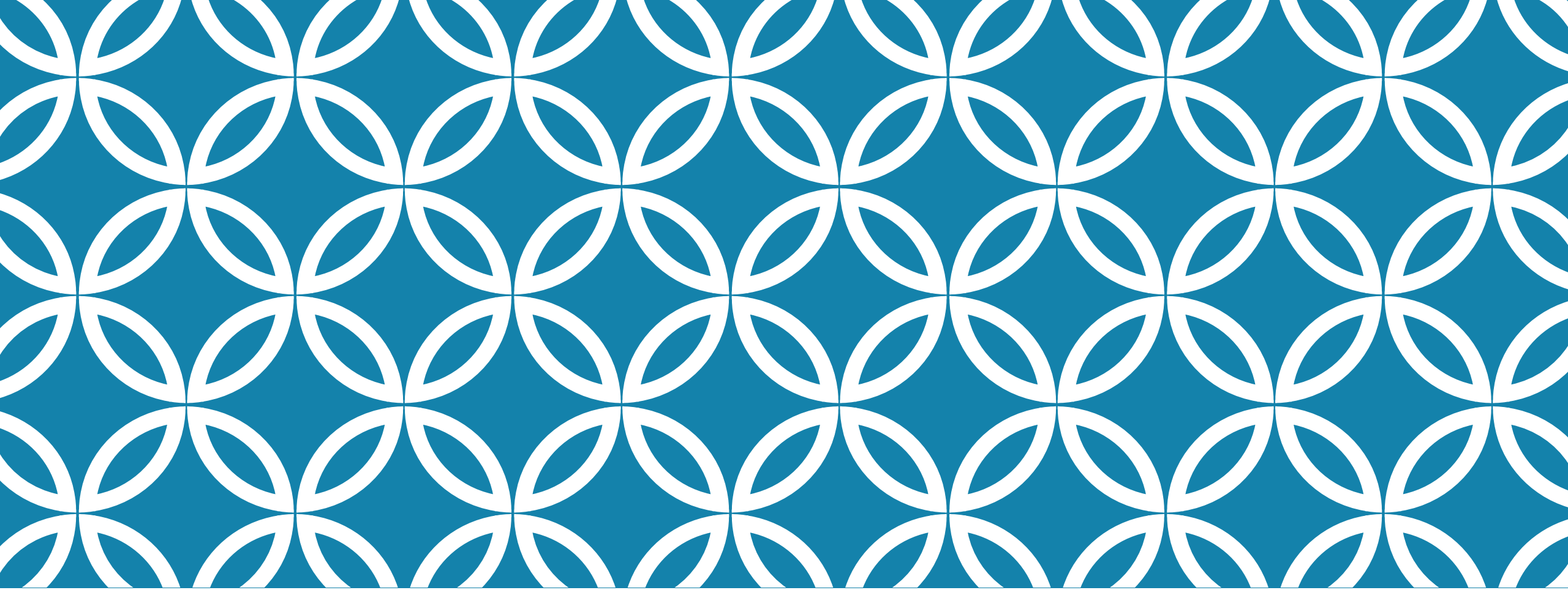


ПРИНЦИПЫ ОРГАНИЗАЦИИ СЕТЕЙ

СЕТИ — ЭТО СИСТЕМЫ, ФОРМИРУЕМЫЕ СОЕДИНЕНИЯМИ.

УЗЕЛ (ХОСТ)

— это любое устройство, отправляющее и получающее информацию по сети.

Примеры общих ресурсов в КС:

- Службы, например службы печати или сканирования
- Пространство хранения на таких устройствах как жесткие диски или оптические диски
- Приложения, например, базы данных
- Информация, хранящаяся на других компьютерах, например, документы и фотографии
- Календари, синхронизированные между компьютером и смартфоном

ПРОМЕЖУТОЧНЫЕ УСТРОЙСТВА

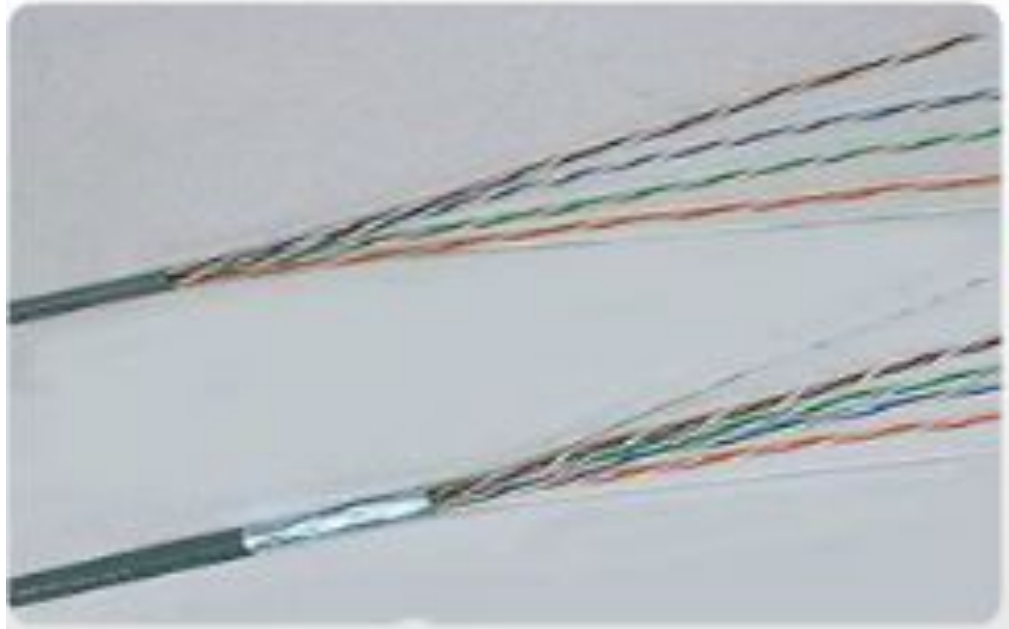
- Коммутатор используется для подключения нескольких устройств к сети.
- Маршрутизатор используется для передачи трафика между различными сетями.
- Беспроводной маршрутизатор подключает к сети несколько беспроводных устройств. Кроме того, беспроводной маршрутизатор часто содержит коммутатор, чтобы проводные устройства могли подключиться к сети.
- Точка доступа (AP) обеспечивает беспроводное соединение, но имеет меньше функций, чем беспроводной маршрутизатор.
- Модем используется для подключения небольшого или домашнего офиса к Интернету.

СРЕДЫ ПЕРЕДАЧИ ДАННЫХ (ПО-АНГЛИЙСКИ ТЕРМИН «СРЕДА ПЕРЕДАЧИ ДАННЫХ» — MEDIA)

Среда передачи данных предоставляет собой канал, по которому сообщение передается от источника к адресату.

МЕДНЫЕ КАБЕЛИ

— для передачи данных между устройствами используются электрические сигналы.



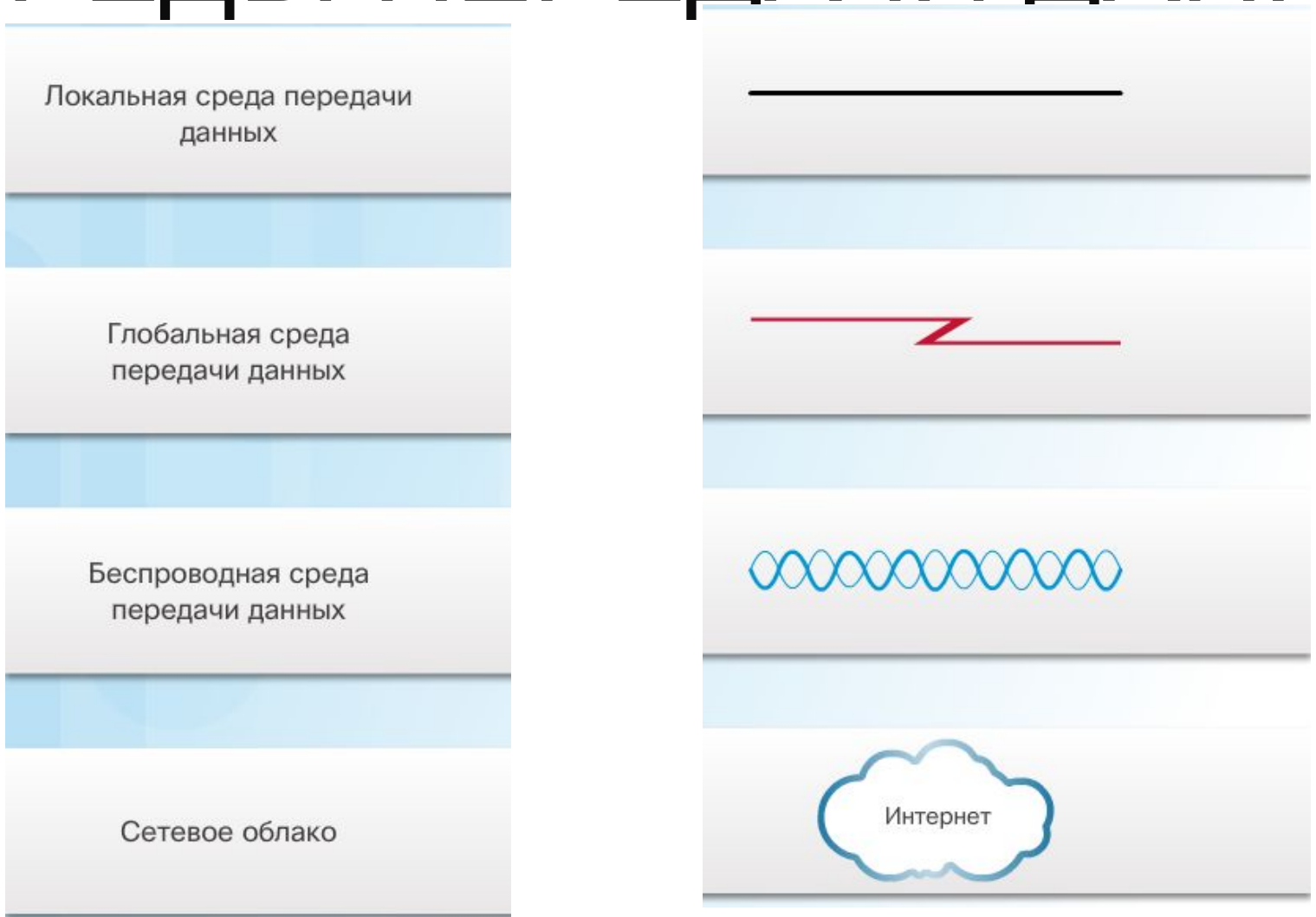
ВОЛОКОННО-ОПТИЧЕСКИЕ КАБЕЛИ

— для передачи информации в виде световых импульсов используется стекловолокно или пластмассовое волокно.

БЕСПРОВОДНЫЕ ПОДКЛЮЧЕНИЯ

— для передачи данных используются радиосигналы, инфракрасная технология или спутниковая связь

ОБОЗНАЧЕНИЯ ТИПОВ СРЕДЫ ПЕРЕДАЧИ ДАННЫХ



ПРОПУСКНАЯ СПОСОБНОСТЬ И ЗАДЕРЖКА

При передаче данных по компьютерной сети они разбиваются на небольшие фрагменты, которые называются пакетами. Каждый пакет содержит информацию об адресе источника и назначения.

Единицы измерения пропускной способности:

бит/с — бит в секунду **Кбит/с — килобит в секунду** **Мбит/с — мегабит в секунду** **Гбит/с — гигабит в секунду**	**1 байт равен 8 битам и обозначается заглавной буквой Б. Это обозначение обычно используется при описании размера файла или емкости хранилища, например: файл размером 2,5 МБ или диск емкостью 2 ТБ.**

ПЕРЕДАЧА ДАННЫХ

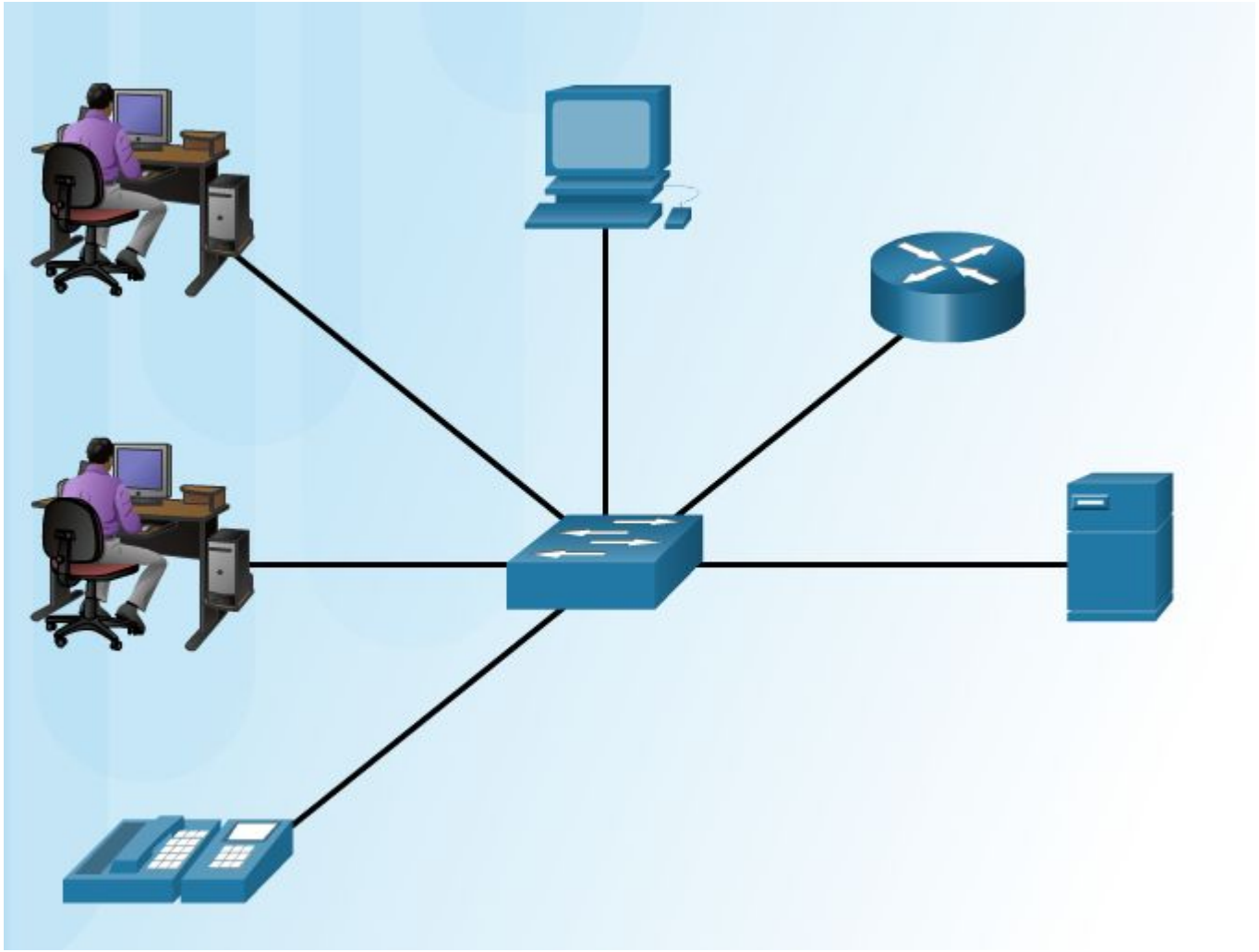
Данные могут передаваться по сети в одном из трех режимов:

- симплексном (одностороннем),
- полудуплексном,
- полнодуплексном (дуплексный — двусторонний).

ТИПЫ СЕТЕЙ

- Компьютерные сети отличаются следующими специфическими характеристиками:
- Площадь покрытия
- Количество подключенных пользователей
- Количество и типы доступных служб
- Область ответственности

ЛОКАЛЬНЫЕ СЕТИ(LAN)



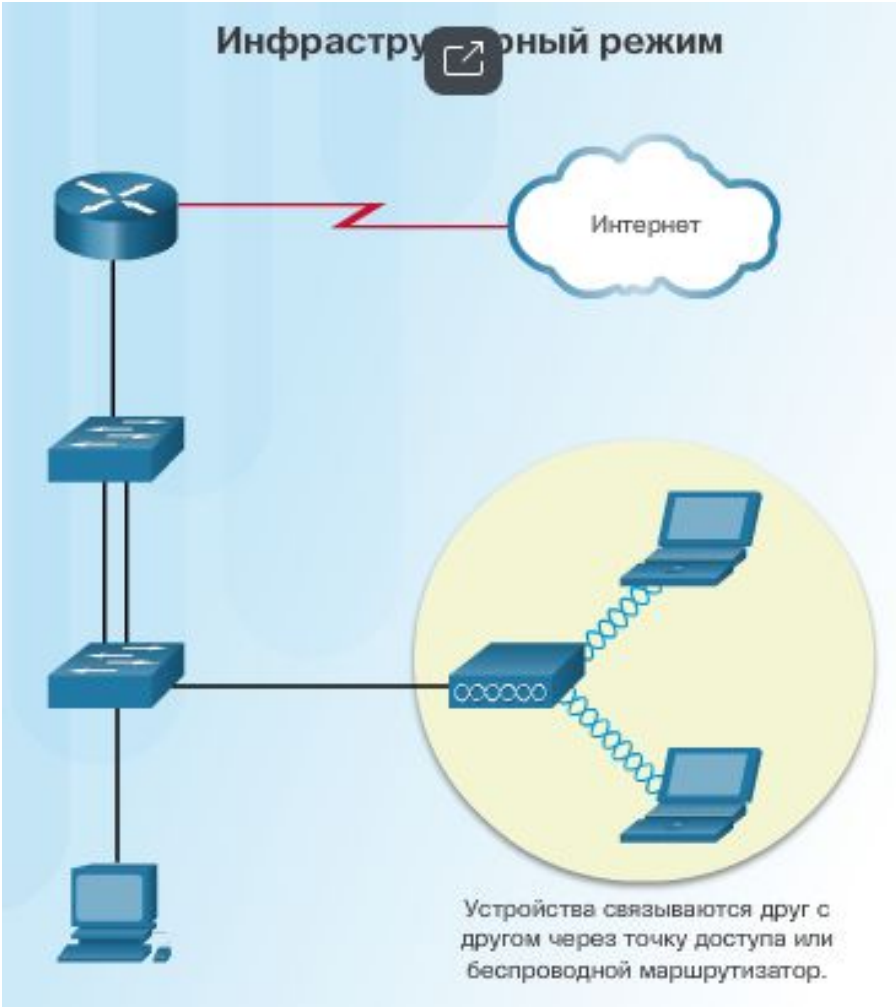
- сеть, охватывающая небольшую географическую область.

БЕСПРОВОДНАЯ ЛОКАЛЬНАЯ СЕТЬ (WLAN)

— это локальная сеть, в которой для передачи данных между беспроводными устройствами используются радиоволны.

WLAN РЕЖИМЫ РАБОТЫ

Infrastructure — беспроводные клиенты подключаются к беспроводному маршрутизатору или точке доступа (AP). Точка доступа на рисунке подключена к коммутатору, который обеспечивает доступ к остальной части сети и Интернету.



WLAN РЕЖИМЫ РАБОТЫ

Ad hoc (прямого подключения) означает, что сеть WLAN создается по мере необходимости. Обычно сети Ad hoc создаются на некоторое время.

ПЕРСОНАЛЬНАЯ СЕТЬ (PAN)

- подключает устройства, такие как мыши, клавиатуры, принтеры, смартфоны и планшетные ПК, находящиеся в пределах досягаемости отдельного пользователя.

- Bluetooth

ПЕРСОНАЛЬНАЯ СЕТЬ (PAN)

Bluetooth — это технология беспроводной связи, позволяющая устройствам обмениваться данными на небольших расстояниях.

- работа в диапазоне от 2,4 до 2,485 ГГц
- Технология активной перестройки частоты AFH (Adaptive Frequency Hopping)

МУНИЦИПАЛЬНЫЕ СЕТИ (MAN)

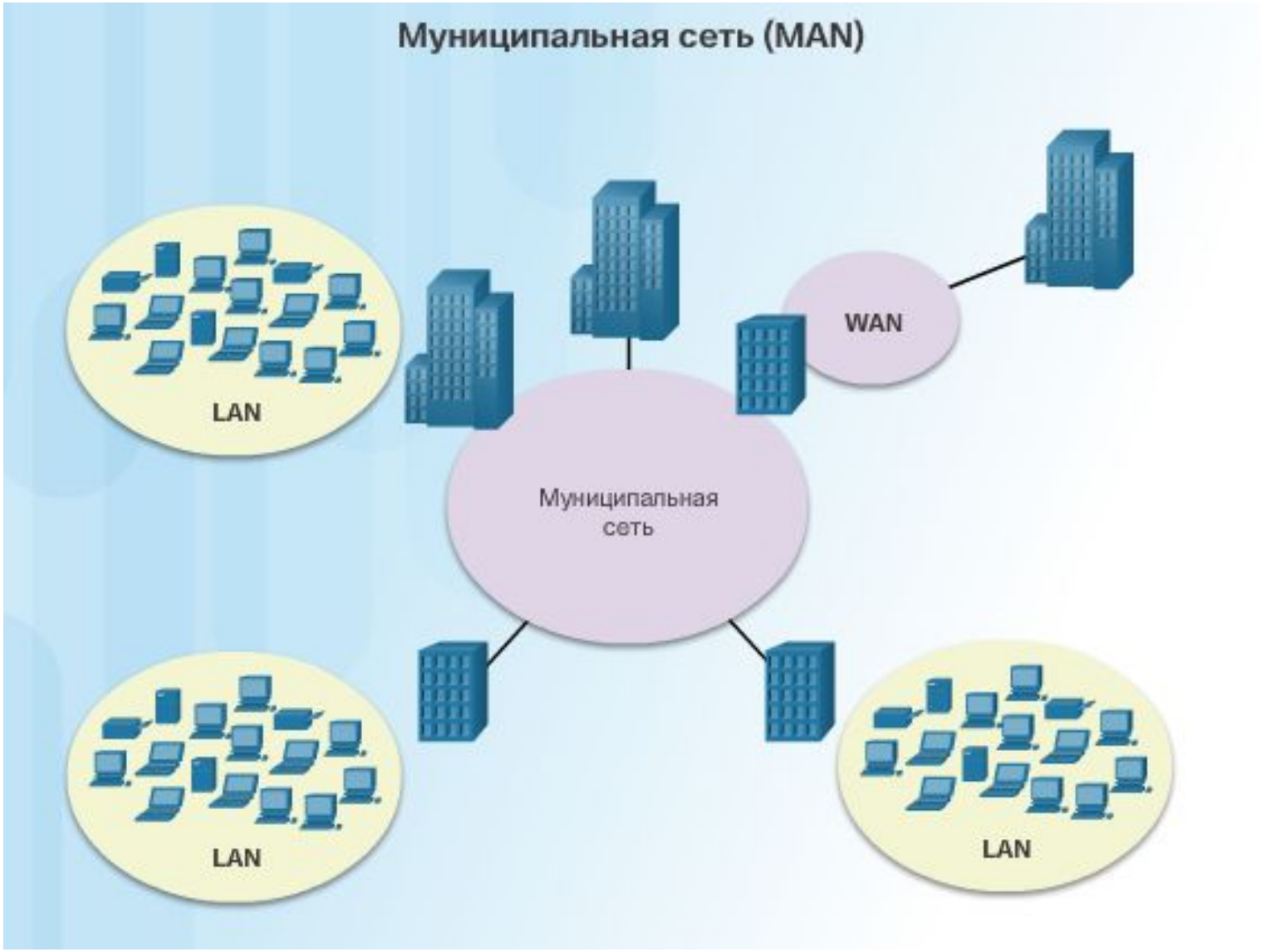
— это сеть, развертываемая в крупном комплексе зданий или на территории целого города.

Пример:

Сеть этого типа состоит из различных зданий, подключенных друг к другу с помощью беспроводных или волоконно-оптических магистральных каналов.

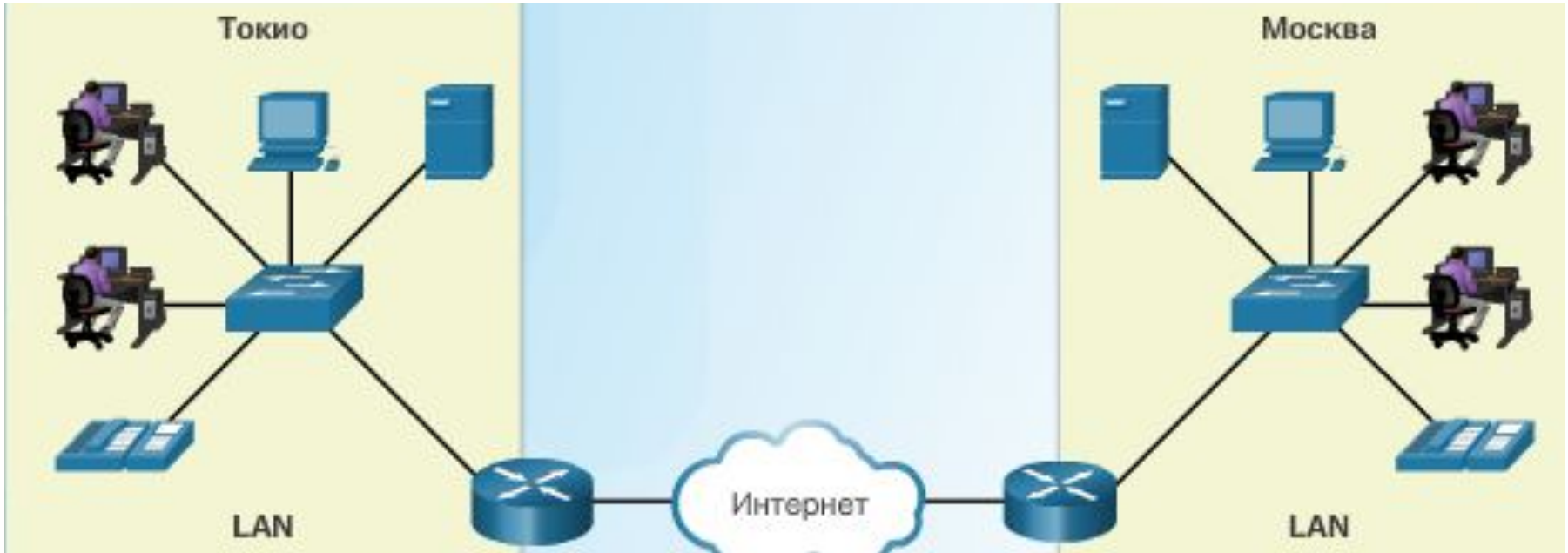
МУНИЦИПАЛЬНЫЕ СЕТИ (MAN)

Муниципальная сеть может функционироват ь в качестве высокоскоростно й сети, предоставляюще й общий доступ к региональным ресурсам.



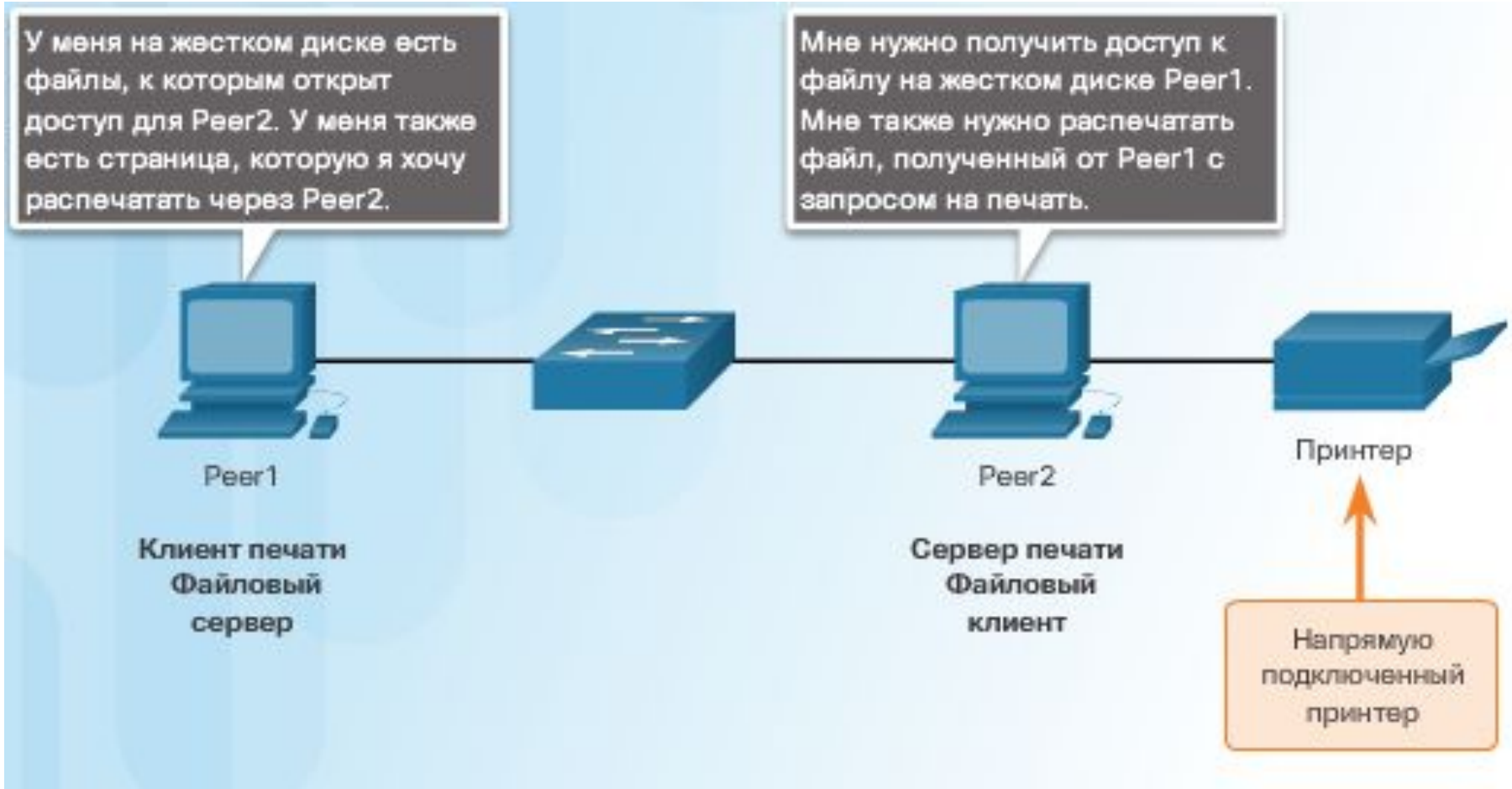
ГЛОБАЛЬНЫЕ СЕТИ(WAN)

-соединяет несколько локальных сетей, расположенных в разных географических местоположениях.



Характерной особенностью глобальной сети является то, что она принадлежит оператору

ОДНОРАНГОВЫЕ СЕТИ (PEER-TO-PEER NETWORK)



отсутствует иерархия компьютеров и нет выделенных серверов.

ОДНОРАНГОВЫЕ СЕТИ ИМЕЮТ РЯД НЕДОСТАТКОВ.

- Отсутствует централизованное администрирование сети.
- Отсутствует централизованная система обеспечения безопасности.
- Сеть становится все более сложной и трудноуправляемой по мере увеличения числа подключенных к ней компьютеров.
- Скорее всего, в такой сети не будет централизованной системы хранения данных. Операции резервного копирования придется выполнять отдельно для каждого компьютера. Ответственность за это будет нести каждый отдельный пользователь.

КЛИЕНТ-СЕРВЕРНЫЕ СЕТИ

На серверы устанавливается программное обеспечение, позволяющее им предоставлять клиентам службы, такие как управление файлами, электронная почта или веб-страницы.

ЭТАЛОННЫЕ МОДЕЛИ

ФУНКЦИИ ПРОТОКОЛОВ

- Идентификация и обработка ошибок
- Сжатие данных
- Определение порядка разделения данных и формирования пакетов
- Назначение адресов пакетам данных
- Определение порядка объявления отправки и получения пакетов данных

Модель OSI

Данные
Данные
Данные
Данные
Блоки
Пакеты
Кадры
Биты

Модель OSI	Уровень	Описание
Уровень приложений	7	Отвечает за предоставление сетевых служб приложениям
Уровень представления	6	Преобразует форматы данных, чтобы обеспечить уровню приложений стандартный интерфейс
Сеансовый уровень	5	Устанавливает и завершает подключения между локальными и удаленными приложениями, а также управляет ими
Транспортный уровень	4	Предоставляет надежный транспорт и управление потоком при передаче данных по сети
Сетевой уровень	3	Отвечает за логическую адресацию и маршрутизацию
Канальный уровень	2	Обеспечивает физическую адресацию и управляет доступом к среде передачи данных
Физический уровень	1	Определяет все электрические и физические требования к устройствам

МОДЕЛЬ TCP/IP

OSI	Уровень TCP/IP	Описание
7 6 5	**Уровень приложений**	На нём работают высокоуровневые протоколы, такие как SMTP и FTP
4	**Транспортный уровень**	Указывает, какое приложение запросило или получает данные через указанные порты
3	**Уровень Интернет (межсетевой уровень)**	На нём происходит IP-адресация и маршрутизация
2 1	**Уровень доступа к сети**	На нём существуют MAC-адресация и физические компоненты сети


Уровень приложений
Система имен
DNS
Конфигурация узла
BOOTP
DHCP
Эл. Почта
SMTP
POP
IMAP
Передача файлов
FTP
TFTP
Веб
HTTP
Транспортный уровень
UDP
TCP
Межсетевой уровень
IP
NAT
Поддержка IP
ICMP
Протоколы маршрутизации
OSPF
EIGRP
Уровень доступа к сети
ARP
PPP
Ethernet
Драйверы интерфейсов

ПРОТОКОЛЫ УРОВНЯ ДОСТУПА К СЕТИ, СТЕКА ПРОТОКОЛОВ TCP/IP.

ПРОТОКОЛ РАЗРЕШЕНИЯ АДРЕСОВ (ADDRESS RESOLUTION PROTOCOL, ARP)

Обеспечивает динамическое сопоставление между IP-адресами и аппаратными адресами

ПРОТОКОЛ ТОЧКА-ТОЧКА (POINT-TO-POINT PROTOCOL, PPP)

Предоставляет средства инкапсуляции пакетов для передачи через последовательный канал

ETHERNET

Определяет правила для стандартов прокладки кабелей и обмена сигналами на уровне доступа к сети

ДРАЙВЕР ИНТЕРФЕЙСОВ

Предоставляет компьютеру инструкции для управления конкретным интерфейсом на сетевом устройстве

ПРОТОКОЛЫ МЕЖСЕТЕВОГО УРОВНЯ, СТЕКА ПРОТОКОЛОВ TCP/IP.

Протоколы:

- Поддержка IP
- Протоколы маршрутизации

ПРОТОКОЛ ИНТЕРНЕТА (INTERNET PROTOCOL, IP)

- Принимает сегменты сообщений с транспортного уровня
- Формирует из них пакеты
- Добавляет в пакеты адресную информацию для доставки конечному получателю по сети.

ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ (NETWORK ADDRESS TRANSLATION, NAT)

Преобразует IP-адреса частной сети в глобальные уникальные публичные IP-адреса

ПОДДЕРЖКА IP: ПРОТОКОЛ УПРАВЛЯЮЩИХ СООБЩЕНИЙ В ИНТЕРНЕТЕ (INTERNET CONTROL MESSEGE PROTOCOL, ICMP)

Обеспечивает обратную связь от узла назначения к исходному узлу, чтобы сообщать об ошибках доставки пакетов

ПРОТОКОЛЫ МАРШРУТИЗАЦИИ: ПРОТОКОЛ ПРЕДПОЧТЕНИЯ КРАТЧАЙШЕГО ПУТИ (OPEN SHORTEST PATH FIRST, OSPF)

- Протокол маршрутизации по состоянию канала
- Иерархическая структура на основе зон
- Протокол внутренней маршрутизации, являющийся открытым стандартом

ПРОТОКОЛЫ МАРШРУТИЗАЦИИ: УСОВЕРШЕНСТВОВАННЫЙ ПРОТОКОЛ ВНУТРЕННЕЙ МАРШРУТИЗАЦИИ МЕЖДУ ШЛЮЗАМИ (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL, EIGRP)

- Проприетарный (принадлежащий компании) протокол маршрутизации Cisco
- Использует составную метрику, основанную на пропускной способности, задержке, нагрузке и

ПРОТОКОЛЫ ТРАНСПОРТНОГО УРОВНЯ, СТЕКА ПРОТОКОЛОВ TCP/IP.

ПРОТОКОЛ ПЕРЕДАЧИ ДАТАГРАММ ПОЛЬЗОВАТЕЛЯ (USER DATAGRAM PROTOCOL, UDP)

- Позволяет процессу, запущенному на одном узле, отправлять пакеты процессу, запущенному на другом узле
- Не подтверждает успешную доставку датаграммы

ПРОТОКОЛ УПРАВЛЕНИЯ ПЕРЕДАЧЕЙ (TRANSMISSION CONTROL PROTOCOL, TCP)

- Обеспечивает надежную связь между процессами, запущенными на разных узлах
- Надежная передача данных с подтверждением успешной доставки

ПРОТОКОЛЫ УРОВНЯ ПРИЛОЖЕНИЙ, СТЕКА ПРОТОКОЛОВ TCP/IP.

Протоколы:

- Система имен
- Конфигурация узла
- Эл. Почта
- Передача файлов
- Веб

СИСТЕМА ИМЕН: СИСТЕМА (ИЛИ СЛУЖБА) ДОМЕННЫХ ИМЕН (DOMAIN NAME SYSTEM ИЛИ SERVICE, DNS)

Преобразует имена доменов, например cisco.com, в IP-адреса.

КОНФИГУРАЦИЯ УЗЛА: ПРОТОКОЛ ЗАГРУЗКИ (BOOTSTRAP PROTOCOL, BOOTP)

- Позволяет бездисковым рабочим станциям узнавать свой IP-адрес, IP-адреса BOOTP-сервера в сети, а также загружать файл в память для запуска компьютера
- BOOTP был вытеснен протоколом DHCP

КОНФИГУРАЦИЯ УЗЛА: ПРОТОКОЛ ДИНАМИЧЕСКОЙ КОНФИГУРАЦИИ СЕТЕВОГО УЗЛА (DYNAMIC HOST CONFIGURATION PROTOCOL, DHCP)

- Динамически присваивает IP-адреса клиентским станциям при запуске
- Позволяет повторно использовать освобождающиеся адреса

ЭЛ. ПОЧТА: ПРОТОКОЛ ПРОСТОГО ОБМЕНА ЭЛЕКТРОННОЙ ПОЧТОЙ (SIMPLE MAIL TRANSFER PROTOCOL, SMTP)

- Позволяет клиентам отправлять электронные сообщения на почтовый сервер
- Позволяет серверам отправлять электронные сообщения на другие серверы

ЭЛ. ПОЧТА: ПРОТОКОЛ ПОЧТОВОГО ОТДЕЛЕНИЯ (POST OFFICE PROTOCOL VERSION 3, POP3)

- Позволяет клиентам получать электронные сообщения с почтового сервера
- Загружает электронные сообщения с почтового сервера на компьютер

ЭЛ. ПОЧТА: ПРОТОКОЛ ДОСТУПА К СООБЩЕНИЯМ В ИНТЕРНЕТЕ (INTERNET MASSAGE ACCESS PROTOCOL, IMAP)

- Позволяет клиентам получать доступ к электронным сообщениям, которые хранятся на почтовом сервере
- Синхронизирует электронные сообщения с почтовым сервером

ПЕРЕДАЧА ФАЙЛОВ: ПРОТОКОЛ ПЕРЕДАЧИ ФАЙЛОВ(FILE TRANSFER PROTOCOL, FTP)

- Устанавливает правила, которые позволяют пользователю получать доступ к файлам на других узлах и обмениваться ими по сети
- Надежный протокол доставки файлов с подтверждением и установлением соединения

ПЕРЕДАЧА ФАЙЛОВ: ПРОСТЕЙШИЙ ПРОТОКОЛ ПЕРЕДАЧИ ФАЙЛОВ (TRIVIAL FILE TRANSFER PROTOCOL, TFTP)

- Простой протокол передачи файлов без установления соединения
- Протокол передачи файлов без подтверждения в режиме негарантированной доставки (“best effort”)
- Накладные расходы ниже, чем у протокола FTP

WEB: ПРОТОКОЛ ПЕРЕДАЧИ ГИПЕРТЕКСТА (HYPERTEXT TRANSFER PROTOCOL, HTTP)

Протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер», то есть предполагается существование:

- Потребителей (клиентов), которые инициируют соединение и посылают запрос;
- Поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые

ПРОТОКОЛЬНЫЙ БЛОК ДАННЫХ (PDU)

7.2.1.5

PROTOCOL DATA UNIT (АНГЛ.) РУССК. — ОБОБЩЁННОЕ НАЗВАНИЕ ФРАГМЕНТА ДАННЫХ НА РАЗНЫХ УРОВНЯХ МОДЕЛИ OSI: КАДР ETHERNET, IP-ПАКЕТ, UDP-ДАТАГРАММА, TCP-СЕГМЕНТ И Т. Д. ПРИМЕРЫ НАЗВАНИЙ НЕКОТОРЫХ ПАКЕТОВ: LACPDU, OAMPDU, BPDU,OSSPDU.

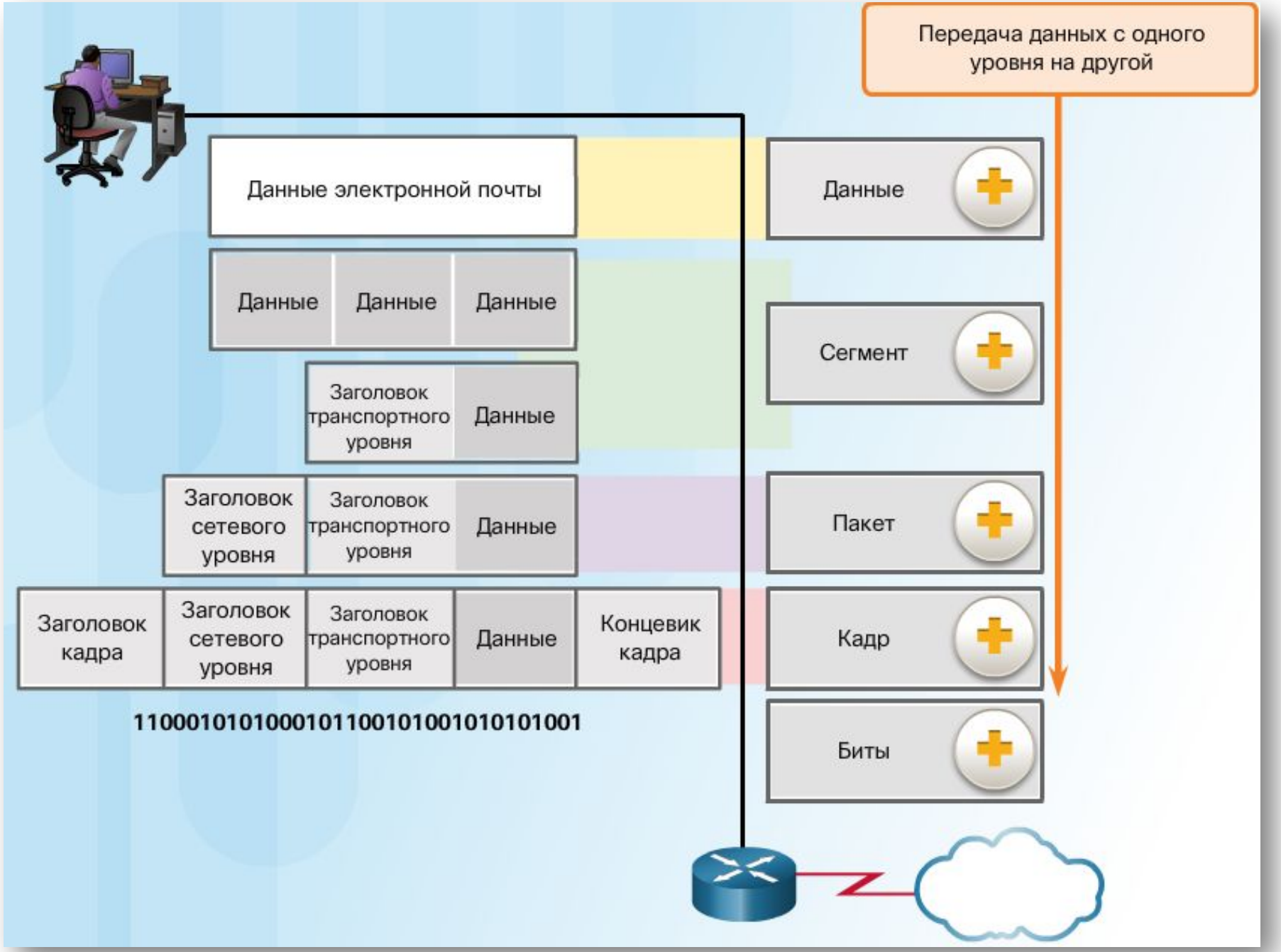
ПРОТОКОЛЬНЫЙ БЛОК ДАННЫХ (PDU)

Сообщение начинается с верхнего прикладного уровня и переходит по уровням TCP/IP к нижнему уровню сетевого доступа. По мере того как данные приложений передаются вниз с одного уровня на другой, на каждом из уровней к ним добавляется информация в соответствии с протоколами. Это называется процессом инкапсуляции.

ПРОТОКОЛЬНЫЙ БЛОК ДАННЫХ (PDU)

Форма, которую принимает массив данных на каждом из уровней, называется протокольным блоком данных (PDU). В ходе инкапсуляции каждый последующий уровень инкапсулирует PDU, полученную от вышестоящего уровня в соответствии с используемым протоколом. На каждом этапе процесса PDU получает другое имя, отражающее новые функции.

ИНКАПСУЛЯЦИЯ



ДАННЫЕ

общий термин для обозначения PDU, используемой на прикладном уровне

СЕГМЕНТ

PDU транспортного уровня

ПАКЕТ

PDU сетевого уровня

КАДР (ЗАВИСИТ ОТ СРЕДСТВА ПОДКЛЮЧЕНИЯ)

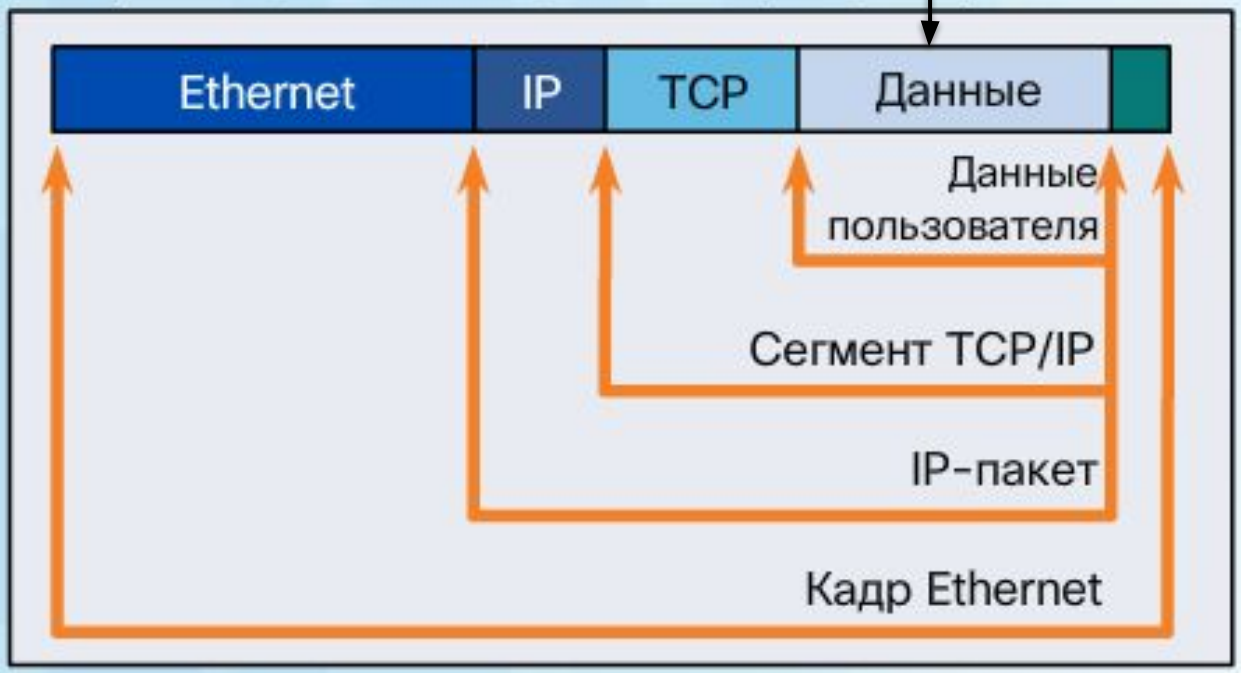
PDU уровня канала данных

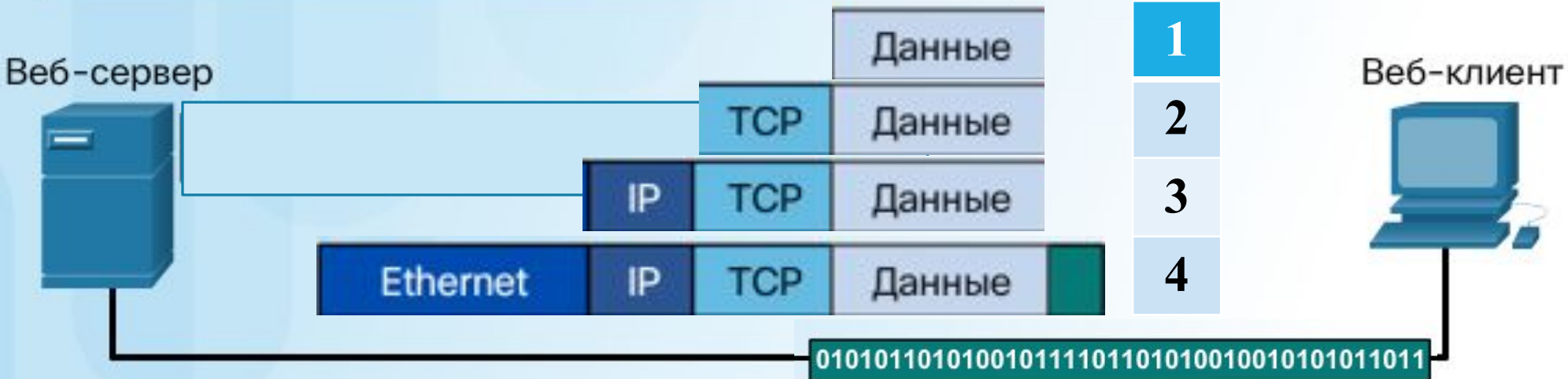
БИТЫ

PDU физического уровня, используемая при физической передаче данных по средству подключения

Взаимодействие протоколов при отправке сообщения

Термины, описывающие инкапсуляцию протоколов

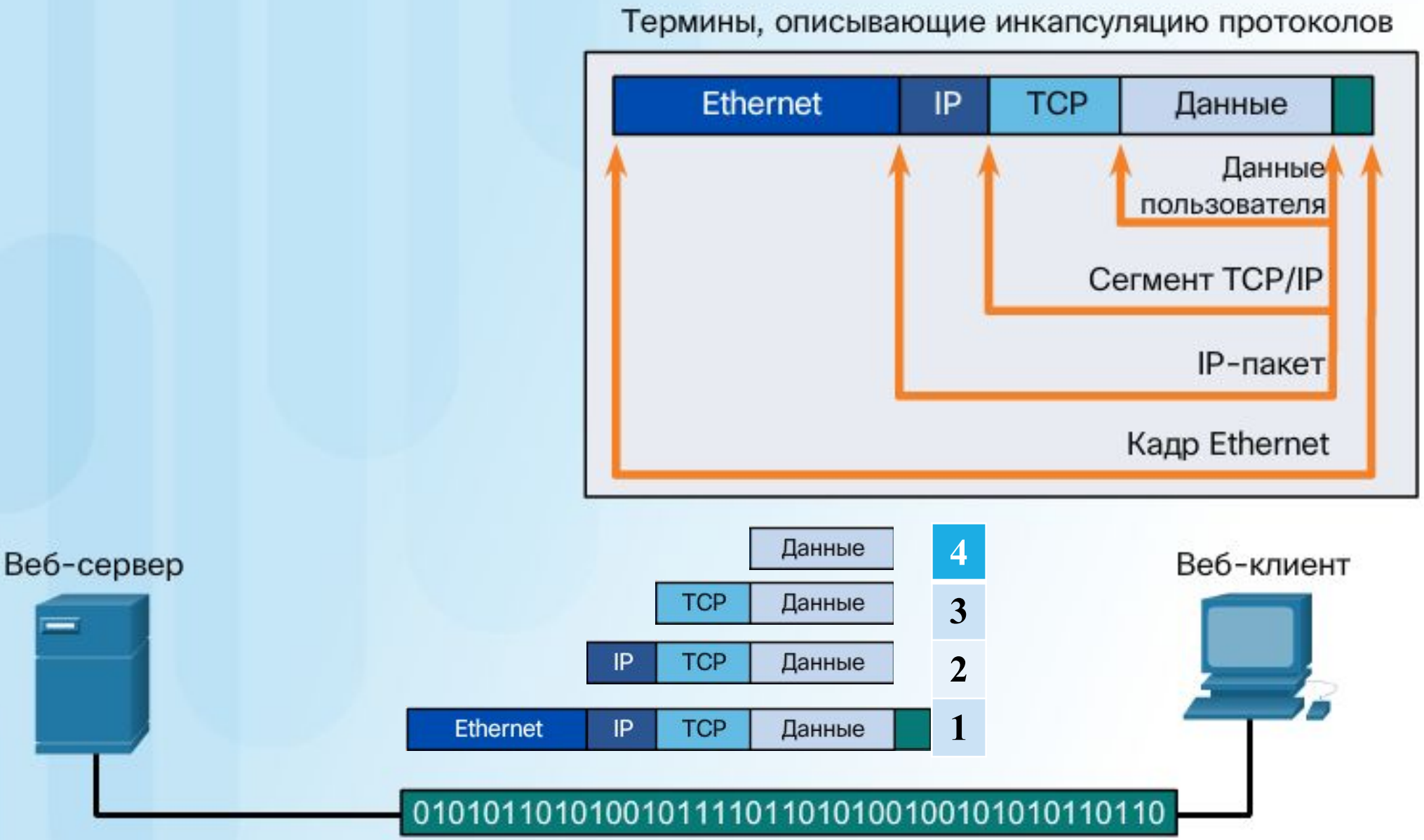




ПРИМЕР ИНКАПСУЛЯЦИИ

При отправке сообщения по сети процесс инкапсуляции идет от верхнего уровня к нижнему. Данные на каждом уровне оказываются вложенными внутрь инкапсулированного протокола. Например, сегмент TCP является частью данных внутри IP-пакета

Взаимодействие протоколов при получении сообщения



ПРИМЕР ДЕКАПСУЛЯЦИИ

Обратный процесс на принимающем узле называется декапсуляцией.

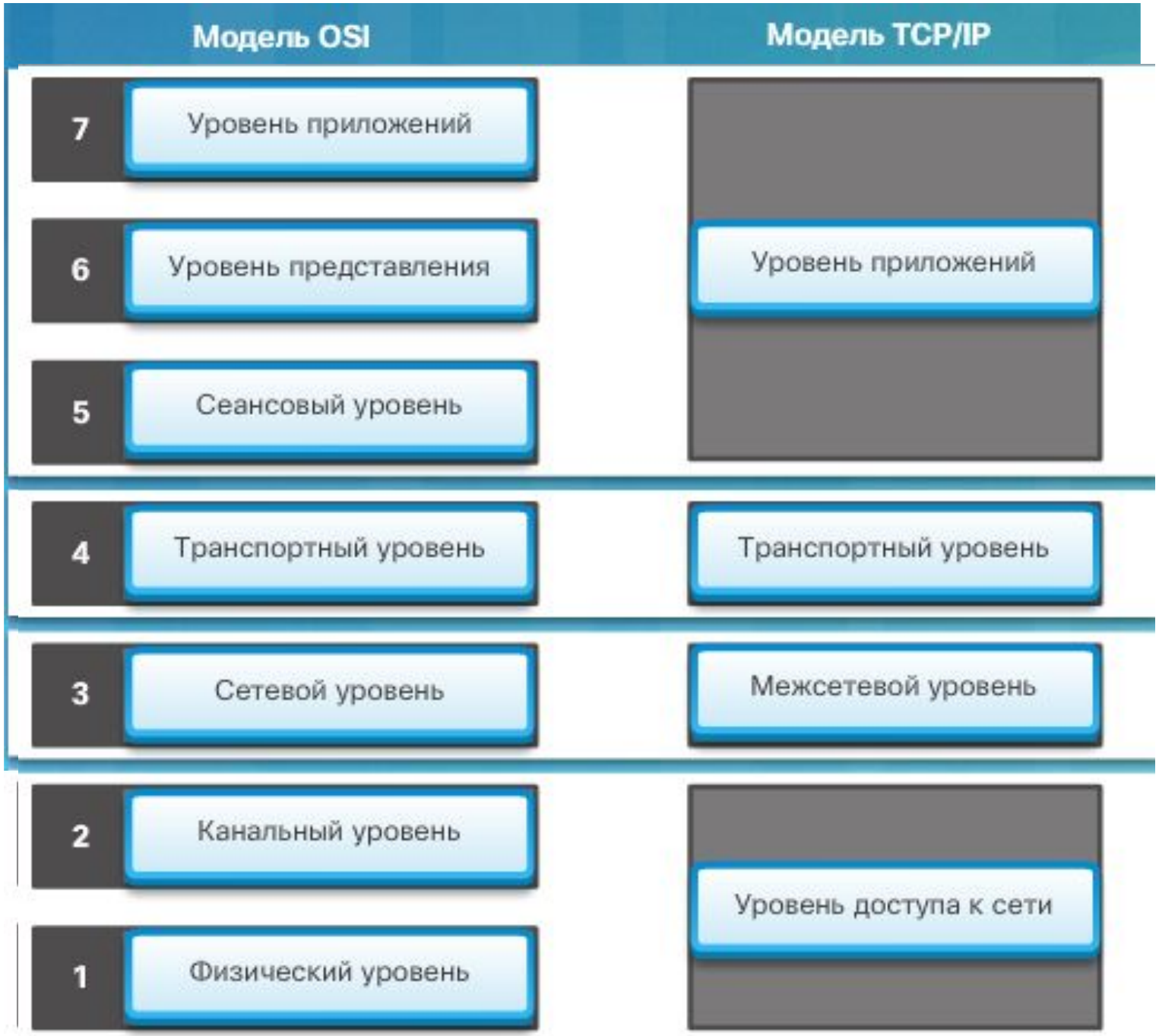
Декапсуляция — это процесс удаления одного или нескольких заголовков принимающим устройством. По мере продвижения данных вверх с одного уровня на другой к приложениям для конечных пользователей они декапсулируются.

Сравнение моделей OSI и TCP/IP

СРАВНЕНИЕ МОДЕЛЕЙ OSI И TCP/IP

Модели OSI и TCP/IP являются эталонными моделями, используемыми для описания процесса передачи данных. Модель TCP/IP используется специально для набора протоколов TCP/IP, а модель OSI — для разработки стандартов связи для оборудования и приложений различных поставщиков.

Модель TCP/IP выполняет ту же процедуру, что и модель OSI, но использует четыре уровня вместо


Модель OSI
Модель TCP/IP
7
Уровень приложений
6
Уровень представления
5
Сеансовый уровень
Уровень приложений
4
Транспортный уровень
Транспортный уровень
3
Сетевой уровень
Межсетевой уровень
2
Канальный уровень
1
Физический уровень
Уровень доступа к сети

CSMA/CD

Протокол Ethernet описывает правила управления передачей данных в сети Ethernet. Чтобы обеспечить совместимость всех устройств Ethernet друг с другом, IEEE разработала стандарты для производителей и программистов по разработке устройств Ethernet.

Архитектура Ethernet основана на стандарте IEEE 802.3. Стандарт IEEE 802.3 определяет, что в сети реализуется способ контроля доступа «множественный доступ с контролем несущей и обнаружением конфликтов (CSMA/CD)».

- **Несущая** — проводник, используемый для передачи данных.
- **Контроль** — каждое устройство прослушивает проводник, чтобы определить, свободен ли он для передачи данных, как показано на рисунке.
- **Множественный доступ** — в сети могут одновременно присутствовать несколько устройств.
- **Обнаружение конфликтов** — конфликт вызывает удвоение напряжения на проводе, распознаваемое сетевыми платами устройств.

В CSMA/CD все устройства прослушивают сетевой проводник и ждут, когда он будет свободен для отправки данных. Этот процесс похож на ожидание сигнала готовности линии на телефоне перед набором номера. Когда устройство определяет, что никакие другие устройства не передают данные, оно пытается отправить данные. Если никакое другое устройство не отправляет данные в это же время, передача на компьютер назначения происходит без проблем. Если в это время другое устройство выполнит передачу, в проводнике возникнет конфликт.

Первая станция, которая обнаруживает конфликт, отправляет сигнал наличия конфликта (jam signal), который говорит всем узлам остановить передачу и запустить алгоритм восстановления после конфликта. Алгоритм восстановления после конфликта вычисляет случайное время, по истечении которого конечная станция пытается повторить передачу. Обычно это случайное время равняется 1 или 2 миллисекундам (мс). Эта последовательность происходит каждый раз при наличии конфликта в сети и может снизить скорость передачи Ethernet на 40 процентов.

- **Примечание**. Большинство сетей Ethernet работает в настоящее время в полнодуплексном режиме. В таком режиме Ethernet конфликты возникают редко, поскольку устройства могут выполнять отправку и прием данных одновременно.

Устройства прослушивают провод

СТАНДАРТЫ КАБЕЛЕЙ ETHERNET

Стандарт IEEE 802.3 определяет несколько физических реализаций, поддерживающих Ethernet. На рисунке приведена сводка стандартов различных типов кабелей Ethernet.

1000BASE-T — в настоящее время наиболее часто реализуемая архитектура Ethernet. Ее название включает в себя характеристики стандарта:

- 1000 означает скорость работы порта: 1000 Мбит/с или 1 Гбит/с.
- BASE означает передачу в основной полосе частот. При передаче в основной полосе частот вся пропускная способность кабеля используется для одного типа сигнала.
- T означает медный кабель (Twisted pair).

Стандарты Ethernet

Стандарты Ethernet	Среды передачи данных	Скорости передачи
10BASE-T	Категория 3	Передача данных со скоростью 10 Мбит/с.
100BASE-TX	Категория 5	На скорости 100 Мбит/с скорости передачи 100BASE-TX в десять раз выше скоростей 10BASE-T.
1000BASE-T	Категория 5e, 6	Архитектура 1000BASE-T поддерживает скорости передачи данных до 1 Гб/с.
10GBASE-T	Категория 6a, 7	Архитектура 10GBASE-T поддерживает скорости передачи данных до 10 Гб/с.

CSMA/CA

IEEE 802.11 — это стандарт, определяющий связь для беспроводных сетей. В беспроводных сетях применяется множественный доступ с контролем использования несущей и предотвращением конфликтов (CSMA/CA).

CMSA/CA не обнаруживает конфликты, а старается избежать их, ожидая своей очереди для передачи. Каждое передающее устройство включает в кадр сведения о времени, необходимом ему для передачи. Все остальные беспроводные устройства принимают эту информацию и знают, как долго среда передачи данных будет занята.

Это означает, что беспроводные устройства работают в полудуплексном режиме.

У точки доступа или беспроводного маршрутизатора эффективность передачи уменьшается по мере подключения все большего количества


В кадре данных беспроводной сети я вижу, что канал будет недоступен определенное время, поэтому я не могу отправить.
Я получаю кадр данных беспроводной сети.
В кадре данных беспроводной сети я вижу, что канал будет недоступен определенное время, поэтому я не могу отправить.

СТАНДАРТЫ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ

IEEE 802.11, или Wi-Fi, представляет собой группу стандартов, которые определяют характеристики радиочастотного излучения, скорость передачи и другие параметры беспроводных локальных сетей. За последние годы разработан ряд реализаций стандарта IEEE 802.11, показанных на рисунке

Стандарты

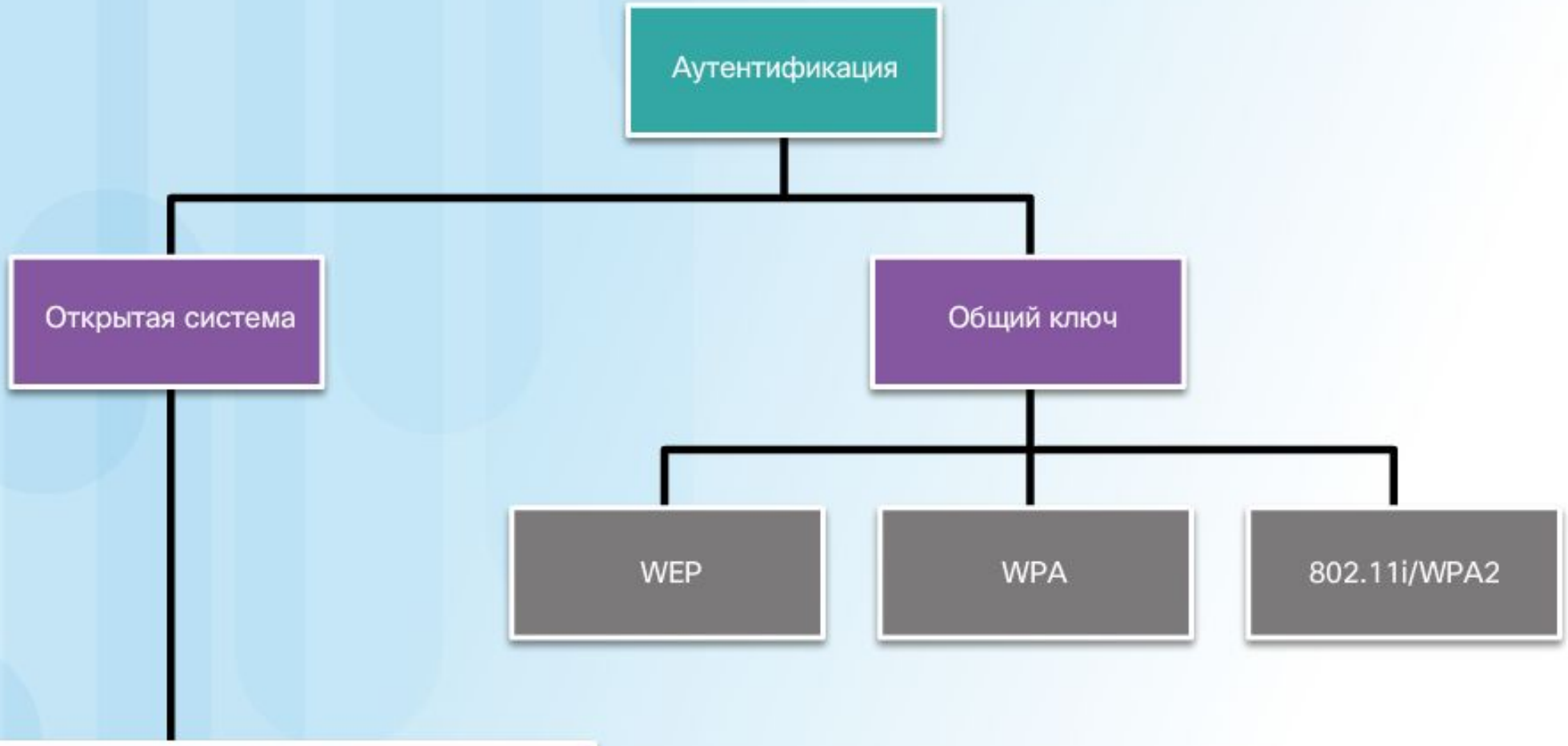
802.11a, 802.11b и 802.11g следует считать устаревшими. Новые сети WLAN должны включать в себя устройства, удовлетворяющие стандарту 802.11ac. В существующих реализациях сетей WLAN рекомендуется при приобретении новых устройств выполнить обновление до 802.11ac.

Стандарт IEEE	Максимальная скорость	Максимальный радиус действия внутри помещений	Частота	Обратная совместимость
802.11a	54 Мбит/с	35 м	5 ГГц	–
802.11b	11 Мбит/с	35 м	2,4 ГГц	–
802.11g	54 Мбит/с	38 м	2,4 ГГц	802.11b
802.11n	600 Мбит/с	70 м	2,4 ГГц и 5 ГГц	802.11a/b/g
802.11ac	1,3 Гбит/с (1300 Мбит/с)	35 м	5 ГГц	802.11a/n

БЕЗОПАСНОСТЬ БЕСПРОВОДНОЙ СЕТИ

Лучший способ защиты беспроводных сетей — использование аутентификации и шифрования. В первоначальном стандарте 802.11 были определены два типа аутентификации.

Методы аутентификации



- **Аутентификация открытой системы** — любое беспроводное устройство может подключиться к беспроводной сети. Этот тип аутентификации следует использовать только в тех случаях, когда безопасность не имеет значения.
- **Аутентификация с помощью общего ключа** — предоставляет механизмы аутентификации и шифрования данных, передаваемых между беспроводным клиентом и точкой доступа.

В СЕТЯХ WLAN ДОСТУПНЫ ТРИ ВАРИАНТА АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ ОБЩЕГО КЛЮЧА.

Эквивалент секретности проводной сети (Wired Equivalent Privacy, WEP) — спецификация обеспечения безопасности WLAN, определенная в первоначальном стандарте 802.11. Однако при передаче пакетов ключ не меняется, поэтому его достаточно легко взломать.

В СЕТЯХ WLAN ДОСТУПНЫ ТРИ ВАРИАНТА АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ ОБЩЕГО КЛЮЧА.

Защищенный доступ к Wi-Fi (Wi-Fi Protected Access, WPA) — этот стандарт использует WEP, но обеспечивает защиту данных при помощи гораздо более надежного протокола шифрования с использованием временных ключей (TKIP). Алгоритм TKIP меняет ключ для каждого пакета, поэтому его гораздо сложнее взломать.

В СЕТЯХ WLAN ДОСТУПНЫ ТРИ ВАРИАНТА АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ ОБЩЕГО КЛЮЧА.

IEEE 802.11i/WPA2 — стандарт IEEE 802.11i является в настоящее время отраслевым стандартом безопасности беспроводных сетей. Версия Wi-Fi Alliance называется WPA2. 802.11i и WPA2 используют для шифрования усовершенствованный стандарт шифрования (Advanced Encryption Standard, AES). В настоящее время AES считается самым надежным

С 2006 года все устройства, на которые нанесен логотип Wi-Fi Certified, сертифицированы для использования WPA2. Поэтому современные беспроводные сети всегда должны использовать стандарт 802.11i/WPA2.

МОДЕМЫ

Модем подключается к Интернету через интернет-провайдера (ISP). Существуют три основных типа модемов. Модемы преобразуют цифровые компьютерные данные в формат, который можно передавать в сеть интернет-провайдера.

АНАЛОГОВЫЙ МОДЕМ

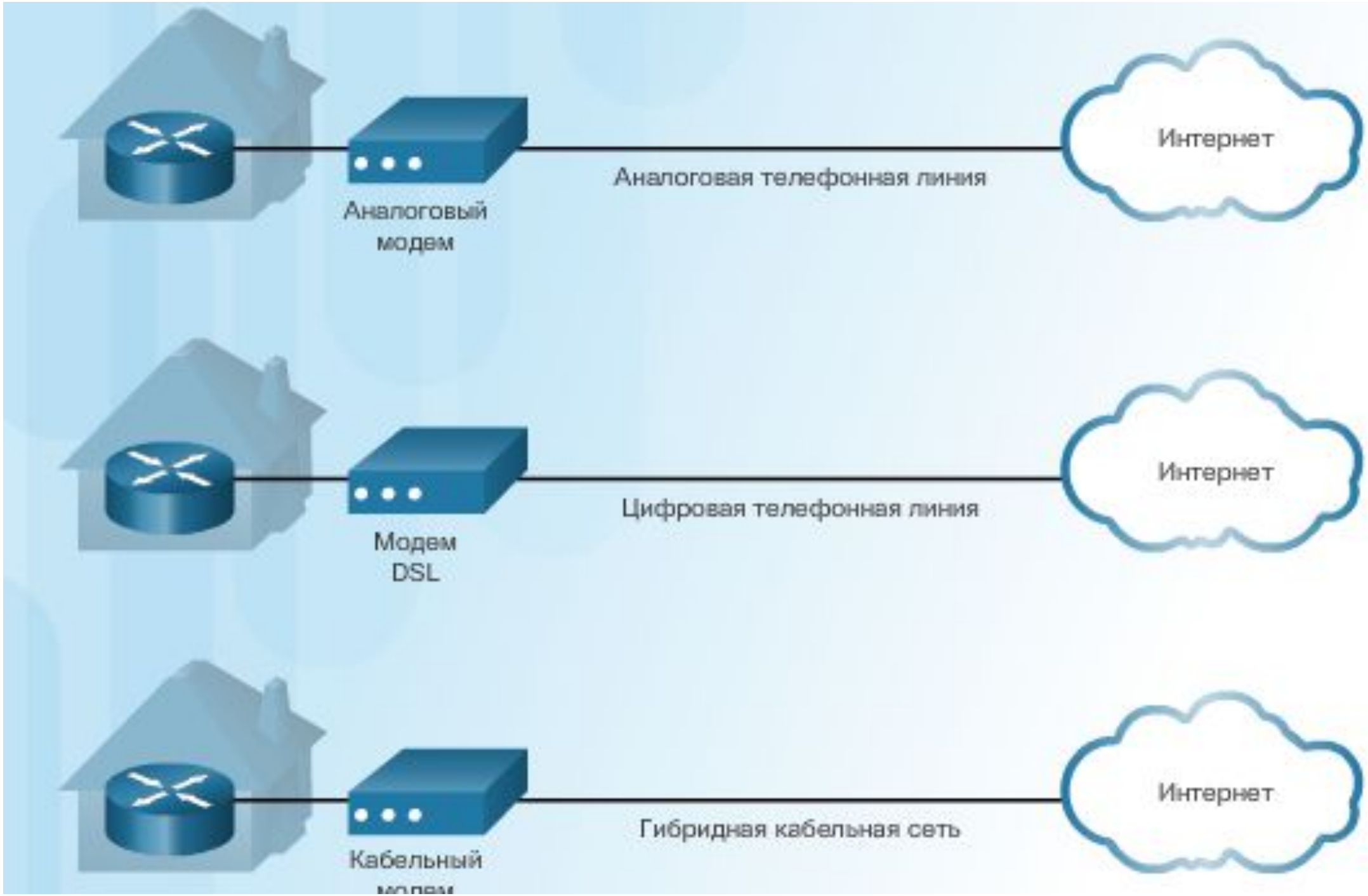
преобразует цифровые данные в аналоговые сигналы и передает их по телефонной линии.

МОДЕМ ЦИФРОВОЙ АБОНЕНТСКОЙ ЛИНИИ (DSL)

соединяет сеть пользователя непосредственно с инфраструктурой цифровой сети телефонной компании.

КАБЕЛЬНЫЙ МОДЕМ

соединяет сеть пользователя с поставщиком услуг кабельного ТВ, который обычно имеет гибридную сеть (HFC) с волоконно-оптическими и коаксиальными кабелями.


Интернет
Аналоговая телефонная линия
Аналоговый модем
Интернет
Цифровая телефонная линия
Модем DSL
Интернет
Гибридная кабельная сеть
Кабельный

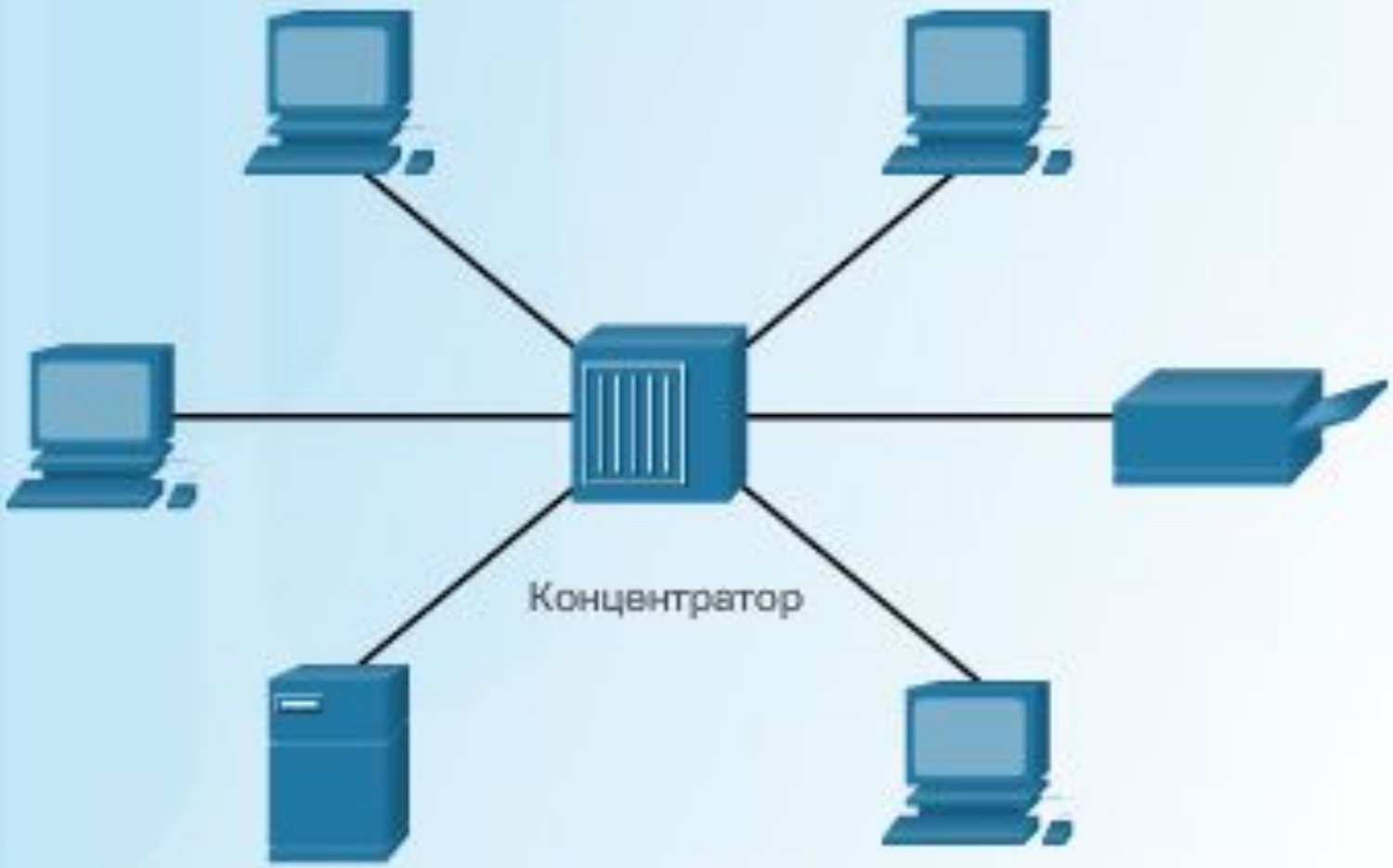
КОНЦЕНТРАТОРЫ, МОСТЫ И КОММУТАТОРЫ

Оборудование, используемое для подключения устройств в локальной сети, прошло путь развития от концентраторов до мостов и коммутаторов.

КОНЦЕНТРАТОРЫ

Концентраторы (hub), принимают данные на одном порте, затем отправляют их на все другие порты. Концентратор расширяет дальность действия сети, поскольку регенерирует (восстанавливает) электрические сигналы. Кроме того, можно подключать концентраторы к другому сетевому устройству, например к коммутатору или маршрутизатору, который, в свою очередь, подключен к другим сегментам сети.

Концентраторы подключают устройства к локальной сети

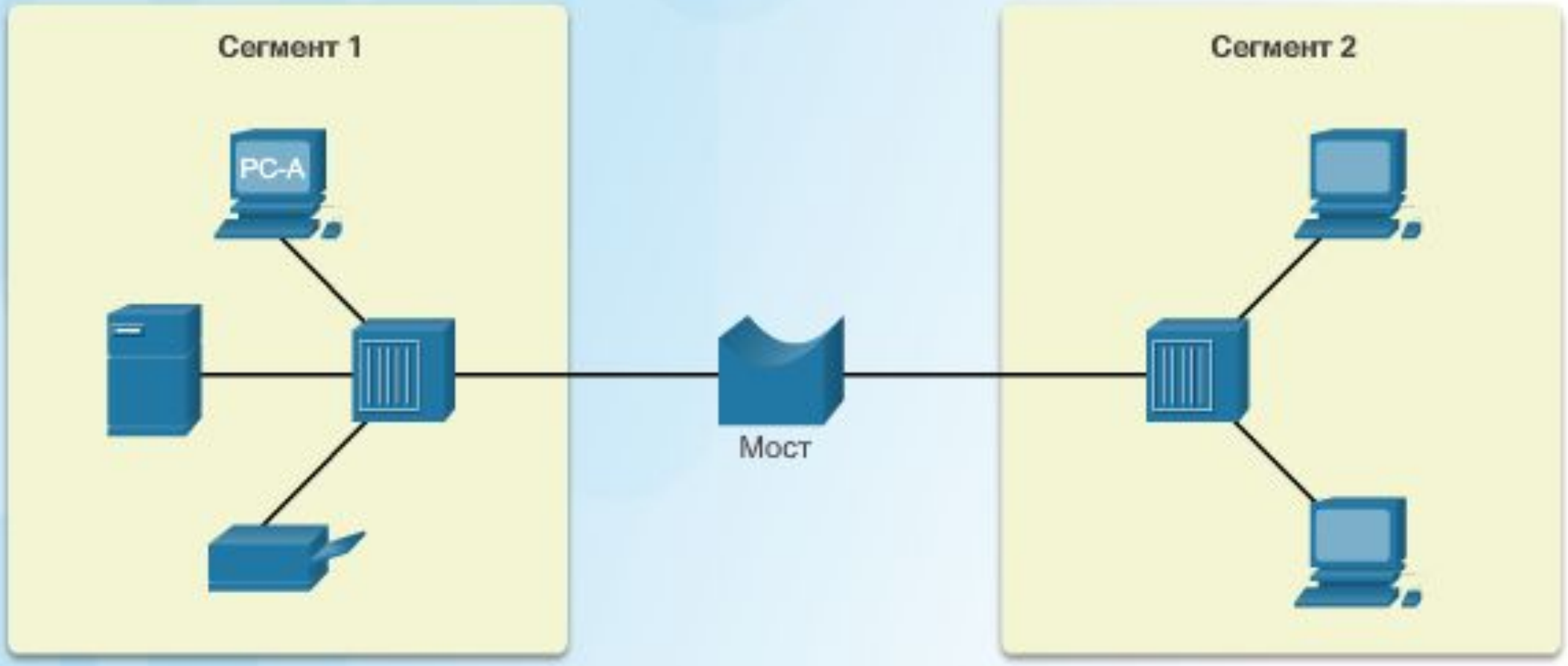


Сегодня концентраторы используются реже, поскольку коммутаторы являются более эффективными и менее дорогостоящими. Концентраторы не выполняют сегментацию (разделение) сетевого трафика. Когда одно устройство отправляет трафик, концентратор передает этот трафик на все подключенные к нему устройства. Полоса пропускания делится между всеми устройствами.

МОСТЫ

Мосты (bridge) были изобретены для разделения локальных сетей на сегменты. Мосты запоминают, какие устройства находятся в каждом сегменте. Поэтому мост может выполнять фильтрацию сетевого трафика между сегментами локальной сети. Это позволяет уменьшить объем трафика между устройствами.

Мосты разделяют LAN на сегменты

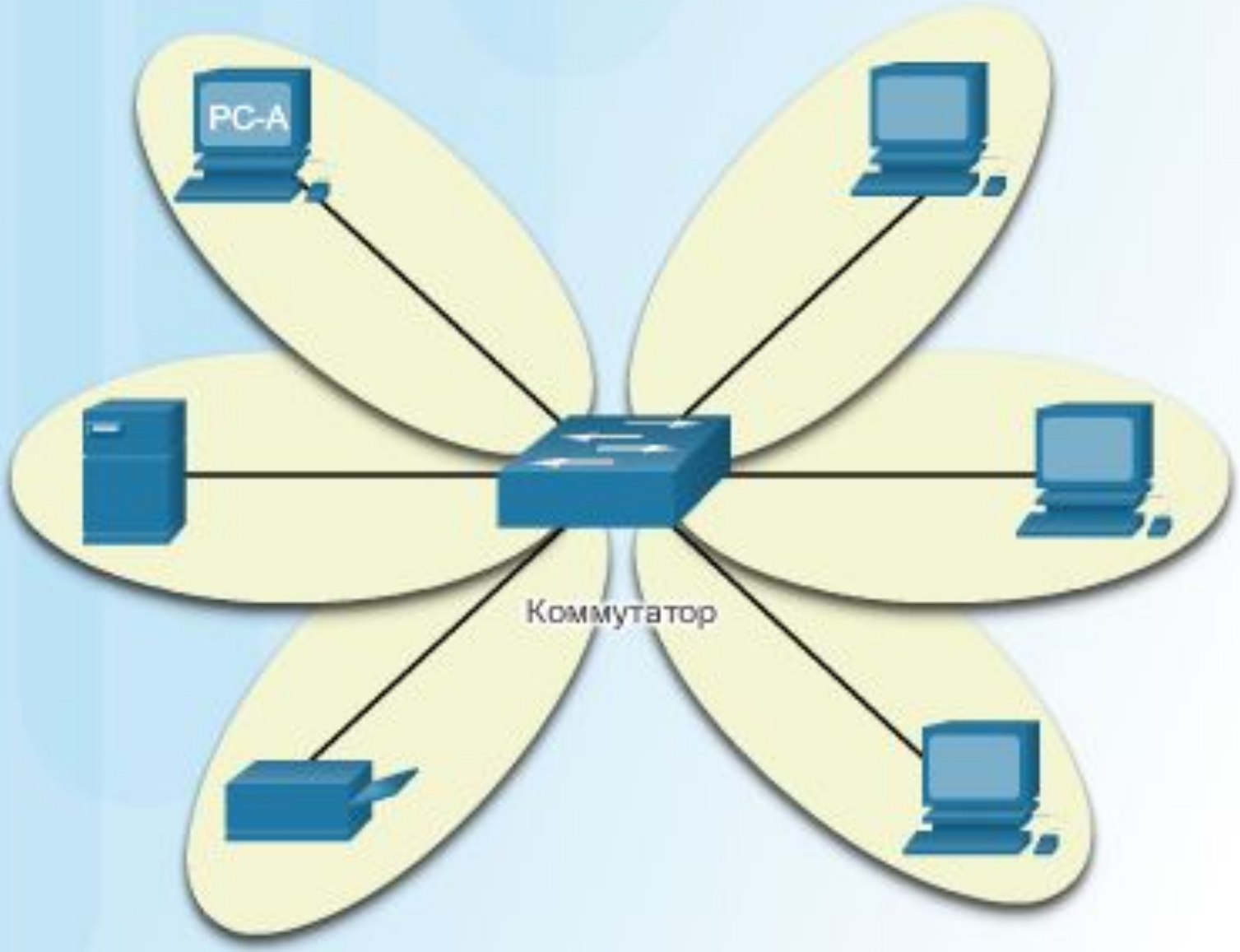


Если компьютеру «PC-A» нужно отправить задание на принтер, трафик не будет передан в сегмент 2. Однако сервер тоже получит копию трафика с заданием для печати.

КОММУТАТОРЫ

Мосты и концентраторы теперь считаются устаревшими устройствами, поскольку коммутаторы (switch) эффективнее и дешевле.

Коммутаторы осуществляют микросегментацию сети LAN



Коммутатор выполняет микросегментацию локальной сети.

Микросегментация означает, что коммутаторы осуществляют фильтрацию и сегментацию сетевого трафика, отправляя данные только на устройство, которому этот трафик адресован.

Такой подход обеспечивает повышение пропускной способности, выделенной для каждого устройства в сети.

Если к каждому порту коммутатора подключено только одно устройство, он работает в полнодуплексном режиме.

У концентраторов такой возможности просто нет.

Когда компьютер «PC-A» отправляет задание на принтер, только принтер получит этот трафик.

Коммутаторы ведут таблицу коммутации. Таблица коммутации содержит список всех MAC-адресов сети, а также список портов коммутатора, через которые доступны устройства с определенными MAC-адресами. Таблица коммутации запоминает MAC-адреса, записывая для каждого входящего кадра MAC-адреса источника и порт, на который этот кадр пришел.

После этого коммутатор создает таблицу коммутации, в которой MAC-адреса сопоставляются с исходящими портами. При получении трафика, предназначенного для определенного MAC-адреса, коммутатор с помощью таблицы коммутации определяет, какой порт следует использовать для отправки сообщения на этот MAC-адрес. Трафик пересылается получателю через этот порт. Отправка трафика только через один конкретный порт непосредственно получателю позволяет не оказывать влияние на другие порты.

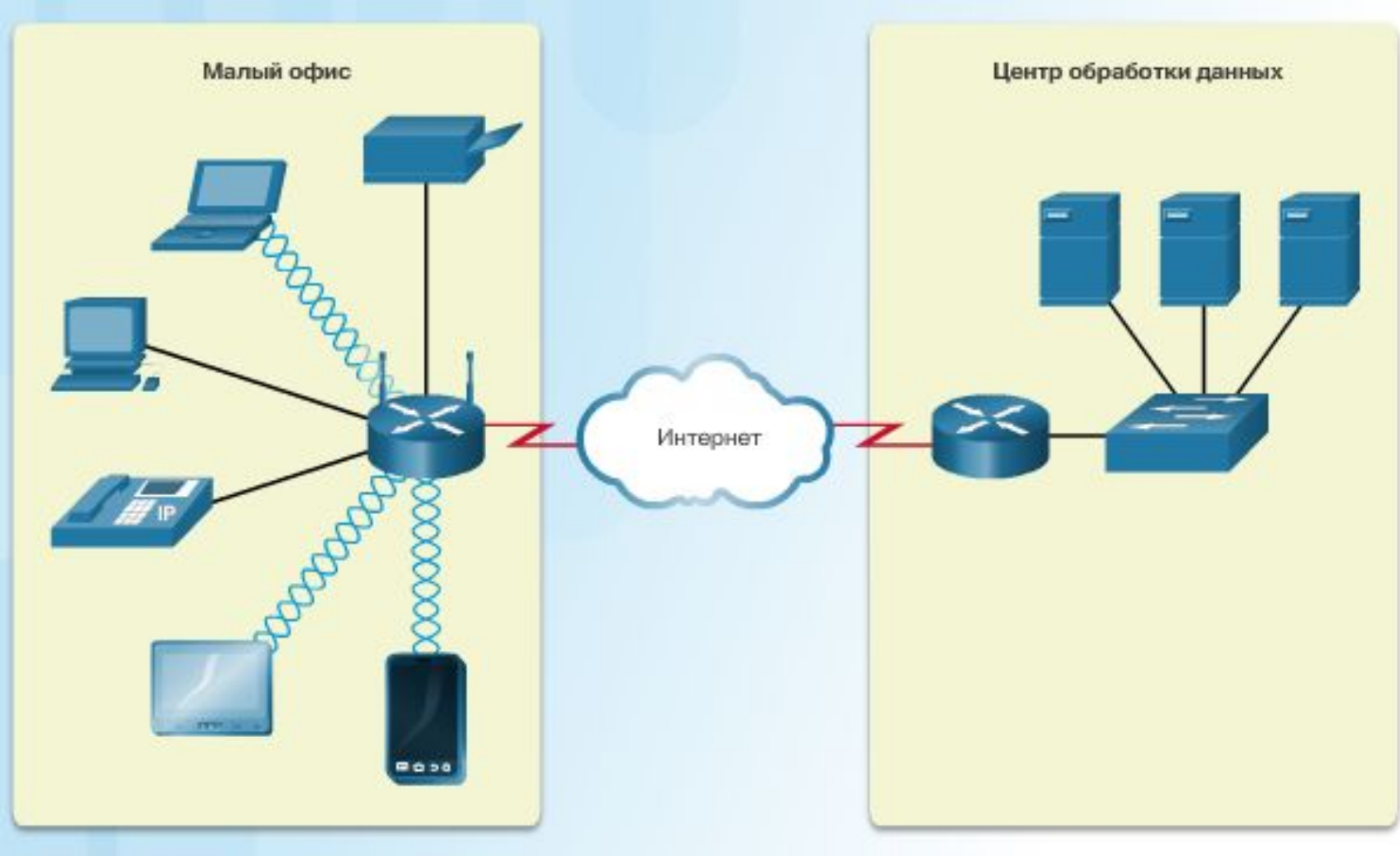
ТОЧКИ БЕСПРОВОДНОГО ДОСТУПА И МАРШРУТИЗАТОРЫ

Точки беспроводного доступа

Точки беспроводного доступа, предоставляют доступ к сети для беспроводных устройств, таких как ноутбуки и планшетные ПК. Точки беспроводного доступа используют радиоволны для связи с беспроводными сетевыми платами в устройствах и с другими беспроводными точками доступа.

Точка беспроводного доступа имеет ограниченную зону покрытия. Для обеспечения адекватной зоны покрытия крупномасштабных беспроводных сетей требуется несколько точек доступа. Точки беспроводного доступа обеспечивают только подключение к сети, в то время как беспроводной маршрутизатор предоставляет дополнительные возможности.

МАРШРУТИЗАТОРЫ



Маршрутизаторы соединяют сети. Коммутаторы используют MAC-адреса для пересылки трафика в рамках одной сети. Маршрутизаторы используют IP-адреса для пересылки трафика в другие сети.

Маршрутизаторы используют IP-адреса для пересылки трафика в другие сети. Маршрутизатором может быть компьютер со специальным сетевым ПО или устройство, собранное производителем оборудования. В крупных сетях маршрутизаторы подключаются к коммутаторам, которые подключаются к локальным сетям. Так подключен маршрутизатор справа. Маршрутизатор выполняет функции шлюза во внешние сети.

Маршрутизатор, изображенный слева, иначе называется многофункциональным устройством или интегрированным маршрутизатором. Он объединяет в себе коммутатор и точку беспроводного доступа. В некоторых случаях удобнее купить и настроить одно устройство, отвечающее всем потребностям, чем покупать отдельное устройство для каждой функции. Это особенно справедливо для небольшого или домашнего офиса. Многофункциональные устройства могут также иметь функции модема

АППАРАТНЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

Интегрированный маршрутизатор может также служить аппаратным межсетевым экраном. Аппаратные межсетевые экраны защищают данные и оборудование в сети от несанкционированного доступа. Аппаратный межсетевой экран располагается между двумя или более сетями, как показано на рисунке. Он не использует ресурсы компьютеров, которые защищает, следовательно, не влияет на производительность обработки данных.

В межсетевых экранах применяются различные методы определения разрешенного и запрещенного доступа к сегментам сети, например список контроля доступа (ACL). Этот список представляет собой файл, используемый маршрутизатором и содержащий правила относительно трафика между сетями.

ПРИ ВЫБОРЕ АППАРАТНОГО МЕЖСЕТЕВОГО ЭКРАНА СЛЕДУЕТ УЧИТЫВАТЬ СЛЕДУЮЩИЕ АСПЕКТЫ.

Занимаемое место — устройство устанавливается отдельно и использует специализированное оборудование.

Стоимость — начальная стоимость обновления оборудования и ПО может быть довольно высокой.

Число компьютеров — устройство обеспечивает защиту нескольких компьютеров.

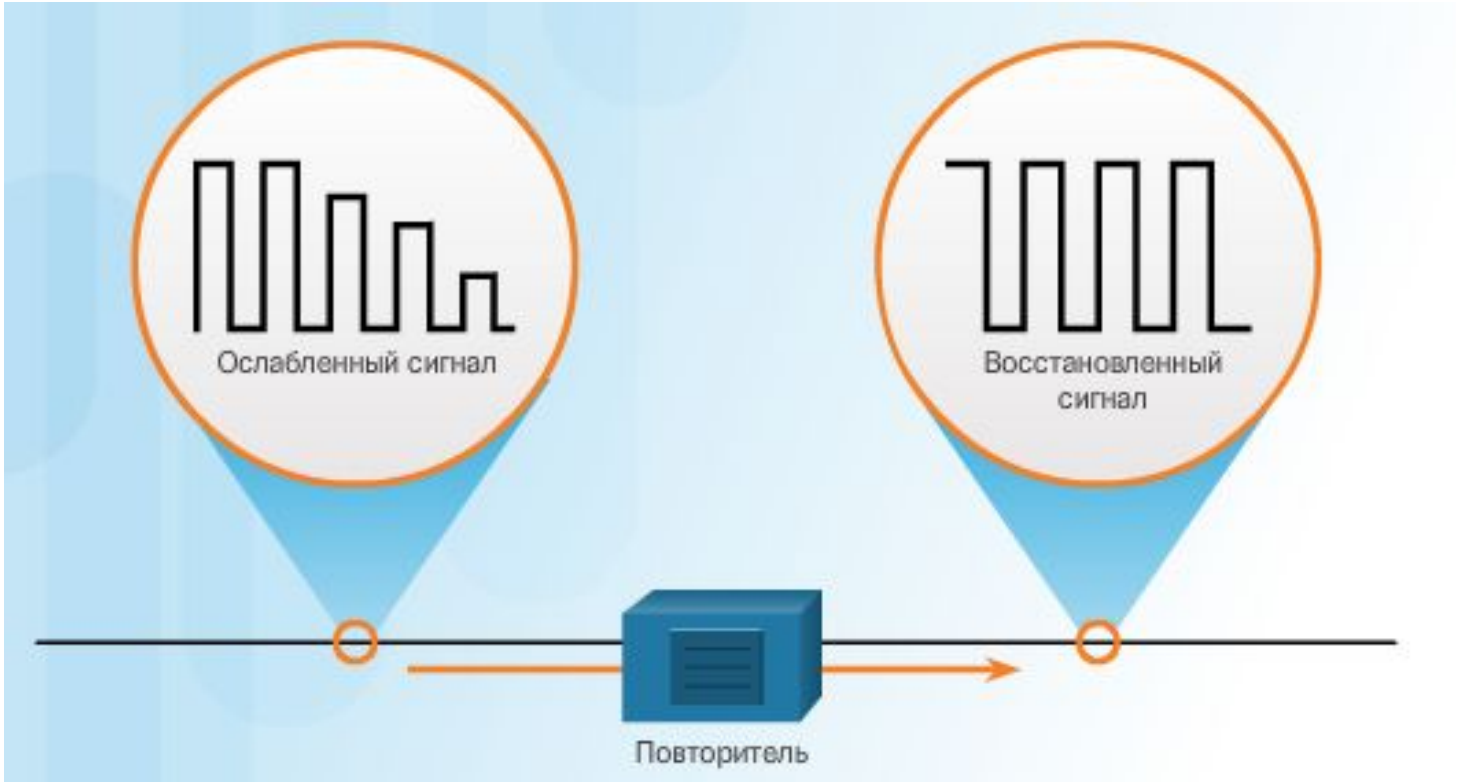
Требования к производительности — незначительное влияние на производительность

ДРУГИЕ УСТРОЙСТВА

КОММУТАЦИОННЫЕ ПАНЕЛИ

Коммутационная панель (или патч-панель), показанная на риске, обычно используется, чтобы собрать в одном месте входящие кабели от различных сетевых устройств. Она обеспечивает точку соединения компьютеров с коммутаторами или маршрутизаторами. Коммутационная панель может иметь или не иметь питание. Коммутационная панель с питанием может регенерировать слабые сигналы перед отправкой их на следующее устройство.

ПОВТОРИТЕЛИ



Регенерация слабых сигналов, показанная на рисунке, является основной функцией повторителей (repeater). Повторители также называются расширителями, поскольку они увеличивают расстояние, на которое можно передавать сигнал. В современных сетях повторители наиболее часто используются для регенерации сигналов в оптоволоконных кабелях.

ПИТАНИЕ ЧЕРЕЗ ETHERNET (POE)

Коммутатор с PoE (Power over Ethernet) передает по кабелю Ethernet вместе с данными постоянный ток небольшой мощности для питания устройств, поддерживающих PoE.

На низковольтные устройства, поддерживающие технологию PoE, такие как точки доступа Wi-Fi, устройства видеонаблюдения и IP-телефоны, питание можно подавать из удаленных местоположений. Устройства с поддержкой технологии PoE могут получать питание по подключениям Ethernet на расстояния до 100 м. Можно также подавать питание через кабель Ethernet с помощью промежуточного PoE-инжектора, показанного на рисунке.