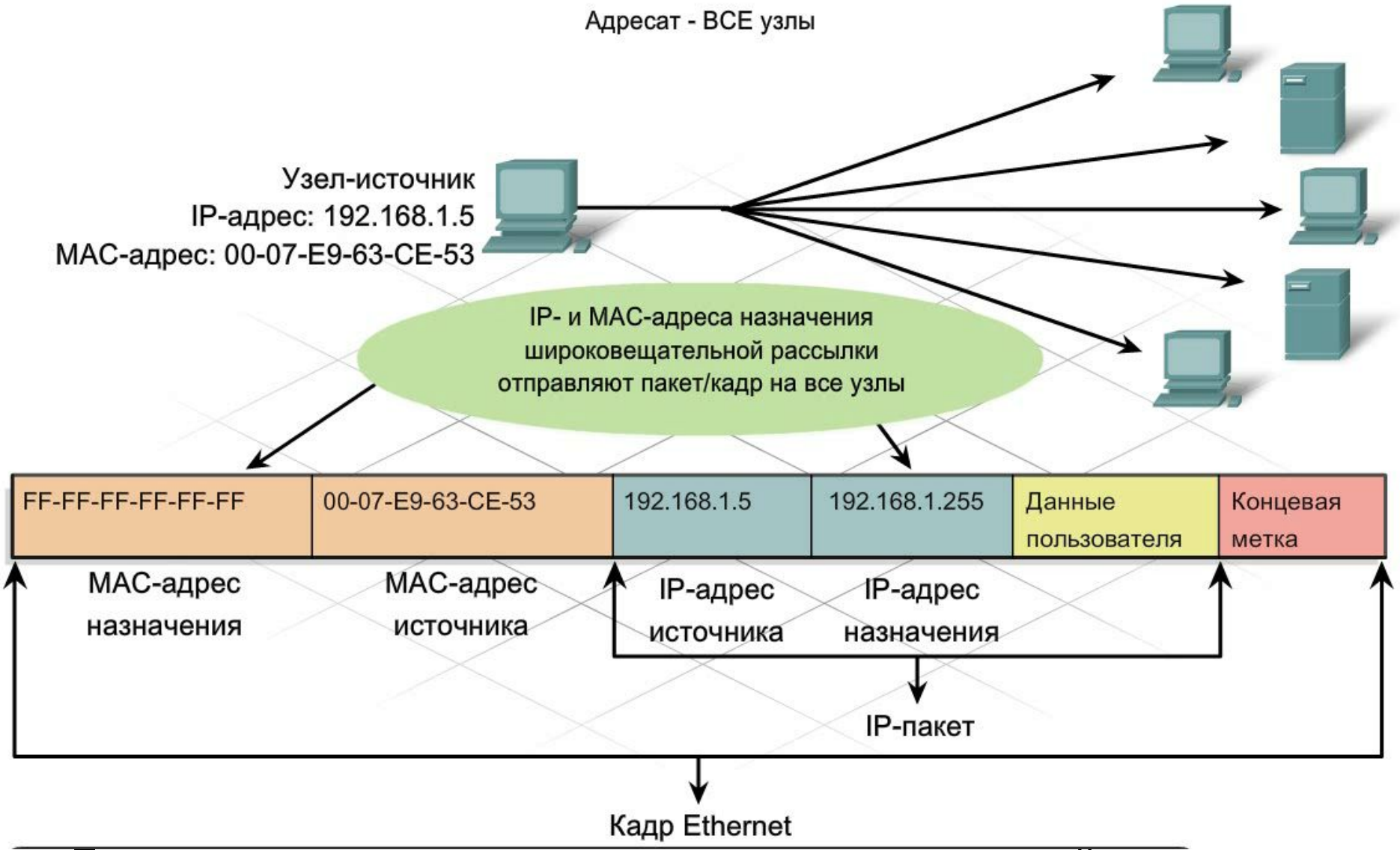


таких адресов зарезервирована сеть 127.0.0.0 класса A.

Различная IP-адресация для различных



Различная IP-адресация для различных



Для сетевого IP-адреса широковещательной рассылки нужен соответствующий MAC-адрес FF-FF-FF-FF-FF-FF в кадре

Различная IP-адресация для различных рассылок

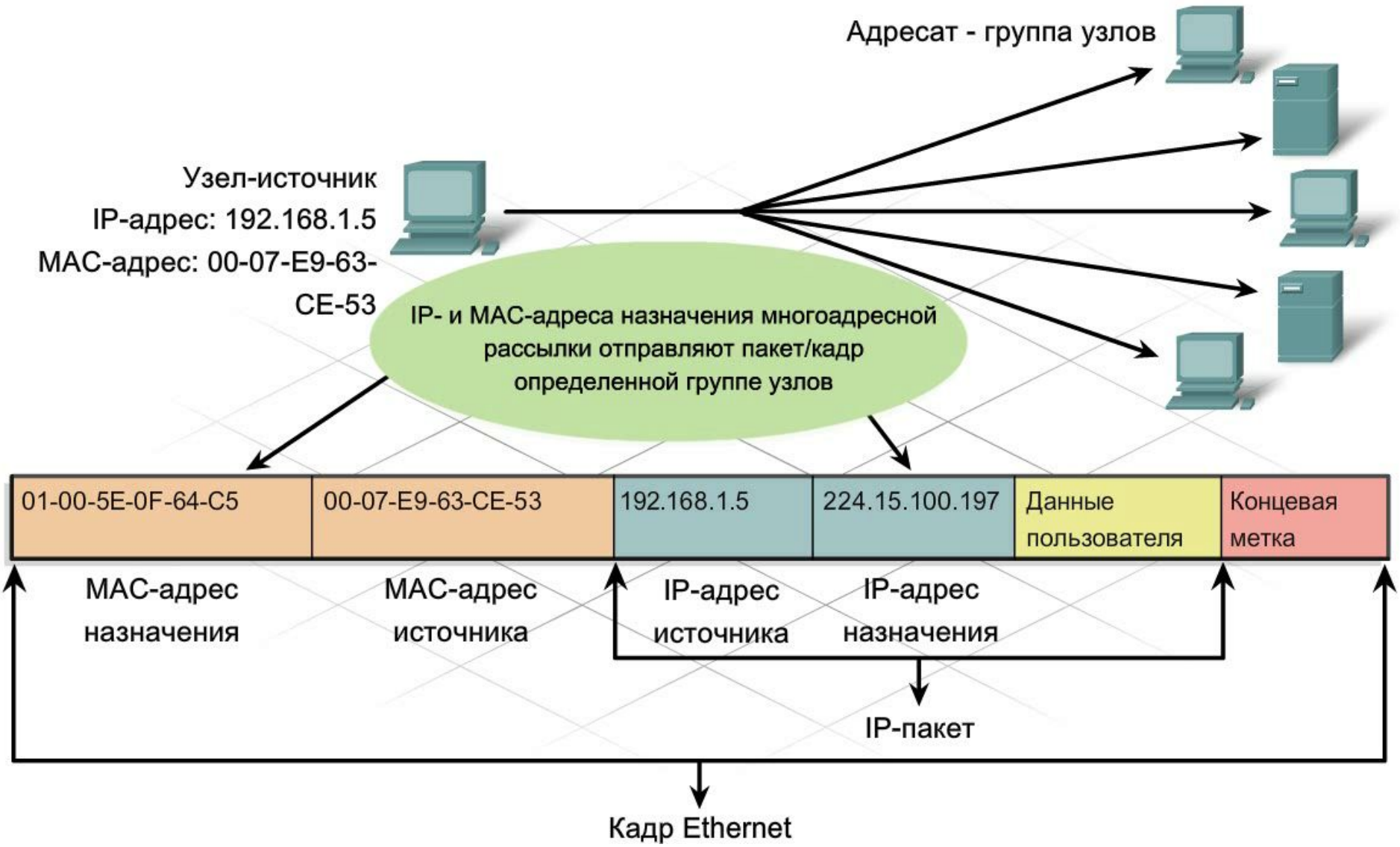
Многоадресная (multicast) рассылка

Адреса многоадресных рассылок позволяют исходному устройству рассылать пакет группе устройств.

Устройства, относящиеся к многоадресной группе, получают ее IP-адрес. Диапазон таких адресов - от 224.0.0.0 до 239.255.255.255. Поскольку адреса многоадресных рассылок соответствуют группам адресов (которые иногда называются группами узлов), они используются только как адресаты пакета. У источника всегда одноадресный адрес.

Адреса многоадресных рассылок используются, например, в дистанционных играх, в которых участвует несколько человек из разных мест. Другой пример - это дистанционное обучение в режиме видеоконференции, где несколько учащихся подключаются к одному и тому же курсу.

Различная IP-адресация для различных



Статическая и динамическая IP-адресация

IP-адреса и или динамически.

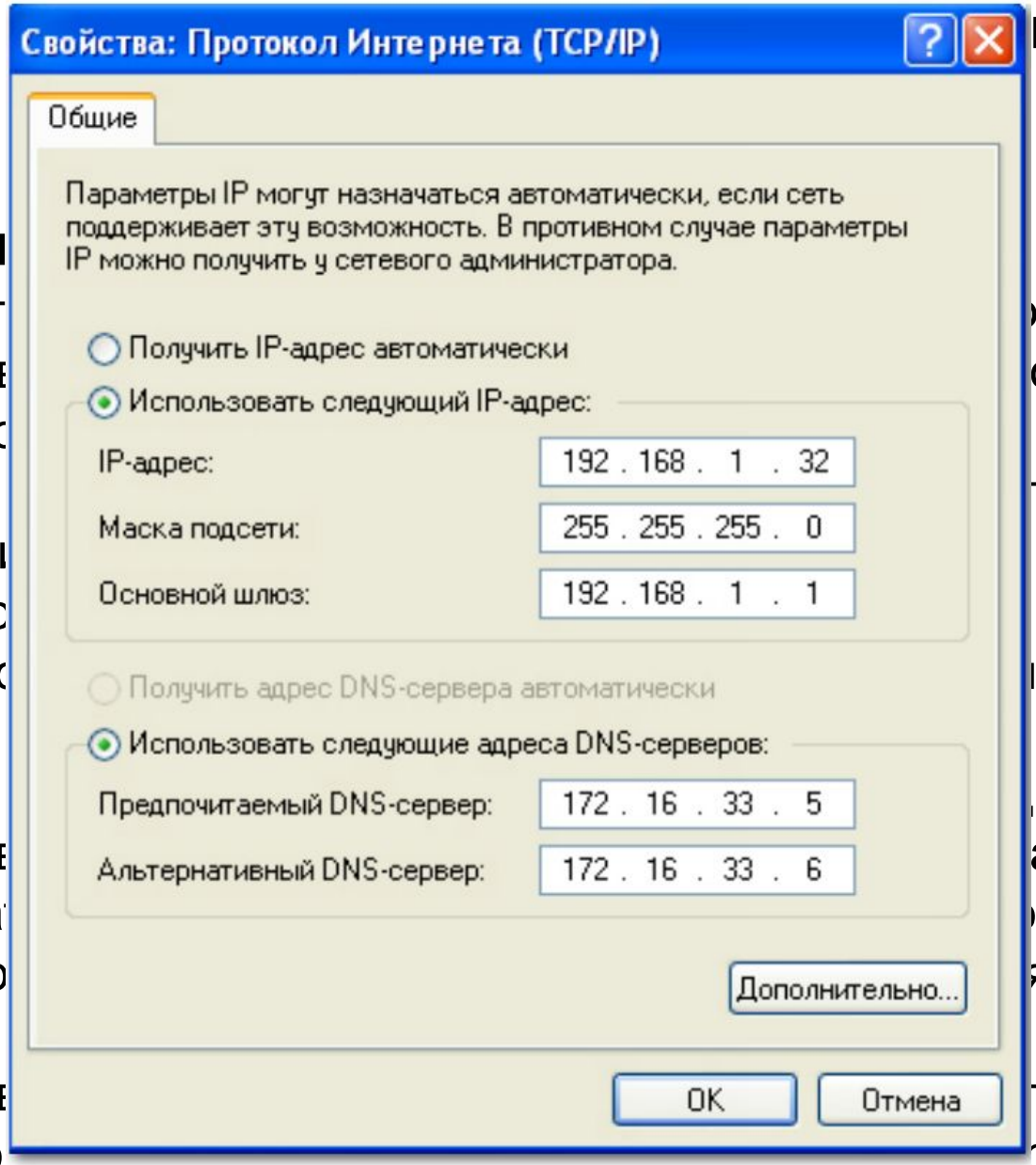
Статически

Используя ст р может вручную настраив о будет IP-адрес, маска подс

У статических пример, их полезно присва сетевым устройствам, котс клиентам. Узлы будут не спо ий IP-адрес изменился.

Статическое п сетевыми ресурсами, но ве ает много времени. При ста вый поиск ошибок в IP-адр я ошибки больше.

При использов ти точный перечень адресо роме того,



Статическая и динамическая IP-адресация

IP-адреса и или
динамическ

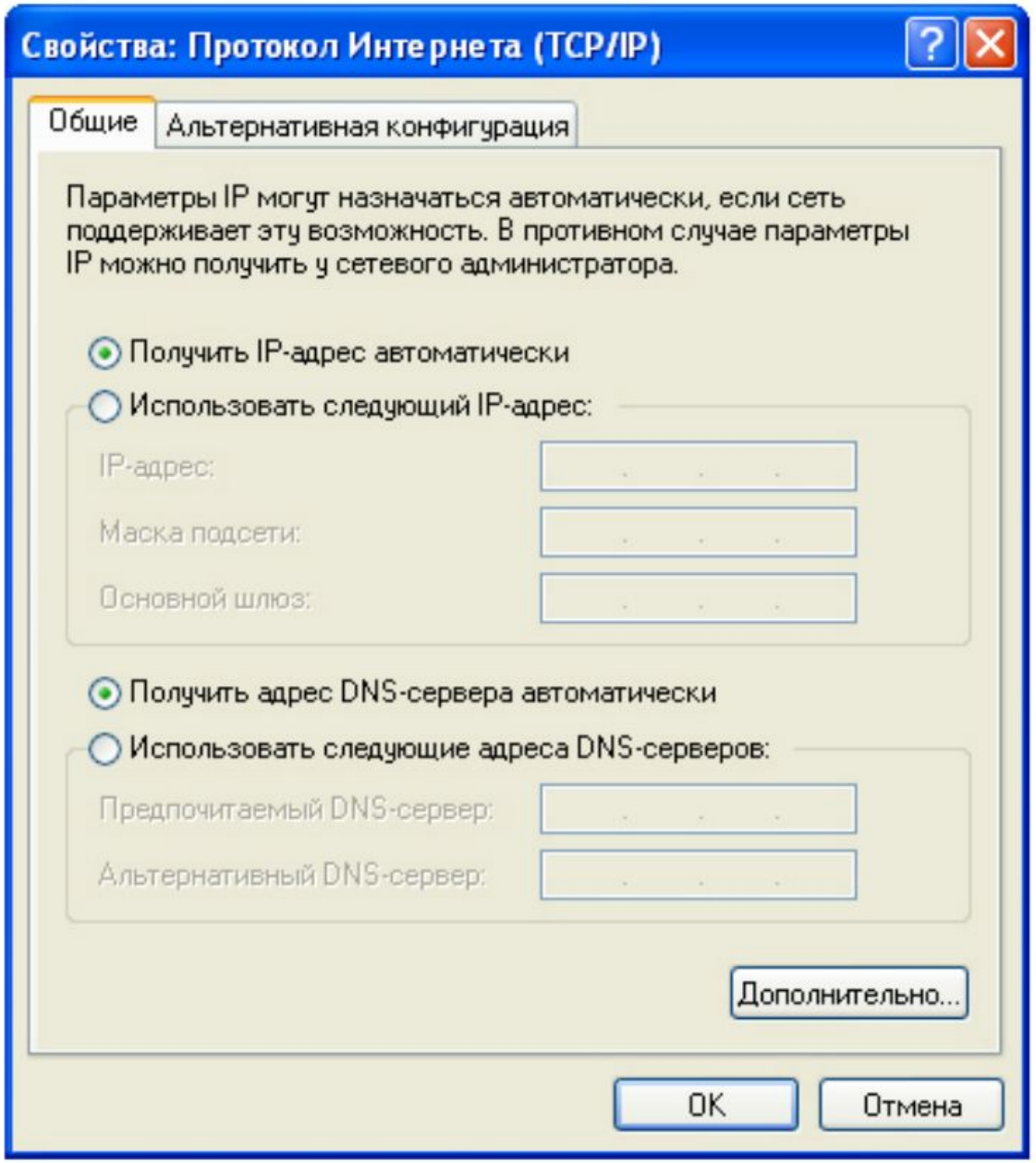
Динамич

Список пол оявляются
новые пользов ть. Другие
устанавливают ганции не
приходилось в го сделать
автоматически ем **Dynamic**
Host Configurati

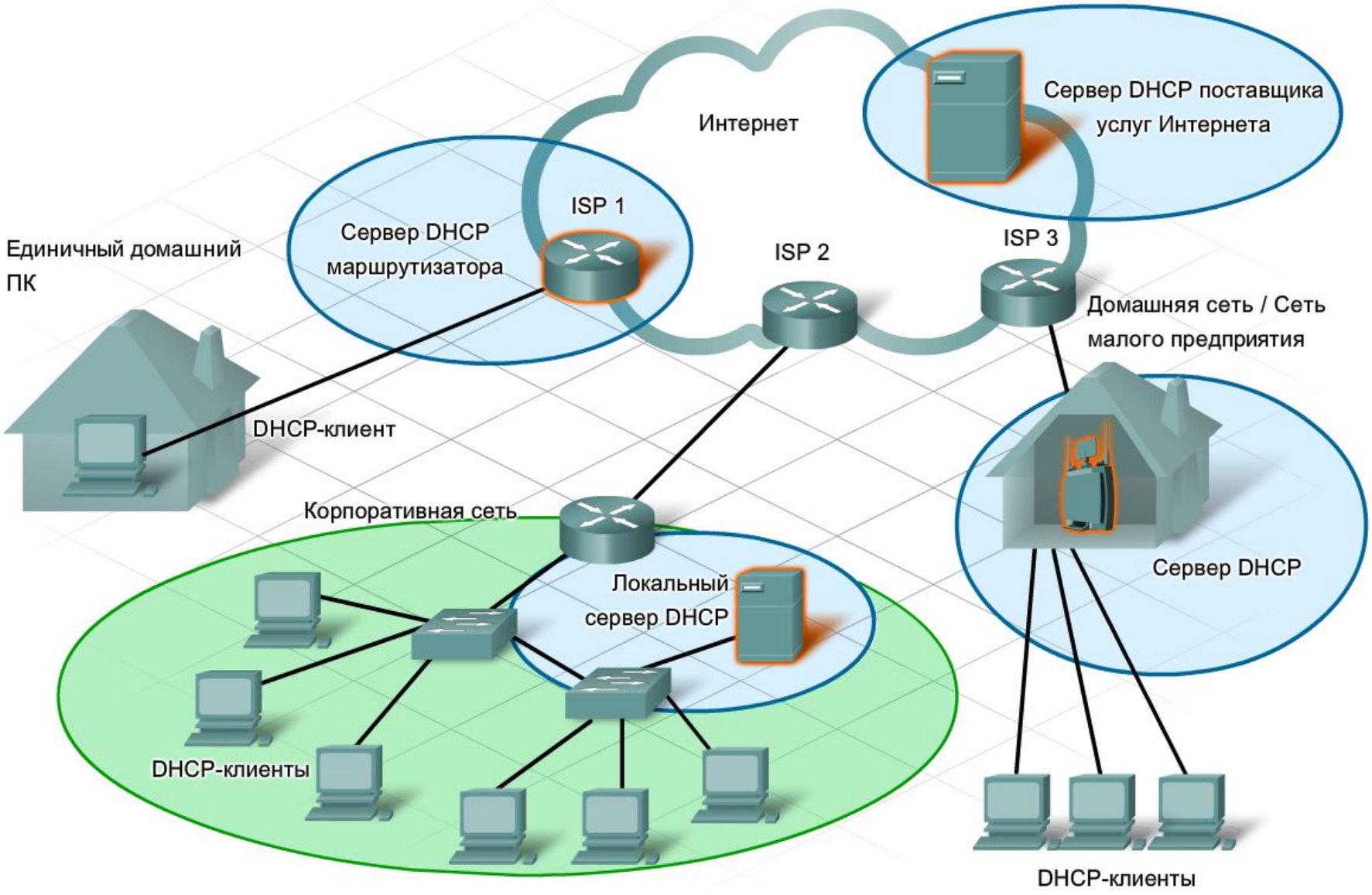
DHCP пред исвоения
информации о основного
шлюза и други

Это наибол P-адресов
узлам в больш циалистов
службы поддер бки.

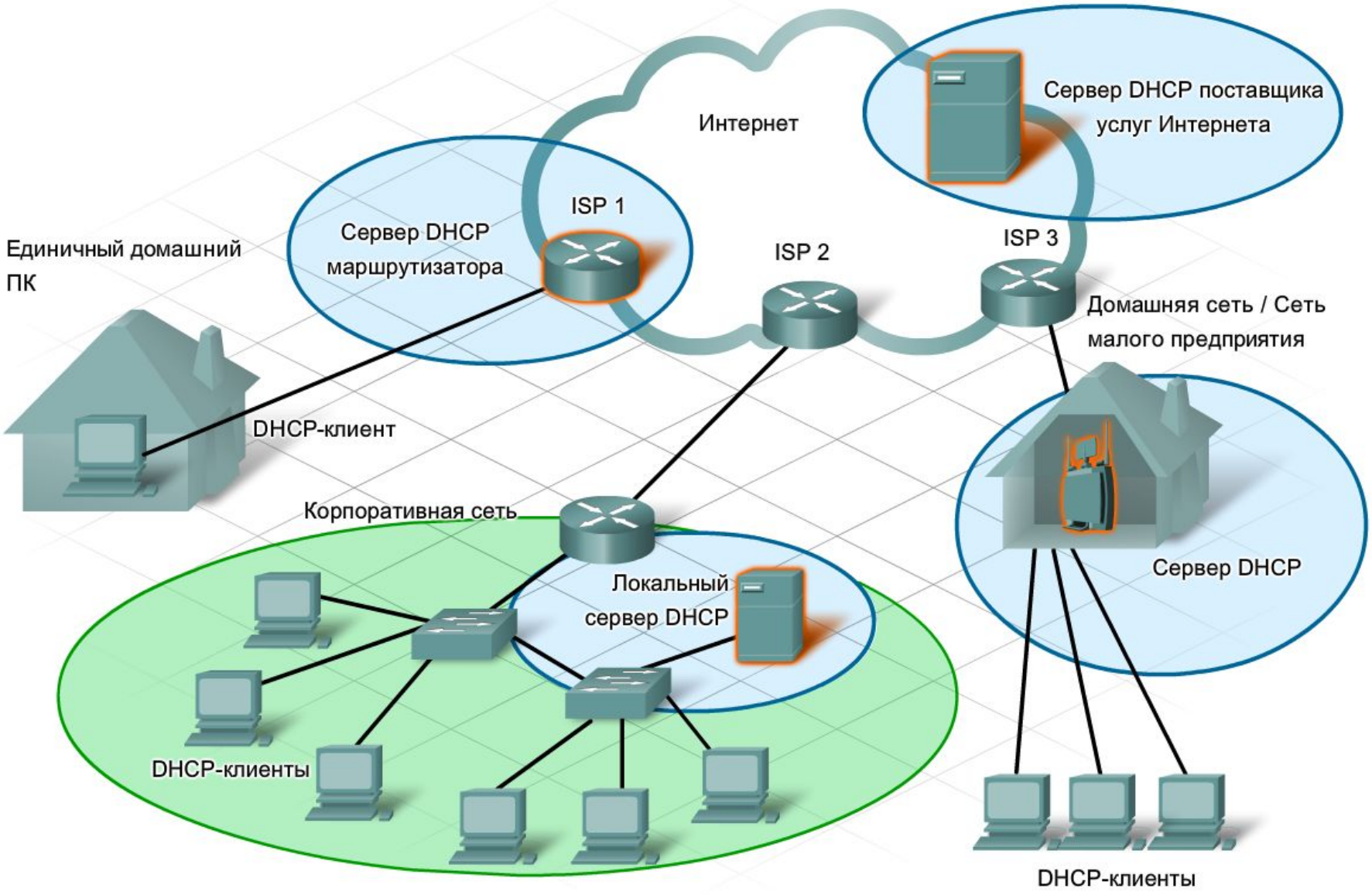
Другое прел ваиваются
узлам времен его адрес
возвращается особенно



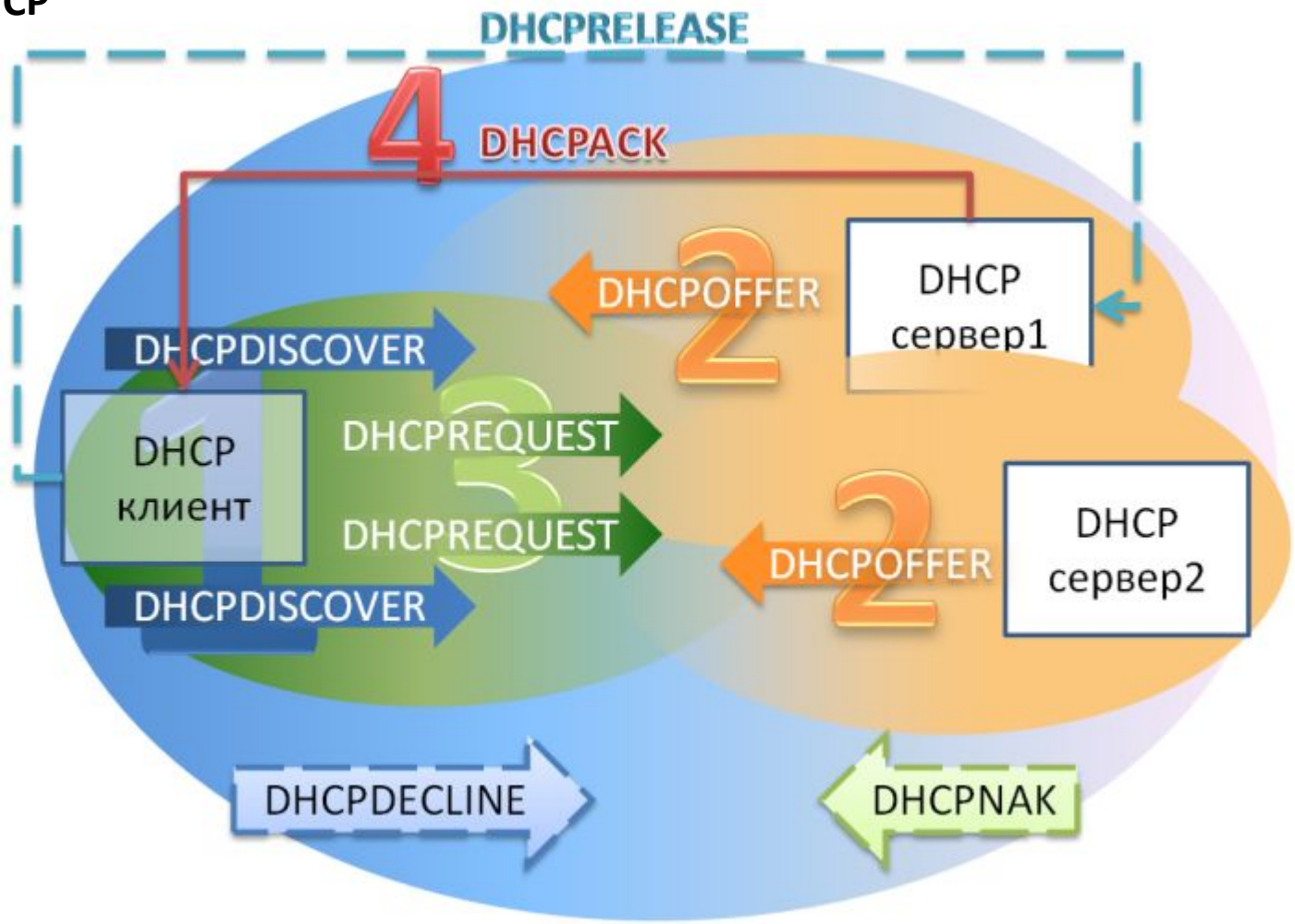
DHCP-серверы



DHCP-серверы

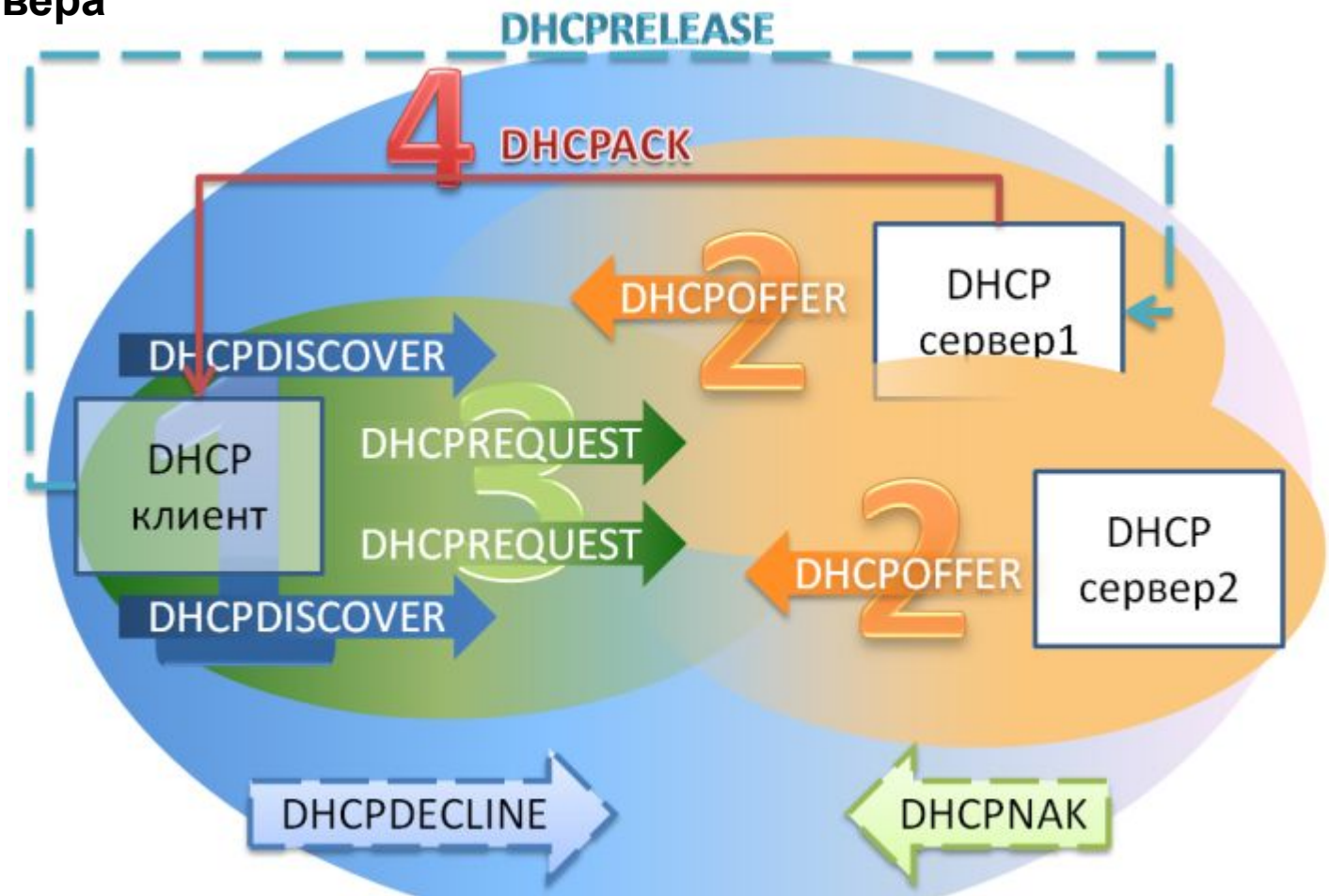


1. Обнаружение DHCP (DHCPDISCOVER)



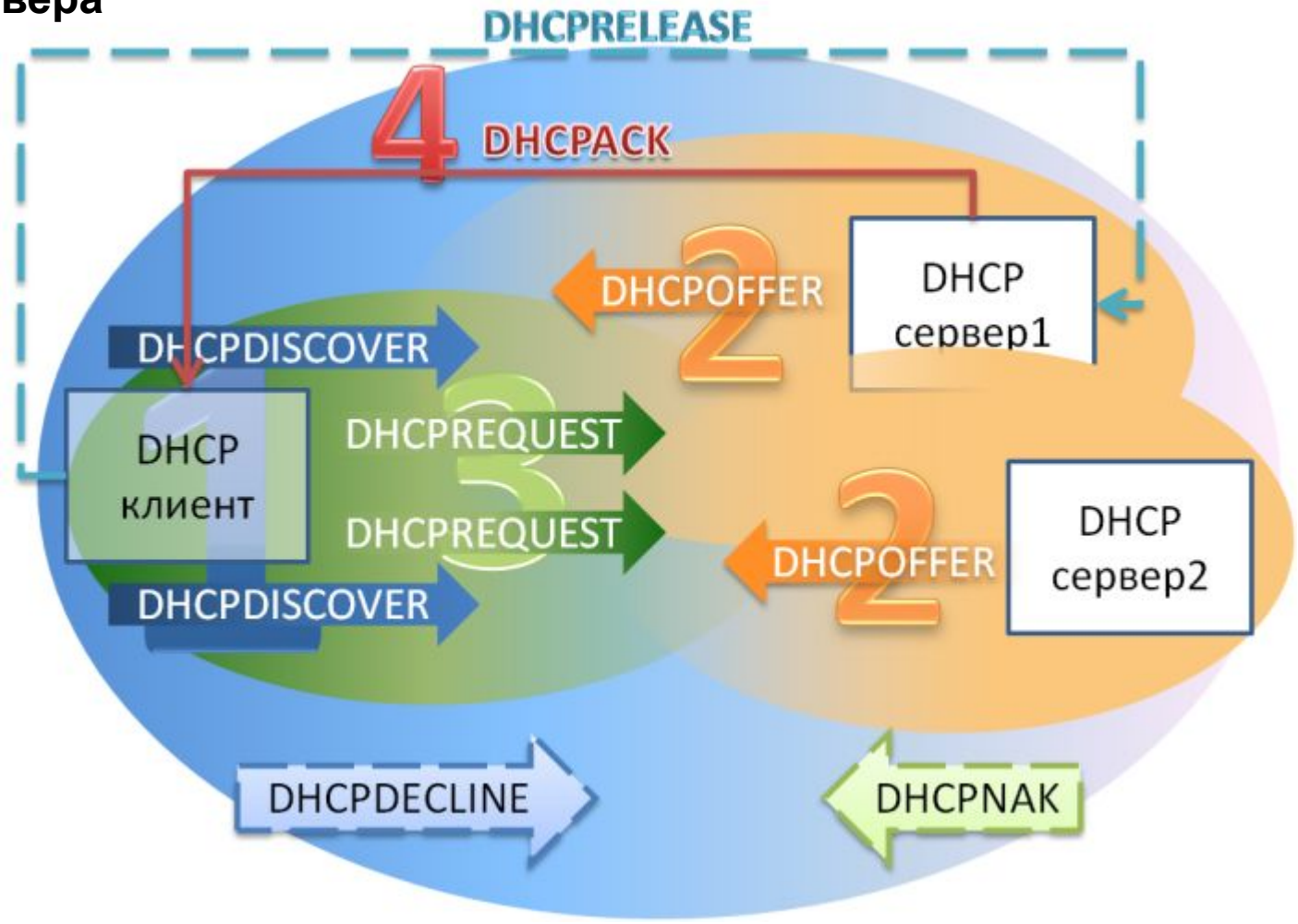
На *первом этапе*, клиент выполняет **широковещательный** запрос по всей физической сети с целью обнаружить доступные DHCP-серверы. Он отправляет сообщение типа **DHCPDISCOVER**, при этом в качестве IP-адреса источника указывается 0.0.0.0 (так как компьютер ещё не имеет собственного IP-адреса), а в качестве адреса назначения — широковещательный адрес 255.255.255.255. Кроме IP источника и назначения, клиент в данном сообщении посылает: *уникальный идентификатор запроса, свой MAC, и, возможно, прошлый присвоенный IP*.

2. Ответ DHCP - сервера (DHCPOFFER)



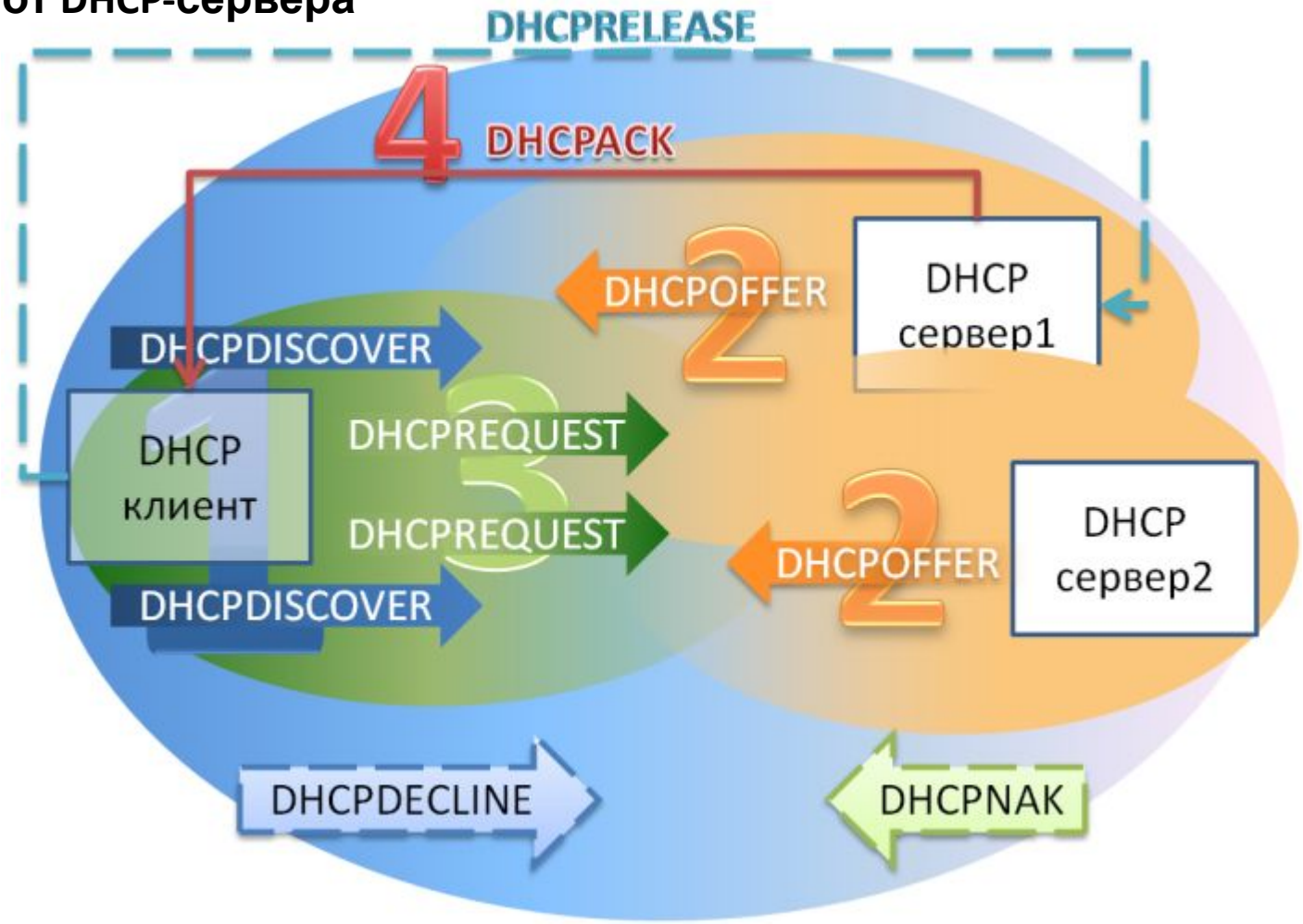
Получив сообщение от клиента, сервера определяют требуемую конфигурацию клиента в соответствии со своими указанными в конфигурационном файле настройками. Все сервера, получившие запрос, формируют ответ (**DHCPOFFER**), содержащий конфигурацию клиента, и отправляют его клиенту на MAC-адрес. В ответе содержится следующая информация: *IP, назначенный хосту, и прочие параметры* (такие, как адреса маршрутизаторов и DNS-серверов). Клиент получает ответы от всех серверов DHCP, функционирующих в сети, из них он должен выбрать тот, который его «устраивает» (обычно - первый).

3. Запрос DHCP-сервера (DHCPREQUEST)



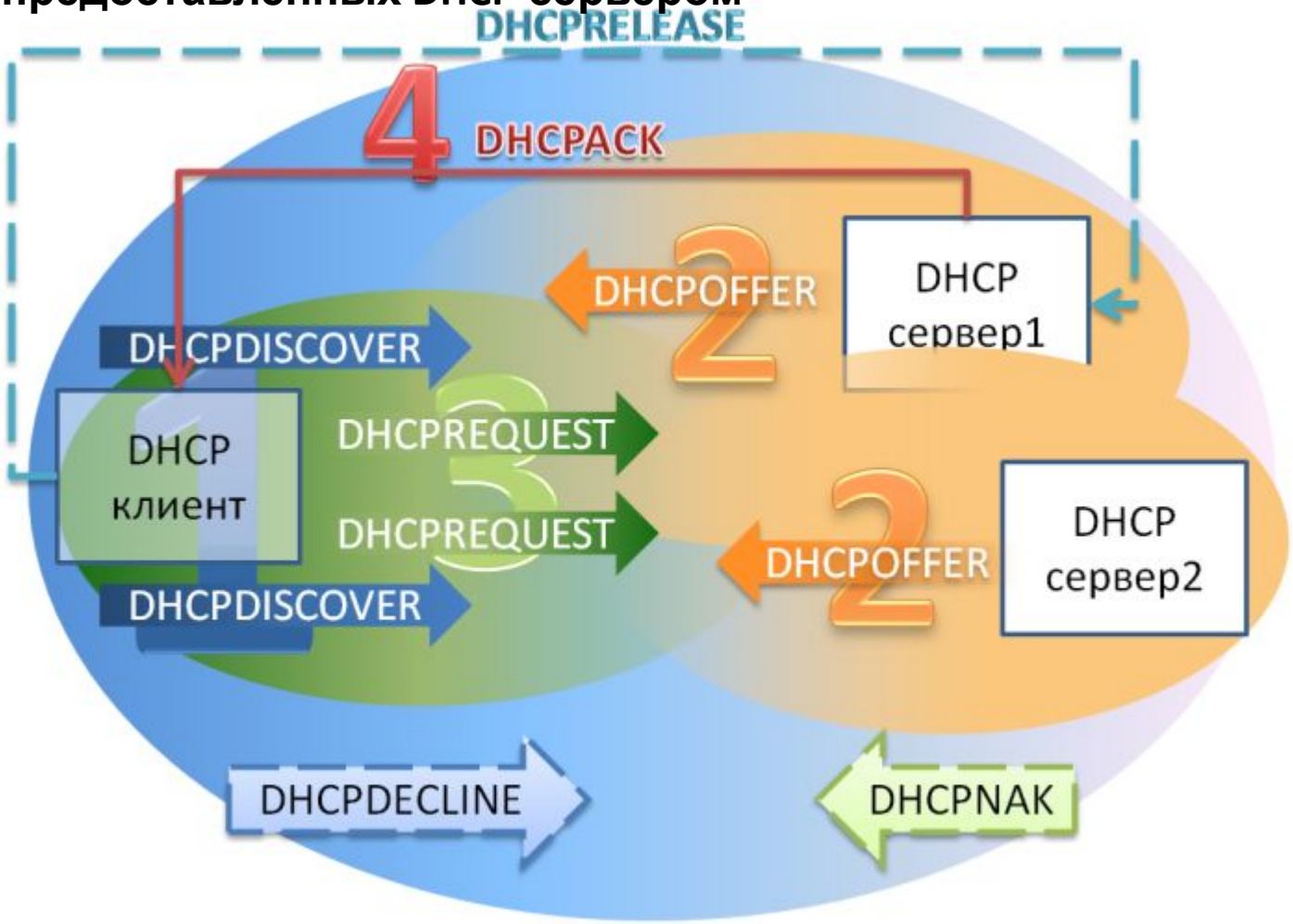
Выбрав одну из конфигураций, предложенных DHCP-серверами, клиент отправляет запрос DHCP (**DHCPREQUEST**). Он рассылается широковещательно. В сообщении содержится информация из сообщения **DHCPDISCOVER** + специальная опция — *идентификатор сервера* — указывающая адрес DHCP-сервера. При этом, сервер, который не выбран в качестве "устраивающего" тоже видит, что он не выбран.

4. Подтверждение от DHCP-сервера (DHCPACK)



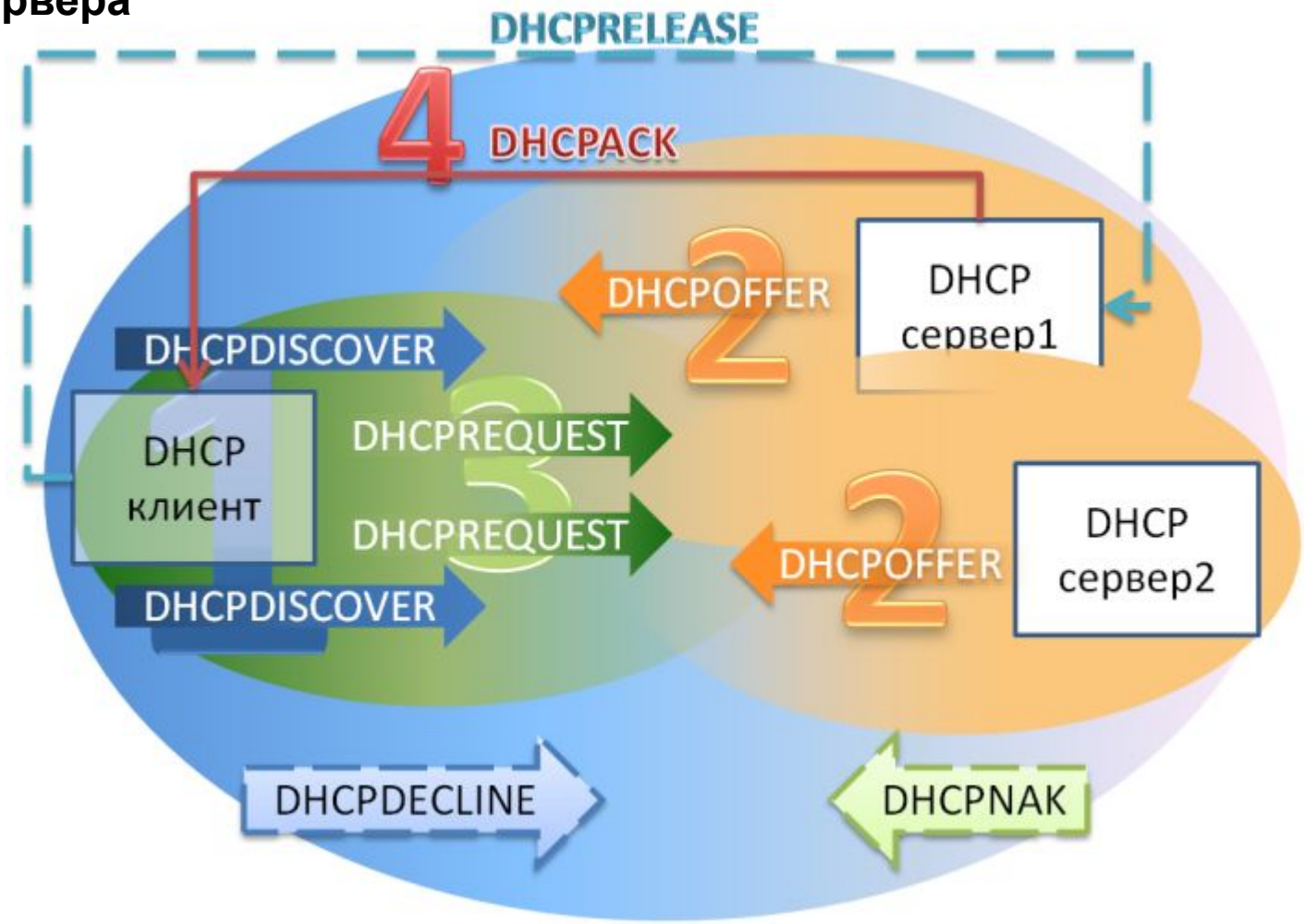
Наконец, сервер подтверждает запрос и направляет это подтверждение (**DHCPACK**) клиенту. После этого клиент должен настроить свой сетевой интерфейс, используя предоставленные опции.

Отказ от настроек, предоставленных DHCP-сервером (DHCPDECLINE)



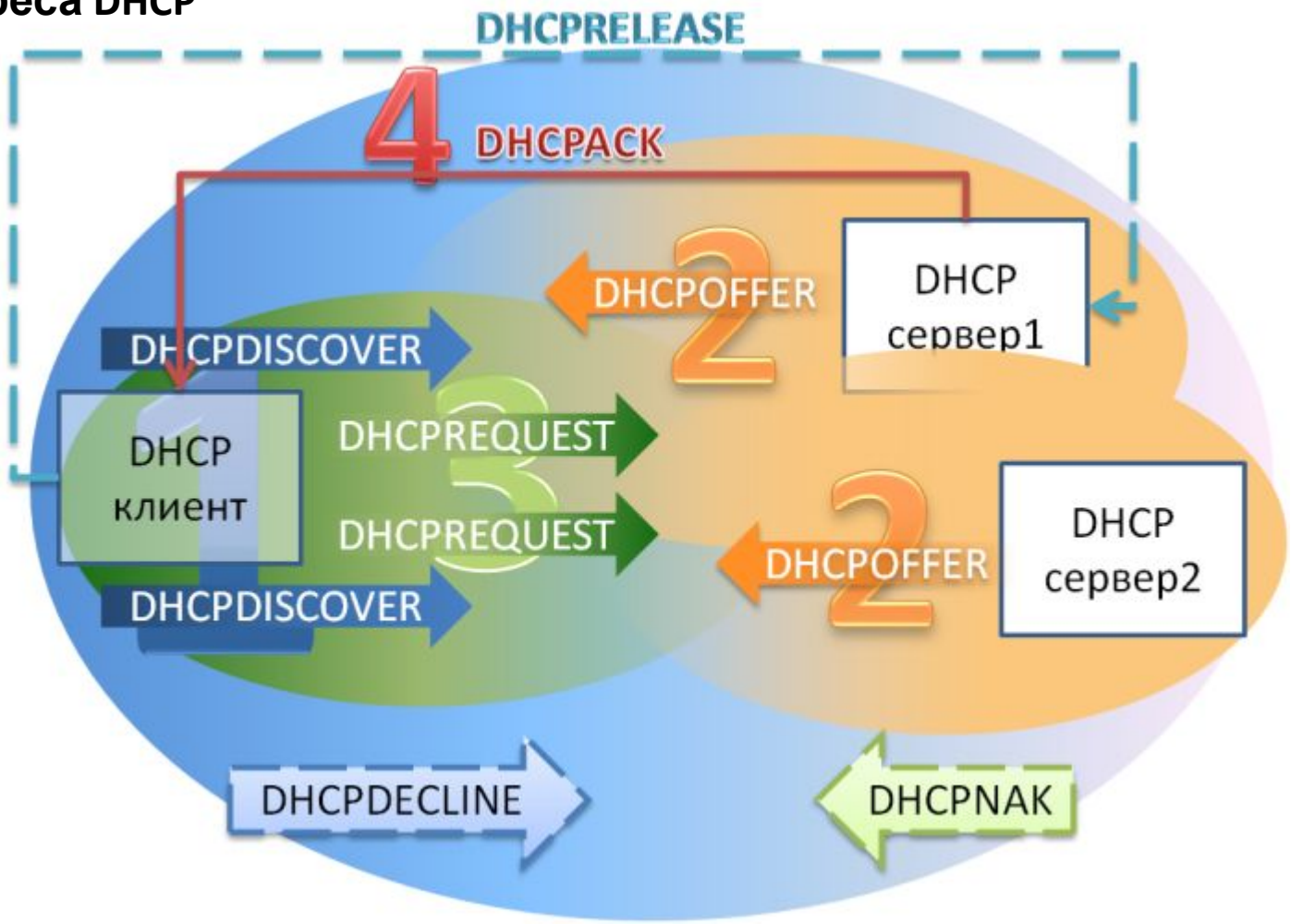
Если после получения подтверждения (**DHCPACK**) от сервера клиент обнаруживает, что указанный сервером адрес уже используется в сети, он рассылает широковещательное сообщение отказа DHCP (**DHCPDECLINE**), после чего процедура получения IP-адреса повторяется.

Отмена от DHCP-сервера (DHCPNAK)



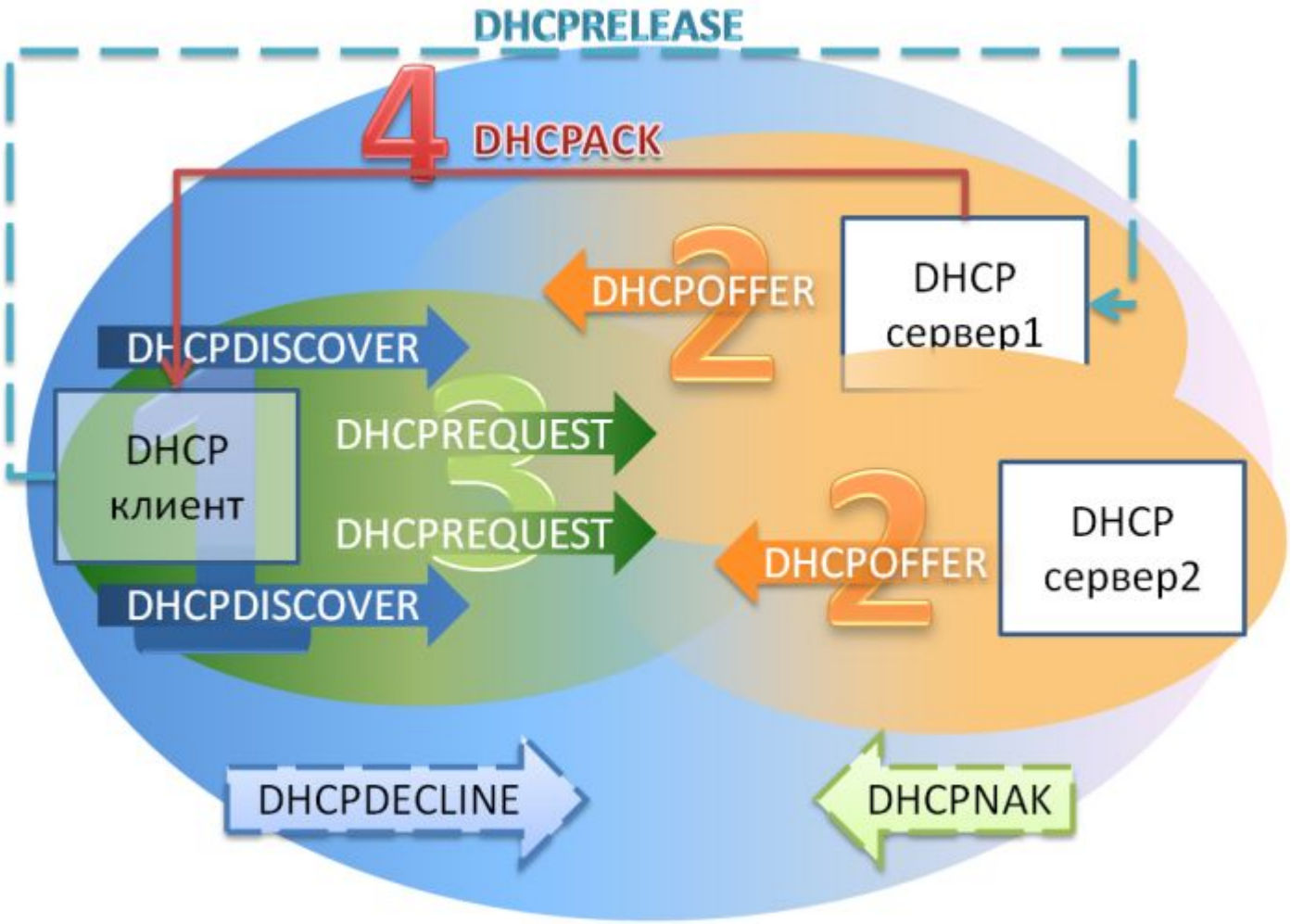
Если по каким-то причинам сервер не может предоставить клиенту запрошенный IP-адрес, или если аренда адреса удаляется администратором, сервер рассылает широковещательное сообщение отмены DHCP (**DHCPNAK**). При получении такого сообщения соответствующий клиент должен повторить процедуру получения адреса.

Освобождение адреса DHCP (DHCPRELEASE)

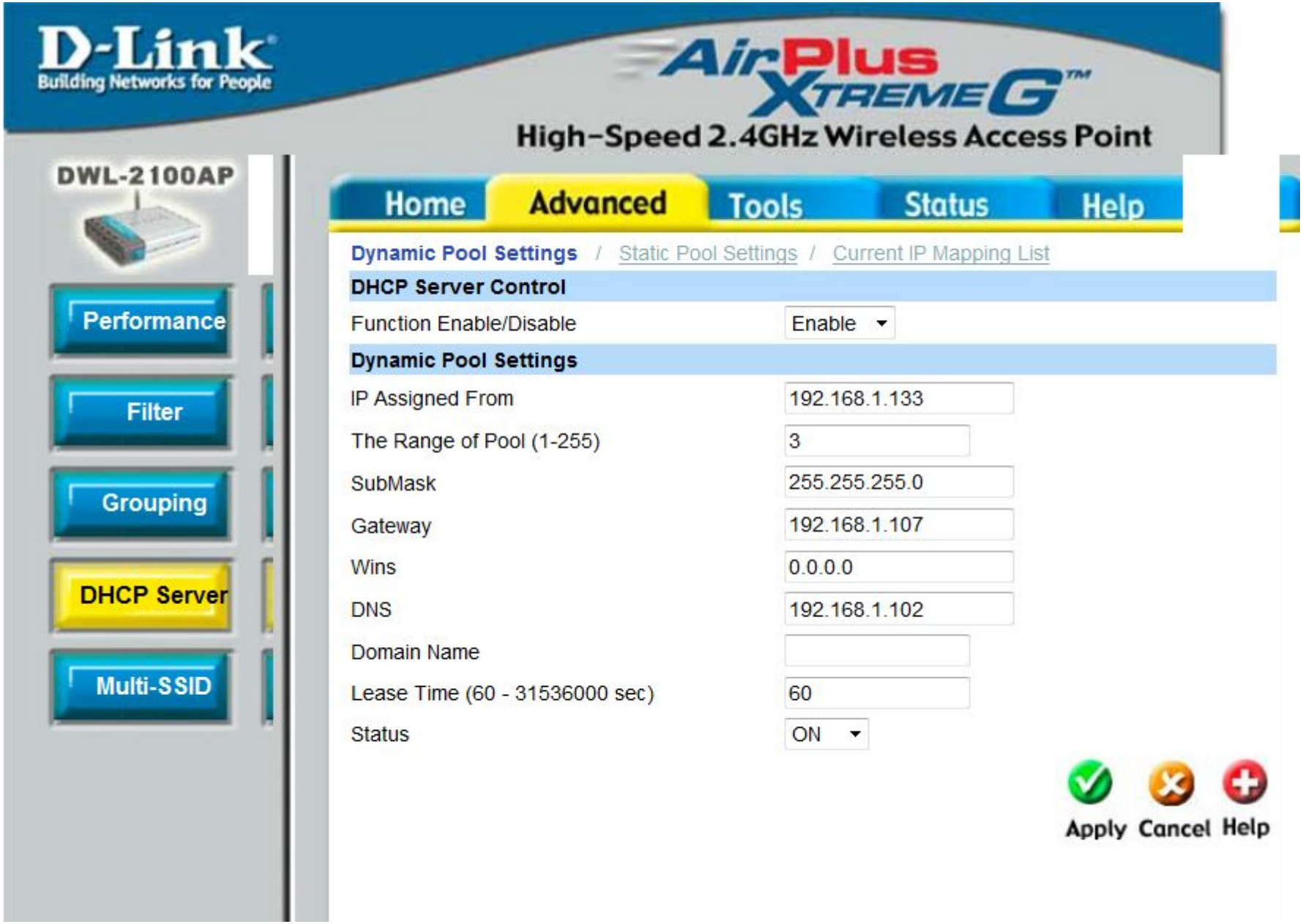


Клиент может явным образом прекратить аренду IP-адреса. Для этого он отправляет сообщение освобождения DHCP (**DHCPRELEASE**) тому серверу, который предоставил ему адрес в аренду.

Информация DHCP (DHCPINFORM)



Сообщение информации DHCP (**DHCPINFORM**) предназначено для определения дополнительных параметров TCP/IP (например, адреса маршрутизатора по умолчанию, DNS-серверов и т. п.) теми клиентами, которым не нужен динамический IP-адрес (то есть адрес которых настроен вручную). Серверы отвечают на такой запрос сообщением подтверждения (**DHCPACK**) без выделения IP-адреса.


D-Link
Building Networks for People
AirPlus XTREME G™
High-Speed 2.4GHz Wireless Access Point
DWL-2100AP
Home
Advanced
Tools
Status
Help
Performance
Filter
Grouping
DHCP Server
Multi-SSID
Dynamic Pool Settings / Static Pool Settings / Current IP Mapping List
DHCP Server Control
Function Enable/Disable
Enable
Dynamic Pool Settings
IP Assigned From
192.168.1.133
The Range of Pool (1-255)
3
SubMask
255.255.255.0
Gateway
192.168.1.107
Wins
0.0.0.0
DNS
192.168.1.102
Domain Name
Lease Time (60 - 31536000 sec)
60
Status
ON
Apply
Cancel
Help

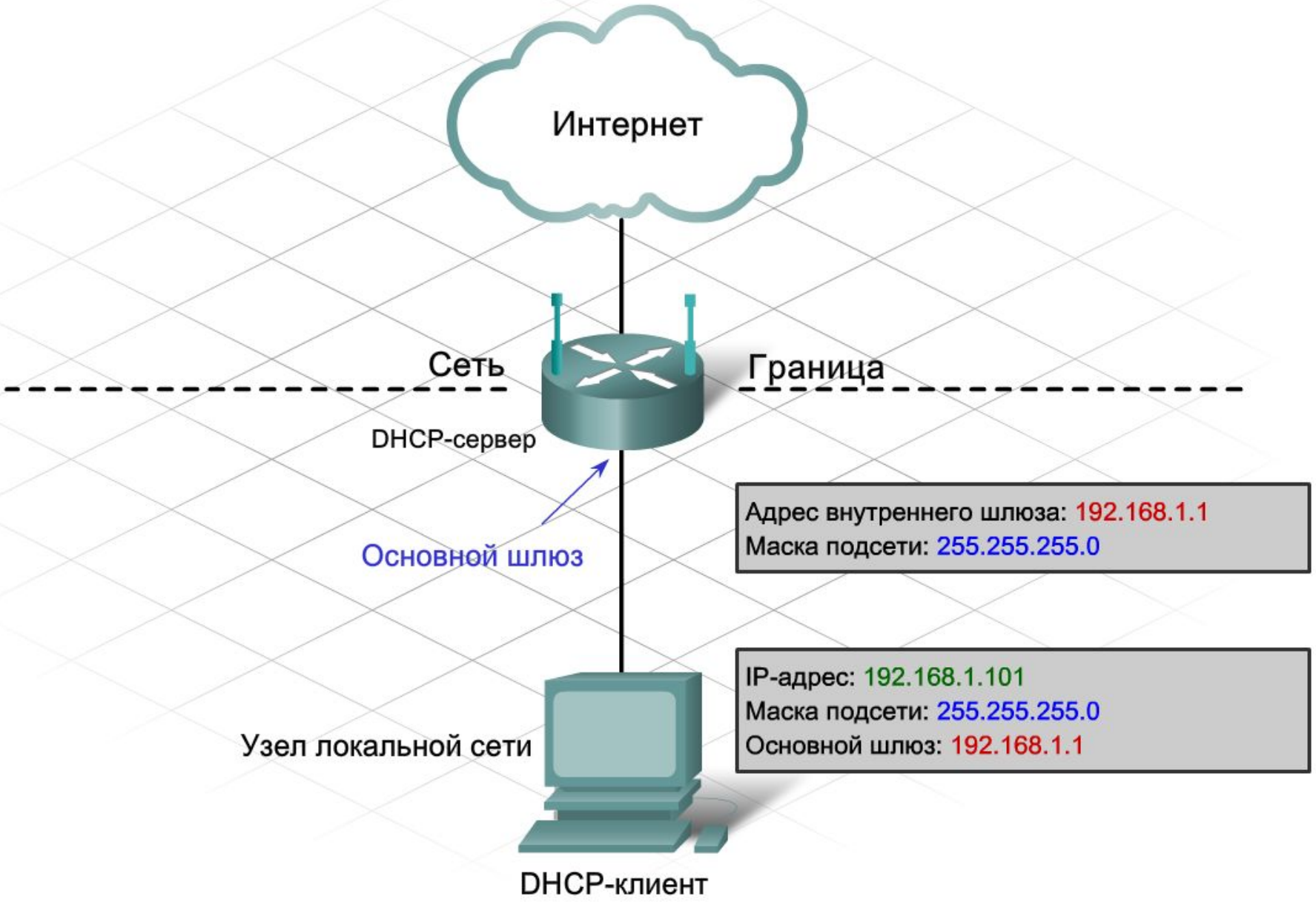
Границы сети и пространство адресов

Маршрутизатор создает шлюз, через который узлы одной сети могут обмениваться данными с узлами других сетей. Каждый интерфейс маршрутизатора подключается к отдельной сети.

Присвоенный интерфейсу IP-адрес идентифицирует непосредственно подключенную локальную сеть.

Каждый узел в сети обязательно использует в качестве шлюза в другие сети маршрутизатор. Соответственно, каждый узел должен знать IP-адрес интерфейса маршрутизатора, подключенного к его сети. Он называется **адресом основного шлюза**. Адрес можно статически настроить на уровне узла или получить динамически, с сервера DHCP.

Границы сети и пространство адресов



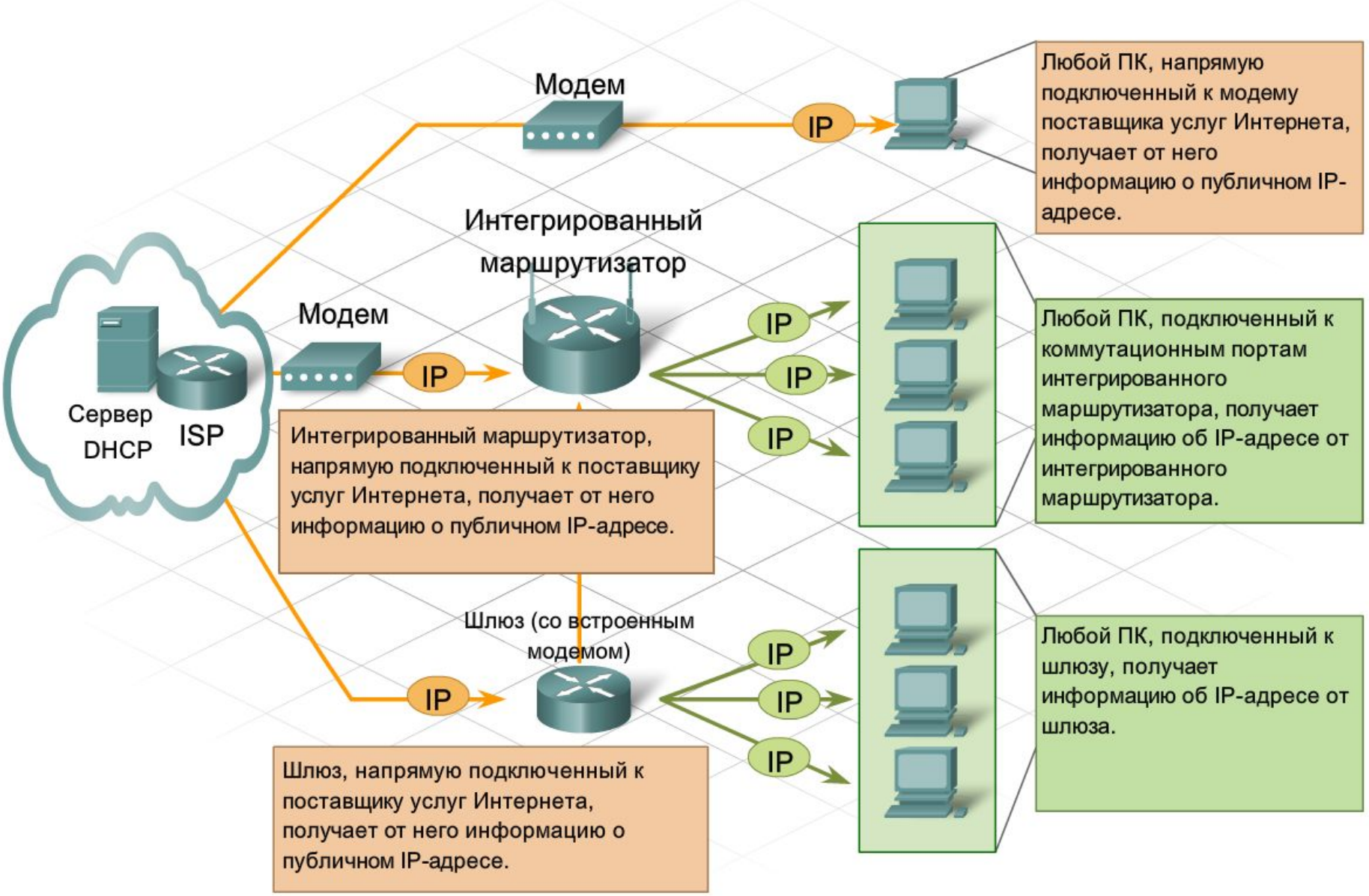
Присвоение адреса

Узлы могут подключаться к поставщику услуг Интернета и Интернету несколькими способами. Получение публичного или частного адреса зависит от метода подключения узла.

Прямое подключение

У некоторых клиентов есть только один компьютер с непосредственным подключением к поставщику услуг Интернета через модем. В данном случае публичный адрес с сервера DHCP поставщика услуг Интернета присваивается только одному узлу.

Присвоение адреса



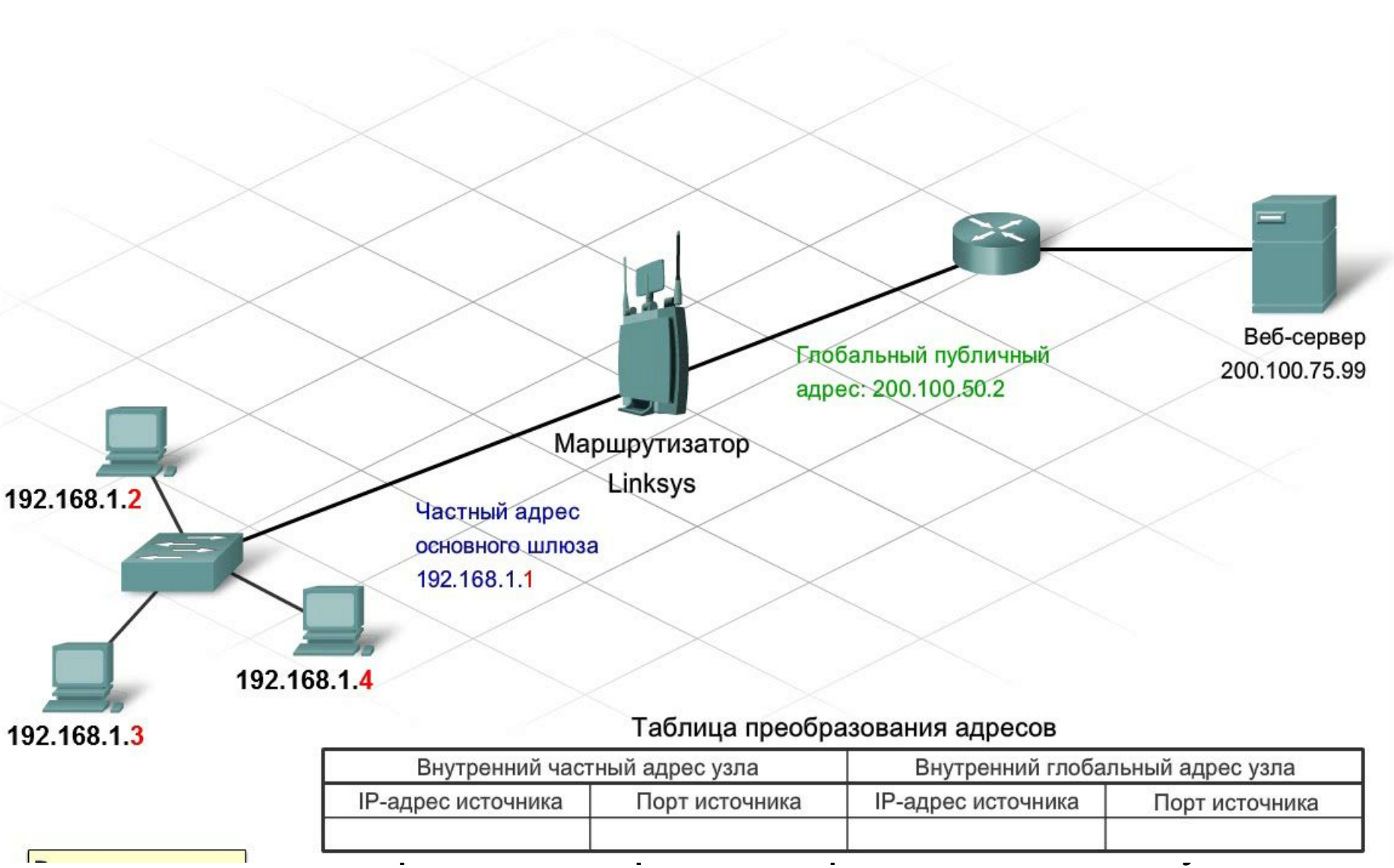


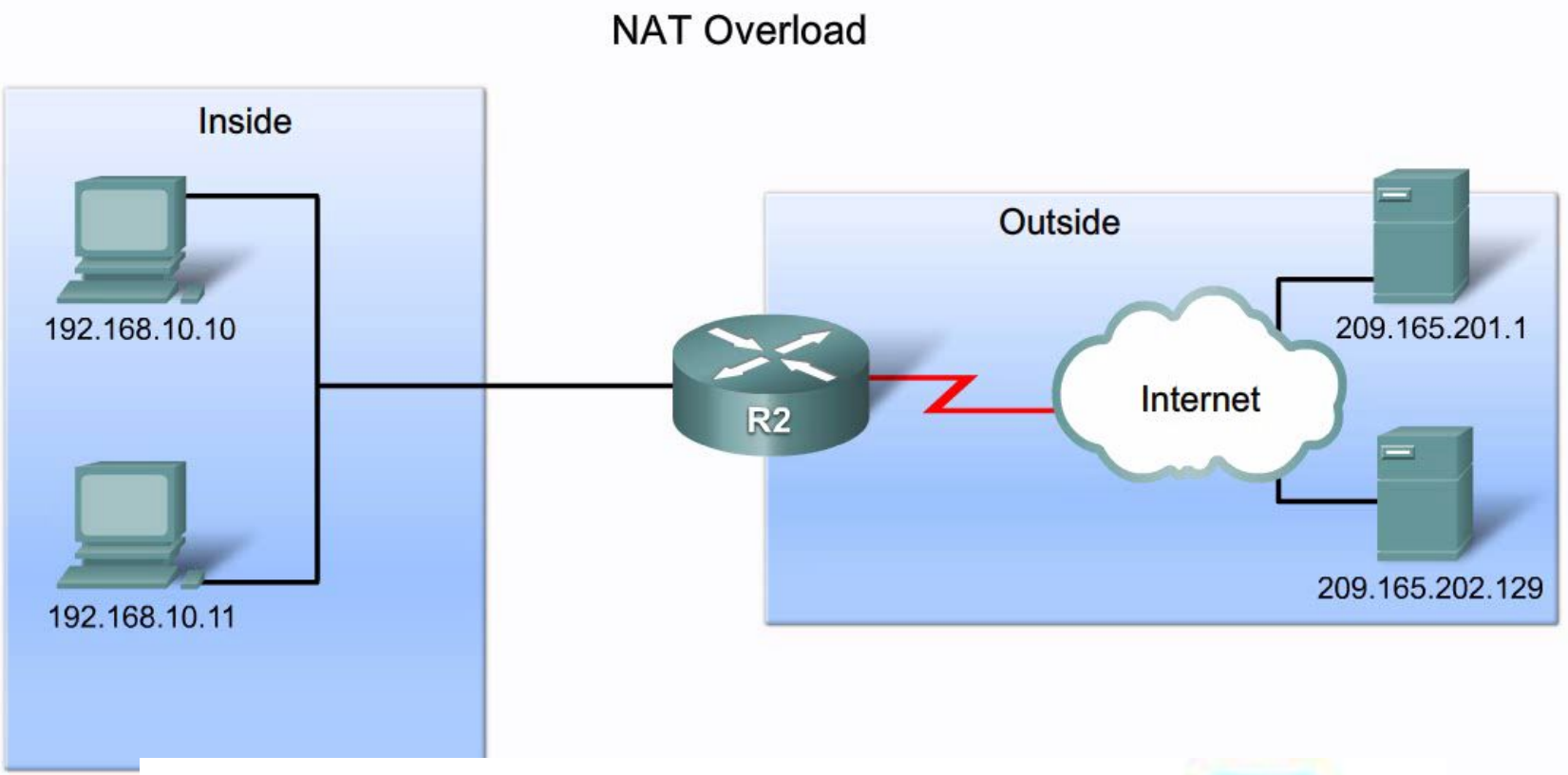
Таблица преобразования адресов

Внутренний частный адрес узла		Внутренний глобальный адрес узла	
IP-адрес источника	Порт источника	IP-адрес источника	Порт источника

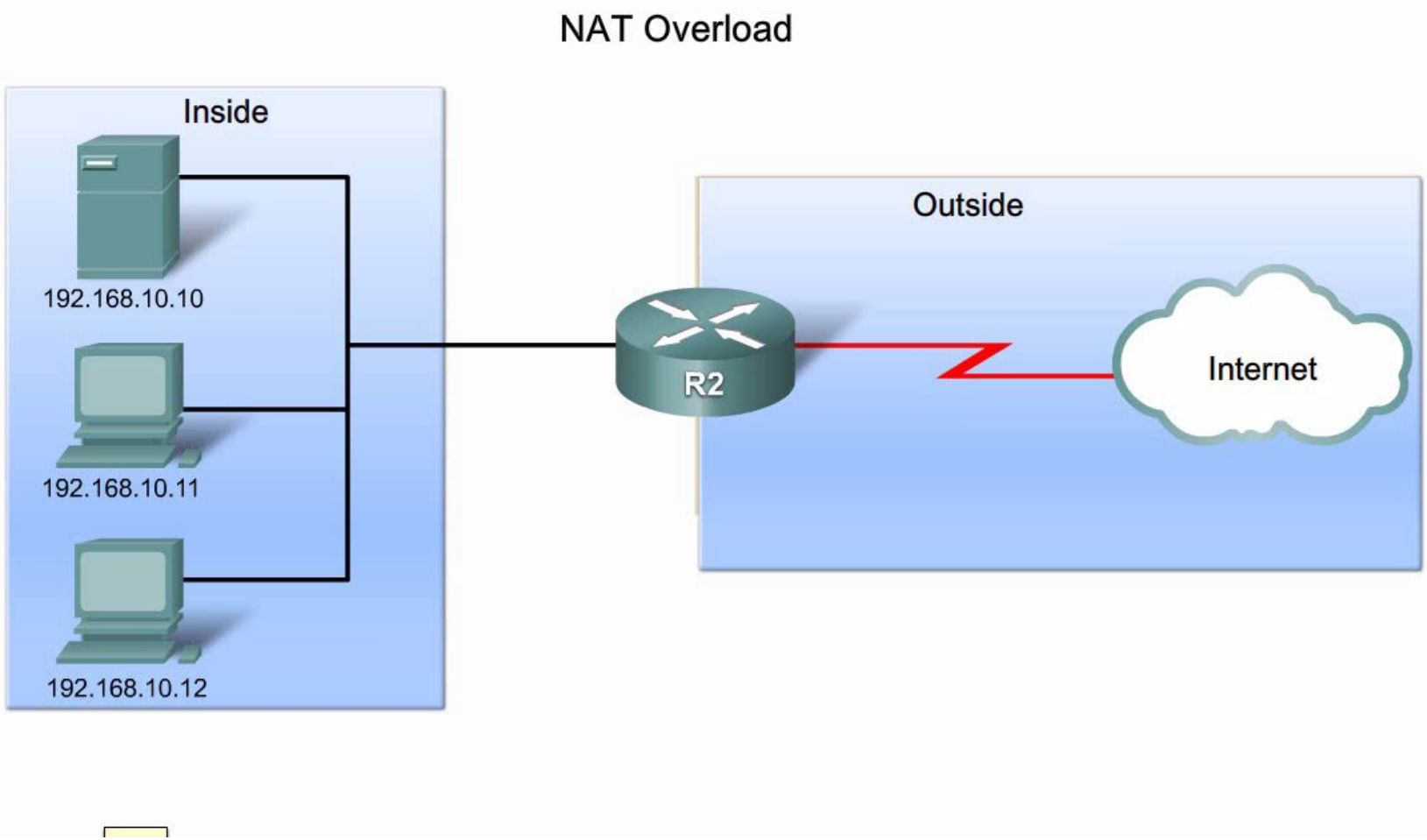
интегрированный маршрутизатор может преобразовать многие внутренние IP-адреса в один публичный.

Хотя каждому узлу во внутренней сети присвоен уникальный частный IP-адрес, они используют **один и тот же**

Перегрузка NAT (NAT Overload)



Перегрузка NAT (NAT Overload)



- V -

IPv6 - адресация

Проблемы с IPv4

Протокол IPv6 разработан как преемник протокола IPv4. В протоколе IPv6 больше 128-битного адресного пространства, что достаточно для 340 ундециллионов адресов. (Это число 340, за которым следует 36 нолей.) Однако IPv6 — не просто большие адреса. Когда специалисты IETF начали разработку преемника IPv4, они использовали эту возможность для устранения ограничений протокола IPv4 и внесения дополнительных улучшений. Среди таких улучшений — протокол управляющих сообщений версии 6 (ICMPv6), который включает в себя разрешение адресов и автонастройку адресов, что отсутствовало в протоколе ICMP для IPv4 (ICMPv4).

Проблемы с IPv4. Потребность в IPv6

31 января 2011г. администрация адресного пространства Интернет IANA назначила последние 2 блока IPv4-адресов /8 региональным Интернет-регистраторам (RIR). Согласно различным прогнозам в период между 2015 и 2020 годами у всех пяти Интернет-регистраторов закончатся IPv4-адреса. Оставшиеся IPv4-адреса будут распределены среди Интернет-провайдеров.

Теоретическое максимальное количество IPv4-адресов — 4,3 миллиарда. Частные адреса RFC 1918 в сочетании с преобразованием сетевых адресов (NAT) служат для замедления истощения адресного пространства IPv4. Преобразование сетевых адресов (NAT) имеет ограничения, которые препятствуют одноранговой связи.

Проблемы с IPv4. Интернет вещей

В будущем Интернет станет неотделим от многих устройств и технического оборудования, в том числе автомобилей и биомедицинских аппаратов, домашней техники и экосистемы. Представьте себе встречу с заказчиком на его территории, которая автоматически запланирована вашим календарным приложением за час до начала обычного рабочего дня. Однако перед встречей вы можете забыть проверить свой календарь или поставить будильник, чтобы встать вовремя, и это повлечёт за собой серьёзные проблемы. Теперь представьте, что календарное приложение напрямую передаёт эту информацию в будильник и автомобиль. Ваша машина автоматически прогреется, чтобы лёд на лобовом стекле растаял прямо перед тем, как вы сядете в машину, а после этого создаст верный маршрут до места встречи.

Проблемы с IPv4. Переход на IPv6

Точно неизвестно, когда мы перейдем на протокол IPv6. В ближайшем будущем протоколы IPv4 и IPv6 будут существовать совместно. Полный переход может занять многие годы. Специалисты IETF создали различные протоколы и инструменты, которые позволяют сетевым администраторам постепенно переводить свои сети на протокол IPv6. Методы перехода можно разделить на 3 категории:

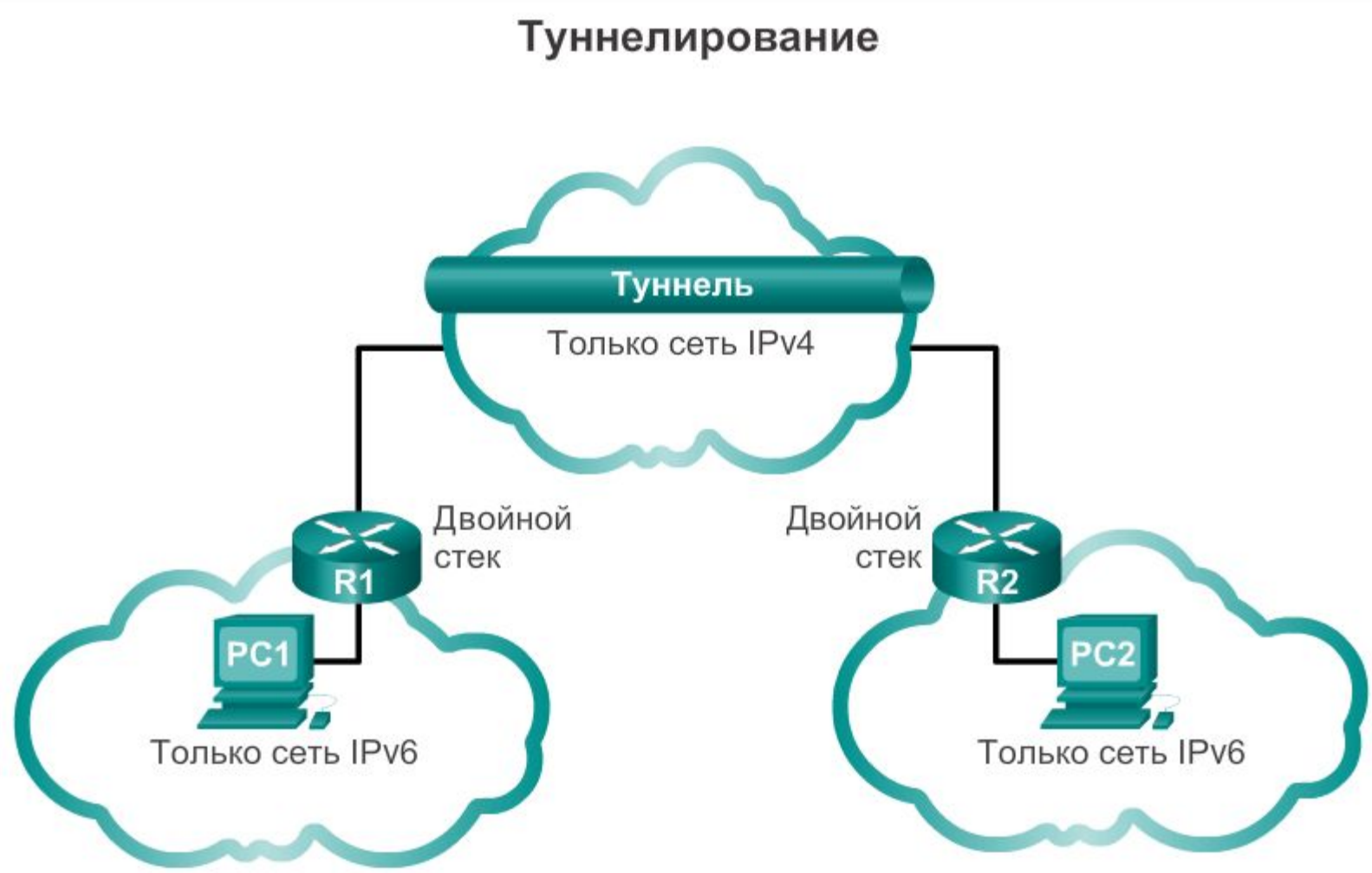
Двойной стек позволяет протоколам IPv4 и IPv6 сосуществовать в одной сети. Устройства с двойным стеком одновременно работают с протокольными стеками IPv4 и IPv6.

Туннелирование – это способ транспортировки IPv6-пакетов через IPv4-сеть. IPv6-пакет инкапсулируется внутри IPv4-пакета, как и другие типы данных.

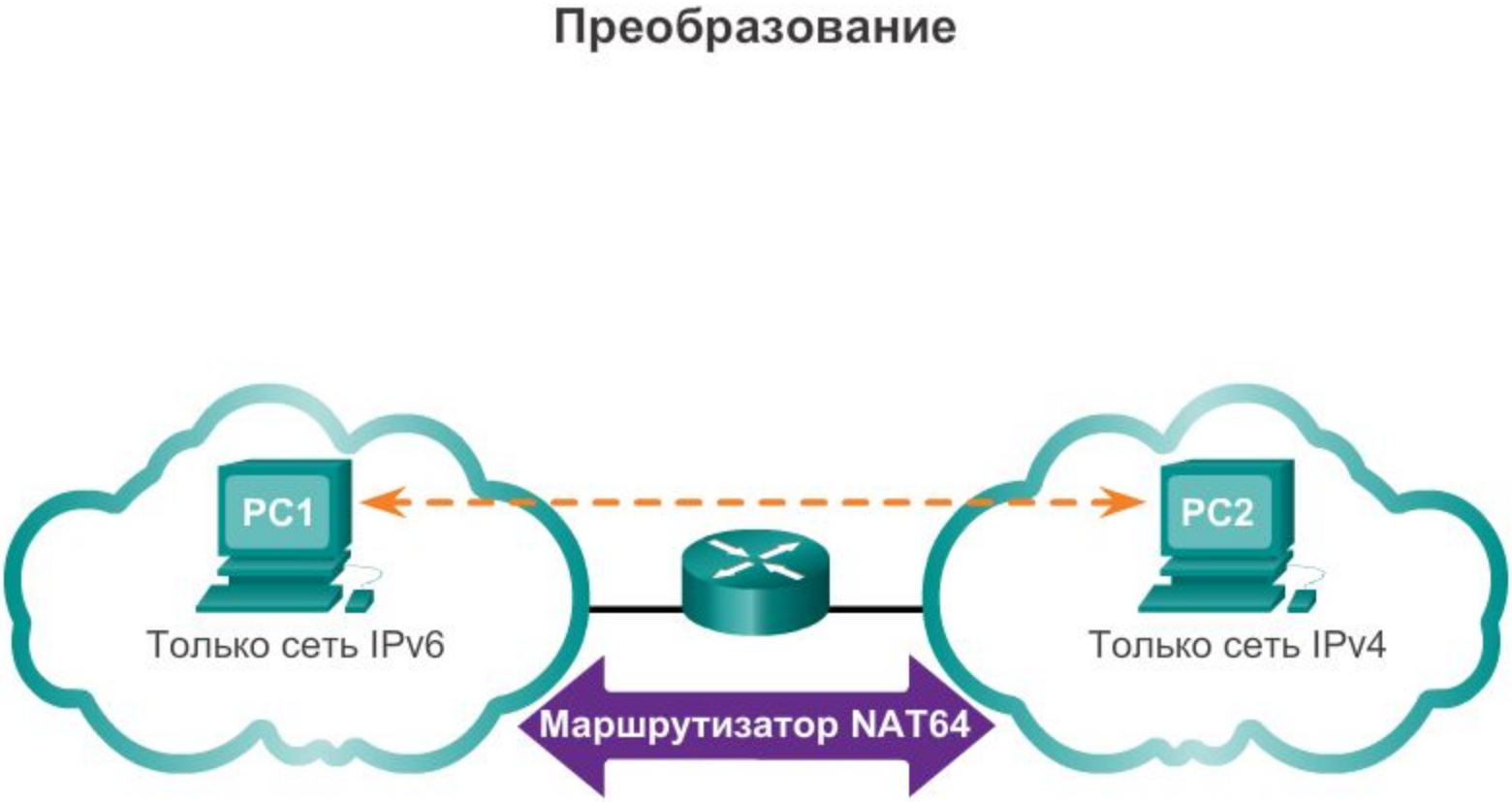
Преобразование сетевых адресов 64 (NAT64) позволяет устройствам под управлением IPv6 обмениваться данными с устройствами под управлением IPv4 с помощью метода преобразования, похожего на метод преобразования из NAT для IPv4. IPv6-пакет преобразовывается в пакет IPv4-пакет и наоборот.

Проблемы с IPv4. Переход на IPv6

Проблемы с IPv4. Переход на IPv6



Проблемы с IPv4. Переход на IPv6



Сетевые IPv6-адреса. Адресация IPv6

В отличие от IPv4-адресов, которые выражены в десятичном формате с разделительными точками, IPv6-адреса представлены с помощью шестнадцатеричных значений. Также шестнадцатеричная система счисления используется для представления адреса управления доступом к среде передачи данных Ethernet (MAC).

Шестнадцатеричная система счисления («Hex») — это удобный способ представления двоичных значений. Так же, как в десятичной системе основанием является 10, в двоичной системе основанием является 2, основание шестнадцатеричной системы счисления — 16.

Система с основанием 16 использует цифры от 0 до 9 и буквы от A до F. Шестнадцатеричная система счисления очень удобна в использовании, поскольку любые четыре бита могут быть представлены одним шестнадцатеричным значением.

Важно отличать шестнадцатеричные значения от десятичных в отношении символов от 0 до 9.

Сетевые IPv6-адреса. Адресация IPv6

Шестнадцатеричное значение обычно представлено в тексте значением, которое располагается после 0x (например, 0x73) или подстрочного индекса 16. В остальных, более редких случаях, за ним может располагаться H (например, 73H). Однако, поскольку подстрочный текст не распознаётся в командной строке или средах программирования, перед техническим представлением шестнадцатеричных значений стоит «0x» (нулевой X). Так, приведённые выше примеры будут отображаться как 0x0A и 0x73 соответственно.

Числовые преобразования между десятичными и шестнадцатеричными значениями не вызывают затруднений, однако быстрое деление или умножение на 16 не всегда удобно.

Обладая определённым опытом, можно распознать шаблоны двоичных разрядов, совпадающих с десятичными и шестнадцатеричными значениями.

Сетевые IPv6-адреса. Адресация IPv6

Шестнадцатеричные преобразования двоичных октетов

Шестнадцатеричное	Десятичное	Двоичное
00	0	0000 0000
01	1	0000 0001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
0A	10	0000 1010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	1000 0000
C0	192	1100 0000
CA	202	1100 1010
F0	240	1111 0000
FF	255	1111 1111

Сетевые IPv6-адреса. Адресация IPv6

Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. Каждые 4 бита представлены одной шестнадцатеричной цифрой, причём общее количество шестнадцатеричных значений равно 32. IPv6-адреса не чувствительны к регистру, их можно записывать как строчными, так и прописными буквами.

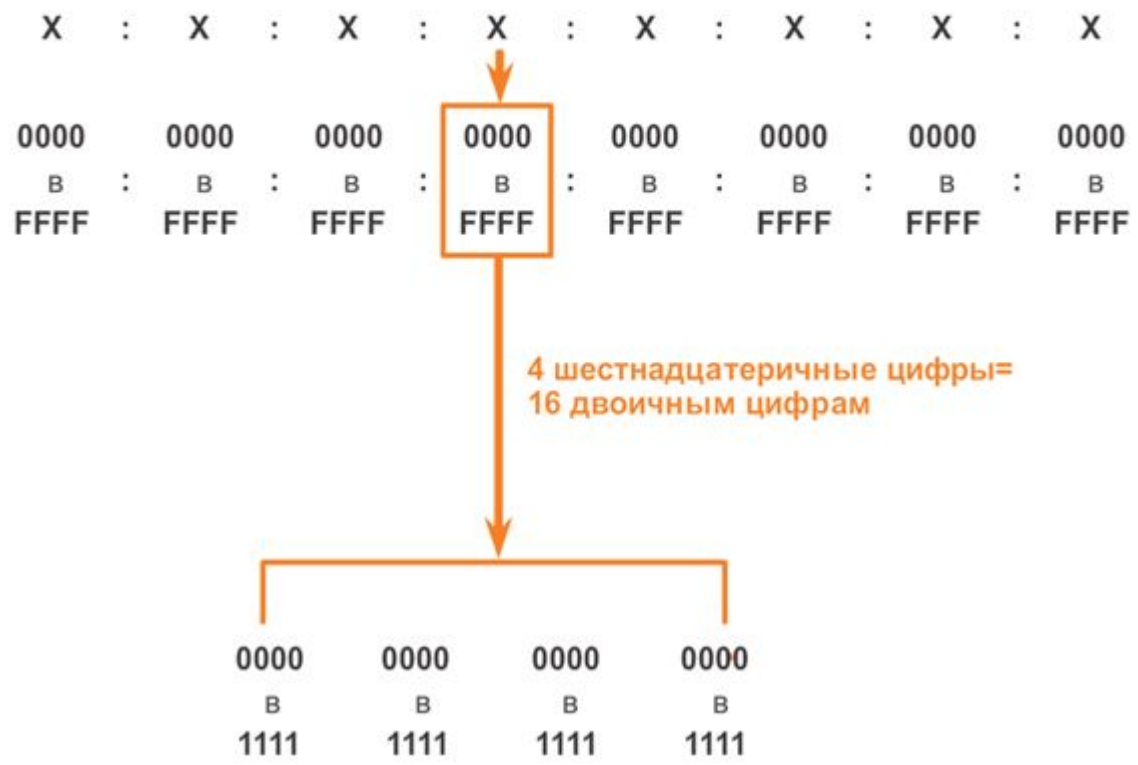
Предпочтительный формат для записи IPv6-адреса

x: x: x: x: x: x: x: x

где каждый «x» состоит из четырёх шестнадцатеричных значений. **Октеты** — это термин, который используется для обозначения 8 бит IPv4-адреса. В IPv6 **хекстет** — это термин, используемый для обозначения сегмента из 16 бит или четырёх шестнадцатеричных значений.

В предпочтительном формате IPv6-адрес записан с помощью 32 шестнадцатеричных цифр. Тем не менее, это не самый оптимальный способ представления IPv6-адреса.

Адресация IPv6. Хекстеты



2001	0DB8	0000	1111	0000	0000	0000	0200
2001	0DB8	0000	00A3	ABCD	0000	0000	1234
2001	0DB8	000A	0001	0000	0000	0000	0100
2001	0DB8	AAAA	0001	0000	0000	0000	0200
FE80	0000	0000	0000	0123	4567	89AB	CDEF
FE80	0000	0000	0000	0000	0000	0000	0001

Сетевые IPv6-адреса. Адресация IPv6

Первое правило для сокращения записи IPv6-адресов – пропуск всех ведущих 0 (нулей) в шестнадцатеричной записи. Например:

01AB можно представить как 1AB
09F0 можно представить как 9F0
0A00 можно представить как A00
00AB можно представить как AB

Это правило применяется только к **ведущим нулям**, а НЕ к последующим, иначе адрес будет записан неясно. Например, шестнадцатеричное число «ABC» может быть представлено как «0ABC» или «ABC0».

Далее рассмотрим примеры того, как пропуск ведущих нулей способствует сокращению размера IPv6-адреса. Для каждого примера показан предпочтительный формат. Обратите внимание, как во многих примерах пропуск ведущих нулей приводит к уменьшенному представлению адреса.

Сетевые IPv6-адреса. Адресация IPv6

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

Предпочтительно	FF02:0000:0000:0000:0000:0001:FF00:0200
Без ведущих нулей	FF02: 0: 0: 0: 0: 1:FF00: 200

Сетевые IPv6-адреса. Адресация IPv6

Второе правило для сокращения записи адресов IPv6 заключается в том, что **двойное двоеточие** (::) может заменить любую **единую, смежную** строку одного или нескольких 16-битных сегментов (хекстетов), состоящих из нулей.

Двойное двоеточие (::) может использоваться в адресе **только один раз**, в противном случае в результате может возникнуть несколько адресов. Сочетание этого правила с методом пропуска нулей помогает значительно сократить запись IPv6-адреса. Это называется сжатым форматом.

Пример неверно сжатого адреса:
2001:0DB8::ABCD::1234
Возможные расширения неоднозначно записанных сжатых адресов:
2001:0DB8::ABCD:0000:0000:1234
2001:0DB8::ABCD:0000:0000:0000:1234
2001:0DB8:0000:ABCD::1234
2001:0DB8:0000:0000:ABCD::1234

Сетевые IPv6-адреса. Адресация IPv6

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

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 ::

Типы IPv6-адресов

Существует три типа IPv6-адресов.

Индивидуальный: служит для определения интерфейса на устройстве под управлением протокола IPv6. Как показано на следующем рисунке, IPv6-адрес источника должен быть индивидуальным.

Групповой: используется для отправки IPv6-пакетов по нескольким адресам назначения.

Произвольный: любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам. Пакет, отправляемый на адрес произвольной рассылки, направляется к ближайшему устройству с этим адресом. Произвольные адреса не рассматриваются в нашем курсе.

В отличие от протокола IPv4, IPv6 **не использует** адрес широковещательной рассылки. Однако есть групповой IPv6-адрес для всех узлов, который даёт аналогичный результат.

Типы IPv6-адресов

Типы IPv6-адресов

Следует помнить, что префикс, или сетевая часть адреса IPv4, может быть обозначен маской подсети в десятичном формате с разделительными точками или длиной префикса (запись с наклонной чертой). Например, IP-адрес 192.168.1.10 с маской подсети в десятичном формате с разделительными точками 255.255.255.0 эквивалентен записи 192.168.1.10/24.

Протокол IPv6 использует длину префикса для обозначения части префикса адреса. IPv6 не использует для маски подсети десятичное представление с разделительными точками. Длина префикса обозначает сетевую часть IPv6-адреса с помощью адреса или длины IPv6-префикса.

Диапазон длины префикса может составлять от 0 до 128. Традиционная длина IPv6-префикса для локальных и других типов сетей — /64. Это означает, что длина префикса, или сетевая часть адреса, составляет 64 бита, а оставшиеся 64 бита остаются для идентификатора интерфейса (узловой части) адреса.

Типы IPv6-адресов

Типы IPv6-адресов

Индивидуальный адрес служит для определения интерфейса устройства под управлением протокола IPv6. Пакет, который отправляется на индивидуальный адрес, будет получен интерфейсом, присвоенным для этого адреса. Как и в случае с протоколом IPv4, IPv6-адрес должен быть индивидуальным. IPv6-адрес назначения может быть как индивидуальным, так и групповым.

Существует шесть типов индивидуальных IPv6-адресов:

Глобальный индивидуальный адрес

Глобальный индивидуальный адрес мало чем отличается от публичного IPv4-адреса. Эти адреса, к которым можно проложить маршрут по Интернету, являются уникальными по всему миру. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически. В динамическом назначении IPv6-адреса устройством имеются некоторые важные отличия по сравнению с динамическим назначением IPv4-адреса.

Типы IPv6-адресов

Локальный адрес канала

Локальные адреса канала используются для обмена данными с другими устройствами по одному локальному каналу. В протоколе IPv6 термин «канал» означает подсеть. Локальные адреса каналов ограничены одним каналом. Они должны быть уникальны только в рамках этого канала, поскольку вне канала к ним нельзя проложить маршрут. Другими словами, маршрутизаторы не смогут пересылать пакеты, имея локальный адрес канала источника или назначения.

Логический интерфейс loopback

Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 состоит из нулей, за исключением последнего бита, который выглядит как ::1/128 или просто ::1 в сжатом формате.

Типы IPv6-адресов

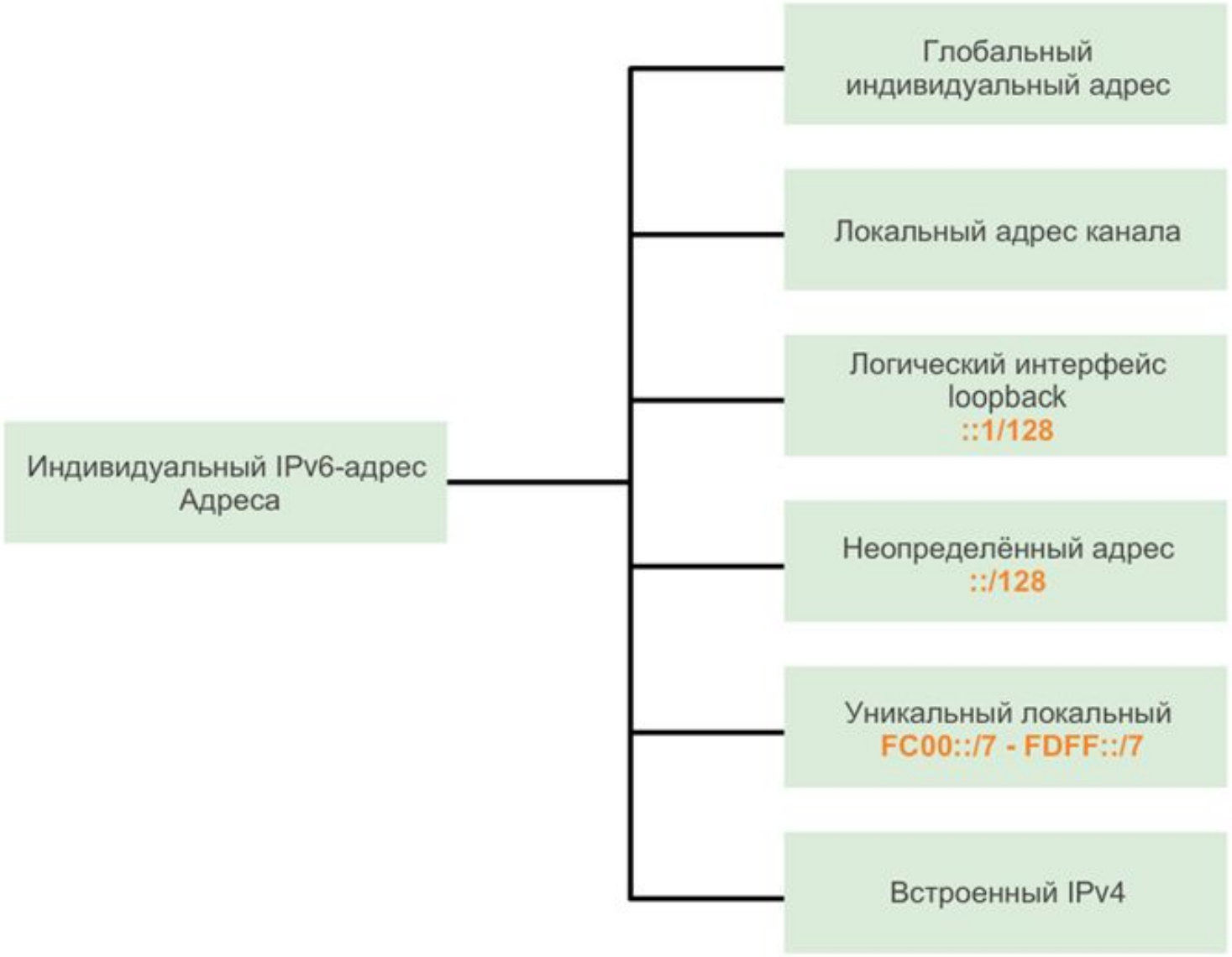
Неопределённый адрес

Неопределённый адрес состоит из нулей и в сжатом формате представлен как ::/128 или просто :: Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес или когда источник пакета не относится к месту назначения.

Уникальный локальный адрес

Уникальные локальные IPv6-адреса имеют некоторые общие особенности с частными адресами RFC 1918 для IPv4, но при этом между ними имеются и значительные различия. Уникальные локальные адреса используются для локальной адресации в пределах узла или между ограниченным количеством узлов. Эти адреса не следует маршрутизировать в глобальном протоколе IPv6. Уникальные локальные адреса находятся в диапазоне от FC00::/7 до FDFF::/7.

Типы IPv6-адресов



Типы IPv6-адресов

Локальный IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 по одному и тому же каналу и только по данному каналу (подсети). Пакеты с локальным адресом канала источника или назначения не могут быть направлены за пределы того канала, в котором пакет создаётся.

В отличие от локальных IPv4-адресов канала, локальные адреса канала IPv6 играют важную роль в различных аспектах сети. Глобальный индивидуальный адрес не обязателен. Однако для содержания локального адреса канала необходим сетевой интерфейс под управлением протокола IPv6.

Если локальный адрес канала не настроен вручную на интерфейсе, устройство автоматически создаёт собственный адрес, не обращаясь к DHCP-серверу. Узлы под управлением IPv6 создают локальный IPv6-адрес канала даже в том случае, если устройству не был назначен глобальный IPv6-адрес. Это позволяет устройствам под управлением IPv6 обмениваться данными с другими устройствами под управлением IPv6 в одной

Типы IPv6-адресов

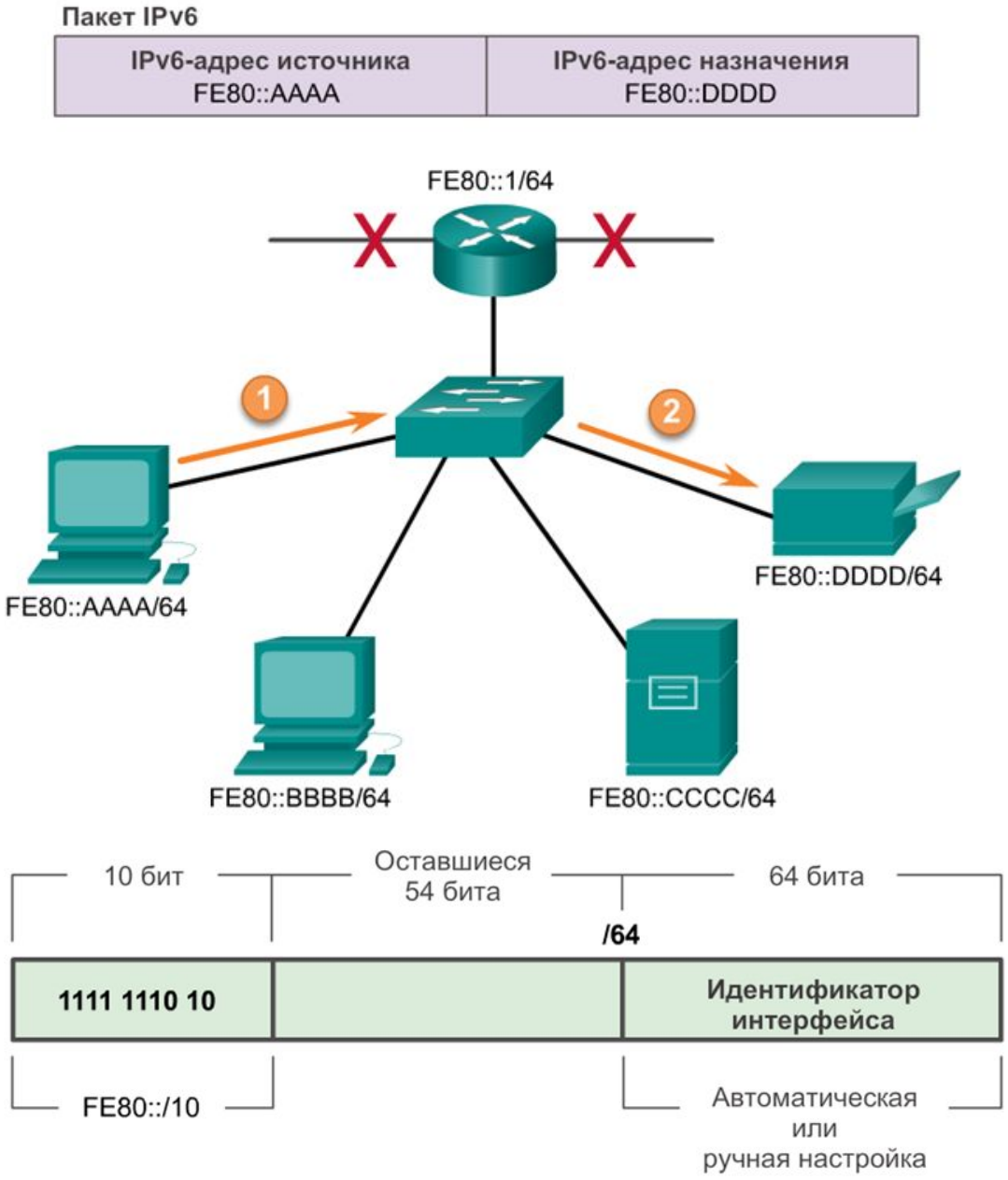
Локальные IPv6-адреса канала находятся в диапазоне FE80::/10. /10 указывает на то, что первые 10 бит — 1111 1110 10xx xxxx. Первый хекстет имеет диапазон от 1111 1110 1000 0000 (FE80) до 1111 1110 1011 1111 (FEBF).

Далее рассмотрим пример коммуникации с помощью локальных IPv6-адресов и формат локального IPv6-адреса.

Локальные IPv6-адреса также используются IPv6-протоколами маршрутизации для обмена сообщениями, а также в качестве следующего адреса пересылки в IPv6-таблице маршрутизации.

Примечание: Как правило, в качестве шлюза по умолчанию для других устройств в канале используется локальный адрес маршрутизатора, а не глобальный индивидуальный адрес.

Типы IPv6-адресов



Типы IPv6-адресов

Глобальные индивидуальные IPv6-адреса уникальны по всему миру и доступны для маршрутизации через Интернет IPv6. Эти адреса эквивалентны публичным IPv4-адресам. Ассоциация по присвоению имен и номеров Интернета (ICANN), оператор Администрации адресного пространства Интернет (IANA), выделяет блоки IPv6-адресов пяти региональным интернет-регистраторам (RIR). В настоящее время назначаются только глобальные индивидуальные адреса с первыми тремя битами 001 или 2000::/3. Это лишь 1/8 от всего доступного адресного пространства IPv6, за исключением очень незначительного количества других типов адресов индивидуальных и групповых адресов.

Примечание: Адрес 2001:0DB8::/32 был зарезервирован для документации, в том числе для использования в примерах.

Типы IPv6-адресов

Глобальный индивидуальный адрес состоит из трёх частей:

- Префикс глобальной маршрутизации
- Идентификатор подсети
- Идентификатор интерфейса

Типы IPv6-адресов

Префикс глобальной маршрутизации — это префиксальная или сетевая часть адреса, назначаемая Интернет-провайдером заказчику или узлу. В настоящее время /48 является префиксом глобальной маршрутизации, который Интернет-регистраторы сейчас назначают своим заказчикам — корпоративным сетям и индивидуальным пользователям. Этого адресного пространства более чем достаточно для большинства заказчиков.

Рассмотрим для примера структуру глобальных индивидуальных адресов, использующих префикс глобальной маршрутизации /48. Префиксы /48 — наиболее распространённые назначаемые префиксы глобальной маршрутизации, которые будут использоваться в большинстве примеров в рамках нашего курса.

Например, IPv6-адрес 2001:0DB8:ACAD::/48 обладает префиксом, который обозначает, что первые 48 бит (3 хекстета) (2001:0DB8:ACAD) — это префиксальная или сетевая часть адреса. Двойное двоеточие (::) перед длиной префикса /48 означает, что остальные адреса состоят из нулей.

Типы IPv6-адресов

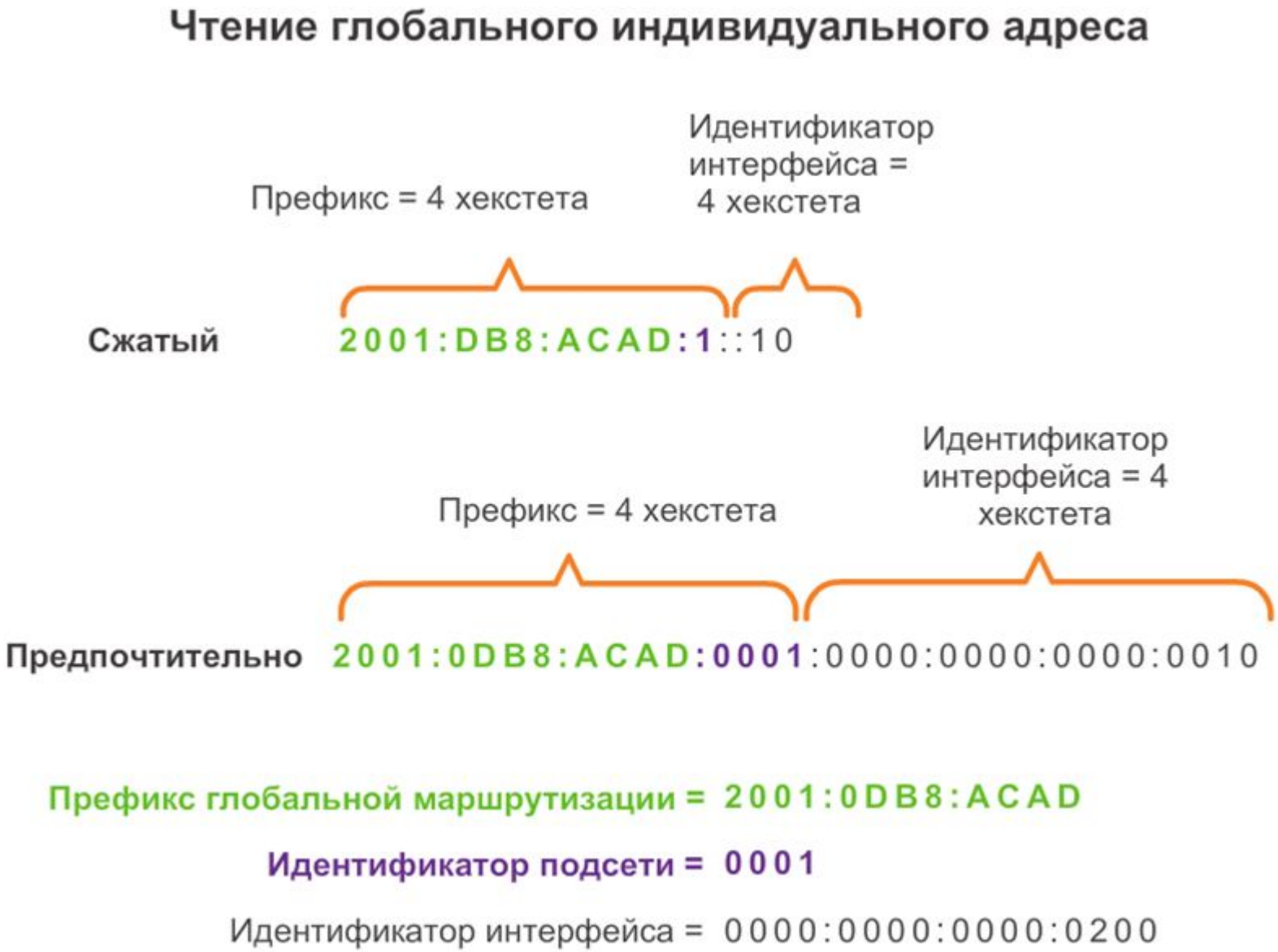
Типы IPv6-адресов

Идентификатор подсети используется организациями для обозначения подсетей в каждом узле.

Идентификатор IPv6-интерфейса эквивалентен узловой части адреса IPv4-адреса. Термин «идентификатор интерфейса» используется в том случае, когда один узел может иметь несколько интерфейсов, каждый из которых обладает одним или более IPv6-адресами.

Примечание: В отличие от IPv4, при использовании протокола IPv6 устройству можно назначить адрес узла, состоящий из одних 0 или из одних 1. Адрес из одних 1 можно использовать по той причине, что в протоколе IPv6 не используются широковещательные адреса. Можно также использовать адрес из одних 0, но он зарезервирован в качестве адреса произвольной рассылки Subnet-Router, и его следует назначать только маршрутизаторам.

Типы IPv6-адресов



Типы IPv6-адресов

Идентификатор подсети используется организациями для обозначения подсетей в каждом узле.

Идентификатор IPv6-интерфейса эквивалентен узловой части адреса IPv4-адреса. Термин «идентификатор интерфейса» используется в том случае, когда один узел может иметь несколько интерфейсов, каждый из которых обладает одним или более IPv6-адресами.

Примечание: В отличие от IPv4, при использовании протокола IPv6 устройству можно назначить адрес узла, состоящий из одних 0 или из одних 1. Адрес из одних 1 можно использовать по той причине, что в протоколе IPv6 не используются широковещательные адреса. Можно также использовать адрес из одних 0, но он зарезервирован в качестве адреса произвольной рассылки Subnet-Router, и его следует назначать только маршрутизаторам.

Индивидуальные IPv6-адреса. Конфигурация маршрутизатора

Большинство команд конфигурации и проверки IPv6 в Cisco IOS похожи на свои IPv4-аналоги. В большинстве случаев единственная разница между ними — использование в командах ipv6 вместо ip.

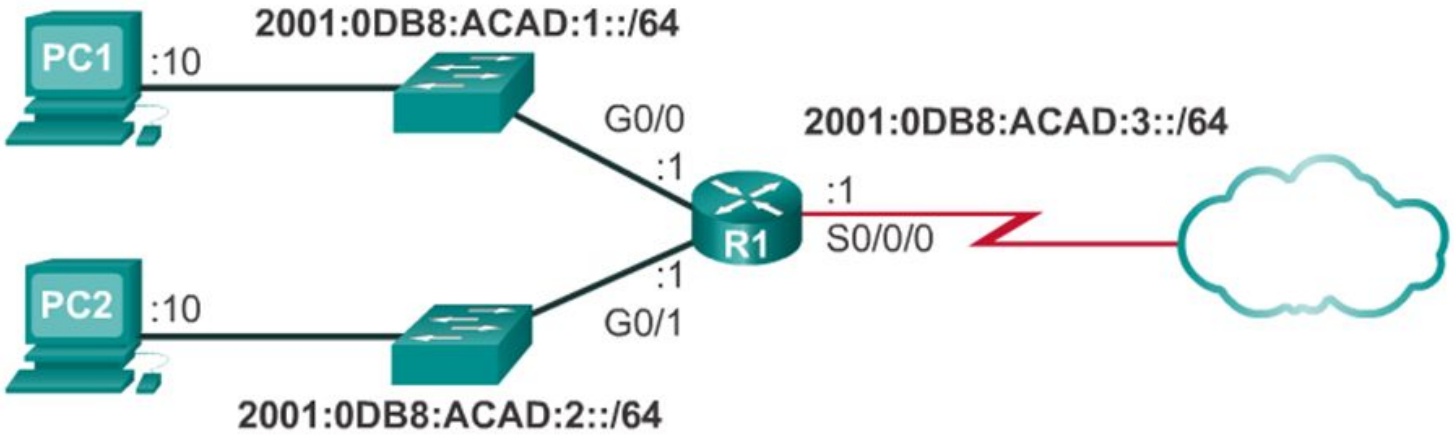
Для настройки глобального индивидуального IPv6-адреса в интерфейсе используется команда из группы interface, которая выглядит следующим образом: ipv6 address ipv6-address/prefix-length.

Обратите внимание, что между ipv6-address и prefix-length отсутствует пробел.

Для примера настройки используется топология, показанная на следующем слайде, и следующие IPv6-подсети:

2001:0DB8:ACAD:0001:/64 (или 2001:DB8:ACAD:1:: /64)
2001:0DB8:ACAD:0002:/64 (или 2001:DB8:ACAD:2:: /64)

Типы IPv6-адресов




```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```

Индивидуальные IPv6-адреса. SLAAC

Автоконфигурация без сохранения состояния адреса (**SLAAC**, **Stateless address autoconfiguration**) – это способ, который позволяет устройству получить свой префикс, длину префикса и адрес шлюза по умолчанию от маршрутизатора IPv6 без помощи DHCPv6-сервера. При использовании SLAAC для получения необходимой информации устройства полагаются на сообщения «Объявления маршрутизатора ICMPv6».

IPv6-маршрутизаторы периодически отправляют сообщения «Объявления маршрутизатора ICMPv6» всем устройствам в сети под управлением IPv6. По умолчанию маршрутизаторы Cisco отправляют такие сообщения каждые 200 секунд на адрес групповой передачи всем IPv6-узлам. IPv6-устройству, находящемуся в сети, не нужно ждать этих периодических сообщений. Устройство может отправить сообщение «Запрос маршрутизатора ICMPv6», который использует адрес групповой передачи всем IPv6-узлам. Когда маршрутизатор IPv6 получает такое сообщение, он сразу же отправляет в ответ объявление маршрутизатора.

Индивидуальные IPv6-адреса. SLAAC

Несмотря на то, что интерфейс маршрутизатора Cisco можно настроить с IPv6-адресом, это не превращает его в «IPv6-маршрутизатор». IPv6-маршрутизатор обладает следующими характеристиками.

1. пересылает IPv6-пакеты между сетями.
2. может быть настроен со статическими IPv6-маршрутами или с динамическим IPv6-протоколом маршрутизации.
3. Отправляет сообщения «Объявления маршрутизатора ICMPv6».

IPv6-маршрутизация не включена по умолчанию. Чтобы маршрутизатор работал как IPv6-маршрутизатор, необходимо использовать команду глобальной конфигурации ipv6 unicast-routing.

Примечание: Маршрутизаторы Cisco по умолчанию работают как IPv4-маршрутизаторы.

Индивидуальные IPv6-адреса. SLAAC

Сообщение «Объявления маршрутизатора ICMPv6» содержит префикс, длину префикса и другие сведения IPv6-устройства. Кроме того, такое сообщение указывает IPv6-устройству, как ему получить информацию по адресации. Сообщение «Объявления маршрутизатора» может выглядеть в одном из следующих 3 вариантов.

Варианты объявлений маршрутизатора

Вариант 1 (только SLAAC) — «Я предоставлю все необходимые вам данные (префикс, длину префикса и шлюз по умолчанию)»
Вариант 2 (SLAAC и DHCPv6) — «Вот моя информация, но вам понадобятся и другие данные, например об DNS-адресах с сервера DHCPv6».
Вариант 3 (только DHCPv6) — «Я не могу вам помочь. Запросите необходимую информацию у сервера DHCPv6».

Индивидуальные IPv6-адреса. SLAAC

Сообщения «Запрос к маршрутизатору» и «Объявление от маршрутизатора»

Варианты объявлений маршрутизатора

Вариант 1 (только SLAAC) — «Я предоставлю все необходимые вам данные (префикс, длину префикса и шлюз по умолчанию)»
Вариант 2 (SLAAC и DHCPv6) — «Вот моя информация, но вам понадобятся и другие данные, например об DNS-адресах с сервера DHCPv6».
Вариант 3 (только DHCPv6) — «Я не могу вам помочь. Запросите необходимую информацию у сервера DHCPv6».

Индивидуальные IPv6-адреса. SLAAC

Вариант 1: только SLAAC. Устройство должно использовать префикс, длину префикса и шлюз по умолчанию, которые содержатся в сообщении «Объявления маршрутизатора». Другая информация недоступна с DHCPv6-сервера.

Вариант 2: SLAAC и DHCPv6. Устройство должно использовать префикс, длину префикса и шлюз по умолчанию, которые содержатся в сообщении «Объявления маршрутизатора». На DHCPv6-сервере доступна и другая информация, например адрес DNS-сервера. Устройство получит эту дополнительную информацию в процессе поисков и запросов к DHCPv6-серверу. Этот процесс называется «DHCPv6 без запоминания состояний», поскольку DHCPv6-серверы не выделяют и не отслеживают какие-либо назначения IPv6-адресов, а предоставляют дополнительную информацию, например об адресе DNS-сервера.

Индивидуальные IPv6-адреса. SLAAC

Вариант 3: только DHCPv6. Устройство не должно использовать информацию из сообщения «Объявления маршрутизатора» для пополнения своей информации об адресации. Вместо этого устройство будет использовать обычные процессы поисков и запросов к DHCPv6-серверам для получения всей своей информации об адресации. Такая информация включает в себя индивидуальный адрес IPv6, длину префикса, адрес шлюза по умолчанию и адреса DNS-серверов. В этом случае DHCPv6-сервер работает как DHCP-сервер, который фиксирует данные аналогично DHCP-серверу для IPv4. DHCPv6-сервер выделяет и отслеживает IPv6-адреса, чтобы не назначать один и тот же IPv6-адрес на нескольких устройствах.

Маршрутизаторы отправляют сообщения «Объявления маршрутизатора ICMPv6», используя локальный адрес канала в качестве IPv6-адреса источника. Устройства, использующие SLAAC, применяют локальные адреса маршрутизатора в качестве адреса шлюза по умолчанию.

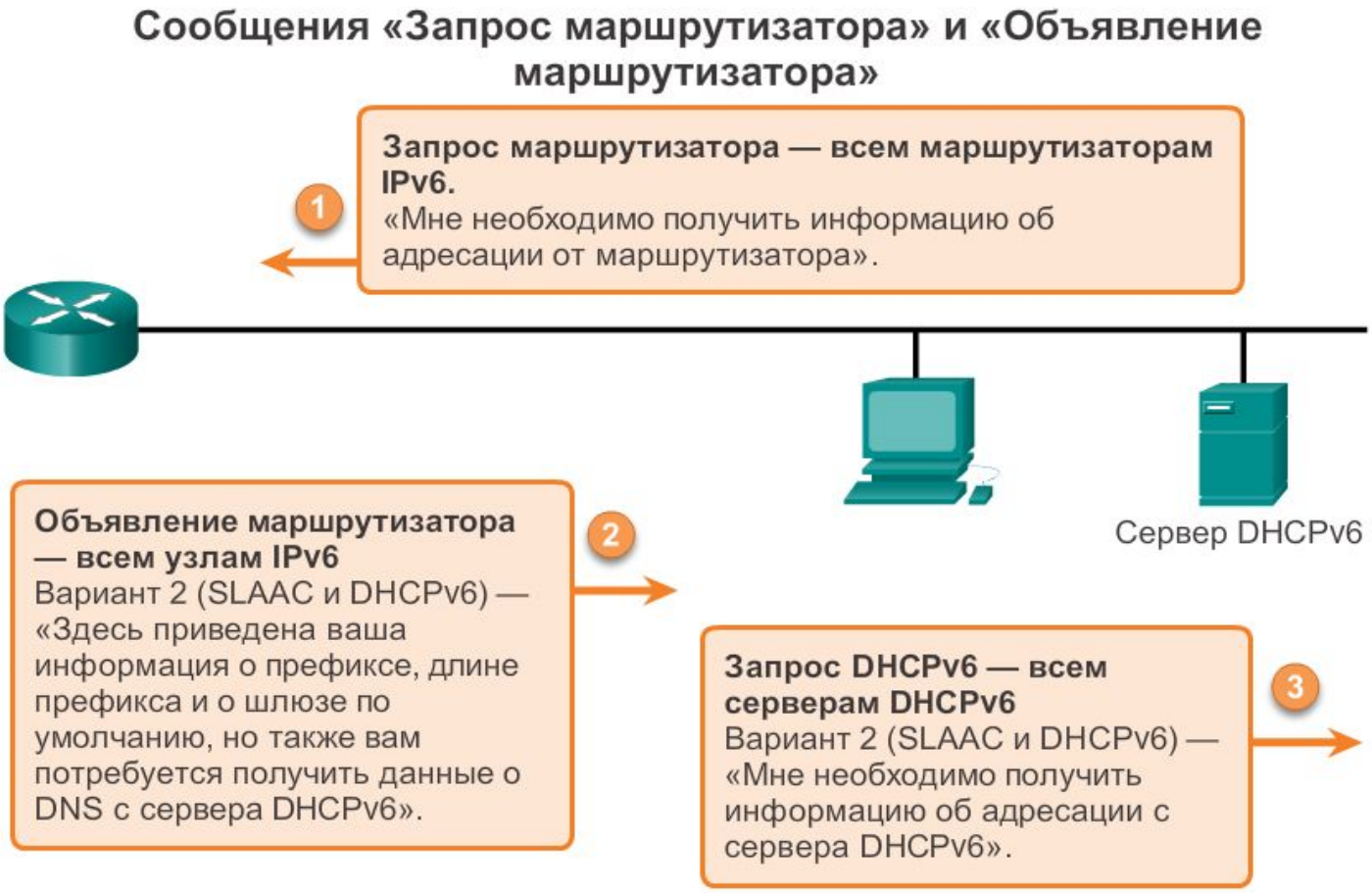
Индивидуальные IPv6-адреса. DHCPv6

Протокол динамической конфигурации сетевого узла для IPv6 (DHCPv6) работает по тем же принципам, что и DHCP-протокол для IPv4. Устройство может автоматически получить свою информацию об адресации, включая глобальный индивидуальный адрес, длину префикса, адрес шлюза по умолчанию и адреса DNS-серверов, с помощью сервисов DHCPv6-сервера.

Устройство может получить всю или часть своей информации об IPv6-адресации с DHCPv6-сервера в зависимости от того, в каком из вариантов представлено объявление маршрутизатора ICMPv6: в варианте 2 (SLAAC и DHCPv6) или в варианте 3 (только DHCPv6). Кроме того, ОС узла может предпочесть проигнорировать любую информацию в сообщении «Объявления маршрутизатора» и получить IPv6-адрес и другие данные непосредственно с DHCPv6-сервера.

Перед развёртыванием IPv6-устройств в сети рекомендуется проверить, соблюдает ли узел варианты в сообщении

Индивидуальные IPv6-адреса. DHCPv6



Примечание. При выборе сообщения «Объявление маршрутизатора» вариант 3 (только DHCPv6) клиенту потребуется получить всю информацию с сервера DHCPv6.

Индивидуальные IPv6-адреса. DHCPv6

Устройство может получить свой индивидуальный IPv6-адрес динамически, а также может быть настроено с несколькими статическими IPv6-адресами на аналогичном интерфейсе. IPv6-протокол разрешает на одном интерфейсе настройку нескольких IPv6-адресов, принадлежащих к одной IPv6-сети.

Также устройство может быть настроено с одним или несколькими IPv6-адресами шлюза по умолчанию. Для получения дополнительной информации о том, каким образом определяется, какой адрес используется в качестве IPv6-адреса источника или какой используется адрес шлюза по умолчанию, см. документ RFC 6724 «Выбор адреса по умолчанию для IPv6».

Индивидуальные IPv6-адреса. DHCPv6

Идентификатор интерфейса

Если клиент не использует информацию, приведённую в объявлении маршрутизатора, и полагается исключительно на DHCPv6-сервер, то DHCPv6-сервер должен предоставить весь глобальный индивидуальный IPv6-адрес, включая префикс и идентификатор интерфейса.

Однако если используется вариант 1 (только SLAAC) или вариант 2 (SLAAC с DHCPv6), то клиент не получает фактическую часть идентификатора интерфейса адреса из этих процессов. Клиентское устройство должно определить собственный 64-битный идентификатор интерфейса либо с помощью расширенного уникального идентификатора EUI-64, либо путём создания случайного 64-битного числа.

Индивидуальные IPv6-адреса. Процесс EUI-64

Организация IEEE разработала **расширенный уникальный идентификатор** (EUI) или изменённый процесс EUI-64. Этот процесс использует 48-битный MAC-адрес Ethernet клиента и в середину этого адреса вставляет ещё 16 бит для создания 64-битного идентификатора интерфейса.

MAC-адреса Ethernet обычно представлены в шестнадцатеричном формате и состоят из двух частей:

Уникальный идентификатор организации (OUI) — это 24-битный (шесть шестнадцатеричных цифр) код поставщика, назначенный IEEE.

Идентификатор устройства — это уникальное 24-битное (6 шестнадцатеричных цифр) значение с общим уникальным идентификатором организации (OUI).

Индивидуальные IPv6-адреса. Процесс EUI-64

Идентификатор интерфейса в формате EUI-64 представлен в двоичном формате и состоит из трёх частей:

24-битный OUI на основе MAC-адреса клиента, в котором седьмой бит является обратным, т.е. если седьмой бит имеет значение 0, то он становится 1, и наоборот.

В середину вставляется 16-битное значение FFFE (в шестнадцатеричной системе счисления)

24-битный идентификатор устройства на основе MAC-адреса клиента

Индивидуальные IPv6-адреса. Процесс EUI-64

Процесс EUI-64 проиллюстрирован далее с помощью MAC-адреса маршрутизатора R1 GigabitEthernet FC99:4775:CEE0.

Шаг 1: разделите MAC-адрес между OUI и идентификатором устройства.

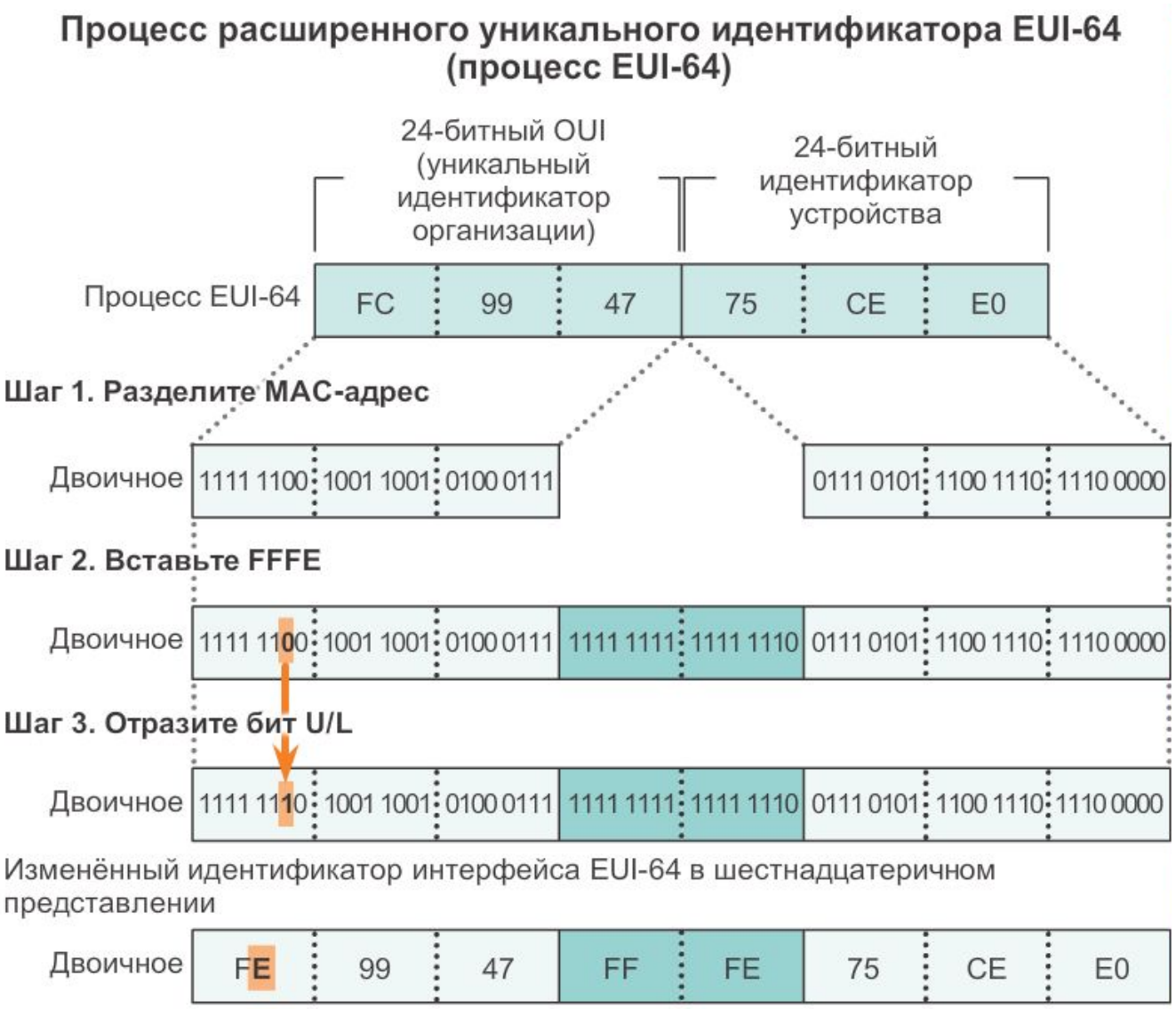
Шаг 2: вставьте шестнадцатеричное значение FFFE в двоичном формате: 1111 1111 1111 1110.

Шаг 3: преобразуйте первые 2 шестнадцатеричных значения уникального идентификатора организации (OUI) в двоичный формат и отразите бит U/L (бит 7). В данном случае 0 в седьмом бите меняется на 1.

В результате генерируется следующий EUI-64 идентификатор интерфейса FE99: 47FF:FE75:CEE0.

Примечание: Использование обратного бита (U/L) и причины для отражения его значения описаны в документе RFC 5342.

Индивидуальные IPv6-адреса. Процесс EUI-64



Индивидуальные IPv6-адреса. Процесс EUI-64

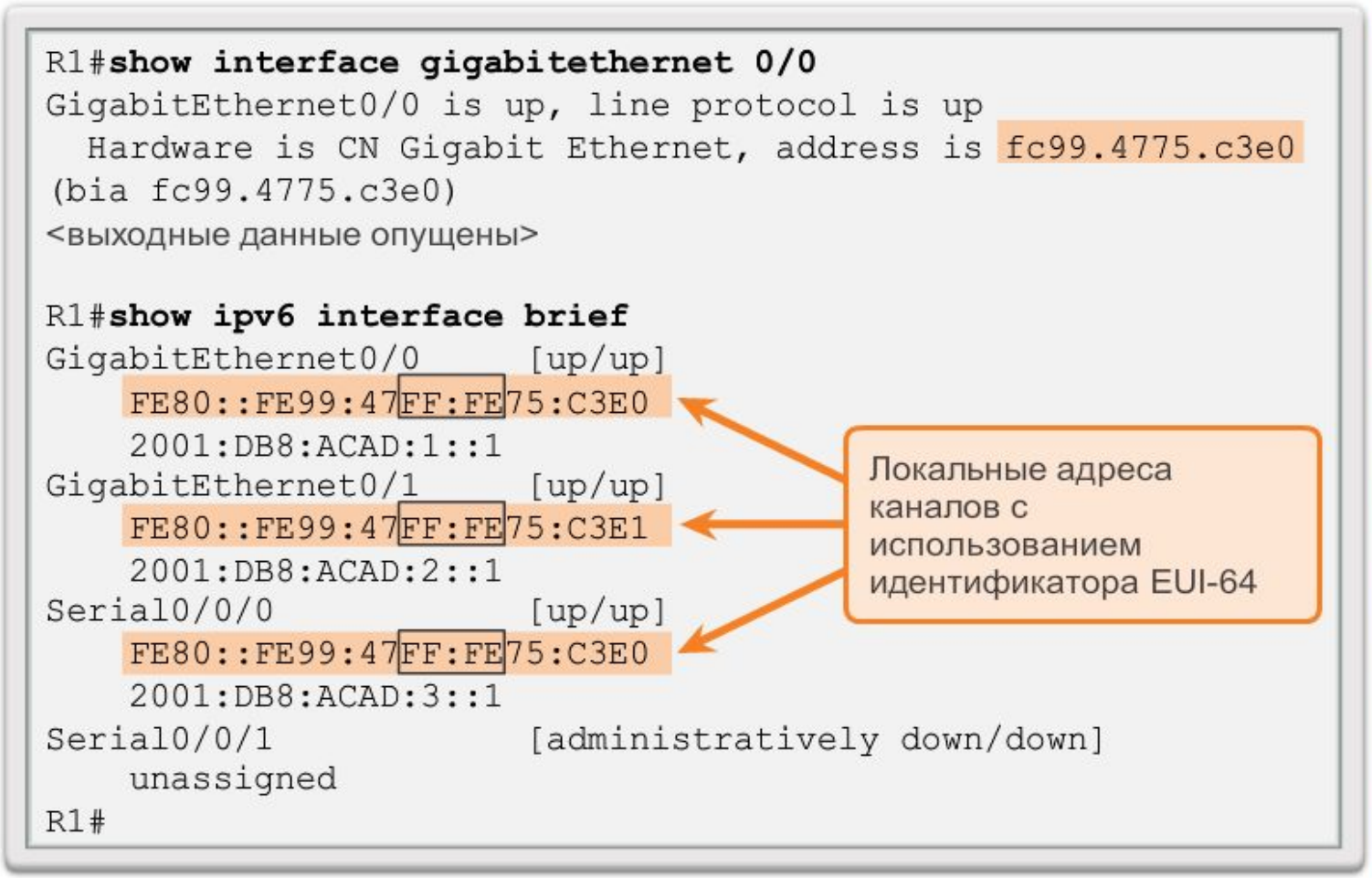
Преимущество EUI-64 MAC-адреса Ethernet заключается в том, что его можно использовать для определения идентификатора интерфейса. Кроме того, сетевые администраторы могут легко отслеживать IPv6-адрес до конечных устройств с помощью уникального MAC-адреса. Однако это беспокоит других пользователей в связи с угрозой их конфиденциальности. Они обеспокоены тем, что их пакеты можно отследить до физического компьютера. Чтобы избежать таких осложнений, можно использовать случайно сгенерированный идентификатор интерфейса.

Случайно сгенерированные идентификаторы интерфейса

В зависимости от операционной системы устройство может использовать случайно сгенерированный идентификатор интерфейса вместо MAC-адресов и EUI-64. Например, начиная с Windows Vista в операционных системах Windows используется случайно сгенерированный идентификатор интерфейса вместо созданного через EUI-64. В ОС Windows XP и в предыдущих операционных системах Windows использовался EUI-64.

Индивидуальные IPv6-адреса. Процесс EUI-64

Как показано на рисунке, чтобы без труда определить, что адрес был создан с помощью EUI-64, нужно поместить FFFE в середину идентификатора интерфейса.



Индивидуальные IPv6-адреса. Процесс EUI-64

После установления идентификатора интерфейса либо с помощью EUI-64, либо через случайную генерацию его можно объединить с префиксом IPv6 для создания глобального индивидуального адреса или локального адреса канала.

- Глобальный индивидуальный адрес. При использовании SLAAC устройство получает свой префикс из объявления маршрутизатора ICMPv6 и объединяет его с идентификатором интерфейса.

- Локальный адрес канала. Локальный префикс начинается с FE80:: /10. Обычно в качестве префикса и длины префикса устройство использует FE80:: /64, за которым следует идентификатор интерфейса

Индивидуальные IPv6-адреса

При использовании варианта SLAAC (только SLAAC или SLAAC с DHCPV6) устройство получает префикс и длину префикса из объявления маршрутизатора ICMPv6. Поскольку префикс адреса был назначен объявлением маршрутизатора, устройство должно обеспечивать только часть идентификатора интерфейса своего адреса. Как было упомянуто ранее, идентификатор интерфейса может быть сгенерирован автоматически с помощью процесса EUI-64 или, в зависимости от ОС, сгенерирован произвольно. С помощью информации из объявления маршрутизатора и идентификатора интерфейса устройство может установить свой глобальный индивидуальный адрес.

После назначения интерфейсу глобального индивидуального адреса устройство под управлением IPv6 автоматически создаёт свой локальный адрес канала. Устройства под управлением IPv6 должны иметь как минимум локальный адрес канала. Как вы помните, локальный IPv6-адрес позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 в одной и той же подсети.

Индивидуальные IPv6-адреса

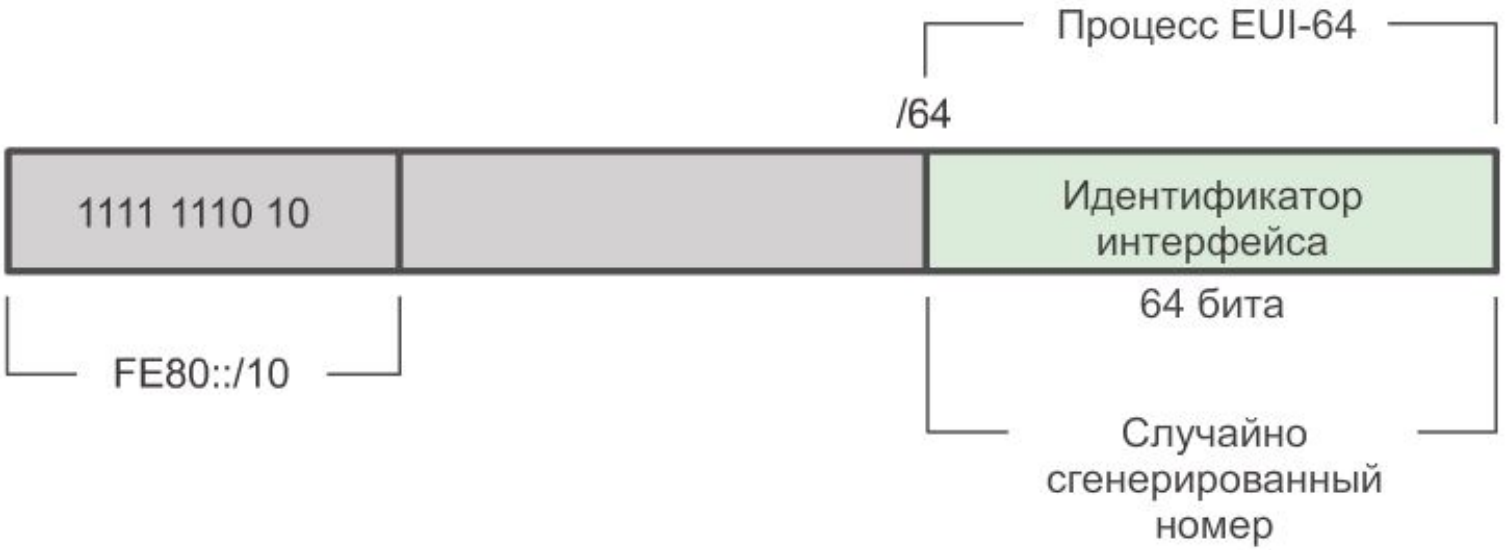
Локальные IPv6-адреса используются для различных целей, указанных ниже.

1. Узел использует локальный адрес канала локального маршрутизатора для IPv6-адреса шлюза по умолчанию.
2. Маршрутизаторы используют локальные адреса канала для обмена сообщениями протокола динамической маршрутизации.
3. Таблицы маршрутизации маршрутизаторов используют локальный адрес канала для определения маршрутизатора следующего перехода при передаче IPv6-пакетов.

Локальный адрес канала можно настроить динамически или настроить вручную в качестве статического локального адреса канала.

Индивидуальные IPv6-адреса

Локальный IPv6-адрес канала



Индивидуальные IPv6-адреса

Динамическое назначение локального адреса канала

Локальный адрес канала динамически создаётся с помощью префикса FE80:: /10 и идентификатора интерфейса.

По умолчанию маршрутизаторы Cisco IOS используют EUI-64 для создания идентификатора интерфейса для всех локальных адресов канала в IPv6-интерфейсах. Для последовательных интерфейсов маршрутизатор будет использовать MAC-адрес интерфейса Ethernet. Помните, что локальный адрес канала должен быть уникальным только в данном канале или сети. Однако недостаток использования динамически назначенного локального адреса канала — это его длина, которая затрудняет определение и запоминание назначенных адресов.

Индивидуальные IPv6-адреса

Статические локальные адреса канала

Ручная настройка локального адреса канала позволяет создавать адрес, который легче узнать и запомнить.

Локальные адреса каналов можно настраивать вручную с помощью аналогичной команды, которая использовалась для создания глобальных индивидуальных IPv6-адресов, но с дополнительным параметром:

```
Router(config-if)#ipv6 address link-local-address link-local
```

Индивидуальные IPv6-адреса

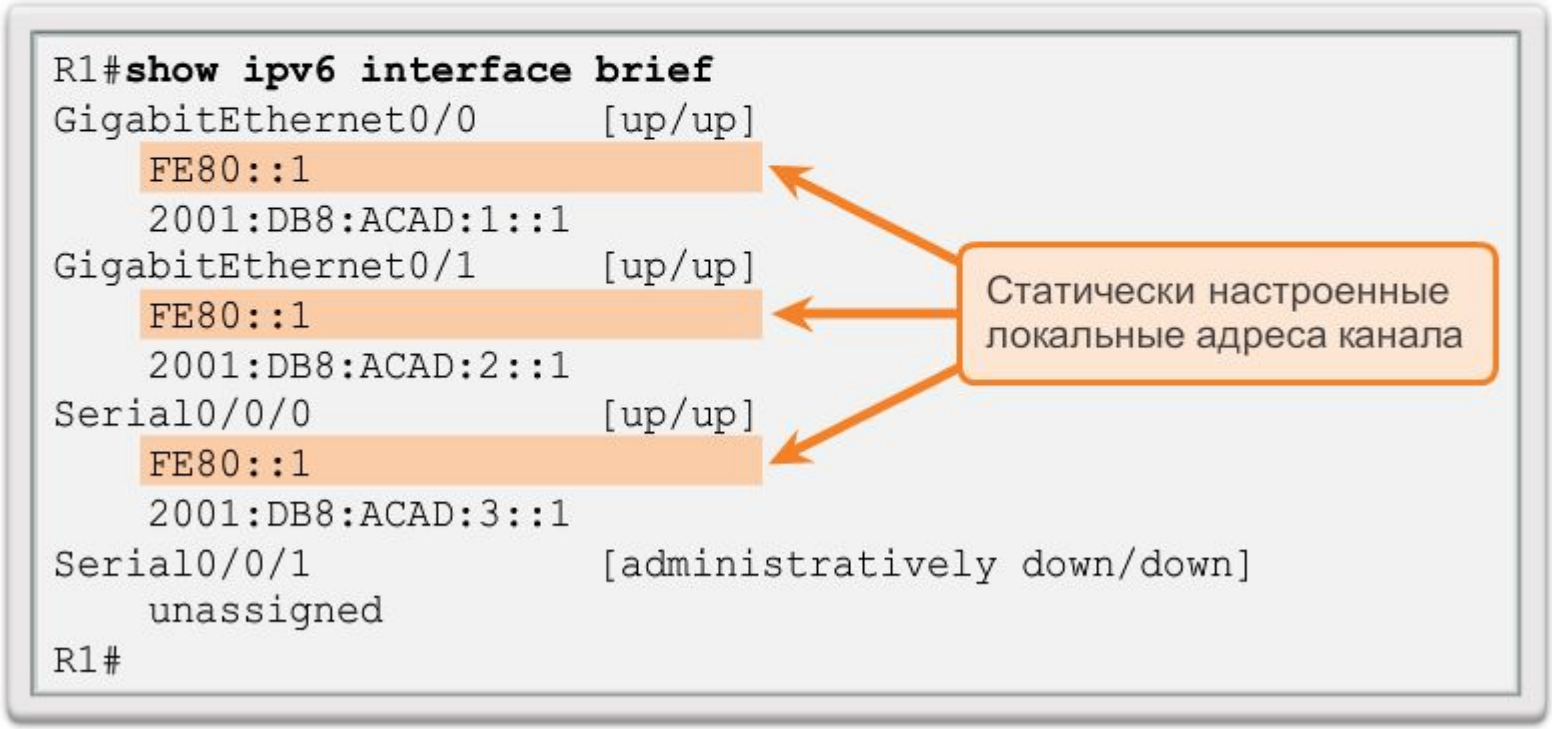
Локальный адрес канала имеет префикс в диапазоне от FE80 до FEBF. Если адрес начинается с этого хекстета (16-битный сегмент), то параметры локального канала должны следовать за адресом.

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

Индивидуальные IPv6-адреса

Далее показана конфигурация локального адреса канала с помощью команды ipv6 address interface. Локальный адрес канала FE80::1 используется для указания на то, что он принадлежит маршрутизатору R1. Такой же локальный адрес канала IPv6 настроен на всех интерфейсах маршрутизатора R1. FE80::1 можно настроить на каждом канале, поскольку он должен быть уникальным только на данном канале.



Групповые IPv6-адреса

Групповые IPv6-адреса мало чем отличаются от групповых IPv4-адресов. Групповой адрес используется для отправки одного пакета по одному или нескольким назначениям (группе мультивещания). Групповые IPv6-адреса имеют префикс FF00::/8.

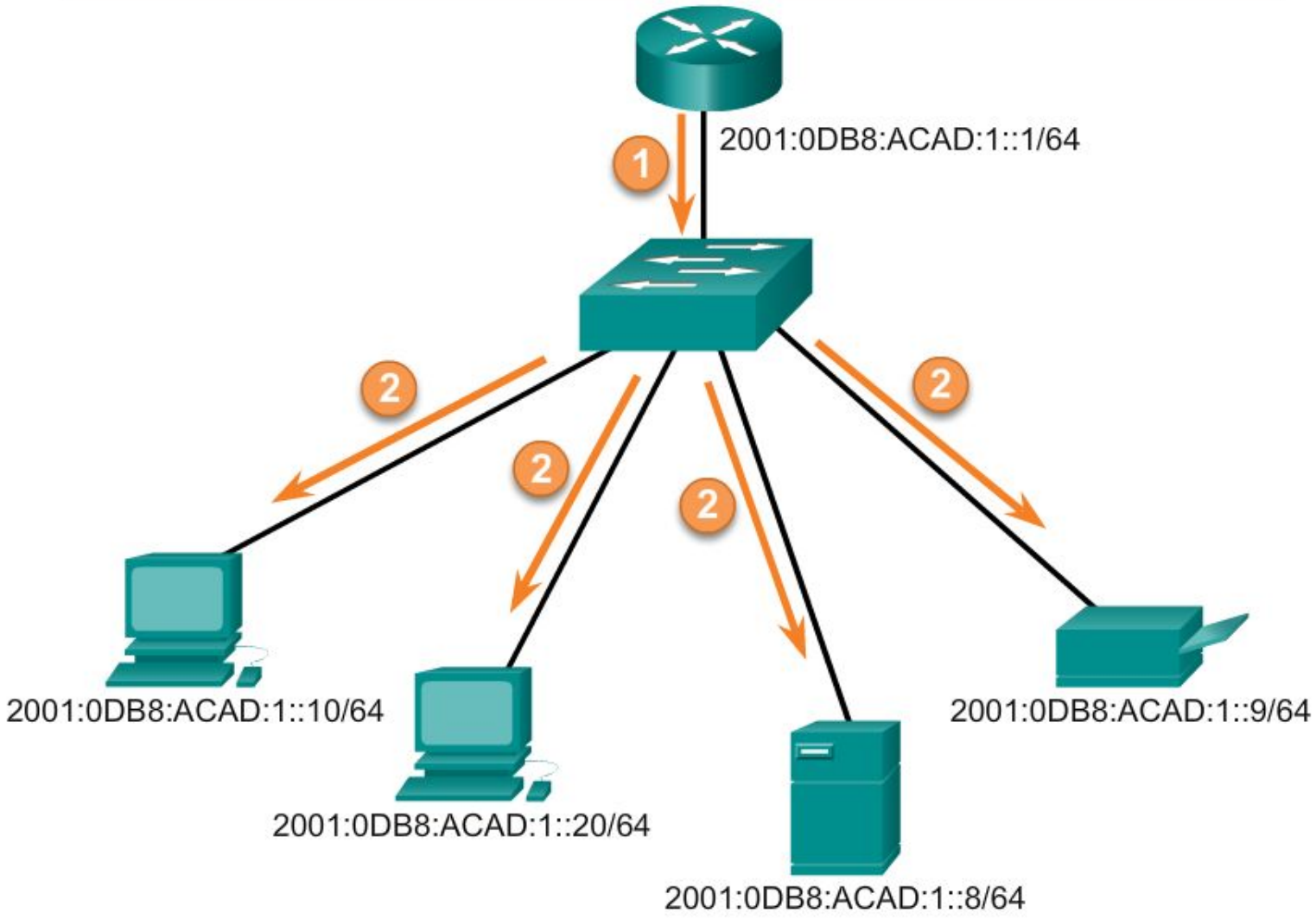
Примечание: Групповые адреса могут быть только адресами назначения, а не адресами источника.

Существует два типа групповых IPv6-адресов:

1. присвоенный групповой адрес
2. групповой адрес запрошенного узла

Групповые IPv6-адреса

IPv6-адрес источника 2001:0DB8:ACAD:1::1	**IPv6-адрес назначения** FF02::1



Групповые IPv6-адреса

Присвоенный групповой адрес

Присвоенные групповые адреса зарезервированы для заданных групп устройств. Присвоенный групповой адрес — это один адрес, используемый для осуществления связи с группой устройств, работающих на одном протоколе или сервисе. Присвоенные групповые адреса используются вместе с конкретными протоколами, например с протоколом DHCPv6.

Рассмотрим две распространённые группы присвоенных групповых IPv6-адресов.

Групповые IPv6-адреса

Группа мультивещания для всех узлов FF02::1. Это группа мультивещания, к которой подключены все устройства под управлением протокола IPv6. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-интерфейсами в канале или сети. Эта группа адресов работает так же, как широковещательный адрес в протоколе IPv4. На рисунке приводится пример осуществления связи с использованием групповых адресов для всех узлов. IPv6-маршрутизатор отправляет объявления маршрутизатора протокола управляющих сообщений версии 6 (RA ICMPv6) группе мультивещания для всех узлов. Объявление маршрутизатора предоставляет всем устройствам IPv6, находящимся в сети, информацию об адресации: префикс, длину префикса и шлюз по умолчанию.

Групповые IPv6-адреса

Группа мультивещания для всех маршрутизаторов FF02::2. Это группа мультивещания, к которой подключены все IPv6-маршрутизаторы. Маршрутизатор становится частью этой группы, когда переходит под управление протоколом IPv6 с помощью команды глобальной конфигурации ipv6 unicast-routing. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-маршрутизаторами в канале или сети.

Устройства под управлением протокола IPv6 отправляют сообщения с запросом маршрутизатора групповому адресу для всех маршрутизаторов. Такие сообщения запрашивают у IPv6-маршрутизатора объявление маршрутизатора, чтобы помочь устройству в процессе адресной конфигурации.

Групповые IPv6-адреса

Многоадресная рассылка запрашиваемого узла похожа на многоадресную рассылку всем узлам. Групповой адрес для всех узлов — это, по сути, то же самое, что и широковещательная IPv4-рассылка. Все устройства в сети должны обрабатывать трафик, отправляемый на адрес всех узлов. Для уменьшения количества устройств, которым необходимо обрабатывать трафик, используйте групповой адрес запрашиваемого узла.

Групповой адрес запрашиваемого узла — это адрес, который соответствует только 24 битам глобального индивидуального IPv6-адреса устройства. Обрабатывать эти пакеты должны только те устройства, которые имеют аналогичные 24 бита в наименее значащей, крайней правой части идентификатора интерфейса.

Групповые IPv6-адреса

Глобальный индивидуальный IPv6-адрес:
2001:0DB8:ACAD:0001:0000:0000:0000:0010

Групповой IPv6-адрес запрашиваемого узла:
FF02::0:FF00:0010

Групповые IPv6-адреса

Групповой IPv6-адрес запрашиваемого узла создаётся автоматически при назначении глобального индивидуального адреса или локального адреса канала. Групповой IPv6-адрес запрашиваемого узла создаётся посредством объединения специального префикса FF02:0:0:0:0:1:FF00::/104 с крайними правыми 24 битами его индивидуального адреса.

Групповой адрес запрашиваемого узла состоит из 2 частей.

1. Групповой префикс FF02:0:0:0:0:1:FF00::/104: первые 104 бита группового адреса запрашиваемого узла.
2. Наименее значимые 24 бита: последние или крайние правые 24 бита группового адреса запрашиваемого узла. Эти биты копируются из крайних правых 24 битов глобального индивидуального адреса или локального

Групповые IPv6-адреса

Существует вероятность того, что у нескольких устройств будет один и тот же групповой адрес запрашиваемого узла. Довольно редко в идентификаторах интерфейса устройств встречаются одинаковые крайние правые 24 бита. Это не влечёт за собой никаких проблем, поскольку устройство по-прежнему будет обрабатывать инкапсулированное сообщение, в котором содержится полный IPv6-адрес запрашиваемого устройства.

Проверка соединения. ICMPv6

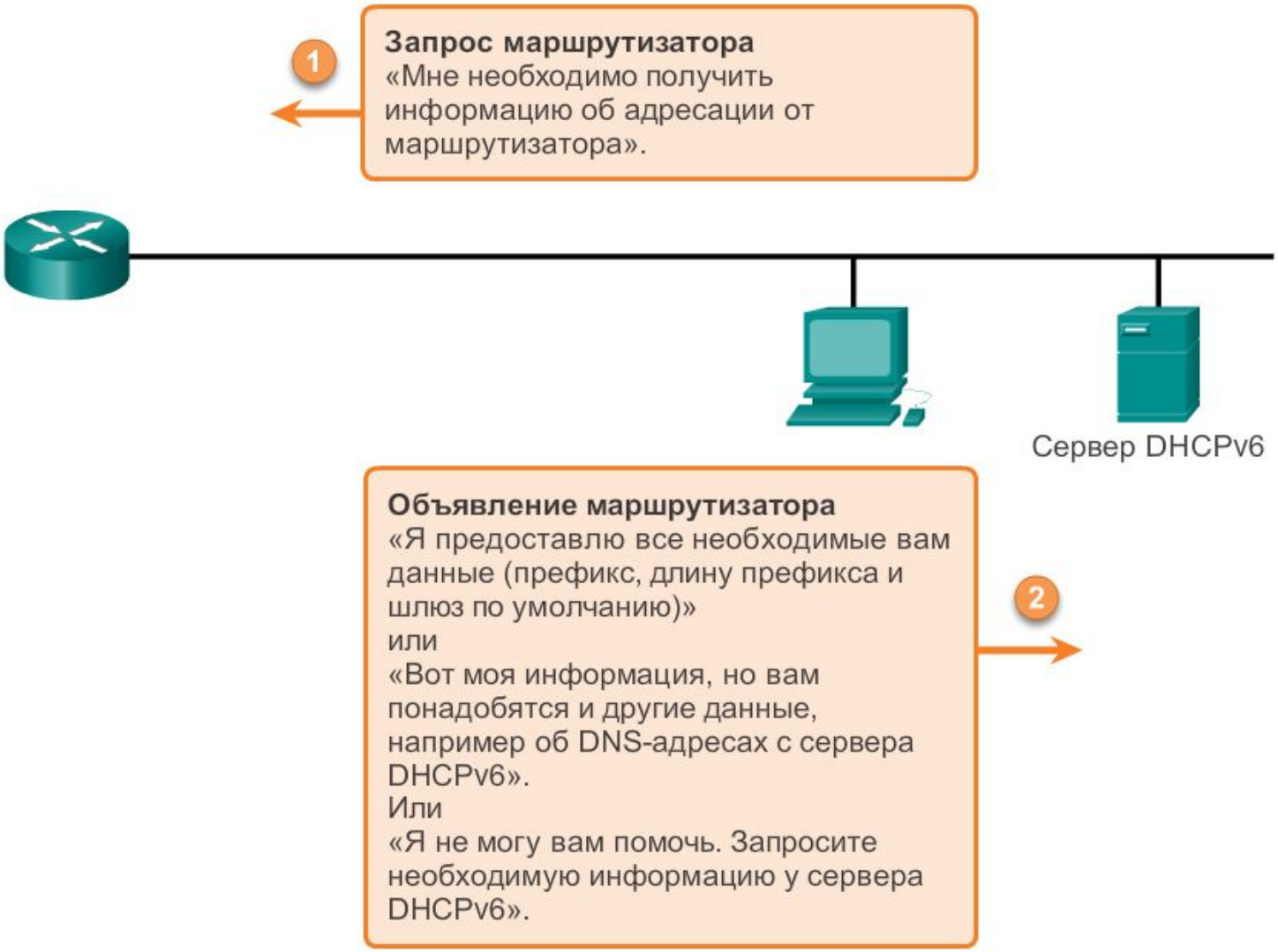
Информационные сообщения и сообщения об ошибках, возникающие в протоколе ICMPv6, очень похожи на сообщения о контроле и ошибках, используемые протоколом ICMPv4. Однако протокол ICMPv6 располагает повышенной функциональностью и новыми возможностями, которых нет в ICMPv4.

ICMPv6 включает четыре новых протокола в составе протокола обнаружения соседних узлов (ND или NDP):

Сообщение «Запрос к маршрутизатору»
Сообщение «Объявление маршрутизатора»
Сообщение «Запрос соседнего узла»
Сообщение «Объявление соседнего узла»
Сообщения «Запрос маршрутизатора» и «Объявление маршрутизатора»

Проверка соединения. ICMPv6

Сообщения «Запрос маршрутизатора» и «Объявление маршрутизатора»



Проверка соединения. ICMPv6

Устройства под управлением протокола IPv6 можно разделить на две категории - маршрутизаторы и узлы. Сообщения «Запрос маршрутизатора» и «Объявление маршрутизатора» передаются между узлами и маршрутизаторами.

Сообщения «Запрос маршрутизатора» (RS): отправляются от узла маршрутизатору, когда узел настроен для автоматического получения своей информации по адресации с помощью SLAAC. Такой запрос отправляется в виде многоадресного сообщения IPv6 для всех узлов.

Проверка соединения. ICMPv6

Сообщение «Объявление маршрутизатора» (RA): отправляется маршрутизаторами для предоставления узлам информации об адресации с помощью SLAAC. Такое сообщение может включать в себя информацию об адресации для узла, например префикс и длину префикса. Маршрутизатор отправляет подобное сообщение либо периодически, либо в ответ на сообщение запроса маршрутизатора. По умолчанию маршрутизаторы Cisco отправляют подобные сообщения каждые 200 секунд. Объявления маршрутизатора отправляются на групповые IPv6-адреса для всех узлов. Узел, использующий SLAAC, выполнит настройку шлюза по умолчанию для локального адреса канала того маршрутизатора, который отправил объявление RA.

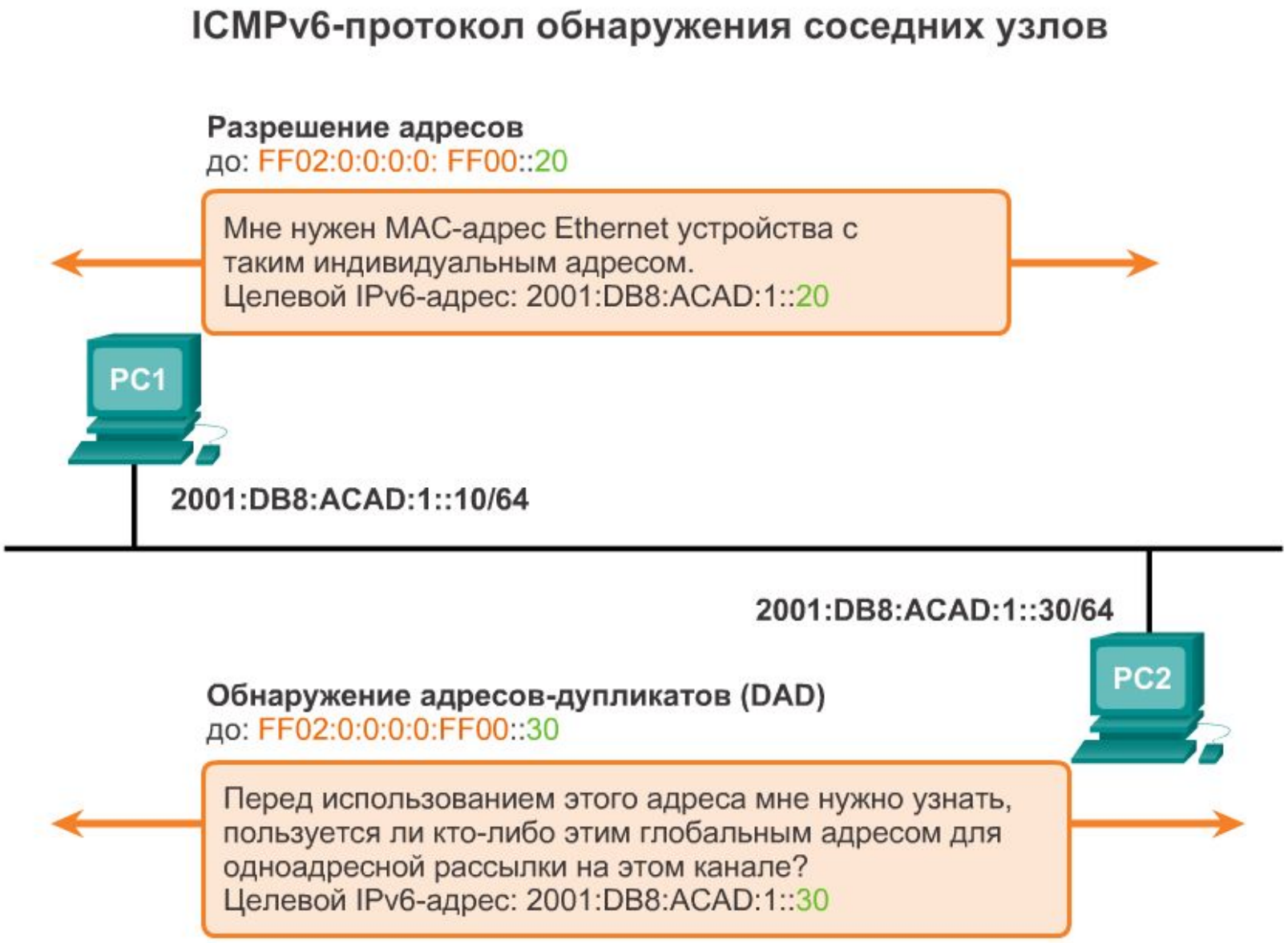
Проверка соединения. ICMPv6

Протокол обнаружения соседских узлов ICMPv6 включает в себя два дополнительных типа сообщений: «Запрос соседнего узла» (NS) и «Объявление соседнего узла» (NA).

Такие сообщения используются для:

1. разрешения адресов
2. обнаружения адресов-дубликатов (DAD)

Проверка соединения. ICMPv6



Проверка соединения. ICMPv6

Разрешение адресов

Разрешение адресов используется в том случае, когда устройству в локальной сети известен индивидуальный IPv6-адрес назначения, но неизвестен MAC-адрес Ethernet. Чтобы определить MAC-адреса назначения, устройство отправляет запрос соседнего узла на адрес запрашиваемого узла. Сообщение будет содержать известный (целевой) IPv6-адрес. Устройство, которое располагает целевым адресом IPv6, отправляет в ответ объявление соседнего узла, которое содержит его MAC-адрес Ethernet.

Проверка соединения. ICMPv6

Обнаружение адресов-дубликатов (DAD)

Когда устройству назначен глобальный индивидуальный адрес или локальный индивидуальный адрес канала, на этом адресе рекомендуется осуществить обнаружение адресов-дубликатов, чтобы убедиться в его уникальности. Для проверки уникальности адреса устройство отправит запрос соседнего узла со своим собственным IPv6-адресом в качестве целевого. Если другое устройство в сети обладает тем же адресом, оно отвечает объявлением соседнего узла. Такое объявление соседнего узла уведомит устройство отправителя о том, что данный адрес уже используется. Если соответствующее объявление соседнего узла не возвращается по истечении определённого периода времени, индивидуальный адрес признаётся уникальным и допустимым к использованию.

Примечание: Обнаружение адресов-дубликатов не обязательно, однако документ RFC 4861 рекомендует применять этот

Полезные ссылки для тех, у кого зашевелились волосы от кажущейся сложности протокола IPv6

https://habrahabr.ru/post/210100/
http://habrahabr.ru/post/210224/
https://habrahabr.ru/post/253803/
http://habrahabr.ru/post/254293/

Частично материал повторяется, частично совпадает с нашим курсом. Но это еще один из вариантов…