



МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени Н.Э. БАУМАНА

Учебное пособие

Учебно-методический комплект

по "Основы телекоммуникационных технологий"
Конспект лекций

ОСНОВЫ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ОСНОВЫ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Муравьев Константин Александрович

КОНТАКТЫ:

- **+7(926)761-13-07**
- **vk.com/kottik_mypp**
- **telegram @kottik_mypp**
- **instagram @kottik_mypp**
- **kostiktakaya@gmail.com**

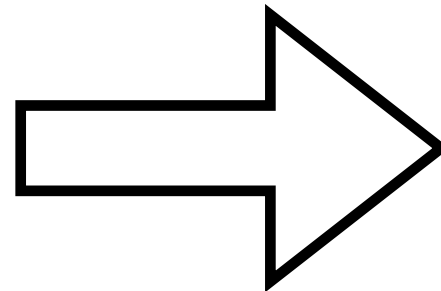
Основы телекоммуникационных технологий

10 лекций

7 семинаров/лаб

2 РК

1 ДЗ



ЗАЧЕТ

1 РК - 23 марта

2 РК - 18 мая

Темы курса

1	Сетевые протоколы и коммуникации
2	Сетевой доступ
3	Ethernet
4	Технологии WLAN
5	Принципы VLAN
6	Сетевой уровень и IP адресация
7	Разделение IP-сетей на подсети
8	Статическая маршрутизация
9	Динамическая маршрутизация
10	Транспортный уровень, NAT
11	Уровень приложений

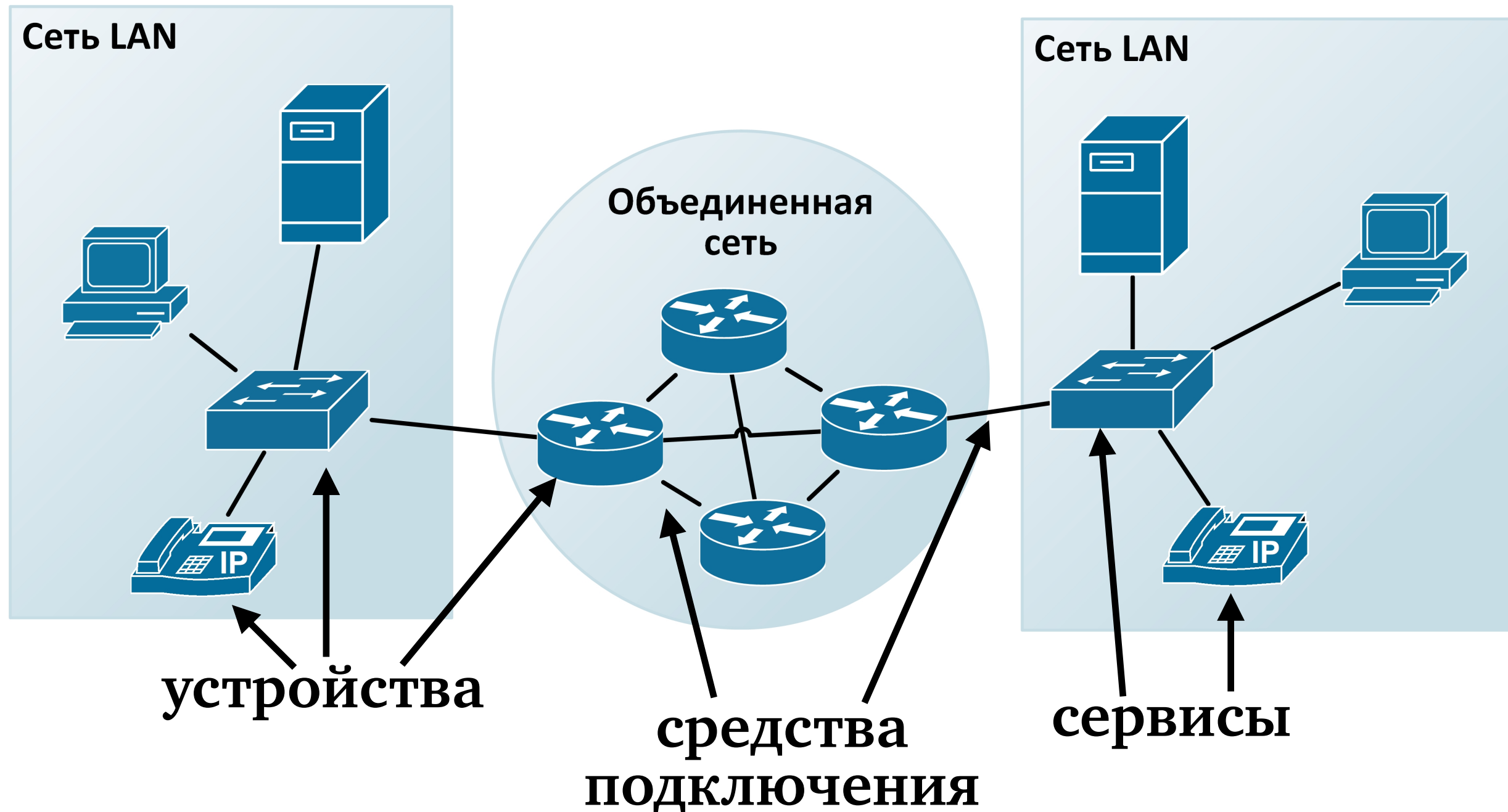
Основы телекоммуникационных технологий

- **Уэнделл Одом. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-105**
- **David Hucaby. CCNA Wireless 200-355 Official Cert Guide**
- **Эви Немет, Гарт Снайдер. Unix и Linux. Руководство системного администратора**

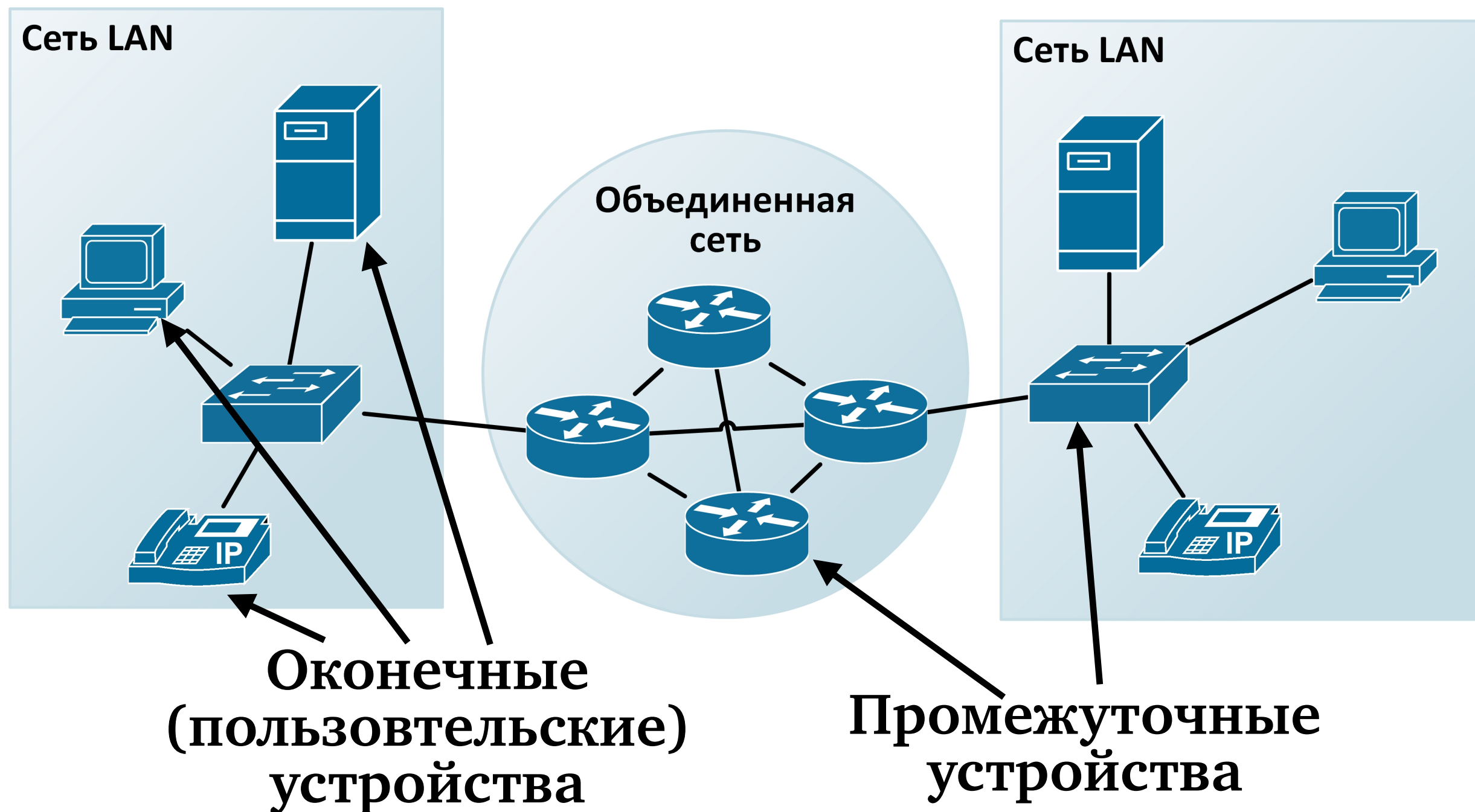
Где нужны сети?

- **В повседневной жизни**
- **В обучении**
- **В работе**
- **В общении**
- **В развитии общества**

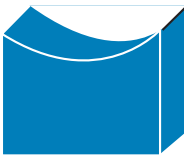
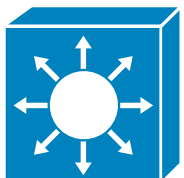
Компоненты сетей



Компоненты сетей



Сетевые устройства

	Персональный компьютер
	Концентратор (hub)
	Мост (bridge)
	Коммутатор (switch)
	Точка доступа (access point)
	Коммутатор 3-его уровня (L3 switch)
	Маршрутизатор (router)

Интерфейс

Интерфейс - формально определенная логическая или физическая граница между независимыми взаимодействующими объектами. Интерфейс задает параметры, процедуры, характеристики взаимодействия.

Физический порт - стандартизированный разъем на сетевом устройстве, для подключения к нему кабелей.

Протокол

Сетевой протокол — набор правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

Сетевая модель

Сетевая модель, или сетевая структура, представляет собой упорядоченный набор документации и стандартов, которому должны соответствовать все устройства в сети для обеспечения ее работоспособности

Сетевая модель

TCP/IP - Transmission Control Protocol/Internet Protocol

OSI - Open System Interconnection

RFC - Requests for Comments

IEEE - Institute of Electrical and Electronic Engineers

Структурная модель стека TCP/IP

Исходная модель	Модернизированная модель	Протоколы
Приложений	Приложений	HTTP, POP3, SMTP
Транспортный	Транспортный	TCP, UDP
Интернет	Сетевой	IP
Доступа к сети	Канальный	Ethernet, PPP
	Физический	

Уровень приложений TCP/IP



Заголовок HTTP GET index.html

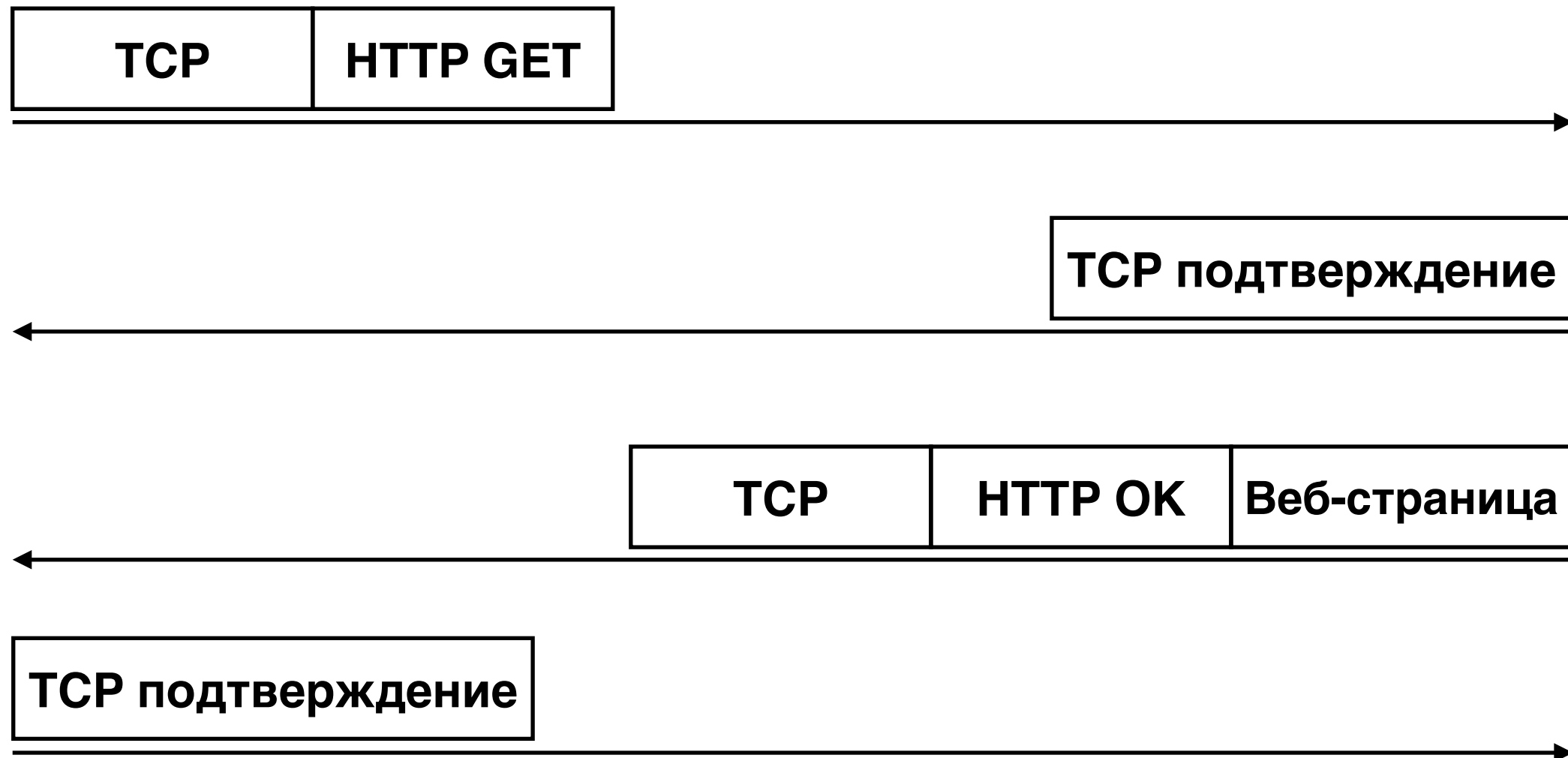
HTTP OK

Содержимое index.html

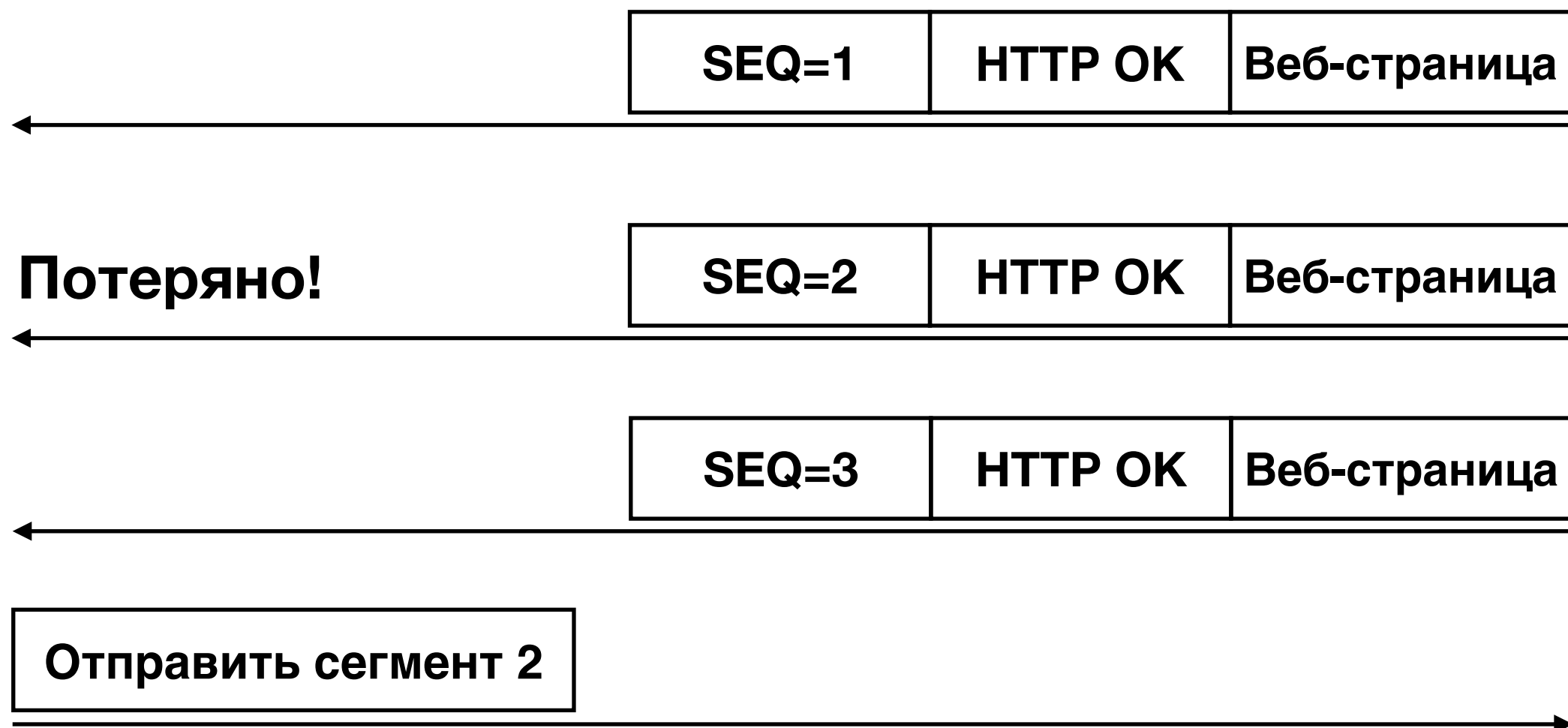
Уровень приложений TCP/IP

Уровень приложений стека TCP/IP предоставляет службы приложениям и программному обеспечению, работающему на компьютере. Сам он не определяет требования непосредственно к приложениям, а стандартизирует службы, которые могут понадобиться приложениям. Другими словами, уровень приложений представляет собой интерфейс между программным обеспечением компьютера и сетью.

Транспортный уровень TCP/IP



Транспортный уровень ТСР/ІР



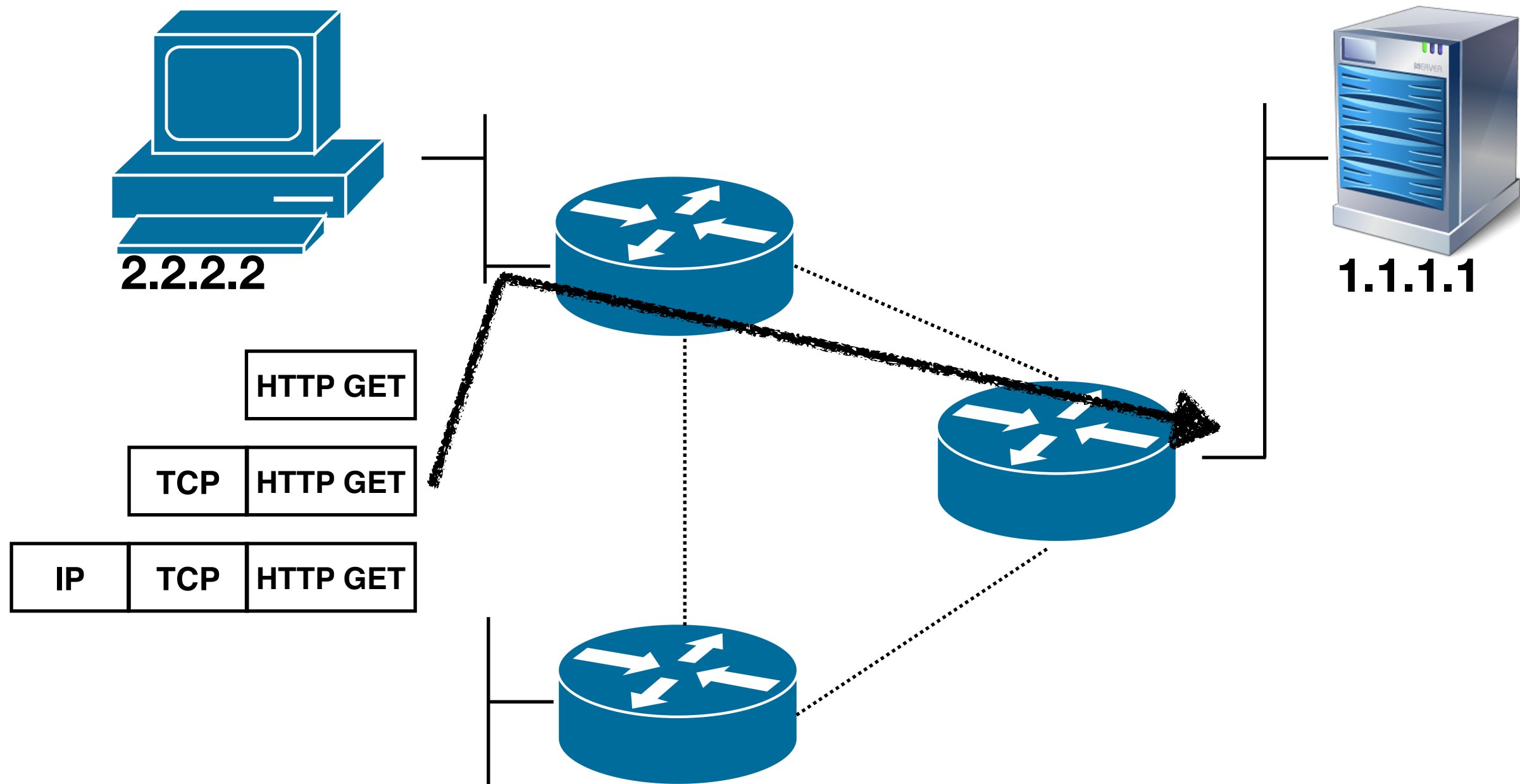
Транспортный уровень ТСР/ІР

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

Транспортный уровень предоставляет транспортные услуги от узла отправителя к узлу получателя. Он поддерживает логическое соединение между конечными точками сетевого маршрута.

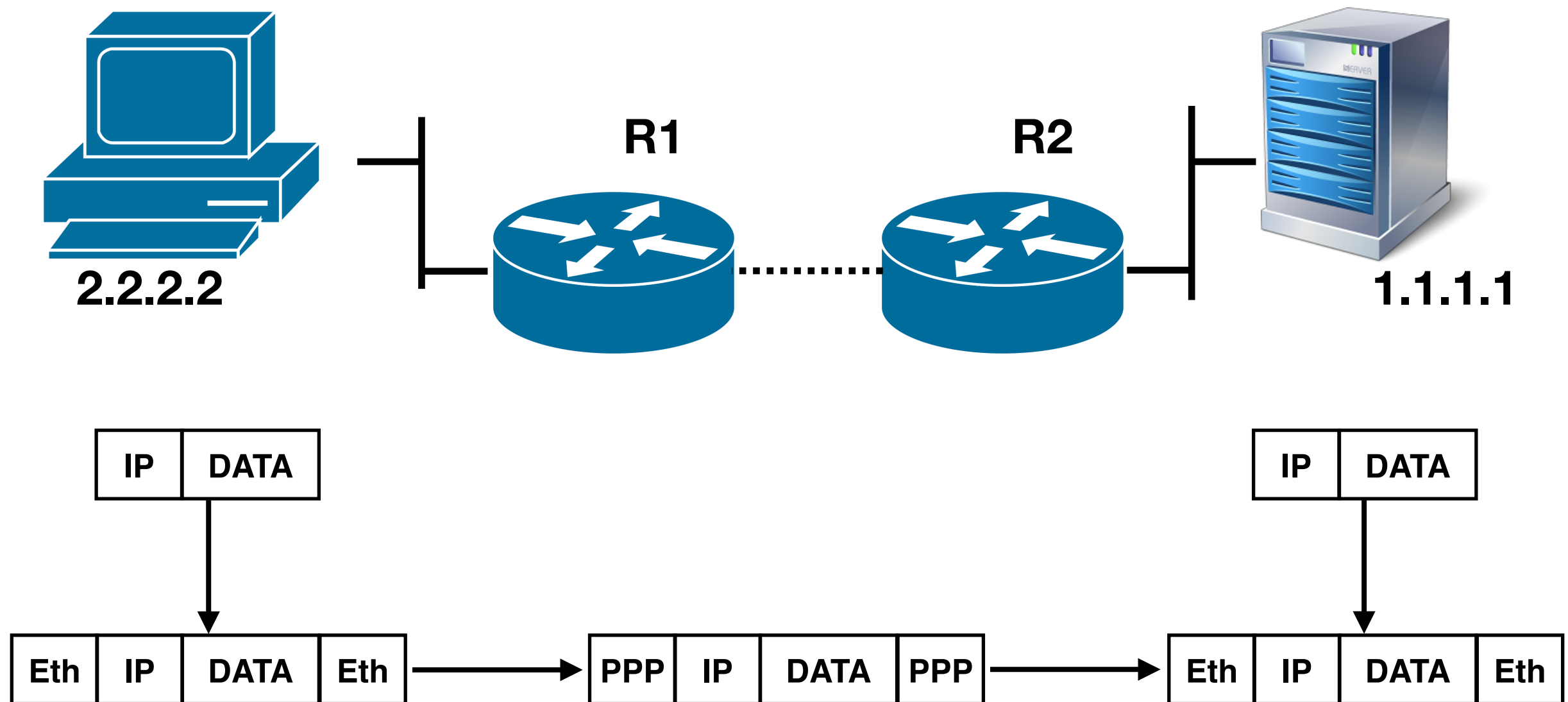
Интернет-уровень TCP/IP



Интернет-уровень TCP/IP

Протокол IP (Internet Protocol) определяет адреса для каждого компьютера или узла в сети, причем каждый узел должен иметь свой собственный уникальный IP-адрес. На интернет-уровне происходит выбор наилучшего маршрута и пересылка пакета, которую выполняют специализированные устройства - маршрутизаторы.

Уровень доступа к сети TCP/IP



Уровень доступа к сети TCP/IP

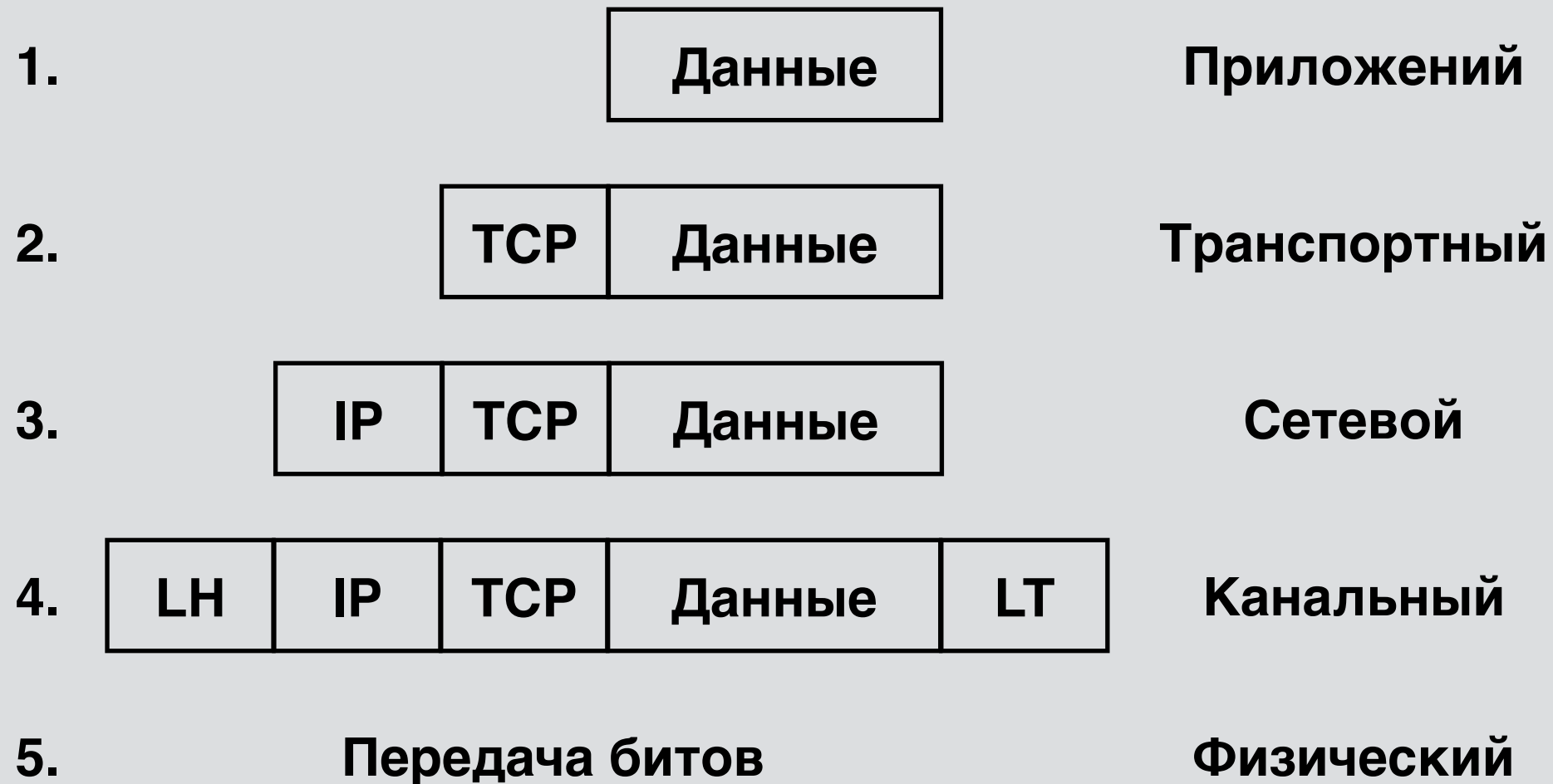
LAN - Local Area Network

WAN - Wide Area Network

Уровень доступа к сети стандартизирует аппаратное обеспечение и протоколы, используемые для передачи данных по физическим сетям. Уровень определяет, как именно узел подключен к физической среде передачи, поверх которой передаются данные.

Канал связи(link) - физическое соединение (или канал) между двумя устройствами и протоколы, используемые для управления этими каналами.

Инкапсуляция данных



Взаимодействие смежных и равноценных уровней

Концепция	Описание
Взаимодействие равноценных уровней между разными компьютерами	Два компьютера используют протокол, чтобы осуществить взаимодействие. Протоколом называют формальный набор правил, соглашений и форматов, в котором также используются заголовки для упорядоченного обмена информацией между компьютерами
Взаимодействие смежных уровней на одном компьютере	В одном компьютере один уровень может предоставлять службы другому. Програмное и аппаратное обеспечение, в котором реализованы процедуры верхнего уровня, запрашивает низлежащий уровень о выполнении некоторой функции

Сетевые топологии

Сетевая топология

Сетевая топология - способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

А - линия

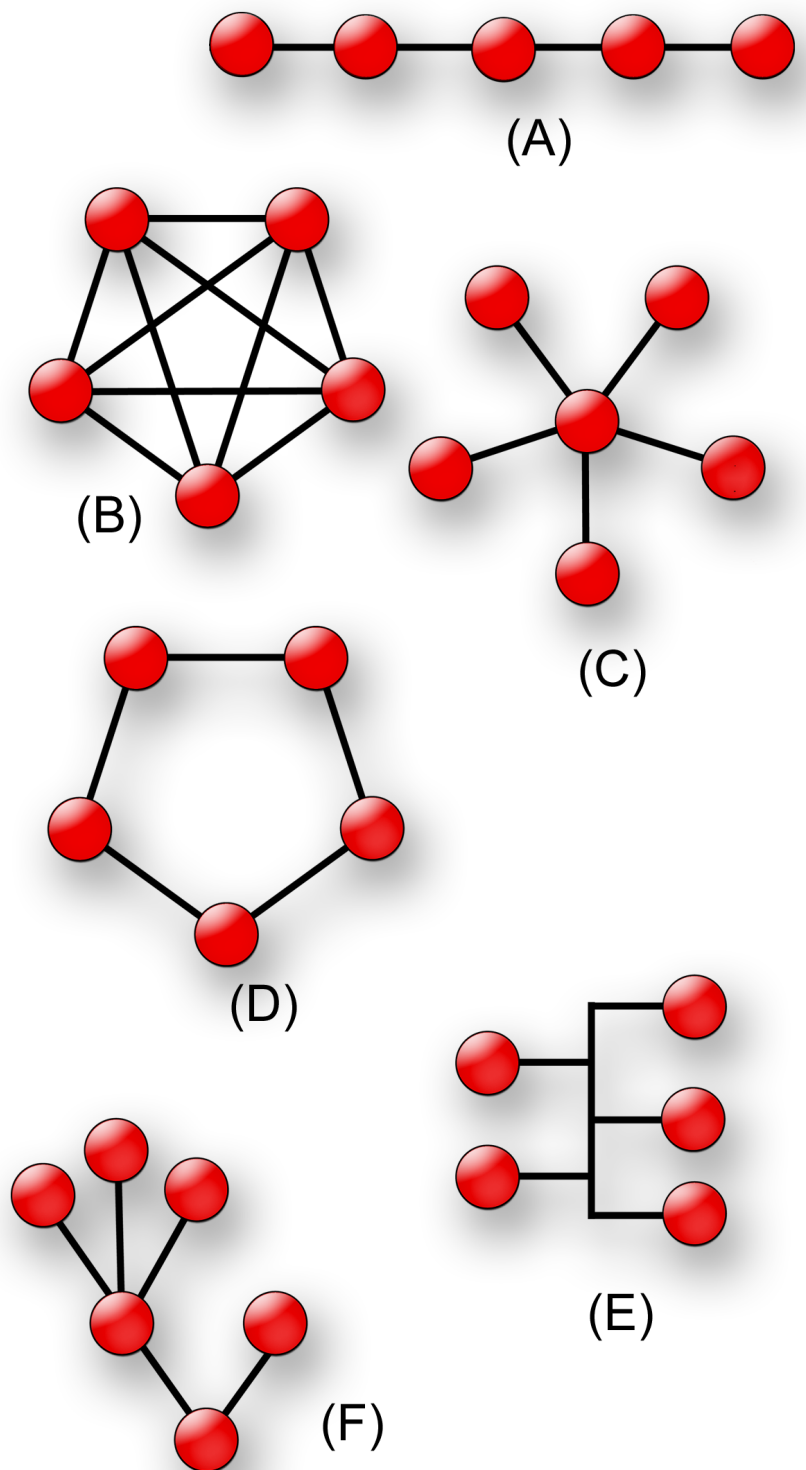
В - полносвязная

С - звезда

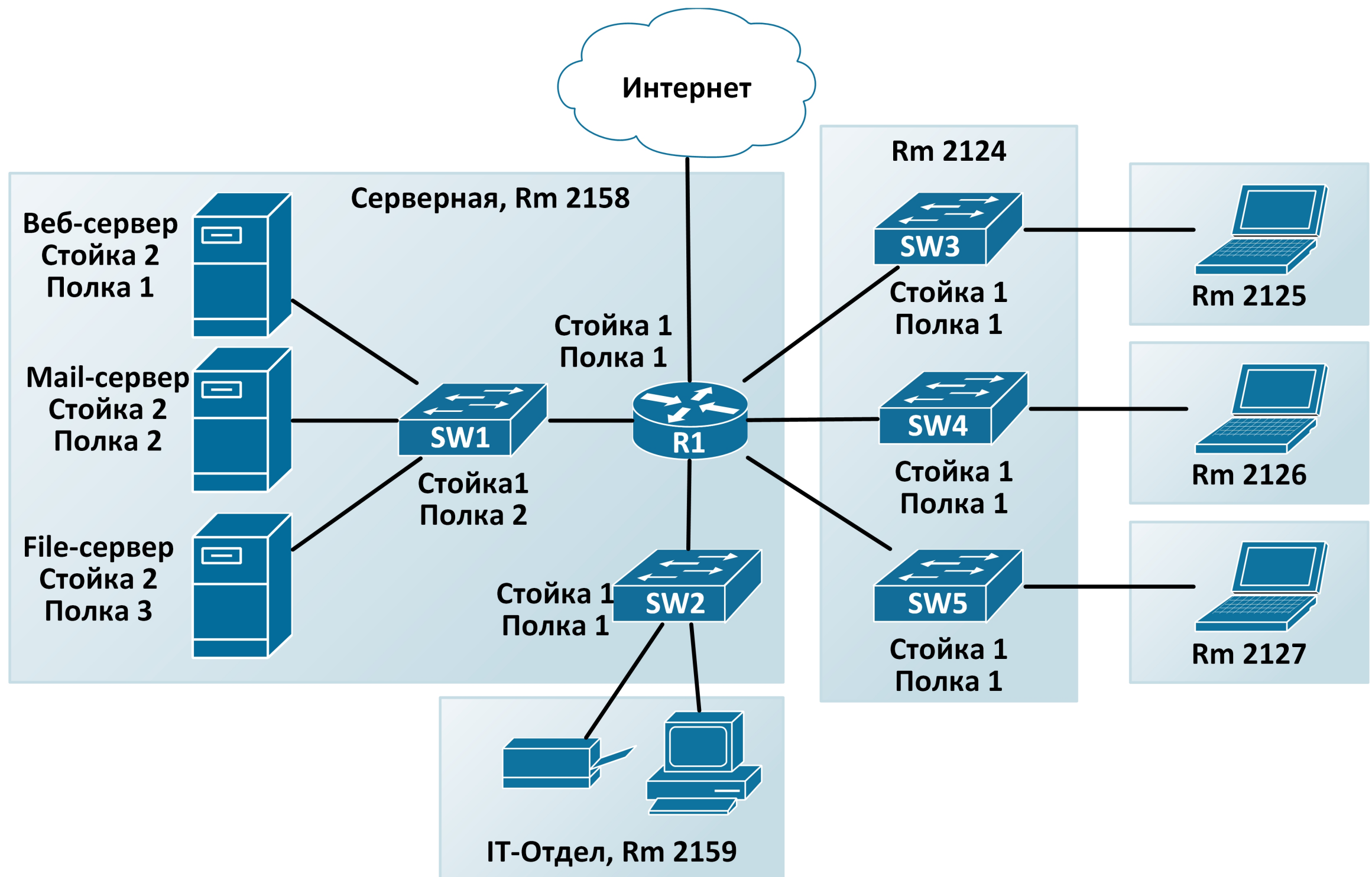
Д - кольцо

Е - общая шина

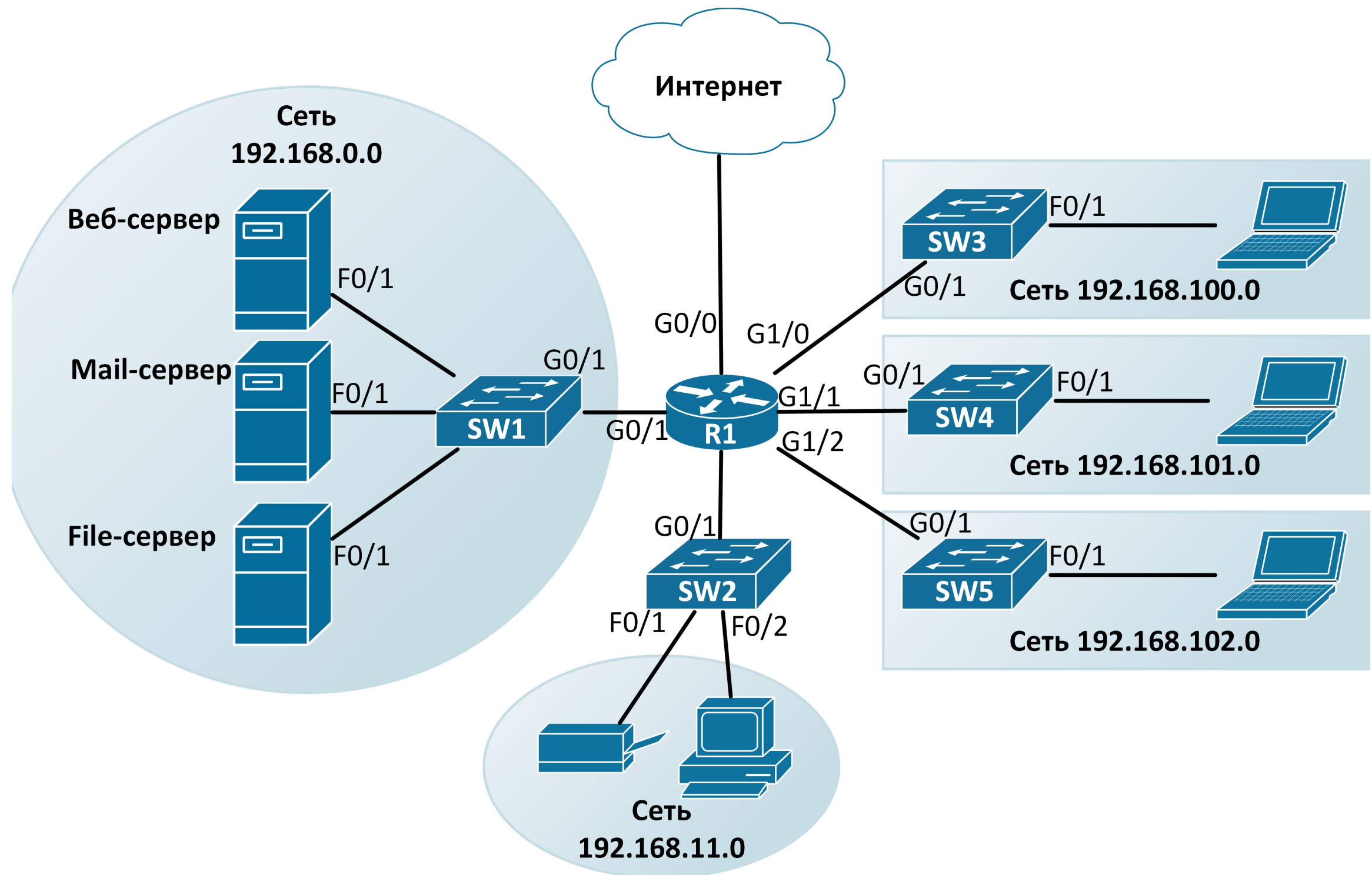
Ф - дерево



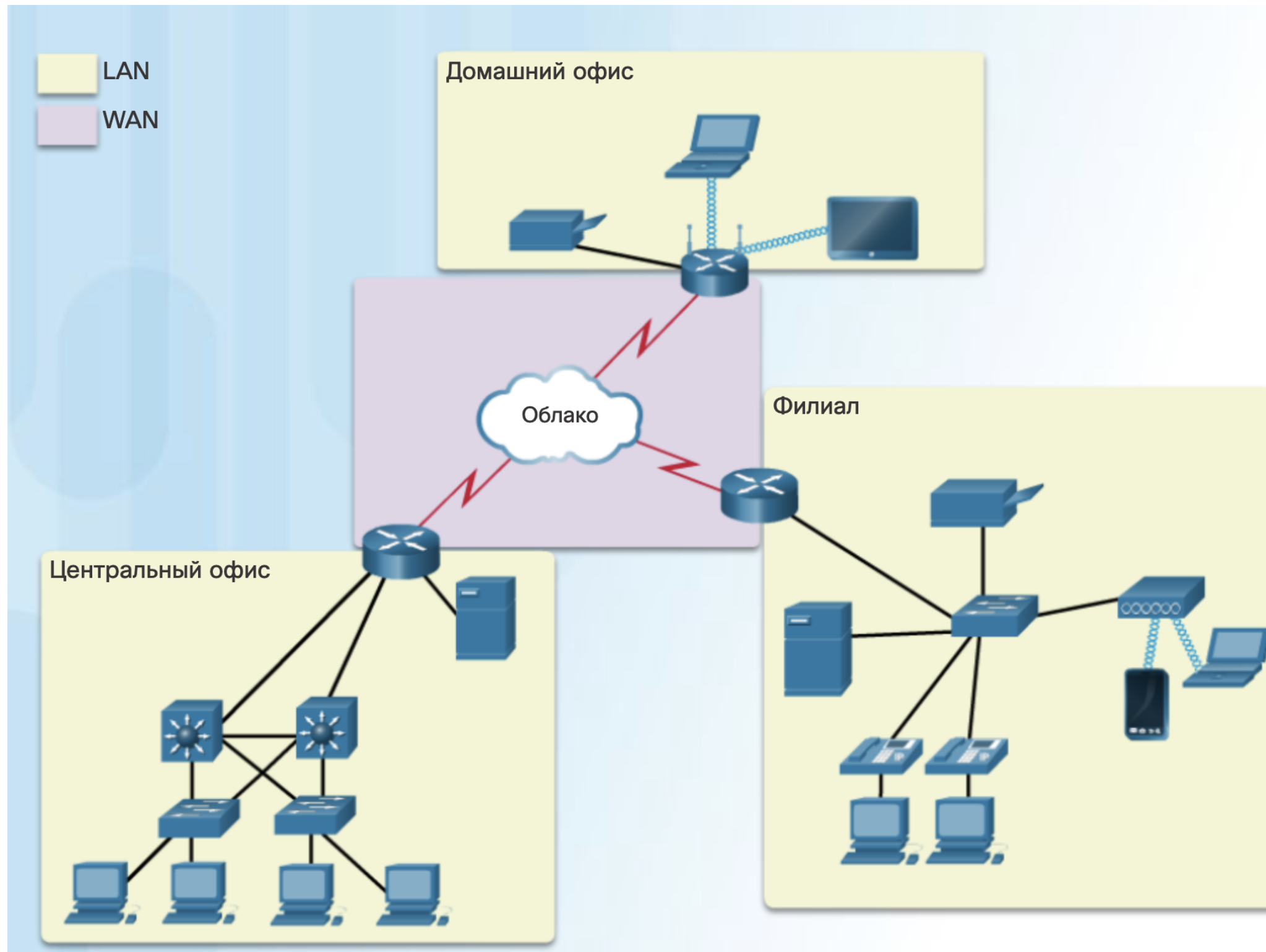
Физическая топология



Логическая топология



Типы сетей

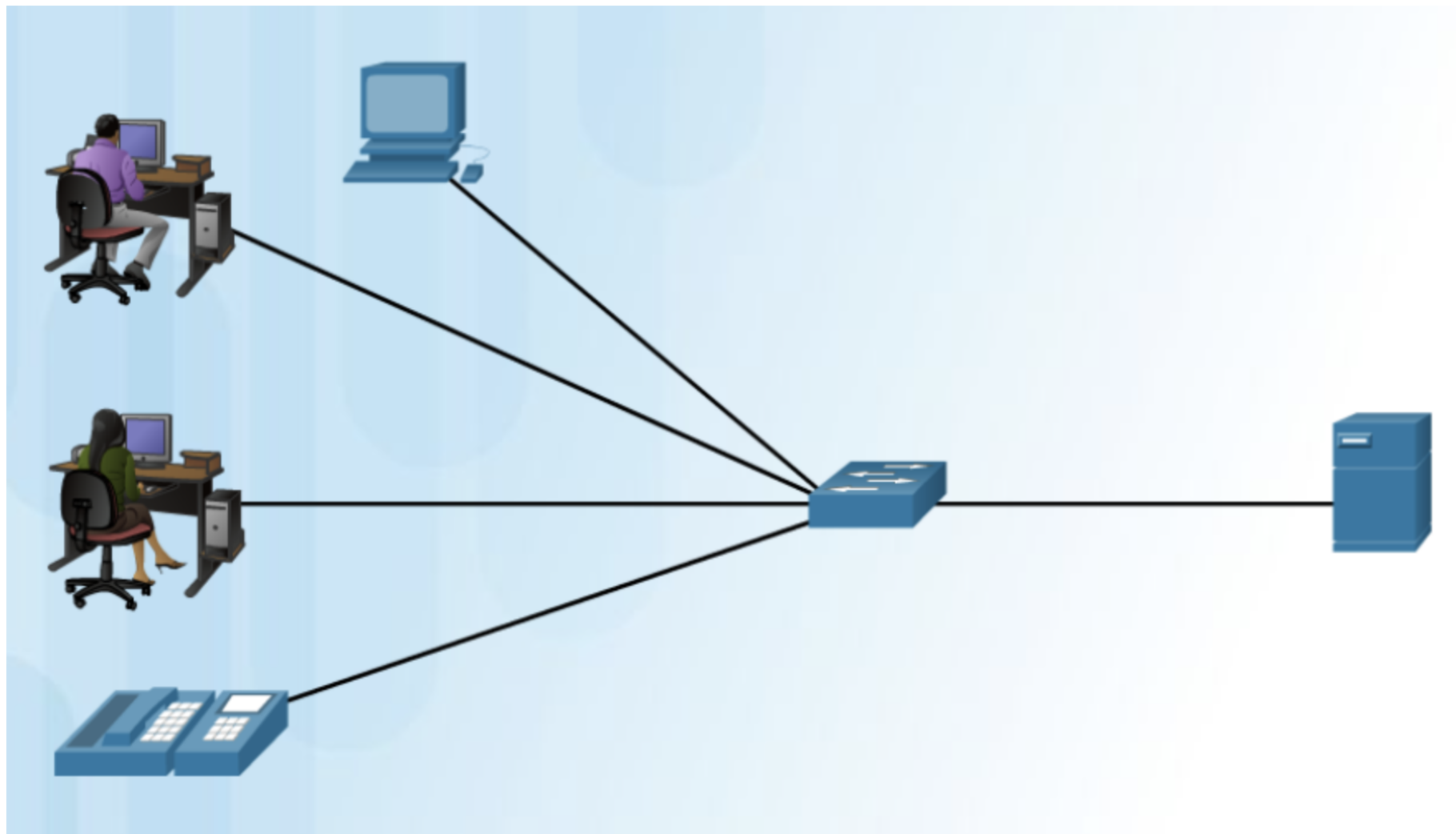


Типы сетей

Локальная сеть (LAN) — сетевая инфраструктура, предоставляющая доступ пользователям и оконечным устройствам на небольшой территории; обычно является домашней сетью, сетью малого или крупного предприятия, управляется одним лицом или ИТ-отделом и принадлежит им.

Глобальная сеть (WAN) — сетевая инфраструктура, предоставляющая доступ к другим сетям на большой территории; обычно принадлежит провайдерам телекоммуникационных услуг и находится под их управлением.

Сети LAN

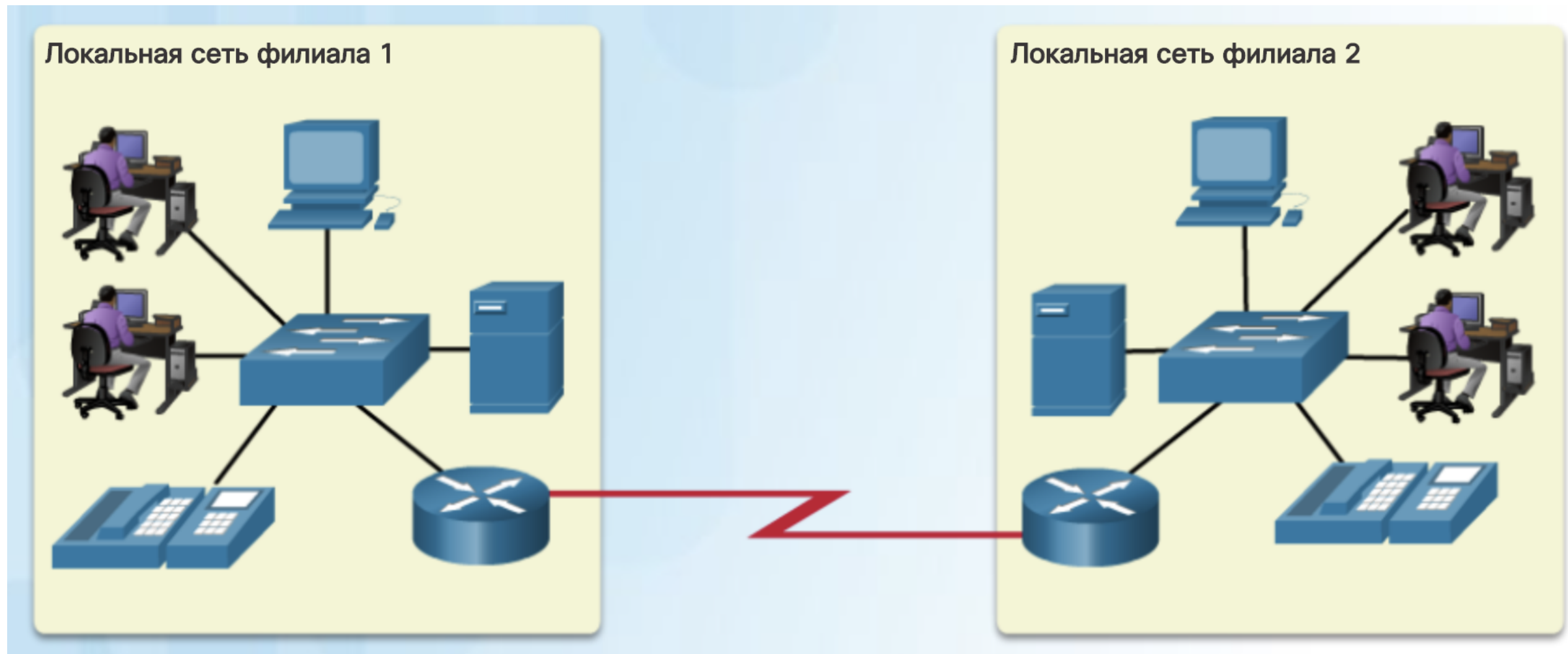


Сети LAN связывают оконечные устройства в ограниченной области, например в доме, школе, офисном здании или комплексе зданий.

Сети LAN обычно администрирует одна организация или частное лицо. Администратор управляет политикой безопасности и контролем доступа на сетевом уровне.

Сети LAN предоставляют высокоскоростной доступ к внутренним оконечным и промежуточным устройствам.

Сети WAN

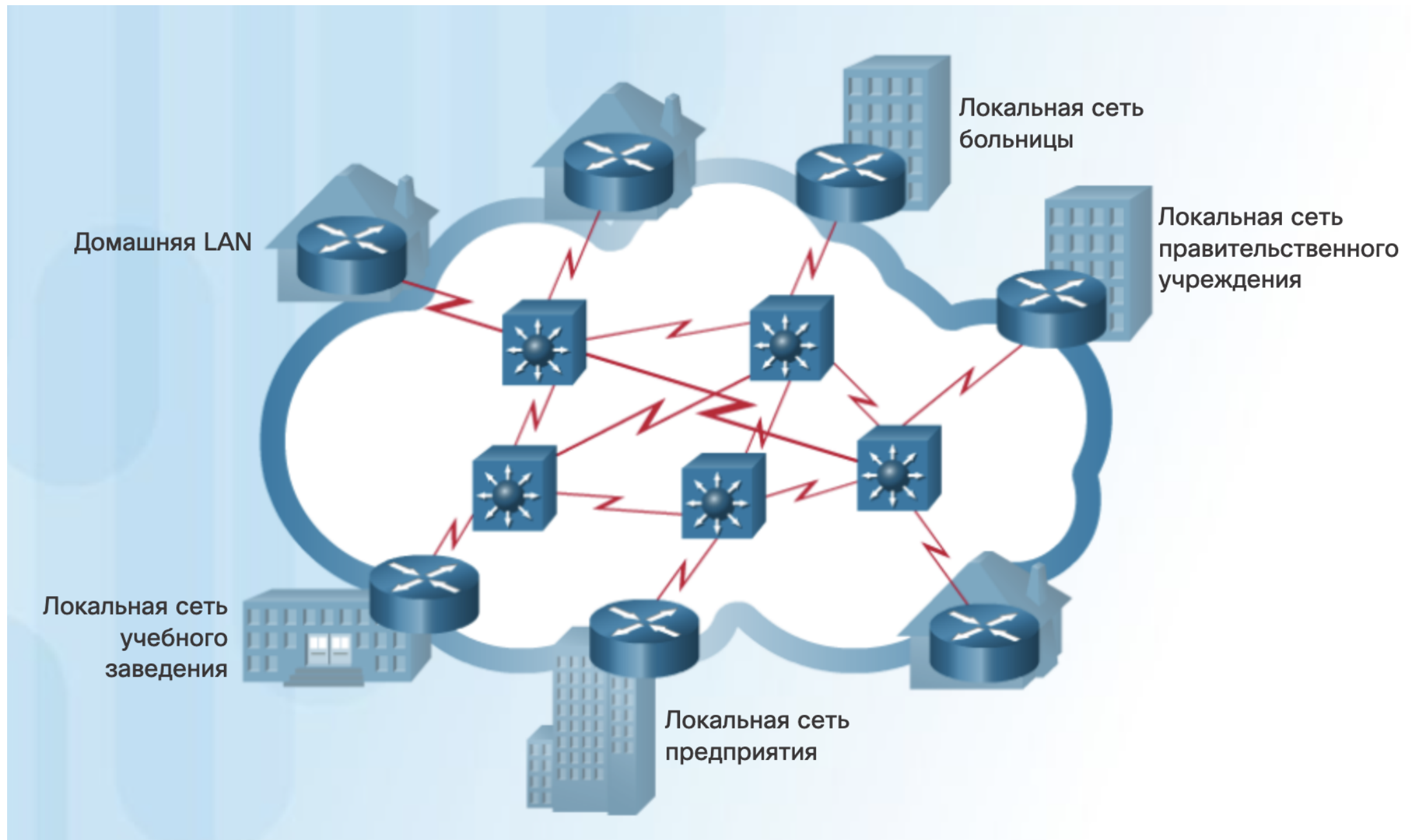


Сети WAN связывают локальные сети в обширных географических областях, таких как города, штаты, регионы, страны или континенты.

Управляют глобальными сетями обычно различные операторы связи.

Сети WAN обычно обеспечивают менее скоростные соединения между локальными сетями.

Интернет



Интернет — это объединение взаимосвязанных сетей в мировом масштабе

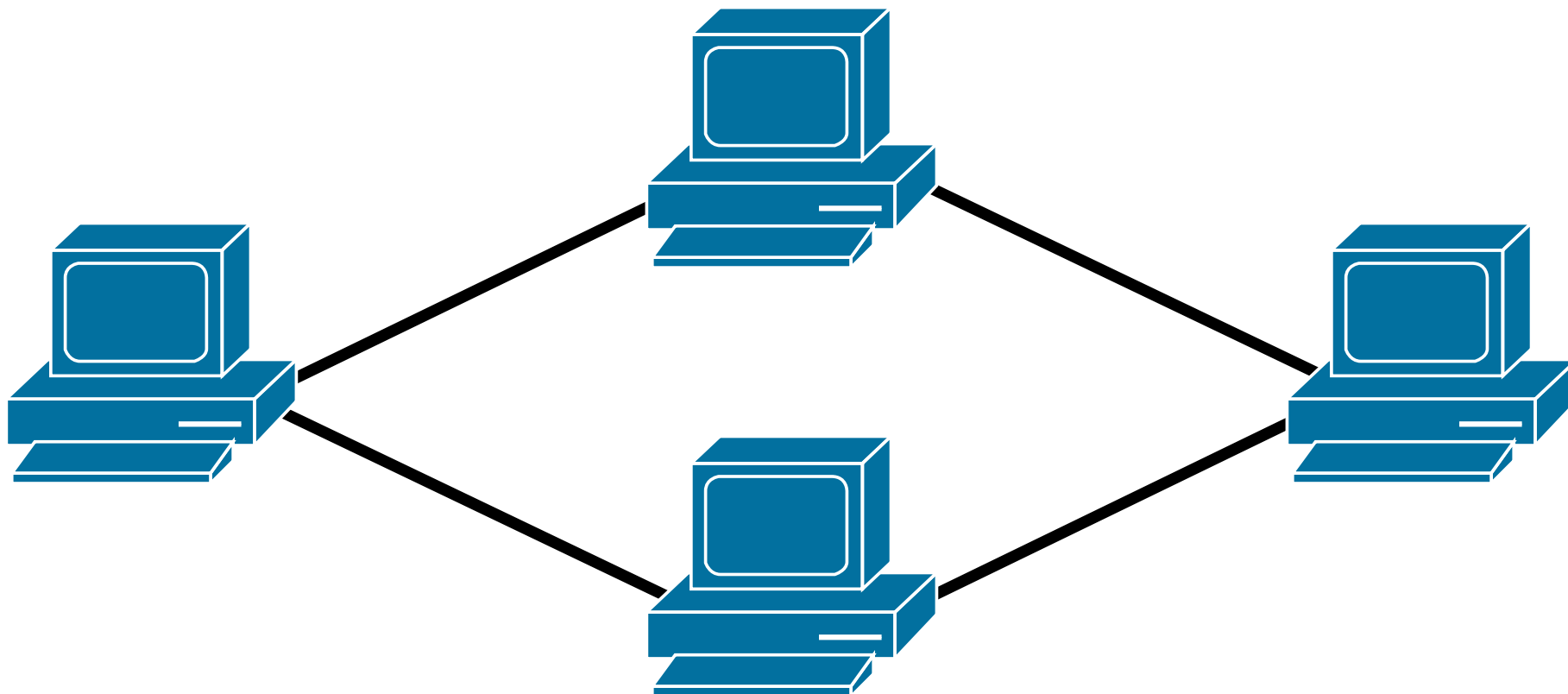
Сетевая ТОПОЛОГИЯ

Топология типа общая шина, представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.



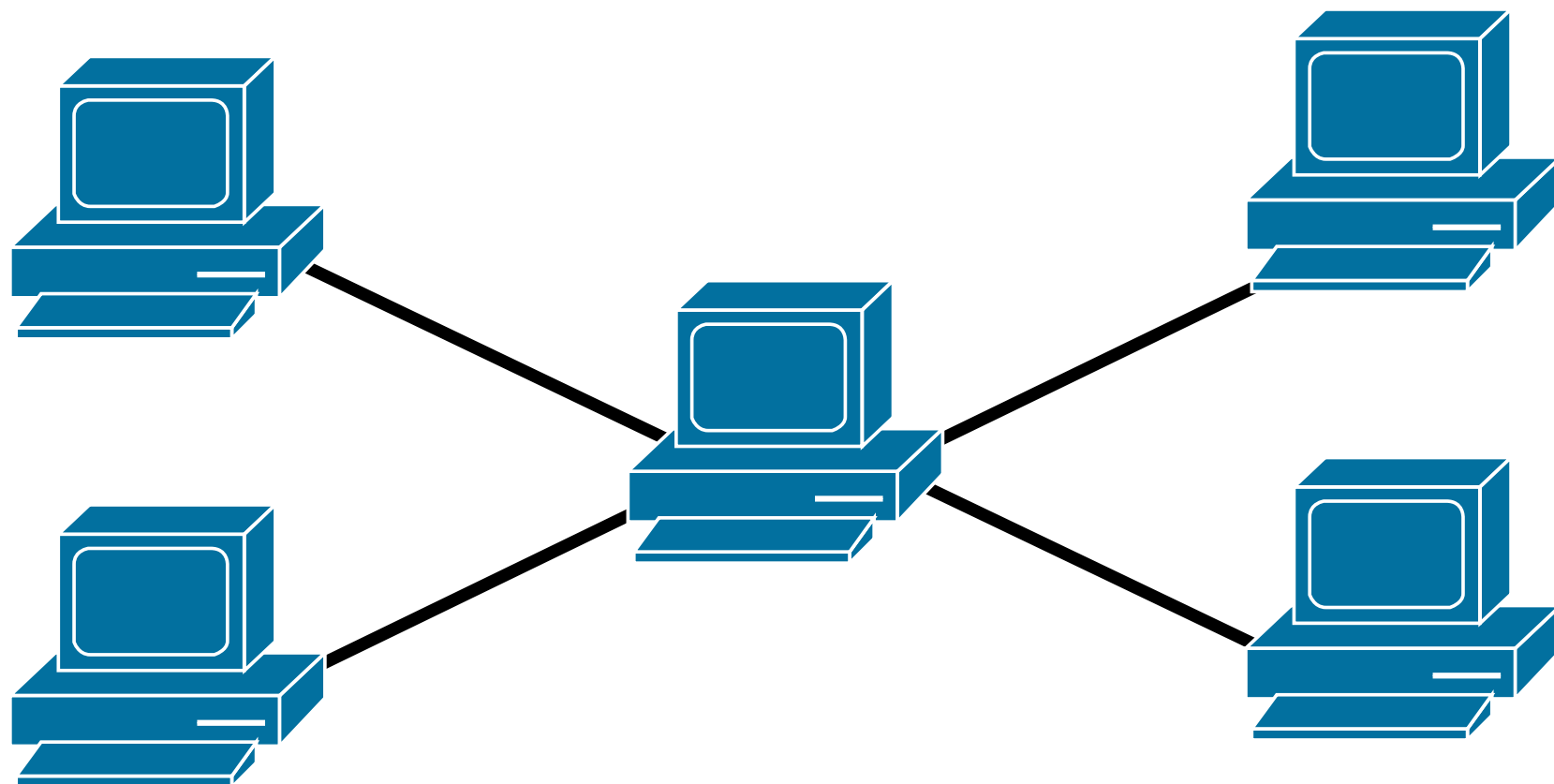
Сетевая топология

Кольцо — это топология, в которой каждый компьютер соединён линиями связи только с двумя другими: от одного он только получает информацию, а другому только передаёт.



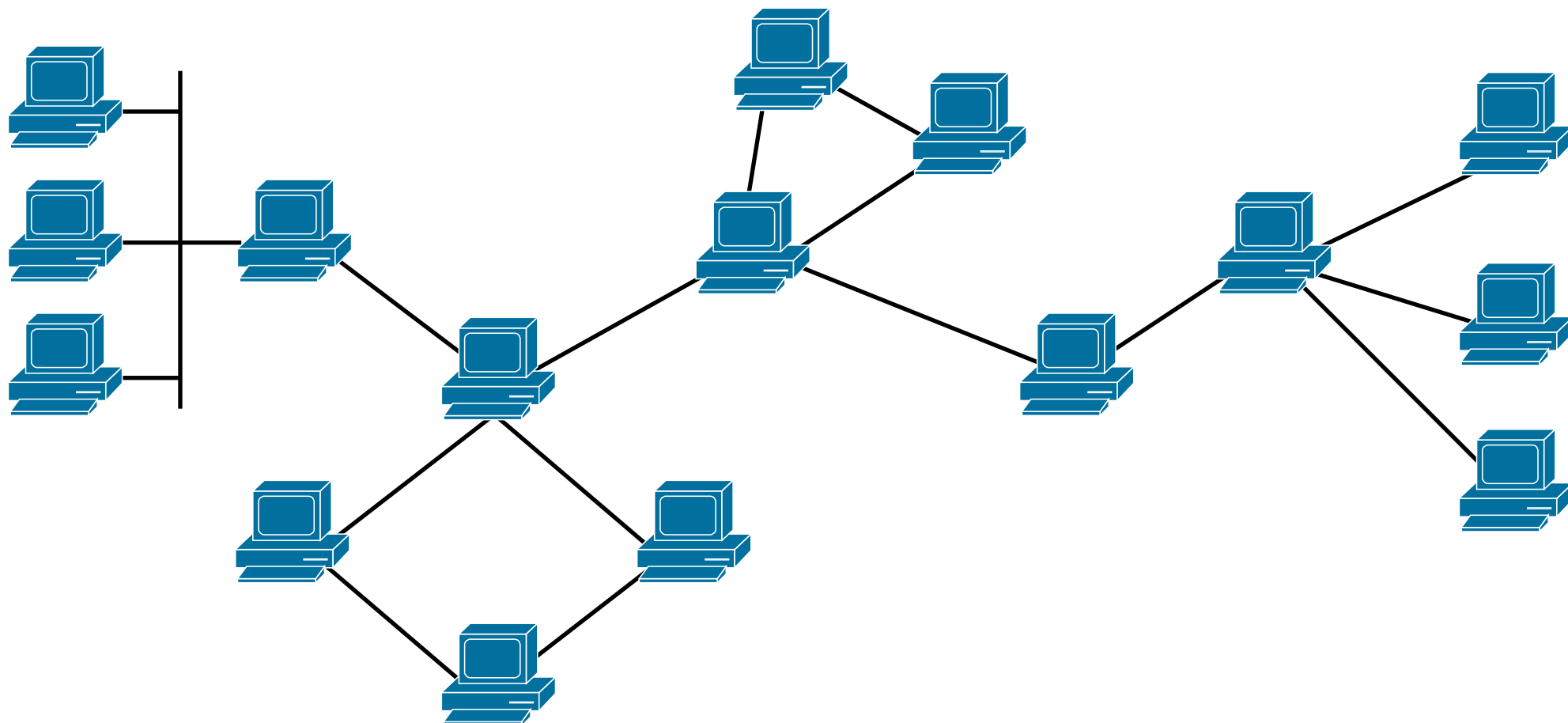
Сетевая топология

Звезда — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу

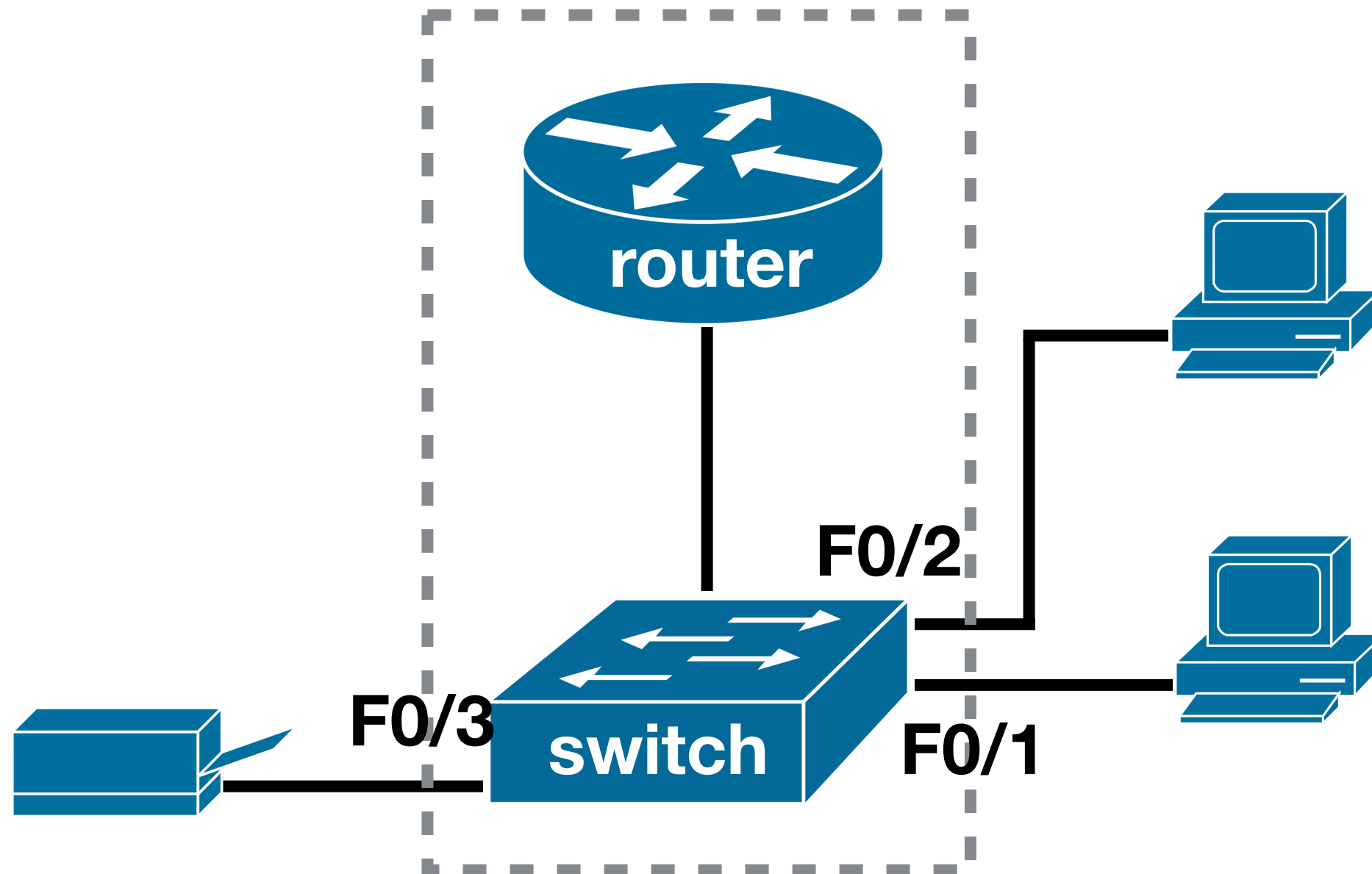


Сетевая топология

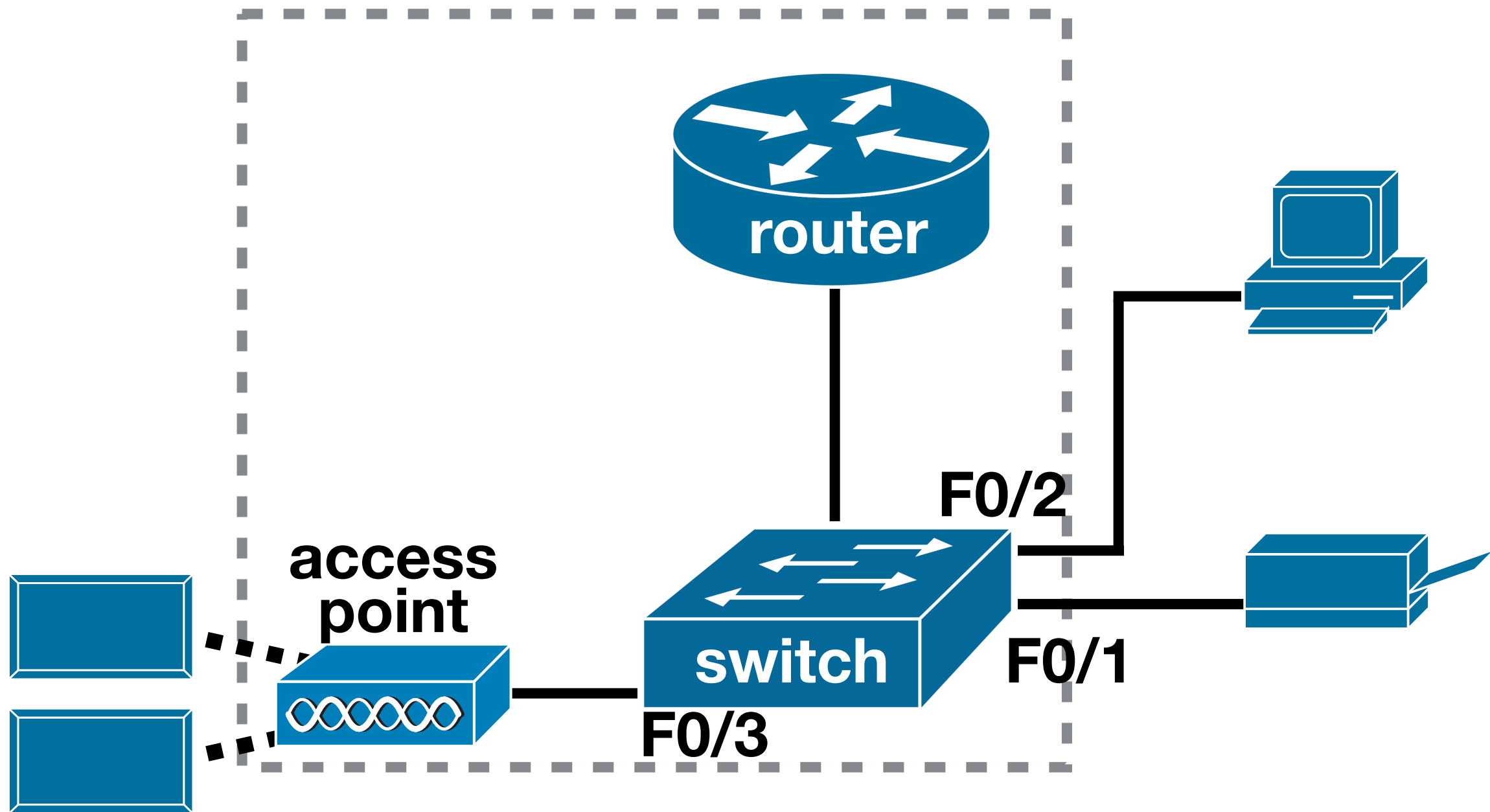
Смешанная топология - объединение нескольких сетевых топологий в одну



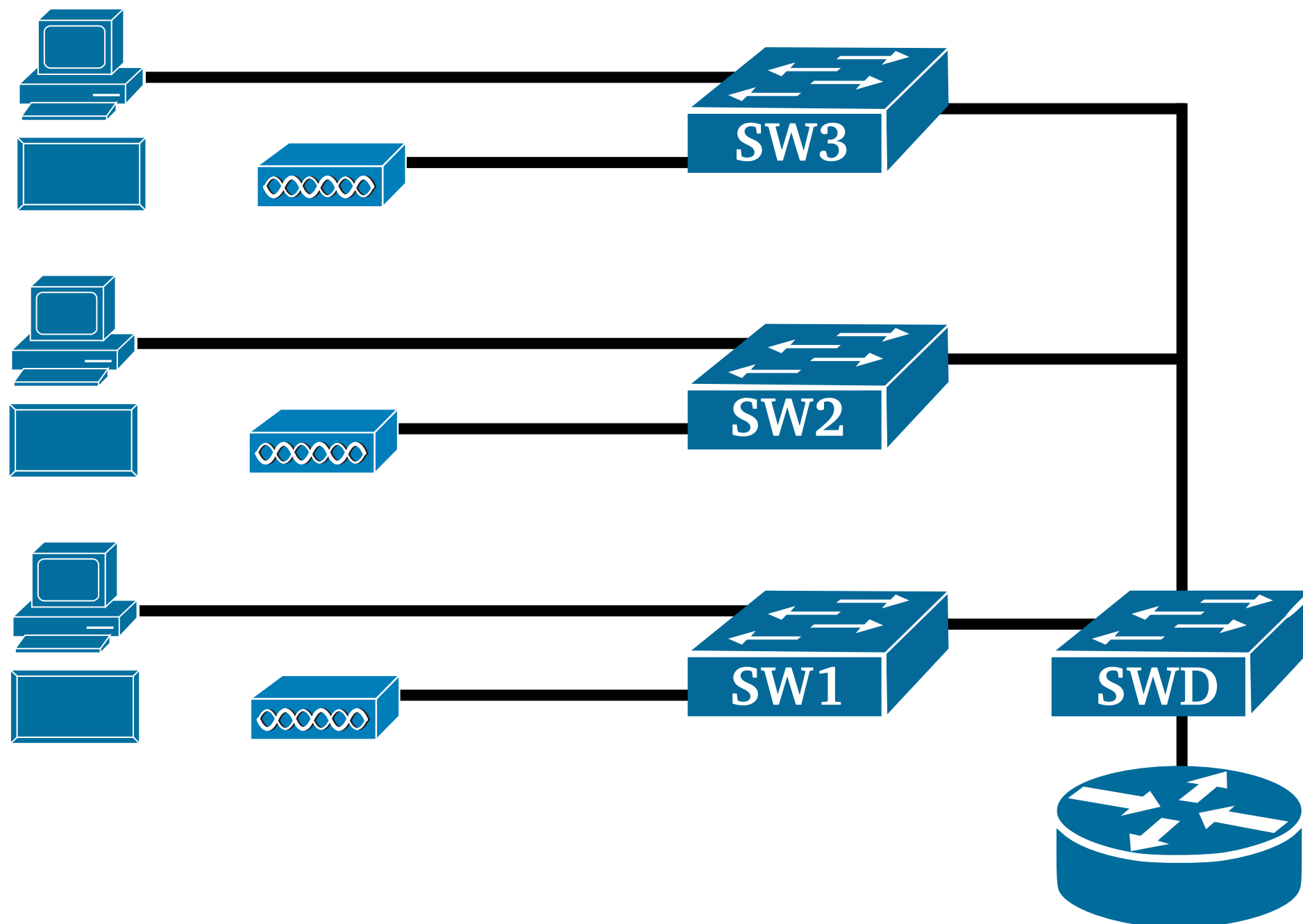
Типичная топология домашней сети



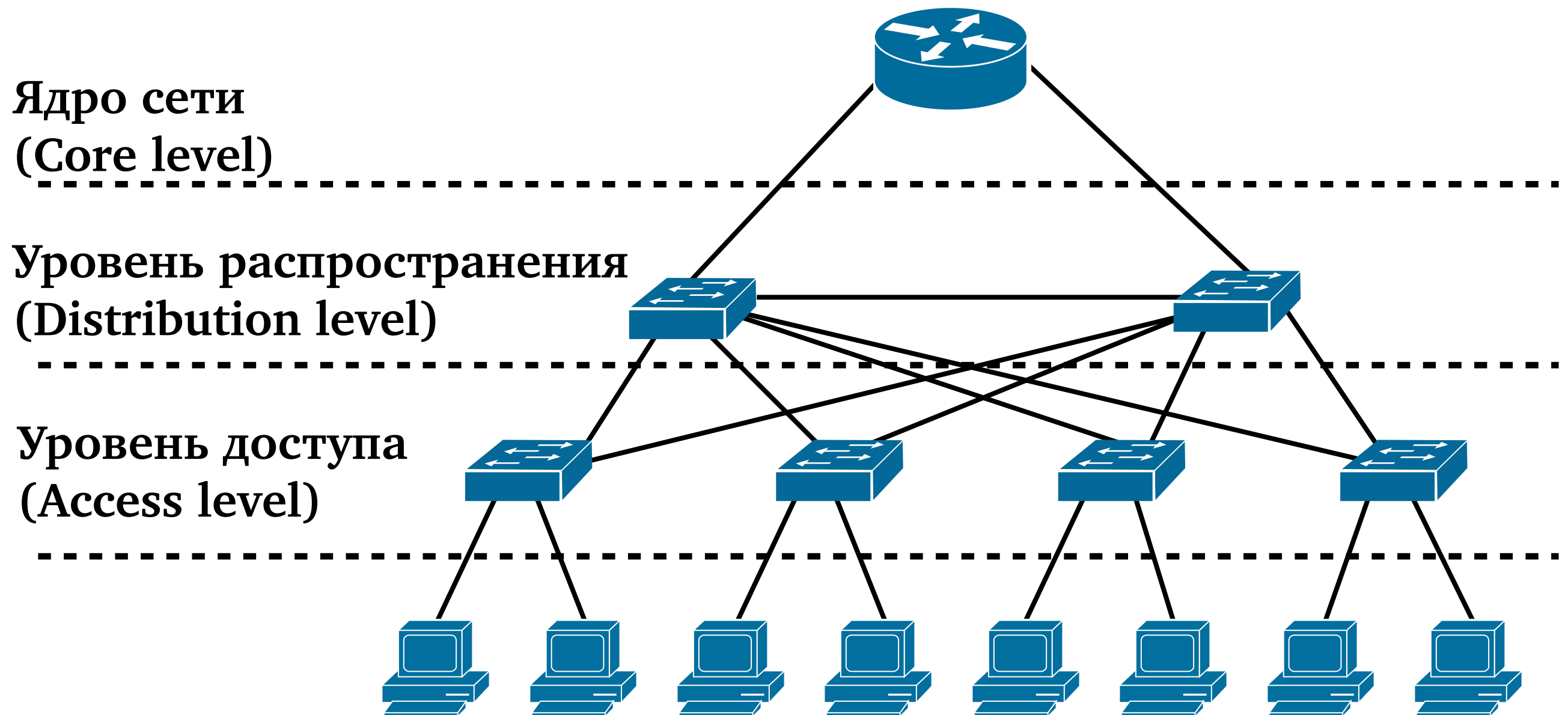
Типичная топология домашней сети



Типичная топология корпоративной сети



Типичная топология корпоративной сети



Эталонная модель OSI

**OSI - Open System Interconnection
PDU - Protocol Data Unit**

Сравнение моделей OSI и TCP/IP

OSI		TCP/IP
Приложений	Application	Приложений
Представления	Presentation	
Сеансовый	Session	
Транспортный	Transport	Транспортный
Сетевой	Network	Сетевой
Канальный	Data link	Канальный
Физический	Physical	Физический

Физический уровень

Физический уровень (physical layer) определяет электрические, процедурные и функциональные спецификации для среды передачи данных, в том числе стандартные разъемы, распайку, назначение контактов, уровни напряжений, кодирование сигнала в среде, методы модуляции световых сигналов, правила активации/деактивации физической среды передачи.

Канальный уровень

Канальный уровень (data link layer) обеспечивает надежную передачу данных по физическому каналу. Он задает правила (протоколы), определяющие, как именно устройство может пересылать данные в определенной среде передачи. Протоколы канального уровня также задают форматы заголовков и концевиков второго уровня. Концевик второго уровня, которым завершаются инкапсулированные данные, обычно содержит поле контрольной суммы фрейма (FCS - Frame Check Sequence), используемое принимающим устройством для контроля ошибок передачи.

Сетевой уровень

Логическая адресация указывает, как именно должен быть сформирован адрес устройства в сети и как он будет использован.

Концепция маршрутизации определяет, как именно специализированные устройства (маршрутизаторы) перенаправляют пакеты к конечному получателю.

Механизм определения маршрутов указывает, как именно протоколы маршрутизации, которым известны абсолютно все маршруты в сети, выбирают и используют наилучший из них.

Сетевой уровень

Сетевой уровень (network layer) является комплексным уровнем, обеспечивающим выбор маршрута и соединение между собой двух рабочих станций, которые могут быть установлены в географически удаленных друг от друга сетях. Он решает три основных задачи: логическая адресация, маршрутизация (перенаправление пакетов) и определение маршрутов в сети.

Транспортный уровень

Транспортный уровень (transport layer) сегментирует данные передающей станции и вновь собирает их в одно целое на принимающей стороне. Протоколы этого уровня предоставляют множество служб, сфокусированных на проблемах доставки данных удаленному компьютеру, например, коррекцией ошибок и контролем потока данных.

Сеансовый уровень

Сеансовый уровень (session layer) устанавливает сеансы связи между двумя рабочими станциями, управляет ими и разрывает их. Он также синхронизирует диалог между уровнями представления двух систем и управляет двунаправленным обменом данными таким образом, что приложения верхних уровней уведомляются о получении некоторого завершеного набора сообщений.

Уровень представления

Уровень представления преобразует данные в один из многочисленных форматов, который поддерживается обеими сторонами, а также отвечает за согласование формата передачи данных, например, кодировку текста, формат изображений и других файлов. К данному уровню относится шифрование, которое является его службой.

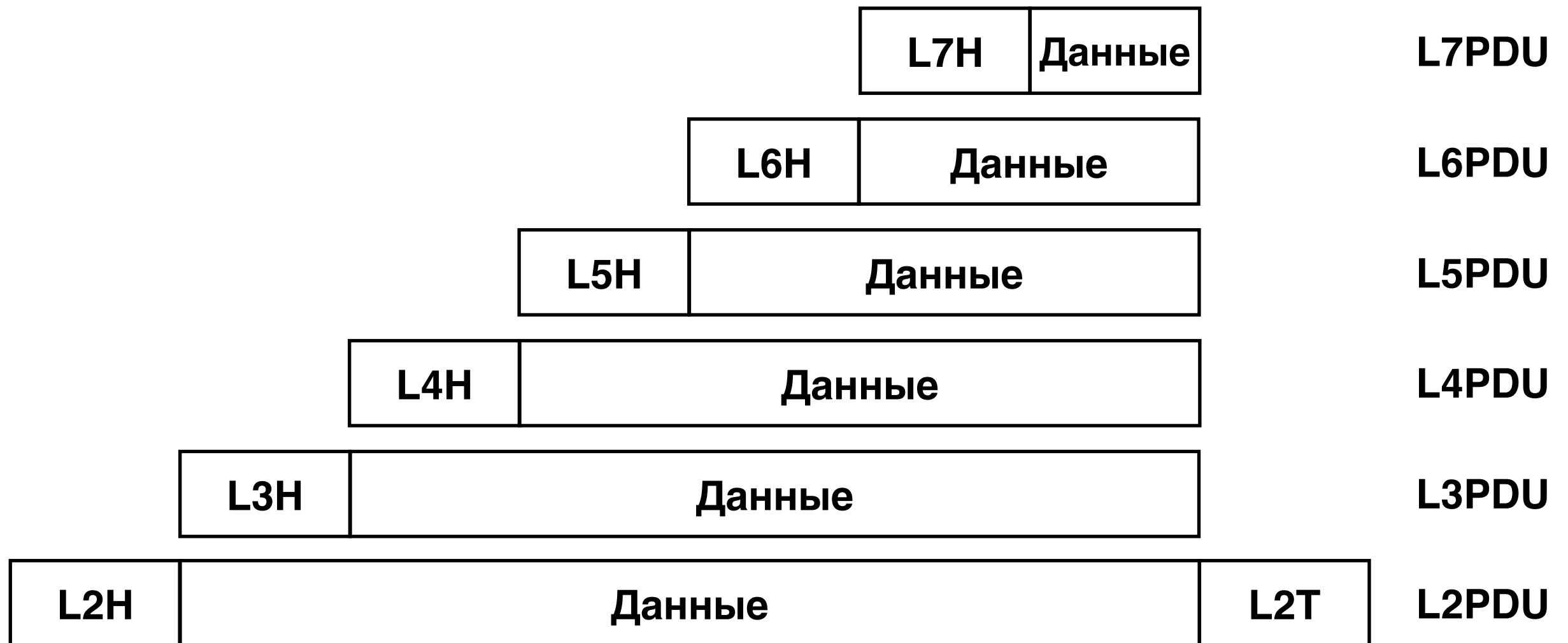
Уровень приложений

Уровень приложений (application layer) является ближайшим к пользователю и предоставляет службы его приложениям. Он является интерфейсом между приложениями и коммуникационным программным обеспечением.

Примеры устройств и протоколов по уровням модели OSI

Название уровня	Протоколы и спецификации	Устройства
Уровни приложений, представления и сеансовый	Telnet, POP3, SMTP, HTTP, FTP, SNMP	Хосты, брандмауэры
Транспортный	TCP, UDP	Хосты, брандмауэры
Сетевой	IP	Маршрутизатор
Канальный	Ethernet, HDLC, Frame Relay, PPP	Коммутатор, кабельный модем, DSL-модем
Физический	Ethernet, RJ-45, V.35, EIA/TIA-232	Концентратор, повторитель

Инкапсуляция и блоки PDU в модели OSI



Преимущества многоуровневых сетевых моделей

- Упрощение решаемых задач. Многоуровневая модель позволяет разделить задачу на меньшие и более простые этапы. Стандартизация интерфейсов взаимодействия уровней позволяет разным производителям создавать устройства, ориентированные на выполнение какой либо определенной функции.
- Упрощение процесса обучения. Людям намного проще изучать детали отдельных протоколов и уровней.
- Упрощение процесса разработки новых устройств. Чем проще продукты и устройства, тем проще и быстрее можно внести в них какие-либо изменения, а также разработать новые продукты.
- Совместимость устройств раз производителей. Если устройства отвечают одним и тем же стандартам, это означает, что компьютеры и сетевое оборудование от разных производителей будет работать корректно.
- Модульные разработки. Один производитель может написать программное обеспечение, работающее на верхних уровнях, а другой разработчик может написать программное обеспечение нижних уровней.

Преимущества многоуровневых сетевых моделей

- Упрощение решаемых задач
- Упрощение процесса обучения
- Упрощение процесса производства
- Совместимость устройств разных производителей
- Стандартизация интерфейсов
- Возможность модульных разработок

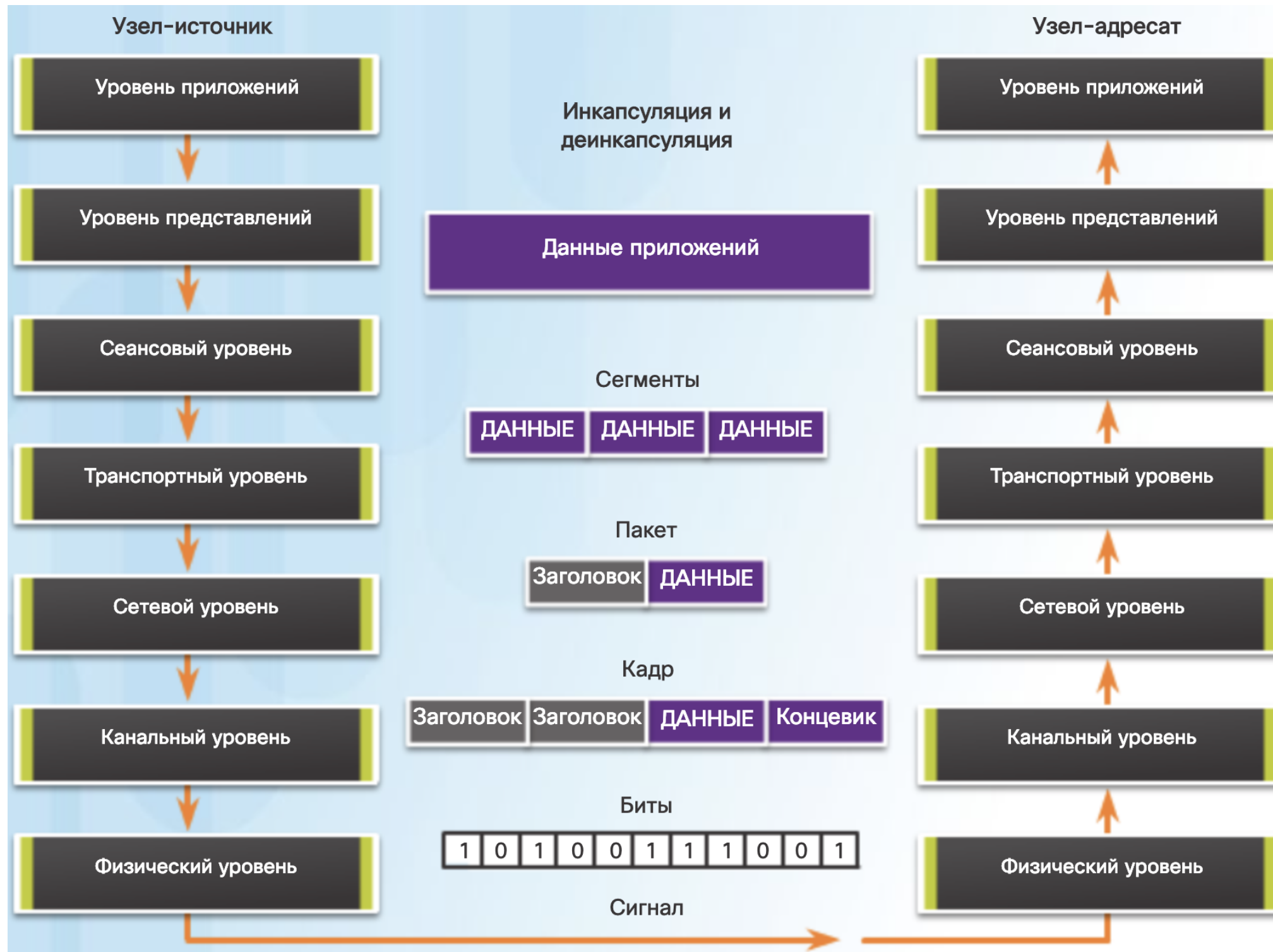
ОСНОВЫ ЛОКАЛЬНЫХ сетей

LAN - Local Area Network

UTP - Unshielded Twisted Pair

SMF - Single Mode Fiber

Представление данных на разных уровнях



Ethernet (IEEE 802.3)

Семейство стандартов, определяющих особенности передачи по конкретному типу кабелей (медный или оптический) на конкретной скорости , а также их максимальную длину; протоколы и правила, которым должны соответствовать узлы, чтобы быть частью одной LAN.

Пропускная способность

Пропускная способность (bandwidth) — это количественная характеристика, отражающая возможности передачи данных по конкретному средству подключения. В цифровых сетях под пропускной способностью понимается объем данных, который можно передать из одной точки в другую за определенное время.

Зависит от физических свойств среды передачи и технологии передачи сигналов.

Производительность (throughput) — это количество битов, передаваемых по средствам подключения за определенный период времени.

Зависит от типа и объема трафика, суммарной задержки между источником и пунктом назначения.

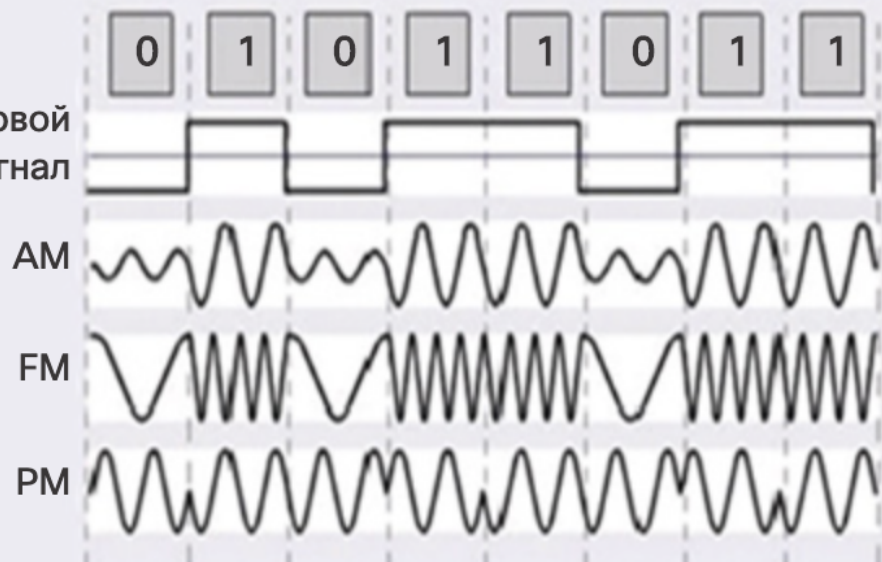
Средства подключения физического уровня

Сигнал исходящих вызовов (Tx)

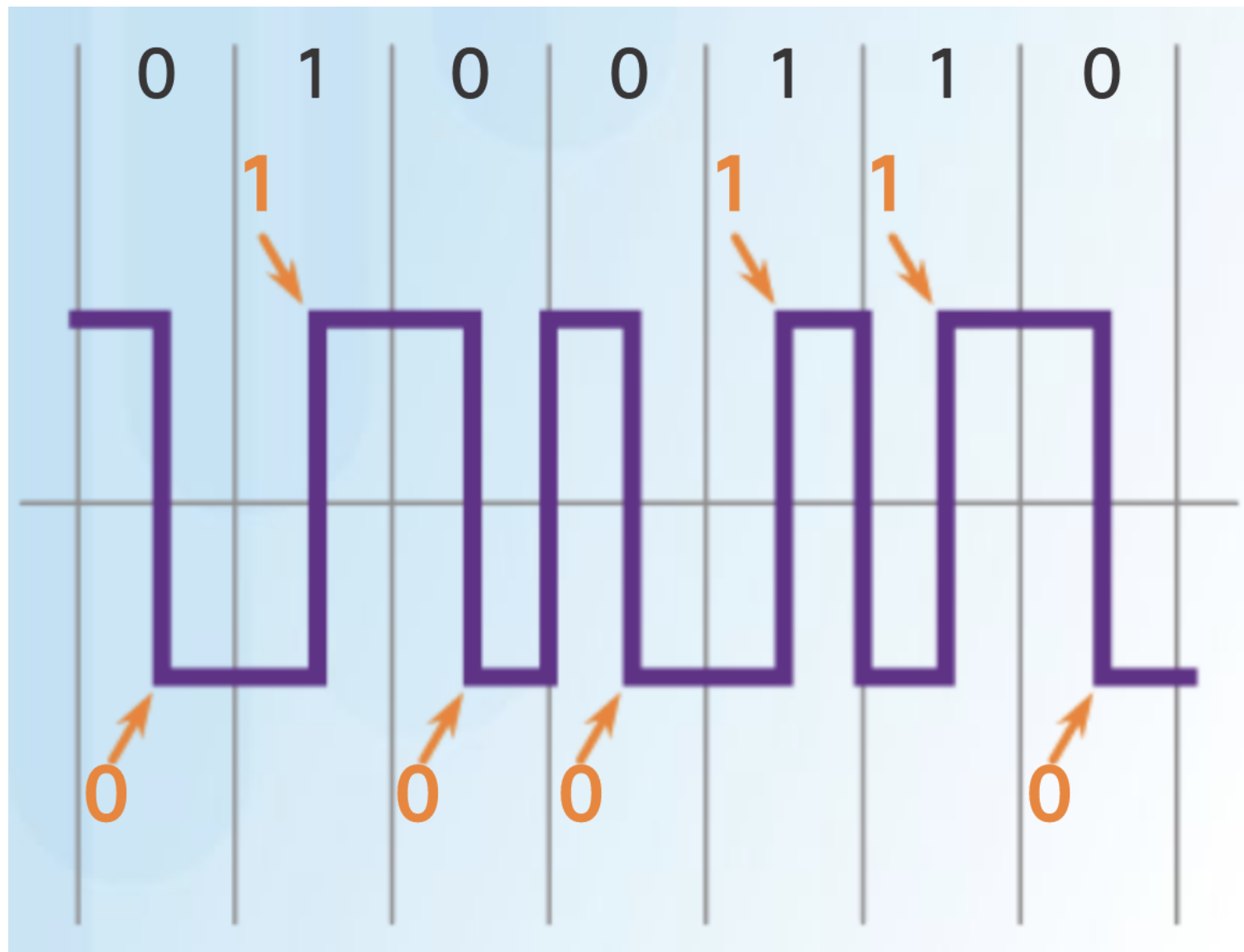


- Медный кабель: сигналы представляют собой последовательность электрических импульсов.
- Оптоволоконный кабель: сигналы представляют собой управляемые изменения светового излучения.
- Беспроводная сеть: сигналы представляют собой радиосигналы микроволнового диапазона.

Цифровой сигнал



Функции физического уровня

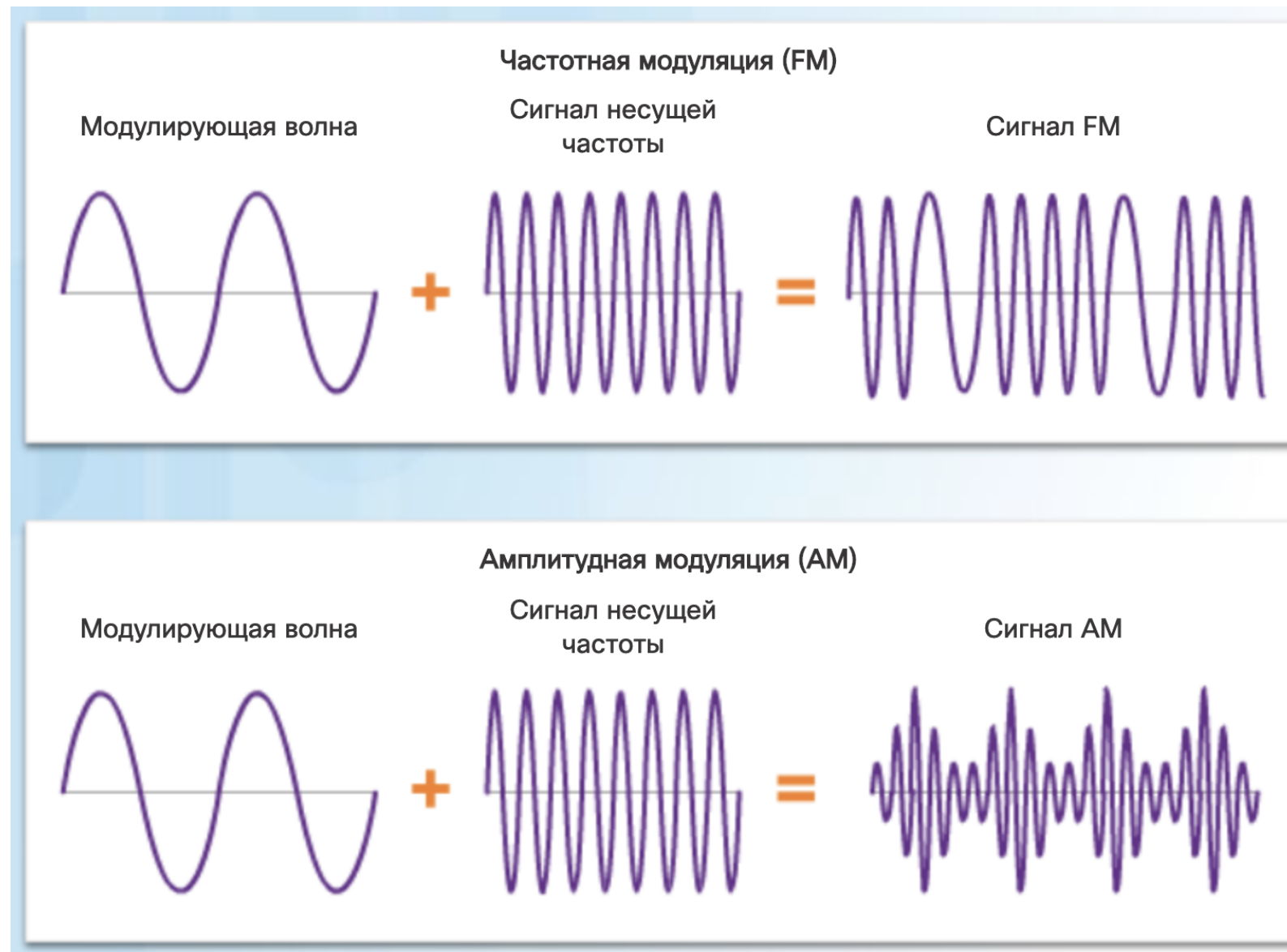


Кодирование — это способ преобразования потока битов в определенный «символ».

Символы — это группы битов, используемые для формирования предсказуемых комбинаций, которые могут распознаваться как отправителем, так и получателем.

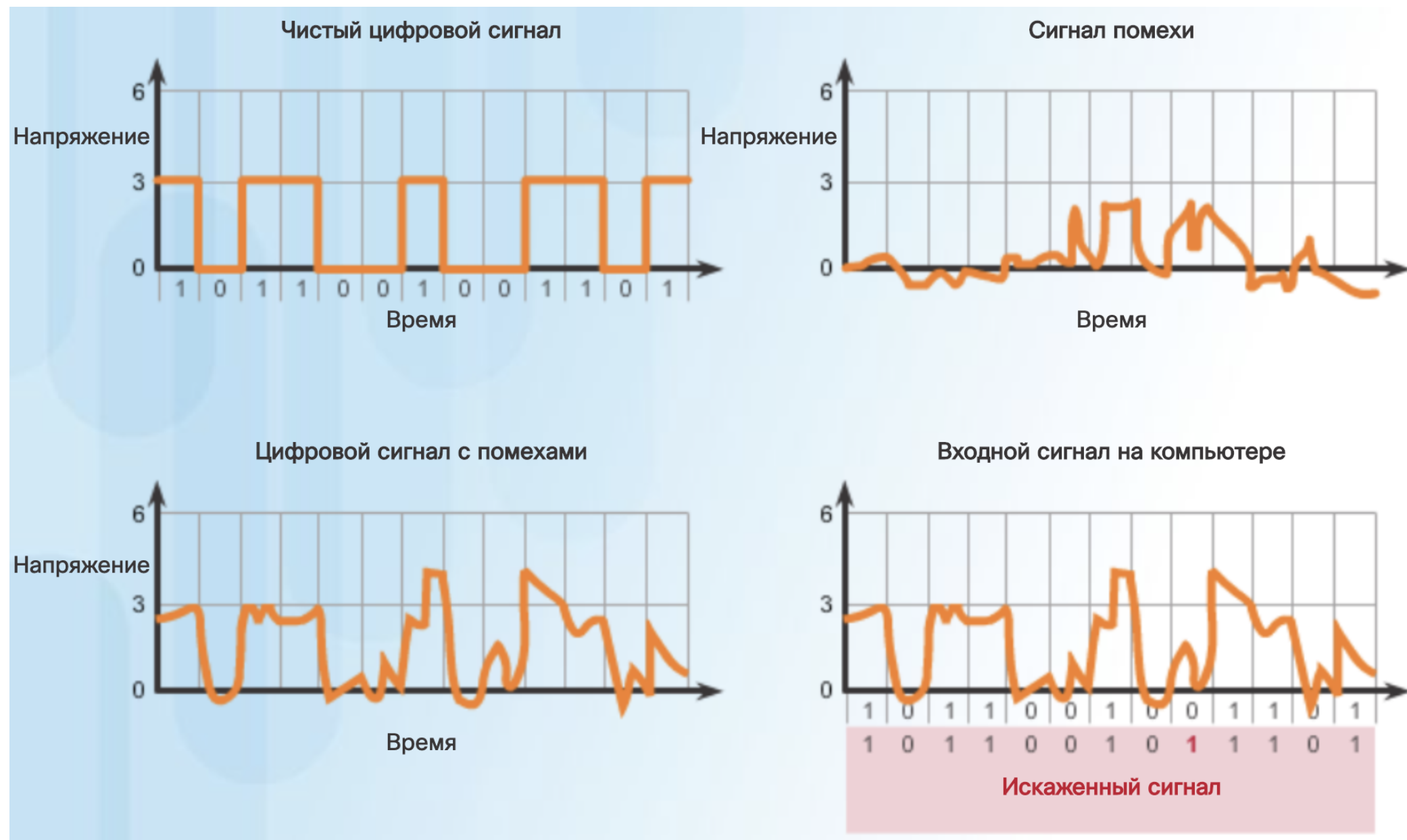
Например, при манчестерском кодировании нули будут представлены переходом от высокого напряжения к низкому; а единицы — переходом от низкого напряжения к высокому.

Функции физического уровня



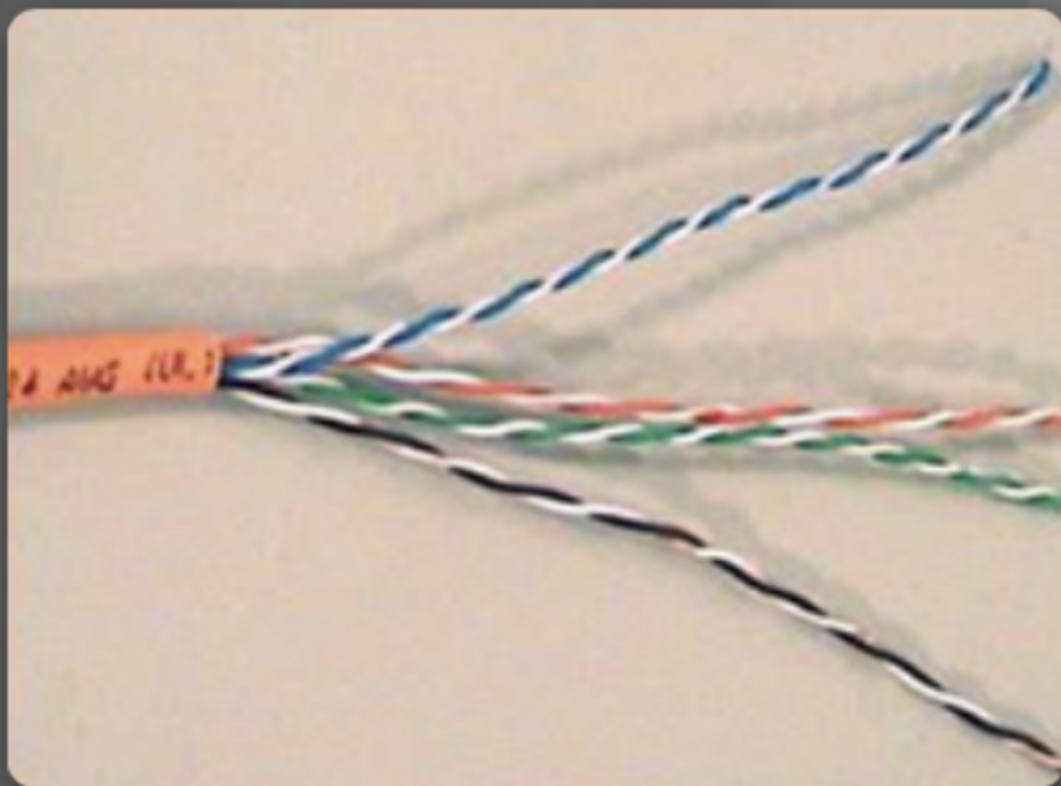
Для представления значений битов «1» и «0» в среде передачи физический уровень должен генерировать электрические, оптические или радиосигналы. Метод представления битов с помощью сигналов называется способом передачи сигналов. Стандарты физического уровня должны определять, какой тип сигнала соответствует единице («1»), а какой нулю («0»).

Функции физического уровня

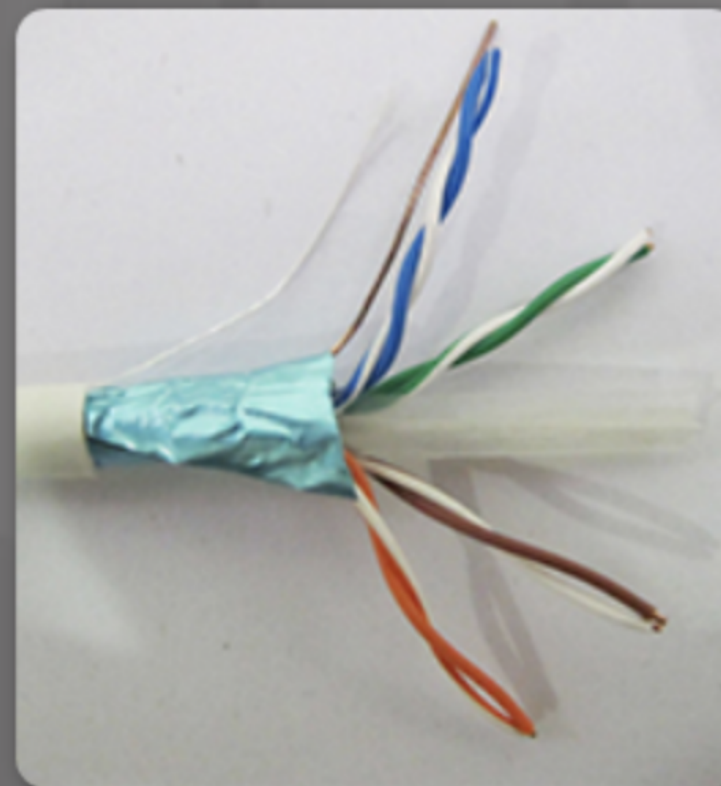


Временные характеристики и значения напряжения электрических импульсов подвержены влиянию электромагнитных и переходных помех.

Типы медных кабелей



Кабель на основе неэкранированной витой пары (UTP)



Кабель на основе экранированной витой пары (STP)



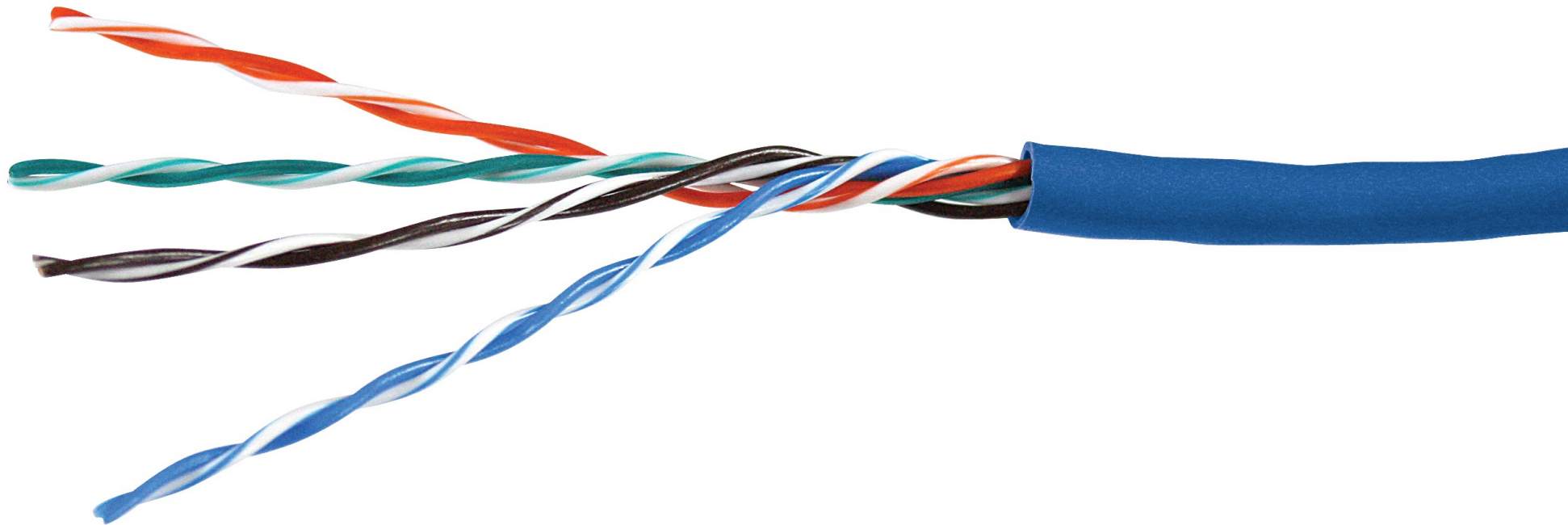
Коаксиальный кабель

Коаксиальный кабель



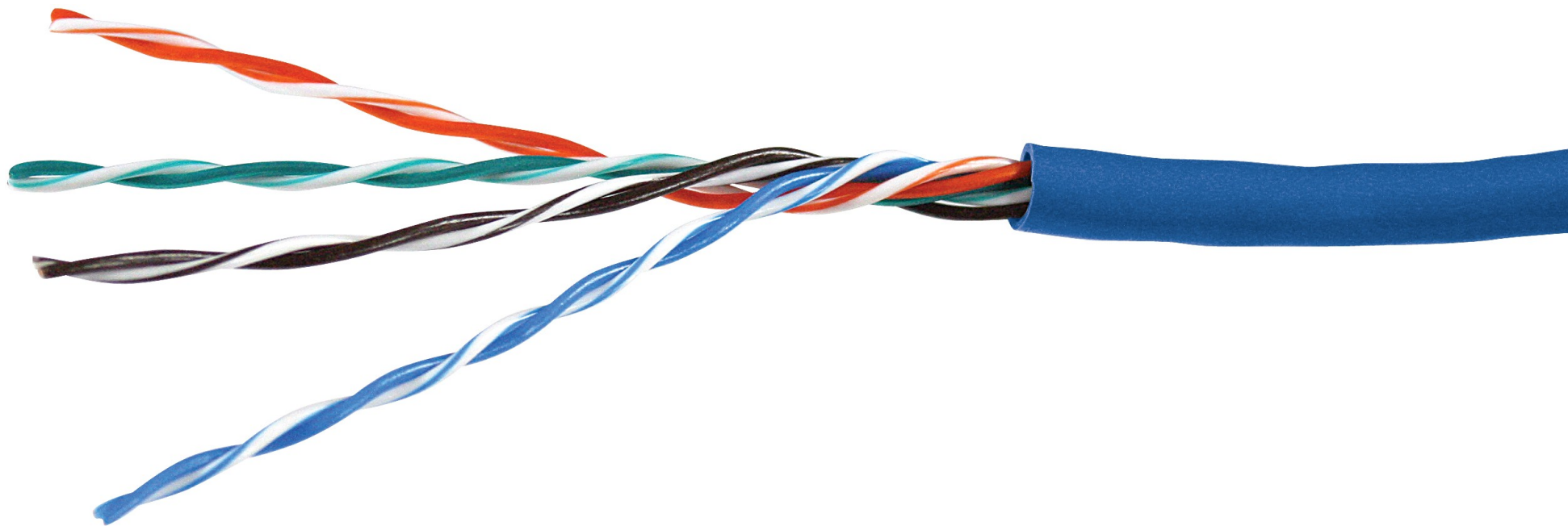
Стандарт	IEEE-номер	Скорость	Макс. расстояние	Тип кабеля
10Base5	802.3	10 Мбит/с	500 м	RG-11
10Base2	802.3	10 Мбит/с	180 м	RG-58

Витая пара



Стандарт	IEEE-номер	Скорость	Макс. расстояние	Тип кабеля
10BaseT	802.3	10 Мбит/с	100 м	UTP cat3
100BaseTX	802.3u	100 Мбит/с	100 м	UTP cat5
1000BaseT	802.3ab	1 Гбит/с	100 м	UTP cat5e, 6
10GBaseT	802.3an	10 Гбит/с	100 м	UTP cat6a, 7
40GBaseT	802.3bq	40 Гбит/с	>30 м	UTP cat8.1

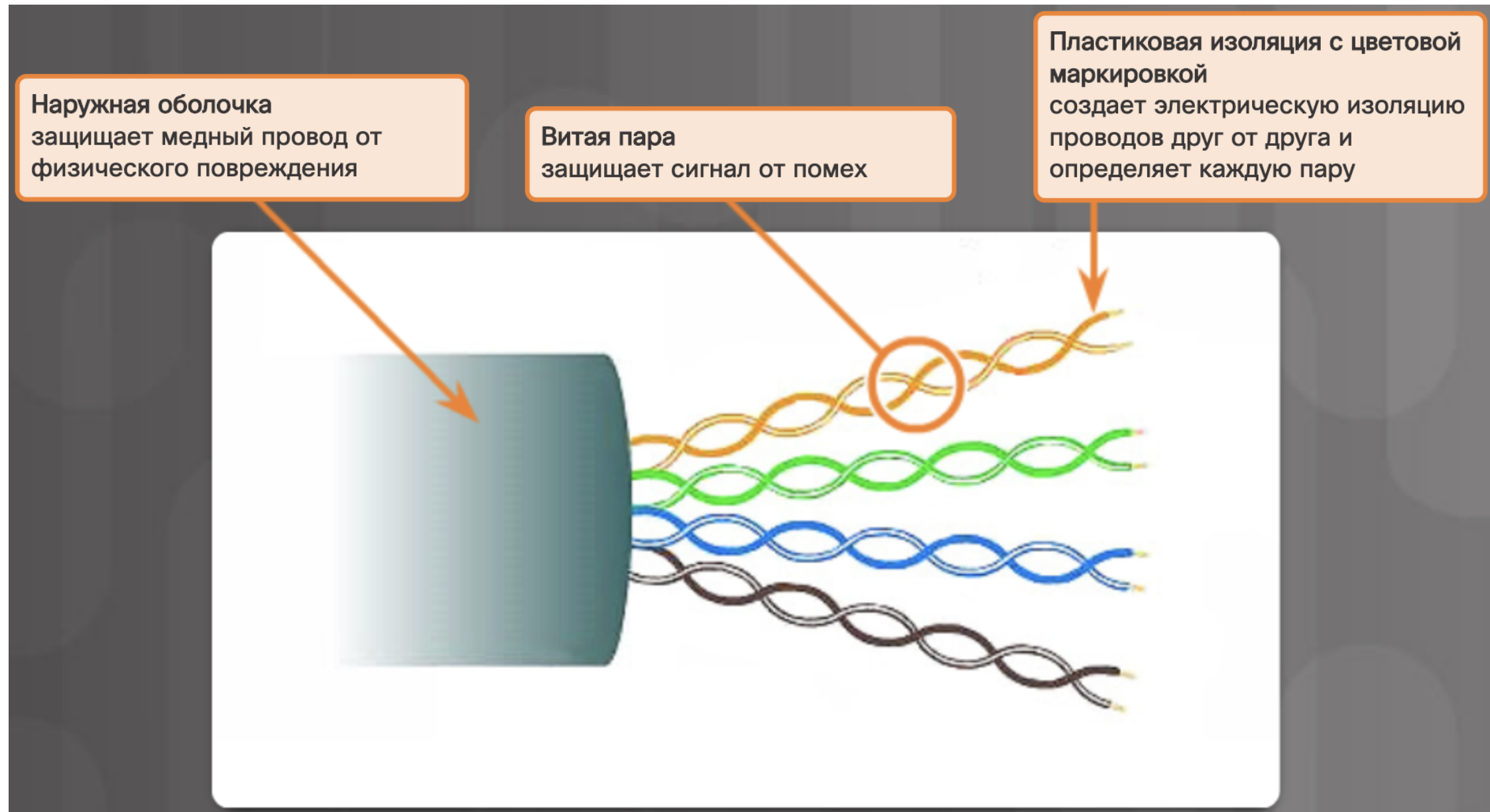
Витая пара



Взаимоподавление. Проектировщики объединяют провода одной электрической цепи в пару. При размещении двух проводов одной электрической цепи в непосредственной близости друг к другу магнитные поля вокруг них противоположны друг другу. Поэтому два магнитных поля взаимно компенсируются, а также обеспечивается компенсация влияния внешних ЭМП и РЧП.

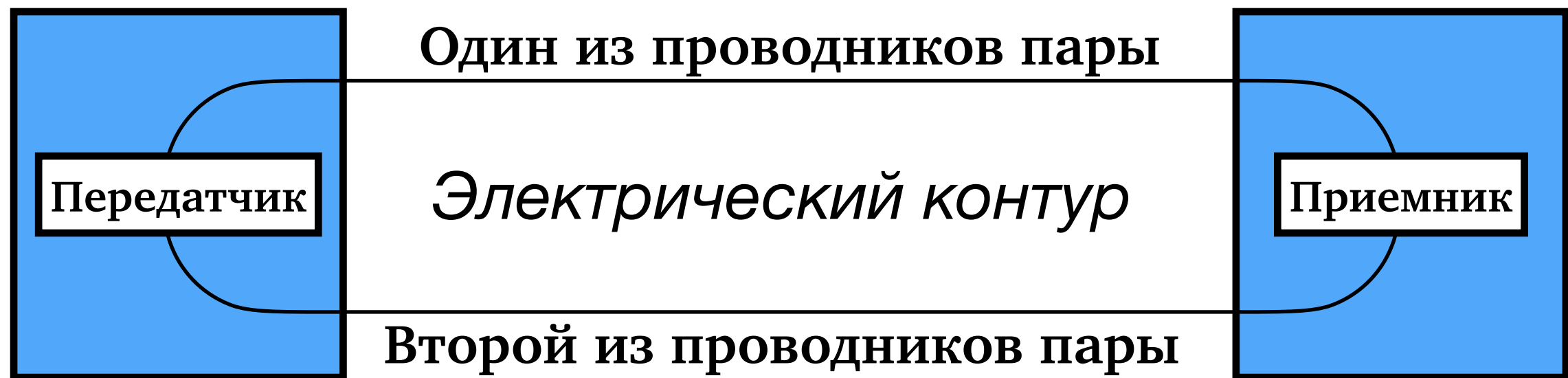
Различный шаг витков в парах. Для повышения эффекта подавления помех используют различный шаг витков в соседних парах одного кабеля. Кабели UTP должны точно соответствовать спецификациям, регламентирующим допустимое количество витков на 1 метр кабеля.

Витая пара



Кабель UTP для локальных сетей состоит из четырех скрученных пар проводников с цветовой маркировкой, которые заключены в общую гибкую пластиковую оболочку. Скручивание проводников снижает влияние помех от других проводников.

Передача данных посредством витой пары

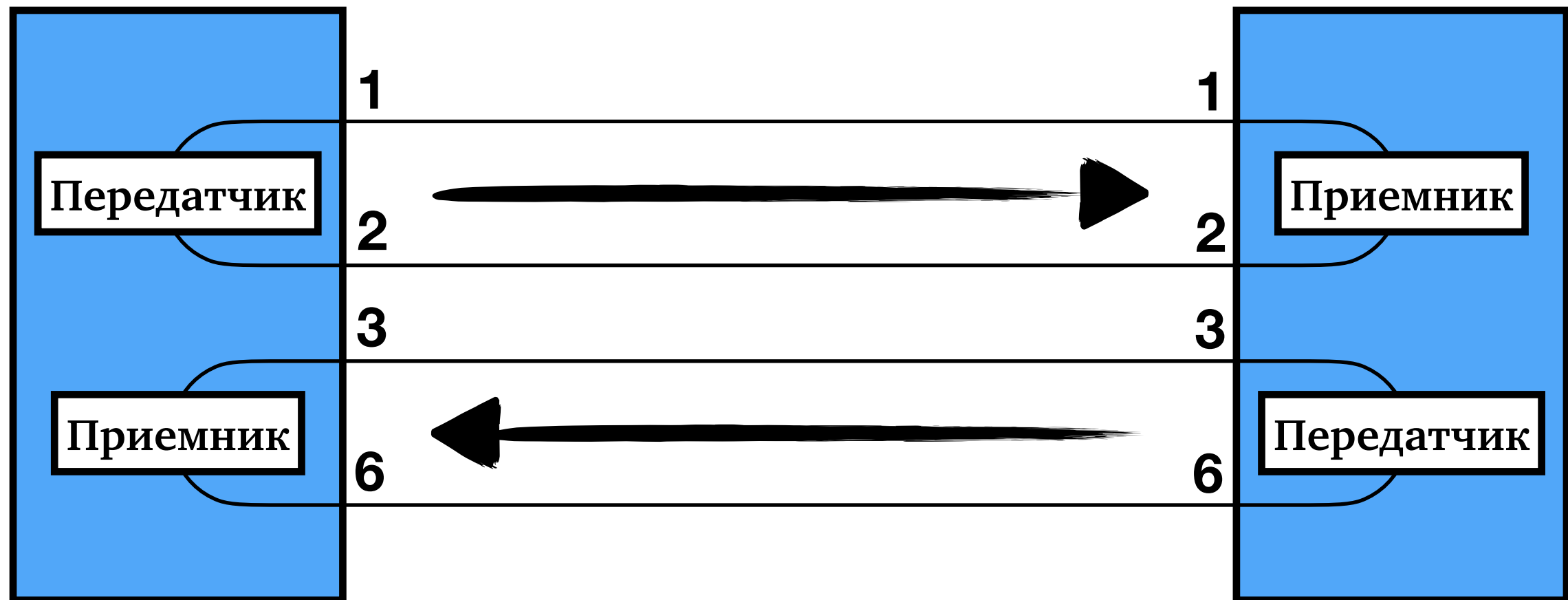


Передача данных по витой паре физически означает использование электрических сигналов, передаваемых по проводникам внутри кабеля.

Для понимания этого необходимо ответить на два вопроса: как сконструировать электрический контур и как передавать логические «0» и «1».

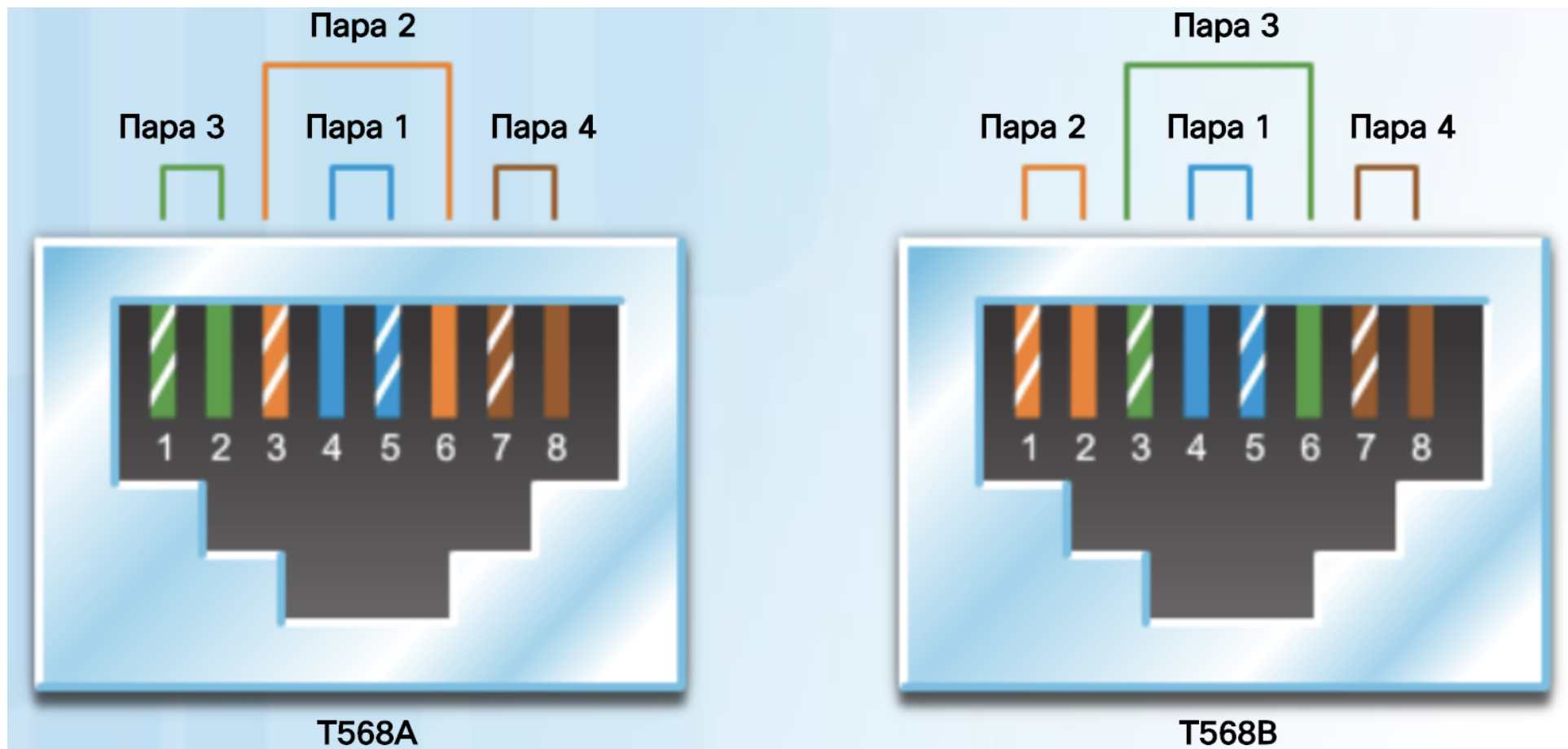
Схема расположения кабелей витой пары по стандарту 10BASE-T

Стандарты 10BASE-T и 100BASE-T подразумевают использование двух пар проводов кабеля UTP, по одной для каждого направления передачи данных



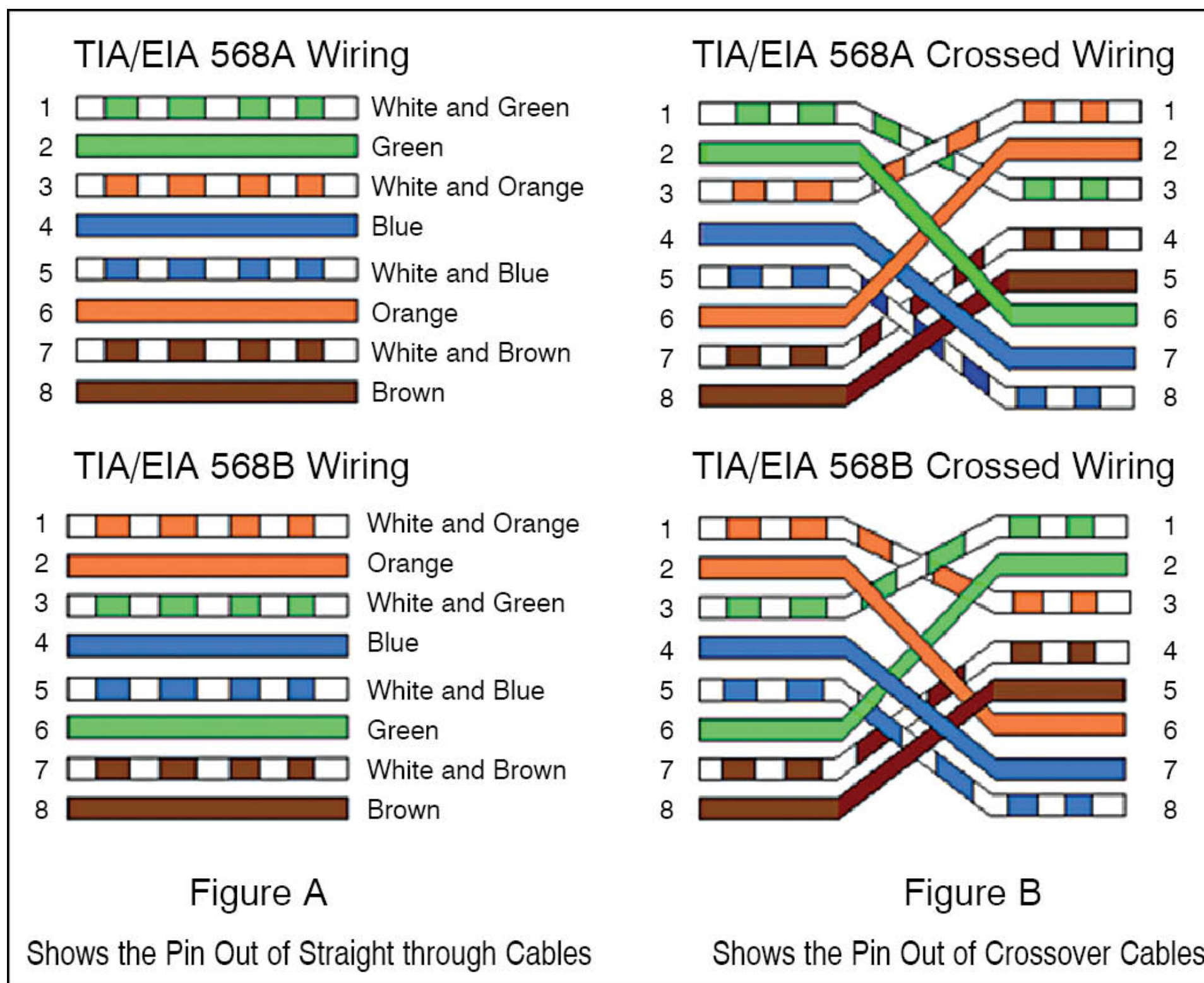
Для правильной передачи информации провода кабеля UTP должны быть подключены к правильным контактным площадкам разъемов RJ45

Типы кабелей UTP



Тип кабеля	Стандарт	Применение
Прямой кабель Ethernet	Оба конца 568А или 568В	используется для подключения узла к коммутатору и коммутатора к маршрутизатору
Перекрестный кабель Ethernet	Один конец 568А, другой - 568В	используется для соединения однотипных устройств, например для подключения коммутатора к коммутатору

ОСНОВЫ ЛОКАЛЬНЫХ СЕТЕЙ



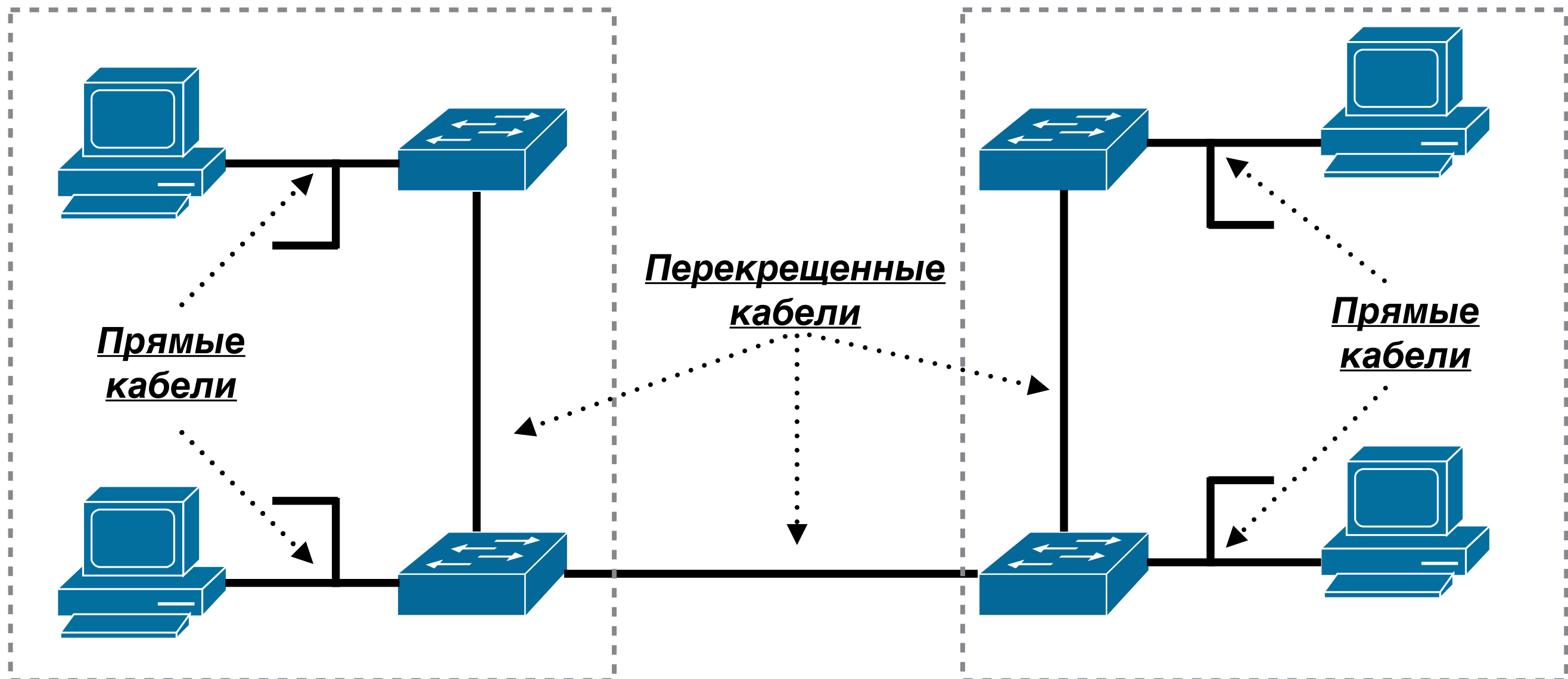
ОСНОВЫ ЛОКАЛЬНЫХ СЕТЕЙ

Передача на контактах 1 и 2

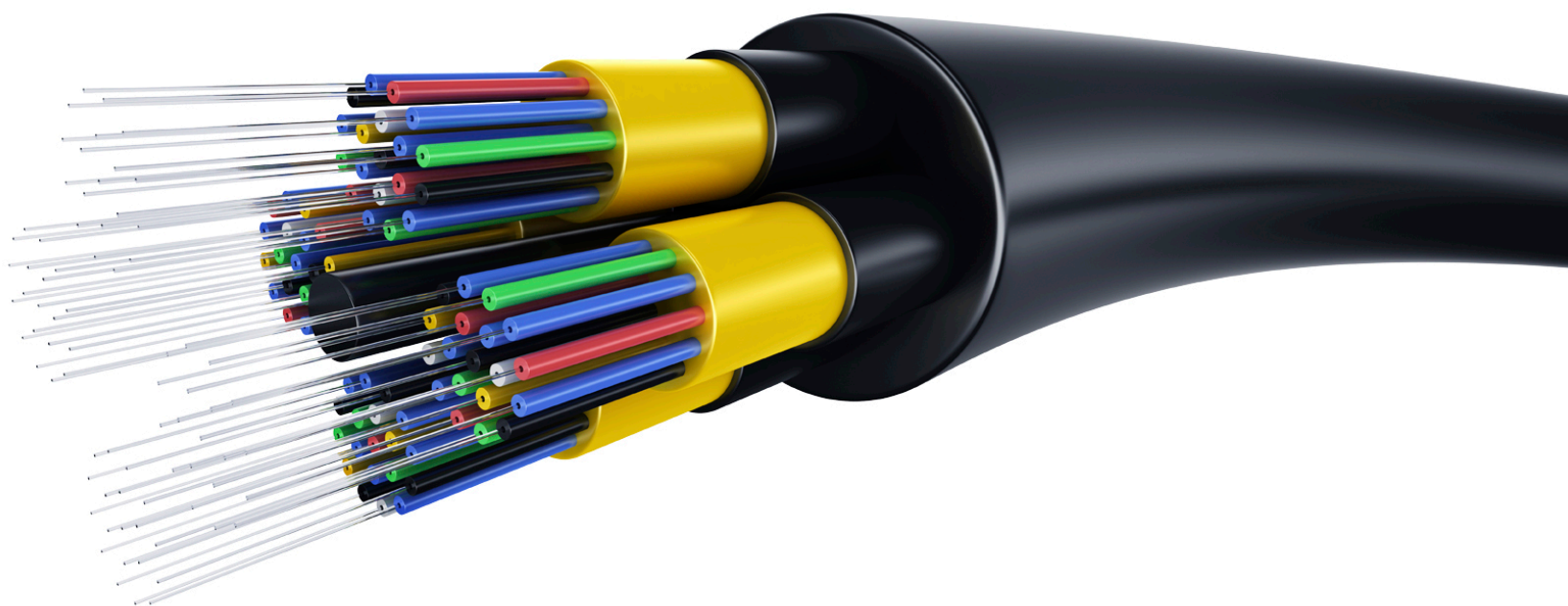
Передача на контактах 3 и 6

Сетевые адаптеры ПК
Маршрутизаторы
Беспроводные точки доступа

Концентраторы
Коммутаторы



Оптическое волокно

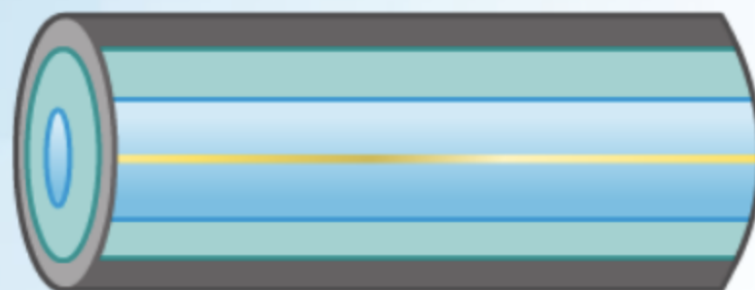
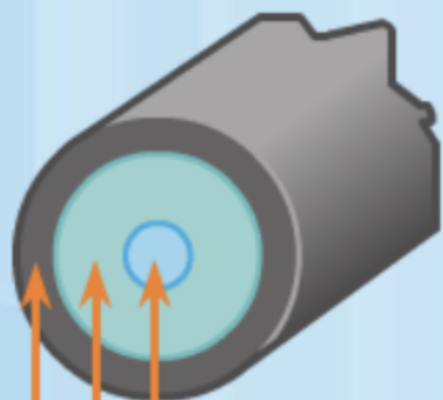


Стандарт	IEEE-номер	Скорость	Макс. расстояние	Тип кабеля
10BaseF	802.3	10 Мбит/с	2 км	MMF
			25 км	SMF
100BaseFX	802.3u	100 Мбит/с	2 км	MMF
			25 км	SMF
1000BaseSX	802.3z	1 Гбит/с	260 м	MMF (62,5 мкм)
			550 м	MMF (50 мкм)
1000BaseLX	802.3z	1 Гбит/с	550 м	MMF (50 мкм)
			3 км	SMF

Оптическое волокно

Одномодовый кабель

Создает прямую траекторию для света



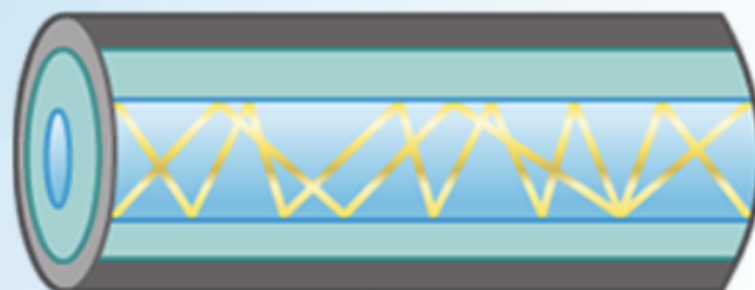
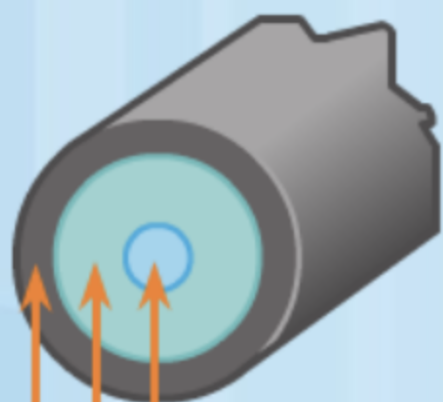
Стеклянный сердечник = 9 микрон

Стеклянная оболочка, 125 микрон в диаметре

Полимерное покрытие

Многомодовый кабель

Позволяет свету проходить по нескольким траекториям



Стеклянный сердечник = 50/62,5 микрон

Стеклянная оболочка, 125 микрон в диаметре

Покрытие

Одномодовый оптоволоконный кабель (ООК). Имеет сердечник очень малого диаметра. Для передачи луча света требуется дорогостоящая лазерная технология. Широко используется для организации линий связи протяженностью несколько сотен километров.

Многомодовый оптоволоконный кабель (МОК). Имеет сердечник большего диаметра. Для передачи световых импульсов используются светодиодные излучатели. Свет, излучаемый светодиодом, входит в многомодовое волокно под разными углами. Многомодовый кабель обеспечивает пропускную способность до 10 Гбит/с на расстоянии до 550 метров.

Недостатки проводных LAN

- Одним кабелем можно соединить только два устройства;**
- Сигнал передается строго по траектории прокладки кабеля;**
- Необходимы разъемы, причем для каждого типа кабеля уникальные;**
- Соединенные устройства недостаточно мобильны.**

Протоколы беспроводной связи на нижних уровнях

Основное семейство протоколов беспроводной связи регламентируется стандартами группы IEEE 802.11 различных версий (b,g,n,ac,ad...).

Также для передачи информации могут применяться такие протоколы и технологии как Bluetooth(IEEE 802.15.1), ZigBee (IEEE 802.15.4), NFC, RFID.

Особенности WLAN

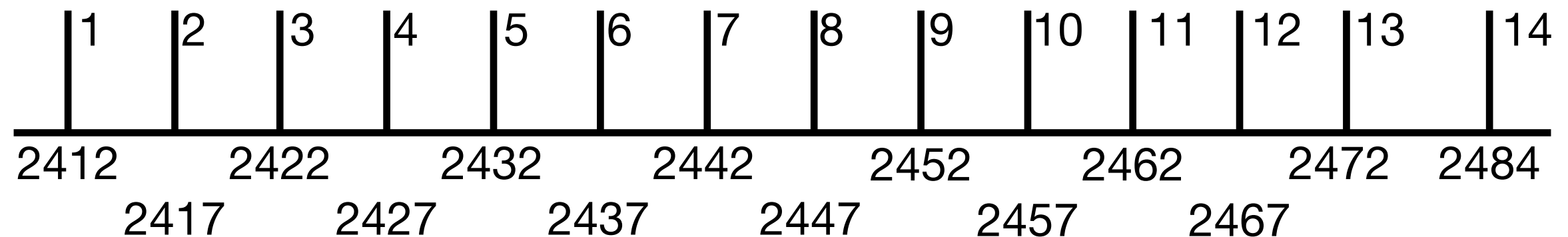
- Зона покрытия. Беспроводные технологии передачи данных хорошо работают на открытых пространствах. Однако некоторые строительные материалы, используемые при возведении зданий и сооружений, а также условия местности могут ограничивать зону покрытия.
- Помехи. Качество беспроводных соединений восприимчиво к помехам и может ухудшаться при работе таких обычных устройств, как беспроводные телефоны, некоторые типы флуоресцентных ламп, микроволновые печи, а также под влиянием других беспроводных коммуникаций.
- Безопасность. Для доступа к среде беспроводного подключения не требуется подключаться к физическим кабелям. Поэтому доступ к этой среде могут получать несанкционированные пользователи и устройства.
- Совместный доступ к средству подключения. Сети WLAN работают в полудуплексном режиме, что означает, что в каждый момент времени передачу или прием может осуществлять только одно устройство. Средства беспроводного подключения совместно используют все беспроводные пользователи. Чем больше пользователей одновременно подключаются к WLAN, тем меньшая пропускная способность приходится на каждого из них.

Свойства радиоволны

- Частота сигнала - количество полных циклов за единицу времени.**
- Амплитуда - максимальное отклонение от нулевого значения.**
- Фаза сигнала - мера сдвига во времени по отношению к началу периода.**

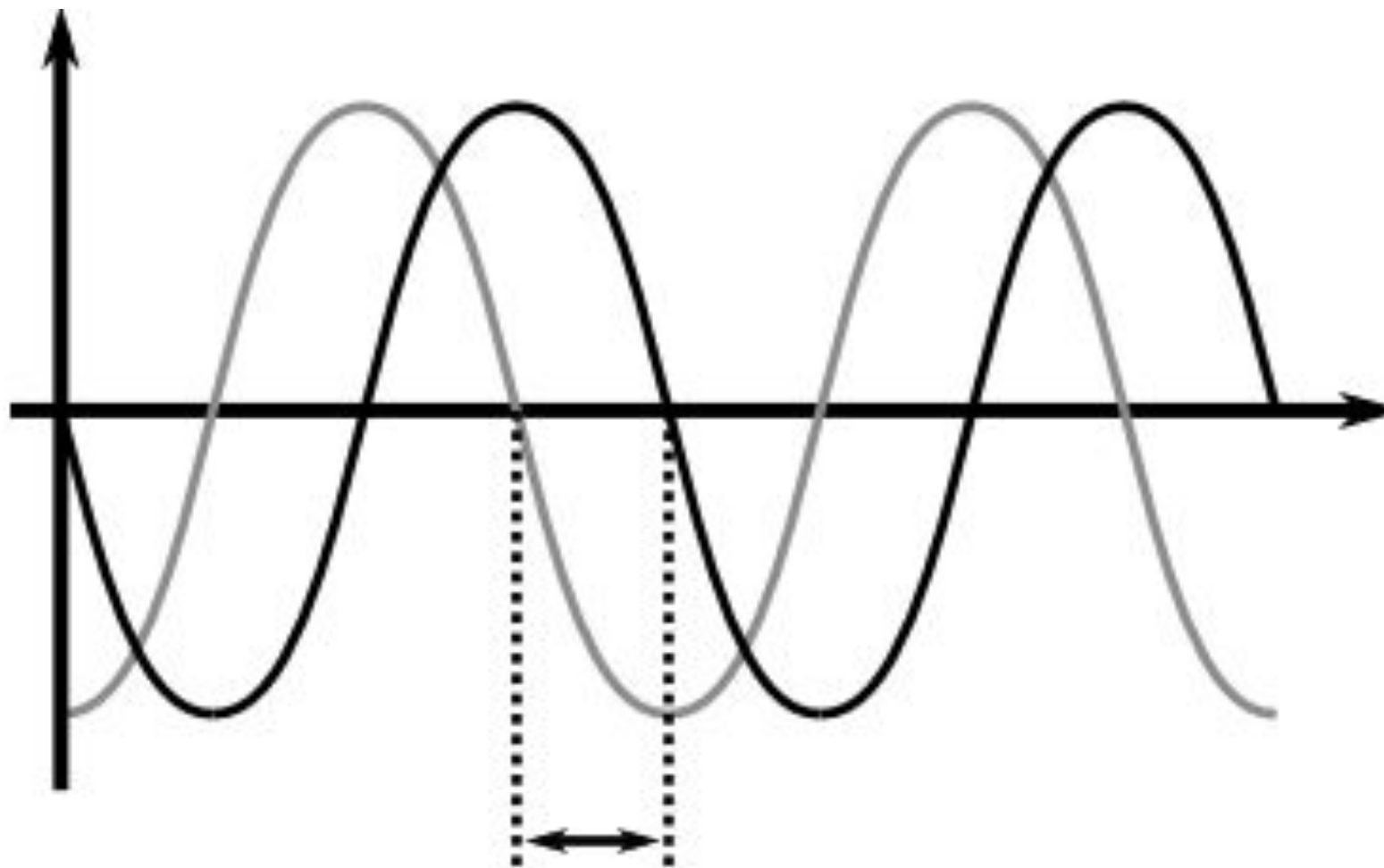
Радиочастоты

- Диапазон частот примерно от 3кГц до 300ГГц называют радиочастотами;
- Два основных используемых в WLAN частотных диапазона - 2,4ГГц и 5ГГц;
- Полосы частот, используемые в них:
 - 2400 - 2483,5 МГц,
 - 5150 - 5250 МГц,
 - 5250 - 5350 МГц,
 - 5470 - 5725 МГц,
 - 5725 - 5825 МГц;



Фаза сигнала

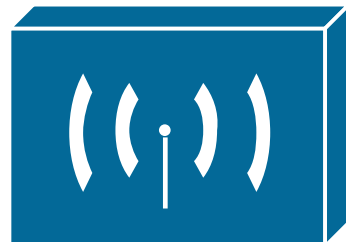
Фаза сигнала - мера сдвига во времени по отношению к началу периода.



Мощность сигнала

Типичный LAN-радиопередатчик имеет мощность от 1 до 100 мВт

T1



1 мВт

T2



10 мВт

T3



100 мВт

$$T2 - T1 = 9 \text{ мВт}$$

$$T2 / T1 = 10$$

$$T3 - T2 = 90 \text{ мВт}$$

$$T3 / T2 = 10$$

T4



0,00001 мВт

T5



10 мВт

$$T5 - T4 = 9,9999 \text{ мВт}$$

$$T5 / T4 = 1000000$$

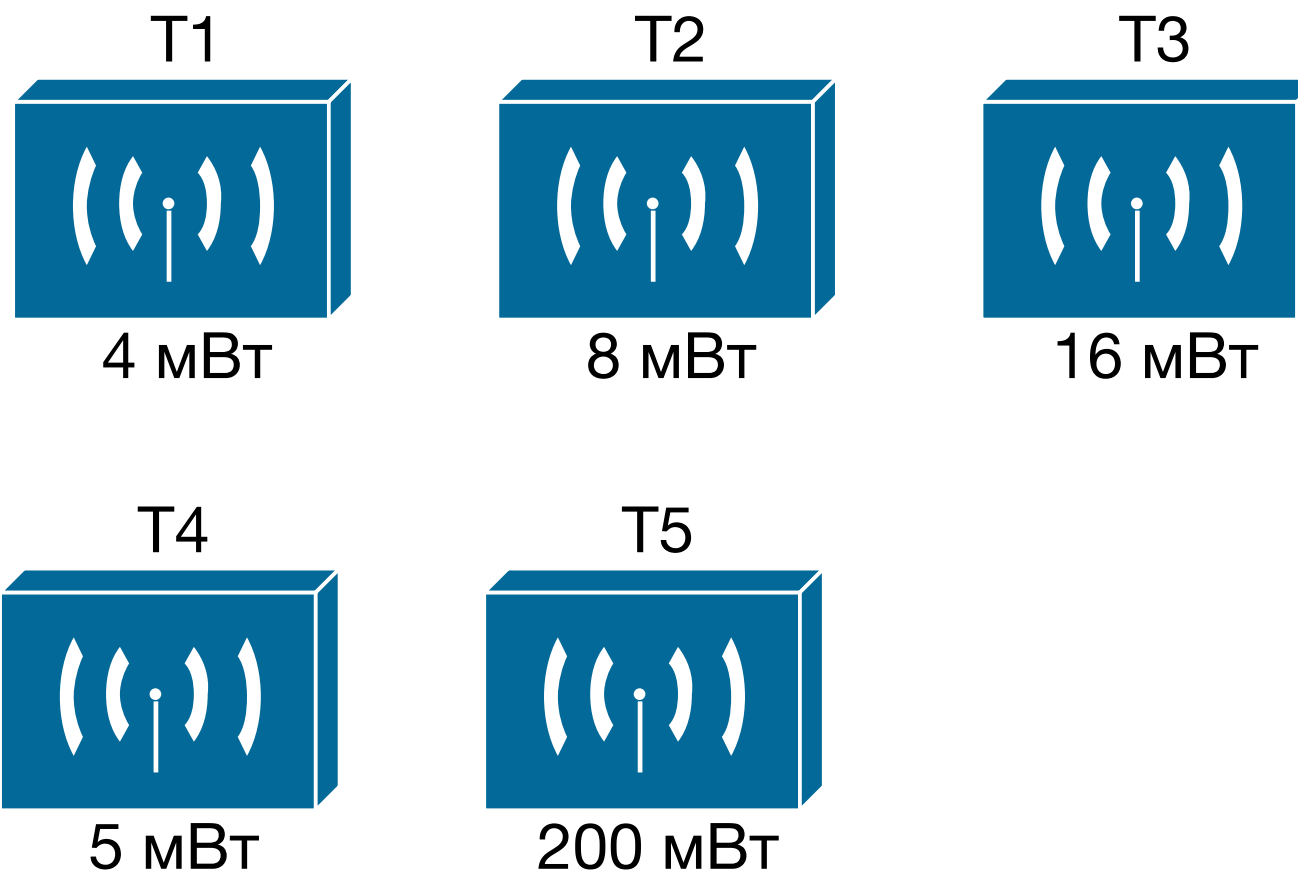
Мощность сигнала

Децибел - удобная функция, использующая логарифм для сравнения двух абсолютных величин:

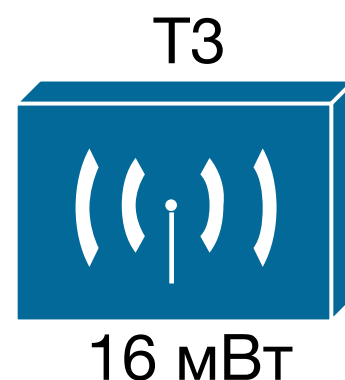
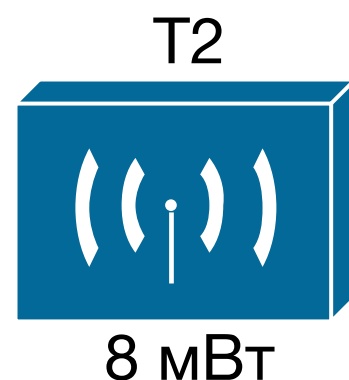
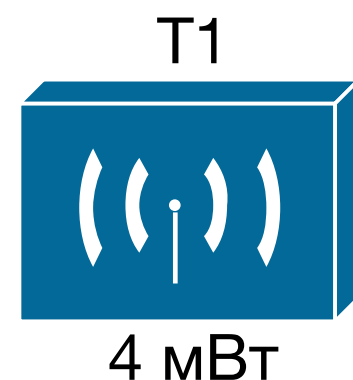
$$\text{dB} = 10(\log_{10}P_2 - \log_{10}P_1) = 10\log_{10}(P_2/P_1)$$

Соотношение мощностей	Значение дБ
1	0 дБ
2	3 дБ
1/2	-3 дБ
10	10 дБ
1/10	-10 дБ

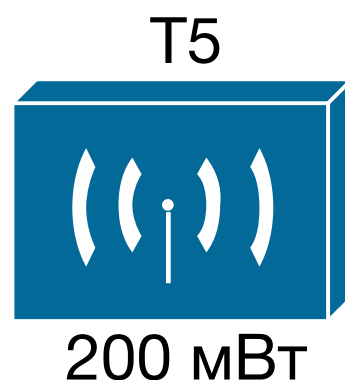
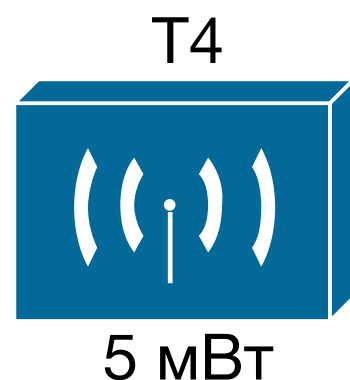
Мощность сигнала



Мощность сигнала

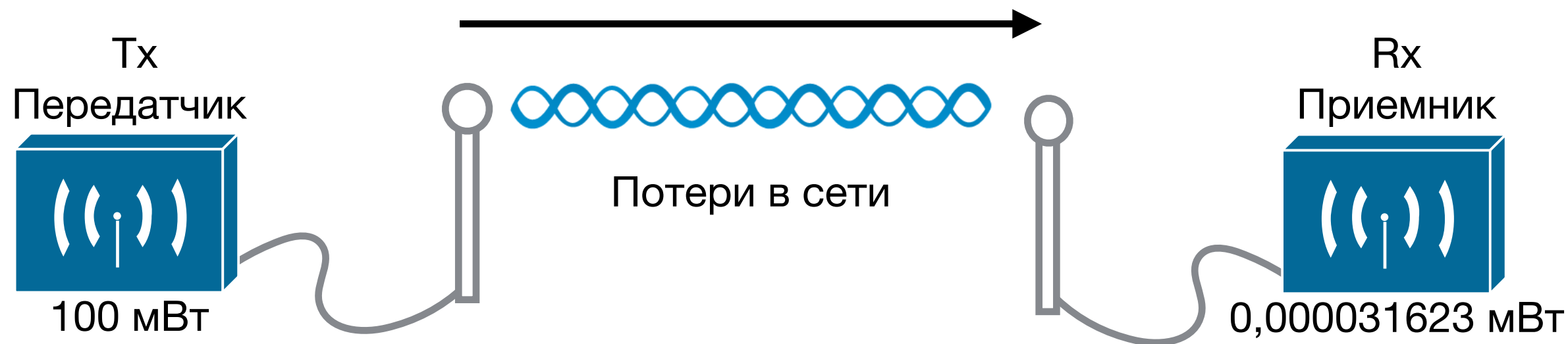


$$\begin{aligned}T2/T1 &= 2 \\ T2 &= T1 + 3\text{дБ} \\ T3/T2 &= 2 \\ T3 &= T2 + 3\text{дБ} \\ T3 &= T1 + 6\text{дБ}\end{aligned}$$

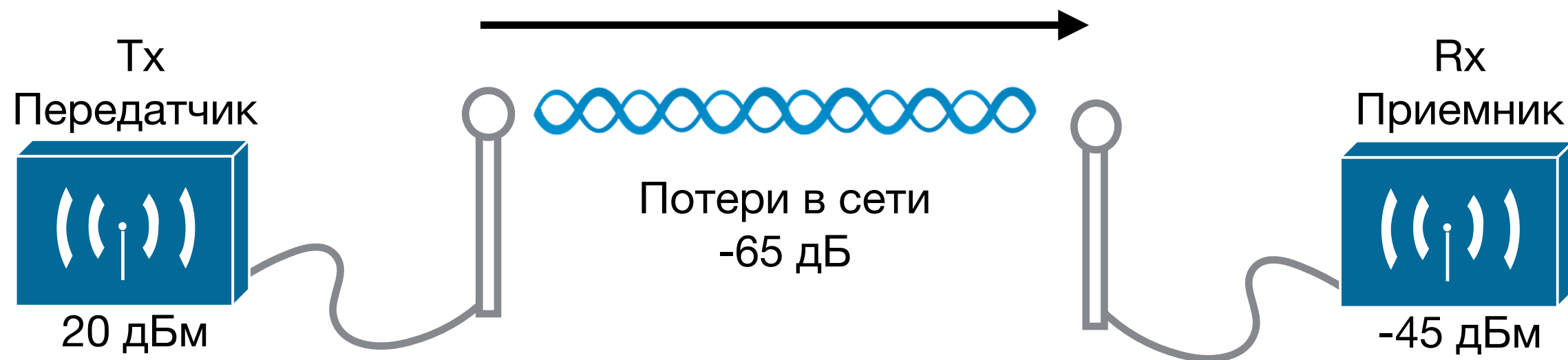


$$\begin{aligned}T5/T4 &= 40 = 2 \times 2 \times 10 \\ T5 &= T4 + 3 + 3 + 10 = T4 + 16\text{дБ}\end{aligned}$$

Мощность сигнала



$$10\log_{10}(0,000031623\text{мВт}/100\text{мВт})=-65\text{дБ}$$



Модуляция сигнала

Радиосигнал в простейшем случае можно модулировать по трем параметрам:

- частота (только в пределах несущей);**
- амплитуда;**
- фаза.**

Отсюда три основных вида модуляции, на базе которых можно построить сложные, такие как DBPSK, DQPSK, CCK, QAM.

Модуляция сигнала

DBPSK - differential binary phase shift keying

Дифференциальная двоичная фазовая модуляция

DQPSK - differential quadrature phase shift keying

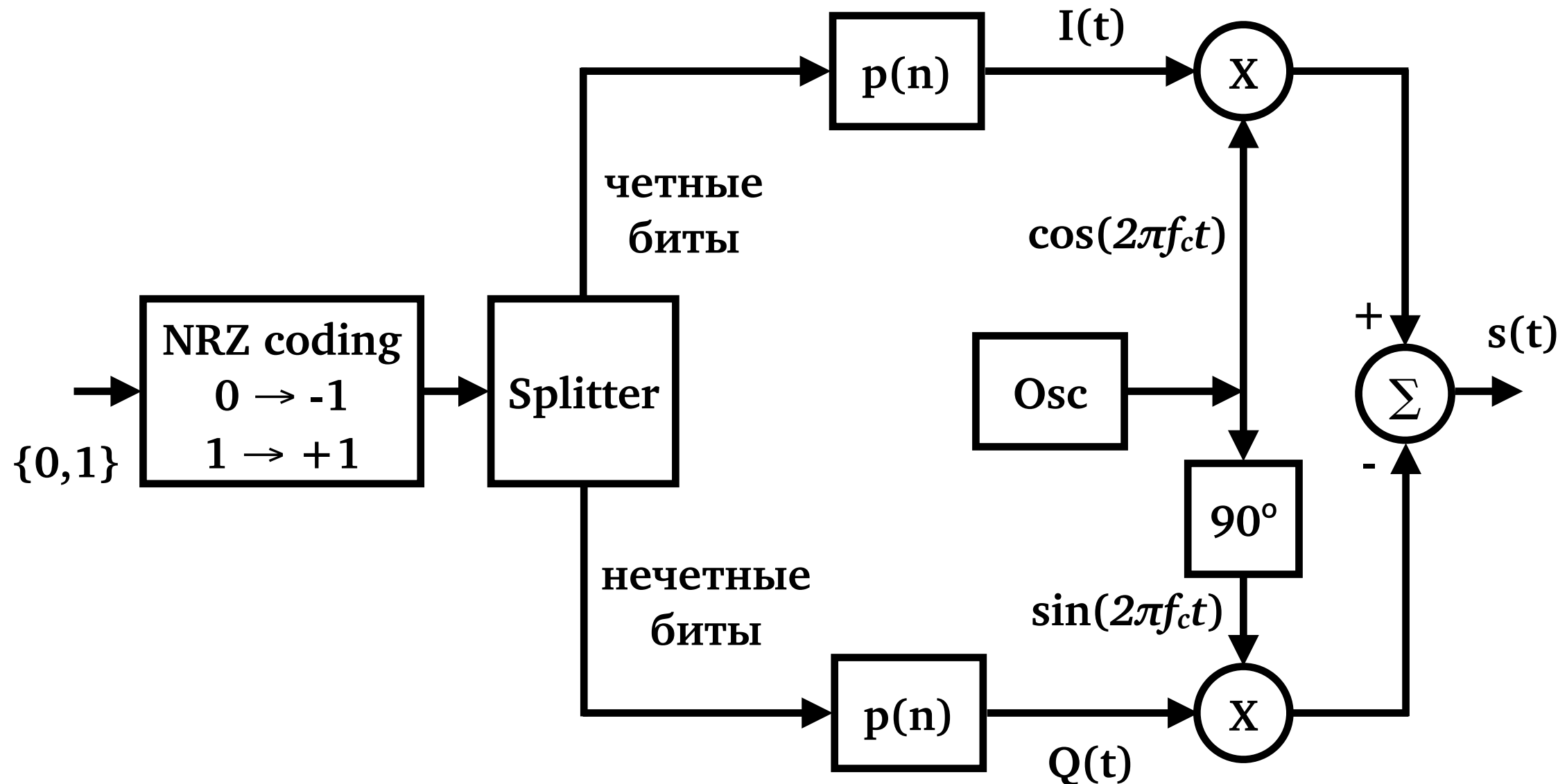
Дифференциальная квадратурная фазовая модуляция

Фаза сигнала несущей смещается или поворачивается в соответствии с передаваемым битом данных.

DBPSK		DQPSK	
«0»	0°	«00»	0°
«1»	180°	«01»	90°
		«10»	180°
		«11»	270°

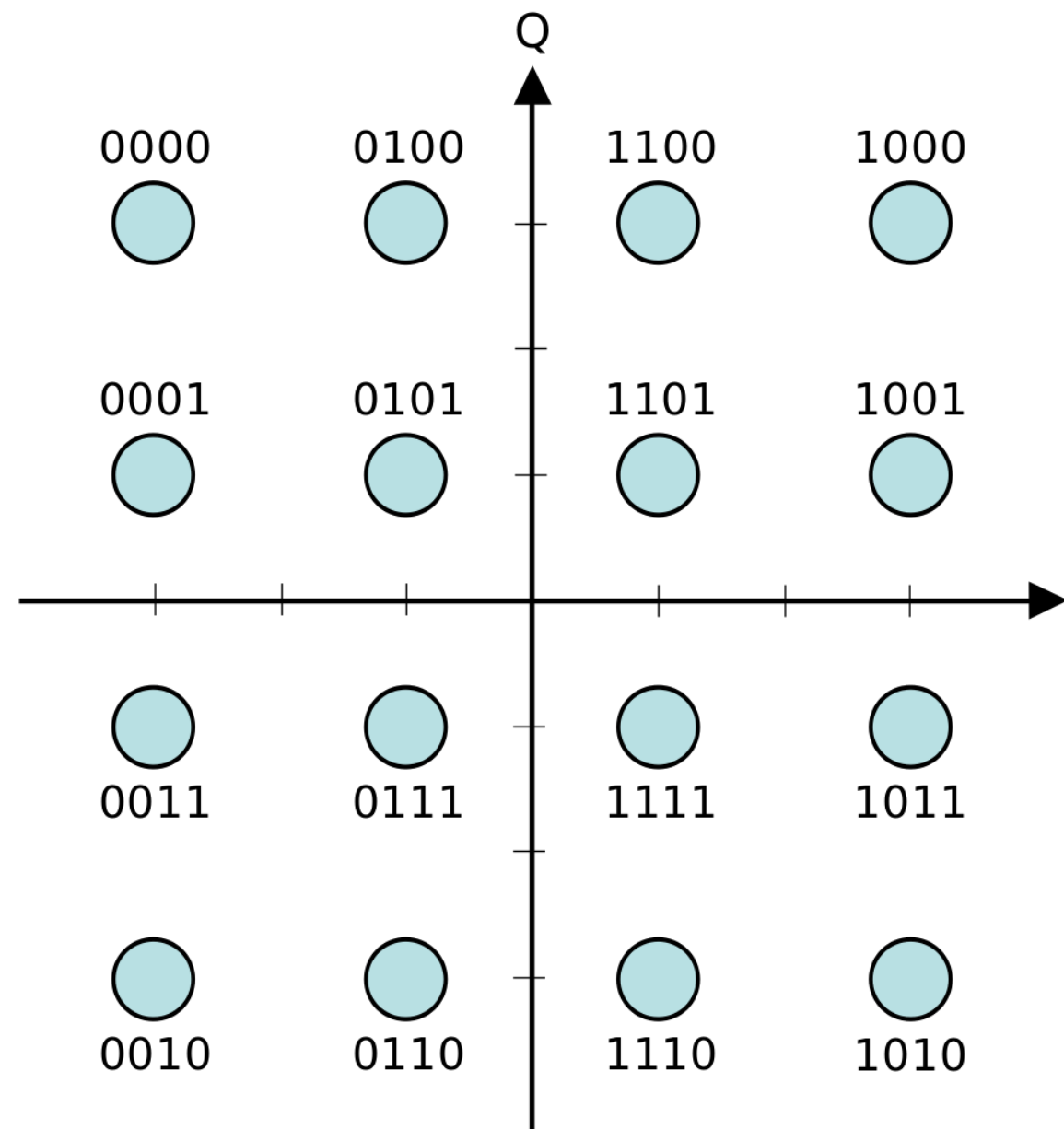
Модуляция сигнала

Схема модулятора QPSK



Модуляция сигнала

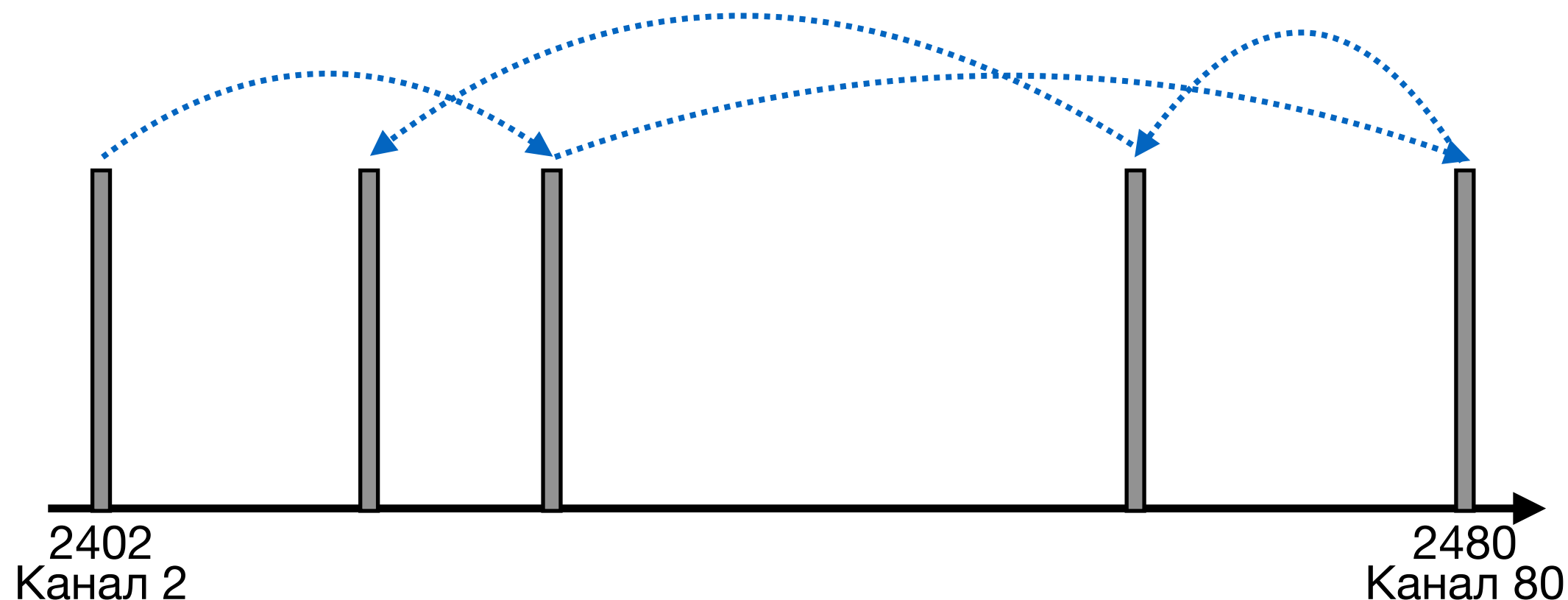
QAM объединяет методы фазового сдвига с возможностью изменять амплитуду для получения большего количества уникальных комбинаций сигнала



Методы расширения спектра

FHSS - Frequency-hopping spread spectrum
Скачкообразная перестройка частоты

Ширина канала - 1 МГц => узкая полоса пропускания
Несколько передатчиков могут мешать друг другу

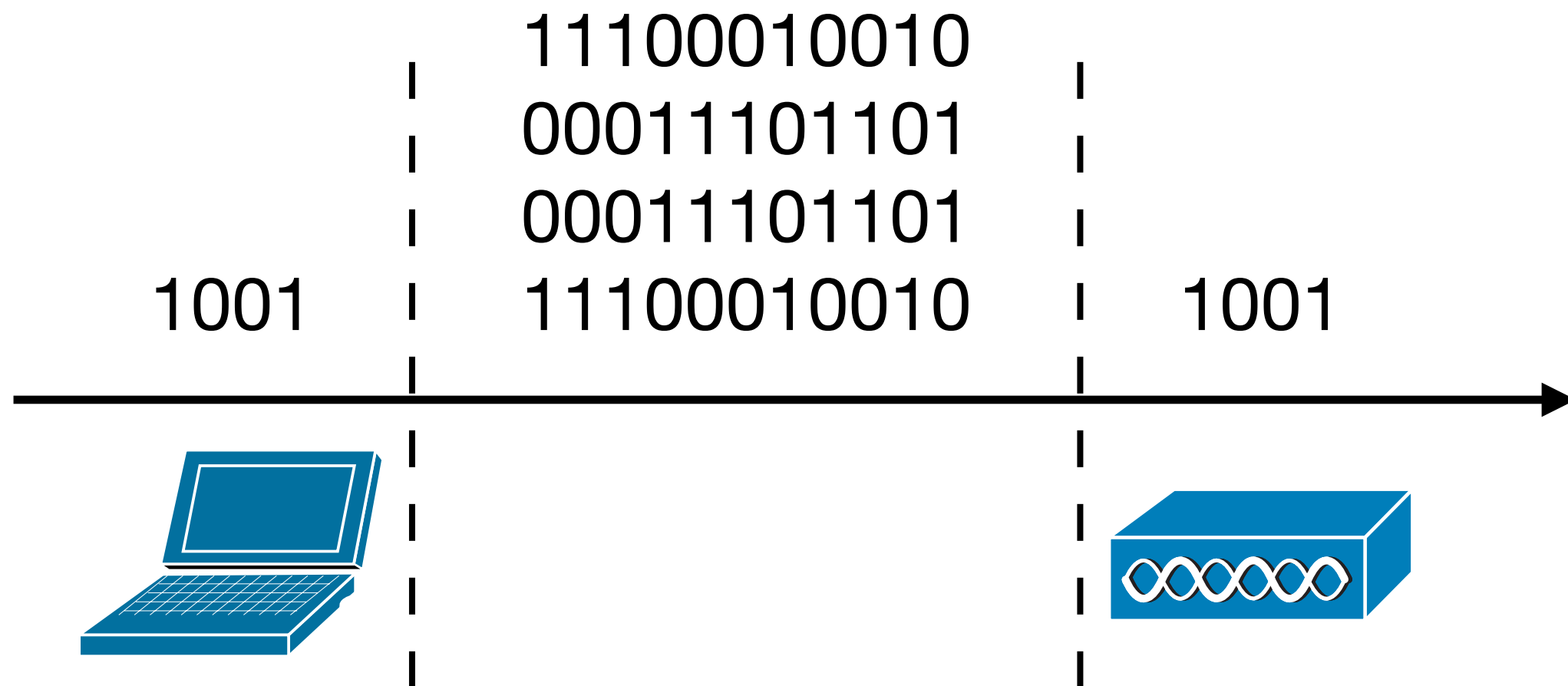


Методы расширения спектра

DSSS - Direct-sequence spread spectrum

Метод прямого расширения спектра

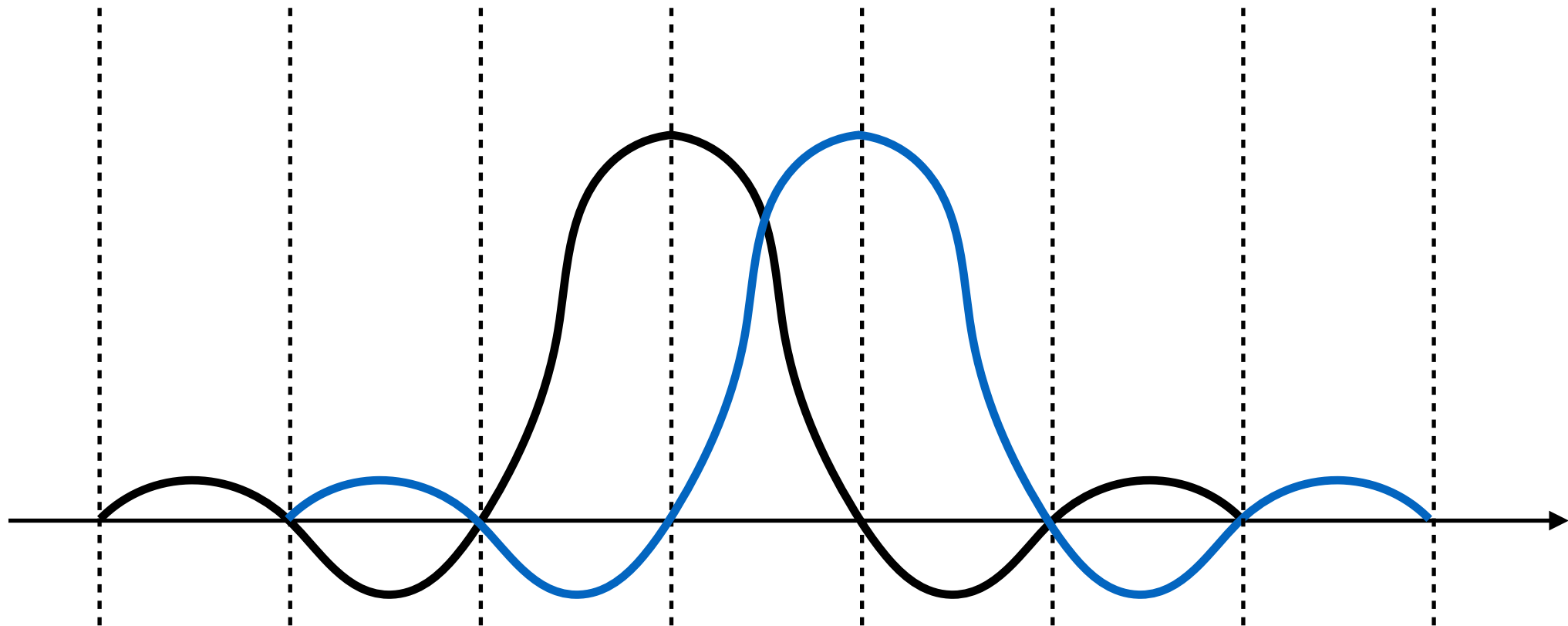
Каждый бит кодируется последовательностью из нескольких сигналов (код Баркера).



Методы расширения спектра

OFDM - Orthogonal frequency-division multiplexing

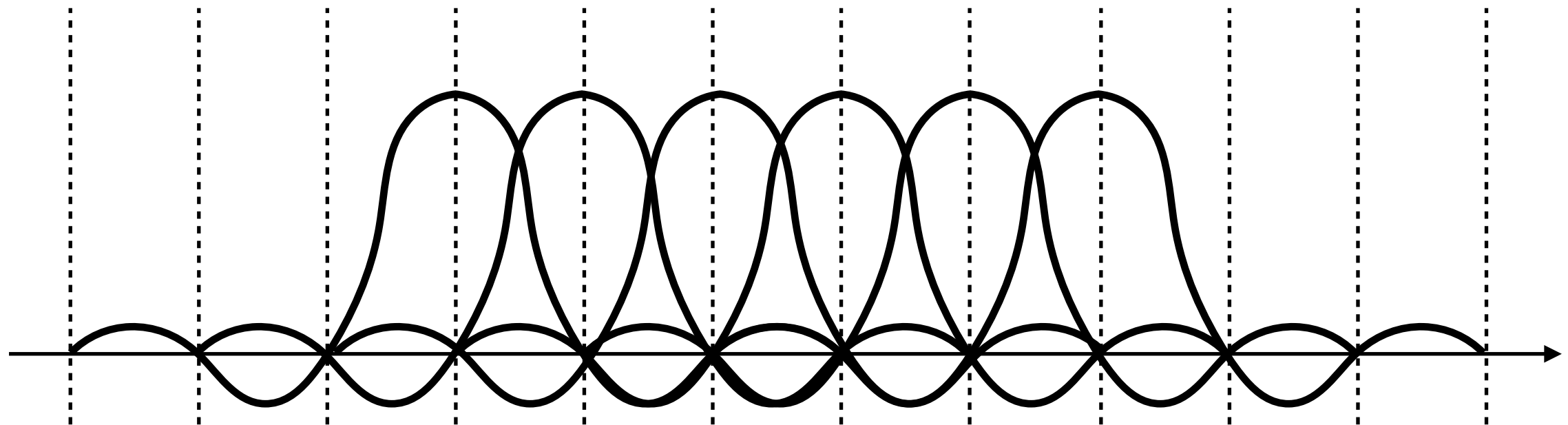
Мультиплексирование с ортогональным разделением частоты



Методы расширения спектра

OFDM - Orthogonal frequency-division multiplexing

Мультиплексирование с ортогональным разделением частоты

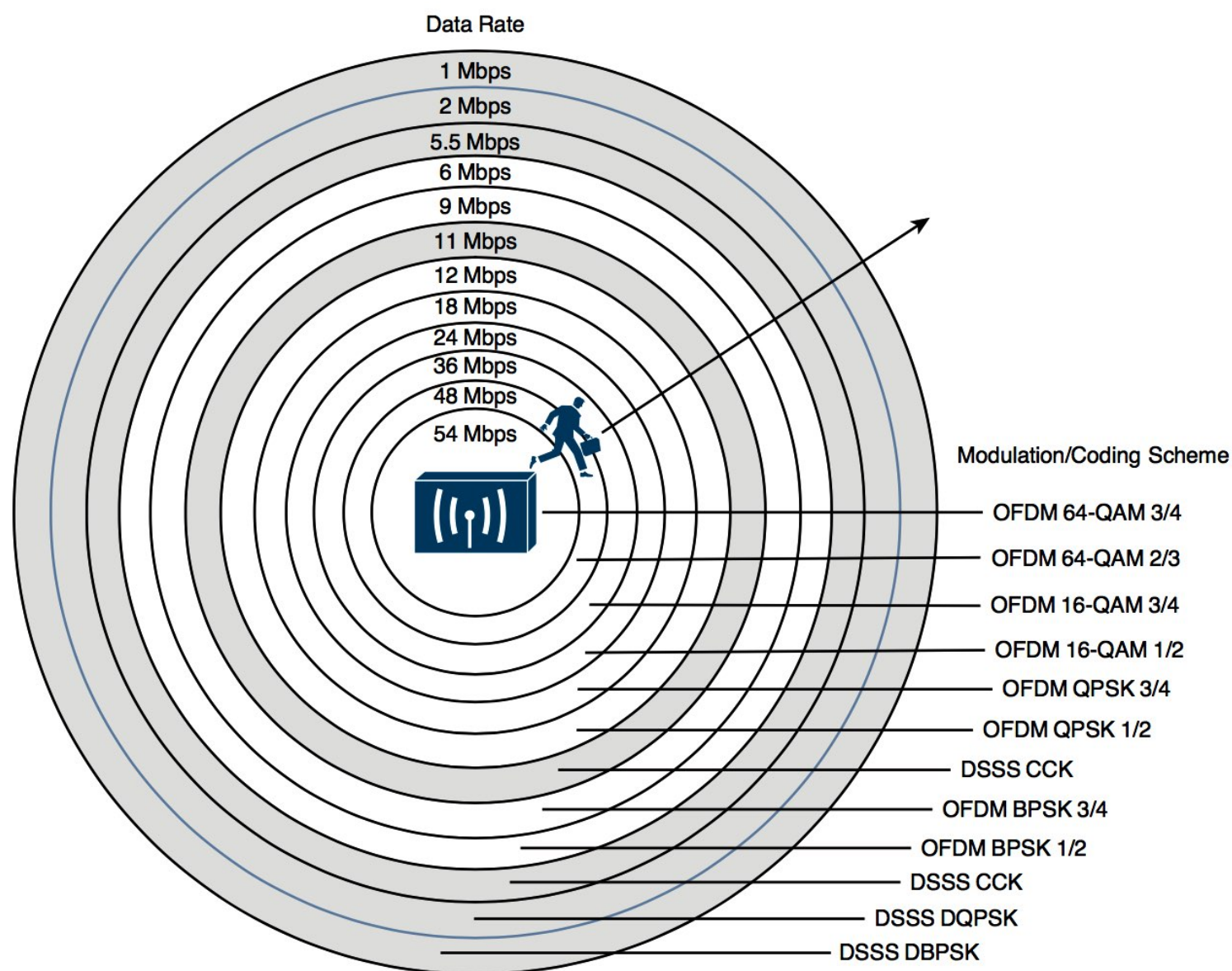


Методы модуляции

DRS - dynamic rate shifting

Динамическое изменение способа передачи

Производится на основе анализа уровней RSSI и SNR



Методы модуляции

Максимальная пропускная способность зависит от:

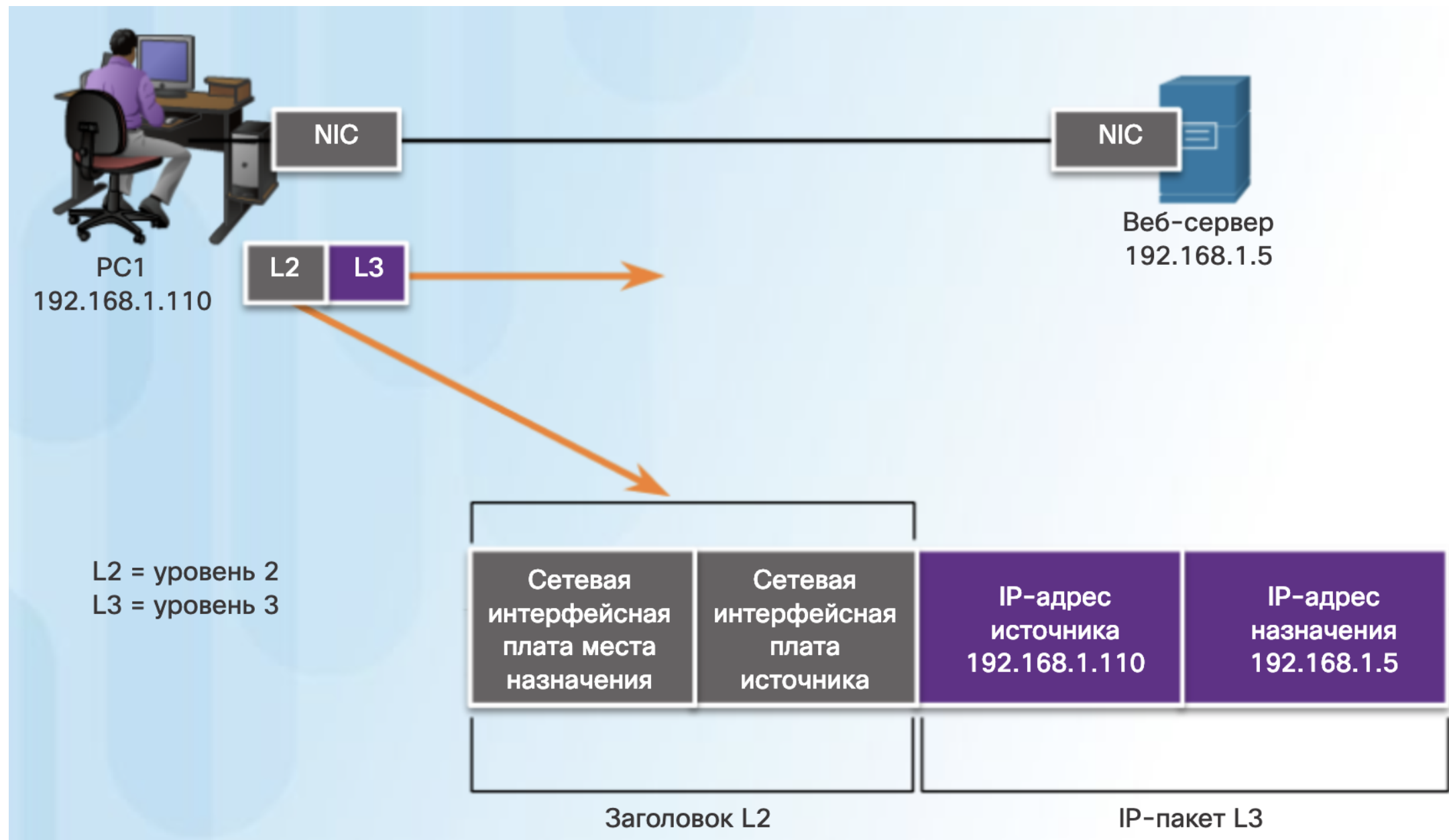
- ширины канала;**
- количества потоков;**
- индекса MCS (Modulation and Coding Scheme), включающего тип модуляции и способ кодирования.**

Индекс MCS

802.11n											802.11ac
HT MCS Index	Spatial Streams	Modulation & Coding	Data Rate GI = 800ns	Data Rate SGI = 400ns	Data Rate GI = 800ns	Data Rate SGI = 400ns	Data Rate GI = 800ns	Data Rate SGI = 400ns	Data Rate GI = 800ns	Data Rate SGI = 400ns	VHT MCS Index
			20MHz	20MHz	40MHz	40MHz	80MHz	80MHz	160MHz	160MHz	
0	1	BPSK 1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	0
1	1	QPSK 1/2	13	14.4	27	30	58.5	65	117	130	1
2	1	QPSK 3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	2
3	1	16-QAM 1/2	26	28.9	54	60	117	130	234	260	3
4	1	16-QAM 3/4	39	43.3	81	90	175.5	195	351	390	4
5	1	64-QAM 2/3	52	57.8	108	120	234	260	468	520	5
6	1	64-QAM 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	6
7	1	64-QAM 5/6	65	72.2	135	150	292.5	325	585	650	7
	1	256-QAM 3/4	78	86.7	162	180	351	390	702	780	8
	1	256-QAM 5/6	n/a	n/a	180	200	390	433.3	780	866.7	9

ОСНОВЫ ЛОКАЛЬНЫХ сетей

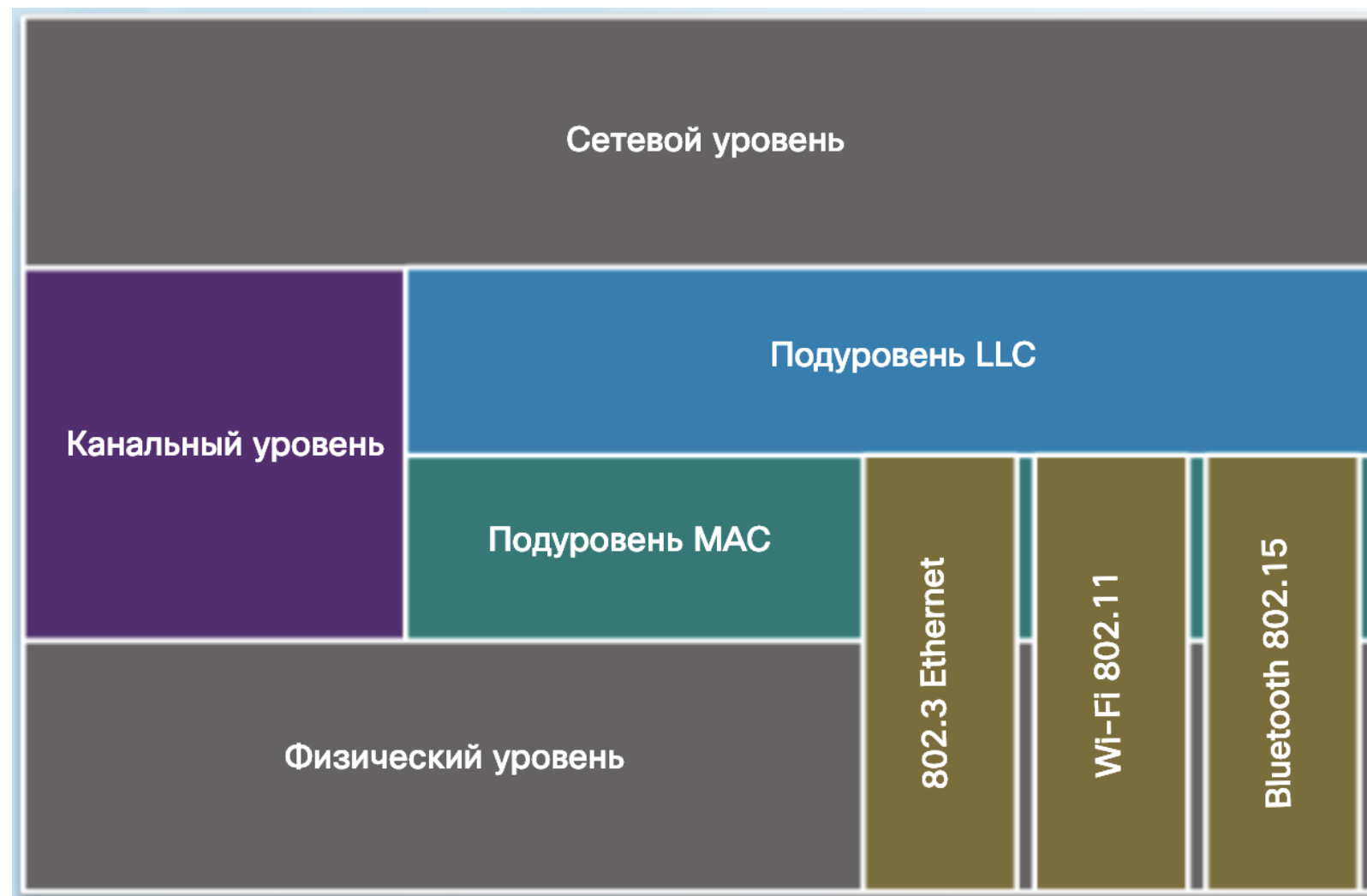
Основы локальных сетей



Функции канального уровня

- Обеспечение доступа вышестоящих уровней к средству подключения**
- Прием пакетов уровня 3 и упаковка их в кадры**
- Подготовка сетевых данных для передачи по физической сети**
- Управление передачей и приемом данных в средстве подключения**
- Обмен кадрами между узлами по физическим средствам сетевого подключения, например по кабелям UTP или оптоволоконным кабелям**
- Прием пакетов и их перенаправление протоколам вышестоящего уровня**
- Обнаружение ошибок**

Подуровни MAC и LLC



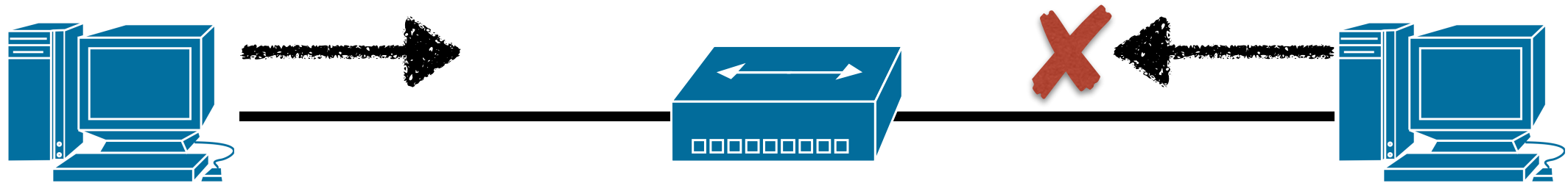
Управление доступом к среде (Media Access Control, MAC). Это нижний подуровень, который определяет процессы доступа к среде, выполняемые оборудованием. Он обеспечивает адресацию канального уровня.

Управление логическим соединением (Logical Link Control, LLC). Этот верхний подуровень взаимодействует с сетевым уровнем. Он помещает в кадр информацию, указывающую, какой протокол сетевого уровня используется для данного кадра. Данная информация позволяет различным протоколам 3-го уровня, таким как IPv4 и IPv6, использовать один и тот же сетевой интерфейс и одно и то же средство подключения.

ОСНОВЫ ЛОКАЛЬНЫХ СЕТЕЙ

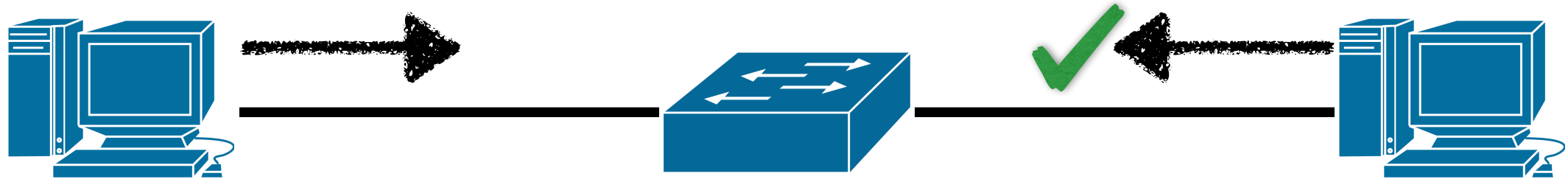
Термин	Описание
Дуплекс	Способ связи, позволяющий одновременно передавать и принимать информацию
Полудуплекс	Логика передачи, при которой устройство отправляет данные только тогда, когда не получает их
Симплекс	Схема связи, позволяющая передавать сигналы только в одном направлении

Полудуплексное соединение



Полудуплексная связь: оба устройства могут передавать и получать информацию через среду, но не одновременно. Полудуплексный режим используется в устаревших шинных топологиях и при использовании концентраторов Ethernet. Сети WLAN также работают в полудуплексном режиме. Полудуплексный режим позволяет осуществлять передачу или прием по общей среде одновременно только одному устройству и используется в случае применения методов конкурентного доступа.

Полудуплексное соединение

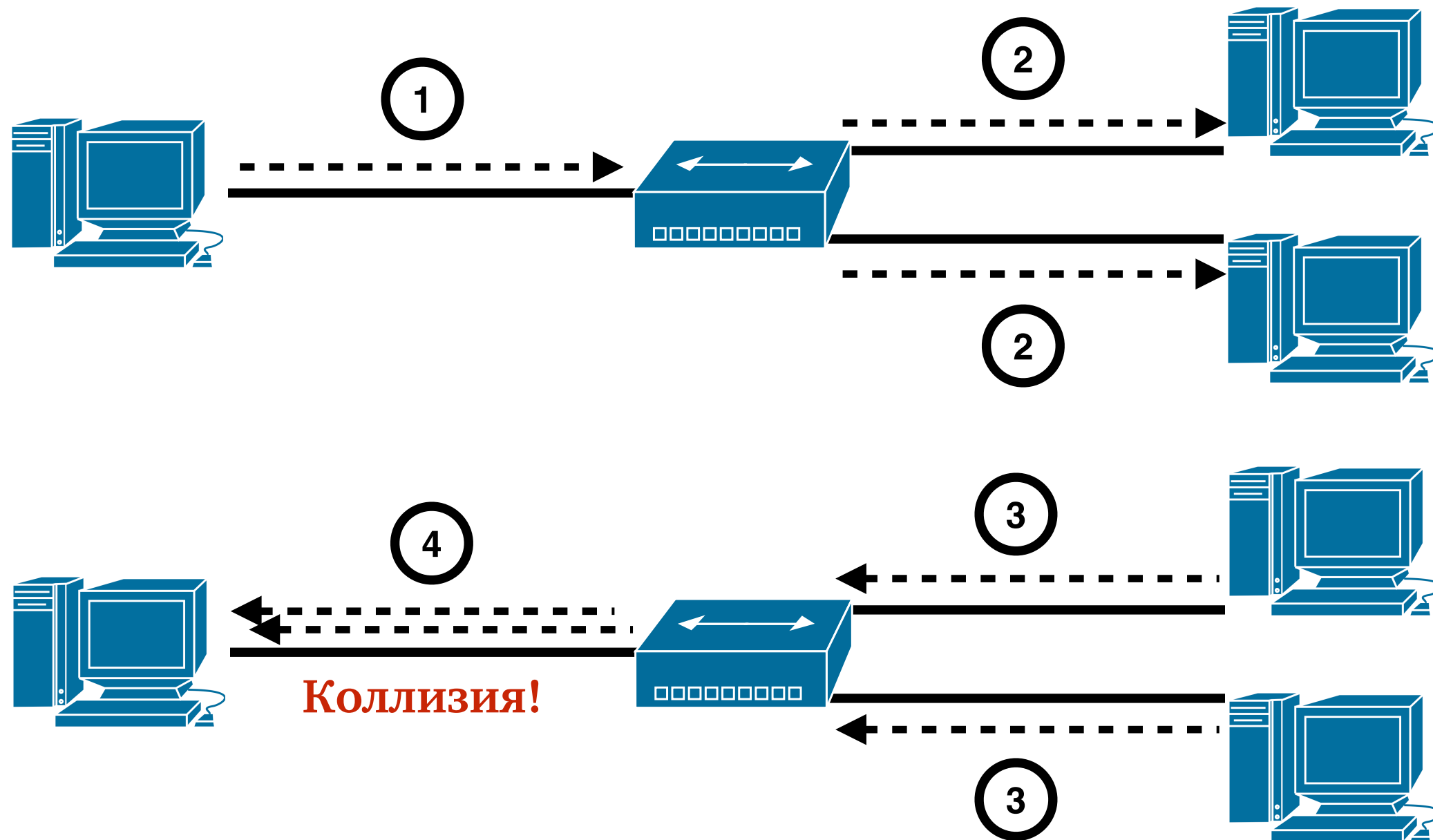


Полнодуплексная связь: оба устройства одновременно могут передавать и принимать данные по средствам подключения. Канальный уровень предполагает одновременную доступность среды обоим узлам для передачи. Коммутаторы Ethernet по умолчанию работают в полнодуплексном режиме

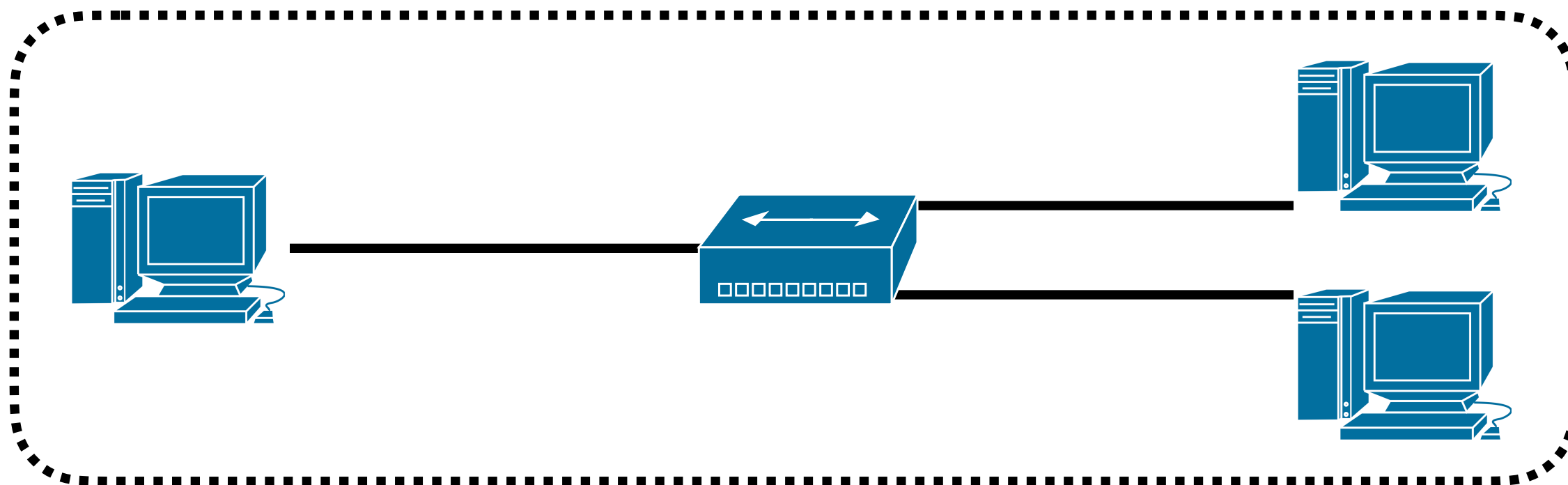
Основы локальных сетей



Основы локальных сетей



Домен коллизий



Домен коллизий - часть сети, все узлы которой конкурируют за общую разделяемую среду передачи данных и каждый узел которой может создать коллизию с другим узлом

CSMA/CD

CSMA/CD - carrier sense multiple access with collision detection

- **CSMA/CD - множественный доступ с контролем несущей и обнаружением конфликтов;**
- **контроль несущей - возможность определить, занят ли канал;**
- **множественный доступ - кто угодно может передавать сообщения;**
- **обнаружение конфликтов - передающая система «знает», если она «перебивает» кого-либо.**

CSMA/CA

CSMA/CD - carrier sense multiple access with collision avoidance

- **CSMA/CD - множественный доступ с контролем несущей и избежанием конфликтов;**
- **контроль несущей - возможность определить, занят ли канал;**
- **множественный доступ - кто угодно может передавать сообщения;**
- **избежание конфликтов - передающая система «знает», как долго среда передачи будет занята.**

Фрейм (кадр) Ethernet

7

1

6

6

2

46-1500

4



Преамбула
(Preamble)

Получатель
(Destination)

Длина/Тип
(Length/Type)

КСФ
(FCS)

РНФ
(SFD)

Отправитель
(Source)

Данные
(Data)

РНФ - Разделитель Начала Фрейма

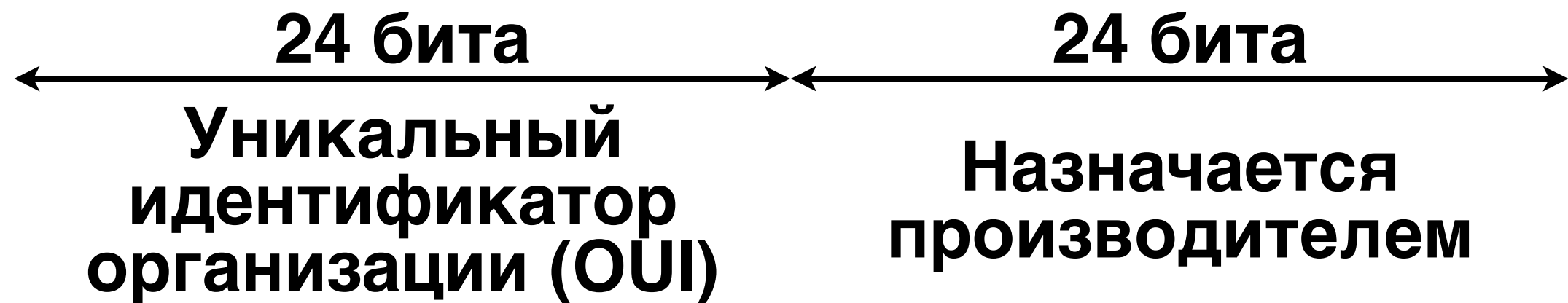
SFD - Start Frame Delimiter

КСФ - Контрольная Сумма Фрейма

FCS - Frame Check Sequence

Адресация в технологии Ethernet

00 60 2F 3A 07 BC



MAC - Media Access Control

OUI - Organizationally Unique Identifier

Варианты записи MAC-адреса

00-60-2F-3A-07-BC

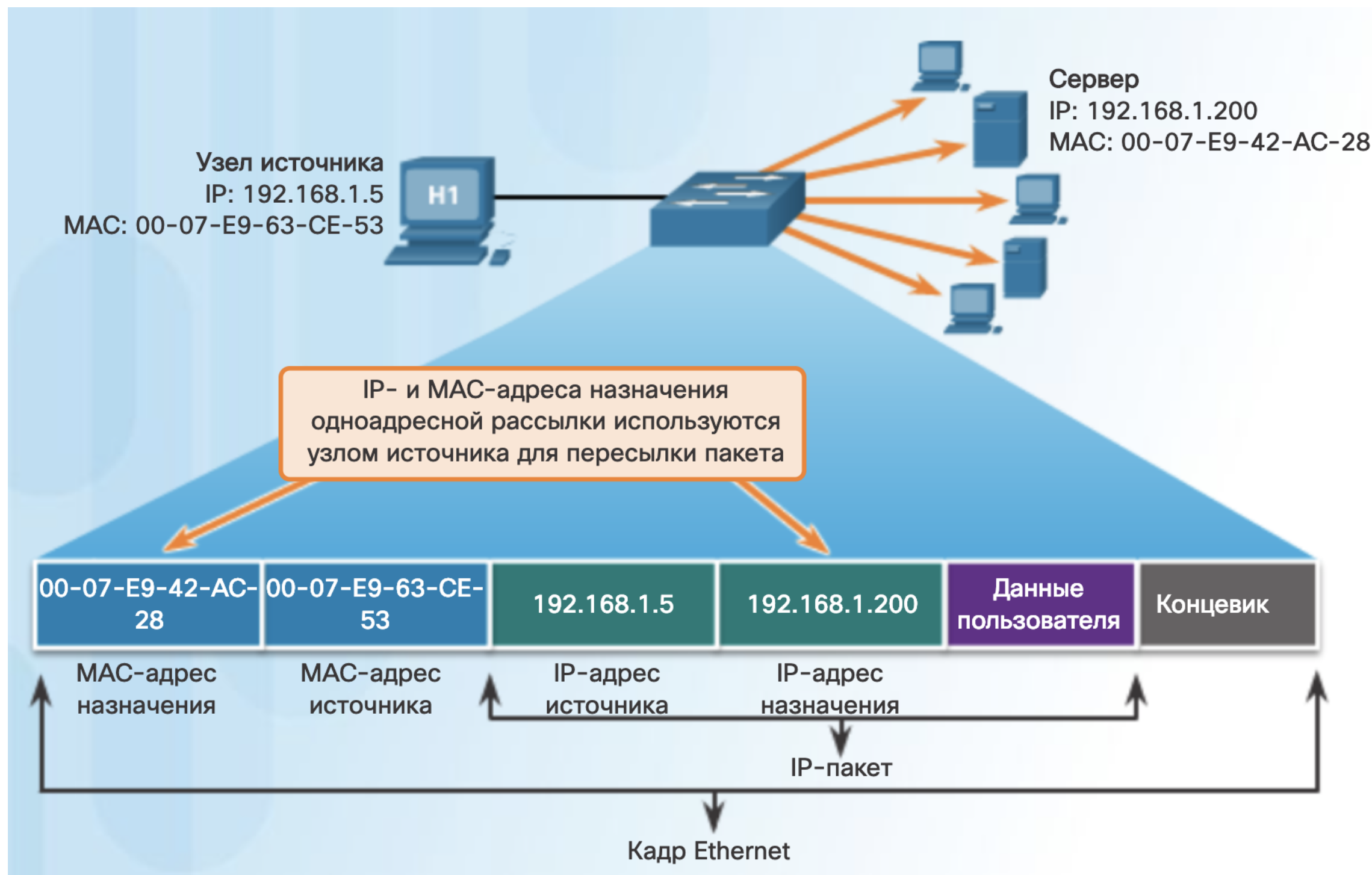
00:60:2F:3A:07:BC

0060.2F3A.07BC

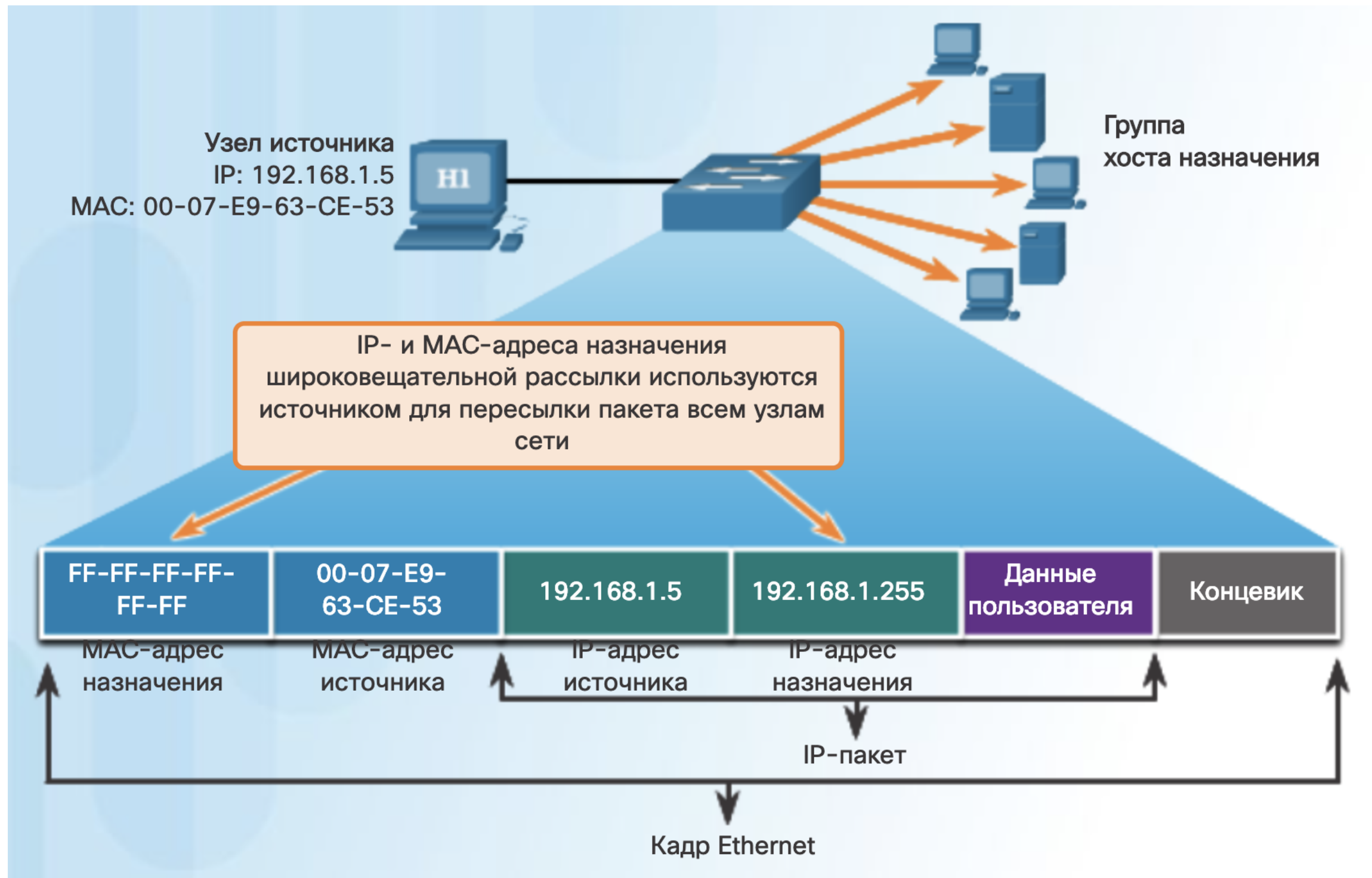
Адресация в технологии *Ethernet*

Термин	Описание
<i>Unicast</i>	Адрес, описывающий единственное устройство в сети
<i>Multicast</i>	Адрес, идентифицирующий заранее заданную группу устройств
<i>Broadcast</i>	Адрес, обозначающий «все устройства в данный момент»

Одноадресатная рассылка



Широковещательная рассылка

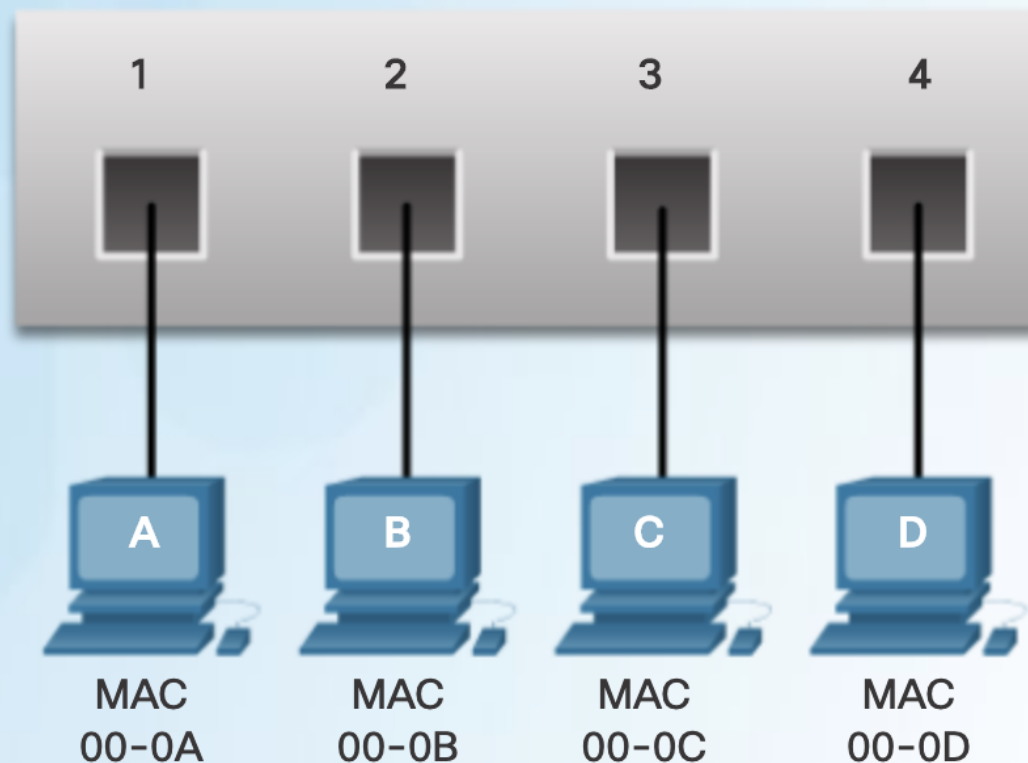


ОСНОВЫ ЛОКАЛЬНЫХ сетей

Коммутатор Ethernet

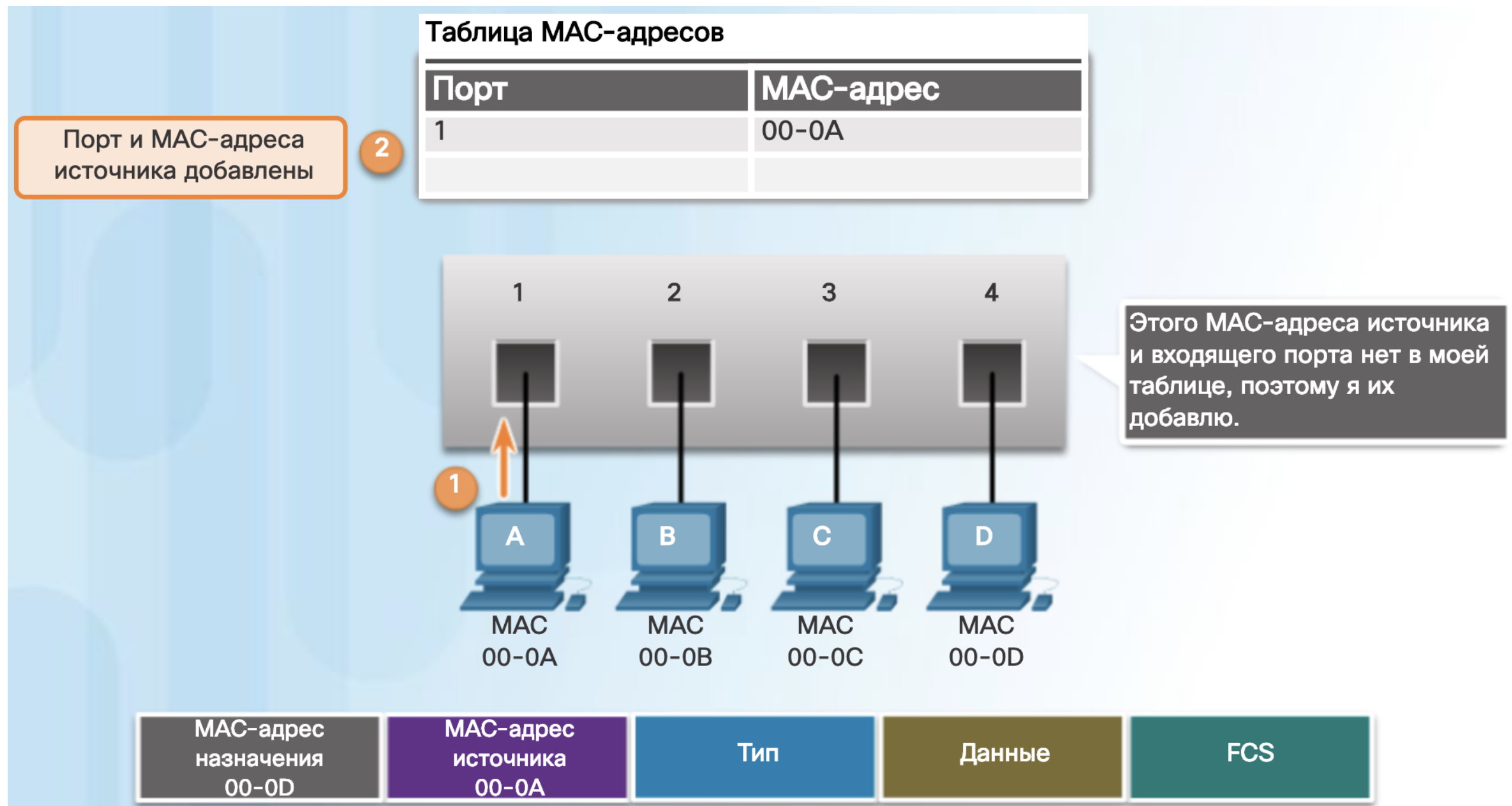
Таблица MAC-адресов

Port	MAC Address

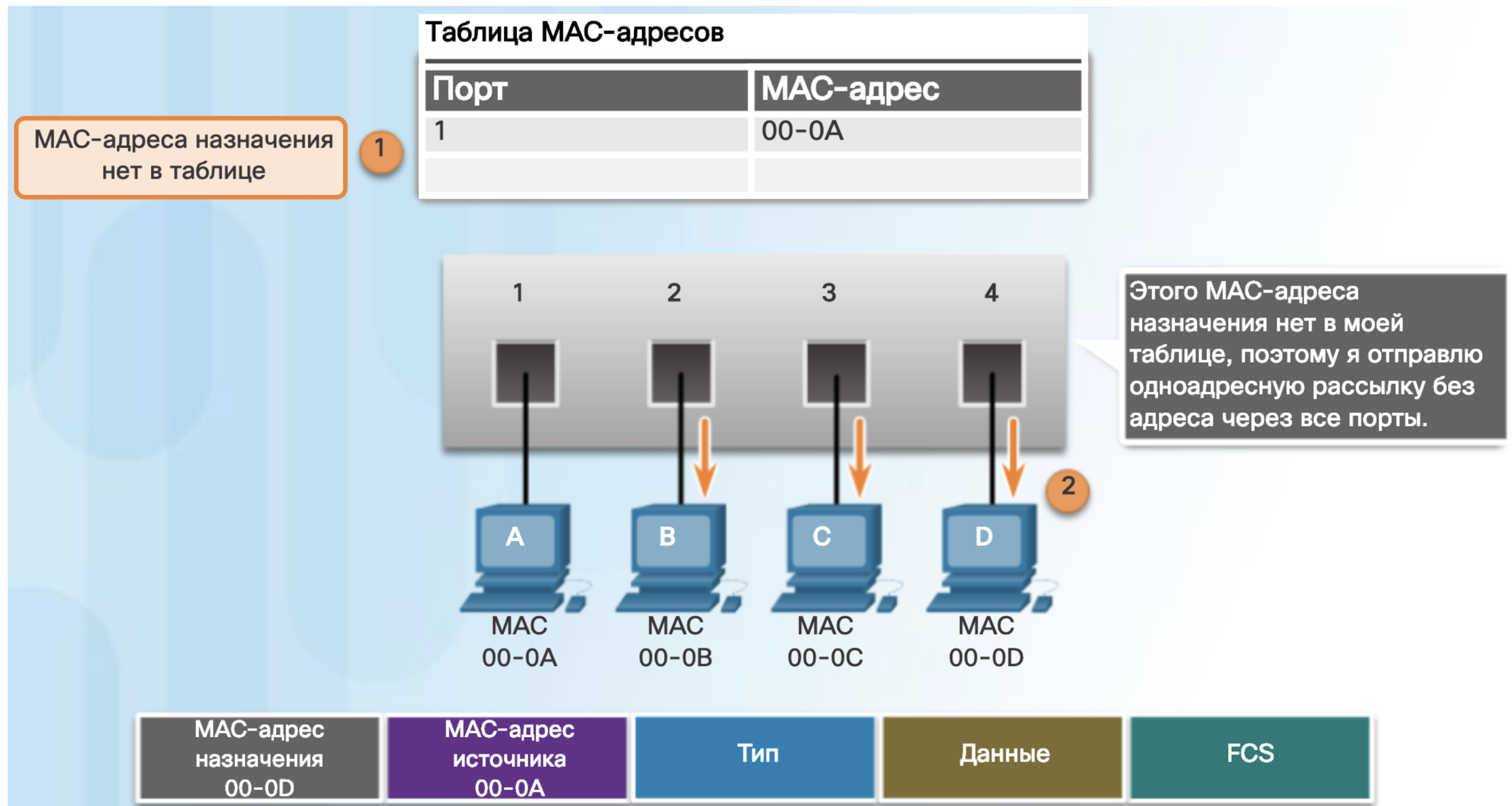


Коммутатор Ethernet уровня 2 использует MAC-адреса для принятия решения о пересылке. Устройство не имеет информации о протоколе, передаваемом в части кадра, выделенной для данных, например, в IPv4-пакете. Коммутатор пересылает пакеты только на основе MAC-адресов Ethernet уровня 2.

Процесс заполнения таблицы MAC-адресов



Процесс заполнения таблицы MAC-адресов

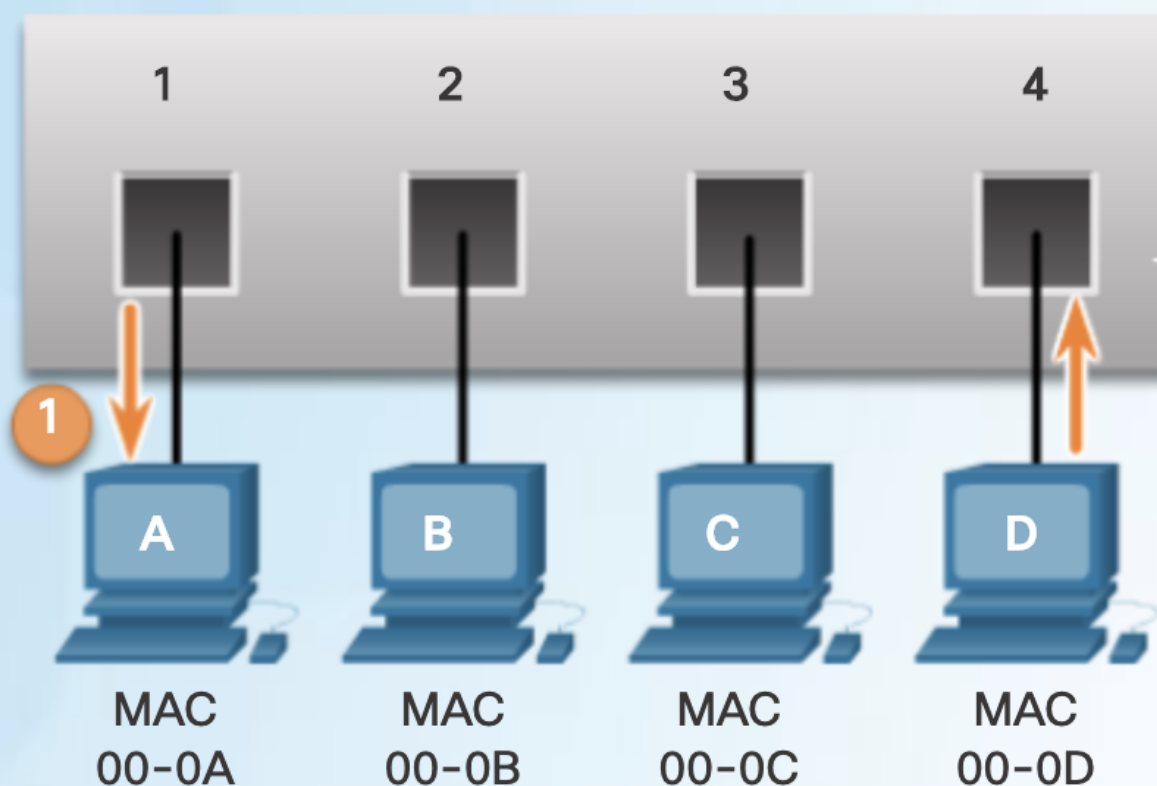


Процесс заполнения таблицы MAC-адресов

Таблица MAC-адресов

Порт	MAC-адрес
1	00-0A
4	00-0D

2



Я знаю MAC-адрес назначения, поэтому перешлю кадр только через порт 1.

MAC-адрес
назначения
00-0A

MAC-адрес
источника
00-0D

Тип

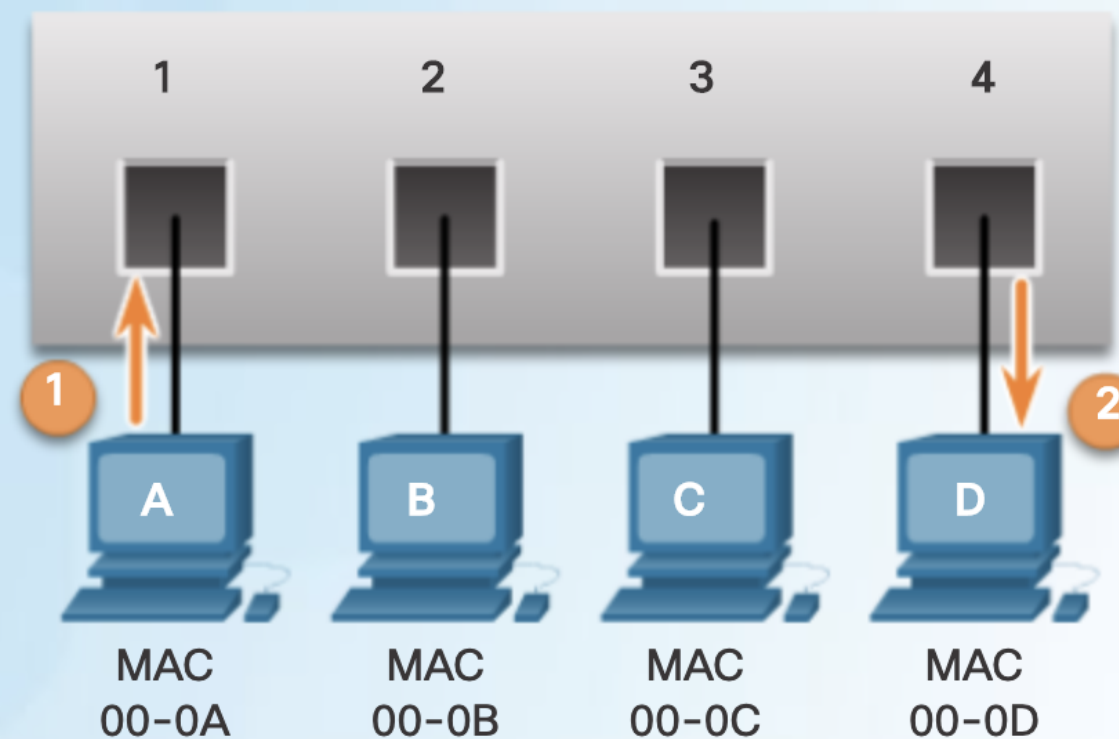
Данные

FCS

Процесс заполнения таблицы MAC-адресов

Таблица MAC-адресов

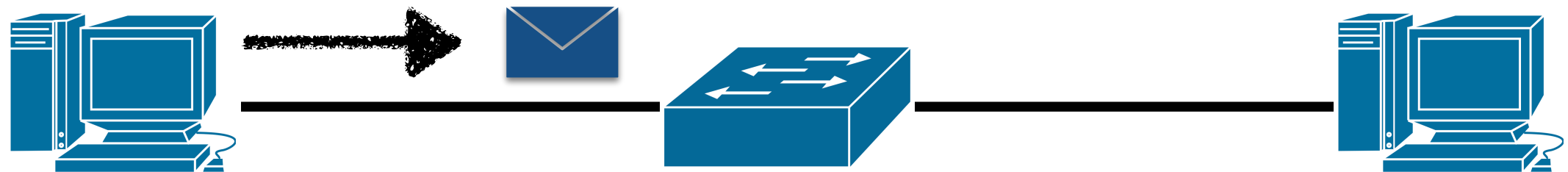
Порт	MAC-адрес
1	00-0A
4	00-0D



MAC-адрес назначения 00-0A	MAC-адрес источника 00-0D	Тип	Данные	FCS
-------------------------------	------------------------------	-----	--------	-----

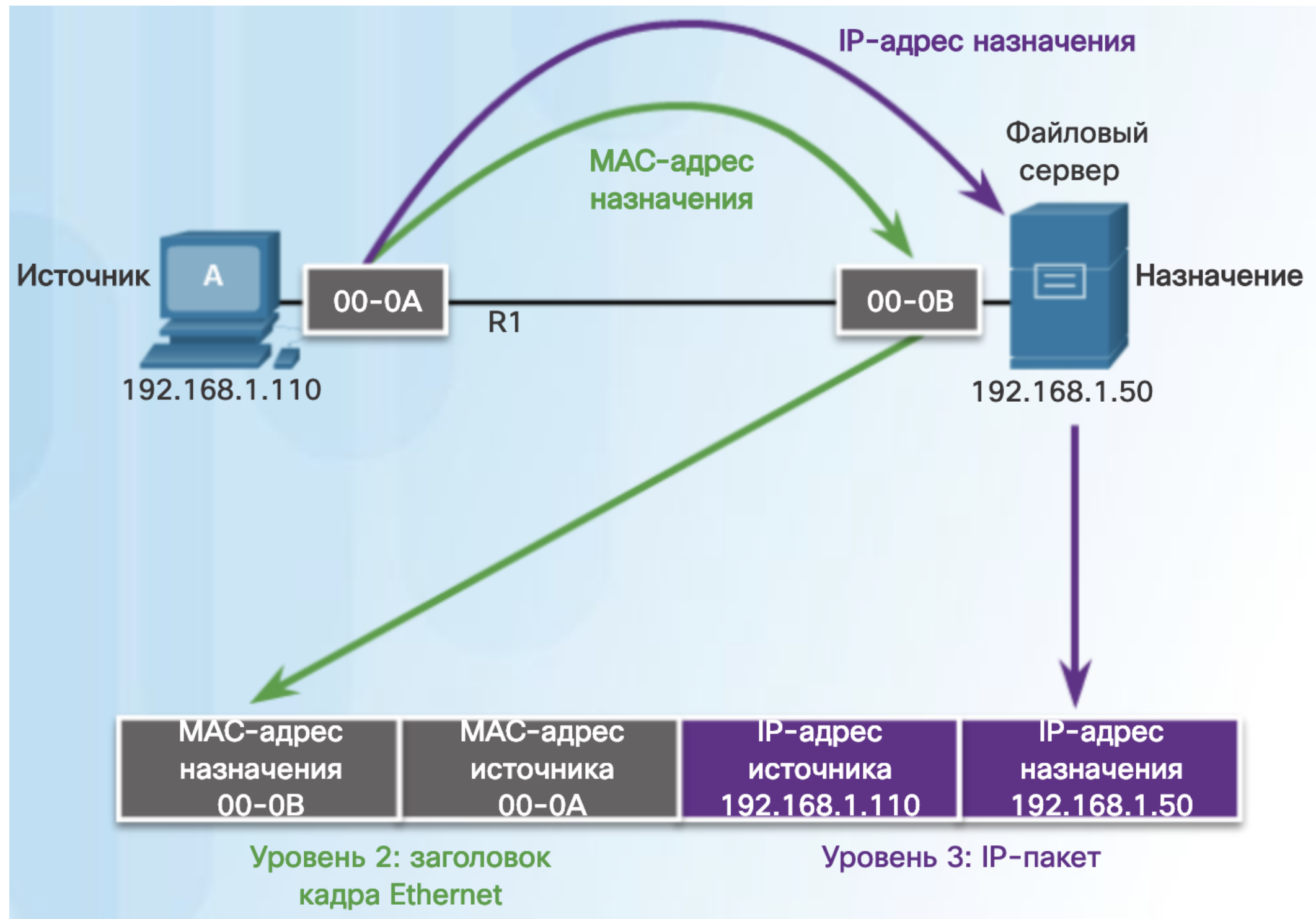
Способы пересылки пакетов

Коммутатор с промежуточным хранением получает кадр целиком и вычисляет циклический избыточный код (CRC). Если значение CRC допустимо, коммутатор ищет адрес назначения, который определяет выходной интерфейс. Затем кадр перенаправляется к правильному порту.

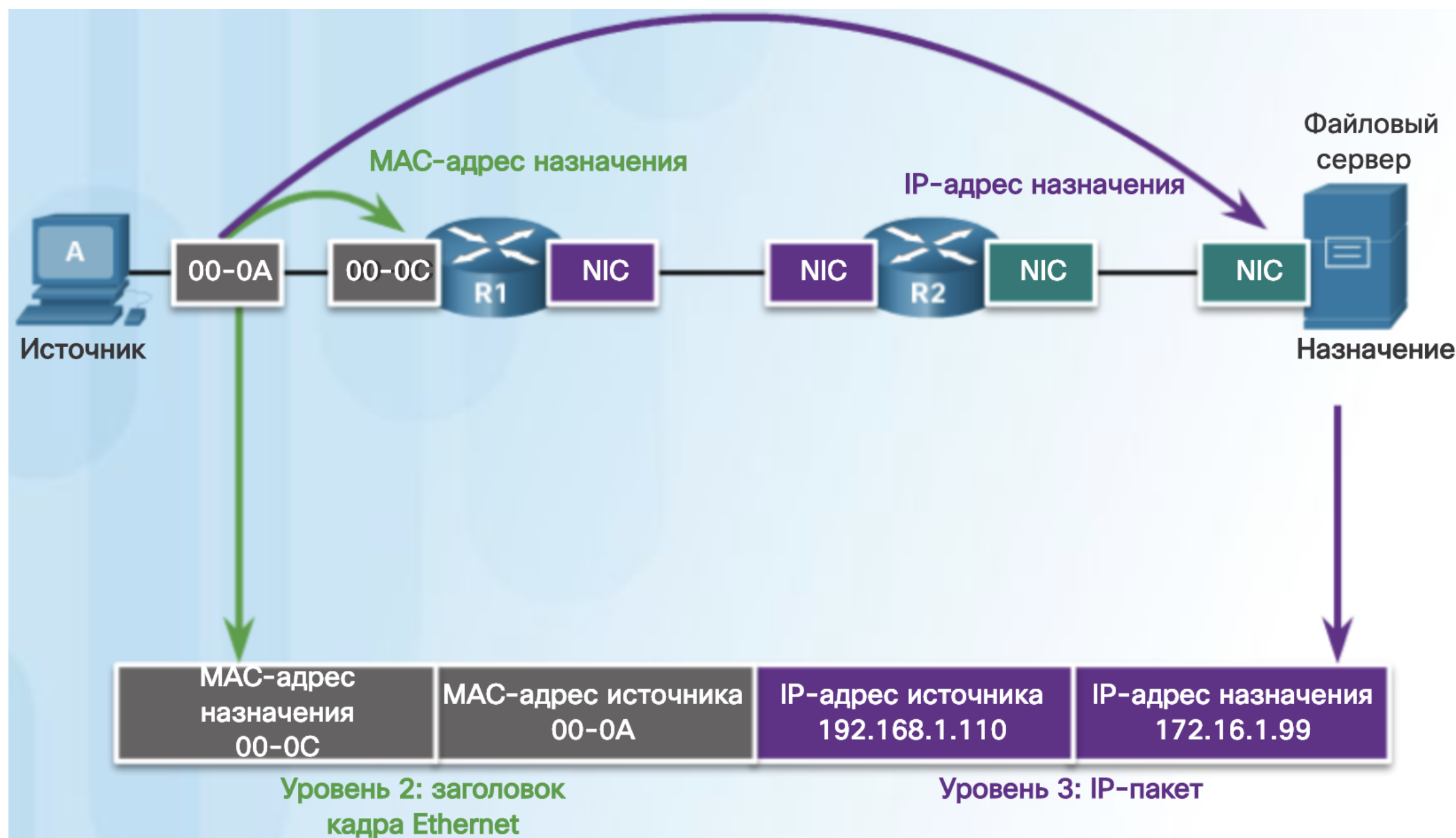


Коммутатор со сквозной коммутацией пересылает данный кадр до его полного получения. Поэтому, как минимум, адрес назначения кадра должен быть прочтен раньше, чем кадр можно будет перенаправить.

Обмен данными в локальной сети



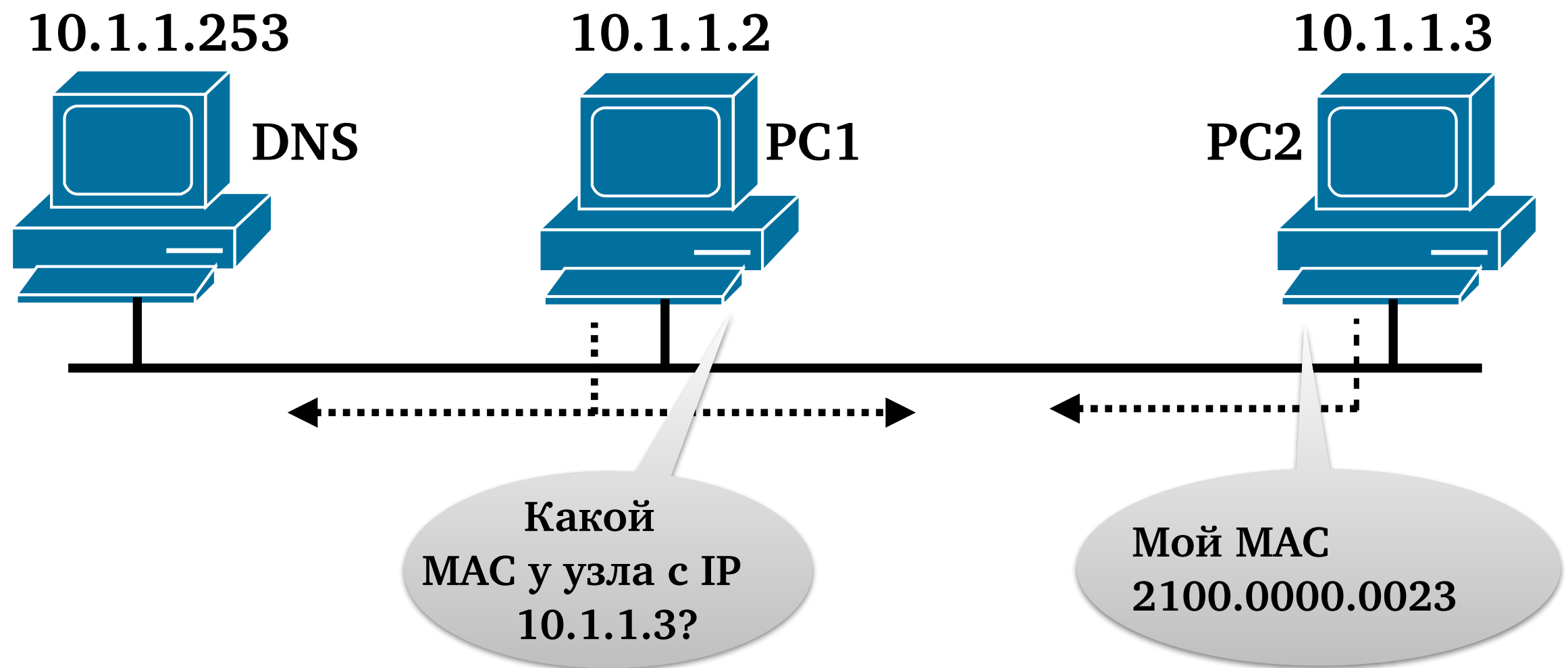
Обмен данными с удаленным устройством



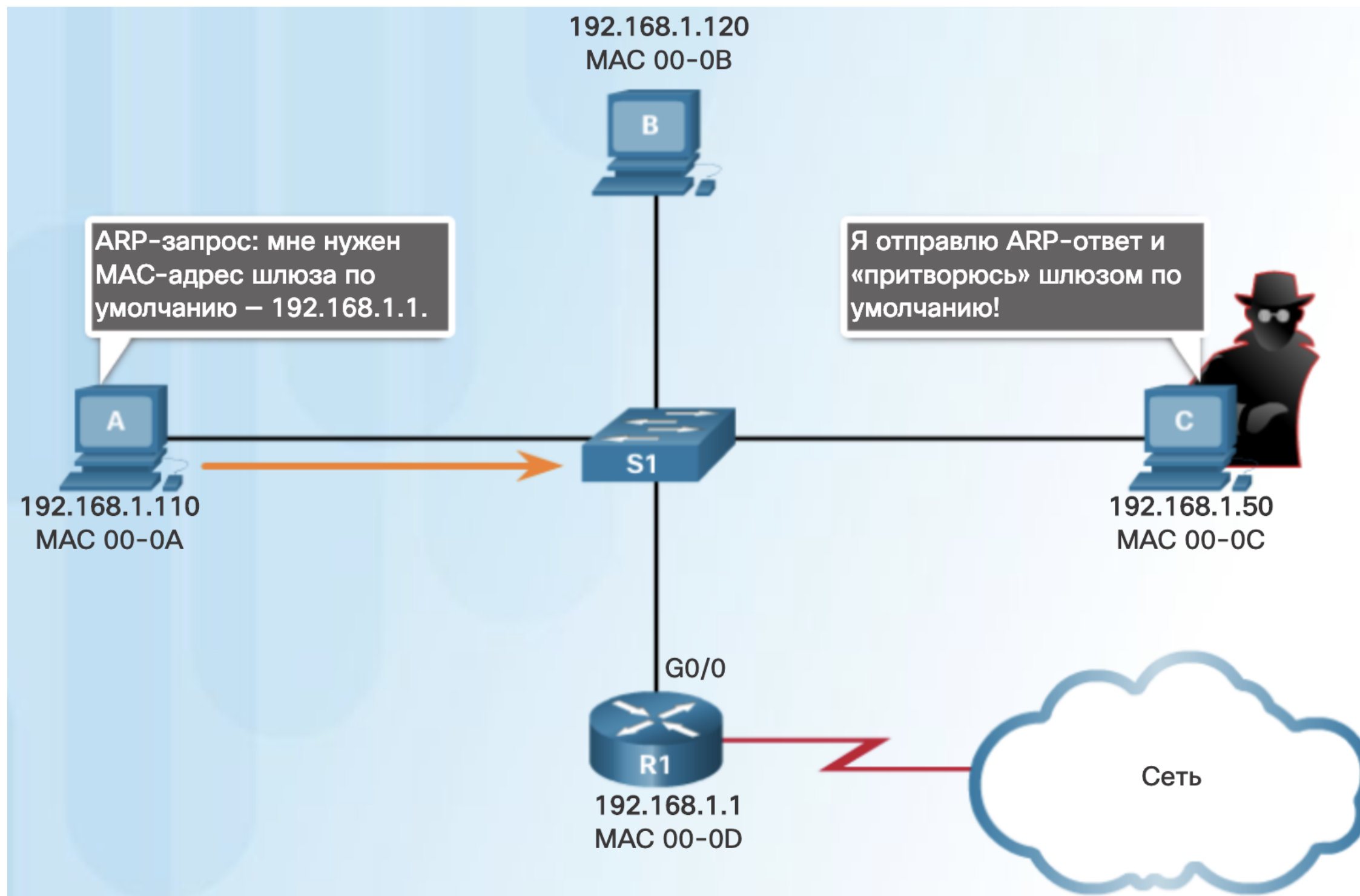
Протокол ARP

ARP - Address Resolution Protocol

Служит для сопоставления MAC и IP адресов и хранения таблицы сопоставлений.



Спуфинг ARP



Сетевой уровень

Сетевой уровень

Сетевой уровень (network layer) является комплексным уровнем, обеспечивающим выбор маршрута и соединение между собой двух рабочих станций, которые могут быть установлены в географически удаленных друг от друга сетях. Он решает три основных задачи: логическая адресация, маршрутизация (перенаправление пакетов) и определение маршрутов в сети.

Протоколы сетевого уровня

IPv4

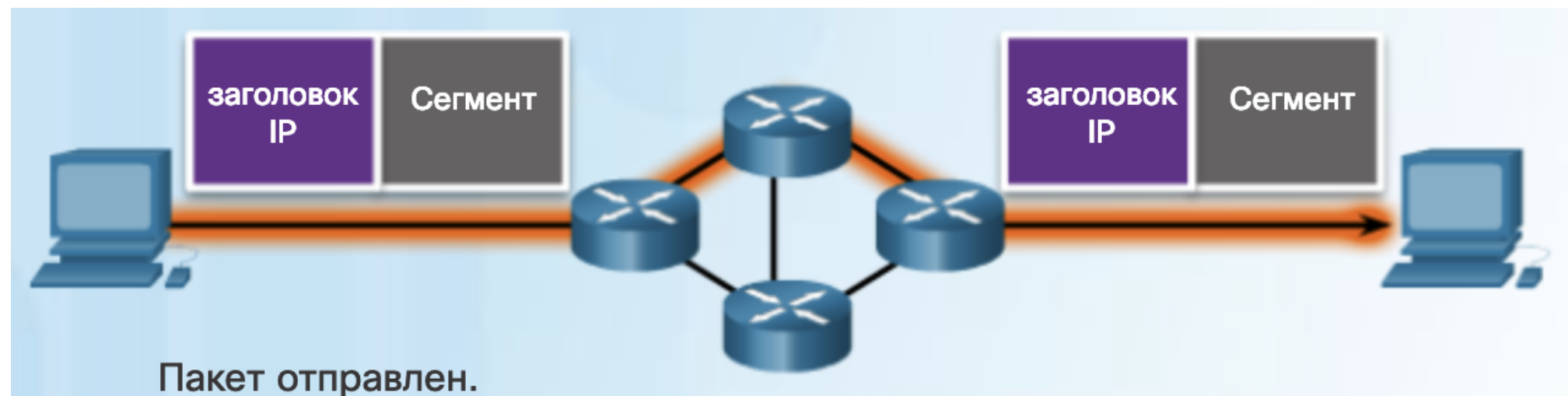
IPv6

Характеристики протокола IP

Без установления соединения.

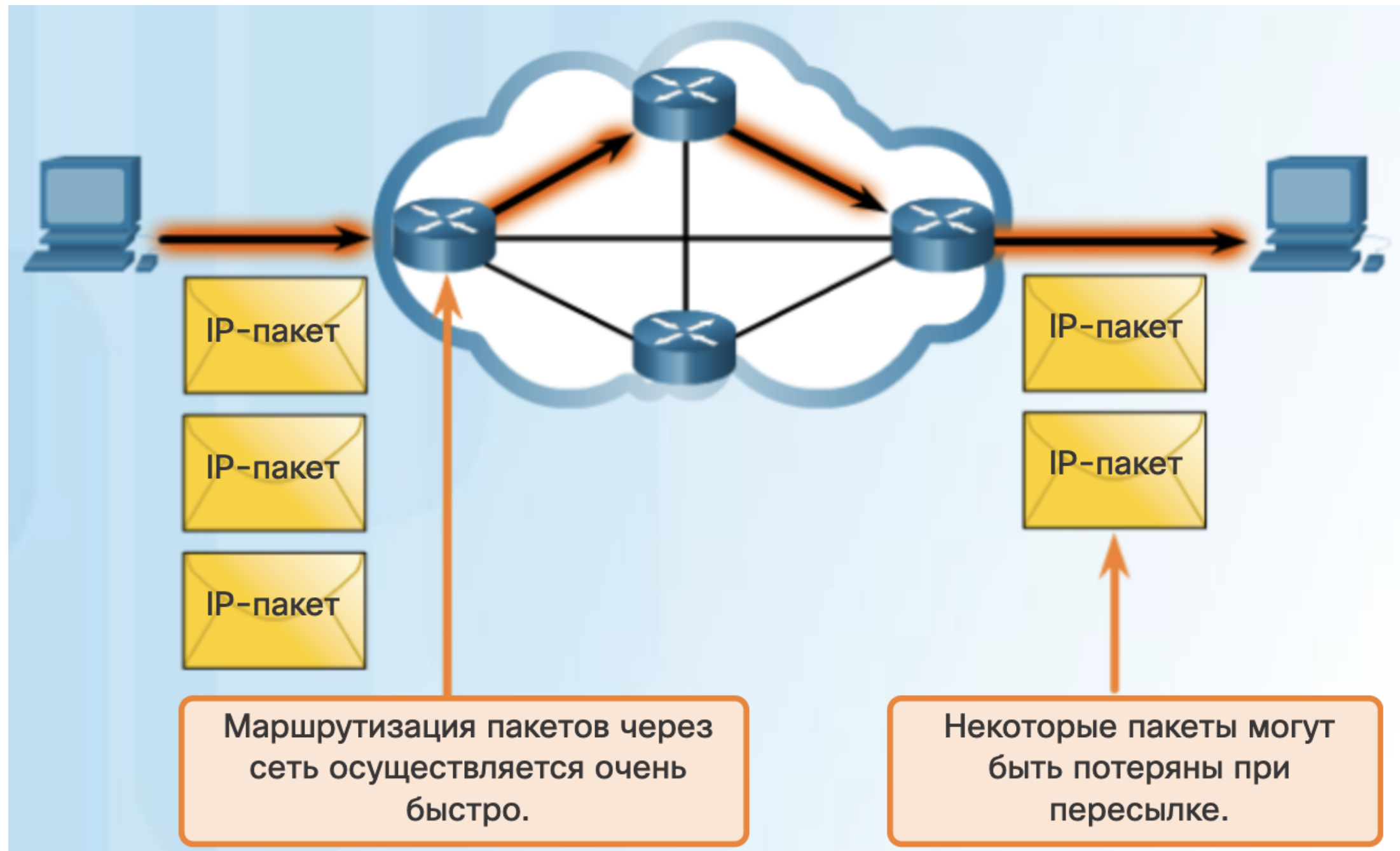
Отправитель не знает, присутствует ли получатель на месте, оставлен ли пакет, прочитает ли его получатель.

Получатель не знает, когда ожидать пакет.



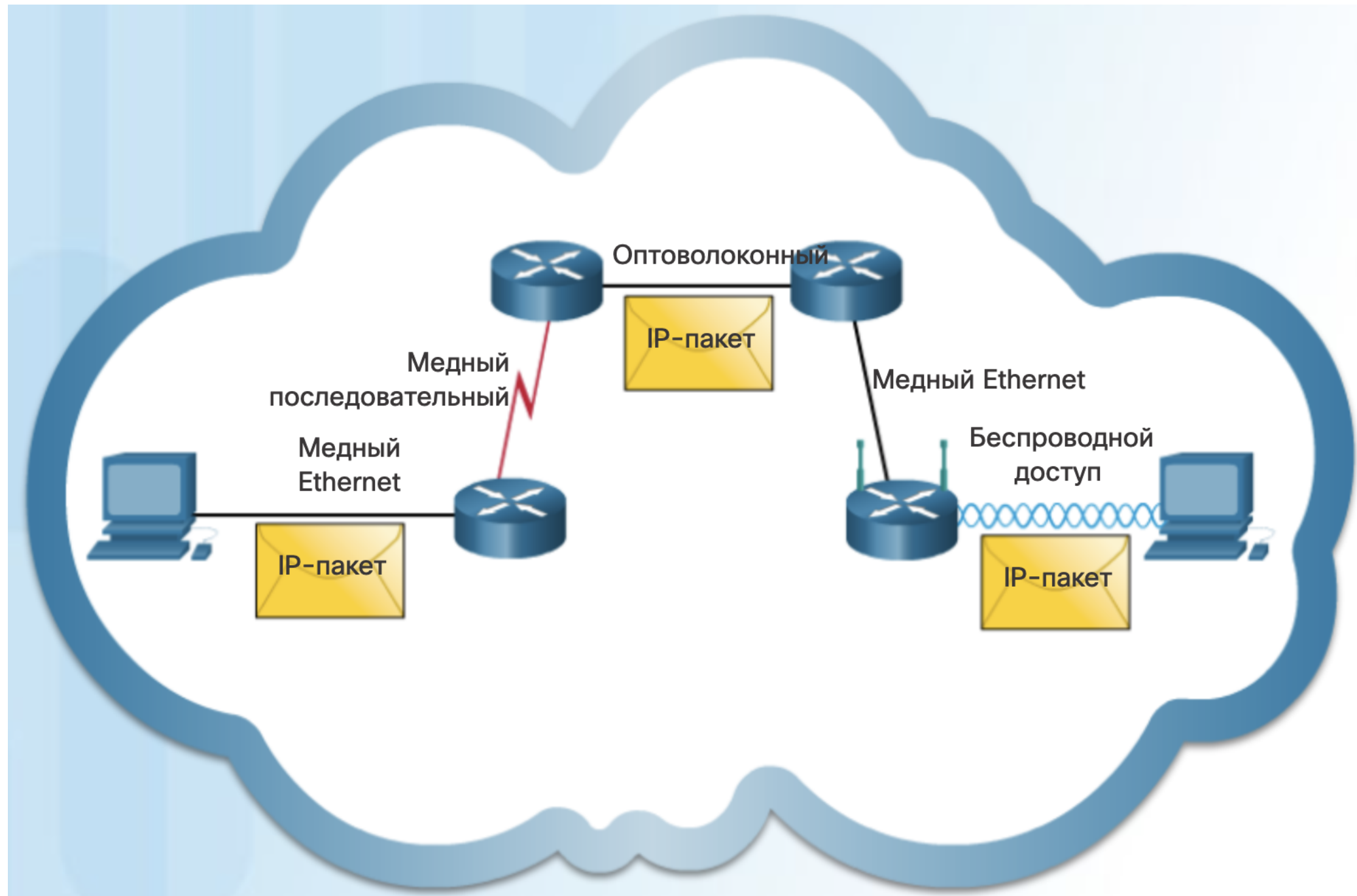
Характеристики протокола IP

Негарантированная доставка.

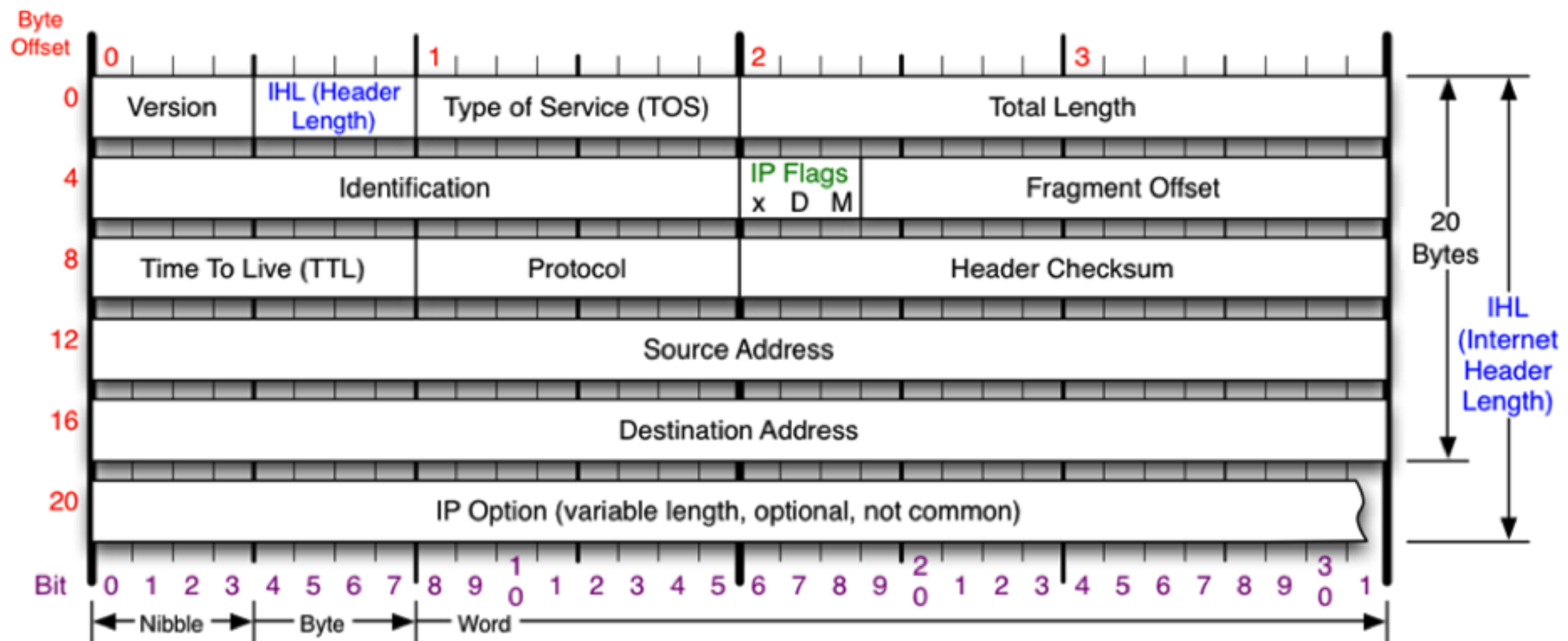


Характеристики протокола IP

Независимость от среды передачи



Заголовок IP-пакета



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

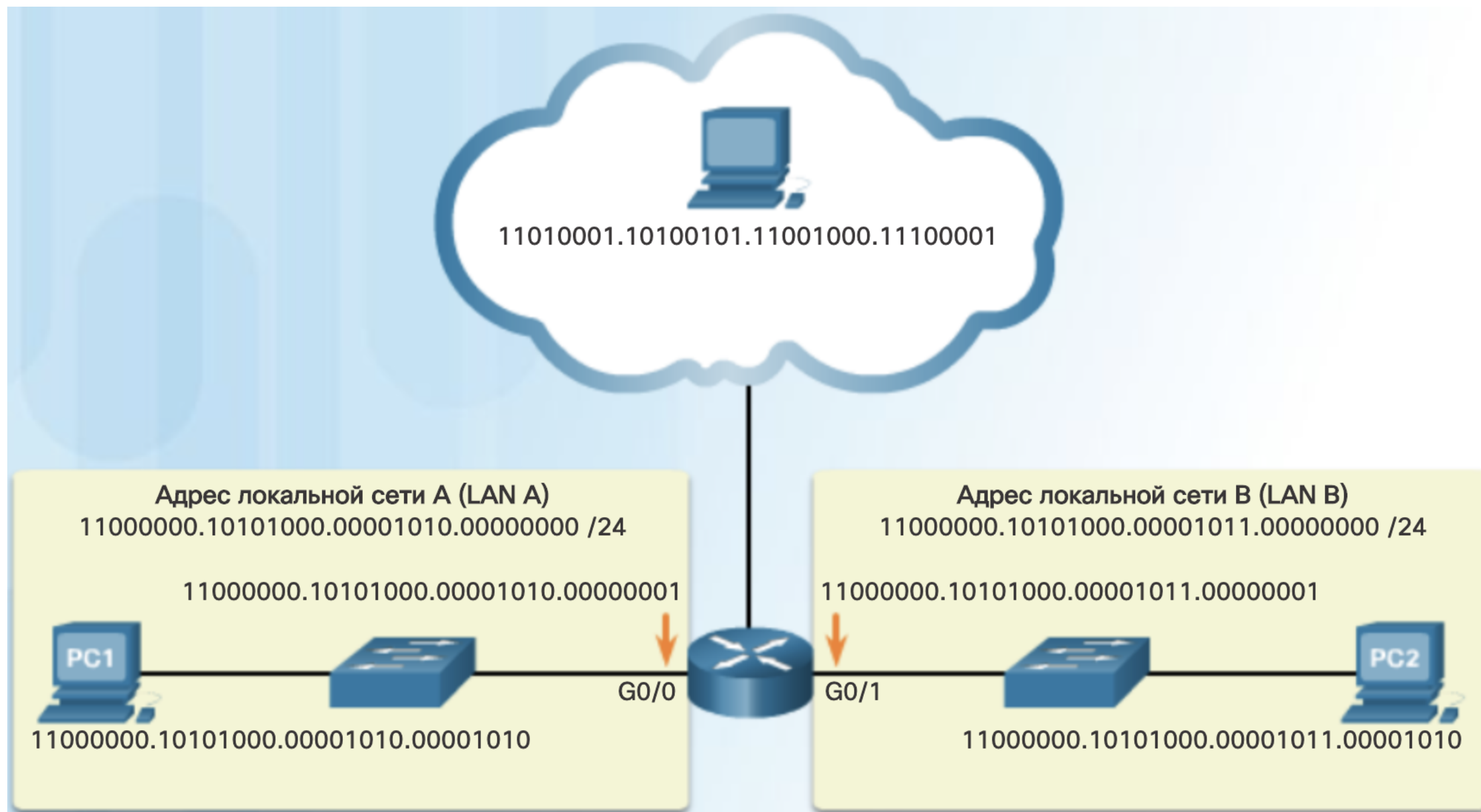
Недостатки IP

Нехватка IP-адресов. IPv4 может предложить лишь ограниченное количество уникальных публичных IP-адресов. Несмотря на то что существует примерно 4 миллиарда IPv4-адресов, ощущается их нехватка.

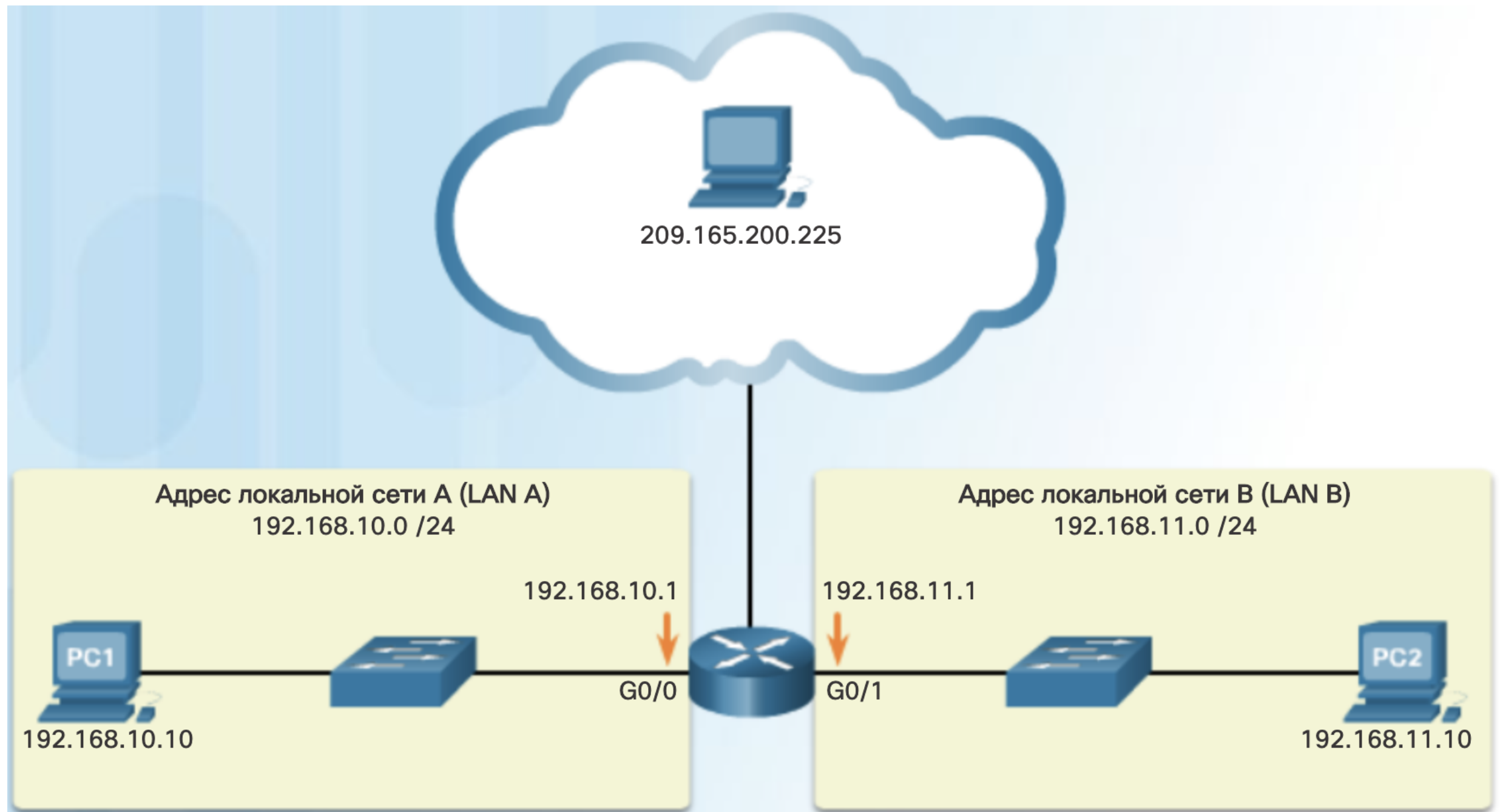
Расширение таблицы интернет-маршрутизации. Таблица маршрутизации используется маршрутизаторами для определения оптимальных путей пересылки данных. По мере увеличения количества серверов (узлов), подключенных к Интернету, также растет число сетевых маршрутов.

Нехватка сквозных соединений. Преобразование сетевых адресов (NAT) представляет собой технологию, которая обычно применяется в сетях IPv4. NAT позволяет различным устройствам совместно использовать один публичный IPv4-адрес. При этом, поскольку публичный IPv4-адрес используется совместно, IPv4-адрес узла внутренней сети скрыт.

IP-адрес



IP-адрес



IP-адрес

80.95.245.70

80	95	245	70
01010000	01011111	11110101	01000110

32-разрядное число, обычно представленное в десятичном виде с разделительными точками.

IP-адрес можно разделить на четыре октета.

Каждый октет может принимать значения от 0 до 255

IP-адрес

192.168.10.165

192	168	10	165
11000000	10101000	00001010	10100101
Сетевая часть			Узловая часть

Биты в сетевой части адреса должны быть одинаковыми у всех устройств, находящихся в одной сети. Биты в узловой части адреса должны быть уникальными для каждого узла в сети. Если два узла имеют одну битовую комбинацию в сетевой части, то эти два узла находятся в одной и той же сети

Маска подсети

255.255.255.0

255	255	255	0
11111111	11111111	11111111	00000000
Сетевая часть			Узловая часть

Маска подсети - 32-битная последовательность 1 и 0, определяющая структуру IP-адреса:

- биты 1 и 0 не должны чередоваться;
- группа 1 находится в левой части;
- группа 0 находится в правой части.

Маска подсети

**Возможные
варианты
октетов
маски
подсети**

Десятичное значение	Двоичное значение
0	00000000
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

Определение адреса сети

IP-адрес	192	168	10	165
	11000000	10101000	00001010	10100101
Маска подсети	255	255	255	0
	11111111	11111111	11111111	00000000
Адрес сети	192	168	10	0
	11000000	10101000	00001010	00000000

Для идентификации сетевой и узловой части IP-адреса маска подсети побитово сравнивается с IP-адресом. Единицы в маске подсети определяют сетевую часть, а нули — узловую часть. Определить адрес подсети можно при помощи логического умножения IP-адреса на маску подсети

Определение адреса сети

Определение сети по IP-адресу и маске

Форма	Десятичная	Двоичная			
Адрес	210.65.20.1	11010010	01000001	00010100	00000001
Маска	255.255.255.0	11111111	11111111	11111111	00000000
Результат	210.65.20.0	11010010	01000001	00010100	00000000

Определение адреса сети

IP-адрес узла	Маска подсети	Адрес сети
172.30.117.221	255.255.240.0	
172.18.212.22	255.255.255.248	
10.63.138.18	255.255.248.0	
10.118.122.180	255.255.255.252	
10.23.202.6	255.255.224.0	

Маска подсети и префикс

Маска подсети	Префикс
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Длина префикса обозначает количество бит, установленных в единицу (1) в маске подсети.

Типы адресов в сети

Сеть

Адрес сети

192.168.10.0/24

.00000000

Адреса узлов

Адрес первого узла

192.168.10.1/24

.00000001

Адрес последнего узла

192.168.1.254/24

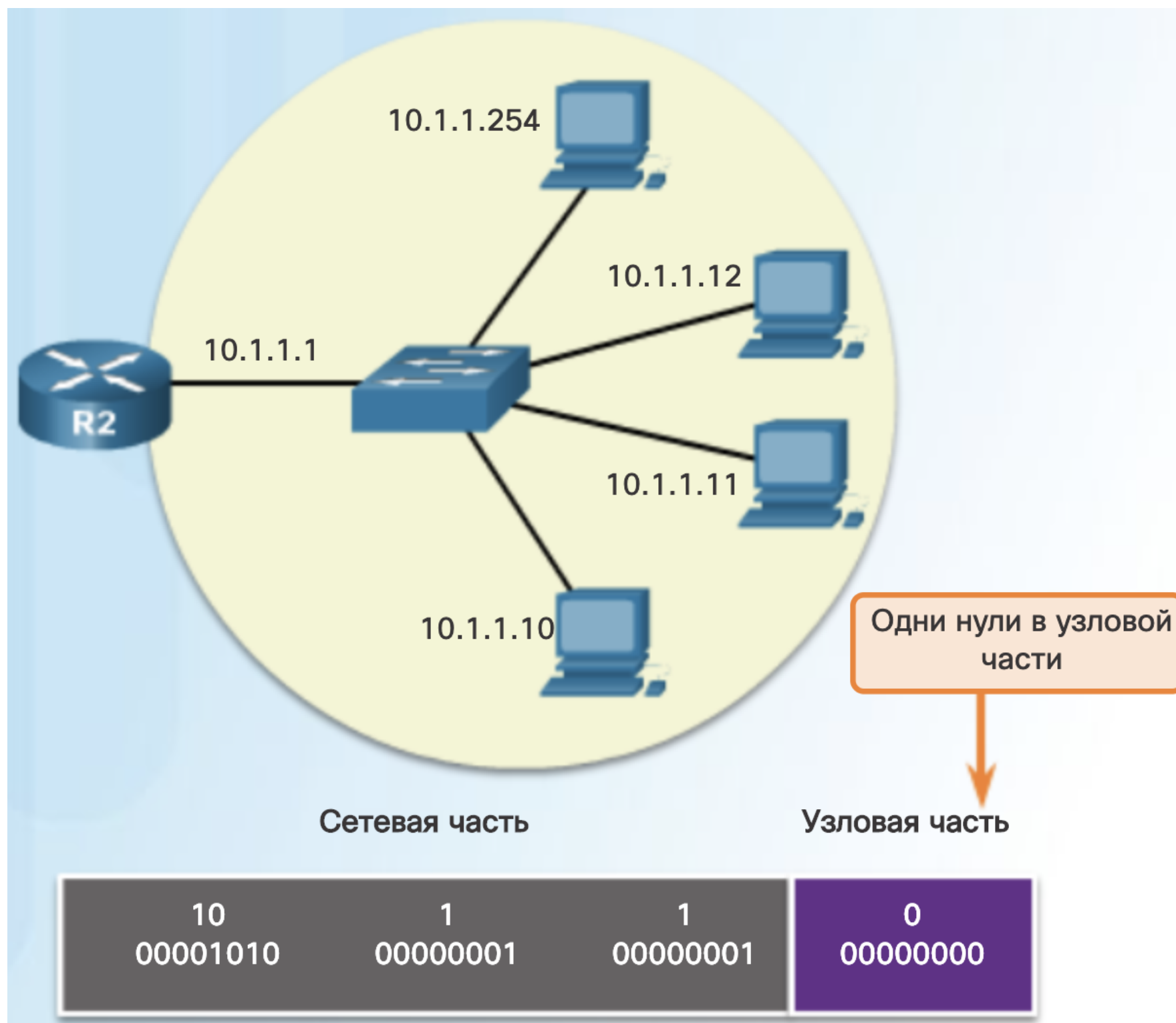
.11111110

Широковещательный
адрес

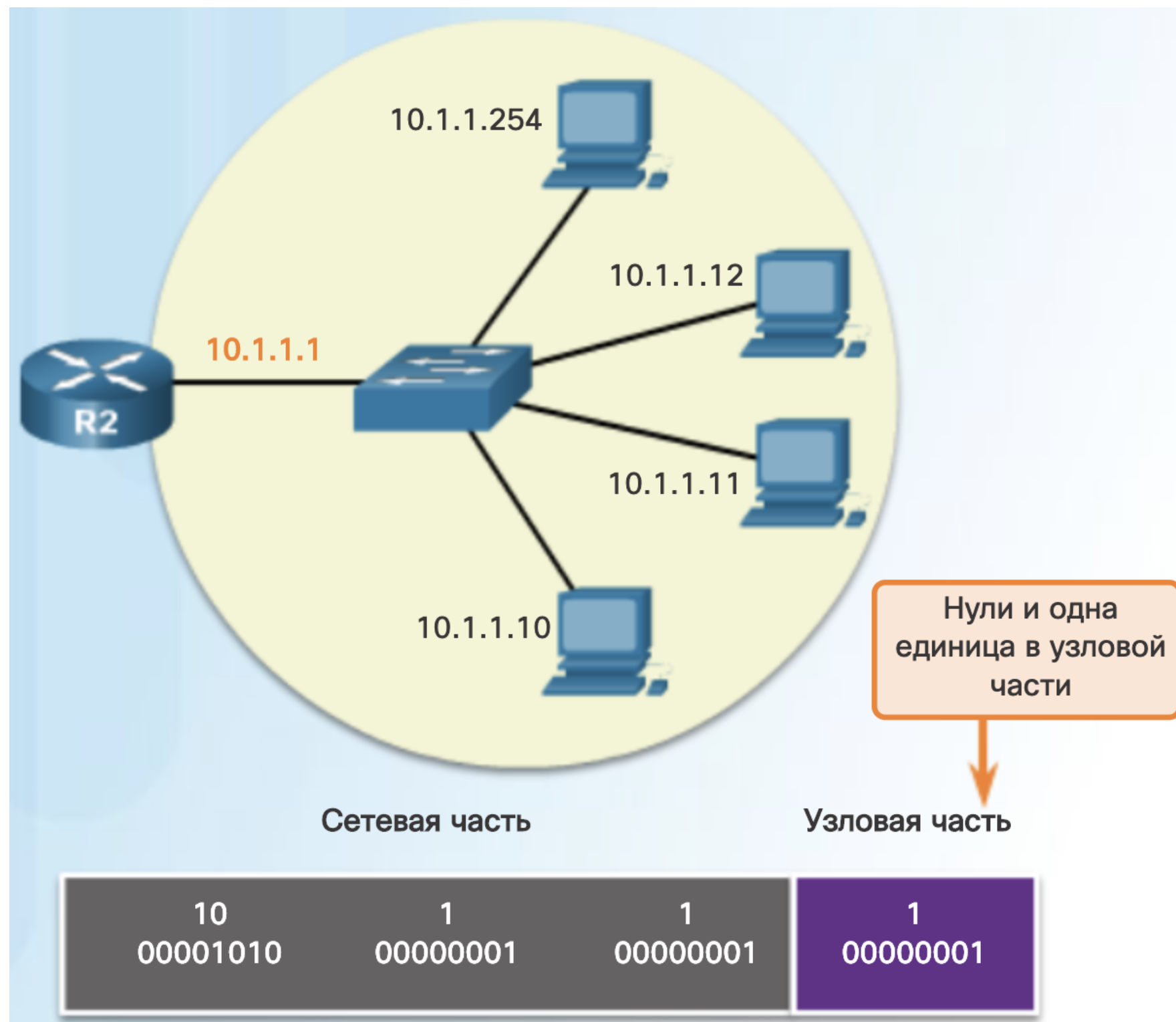
192.168.1.255/24

.11111111

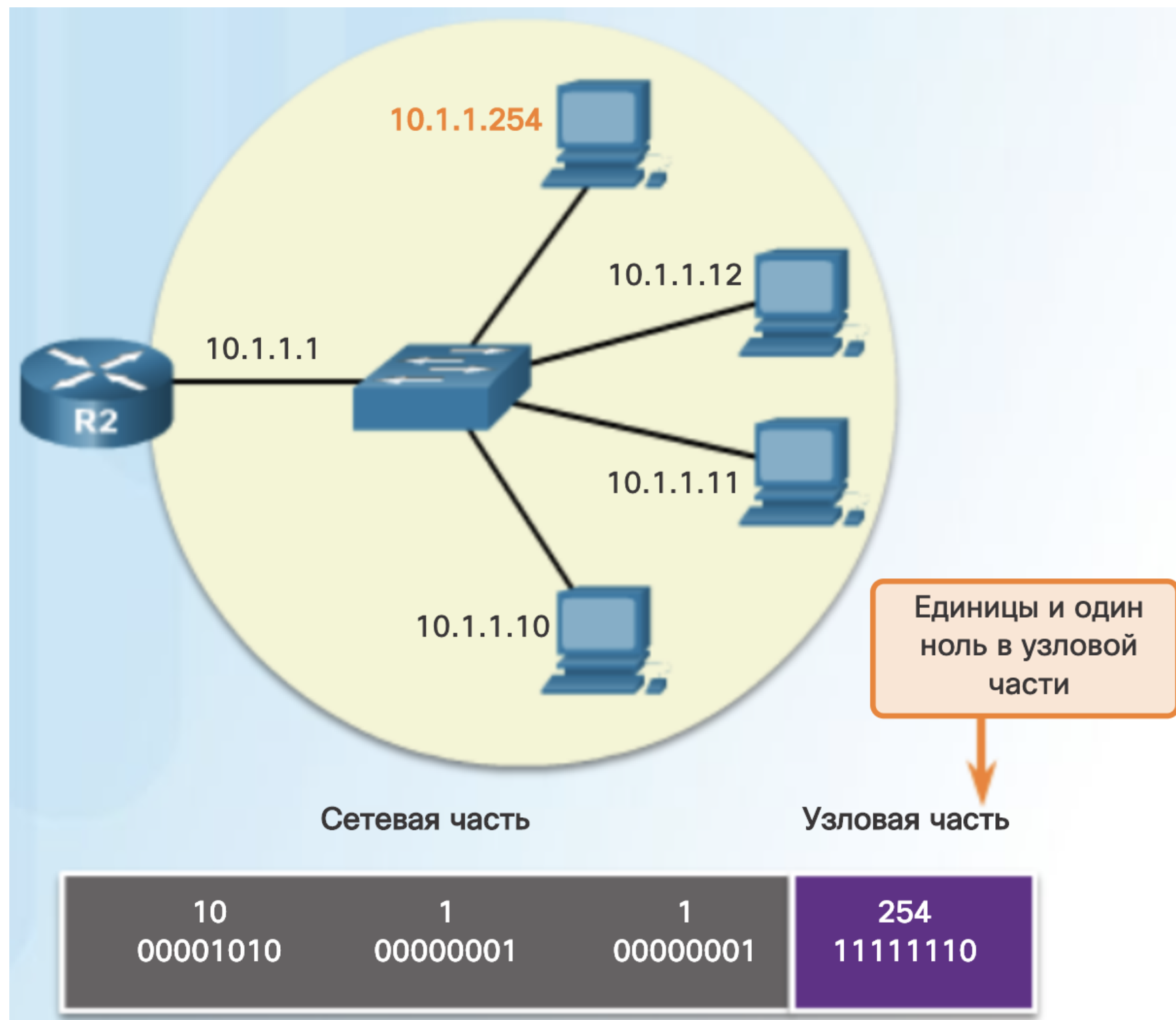
Адрес сети



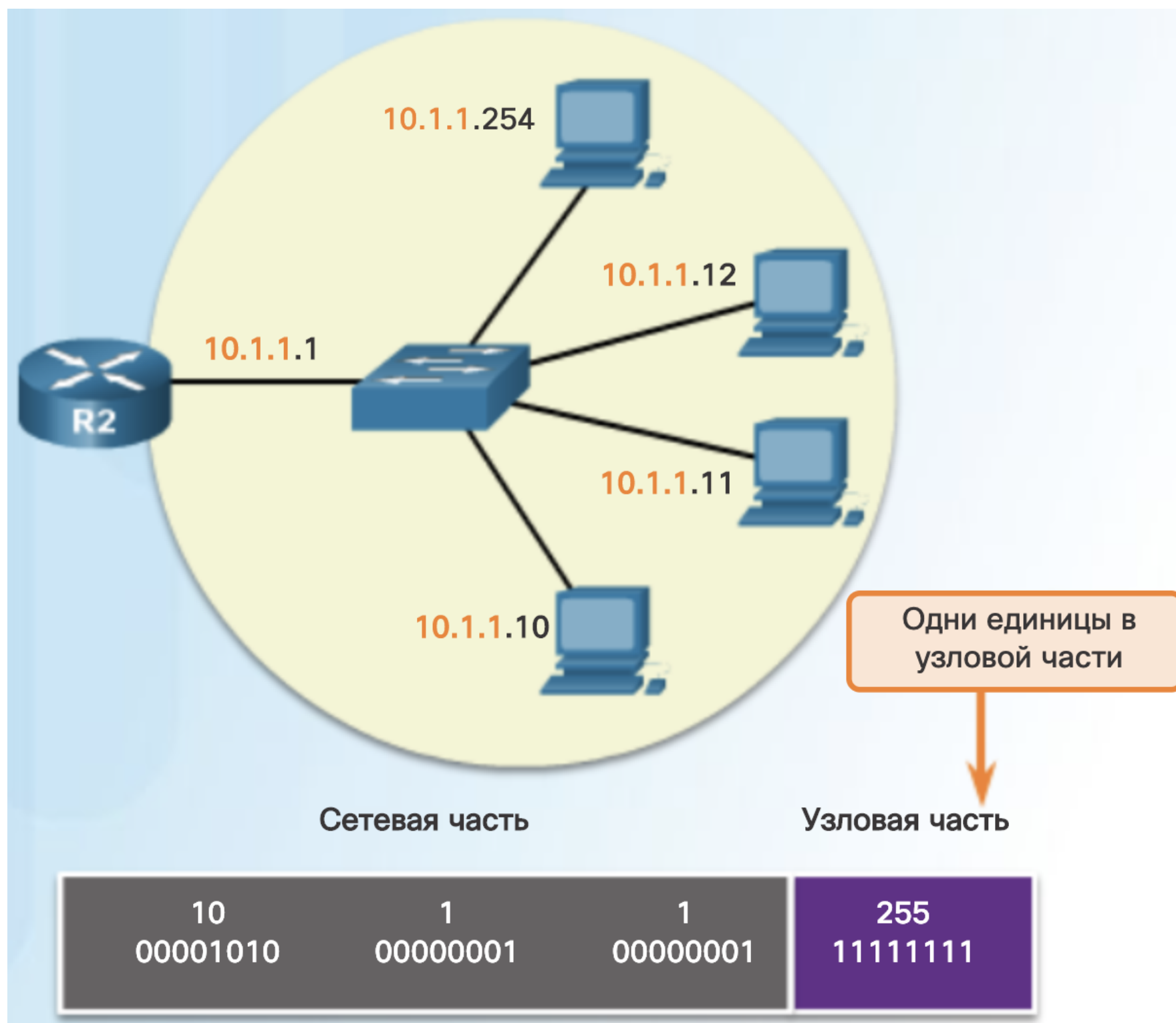
Первый адрес узла



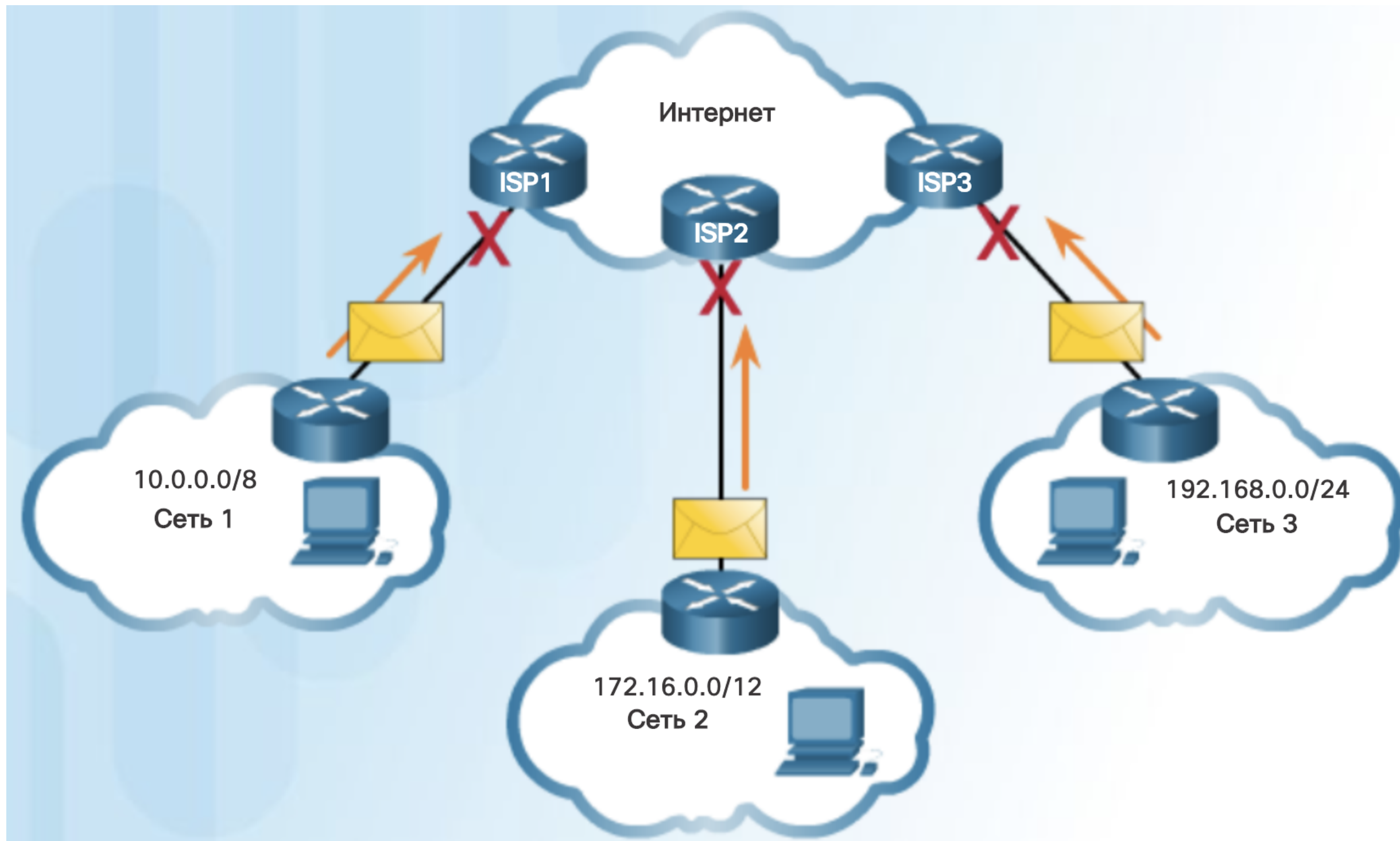
Последний адрес узла



Широковещательный адрес



Типы IP-адресов



«Особые» группы IP-адресов

Частные адреса:

10.0.0.0-10.255.255.255 (10.0.0.0/8)

172.16.0.0 - 172.31.255.255 (172.16.0.0/12)

192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

127.0.0.0/8 - внутренний адрес сетевой карты

169.254.0.0/16 - используются клиентом DHCP для самостоятельной конфигурации в случае, если ни один DHCP-сервер не доступен

Разделение сетей на подсети

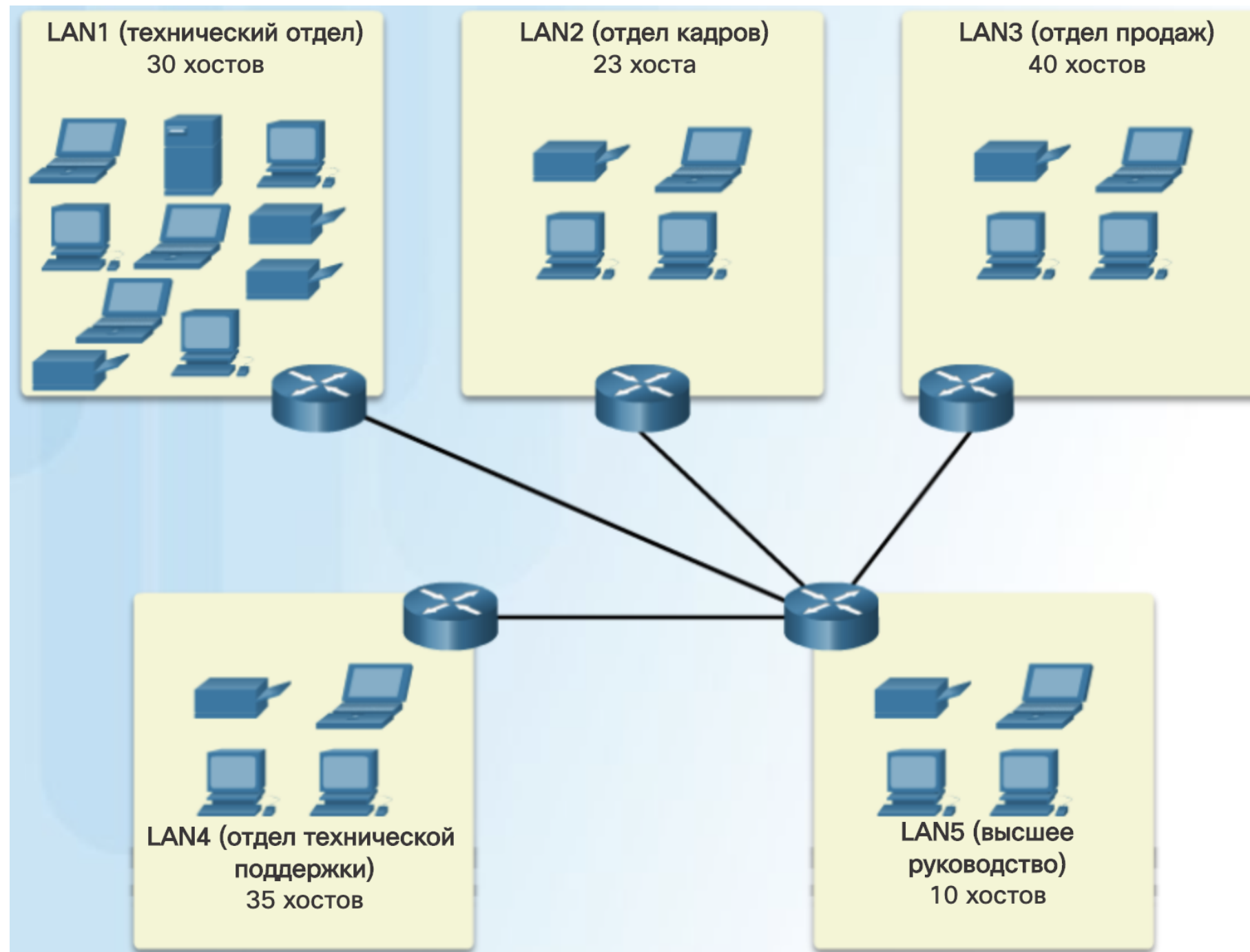
При планировании подсетей нужно учесть два параметра.

- Необходимое количество адресов узлов в каждой сети
- Необходимое количество отдельных подсетей.

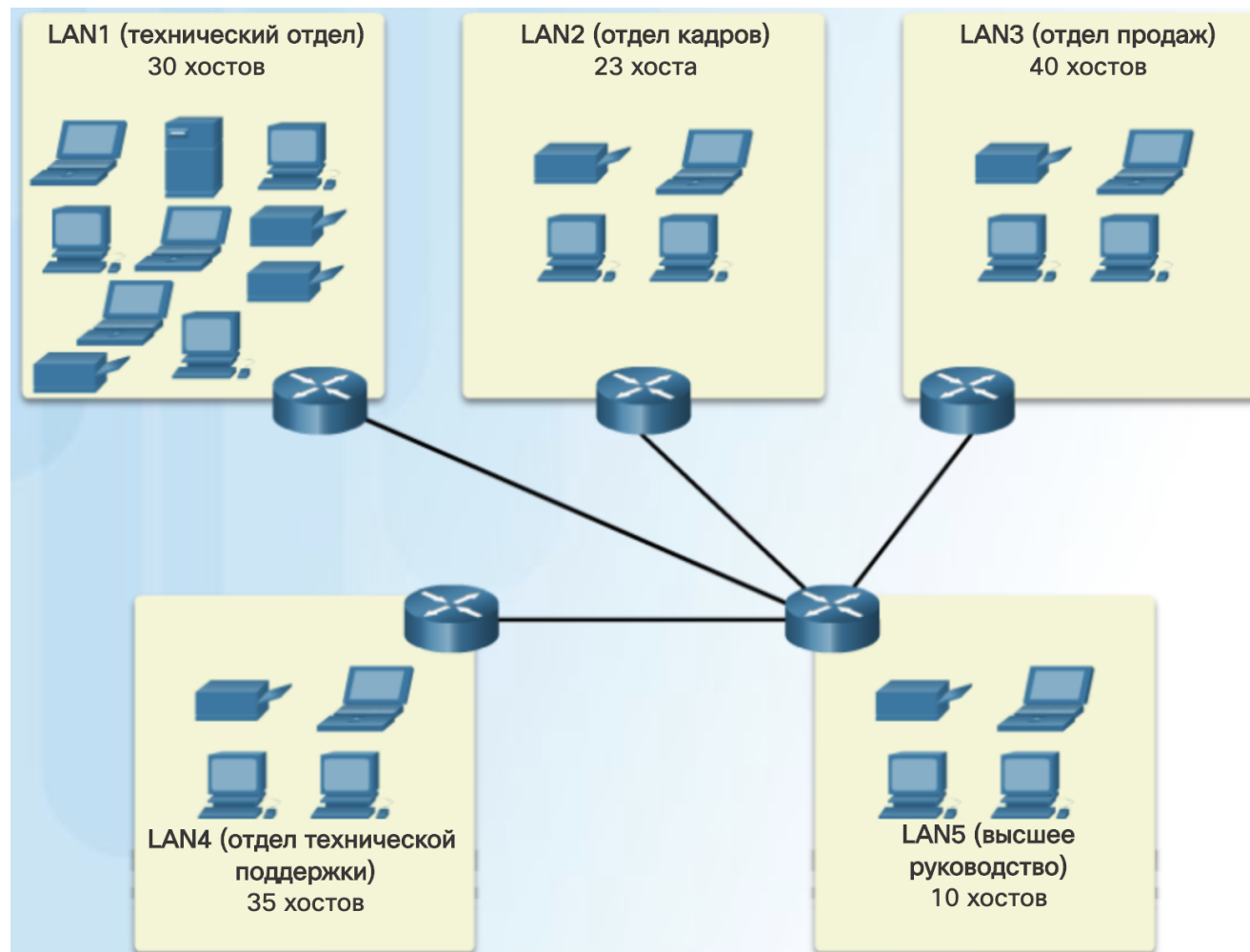
Длина префикса	Маска подсети	Маска в двоичной системе s=сеть, h=узел	Кол-во подсетей	Кол-во узлов
/24	255.255.255.0	SSSSSSSS.SSSSSSSS.SSSSSSSS.hhhhhhhh 11111111.11111111.11111111.00000000	1	254
/25	255.255.255.128	SSSSSSSS.SSSSSSSS.SSSSSSSS.shhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	SSSSSSSS.SSSSSSSS.SSSSSSSS.sshhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	SSSSSSSS.SSSSSSSS.SSSSSSSS.ssshhhhh 11111111.11111111.11111111.11100000	8	30

Разделение сетей на подсети

172.16.0.0/22
10101100.00010100.000000|00.00000000/22
сетевая часть узловая часть



Разделение сетей на подсети



172.16.0.0/22
10101100.00010100.000000|00.00000000/22
сетевая часть узловая часть

Топология состоит из 5 сегментов локальной сети (LAN) и 4 межсетевых соединений между маршрутизаторами. Таким образом, требуются 9 подсетей. Самая большая подсеть должна содержать 40 узлов.

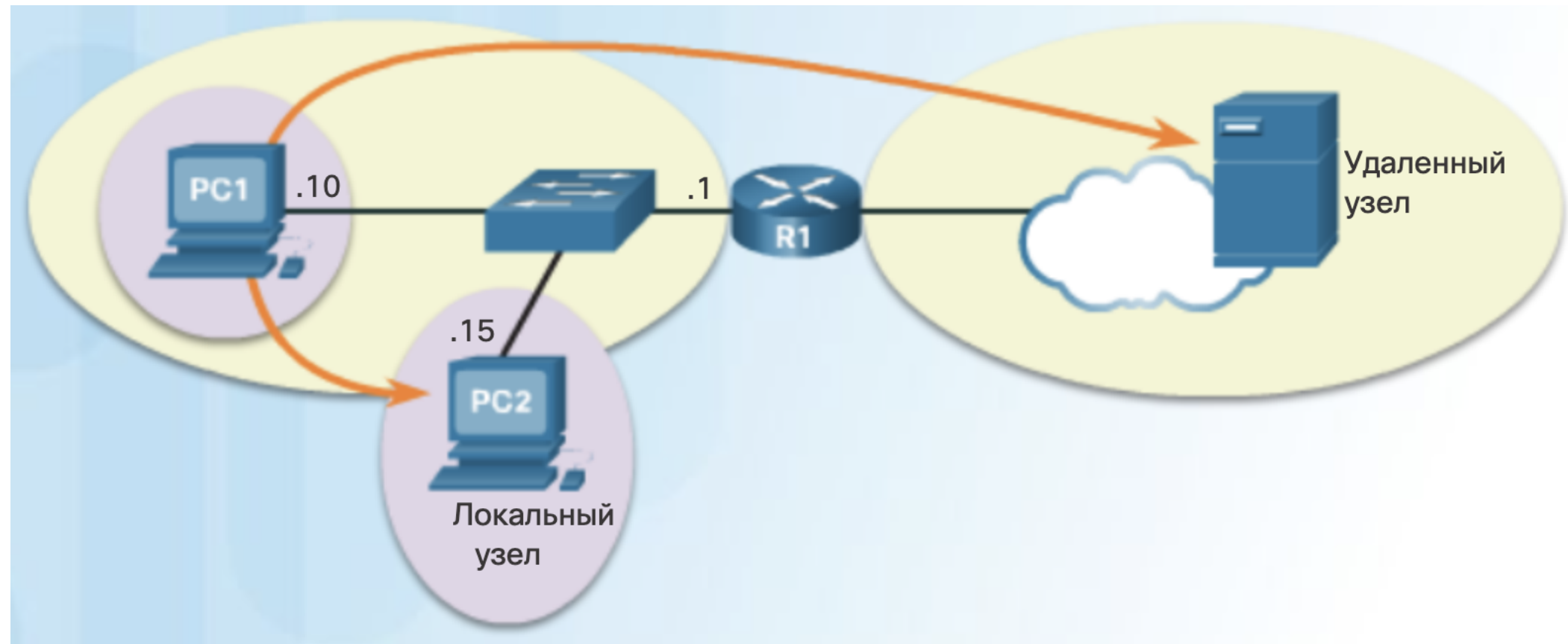
Сетевой адрес 172.16.0.0/22 имеет 10 бит в узловой части. Поскольку самой крупной подсети требуется 40 узлов, для обеспечения их адресации требуется не менее 6 бит в узловой части. Это число определяется по следующей формуле: $2^6 - 2 = 62$ узла.

По формуле определения количества подсетей получаем 16 подсетей: $2^4 = 16$. Это соответствует нашим требованиям и обеспечивает некоторый запас для роста в будущем. Таким образом, первые 4 бита в узловой части можно использовать для создания подсетей. Если заимствовать 4 бита, новая длина префикса будет /26 с маской подсети 255.255.255.192.

172.16.0.0/26
10101100.00010100.00000000.00|000000/26
сетевая часть узловая часть

Маршрутизация

Тип узла назначения



Узел может отправить пакет на следующие адреса.

- **Самому себе.** Узел может отправить эхо-запрос на специальный IPv4-адрес, который представлен как 127.0.0.1 и называется интерфейсом loorback. Отправка эхо-запроса на интерфейс loorback тестирует стек протокола TCP/IP на узле.
- **Локальный узел.** Узел в той же локальной сети, в которой также находится отправляющий узел. Узлы используют один и тот же сетевой адрес.
- **Удаленный узел.** Узел в удаленной сети. Узлы не используют один и тот же сетевой адрес.

Шлюз по умолчанию



Шлюз по умолчанию

Шлюз по умолчанию — это сетевое устройство, которое направляет трафик в другие сети. Это маршрутизатор, который может направлять трафик за пределы локальной сети:

- направляет трафик в другие сети;
- имеет IP-адрес в том же диапазоне, что и другие узлы в сети;
- может принимать входящие данные и передавать данные наружу.

Таблица маршрутизации

netstat -r

route print

show ip route

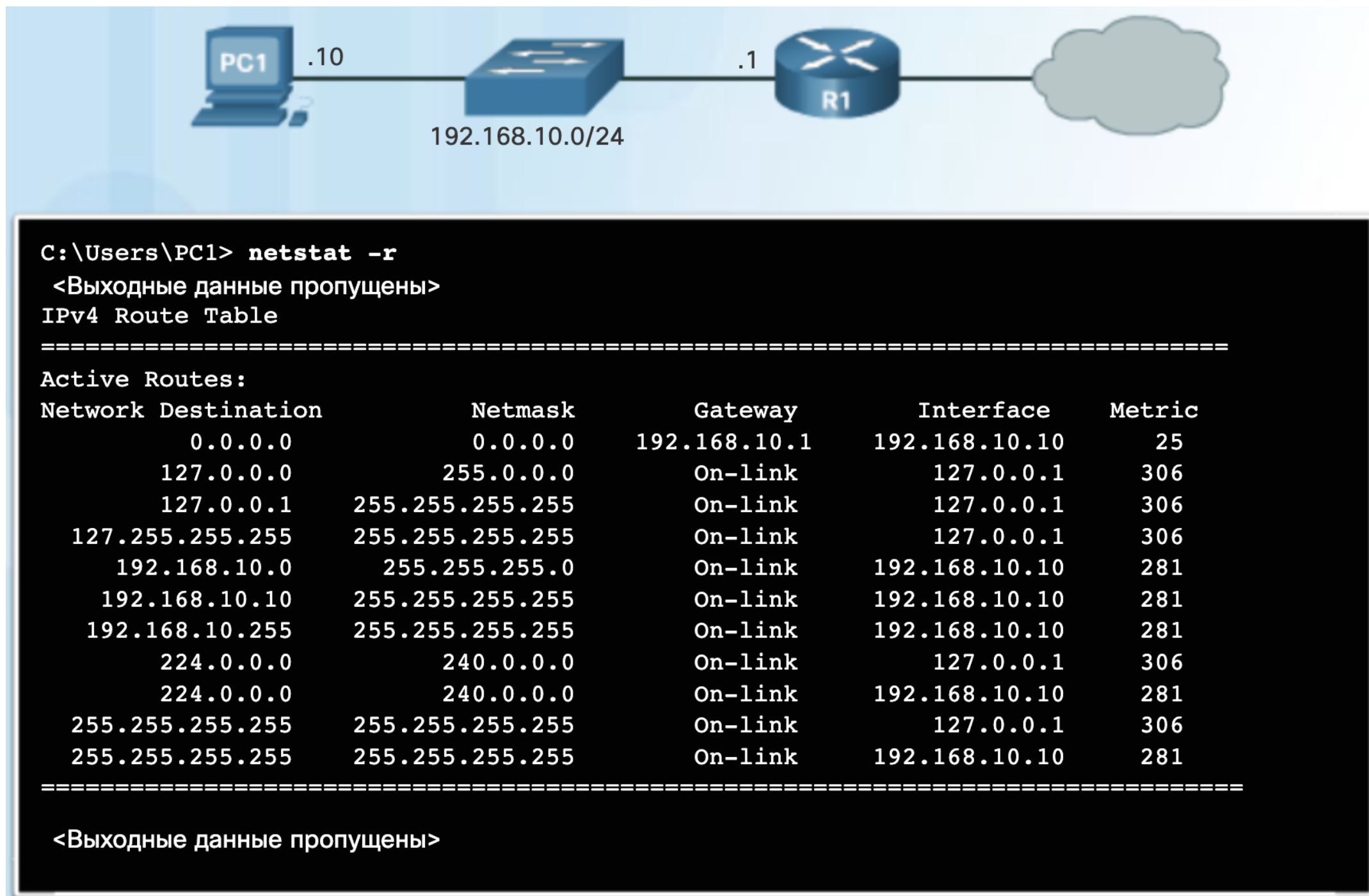


Таблица маршрутизации

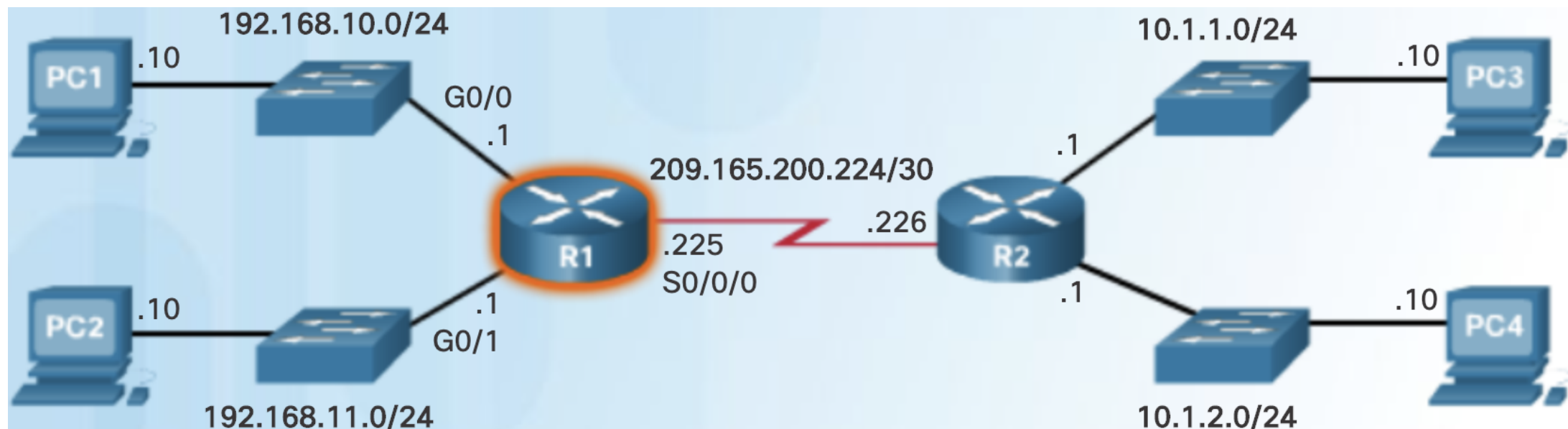


Таблица маршрутизации

В таблице маршрутизации маршрутизатора может храниться следующая информация.

- **Маршруты с прямым подключением.** Эти маршруты предоставляются активными интерфейсами маршрутизаторов. Маршрутизаторы добавляют маршрут с прямым подключением, когда интерфейс настроен с IP-адресом и активирован.
- **Удаленные маршруты.** Эти маршруты предоставляются удаленными сетями, подключенными к другим маршрутизаторам. Маршруты к этим сетям могут быть настроены на локальном маршрутизаторе вручную сетевым администратором или назначены динамически с помощью протоколов динамической маршрутизации.
- **Маршрут по умолчанию.** Подобно узлу, маршрутизаторы также используют маршрут по умолчанию в качестве последнего средства, если иного маршрута до нужной сети в таблице маршрутизации нет.

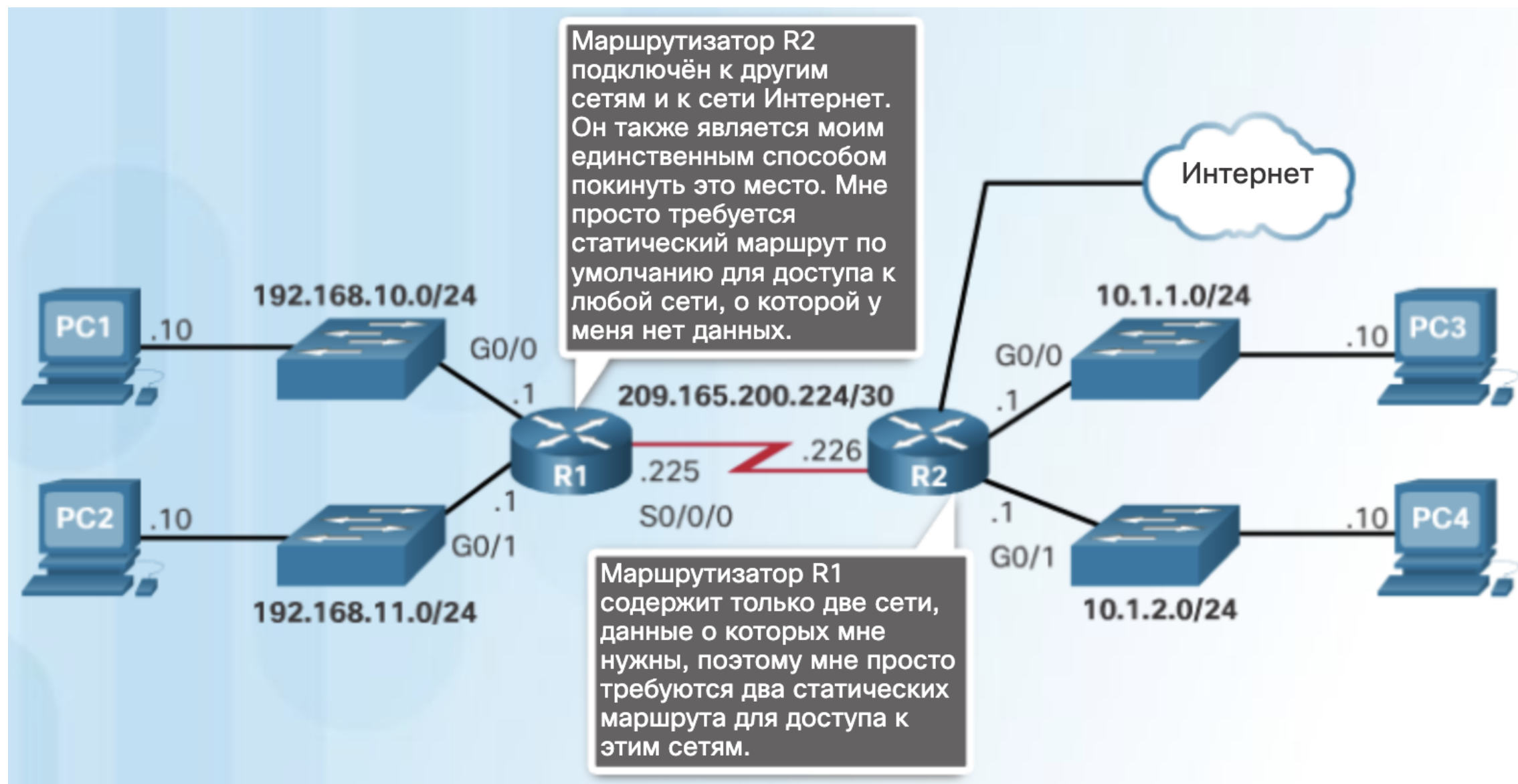
Таблица маршрутизации



Gateway of last resort is not set

```
10.0.0.0/24 is subnetted, 2 subnets
D      10.1.1.0/24 [90/2172416] via 209.165.200.226, 00:00:44, Serial0/0/0
D      10.1.2.0/24 [90/2172416] via 209.165.200.226, 00:00:44, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected, GigabitEthernet0/0
L      192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.11.0/24 is directly connected, GigabitEthernet0/1
L      192.168.11.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.224/30 is directly connected, Serial0/0/0
L      209.165.200.225/32 is directly connected, Serial0/0/0
```

Статическая маршрутизация

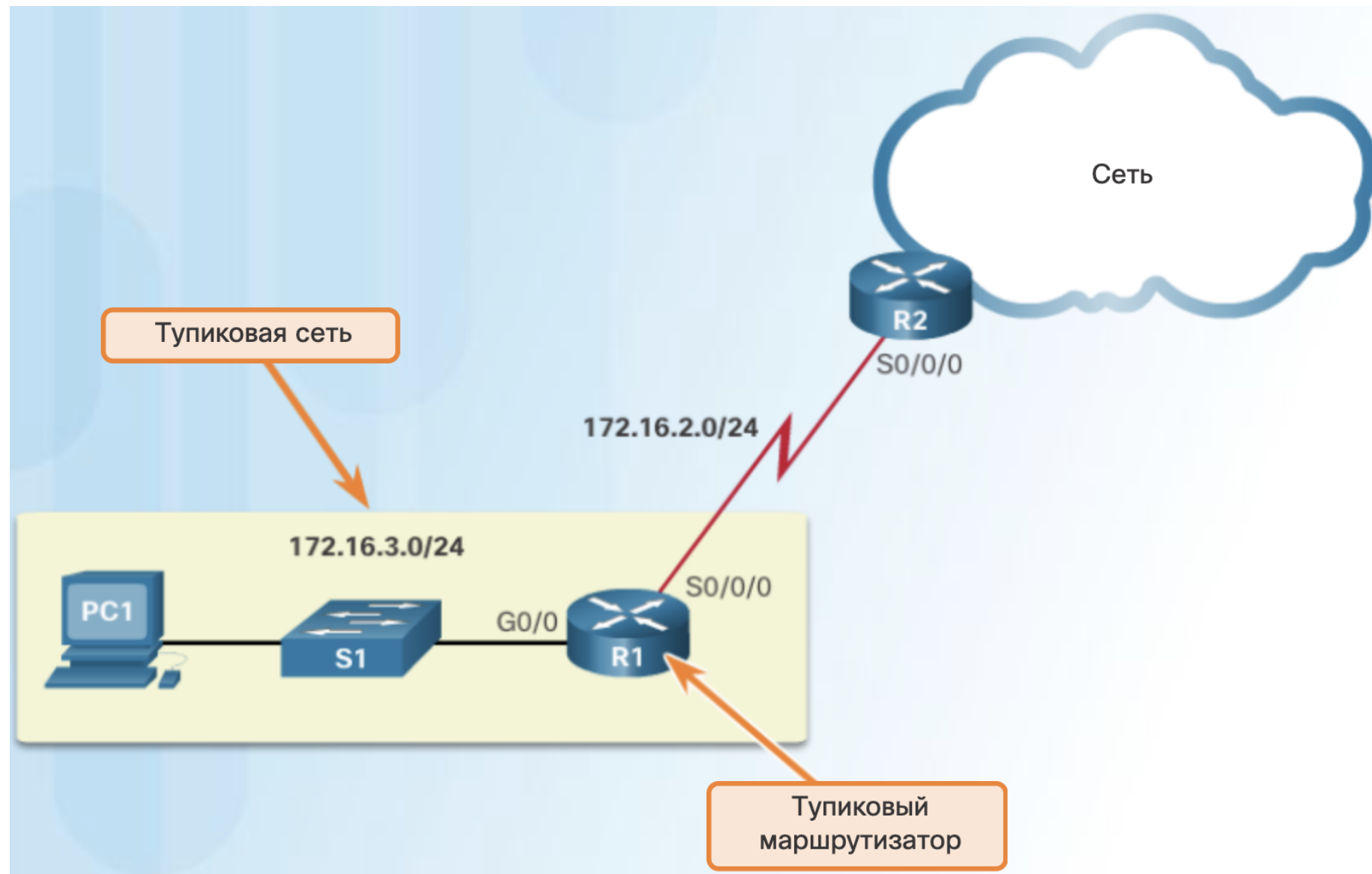


Статическая маршрутизация

Статическая маршрутизация используется в трех ситуациях:

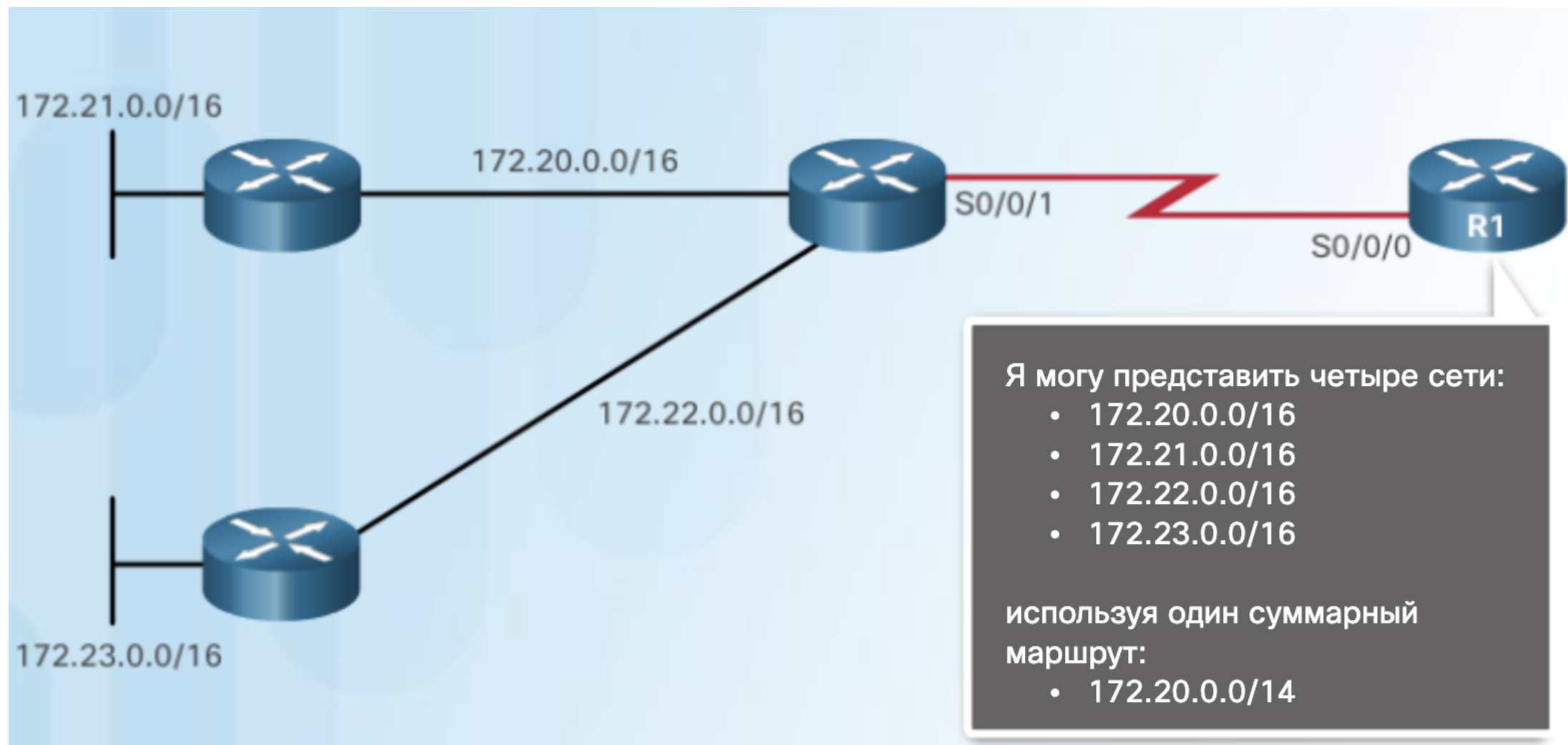
- обеспечение **упрощенного обслуживания** таблицы маршрутизации в небольших сетях, которые не планируется существенно расширять;
- **маршрутизация к тупиковым сетям и от них**; тупиковая сеть представляет собой сеть, доступ к которой осуществляется через один маршрут, и маршрутизатор имеет только одно соседнее устройство;
- **использование единого маршрута по умолчанию** для представления пути к любой сети, не имеющего более точного совпадения с другим маршрутом в таблице маршрутизации.

Статическая маршрутизация



У любой сети, подключенной к маршрутизатору R1, будет только один путь для доступа к другим местам назначения (к сетям, подключенным к маршрутизатору R2, или к местам назначения за пределами маршрутизатора R2). Это означает, что сеть 172.16.3.0 является тупиковой, а маршрутизатор R1 – тупиковым маршрутизатором.

Суммарный статический маршрут



Для уменьшения числа записей в таблице маршрутизации можно объединить несколько статических маршрутов в один статический маршрут. Это возможно при следующих условиях:

- Сети назначения являются смежными и могут быть объединены в один сетевой адрес.
- Все статические маршруты используют один и тот же выходной интерфейс или один IP-адрес следующего перехода.

Настройка статического маршрута

Router(config)#**ip route** *network-address subnet-mask {ip-address|exit-intf}*

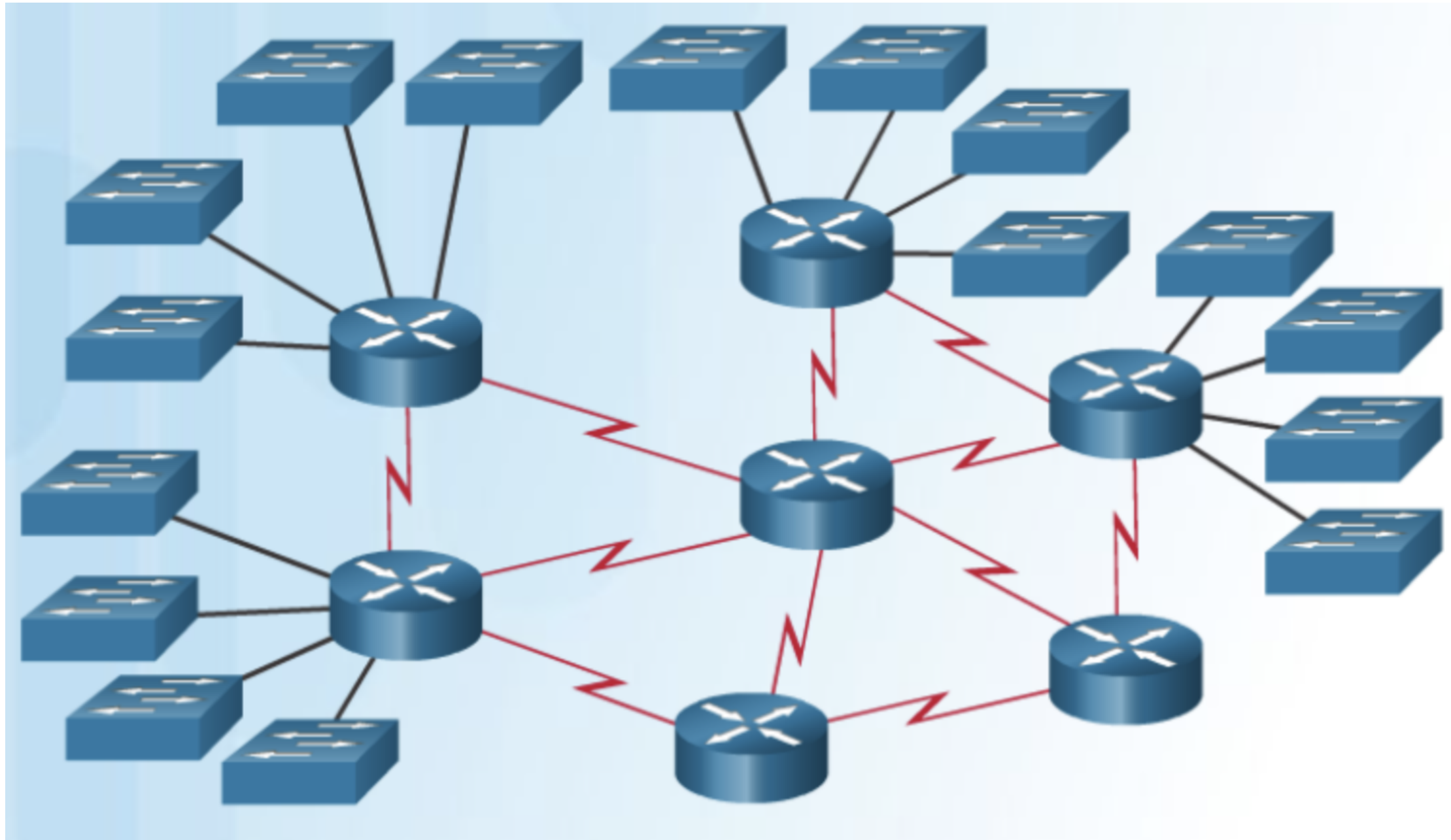
Параметр	Описание
network-address	Адрес удаленной сети назначения, который необходимо добавить в таблицу маршрутизации
subnet-mask	• Маска подсети удаленной сети назначения, которую необходимо добавить в таблицу маршрутизации. • Маску подсети можно изменить для объединения группы сетей.
ip-address	• Как правило, называется IP-адресом маршрутизатора следующего перехода. • Обычно используется при подключении к среде широковещательного доступа (т. е. Ethernet). • Обычно создает рекурсивный поиск
exit-intf	• Используйте выходной интерфейс для пересылки пакетов в сеть назначения. • Также называется напрямую подключенным статическим маршрутом. • Обычно используется при подключении к сети в конфигурации «точка-точка».
distance	• (Дополнительно) Настраивает административное расстояние. • Обычно используется для настройки плавающего статического маршрута.

Преимущества и недостатки статической маршрутизации

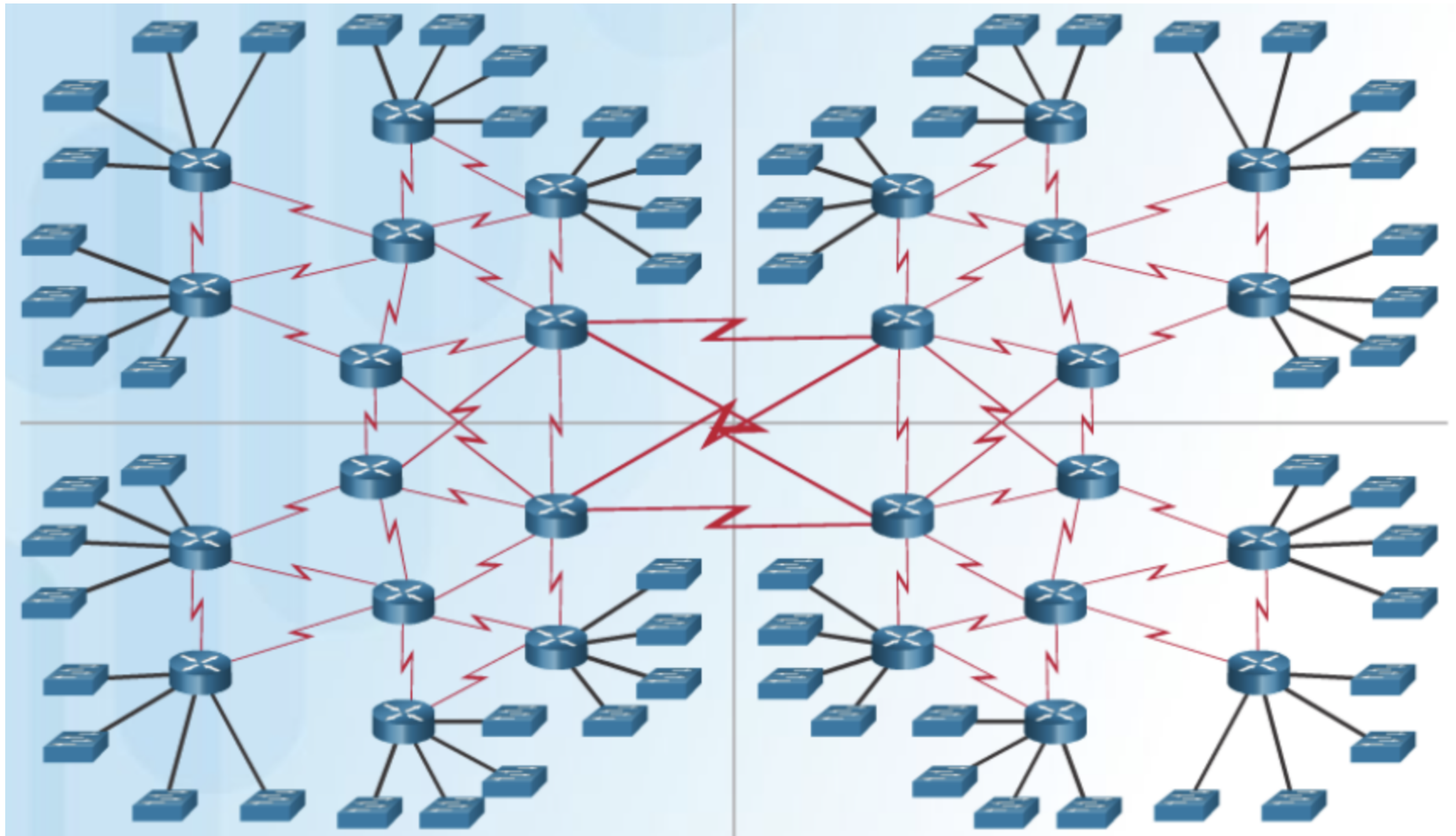
Преимущества	Недостатки
Простота внедрения в небольшой сети.	Подходит только для простых топологий или специальных задач (например, статический маршрут по умолчанию).
Высокий уровень безопасности. В отличие от протоколов динамической маршрутизации отправка объявлений не выполняется.	Сложность конфигурации значительно возрастает по мере роста сети.
Маршрут к месту назначения остаётся неизменным.	При необходимости изменения маршрутизации конфигурирование выполняется вручную.
Алгоритм маршрутизации или механизм обновления не требуется, следовательно, нет необходимости в дополнительных ресурсах (ЦП или ОЗУ).	

Реализация статической маршрутизации в небольшой сети не представляет сложностей. Статические маршруты остаются неизменными, благодаря чему устранить неполадки, связанные с ними, относительно просто. При статической маршрутизации не требуется рассылка сообщений об обновлениях, поэтому нагрузка на вычислительные ресурсы почти полностью отсутствует.

Динамическая маршрутизация



Динамическая маршрутизация

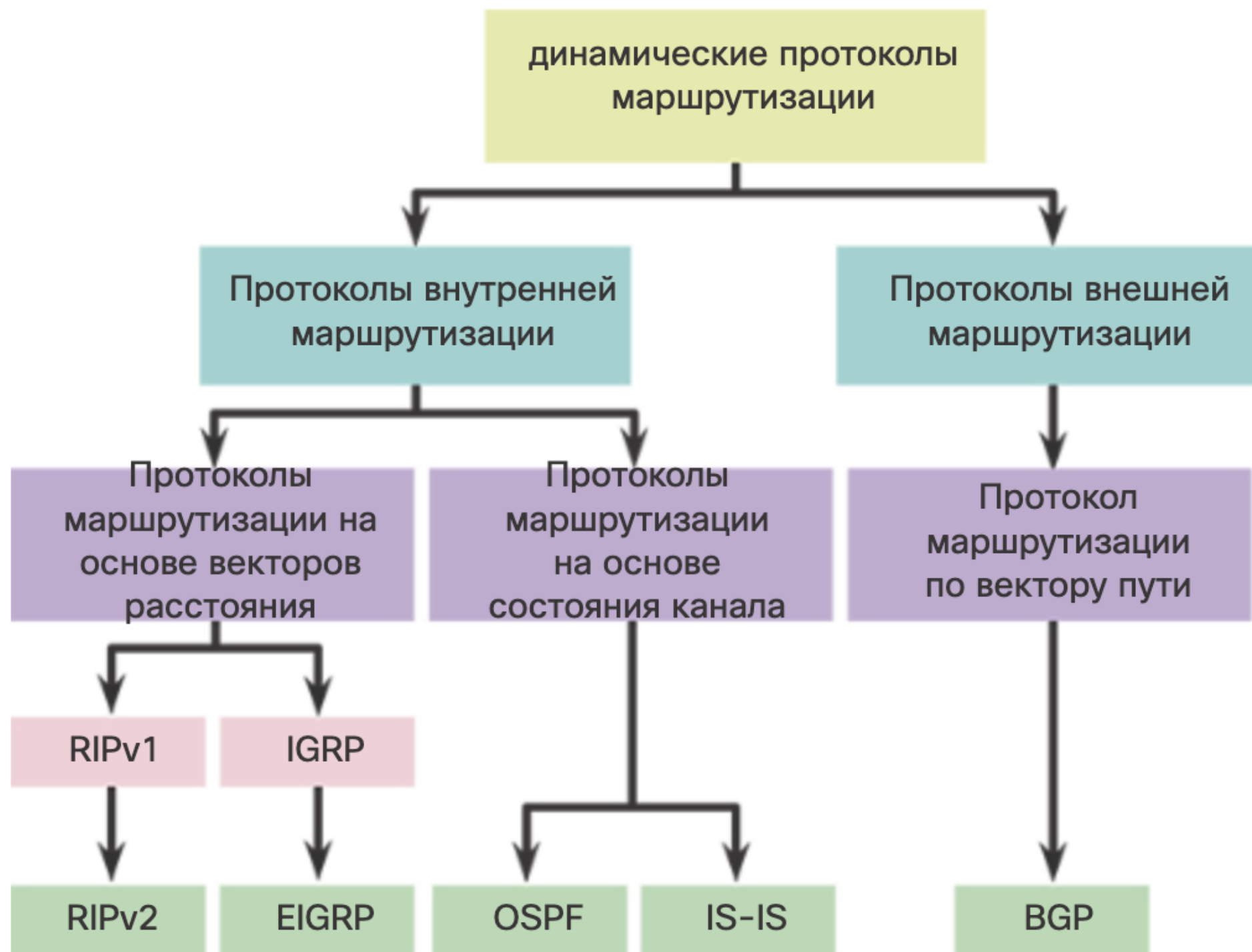


Динамическая маршрутизация

Протокол маршрутизации представляет собой набор процессов, алгоритмов и сообщений, используемых для обмена данными маршрутизации и наполнения таблицы маршрутизации оптимальными путями. Протоколы динамической маршрутизации используются для решения следующих задач:

- обнаружение удаленных сетей;
- обновление данных маршрутизации;
- выбор оптимального пути к сетям назначения;
- поиск нового оптимального пути в случае, если текущий путь недоступен.

Динамическая маршрутизация



Динамическая маршрутизация

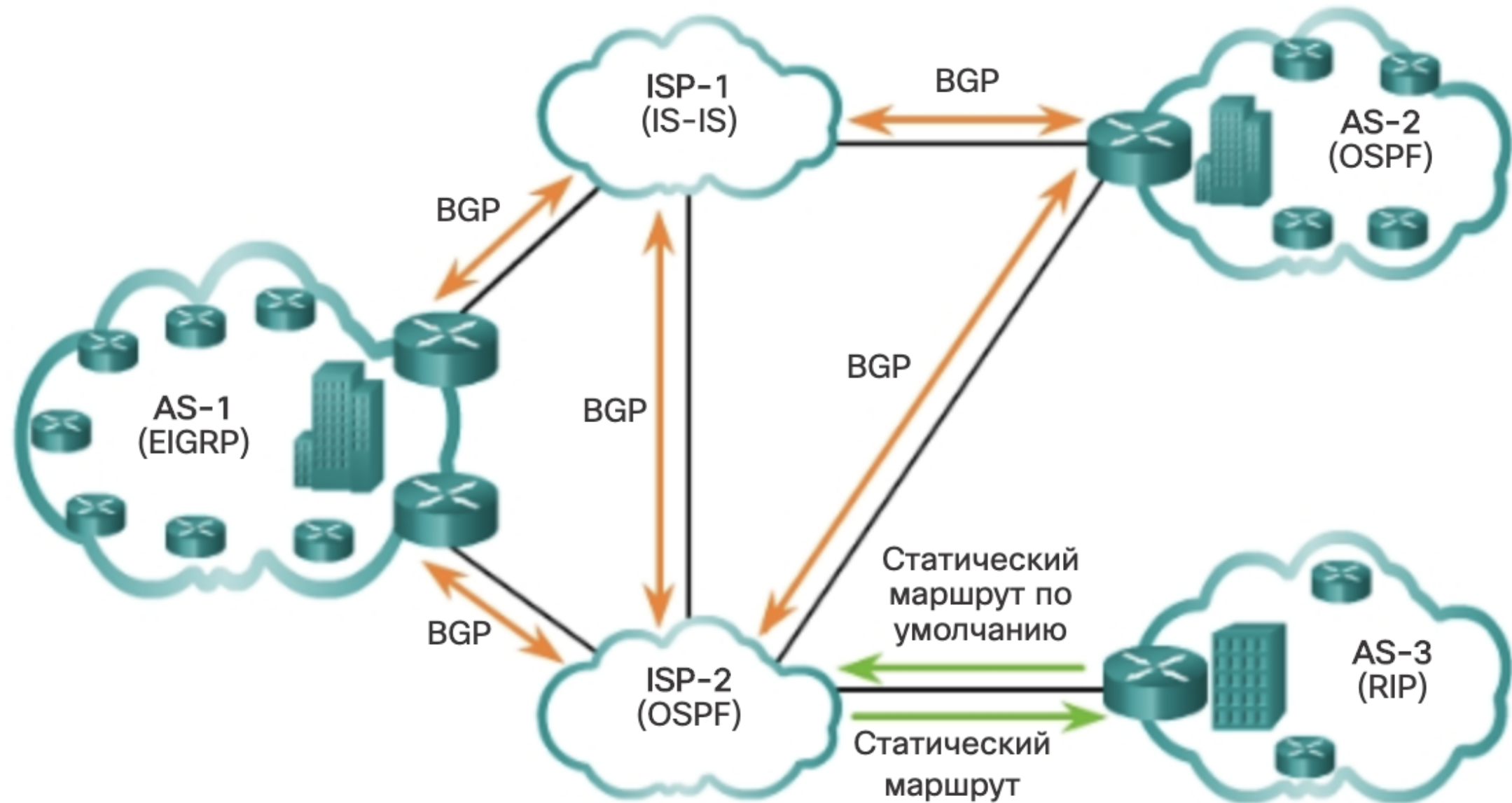
- **RIPv1 (устаревший)** — дистанционно-векторный классовый протокол внутренней маршрутизации;
- **IGRP (устаревший)** — дистанционно-векторный классовый протокол внутренней маршрутизации, разработанный компанией Cisco (не используется после выхода IOS 12.2 и более поздних версий);
- **RIPv2** — бесклассовый протокол вектора расстояния внутренней маршрутизации;
- **EIGRP** — дистанционно-векторный бесклассовый протокол внутренней маршрутизации, разработанный компанией Cisco;
- **OSPF** — бесклассовый протокол внутренней маршрутизации, по состоянию канала;
- **IS-IS** — бесклассовый протокол внутренней маршрутизации, по состоянию канала;
- **BGP** — бесклассовый протокол внешней маршрутизации, по вектору маршрута.

Динамическая маршрутизация

Сеть Интернет основана на концепции автономной системы, в связи с чем она требует протоколы маршрутизации двух типов:

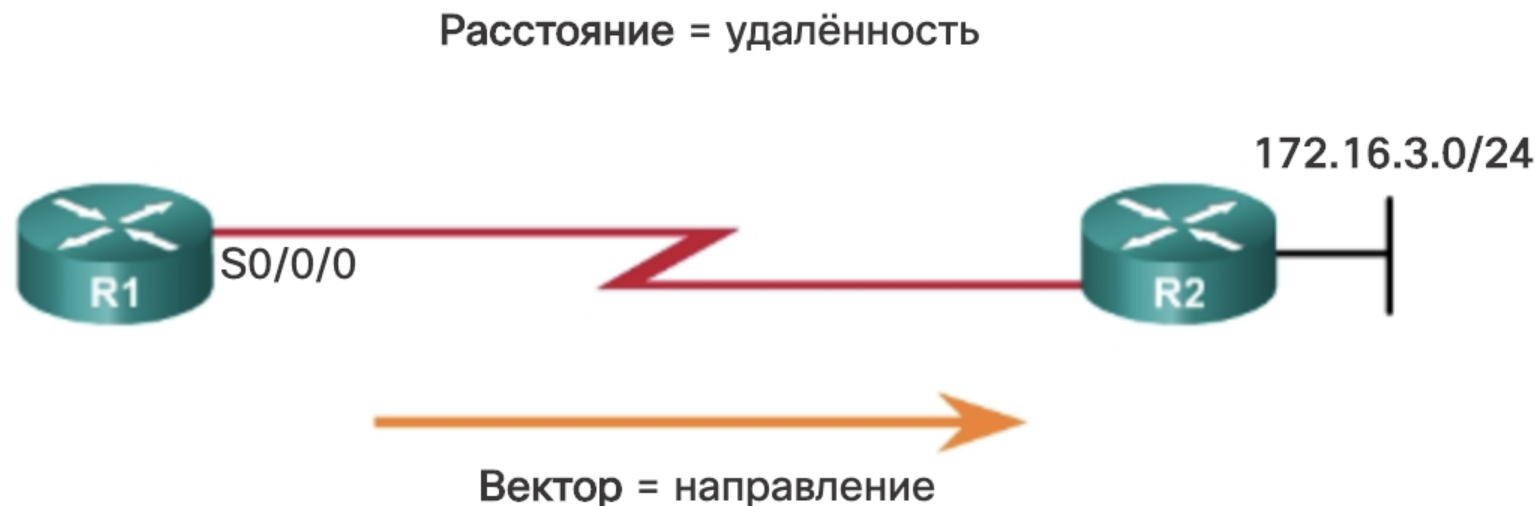
- **Протоколы внутренней маршрутизации**, используемые для маршрутизации внутри автономной системы. Данный тип маршрутизации также называют внутренней маршрутизацией автономной системы. Компании, организации и даже операторы связи используют протоколы внутренней маршрутизации в своих внутренних сетях. К протоколам внутренней маршрутизации относятся протоколы RIP, EIGRP, OSPF и IS-IS.
- **Протоколы внешнего шлюза (EGP)**, используемые для маршрутизации между автономными системами. Маршрутизацию данного типа также называют внешней маршрутизацией автономной системы. Взаимодействие между сетями операторов связи и крупных компаний может осуществляться посредством протокола внешней маршрутизации. Протокол пограничного шлюза (BGP) является единственным в настоящее время официальным протоколом маршрутизации EGP, используемым в Интернете.

Динамическая маршрутизация



Автономная система (AS) представляет собой систему маршрутизаторов, управляемых одним оператором, например компанией или организацией. Автономную систему также называют доменом маршрутизации. К стандартным примерам автономной системы можно отнести внутреннюю сеть компании и сеть интернет-провайдера.

Дистанционно-векторные протоколы маршрутизации



«Дистанционно-векторный» означает, что маршруты объявляются путем указания двух характеристик:

- **Расстояние** — определяет удаленность сети назначения; основывается на таких метриках, как число переходов, стоимость, полоса пропускания, значение задержки и т. д.
- **Вектор** определяет направление маршрутизатора следующего перехода или выходного интерфейса маршрута для доступа к адресу назначения.

В примере на рисунке маршрутизатор R1 располагает данными о том, что расстояние до сети 172.16.3.0/24 равно одному переходу в направлении от интерфейса S0/0/0 к маршрутизатору R2.

Протоколы маршрутизации по состоянию канала



Протоколы маршрутизации по состоянию канала пересылают обновления при изменении состояния канала.

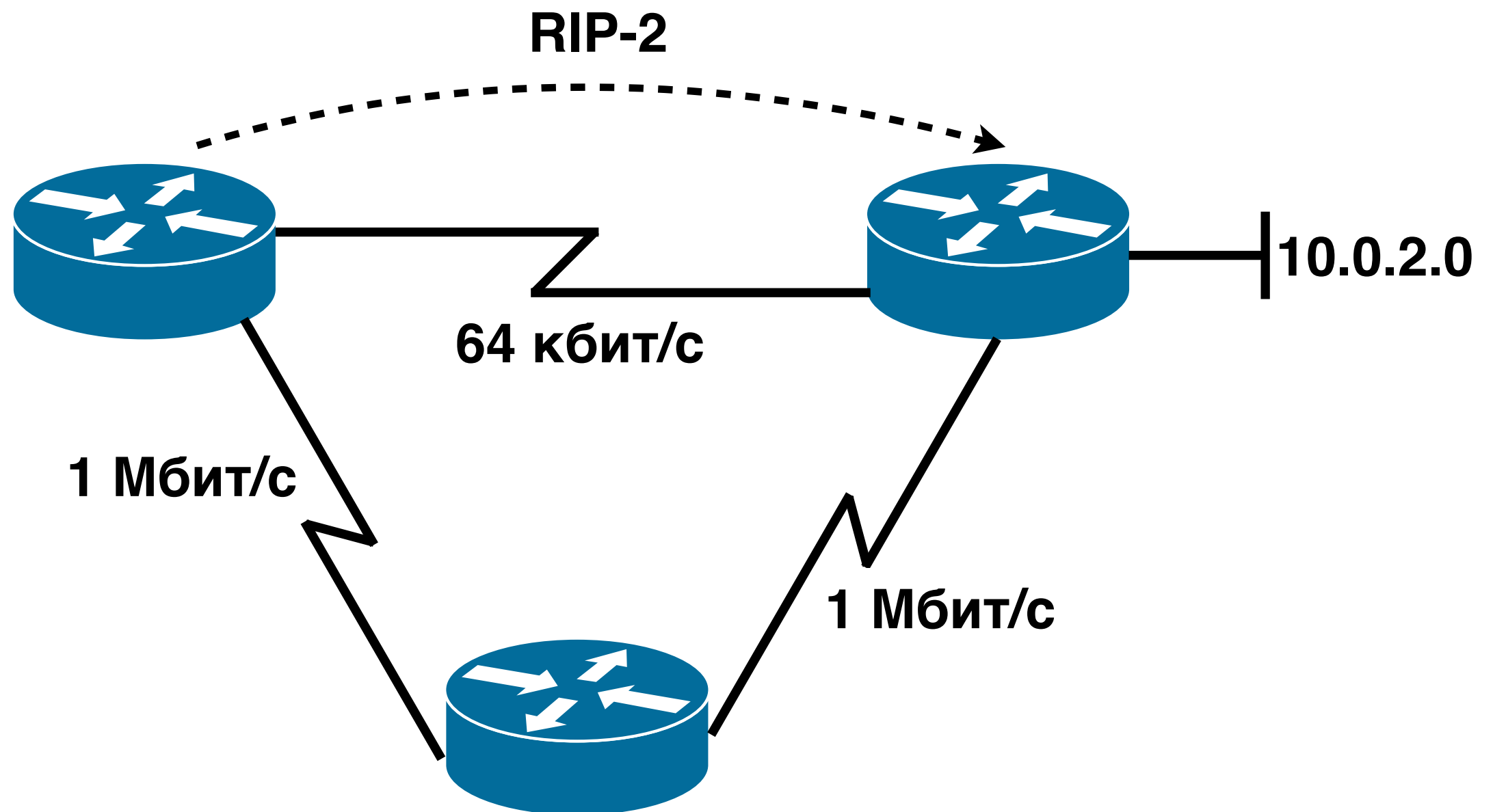
Метрики протоколов маршрутизации

Метрика представляет собой измеряемое значение, которое назначается протоколом маршрутизации различным маршрутам с учетом полезности того или иного маршрута. В ситуациях, когда доступно несколько маршрутов к одной удаленной сети, метрики маршрутизации используются для определения общей «стоимости» пути от источника до места назначения.

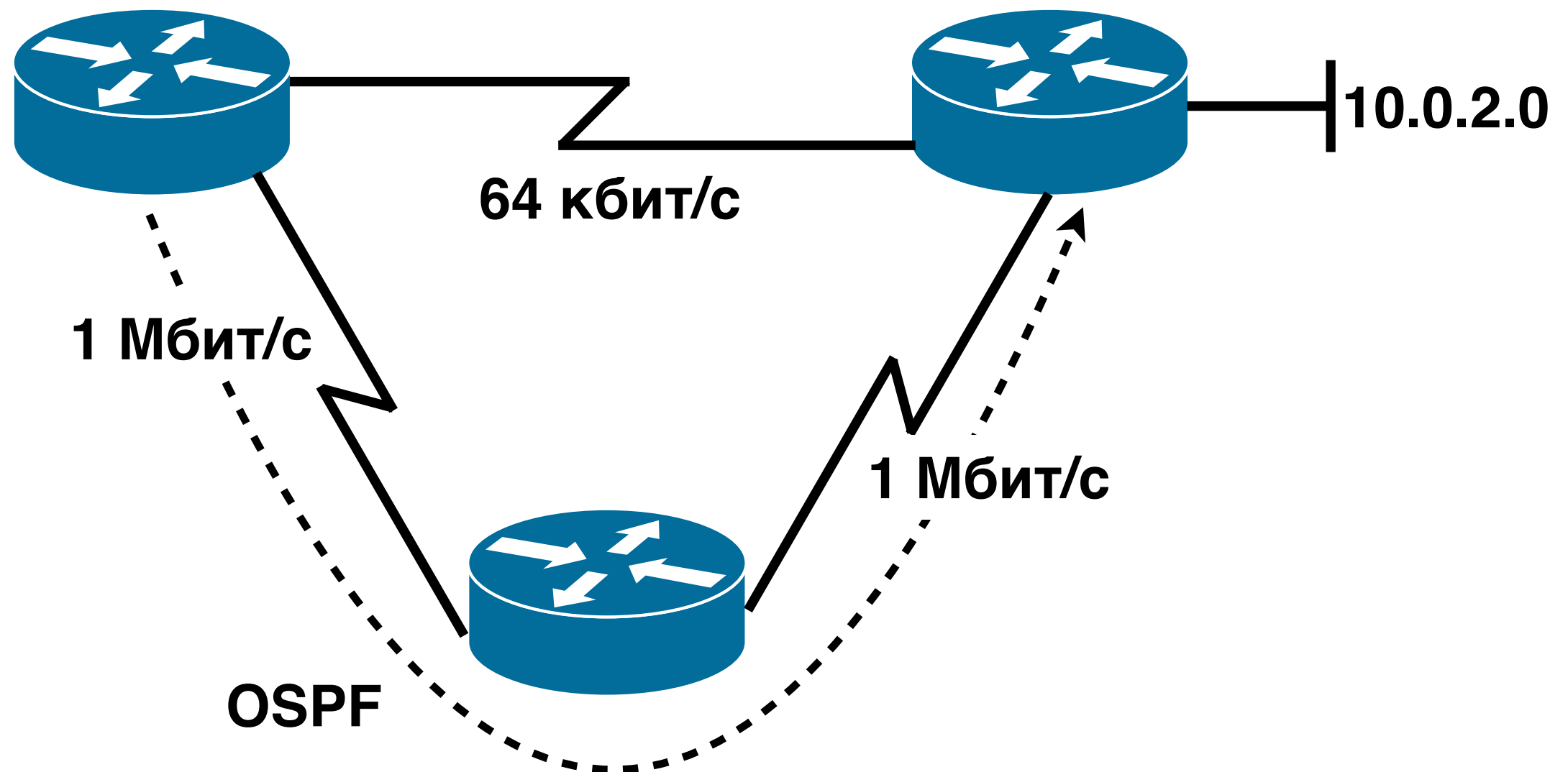
- **Протокол RIP** — количество переходов.
- **Протокол OSPF («алгоритм кратчайшего пути»)** — метрика, основанная на суммарной полосе пропускания от источника до места назначения.
- **Протоколы EIGRP** — минимальная пропускная способность, задержка, нагрузка, надежность и максимальный размер пакета (MTU).

Метрика, используемая одним протоколом маршрутизации, несопоставима с метрикой, используемой другим.

Метрики протоколов маршрутизации



Метрики протоколов маршрутизации



Транспортный уровень

Транспортный уровень ТСР/IP

TCP - *Transmission Control Protocol*

UDP - *User Datagram Protocol*

Транспортный уровень предоставляет транспортные услуги от узла отправителя к узлу получателя. Он поддерживает логическое соединение между конечными точками сетевого маршрута.

Транспортный уровень TCP/IP

UDP



IP-телефония



Видеотрансляция
в реальном
времени

Требования к протоколу:

- Высокая скорость
- Низкие накладные расходы
- Не требуются подтверждения
- Нет повторной отправки потерянных данных
- Обработка данных в том порядке, в каком они были получены

TCP



SMTP/POP
(электронная
почта)



HTTP

Требования к протоколу:

- Надежность
- Подтверждение данных
- Повторная отправка потерянных данных
- Доставка данных в порядке их отправки

Функции протоколов TCP и UDP

Функция	TCP	UDP
Мультиплексирование с использованием портов	✓	✓
Восстановление после ошибок	✓	✗
Управление потоком с использованием окон	✓	✗
Установка и прекращение соединения	✓	✗
Упорядоченная передача данных и их сегментация	✓	✗

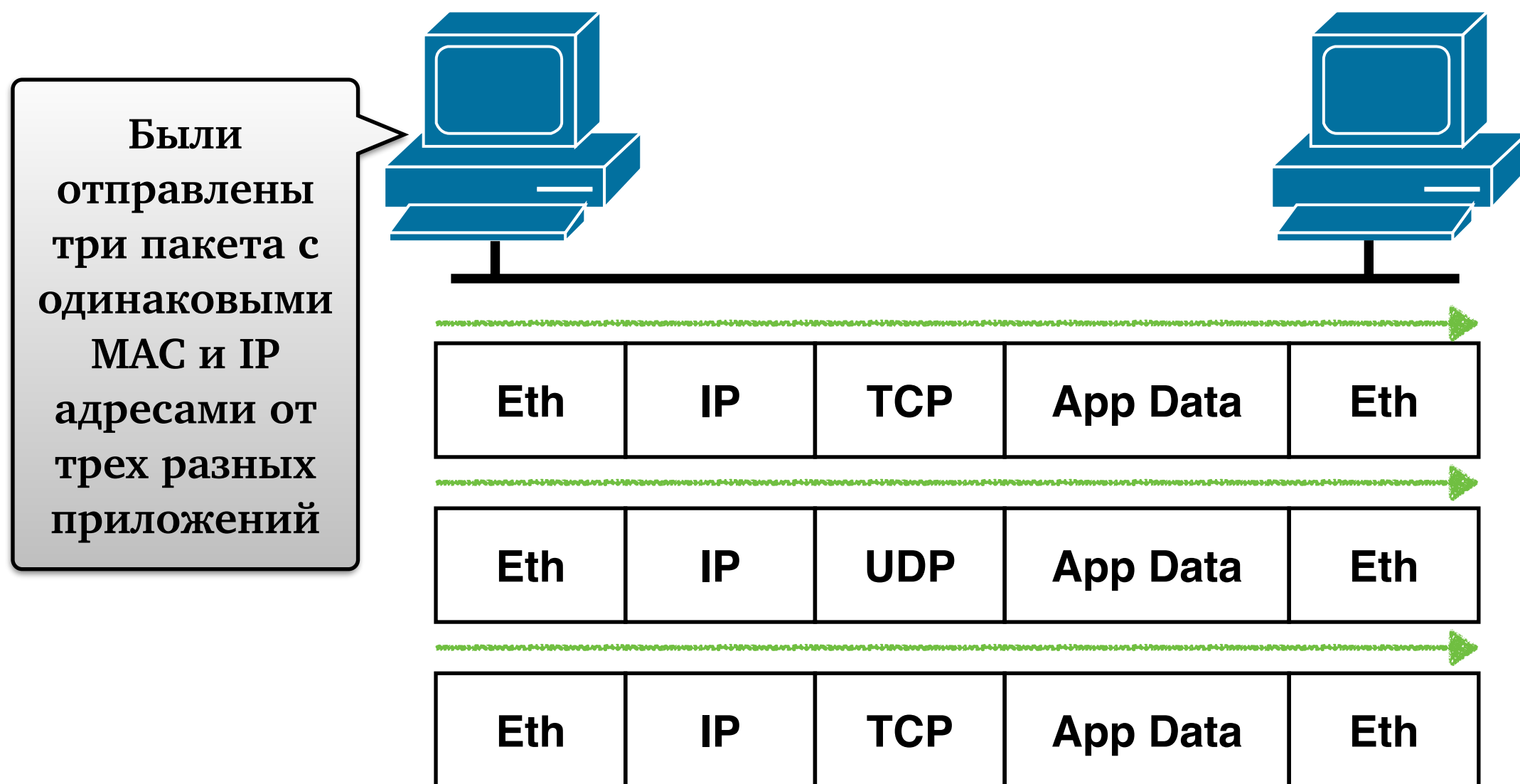
Заголовок TCP-сегмента



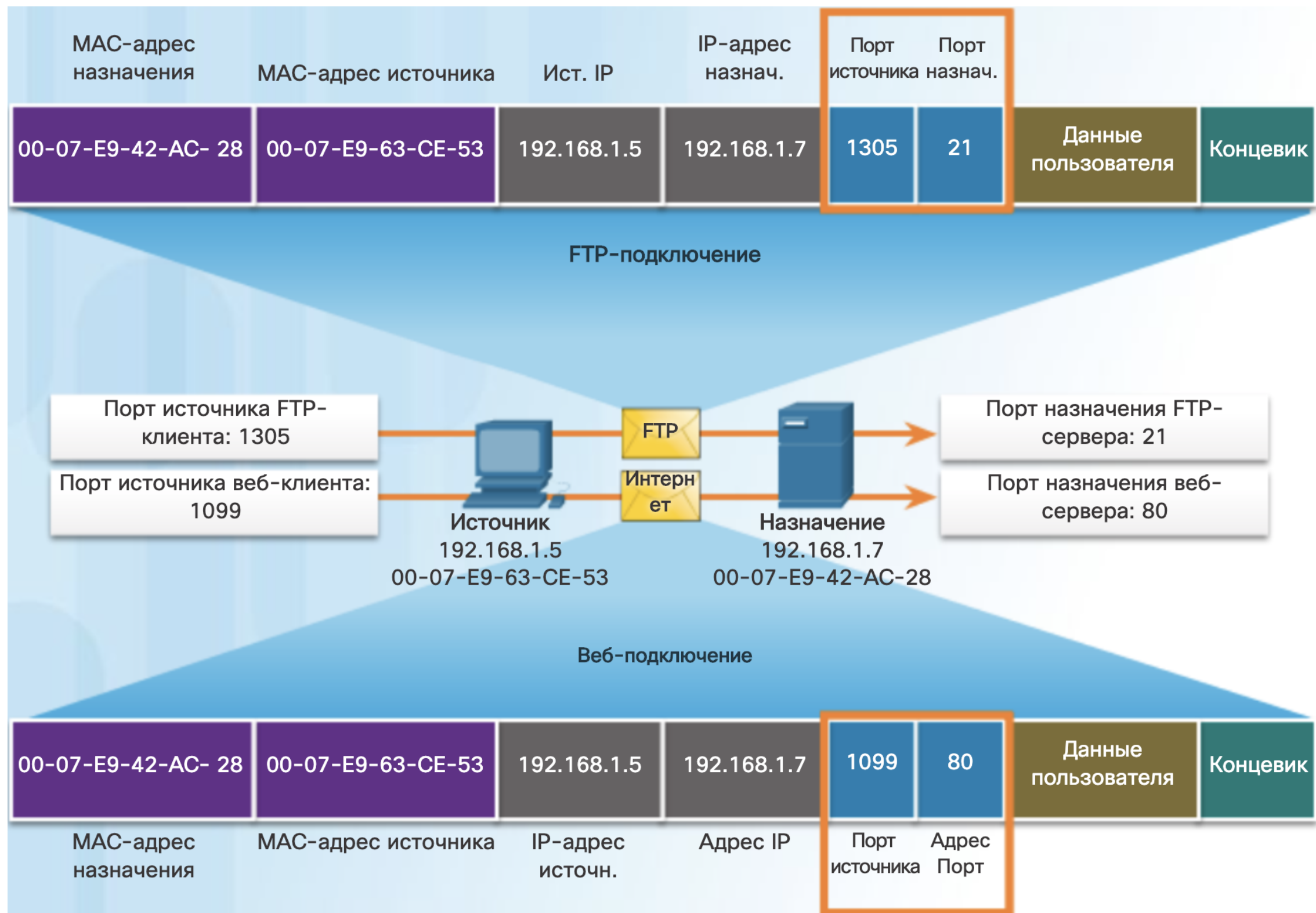
Заголовок UDP-сегмента



Мультиплексирование с использованием портов



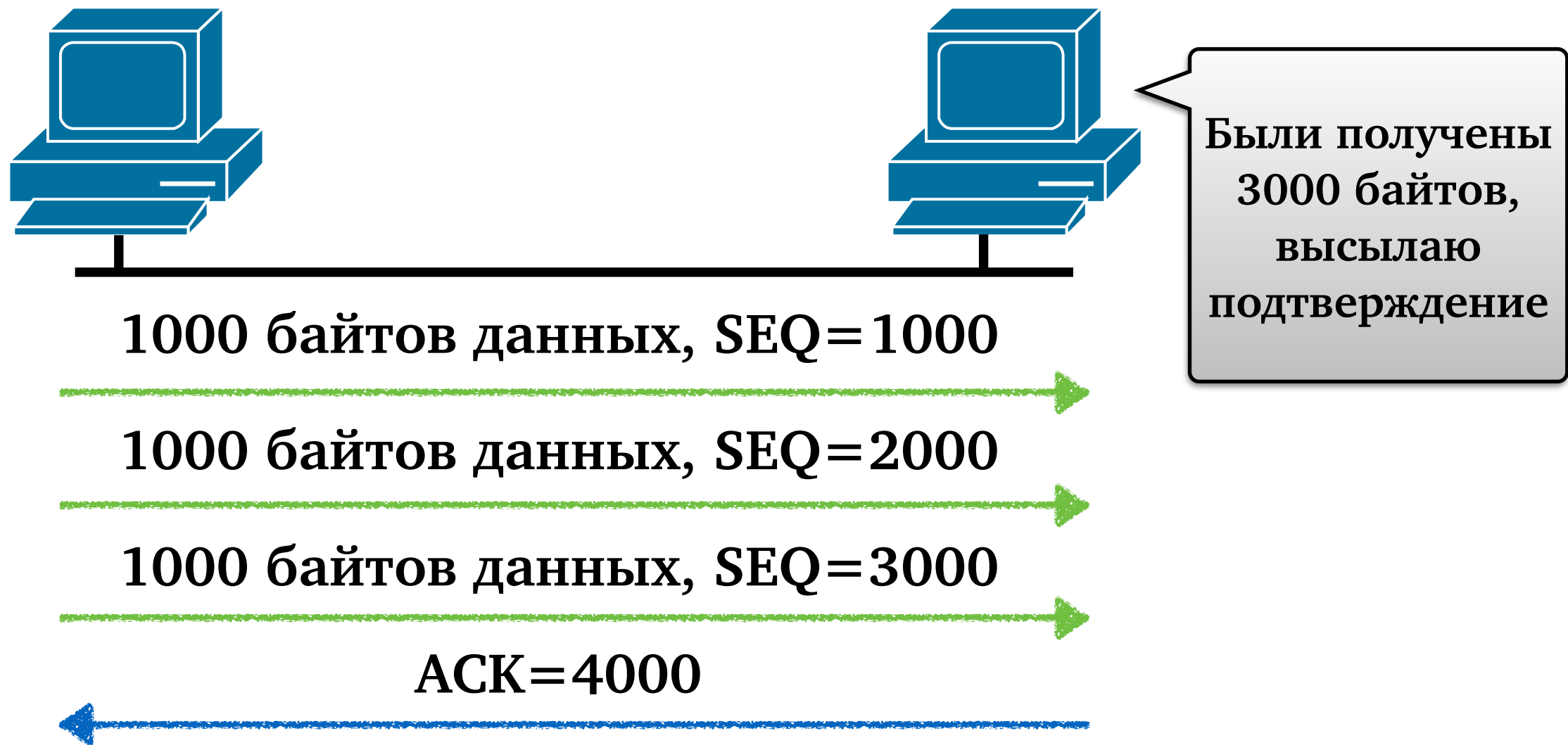
Порты транспортного уровня



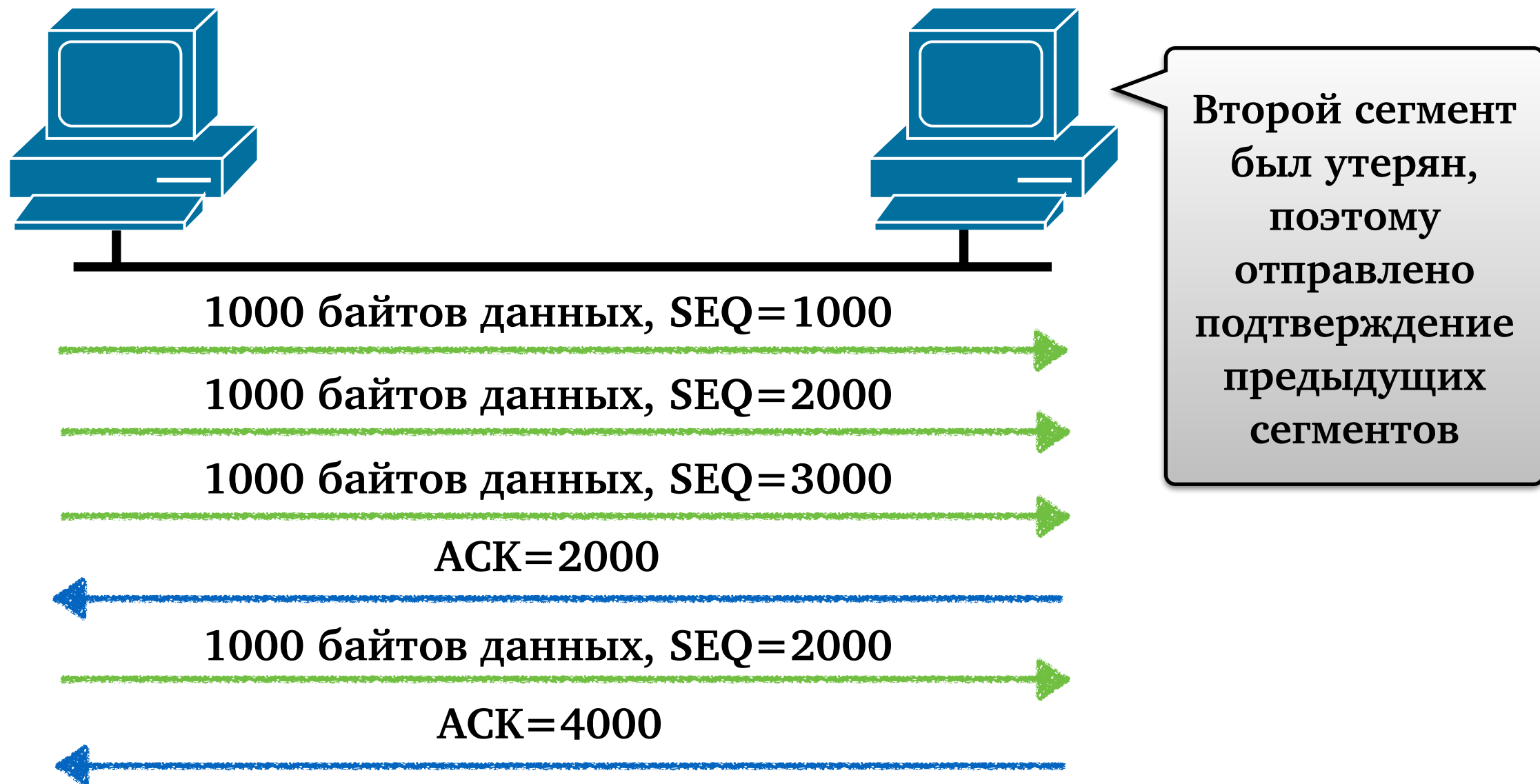
Зарезервированные номера портов

Номер порта	Протокол	Приложение
20	TCP	Данные FTP
21	TCP	Управление FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP, UDP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	UDP	HTTP
110	UDP	POP3
161	UDP	SNMP
443	TCP	SSL

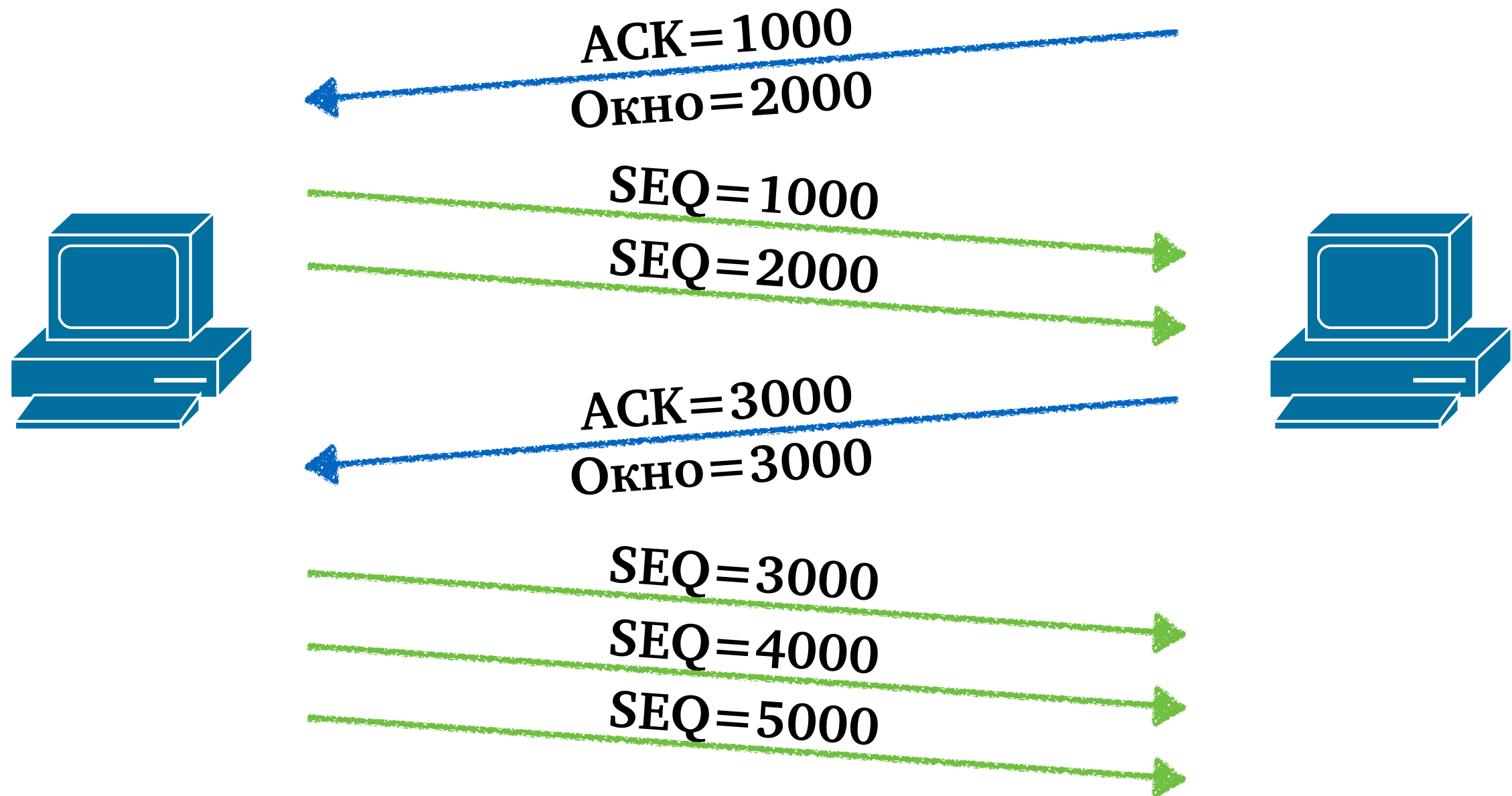
Восстановление данных после ошибок



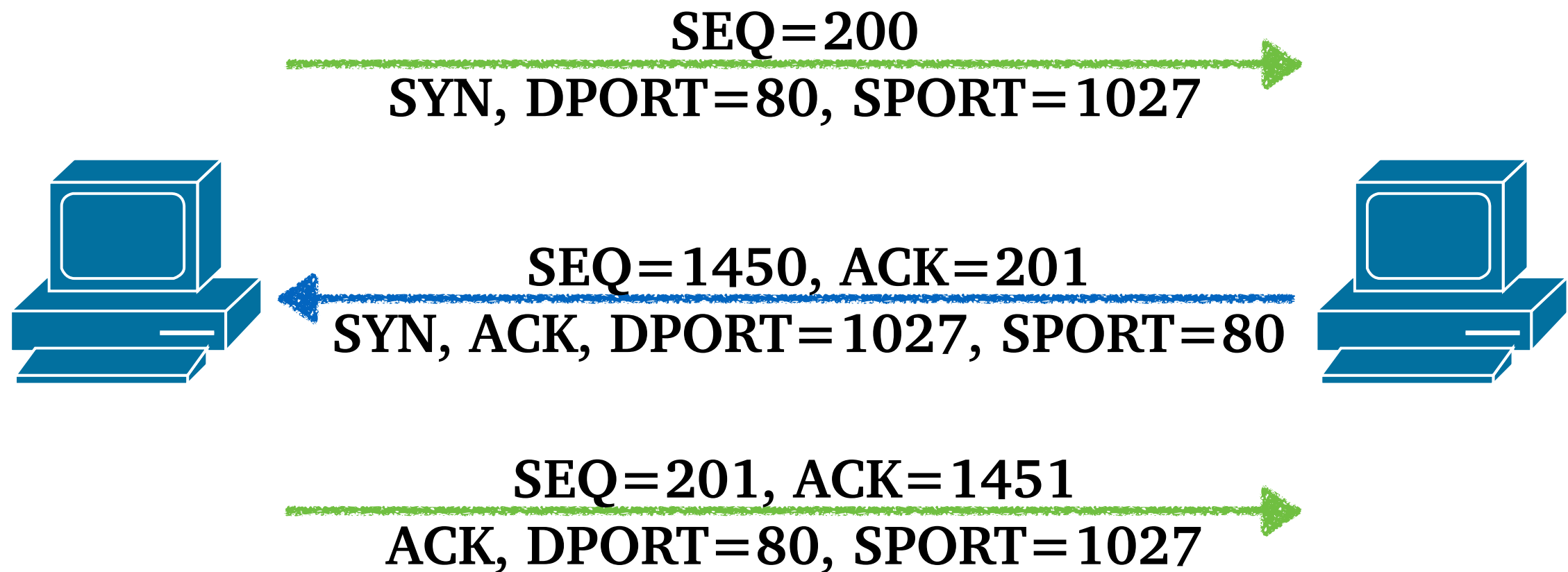
Восстановление данных после ошибок



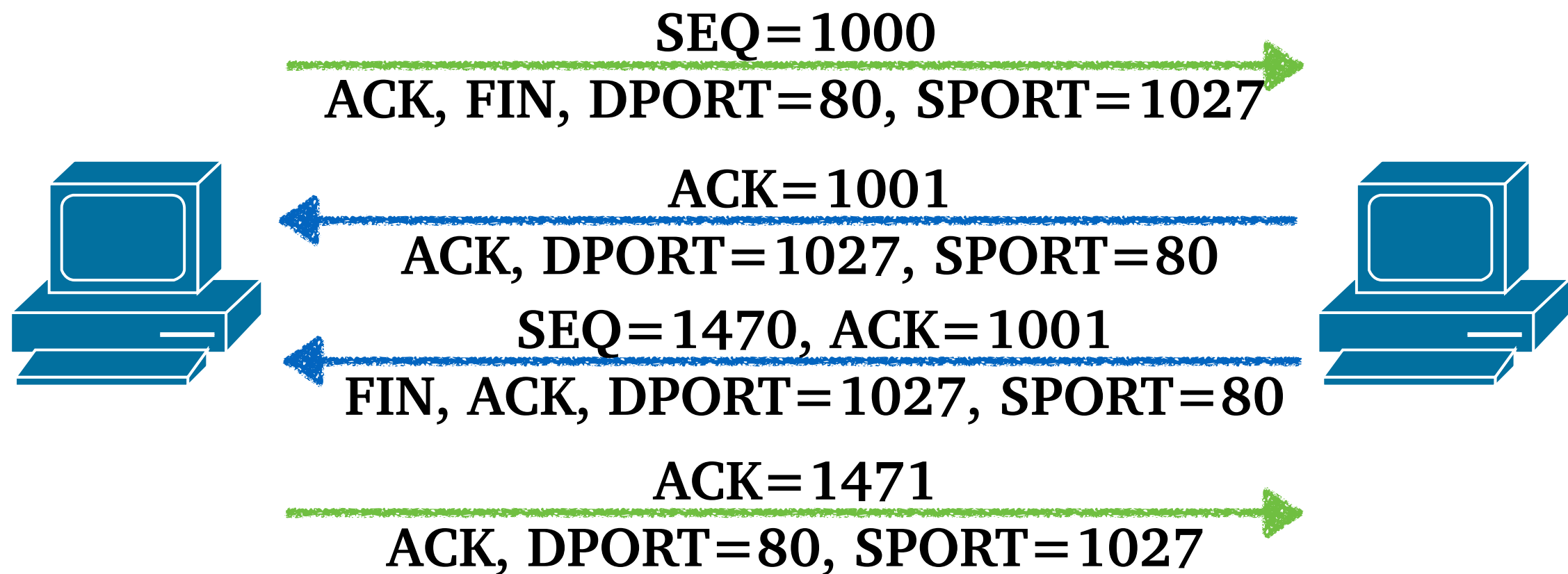
Управление потоком с использованием окон



Установка и разрыв соединения



Установка и разрыв соединения



Сокет

Сокетом называется набор из

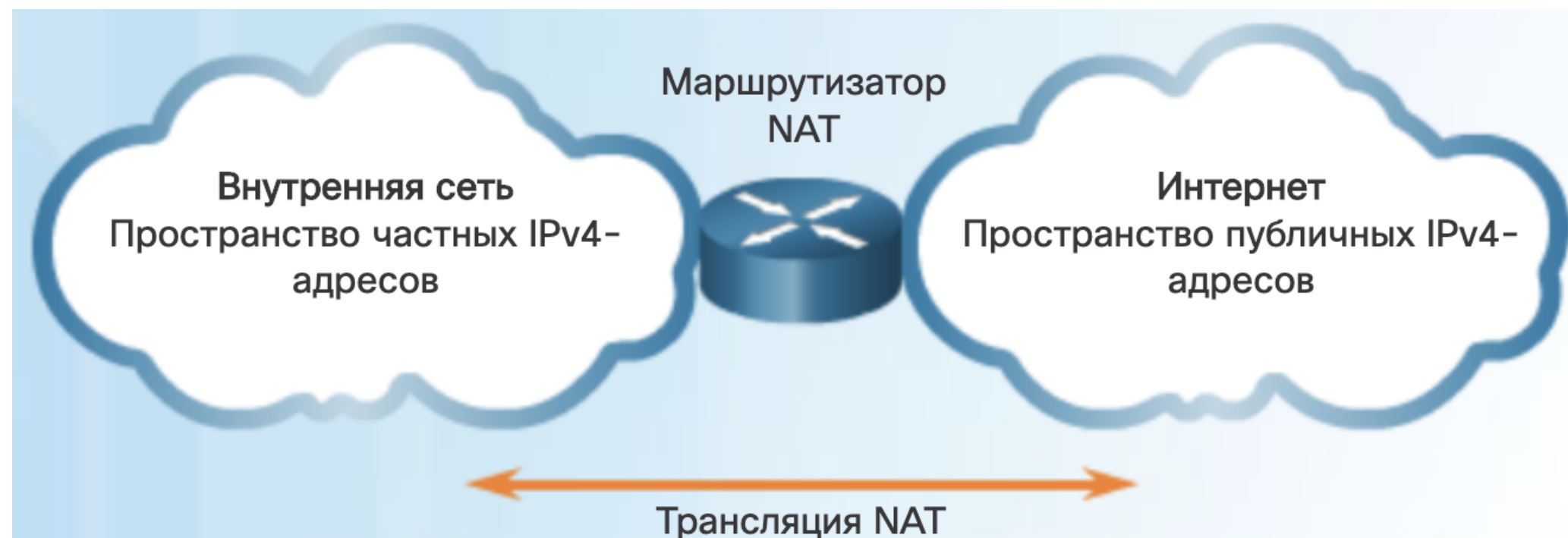
- IP адреса;**
- транспортного протокола;**
- номера порта.**

Сокеты позволяют различать несколько процессов, выполняющихся на клиенте, а также распознавать различные подключения к процессу сервера.

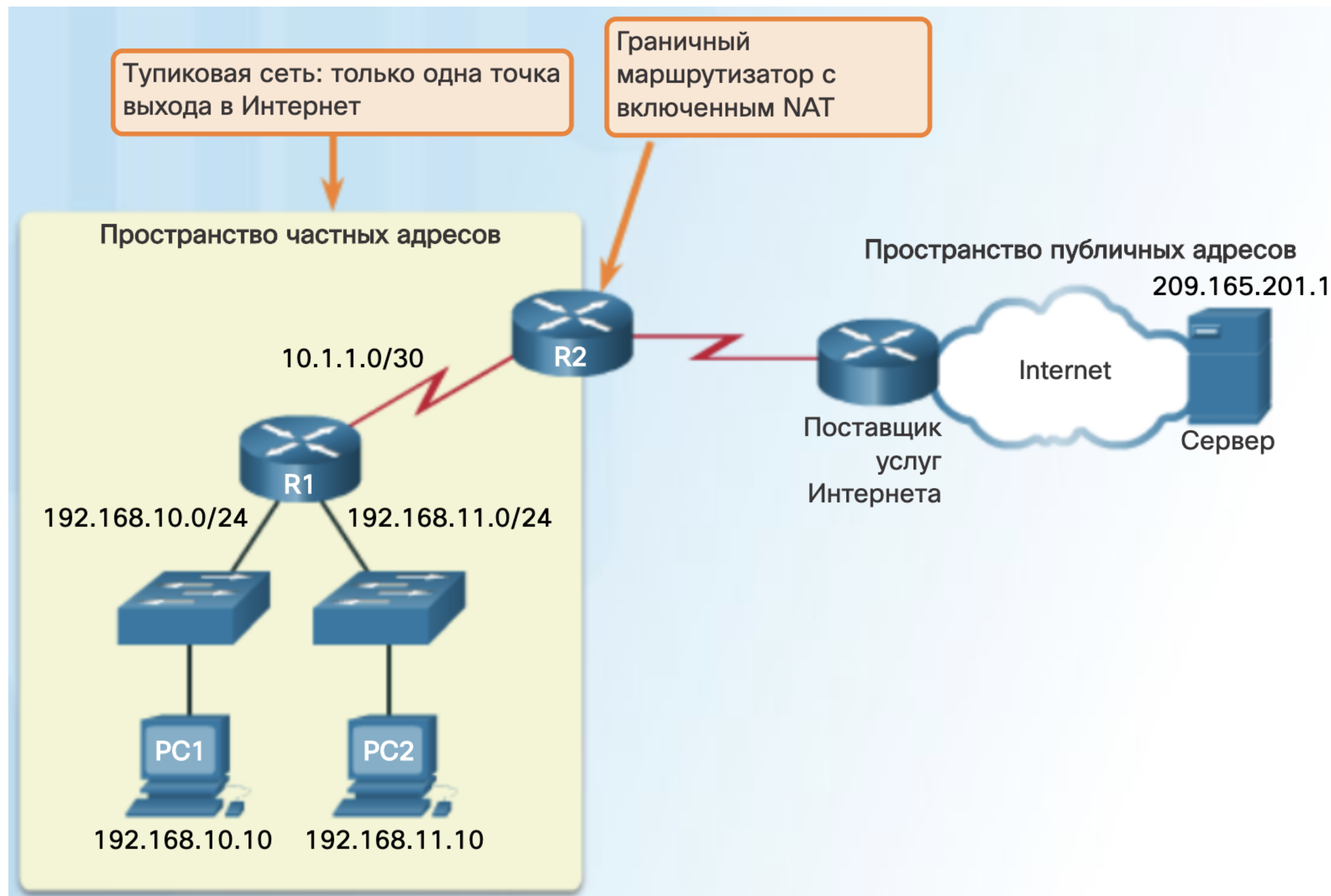
Механизм NAT

Пространство частных IP-адресов

Класс	Диапазон адресов	Префикс
A	10.0.0.0 - 10.255.255.255	/8
B	172.16.0.0 - 172.31.255.255	/16
C	192.168.0.0 - 192.168.255.255	/24



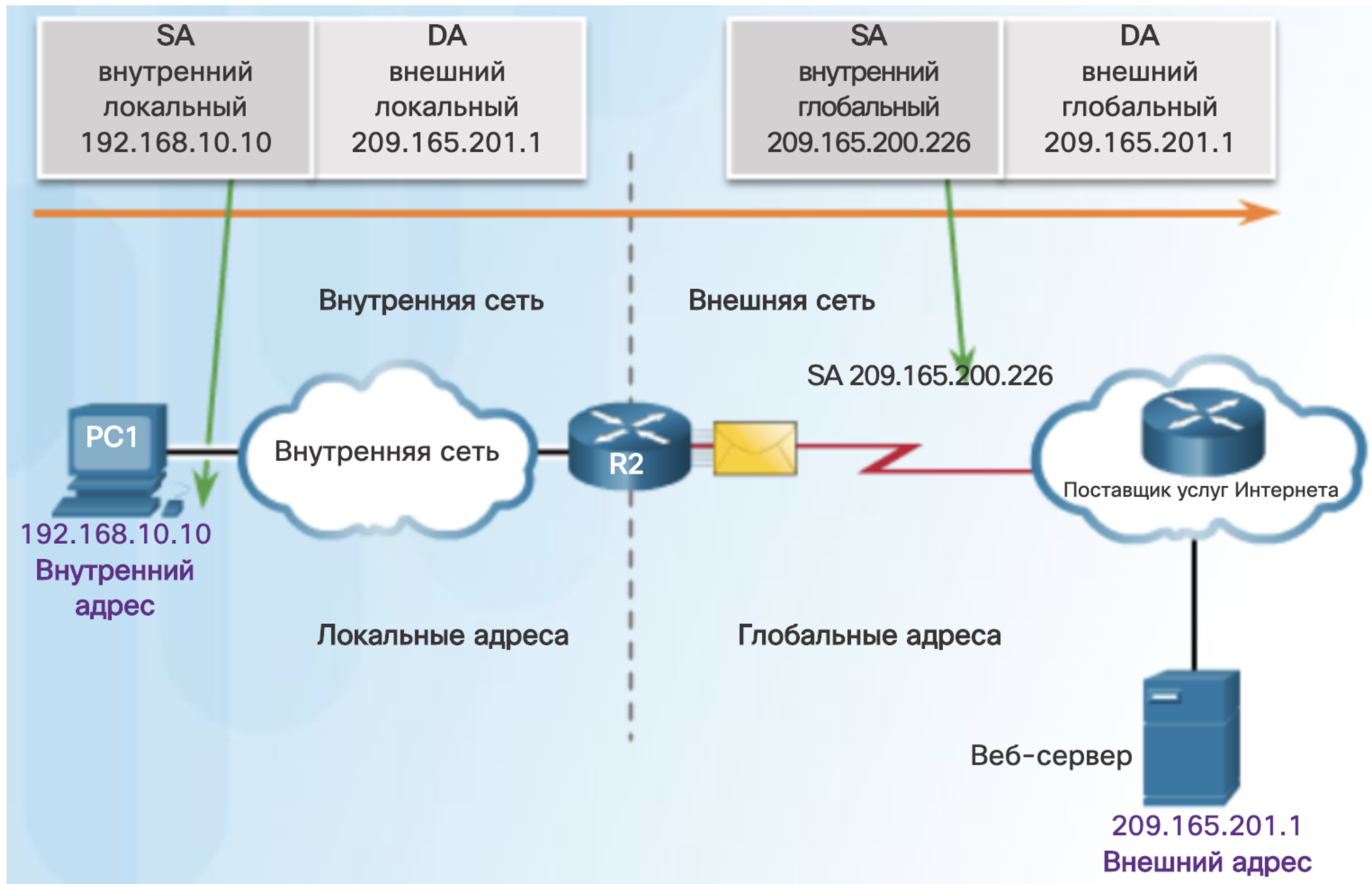
Механизм NAT



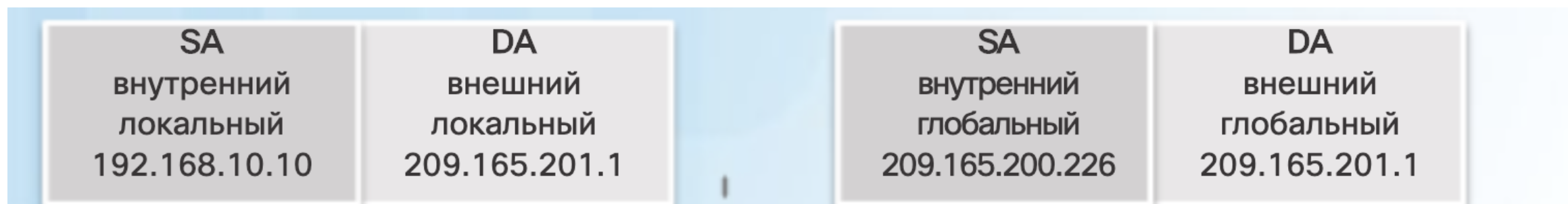
Механизм NAT

Преобразование NAT используется в различных целях, однако основной задачей данного механизма является экономия публичных IPv4-адресов. Это достигается за счет того, что для внутреннего взаимодействия в сетях используются частные IPv4-адреса, а преобразование в публичные адреса происходит только в случае необходимости. Дополнительное преимущество NAT — повышение степени конфиденциальности и безопасности сети — объясняется тем, что данный механизм скрывает внутренние IPv4-адреса от внешних сетей.

Механизм NAT



Механизм NAT



При определении используемого типа адреса важно помнить, что терминология NAT всегда применяется с точки зрения устройства, адрес которого будет транслироваться:

- **Внутренний адрес** — это адрес устройства, преобразуемый механизмом NAT.
- **Внешний адрес** — это адрес устройства назначения.

В рамках NAT по отношению к адресам также используется понятие локальности или глобальности:

- **Локальный адрес** — это любой адрес, появляющийся во внутренней части сети.
- **Глобальный адрес** — это любой адрес, появляющийся во внешней части сети.

Механизм NAT

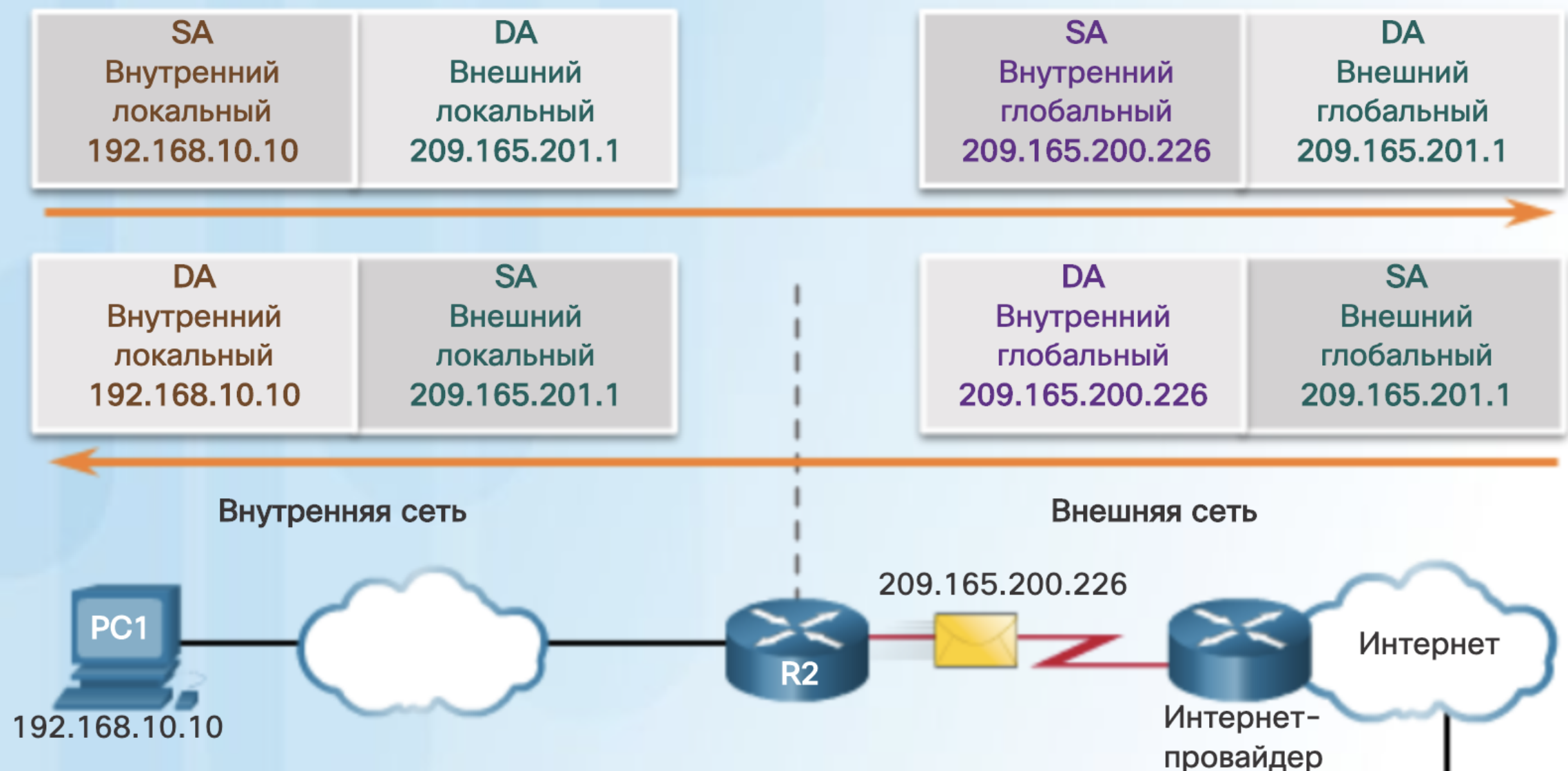


Таблица NAT маршрутизатора R2

PC1		Веб-сервер	
Внутренний глобальный адрес	Внутренний локальный адрес	Внешний локальный адрес	Внешний глобальный адрес
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

Static NAT

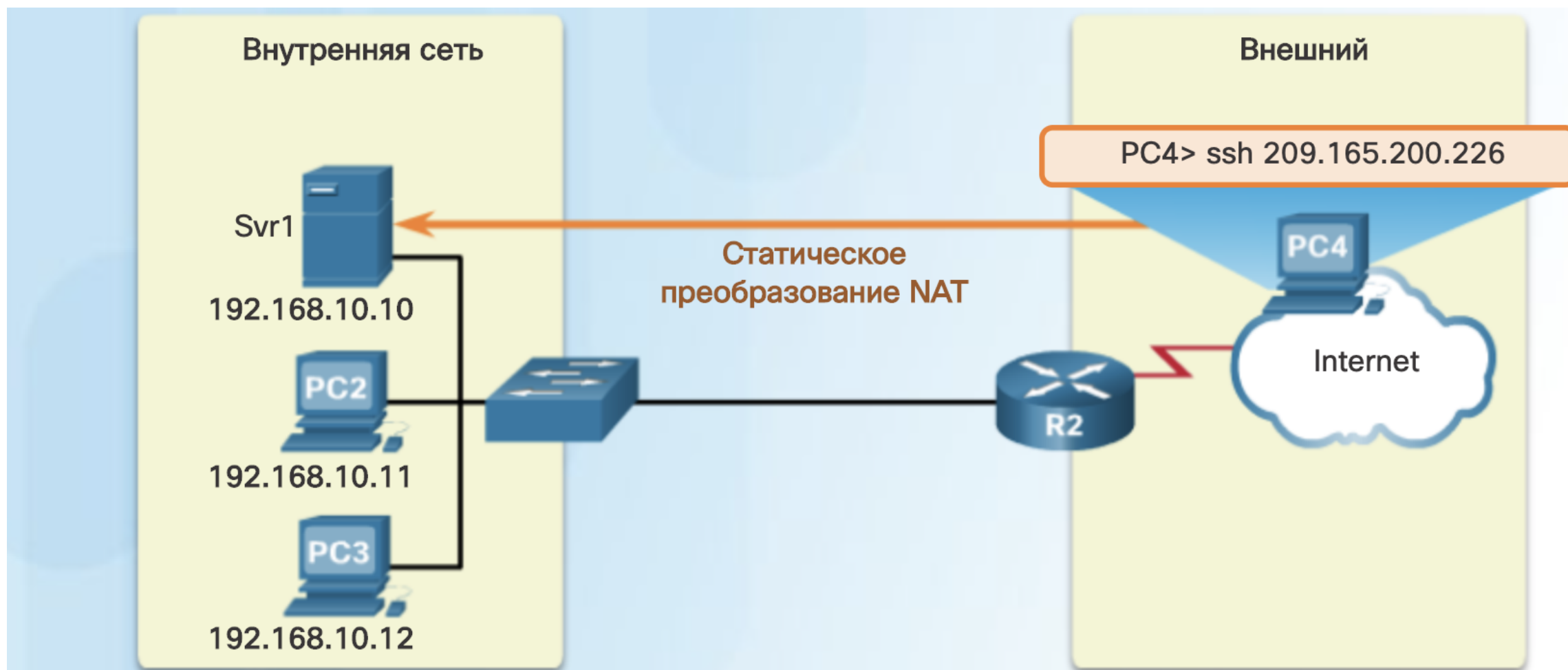
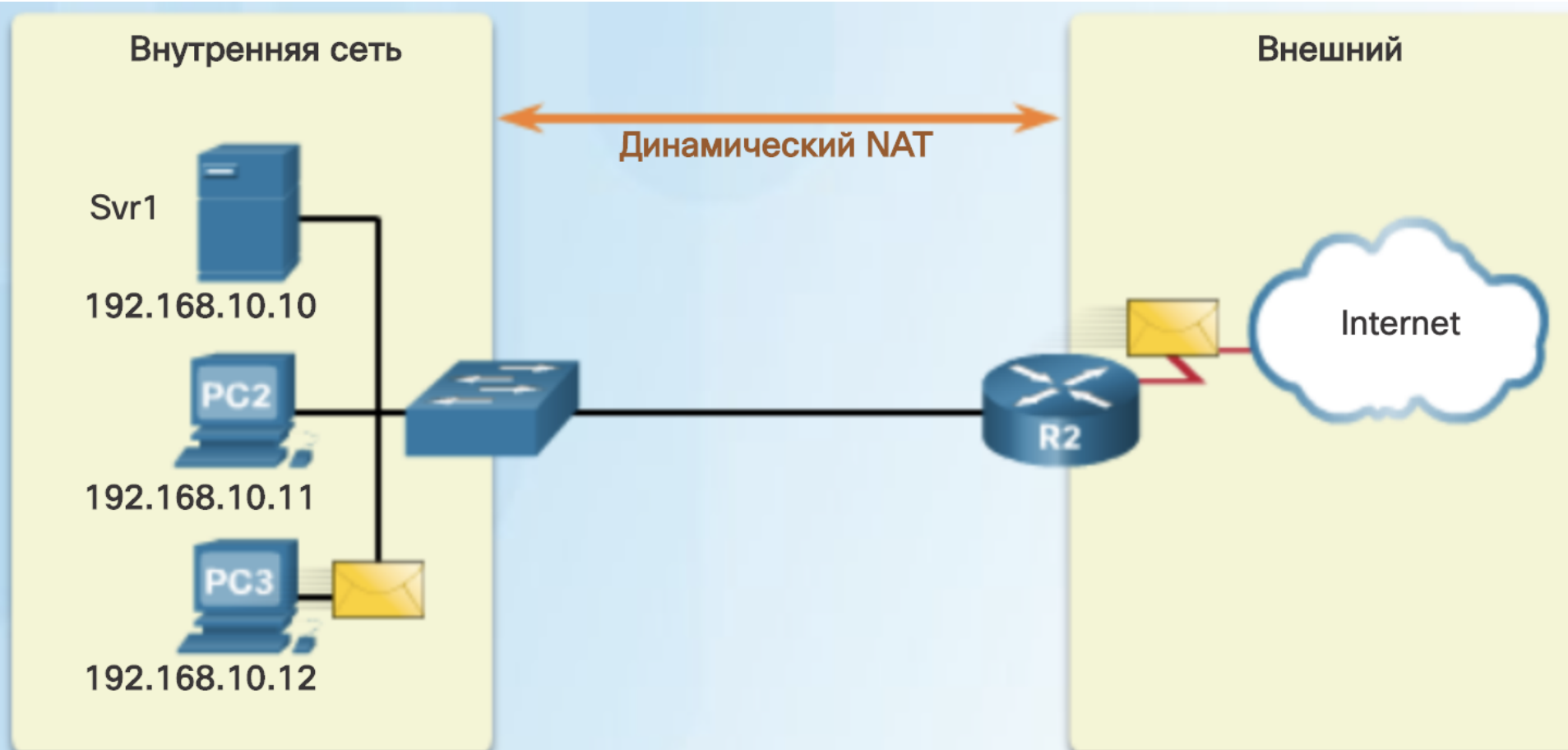


Таблица статических преобразований NAT

Внутренний локальный адрес	Внутренний глобальный адрес – адреса доступны через маршрутизатор R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

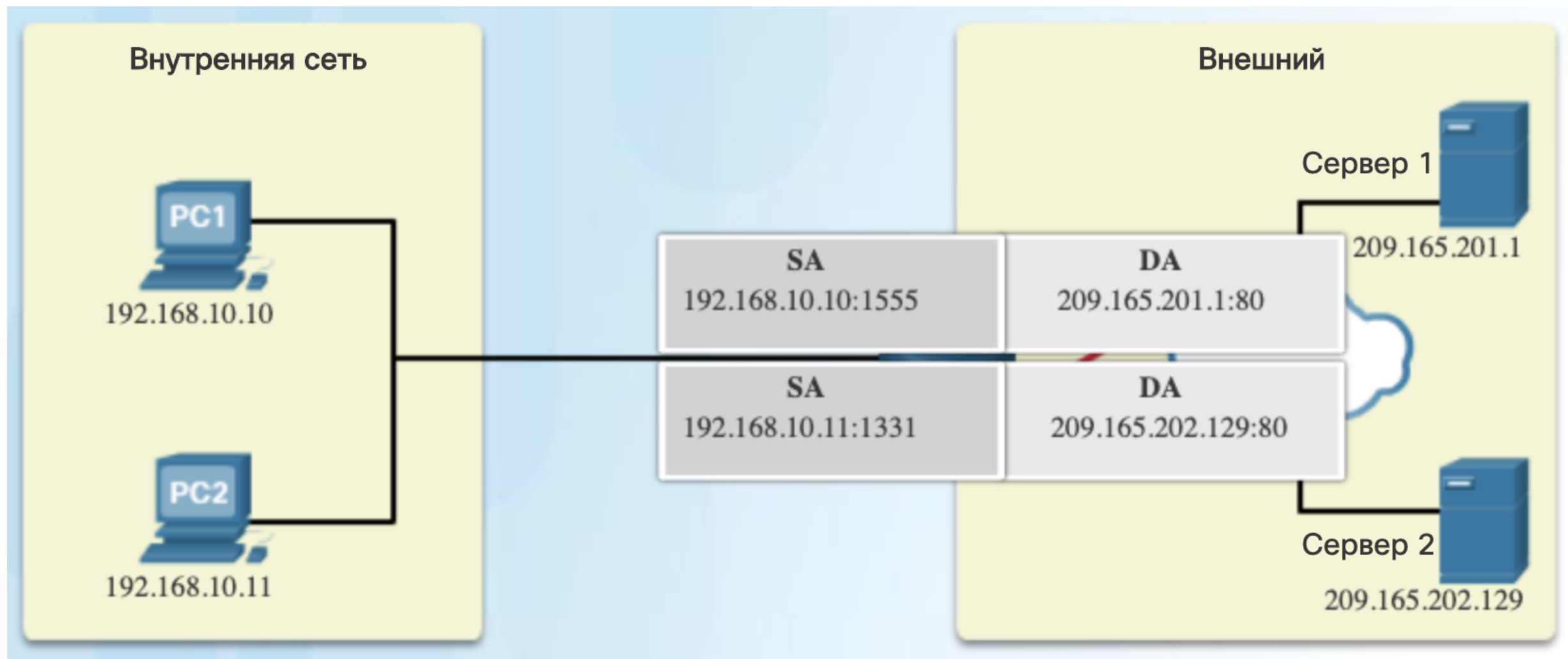
Dynamic NAT



Пул NAT IPv4

Внутренний локальный адрес	Внутренний пул глобальных адресов – адреса доступны через маршрутизатор R2
192.168.10.12	209.165.200.226
Присутствует	209.165.200.227
Присутствует	209.165.200.228
Присутствует	209.165.200.229
Присутствует	209.165.200.230

NAT overload (PAT)



Преобразование адреса и номера порта (PAT), также называемое NAT с перегрузкой, сопоставляет множество частных IPv4-адресов одному или нескольким публичным IPv4-адресам. Так работает большинство домашних маршрутизаторов. Интернет-провайдер назначает один адрес маршрутизатору, при этом еще несколько домашних устройств могут одновременно получать доступ к Интернету. NAT с перегрузкой — это наиболее распространенный метод преобразования.

NAT overload (PAT)

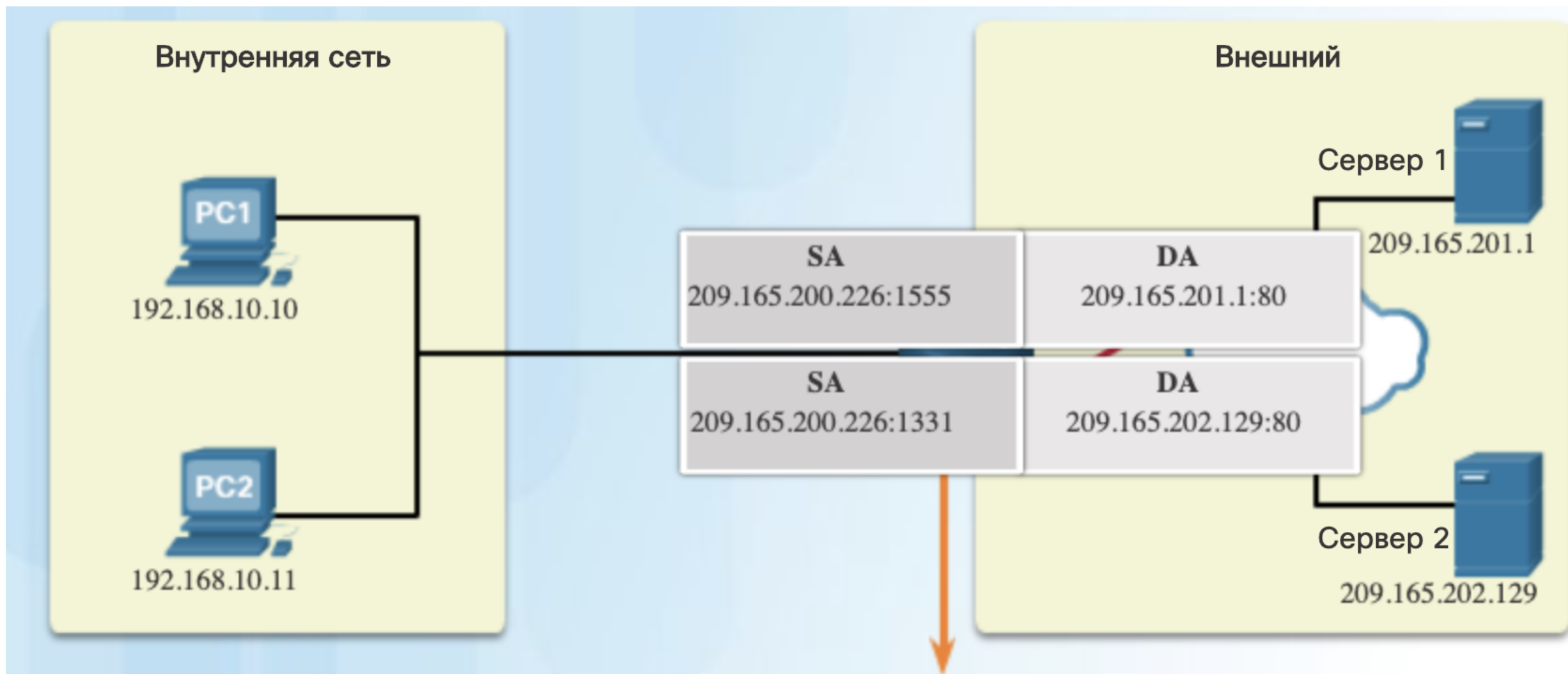
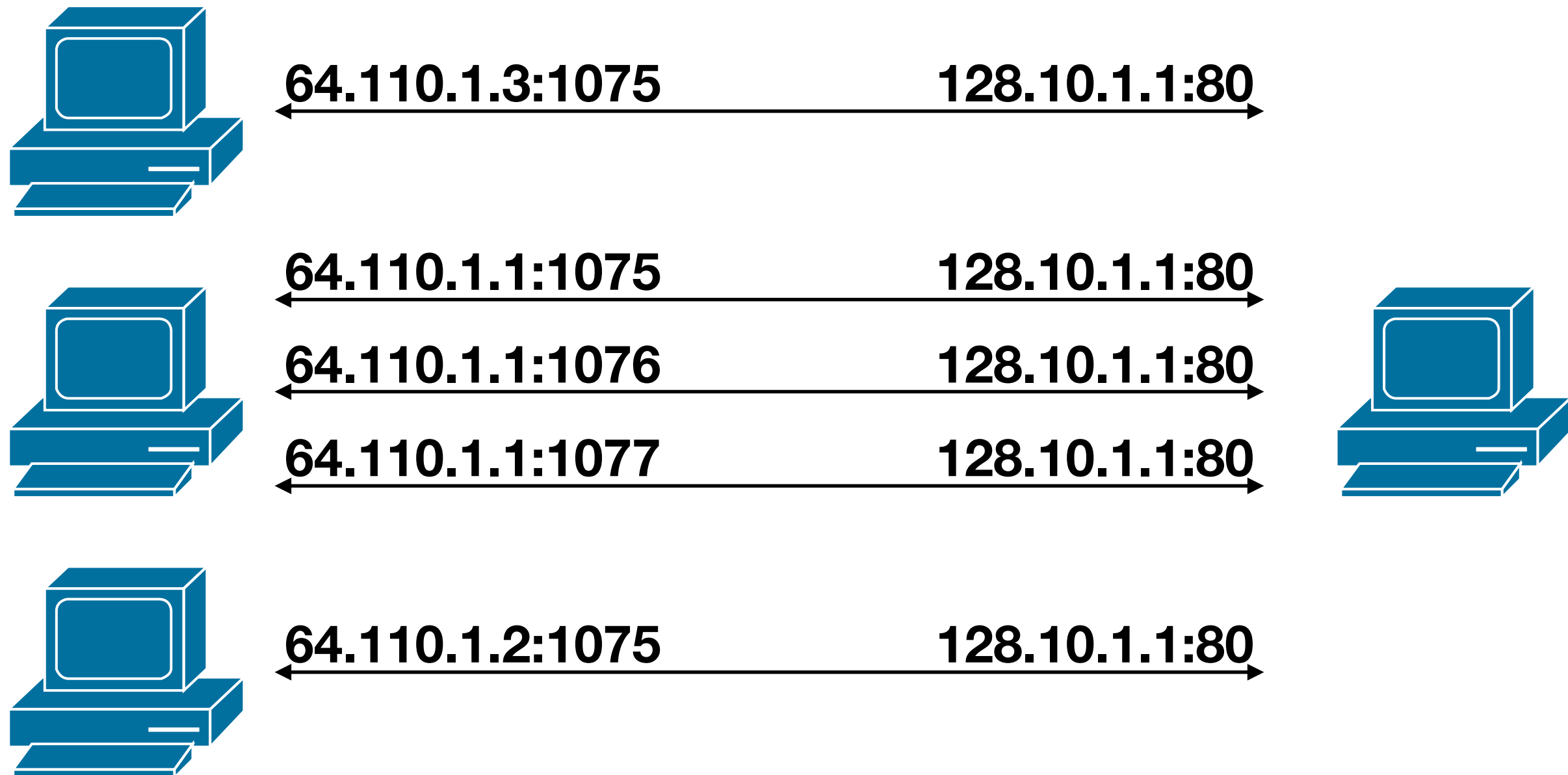


Таблица преобразований NAT с перегрузкой

Внутренний глобальный IP-адрес	Внутренний локальный IP-адрес	Внешний локальный IP-адрес	Внешний глобальный IP-адрес
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Механизм NAT



Преимущества NAT

NAT обеспечивает множество преимуществ, в том числе следующие:

- NAT сохраняет официально зарегистрированную схему адресации, разрешая частное использование внутренних сетей. NAT экономит адреса благодаря мультиплексированию приложений на уровне портов.
- NAT повышает гибкость подключений к публичной сети.
- NAT обеспечивает постоянство схем внутренней сетевой адресации.
- NAT скрывает IPv4-адреса конечного пользователя.

Основы сетевой безопасности

ОСНОВЫ сетевой безопасности

Концепции безопасности:

Конфиденциальность - подразумевает, что только уполномоченные лица/системы могут просматривать конфиденциальную или секретную информацию

Целостность данных означает, что изменения, вносимые в данные, вносятся только уполномоченными лицами / системами

Доступность - если сеть или ее данные недоступны для авторизованных пользователей, это может оказать влияние на компании и пользователей, которые полагаются на сеть как на инструмент бизнеса

VPN

VPN - Virtual Private Network

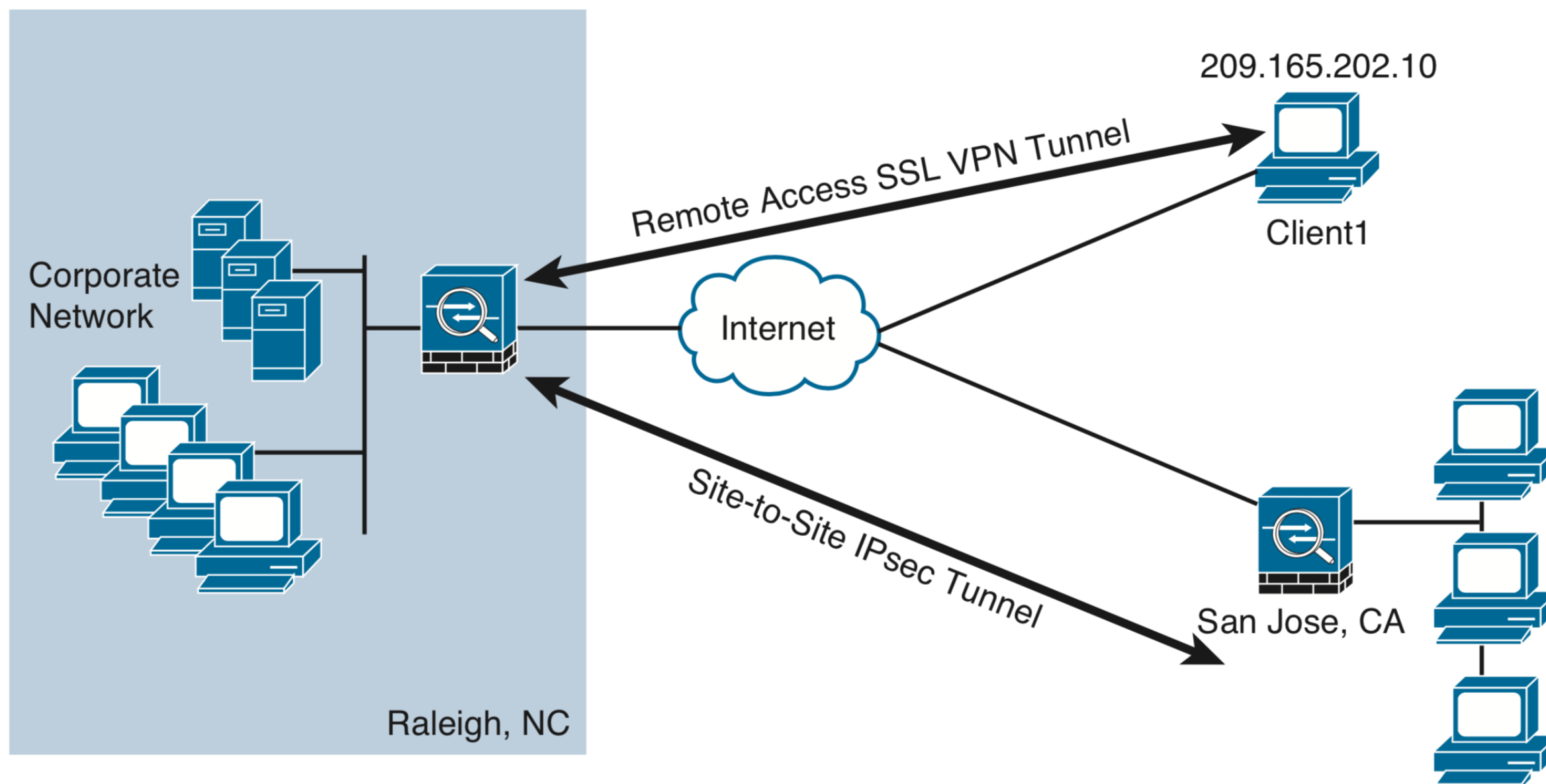
Network подразумевает соединение между двумя удаленными устройствами, **Virtual** - что это соединение логическое, а **Private** - что это соединение не публичное, подразумевает авторизацию.

Преимущества VPN: конфиденциальность, целостность данных, аутентификация, защита от повторов.

Технологии VPN:

IPSec, SSL, MPLS

Топология VPN



Remote Access VPN применяется в случае подключения клиента к сети

Site-to-site VPN - в случае организации канала между двумя сетями

VPN

Конфиденциальность VPN обеспечивается отправителем сообщения, который выполняет шифрование пакета перед отправкой.

Шифр - алгоритм и/или формула для кодирования данных, они общеизвестны.

Ключ - параметр для алгоритма (шифра), которая и делает сообщение секретным.

Целостность данных обеспечивается хэшированием - это процесс подсчета хэш-суммы всего отправляемого пакета и добавление ее к отправляемой информации.

Если злоумышленник внедряет биты или данные в пакеты сеанса VPN, целостность данных может пострадать, если изменение данных останется незамеченным.

VPN

Возможность проверки или аутентификации устройства, к которому вы подключены, является важным аспектом VPN. Вы можете аутентифицировать одноранговый узел на другом конце VPN-туннеля несколькими различными способами:

- **PSK (PreShared Keys) - предварительно сгенерированные ключи, используемые только для аутентификации**
- **PKI (Public Key Infrastructure) - пары открытого и закрытого ключей, используемые только для аутентификации**
- **Аутентификация пользователя (в сочетании с VPN с удаленным доступом)**

Основные компоненты криптографии

Шифр - это набор правил, алгоритм, показывающий, как можно выполнить шифрование или дешифрование данных.

Блочный шифр использует симметричный ключ и работает с группой байтов - блоком:

- Advanced Encryption Standard (AES)
- Triple Digital Encryption Standard (3DES)
- Blowfish
- Digital Encryption Standard (DES)
- International Data Encryption Algorithm (IDEA)

Потоковый шифр использует симметричный ключ для побитового шифрования данных. Поскольку поток шифров не ограничен размером блока, издержки могут быть немного меньше, чем у блочного шифра, который требует заполнения для завершения размера блока.

Основные компоненты криптографии

Алгоритм симметричного шифрования использует один и тот же ключ для шифрования и дешифрования данных. Типичные примеры таких алгоритмов: DES, 3DES, AES, IDEA, RC2, RC4, RC5, RC6, Blowfish.

Симметричные алгоритмы быстрее и требуют меньше вычислительных ресурсов, поэтому они применяются чаще.

Основные компоненты криптографии

Примером асимметричного алгоритма является использование открытого и закрытого ключа, когда данные шифруются закрытым ключом, а расшифрованы могут быть открытым ключом на другой стороне. Таким образом, закрытый ключ никогда не передается, и вероятность, что он будет скомпрометирован, гораздо меньше.

При использовании пар ключей высока нагрузка на процессор, поэтому асимметричные алгоритмы применяются редко.

Они используются для аутентификации партнера и защищенной передаче ключей симметричного алгоритма.

Основные компоненты криптографии

Примеры асимметричных алгоритмов:

RSA: назван в честь Ривеста, Шамира и Адлемана, которые создали алгоритм. В основном применяется для аутентификации. Также известен как (PKCS) # 1. Длина ключа может составлять от 512 до 2048, а минимальный размер для обеспечения безопасности - не менее 1024.

DH: протокол обмена ключами Диффи-Хеллмана. DH - это асимметричный алгоритм, который позволяет двум устройствам согласовывать и устанавливать общий секретный ключ (ключи) по ненадежной сети. Интересная особенность DH состоит в том, что, хотя сам алгоритм является асимметричным, ключи, сгенерированные обменом, являются симметричными ключами, которые затем могут использоваться с симметричными алгоритмами.

Основные компоненты криптографии

Хеширование - это метод, используемый для проверки целостности данных. Криптографическая хеш-функция - это процесс, который принимает блок данных и создает небольшое хеш-значение фиксированного размера. Это односторонняя функция, означающая, что если два разных компьютера берут одинаковые данные и запускают одну и ту же хеш-функцию, они должны получить одинаковое хеш-значение фиксированного размера.

Три наиболее популярных типа хешей:

- Message digest 5 (MD5): создает 128-битный хеш.
- Secure Hash Algorithm 1 (SHA-1): создает 160-битный хеш.
- Secure Hash Algorithm 2 (SHA-2): опционально создает хеш от 224 до 512 бит.

Основные компоненты криптографии

Цифровая подпись, по аналогии с рукописной, позволяет идентифицировать субъект. Обеспечивает следующий функционал:

- Аутентификацию;**
- Целостность данных;**
- Невоспроизводимость.**

Основные компоненты криптографии

Последовательность действий при обмене информации:

- получить хеш отправляемого пакета;
- зашифровать его закрытым ключом;
- прикрепить полученный хеш к пакету при отправке.

Таким образом мы получили подписанный пакет информации, а прикрепляемый хеш называется цифровой подписью. Да, она рассчитывается каждый раз при подписании нового пакета или файла.