Определение сети

Сети — это системы, формируемые соединениями. Например, дороги, соединяющие группы людей, формируют физическую сеть. Связи между вами и вашими друзьями формируют вашу личную сеть. Веб-сайты, позволяющие отдельным пользователям связываться со страницами друг друга, называются социальными

Узлы(хост)

Узел (хост) — это любое устройство, отправляющее и получающее информацию по сети. Принтер, подключенный к ноутбуку, является периферийным устройством. Если же принтер подключен к сети напрямую, он функционирует в качестве узла.

Компьютерные сети используются

Компьютерные сети используются в организациях, школах, государственных учреждениях и дома. Многие сети подключены друг к другу через Интернет. В сети можно совместно пользоваться ресурсами различных типов

- 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

Компьютерные сети содержат множество устройств, находящихся между узлами. Эти промежуточные устройства обеспечивают передачу данных с одного узла на другой.

Среды передачи данных

Обмен данными по сети осуществляется в сетевой среде. Сетевая среда создает канал, по которому сообщение передается от источника к получателю. Существует несколько типов сетевых сред.

- **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

Пропускная способность и задержка

Пропускная способность сети аналогична количеству полос автотрассы. Количество полос автотрассы — это количество автомобилей, которые могут одновременно ехать по трассе. Трасса с восемью полосами может пропустить в четыре раза больше автомобилей, чем двухполосная. В этом примере автомобили и грузовики представляют собой данные.

- бит/с — бит в секунду
- Кбит/с — килобит в секунду
- Мбит/с — мегабит в секунду
- Гбит/с — гигабит в секунду

Количество времени, которое тратится на передачу данных от источника получателю, называется **задержкой**

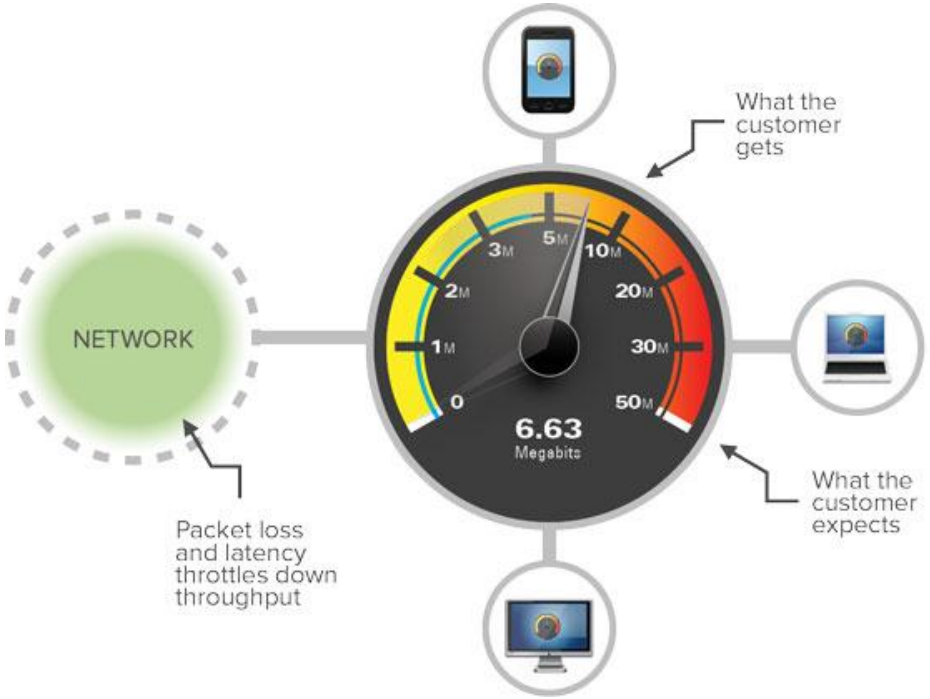
На пути автомобиля по городу встречаются красные сигналы светофора или объезды. Передача данных замедляется в зависимости от сетевых устройств и длины кабелей. Сетевые устройства увеличивают задержку при обработке и пересылке данных.

О битах, байтах и скорости интернет соединения

Бит это самая наименьшая единица измерения количества информации. Наравне с битом активно используется байт. Байт равен 8 бит.

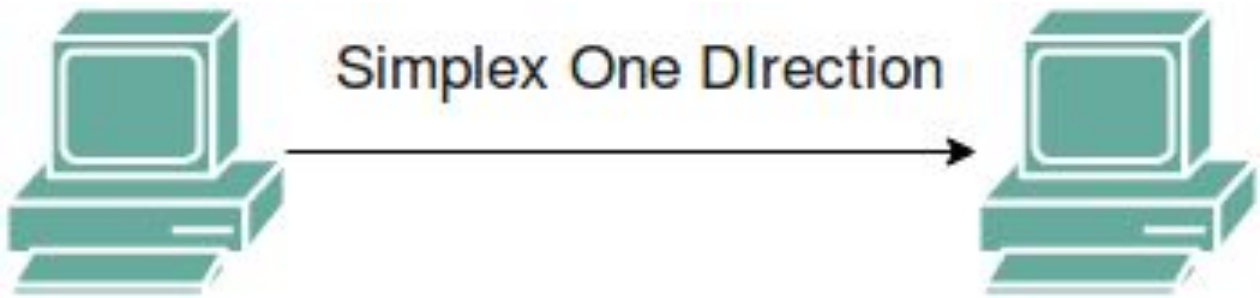
Название	Аббревиатура английская	Аббревиатура русская	Значение
бит	bit (b)	б	0 или 1
байт	Byte (B)	Б	8 бит
килобит	kbit (kb)	кбит (кб)	1000 бит
килобайт	KByte (KB)	КБайт (КБ)	1024 байта
мегабит	mbit (mb)	мбит (мб)	1000 килобит
мегабайт	MByte (MB)	МБайт (МБ)	1024 килобайта
гигабит	gbit (gb)	гбит (гб)	1000 мегабит
гигабайт	GByte (GB)	ГБайт (ГБ)	1024 мегабайта

Подключения это количество получаемой или отправляемой вашим компьютером информации в единицу времени. В качестве единицы времени в данном случае принято считать секунду а в качестве количества информации кило или мегабит.



Таким образом, если ваша скорость 128 Kbps это означает, что ваше соединение имеет пропускную способность 128 килобит в секунду или же 16 килобайт в секунду.

Передача данных



СИМПЛЕКСНЫЙ РЕЖИМ

В этом типе режима передачи связь является однонаправленной, то есть данные могут передаваться только в одном направлении. Это означает, что вы не можете отправить сообщение обратно отправителю, как на улице с односторонним движением.

Примером симплексной передачи является сигнал, отправляемый с телевизионной станции на домашний телевизор.

ПРЕИМУЩЕСТВО СИМПЛЕКСНОГО РЕЖИМА

В этом режиме станция может использовать всю пропускную способность канала связи, поэтому одновременно может передаваться больше данных.

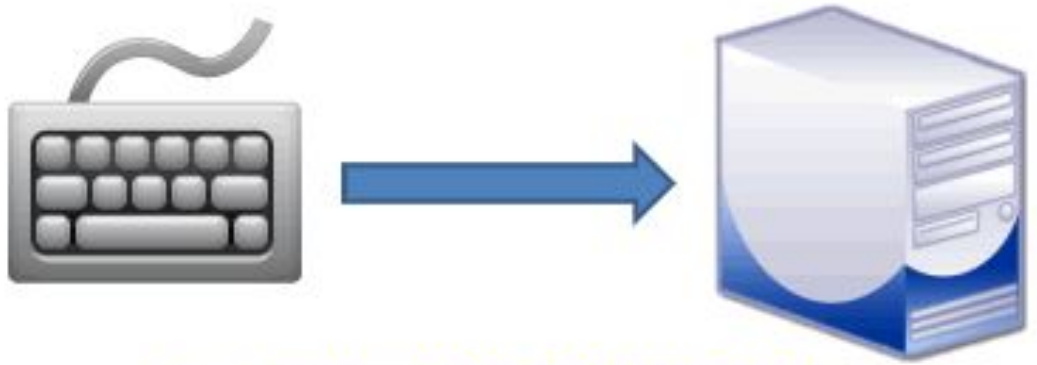


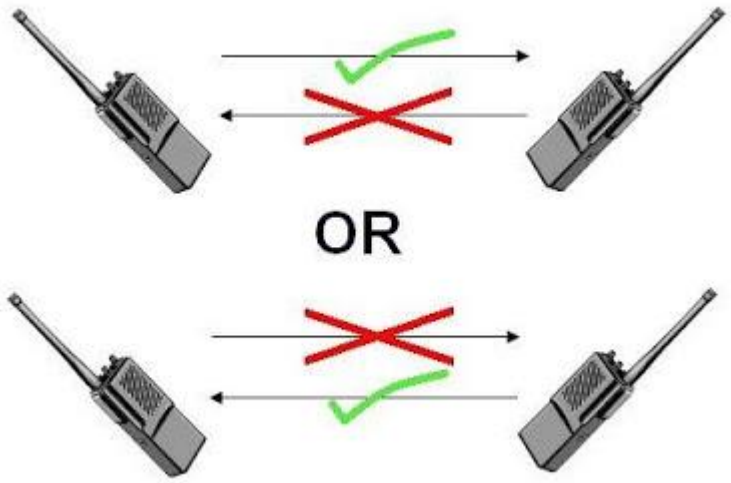
Fig: Simplex Mode of Transmission

НЕДОСТАТОК СИМПЛЕКСНОГО РЕЖИМА

В основном коммуникации требуют двустороннего обмена данными, но это однонаправленный обмен, поэтому здесь нет связи между устройствами.

Полудуплексный режим

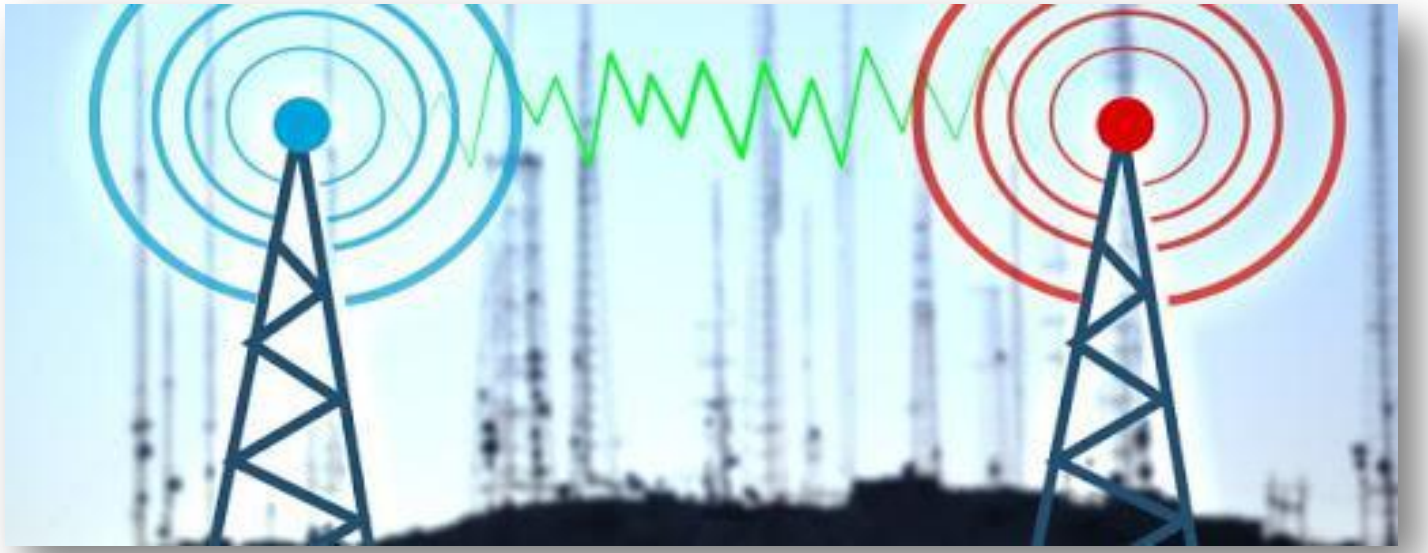
Передача данных, при которой в каждый момент времени можно отправлять сообщение только в одном направлении, называется полудуплексной



Пример:
Это как однополосная дорога с двунаправленным движением. Пока машины едут в одном направлении, машины, идущие в другую сторону, должны ждать.

ПРЕИМУЩЕСТВО ПОЛУДУПЛЕКСНОГО РЕЖИМА

В полудуплексном режиме вся пропускная способность канала берется на себя любым из двух устройств, передающих одновременно.

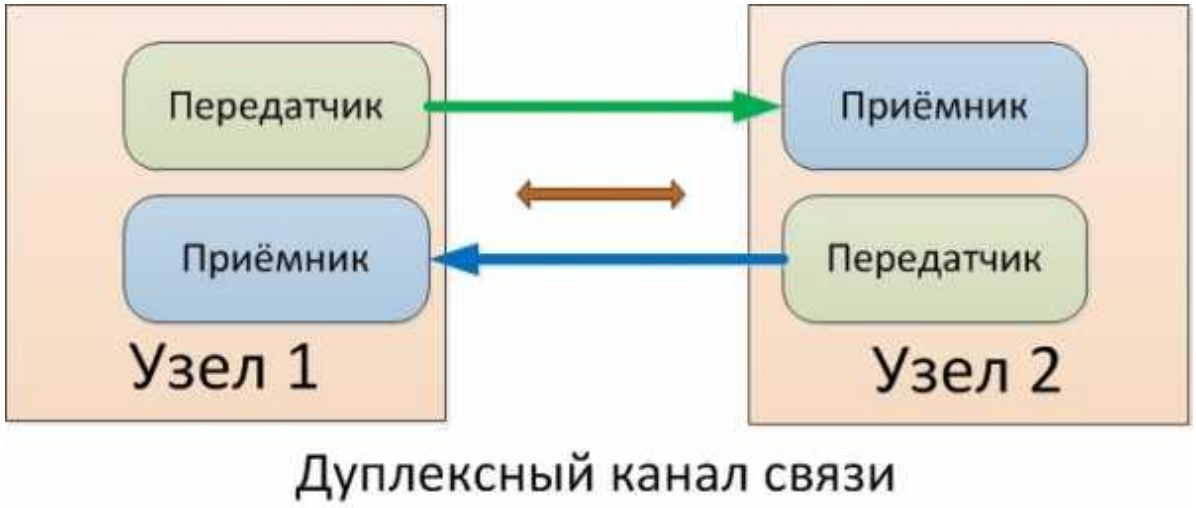


НЕДОСТАТОК ПОЛУДУПЛЕКСНОГО РЕЖИМА

Это вызывает задержку в отправке данных в нужное время, так как когда одно устройство отправляет данные, то другое должно ждать отправки данных.

Полнодуплексный режим

Передача данных в обоих направлениях одновременно называется полнодуплексной



Пример:
По телефонной линии два человека общаются друг с другом, оба могут говорить и слушать друг друга одновременно, это полнодуплексная передача.

Другой пример – улица с двусторонним движением, движение по которой осуществляется одновременно в обоих направлениях.

ПРЕИМУЩЕСТВО ПОЛНОДУПЛЕКСНОГО РЕЖИМА

Обе станции могут отправлять и получать данные одновременно, поэтому емкость канала может быть разделена.

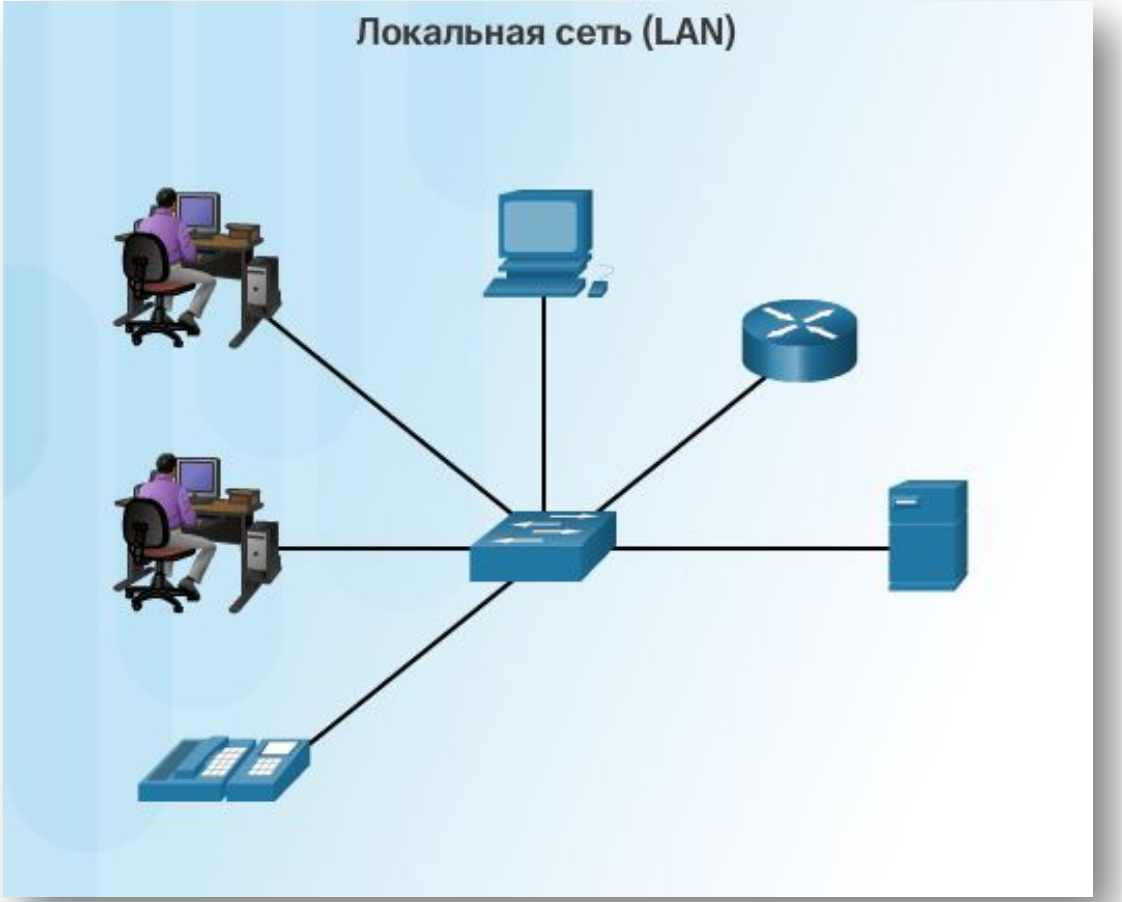
НЕДОСТАТОК ПОЛНОДУПЛЕКСНОГО РЕЖИМА

Полоса пропускания канала связи делится на две части, если между устройствами нет выделенного пути.

Локальные сети

Компьютерные сети отличаются следующими специфическими характеристиками:

- Площадь покрытия
- Количество подключенных пользователей
- Количество и типы доступных служб
- Область ответственности



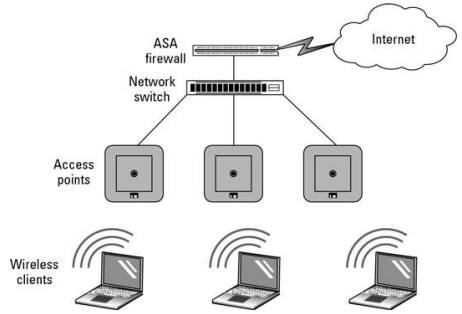
Традиционно локальная сеть (LAN) определяется как сеть, охватывающая небольшую географическую область. Однако характерной особенностью современной локальной сети является то, что она обычно принадлежит одному человеку, например хозяину дома или малого предприятия, или управляется ИТ-отделом, например в школе или компании. Этот человек или группа применяют к сети политики безопасности и контроля доступа.

Беспроводная локальная сеть (WLAN)

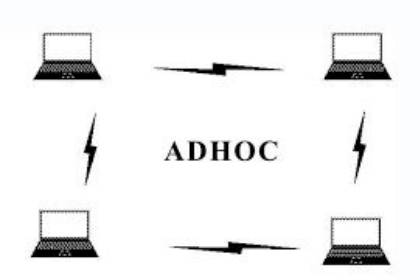
Беспроводная локальная сеть (WLAN) — это локальная сеть, в которой для передачи данных между беспроводными устройствами используются радиоволны.

Виды беспроводных локальных сетей

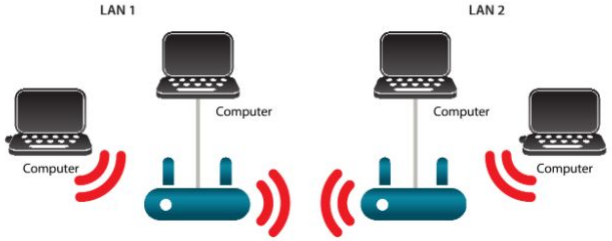
- **Infrastructure Mode.** Это система, когда все беспроводные устройства общаются между собой с помощью отдельной точки доступа. Подключение осуществляется с помощью индикатора.



- **Adhoc.** Это особенный режим, который позволяет вообще не использовать точку доступа. Связь в данной ситуации обеспечивается непосредственно между устройствами. Этот режим называют иначе равный с равным.



- **Access Point Bridge.** Это тот случай, когда беспроводная технология расширяет возможности сети. В этой ситуации точка доступа подключается не только к устройствам, но и к коммутатору, что обеспечивает соединение проводной и беспроводной сети.



- **Point-to-point** – это специальная система соединения двух проводных сетей с помощью точки доступа беспроводной сети.

Можно выделить сразу несколько сфер использования данной сети:

- Создание беспроводных локальных сетей. Они помогают работать в самых разнообразных конторах. С помощью подобной связи сотрудники с легкостью обмениваются информацией и документами.

- Расширение возможностей сетей – теперь можно попасть в интернет из любой точки, и он будет работать стабильно и с высокой скоростью.

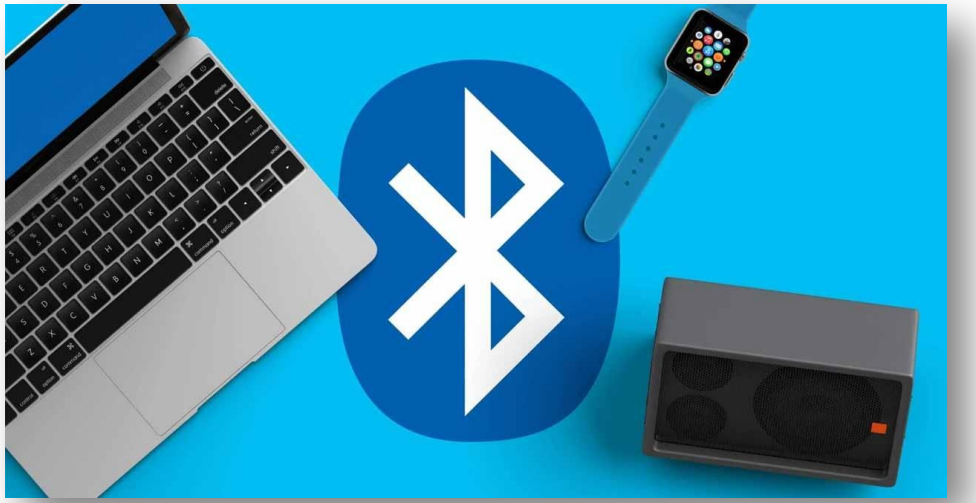
- Универсальный доступ. В зоне покрытия этой сети очень легко войти в интернет с любого устройства.

Персональная сеть (PAN) Bluetooth(7 2,4 до 2,485 ГГц).

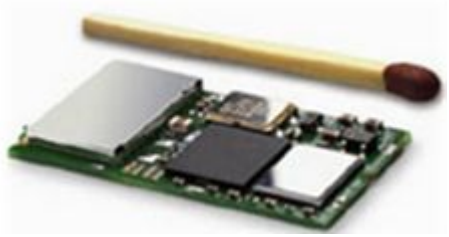
Персональная сеть (PAN) подключает устройства, такие как мыши, клавиатуры, принтеры, смартфоны и планшетные ПК, находящиеся в пределах досягаемости отдельного пользователя. Все эти устройства подключаются к одному узлу, чаще всего с помощью технологии Bluetooth.

Bluetooth

Bluetooth позволяет этим устройствам общаться, на расстоянии от 1 до 100 метров друг от друга (дальность сильно зависит от преград и помех), даже в разных помещениях.



Bluetooth - это маленький чип , представляющий собой высокочастотный (2.4 - 2.48 ГГц) приёмопередатчик.



Безопастность *Bluetooth*

Устройства с Bluetooth 4.0 и 5.0 оказались подверженными взлому, и это нельзя исправить

Исследователи из США и Швейцарии независимо друг от друга обнаружили новую уязвимость в некоторых реализациях протокола Bluetooth версий от 4.0 до 5.0. С помощью неё злоумышленники могут получить полный доступ к смартфону путём перезаписи ключей, необходимых для сопряжения устройств. Уязвимость получила название BLURtooth.

Безопастность *Bluetooth*

В зависимости от выполняемых задач спецификация Bluetooth предусматривает три режима защиты, которые могут использоваться как по отдельности, так и в различных комбинациях:

1. В первом режиме — минимальном (который обычно применяется по умолчанию) — никаких мер для безопасного использования Bluetooth-устройства не предпринимается. Данные кодируются общим ключом и могут приниматься любыми устройствами без ограничений.
2. Во втором режиме осуществляется защита на уровне устройств, то есть активируются меры безопасности, основанные на процессах опознания/аутентификации (authentication) и разрешения/авторизации (authorization). В этом режиме определяются различные уровни доверия (trust) для каждой услуги, предложенной устройством. Уровень доступа может указываться непосредственно в чипе, и в соответствии с этим устройство будет получать определенные данные от других устройств.
3. Третий режим — защита на уровне сеанса связи, где данные кодируются 128-битными случайными числами, хранящимися в каждой паре устройств, участвующих в конкретном сеансе связи. Этот режим требует опознания и использует кодировку/шифрование данных (encryption).

RFID

RFID использует частоты в диапазоне от 125 до 960 МГц для уникальной идентификации объектов, например, в отделах отгрузки продукции, как показано на рисунке. Активные RFID-метки со встроенной батареей могут транслировать идентификатор на расстояние до 100 метров.

Для работы с пассивными RFID-метками требуется RFID-сканер, генерирующий радиоволны для активации и считывания метки. Пассивные RFID-метки обычно используются для сканирования на близком расстоянии, однако радиус их действия может достигать 25 м.

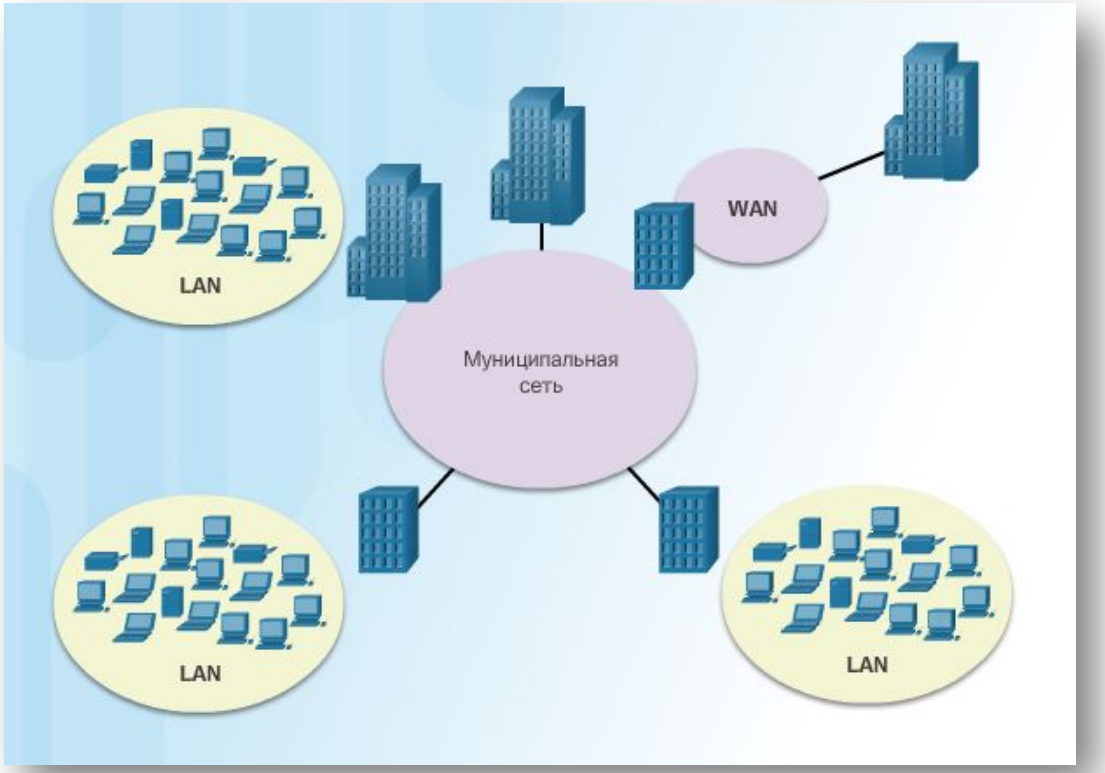
NFC

Технология NFC работает на частоте 13,56 МГц и является подмножеством стандартов RFID. NFC предназначена для выполнения безопасных транзакций. Например, покупатель может оплачивать товары или услуги, проводя телефоном возле платежного терминала

На основании уникального идентификатора сумма оплаты списывается напрямую с банковского счета. Технология NFC также используется в общественном транспорте, на общественных парковках и во многих других областях.

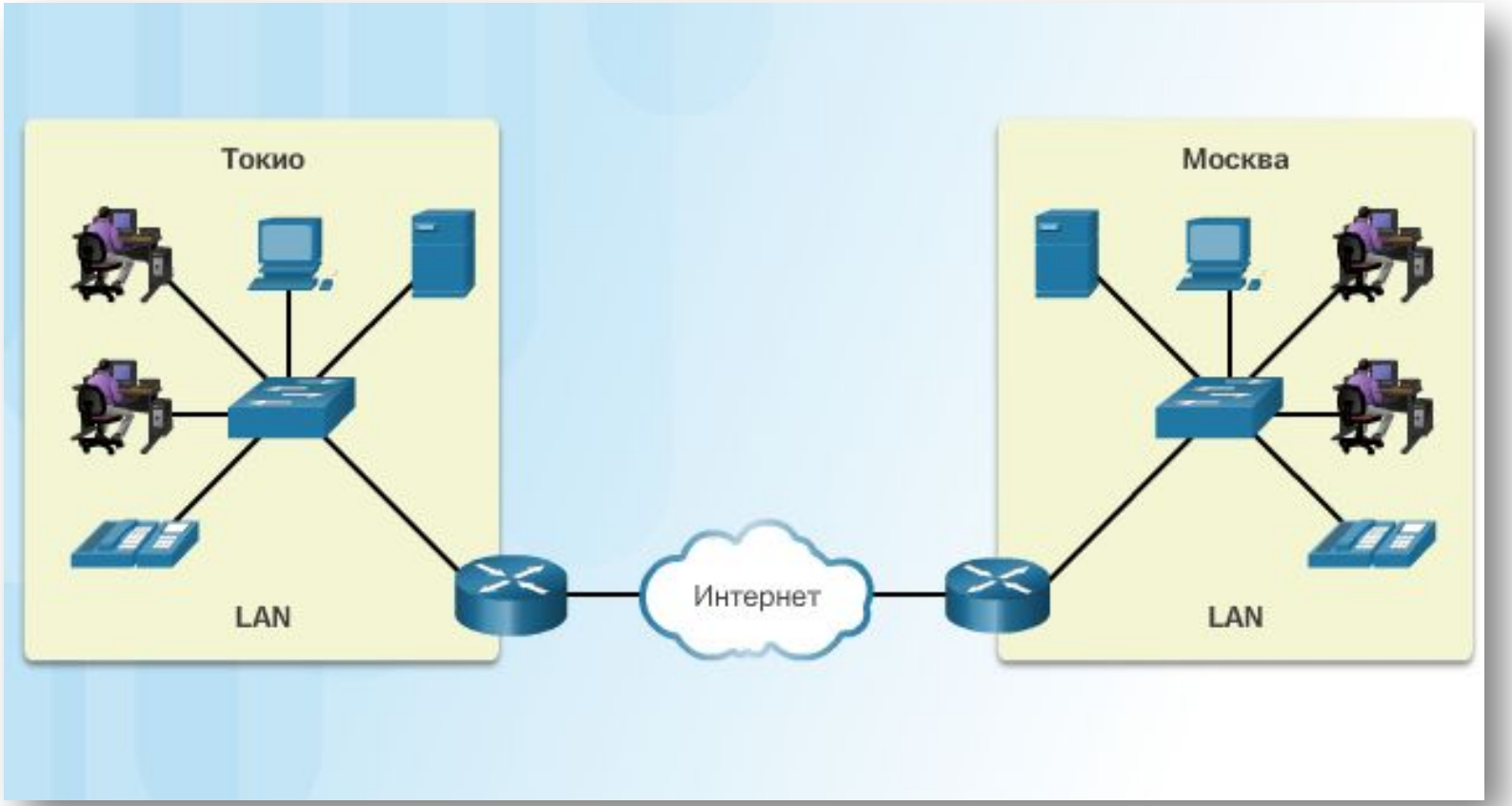
Муниципальные сети (MAN)

Муниципальная сеть (Metropolitan Area Network — MAN) — это сеть, развертываемая в крупном комплексе зданий или на территории целого города.



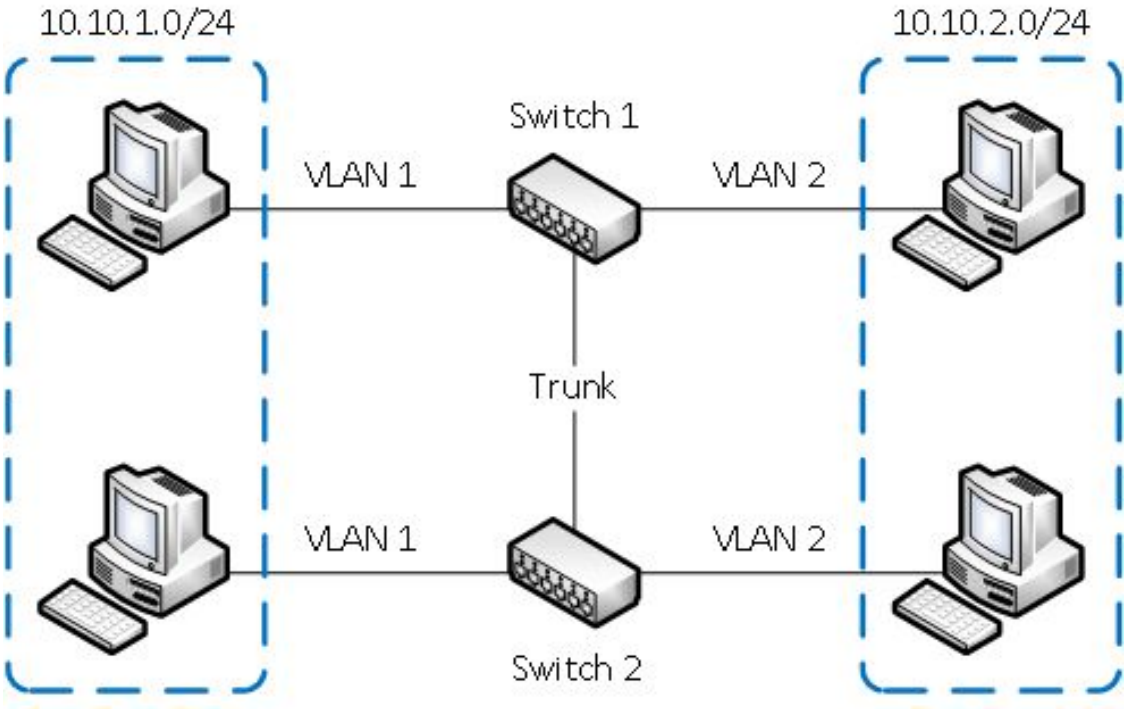
Глобальные сети WAN

Глобальная сеть (WAN) соединяет несколько локальных сетей, расположенных в разных географических местоположениях.

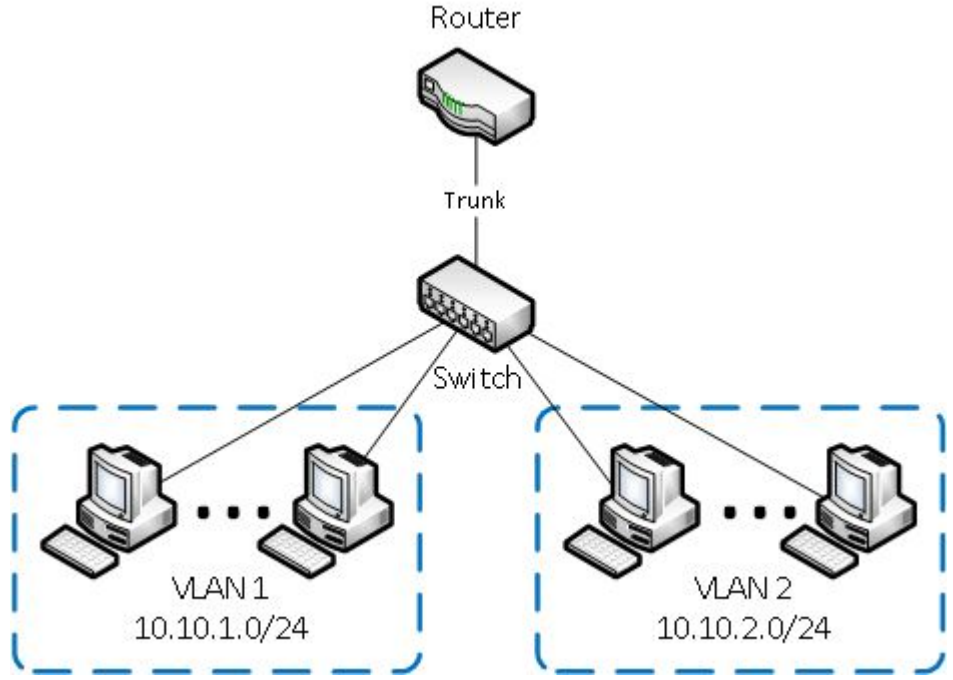


VLAN (Virtual Local Area Network, виртуальная локальная сеть)

это функция в роутерах и коммутаторах, позволяющая на одном физическом сетевом интерфейсе (Ethernet, Wi-Fi интерфейсе) создать несколько виртуальных локальных сетей. VLAN используют для создания логической топологии сети, которая никак не зависит от физической топологии.



Объединение в единую сеть компьютеров, подключенных к разным коммутаторам.



Разделение в разные подсети компьютеров, подключенных к одному коммутатору.

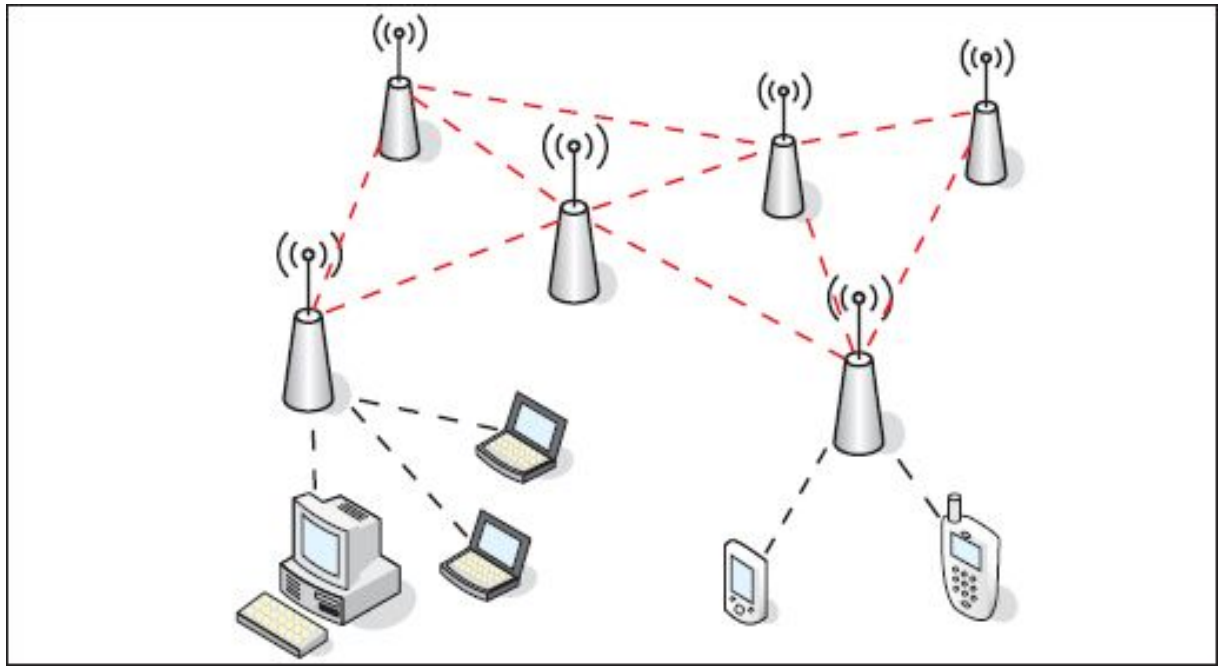
Достоинства использования VLAN

- **Гибкое разделение устройств на группы**
  Как правило, одному VLAN соответствует одна подсеть. Компьютеры, находящиеся в разных VLAN, будут изолированы друг от друга. Также можно объединить в одну виртуальную сеть компьютеры, подключенные к разным коммутаторам.
- **Уменьшение широковещательного трафика в сети**
  Каждый VLAN представляет отдельный широковещательный домен. Широковещательный трафик не будет транслироваться между разными VLAN. Если на разных коммутаторах настроить один и тот же VLAN, то порты разных коммутаторов будут образовывать один широковещательный домен.
- **Увеличение безопасности и управляемости сети**
  В сети, разбитой на виртуальные подсети, удобно применять политики и правила безопасности для каждого VLAN. Политика будет применена к целой подсети, а не к отдельному устройству.
- **Уменьшение количества оборудования и сетевого кабеля**
  Для создания новой виртуальной локальной сети не требуется покупка коммутатора и прокладка сетевого кабеля. Однако вы должны использовать более дорогие управляемые коммутаторы с поддержкой VLAN.

Беспроводная ячеистая сеть (WMN) представляет собой коммуникационная сеть из радио узлов , организованных в виде сетчатой топологии . Это также может быть форма беспроводной одноранговой сети .

WMN

Беспроводная ячеистая сеть (WMN) использует несколько точек доступа для расширения покрытия сети WLAN. В топологии присутствует беспроводной маршрутизатор. Две беспроводных точки доступа расширяют покрытие сети WLAN внутри дома. Коммерческие предприятия и муниципальные организации также могут использовать сети WMN для быстрого расширения зоны покрытия.



VPN (англ. Virtual Private Network — виртуальная частная сеть) — это безопасное, зашифрованное подключение между двумя сетями или между отдельным пользователем и сетью. Сети VPN позволяют пользоваться Интернетом, сохраняя конфиденциальность.

Например, компания, в которой вы работаете, может использовать виртуальную частную сеть для удалённых сотрудников. С помощью VPN они подключаются к рабочей сети

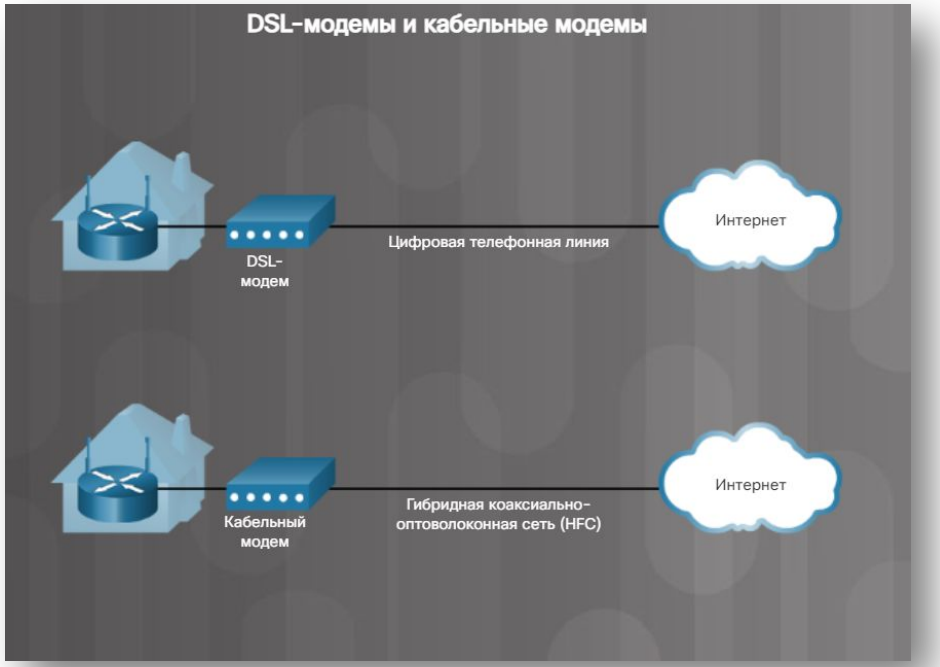
Сейчас встроенные VPN-клиенты есть во всех актуальных операционных системах, в том числе в Android, iOS, Windows, macOS и Linux.

Цифровая абонентская линия (DSL), кабельная и оптоволоконная линии

DSL относится к непрерывно доступным службам, т. е. нет необходимости каждый раз набирать номер для подключения к Интернету. Голос и данные передаются по медному телефонному кабелю на разных частотах. Специальный фильтр предотвращает взаимные помехи между сигналами DSL и телефонными сигналами.

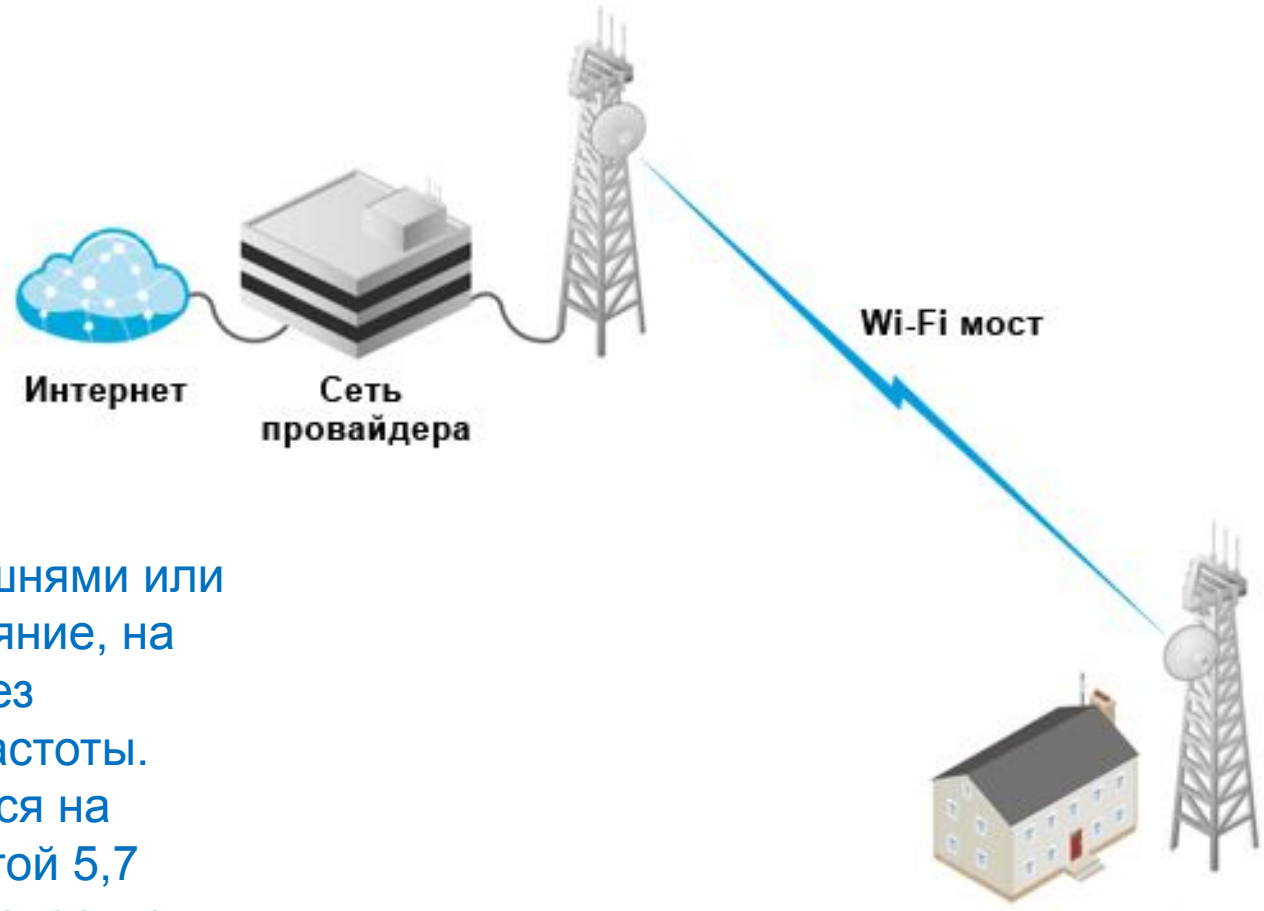
Кабельная линия

Для кабельного подключения к Интернету телефонная линия не нужна. В этом случае используется коаксиальный кабель, изначально предназначенный для передачи кабельного телевидения



Беспроводной доступ к Интернету в зоне прямой видимости

для доступа к Интернету используется радиосигнал. Радиосигнал от вышки поступает в приемник, который пользователь подключает к компьютеру или сетевому устройству. При этом вышка должна находиться в зоне прямой видимости от абонента.



Вышка может быть соединена с другими башнями или с магистральным интернет-каналом. Расстояние, на которое может передаваться радиосигнал без существенной потери качества зависит от частоты. Сигнал частотой 900 МГц может передаваться на расстояния до 65 км, тогда как сигнал частотой 5,7 ГГц — всего на 3 км. На уровень сигнала и качество связи могут влиять погодные условия, деревья и высокие здания.

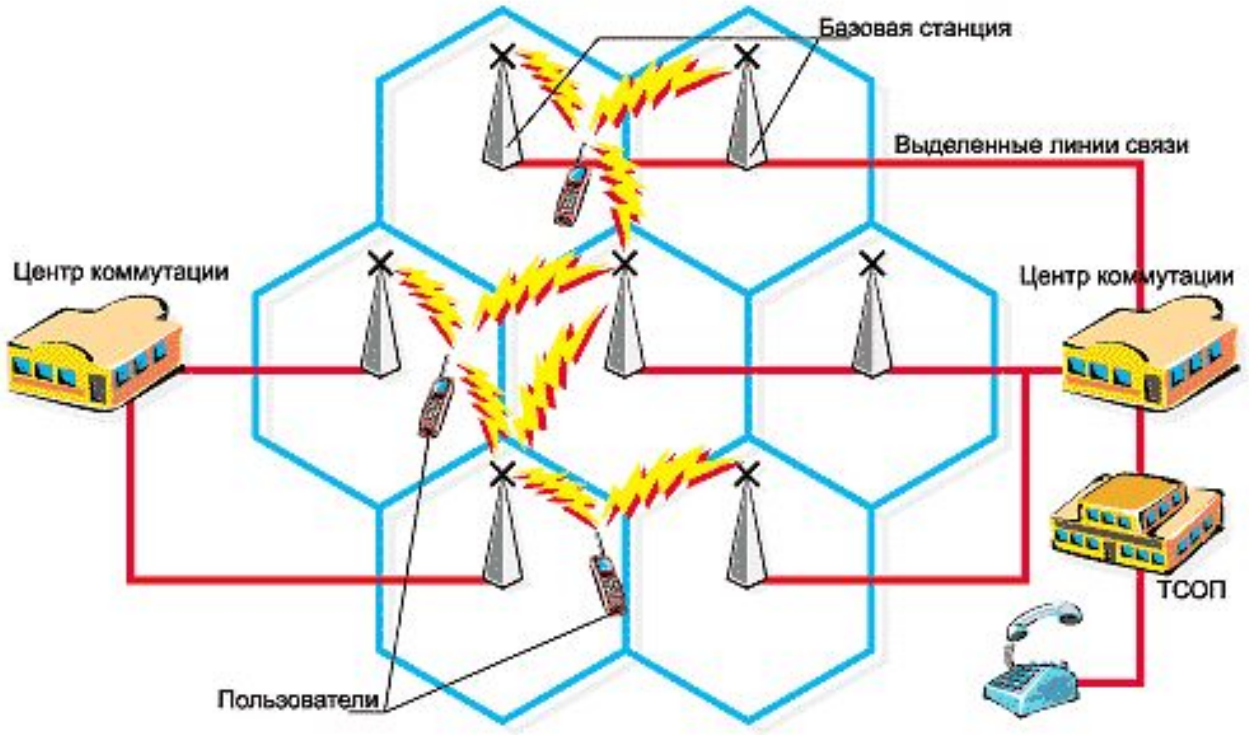
Спутниковая линия

это альтернативный вариант для тех клиентов, у которых нет доступа к кабельным или DSL-подключениям.

Скорость получения данных может достигать 10 Мбит/с и более, тогда как скорость отправки примерно в десять раз меньше.

Сотовая линия

Технология сотовой связи основывается на сети башен, охватывающих зону покрытия пользователей и обеспечивающих бесперебойный доступ к услугам сотовой связи и к Интернету.

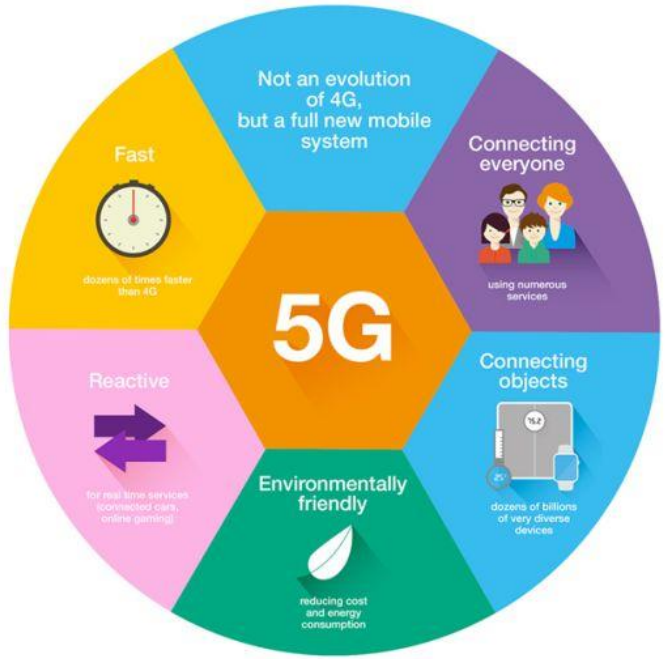


Сотовая связь

- **1G** — только аналоговая голосовая связь
- **2G** — цифровая голосовая связь, конференц-связь и идентификация вызывающего абонента; скорость передачи данных ниже 9,6 Кбит/с
- **2.5G** — скорость передачи данных от 30 Кбит/с до 90 Кбит/с; поддерживает просмотр веб-страниц, коротких аудиозаписей и видеоклипов, загрузку игр, приложения и мелодий вызова
- **3G** — скорость передачи данных от 144 Кбит/с до 2 Мбит/с; поддерживает полноценный просмотр видео, потоковую музыку, 3D-игры и ускоренный просмотр веб-страниц
- **3.5G** — скорость передачи данных от 384 Кбит/с до 14,4 Мбит/с; поддерживает высококачественное потоковое видео, высококачественную видеоконференц-связь и IP-телефонию
- **4G** — скорость передачи данных от 5,8 Мбит/с до 672 Мбит/с (мобильная связь) или до 1 Гбит/с (стационарная связь); поддерживает передачу голоса по IP, игровые услуги, высококачественное потоковое мультимедиа и IPv6

5G

- Стандарт 5G был принят в июне 2018 года, сейчас он внедряется только в отдельных регионах.
- 5G поддерживает широкий спектр приложений, включая дополненную реальность (AR), виртуальную реальность (VR), умные дома, умные автомобили и любые другие сценарии, предполагающие обмен данными между устройствами.
- Скорость: от 400 Мбит/с до 3 Гбит/с (получение данных); от 500 Мбит/с до 1,5 Гбит/с (передача данных).



6G

После развертывания сетей сотовой связи 5 поколения 5G усилился интерес ученых и инженеров к разработке оборудования следующего поколения сотовой связи. Специалисты сходятся во мнении, что в нем получат дальнейшее развитие подходы, недостаточно полно реализованные в предыдущем поколении, основанные на применении искусственного интеллекта, квантовых коммуникаций, что позволит достичь скорости передачи данных от сотен Гбит/с до 1 ТБит/с.

Сотовые сети используют по крайней мере одну из следующих технологий:

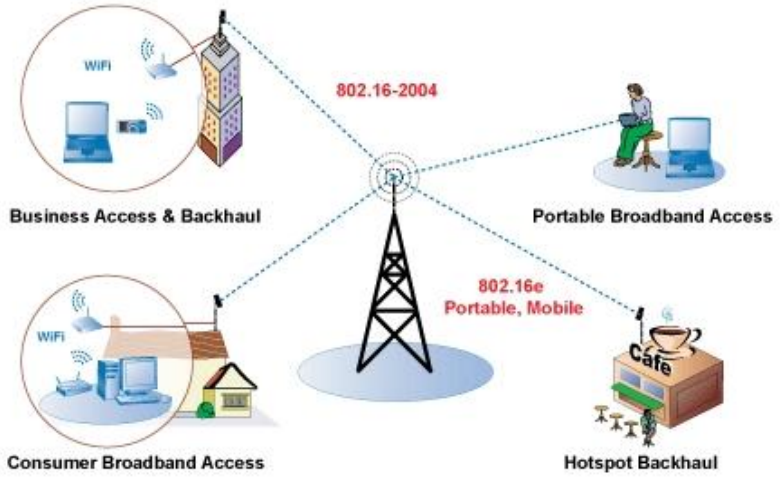
- **Глобальная система мобильной связи (GSM)** — стандарт, используемый для сотовой связи по всему миру
- **Система пакетной радиосвязи общего назначения (GPRS)** — служба передачи данных для пользователей GSM
- **Четырехдиапазонная связь** — позволяет сотовому телефону работать на всех четырех частотах GSM: 850 МГц, 900 МГц, 1800 МГц и 1900 МГц
- **Служба коротких сообщений (SMS)** — служба передачи данных, используемая для отправки и получения текстовых сообщений
- **Служба мультимедийных сообщений (MMS)** — служба передачи данных, используемая для отправки и получения текстовых сообщений, которые могут включать в себя мультимедийное содержимое
- **Enhanced Data Rates for GSM Evolution (EDGE)** — повышение скорости передачи данных и их надежности цифровая технология беспроводной передачи данных для мобильной связи, которая функционирует как надстройка над 2G и 2.5G (GPRS)-сетями

EV-DO (Evolution-Data Only) - технология высокоскоростной передачи данных, используемая в сетях сотовой связи стандарта CDMA. Максимальная скорость загрузки в сетях CDMA2000 1x EV-DO rev.A - до 3,1 Мбит/с, в сетях EV-DO rev.B - до 73,5 Мбит/с.

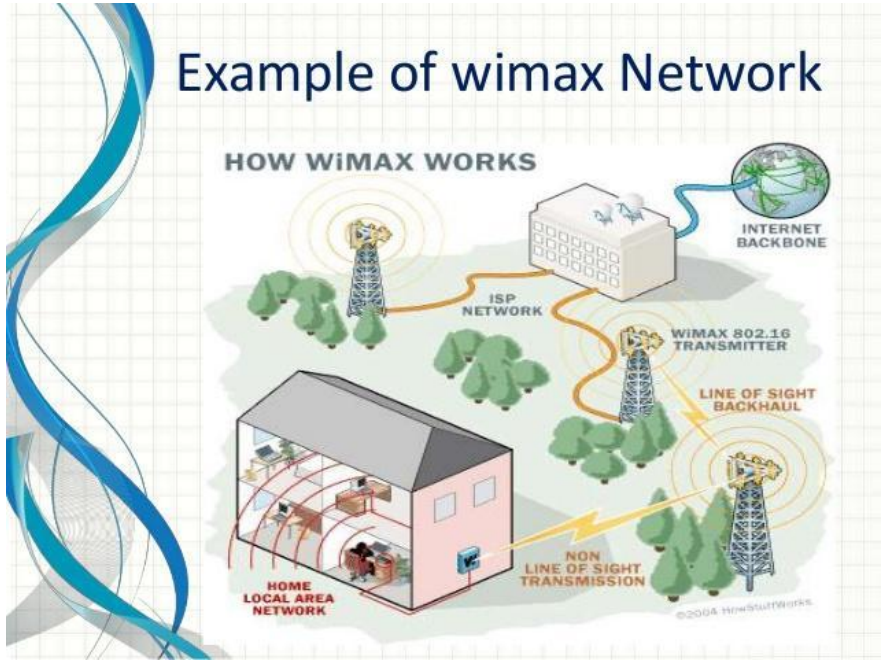
HSDPA (*High-Speed Downlink Packet Access* — высокоскоростная пакетная передача данных от базовой станции к мобильному телефону) — протокол передачи данных мобильной связи 3G (третьего поколения) из семейства HSPA.

WiMAX

стандартная технология беспроводной связи для обеспечения высокоскоростного широкополосного подключения на большие расстояния для внутренних и коммерческих целей. Это технология беспроводного мобильного доступа 4-го поколения.



Радиус действия WiMAX обеспечивает связь как при прямой видимости, так и вне ее. Для связи с прямой видимостью, с помощью сильных антенн, возможна зона покрытия до 9300 квадратных километров. Нелинейная связь с помехами подобна Wi-Fi-соединению, и охватывает радиус около 50 км.



Принцип работы WiMAX аналогичен принципу Wi-Fi. Компьютер или ноутбук, оснащенные WiMAX, будут получать данные от передающей станции, используя зашифрованные ключи данных. Система WiMAX состоит из вышки (базовой станции) и приемника WiMAX. Базовая станция может обеспечить покрытие большой площади, в то время как приемник WiMAX может быть ноутбуком или PCMCIA картой, который принимает сигналы от БС. Станция на вышке может быть подключена непосредственно к Интернету с использованием высокоскоростной полосы пропускания, проводного соединения или другой базовой станции с WiMAX.

IEEE стандарты WiMAX & Wifi

В то время как Wi-Fi основан на стандарте IEEE 802.11, WiMAX основан на стандарте IEEE 802.16. Стандарт IEEE 802.11 (рабочая группа LAN) используется для обеспечения беспроводной связи на короткие расстояния по беспроводной локальной сети (WLAN). Популярные версии: IEEE 802.11b, 802.11g, 802.11n, 802.11 ac и 802.11ac wave2. Стандарт IEEE 802.16 (рабочая группа широкополосного беспроводного доступа) подобен стандарту IEEE 802.11 в архитектуре, но отличается тем, что он обеспечивает стандарты для широкополосных беспроводных городских сетей (WMAN).

Диапазон рабочей частоты

Более высокий частотный диапазон был установлен исходным стандартом 802.16a, тогда как нижний частотный диапазон был установлен позже стандартом 802.16d, что позволяет уменьшить затухание и улучшить характеристики. В то время как диапазон частот от 2,5 до 3,5 ГГц лицензируется, частотный спектр 5,8 ГГц не имеет лицензии.

Тип связи

WiMAX поддерживает полнодуплексную связь

Безопасность

WiMAX использует протоколы безопасности, такие как протокол управления ключами секретности 2 (PKMP2), протокол расширяемой аутентификации (EAP) и стандарт расширенного шифрования (EAS). Эти протоколы обеспечивают защиту качества обслуживания (QoS) как аудио-, так и видеопотоков

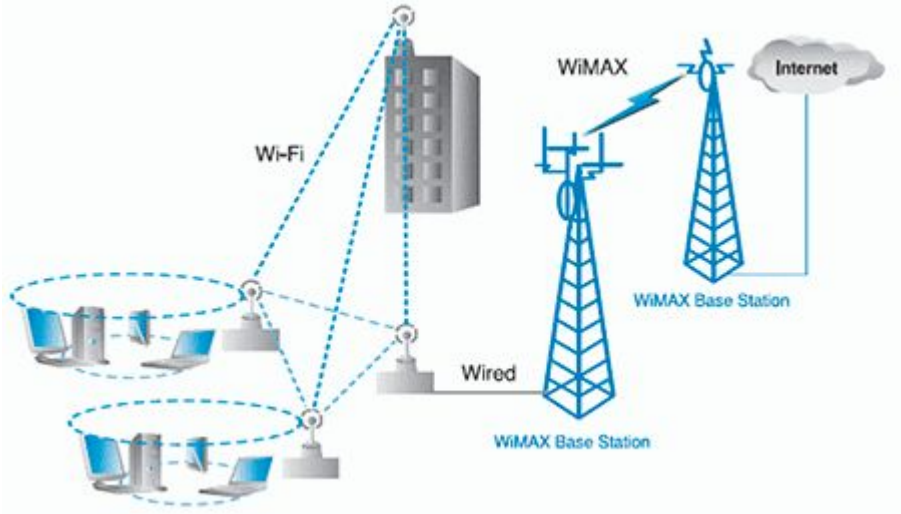
Будущее с WiMAX

WiMAX, похоже, является многообещающей платформой беспроводной сети следующего поколения с высокой скоростью и большими возможностями зоны покрытия. Он не требует прямой видимости и может эффективно использовать полосы пропускания. В настоящее время ожидается, что WiMAX заменит существующие технологии DSL и другие кабельные широкополосные технологии, так как различные компании используют WIMAX для обеспечения широкополосных соединений. Он также может быть заменой для технологий мобильной связи, таких как GSM и CDMA. Используя WiMAX, можно создавать соединения точка-точка.

WiMAX использует передачу по УКВ (ультракоротким волнам), обычно на частотах от 2 до 11 ГГц. Волны этих частот, в отличие от волн более высоких частот, лучше преодолевают физические препятствия, поскольку они могут лучше их огибать.

Существуют два способа передачи сигнала в сетях WiMAX:

- **Fixed WiMAX** (Фиксированный WiMAX) — сеть «точка-точка» или «точка-многоточка» со скоростью до 72 Мбит/с на расстоянии до 50 км.
- **Mobile WiMAX** (Мобильный WiMAX) — мобильная служба, похожая на Wi-Fi, но с более высокими скоростями и большей дальностью передачи.



Мобильная точка доступа и раздача Интернета с мобильного телефона

Такое подключение, так называемую «раздачу подключения к сети», можно организовать с помощью Wi-Fi, Bluetooth или кабеля USB. Подключенные устройства могут выходить в Интернет через подключение сотового телефона. Сотовый телефон, который разрешает устройствам Wi-Fi устанавливать соединение и использовать мобильную сеть, именуется мобильной точкой доступа.

Раздача интернета. Точка доступа Wi-Fi

ZigBee и Z-Wave

Zigbee and Z-Wave — это два стандарта для технологий «умного дома», которые позволяют пользователям объединять несколько устройств в беспроводную ячеистую сеть. Обычно для управления подключенными устройствами используют смартфон

Zigbee

Протокол Zigbee использует компактные маломощные цифровые радиопередатчики на основе стандарта IEEE 802.15.4 для персональных беспроводных сетях с низкой скоростью передачи данных (LR-WPAN), которые ориентированы на применение недорогих, низкоскоростных устройств. Zigbee использует частотный диапазон от 868 МГц до 2,4 ГГц, дальность связи не превышает 10-20 метров. Скорость передачи данных по протоколу Zigbee варьируется в пределах от 40 до 250 кбит/с, общее количество подключенных устройств может достигать 65 000.

Z-Wave

Z-Wave — это проприетарный стандарт, который в настоящее время принадлежит компании Silicon Labs. Однако в 2016 году была представлена открытая версия Z-Wave (для уровня взаимодействия). К открытым стандартам Z-Wave относятся стандарт безопасности S2, Z/IP для передачи сигналов Z-Wave по IP-сетям, а также межплатформенное ПО Z-Ware.

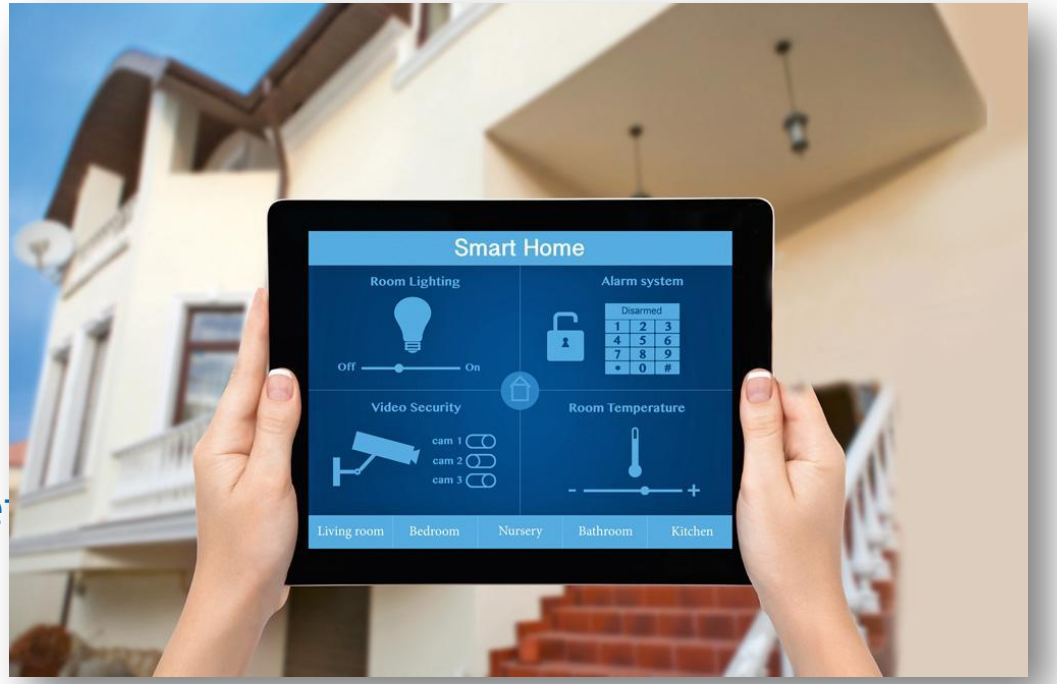
В разных странах Z-Wave работает на разных частотах: от 865,2 МГц в Индии до 922-926 МГц в Японии. В Северной Америке Z-Wave использует частоту 908,42 МГц. Z-Wave может передавать данные на расстояние до 100 м, но при этом скорость будет меньше, чем в стандарте Zigbee, от 9,6 до 100 кбит/с. Z-Wave позволяет объединять в одну беспроводную ячеистую сеть до 232 устройств.

СИСТЕМА «УМНЫЙ ДОМ» — ТЕХНОЛОГИЯ БУДУЩЕГО

ВОЗМОЖНОСТИ УМНОГО ДОМА

Умный дом осуществляет управление:

- светом и электричеством;
- климатом и вентиляцией;
- охраной и безопасностью;
- прочими системами, например осуществляет уборку, полив территории и т.д.



ОСВЕЩЕНИЕ

По части организации освещения умному дому просто нет равных. Он может автоматически открывать и закрывать шторы (жалюзи), используя специальные датчики движения, включать и выключать свет, а также регулировать внешнюю подсветку.

12 999 ₴

КЛИМАТ

Как правило, она включает в себя несколько элементов:

- центральный котел с сетью труб;
- теплые полы;
- кондиционеры и обогреватели;
- датчики для умного дома (температуры и влажности);
- панель управления.

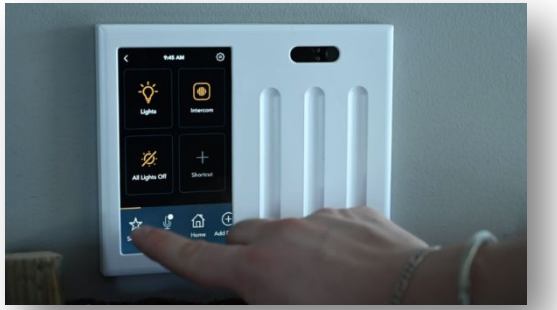
Оборудование для умного дома можно запрограммировать на поддержание определенной температуры и влажности, а также составить график их включения и выключения.

БЕЗОПАСНОСТЬ

Умный дом защитит вас по всем этим направлениям:

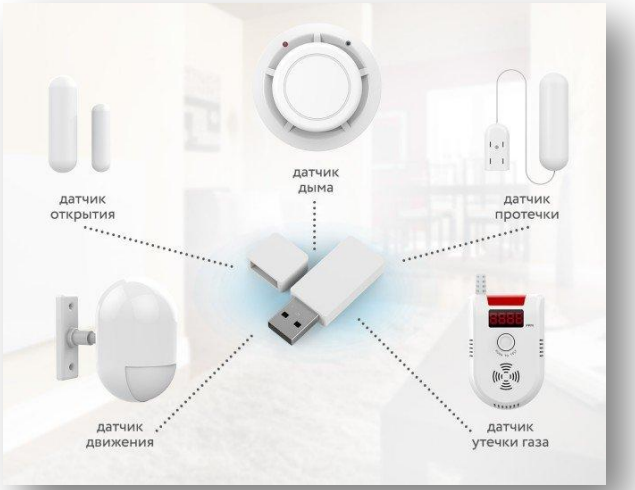
- Датчики утечки воды и газа — система умного дома хороша тем, что она мгновенно реагирует на происходящие изменения и в случае чего устраняет негативные последствия неполадки. Если оборудование зафиксирует какие-либо нарушения, оно моментально перекроет воду или газ в доме.
- Противопожарные датчики. На сегодняшний день на рынке представлен самый широкий спектр устройств, следящих за противопожарной безопасностью. При обнаружении дыма оно запустит самосрабатывающие огнетушители и даже вызовет пожарную службу!
- Датчики проникновения, фиксирующие движение на территории и включающие сигнализацию.
- Камеры, благодаря которым пользователь умного дома в любой момент может узнать, что происходит в других комнатах и на улице. Очень полезная вещь для семей с маленькими детьми.

КОМПОНЕНТЫ УМНОГО ДОМА



- Главная часть умного дома — это его управляющий контроллер. Контроллер — это сервер для умного дома, он объединяет все устройства в одну целостную систему и обеспечивает их взаимодействие.
- Также большое значение имеют системы расширения связи, включающие в себя роутеры, коммутаторы и т.д.

- С помощью приборов коммутации электрической цепи происходит включение или выключение нужного механизма или устройства.
- Датчики и сенсоры, а также измерительные приборы разного направления.
- Элементы, за счет которых происходит непосредственное управление всей системой или ее частями.
- Сама техника (камеры, осветители и т.д.).



Модуль управления «умным домом» Rubetek RM-3712

ПРОБЛЕМЫ УМНЫХ ДОМОВ

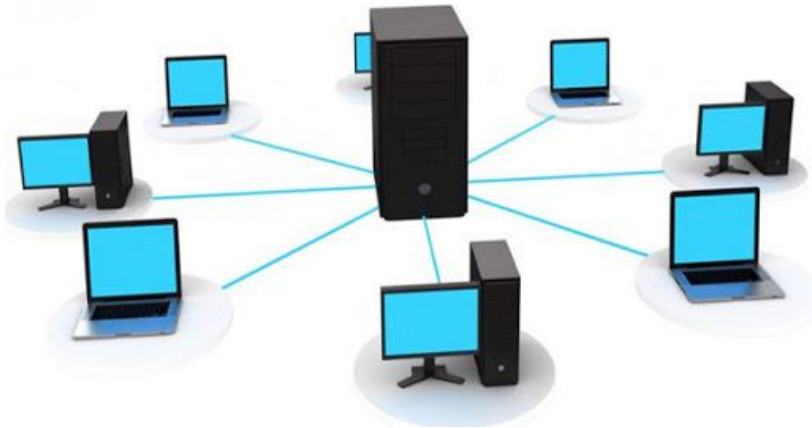
- Частые поломки. Следует помнить, что любая техника часто ломается. Включая в себя множество устройств, умные дома ломаются еще чаще, а замена или починка каждого датчика может стоить достаточно дорого. К сожалению, за комфорт приходится платить.
- Энергосбережение. Поскольку все устройства умного дома подключены к электросети, в совокупности они потребляют большое количество энергии, нанося значительный ущерб кошельку своего владельца.
- Хакерские атаки. Контроллеры для умного дома тоже подвержены хакерским атакам. Однако при оценке этого недостатка сначала стоит задуматься: пойдет ли кто-то на подобные действия, чтобы навредить вам? Конечно, если вы обычный человек, добраться до вас можно гораздо более простыми методами, тем не менее риск есть всегда.
- Человеческий фактор. У людей, не дружащих с техникой, управление умным домом может вызвать проблемы. Этот факт стоит принять во внимание, особенно если в вашей семье есть такой человек.

Одноранговые сети

В одноранговой сети (peer-to-peer network) отсутствует иерархия компьютеров и нет выделенных серверов. Все устройства, которые также называются клиентами, обладают равными возможностями и обязанностями. Отдельные пользователи несут ответственность за свои ресурсы и могут самостоятельно решать, какие данные и устройства устанавливать и к каким данным и устройствам предоставлять общий доступ. Поскольку отдельные пользователи отвечают за ресурсы на своих компьютерах, в сети отсутствует центральная точка управления или администрирования.

Одноранговые сети имеют ряд недостатков.

- Отсутствует централизованное администрирование сети. Это затрудняет определение пользователей, контролирующих ресурсы в этой сети.
- Отсутствует централизованная система обеспечения безопасности. Каждый компьютер использует отдельные средства обеспечения безопасности для защиты данных.
- 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

Иерархические, созданные на базе серверов – такие сети обеспечивают высокую производительность и надежность хранения информации при большом количестве пользователей

Сервер - специальный управляющий компьютер, предназначенный для:

1. хранения данных для всей сети.
2. подключения периферийных устройств;
3. централизованного управления всей сетью;
4. определения маршрутов передачи сообщений.

Топология локальных сетей

Под *топологией вычислительной сети* понимается способ соединения ее отдельных компонентов (компьютеров, серверов, принтеров и т.д.). Различают три основные топологии:

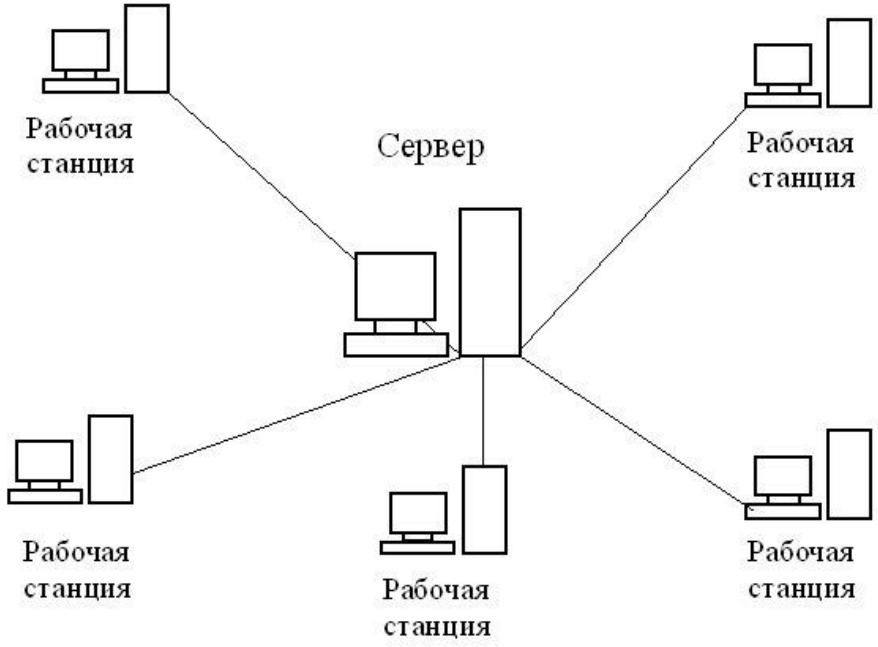
При использовании топологии **типа звезда** информация между клиентами сети передается через единый центральный узел. В качестве центрального узла может выступать сервер или специальное устройство – концентратор (Hub)

Преимущества данной топологии состоят в следующем:

1. Высокое быстродействие сети, так как общая производительность сети зависит только от производительности центрального узла.
2. Отсутствие столкновения передаваемых данных, так как данные между рабочей станцией и сервером передаются по отдельному каналу, не затрагивая другие компьютеры.

Однако помимо достоинств у данной топологии есть и недостатки:

1. Низкая надежность, так как надежность всей сети определяется надежностью центрального узла. Если центральный компьютер выйдет из строя, то работа всей сети прекратится.
2. Высокие затраты на подключение компьютеров, так как к каждому новому абоненту необходимо ввести отдельную линию.



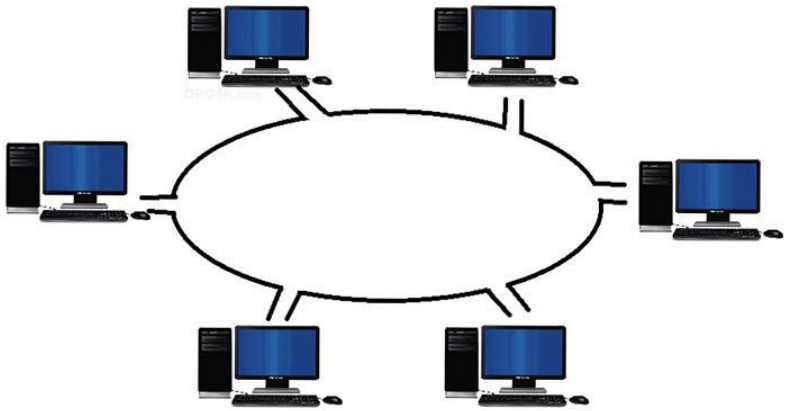
При топологии **типа кольцо** все компьютеры подключаются к линии, замкнутой в кольцо. Сигналы передаются по кольцу в одном направлении и проходят через каждый компьютер.

Преимущества топологии типа кольцо состоят в следующем:

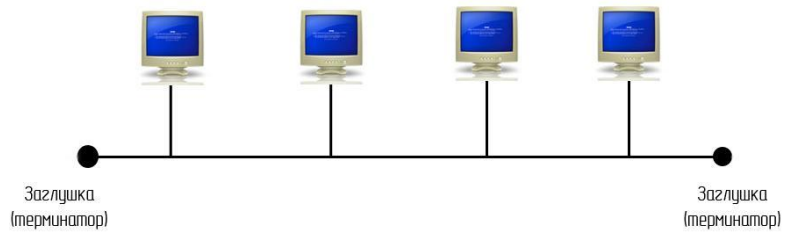
1. Пересылка сообщений является очень эффективной, т.к. можно отправлять несколько сообщений друг за другом по кольцу. Т.е. компьютер, отправив первое сообщение, может отправлять за ним следующее сообщение, не дожидаясь, когда первое достигнет адресата.
2. Протяженность сети может быть значительной. Т.е. компьютеры могут подключаться к друг к другу на значительных расстояниях, без использования специальных усилителей сигнала.

К недостаткам данной топологии относятся:

1. Низкая надежность сети, так как отказ любого компьютера влечет за собой отказ всей системы.
2. Для подключения нового клиента необходимо отключить работу сети.
3. При большом количестве клиентов скорость работы в сети замедляется, так как вся информация проходит через каждый компьютер, а их возможности ограничены.
4. Общая производительность сети определяется производительностью самого медленного компьютера.



При топологии типа **общая шина** все клиенты подключены к общему каналу передачи данных. При этом они могут непосредственно вступать в контакт с любым компьютером, имеющимся в сети.



Преимущества топологии общая шина:

1. Вся информация находится в сети и доступна каждому компьютеру.
2. Рабочие станции можно подключать независимо друг от друга. Т.е. при подключе нового абонента нет необходимости останавливать передачу информации в сети.
3. Построение сетей на основе топологии общая шина обходится дешевле, так как отсутствуют затраты на прокладку дополнительных линий при подключении нового клиента.
4. Сеть обладает высокой надежностью, т.к. работоспособность сети не зависит от работоспособности отдельных компьютеров.

К недостаткам топологии типа общая шина относятся:

1. Низкая скорость передачи данных, т.к. вся информация циркулирует по одному каналу (шине).
2. Быстродействие сети зависит от числа подключенных компьютеров. Чем больше компьютеров подключено к сети, тем медленнее идет передача информации от одного компьютера к другому.
3. Для сетей, построенных на основе данной топологии, характерна низкая безопасность, так как информация на каждом компьютере может быть доступна с любого другого компьютера.

Открытые стандарты

Открытые стандарты способствуют совместимости, конкуренции и инновациям. Кроме того, они гарантируют, что продукт отдельной компании не сможет монополизировать рынок или получить несправедливое преимущество по сравнению с конкурентами.

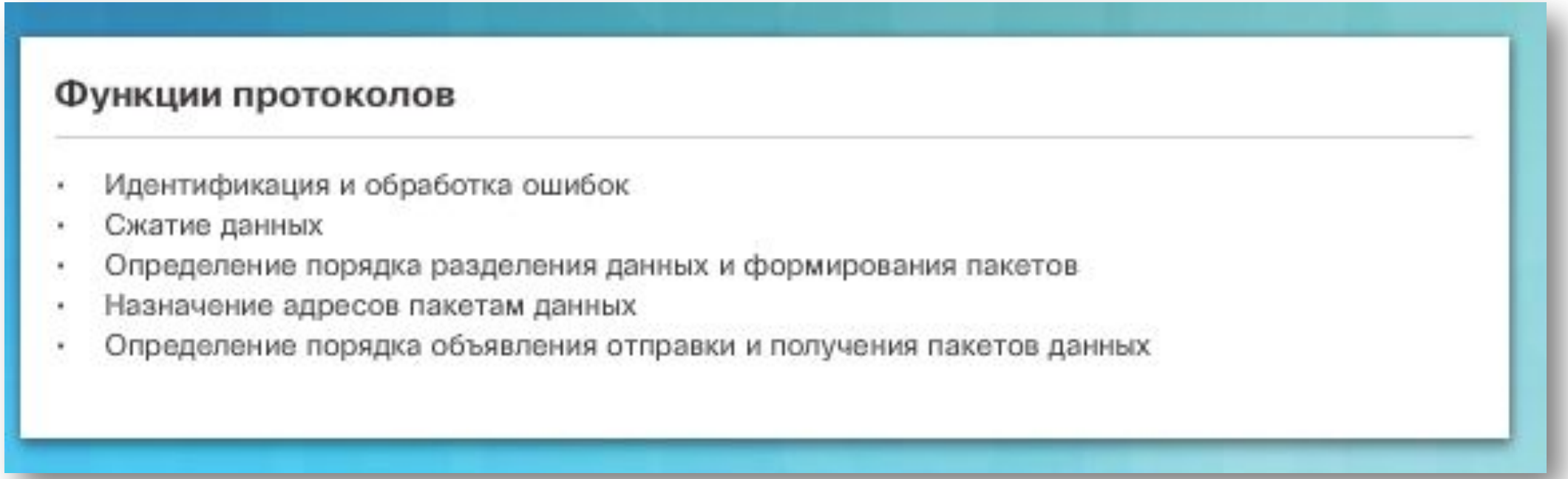
Хороший пример — покупка беспроводного маршрутизатора для дома

Преимущество открытых систем:

- Возможность строить сети из оборудования разных производителей
- Безболезненная замена оборудования сети
- Легкость объединения нескольких сетей

Протоколы

Протоколы Интернета — это наборы правил, регулирующие обмен данными между компьютерами в сети. Спецификации протокола определяют формат сообщений, участвующих в обмене.

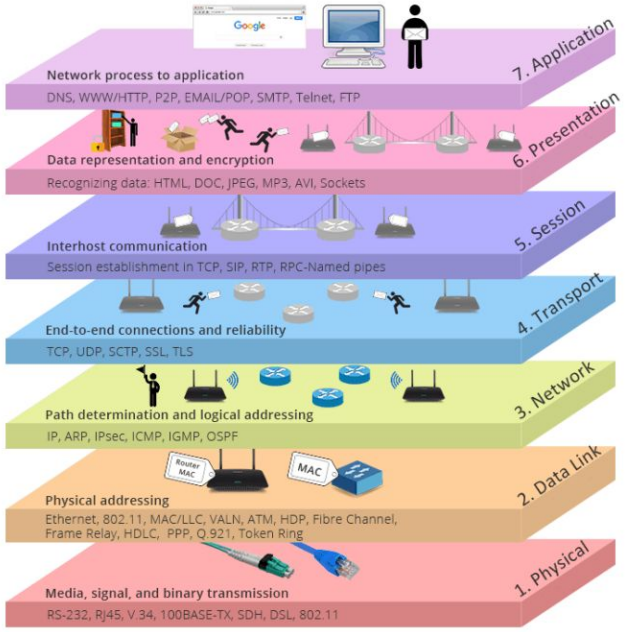


Для надежной доставки пакетов важны сроки. Согласно протоколам, сообщения должны поступать в течение определенных промежутков времени, чтобы компьютерам не приходилось ждать сообщения бесконечно, например если сообщения потерялись

Эталонная модель организации сетей (Open Systems Interconnection) Общий зык для описания компьютерных сетей

Принята в качестве стандарта организации сетей(ISO) 1983 г.

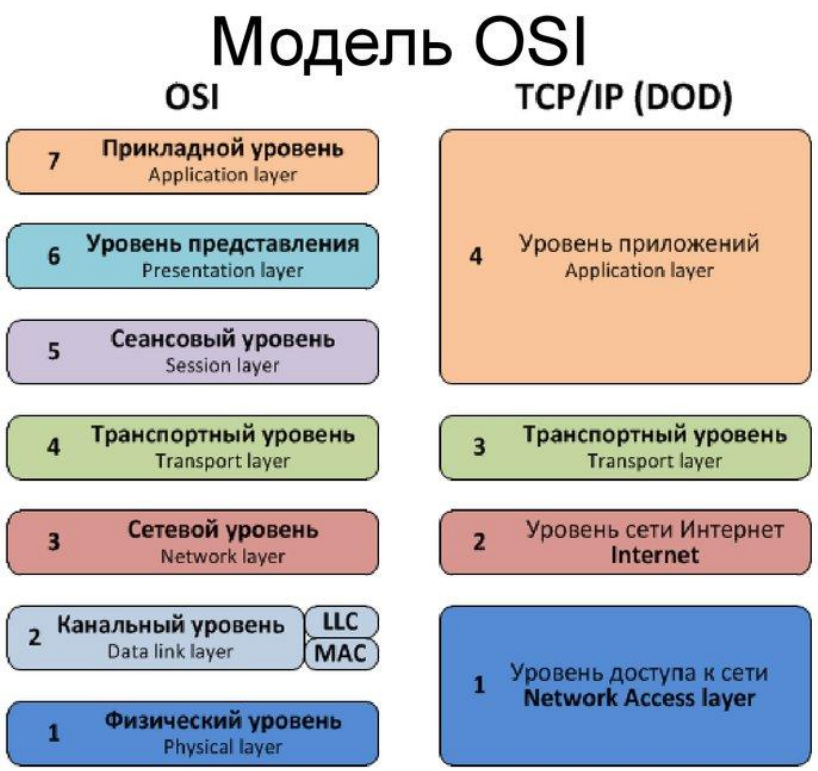
- Описывает из каких уровней состоит сеть
- Что должен делать тот или иной уровень



Эталонная модель OSI

Модель OSI		
Тип данных	**Уровень (layer)**	**Функции**
Данные	7. Прикладной (application)	Доступ к сетевым службам
	6. Уровень представления (presentation)	Представление и шифрование данных
	5. Сеансовый (session)	Управление сеансом связи
Сегменты	4. Транспортный (transport)	Прямая связь между конечными пунктами и надежность
Пакеты (датаграммы)	3. Сетевой (network)	Определение маршрута и логическая адресация
Кадры	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа со средой передачи, сигналами и двоичными данными

Эталонная модель OSI



Модель OSI

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

Физический уровень(бит)

- Передача битов по каналу связи
- Представление битов в виде сигналов(в зависимости по какому каналу передаются биты)

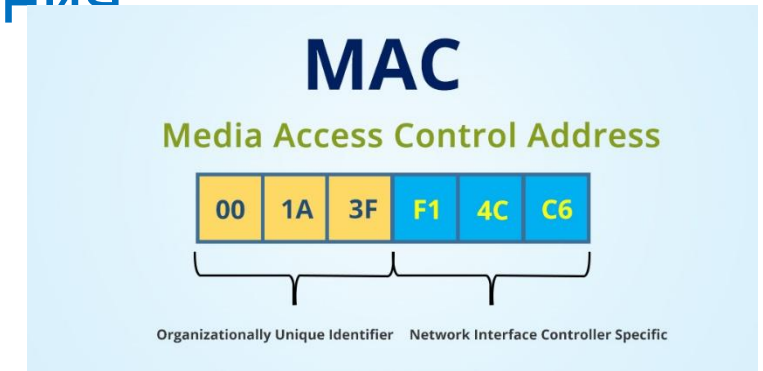
электрические провода, радиосвязь, волоконно-оптические провода, Wi-Fi

Канальный уровень(кадр)

- Передает не отдельные биты а сообщения
- Обнаруживает и корректирует ошибки
- Обеспечивает уведомления о неисправностях

Заголовок-Пакет-Концевик

MAC (Media Access Control) — обеспечивает специальные методы доступа к среде распространения



Сетевой уровень(пакет)

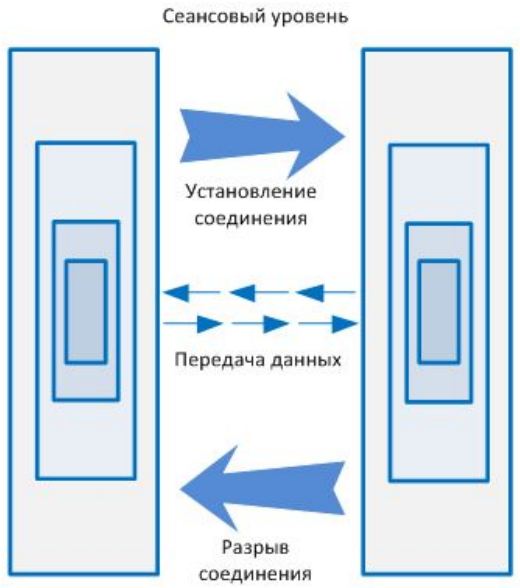
- Объединяет сети построенные на основе разных технологий
- Создание составной сети
- Адресация
- Определения маршрута пересылки пакета в составной сети (маршрутизация)

Транспортный уровень(сегмент-дейтаграмма)

- Обеспечивают передачу данных между процессами на хостах
- Управление надежностью

Сеансовый уровень(сообщение)

- Позволяет устанавливать сеансы связи
- Управление диалогом(очередность передачи сообщений)
- Предоставляет защиту от разрыва сетевого соединения



Уровень представления(сообщение)

- Обеспечивает формат данных понятных получателю (синтаксис и семантику(смысл))
- Шифрование и дешифрование

Прикладной уровень(сообщение)-ради чего строится сеть

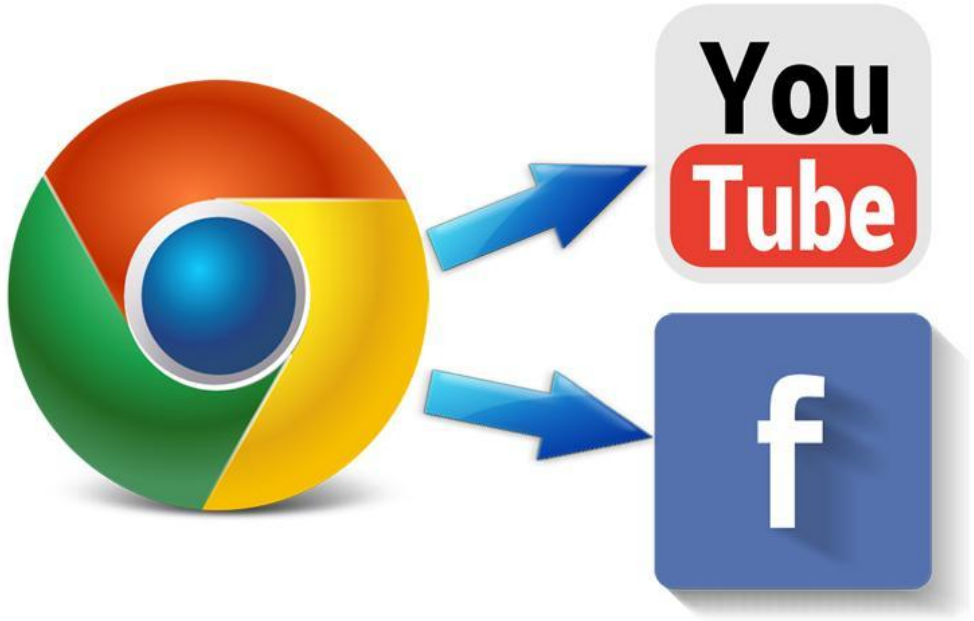
Набор приложений полезных пользователям

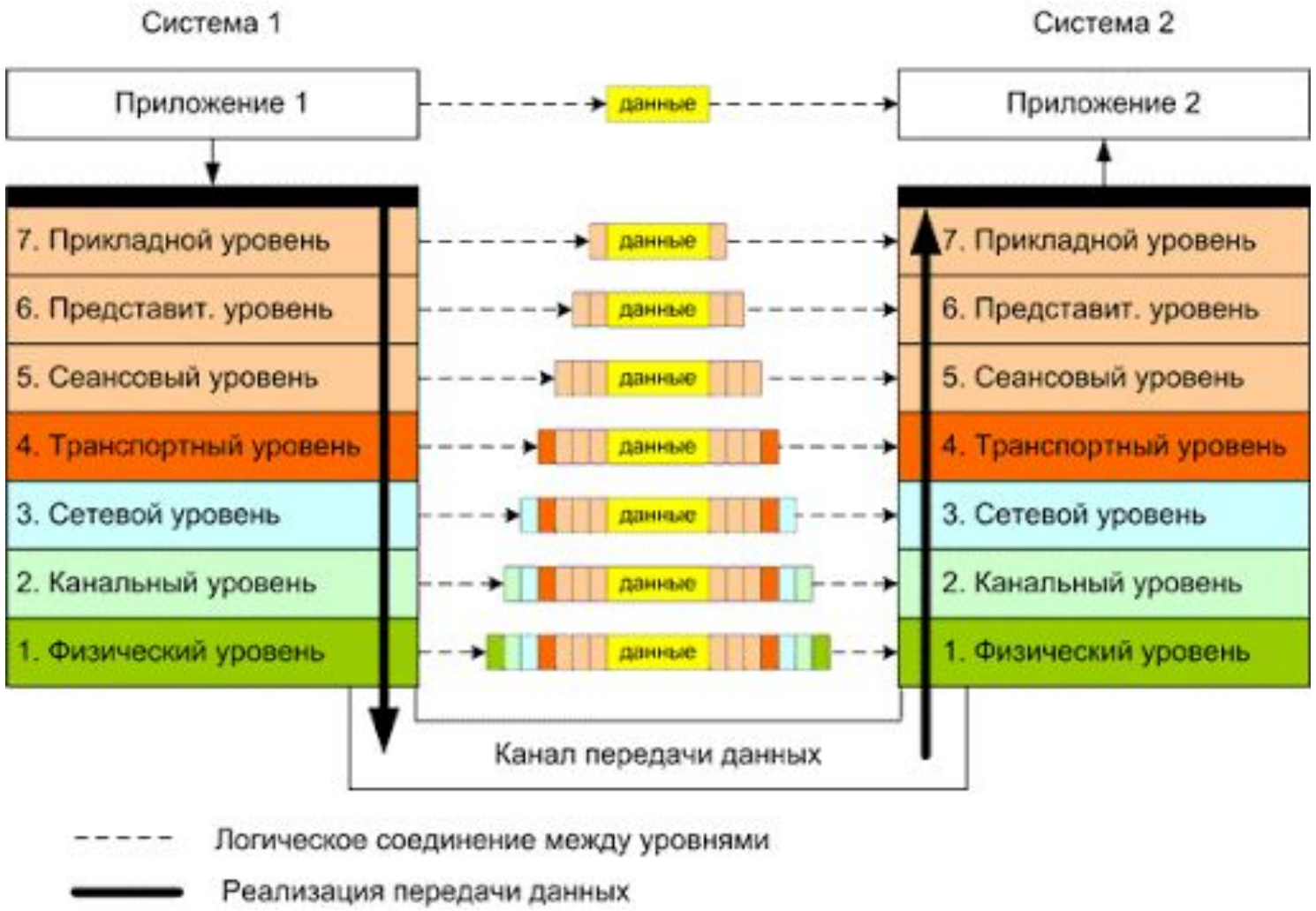
Web-страницы

Соцсети

Видео-аудио связь

Электронная почта




Система 1
Система 2
Приложение 1
данные
Приложение 2
7. Прикладной уровень
6. Представит. уровень
5. Сеансовый уровень
4. Транспортный уровень
3. Сетевой уровень
2. Канальный уровень
1. Физический уровень
данные
данные
данные
данные
данные
данные
7. Прикладной уровень
6. Представит. уровень
5. Сеансовый уровень
4. Транспортный уровень
3. Сетевой уровень
2. Канальный уровень
1. Физический уровень
Канал передачи данных
Логическое соединение между уровнями
Реализация передачи данных

Сетевое оборудование

- Сетевой уровень- маршрутизатор
- Канальный уровень–коммутатор ,точка доступа
- Физический уровень- концентратор

Модель TCP/IP

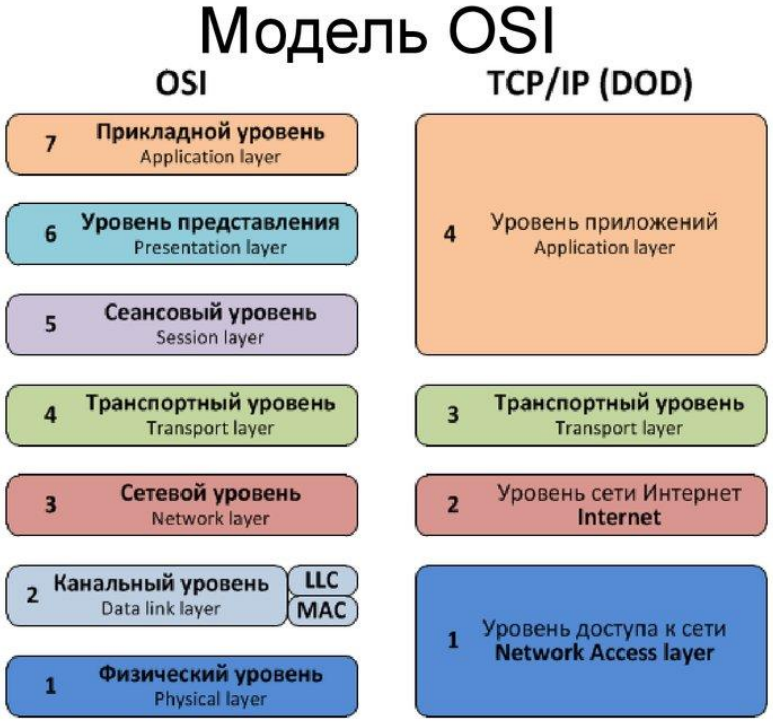
1 Сетевых интерфейсов(Ethernet,Wi-Fi и др.)

2 Интернет (Обеспечивает поиск маршрутов в составной сети

3 Транспортный уровень(Обеспечивает связь между двумя процессами на разных компьютерах)

4 Прикладной уровень(объеденил три уровня модели OSI)

Модель TCP/IP



Сравнение OSI и TCP/IP

Модель OSI:

- Хорошая теоретическая проработка
- Протоколы не используются

Модель TCP/IP:

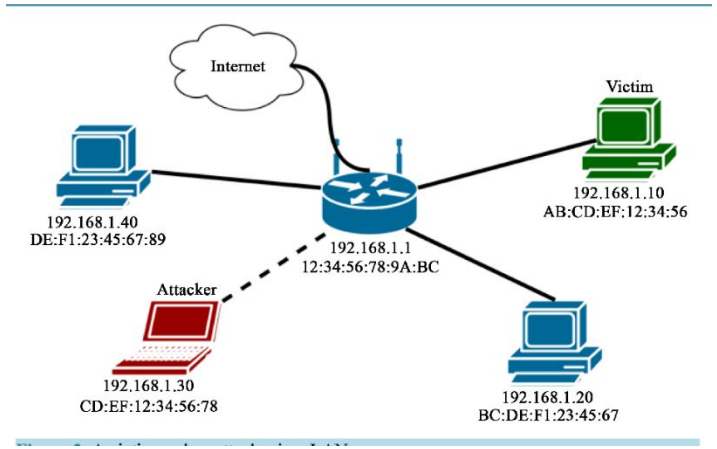
- Протоколы широко применяются
- Подходит только для описания сетей стека протокола TCP/IP

Применения:

- OSI-модель для описания разных типов сетей
- TCP/IP-протоколы ,основа интернет

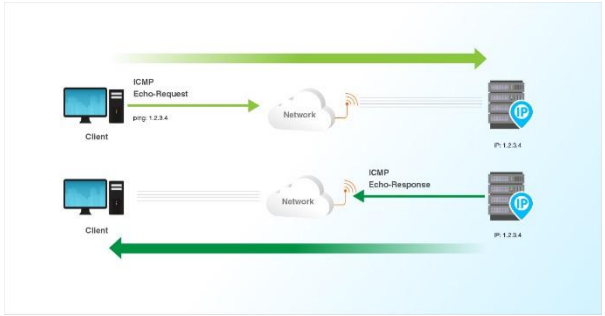
Уровень доступа к сети

- **ARP**-Обеспечивает динамическое сопоставление между IP-адресами и аппаратными адресами
- **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



Межсетевой уровень

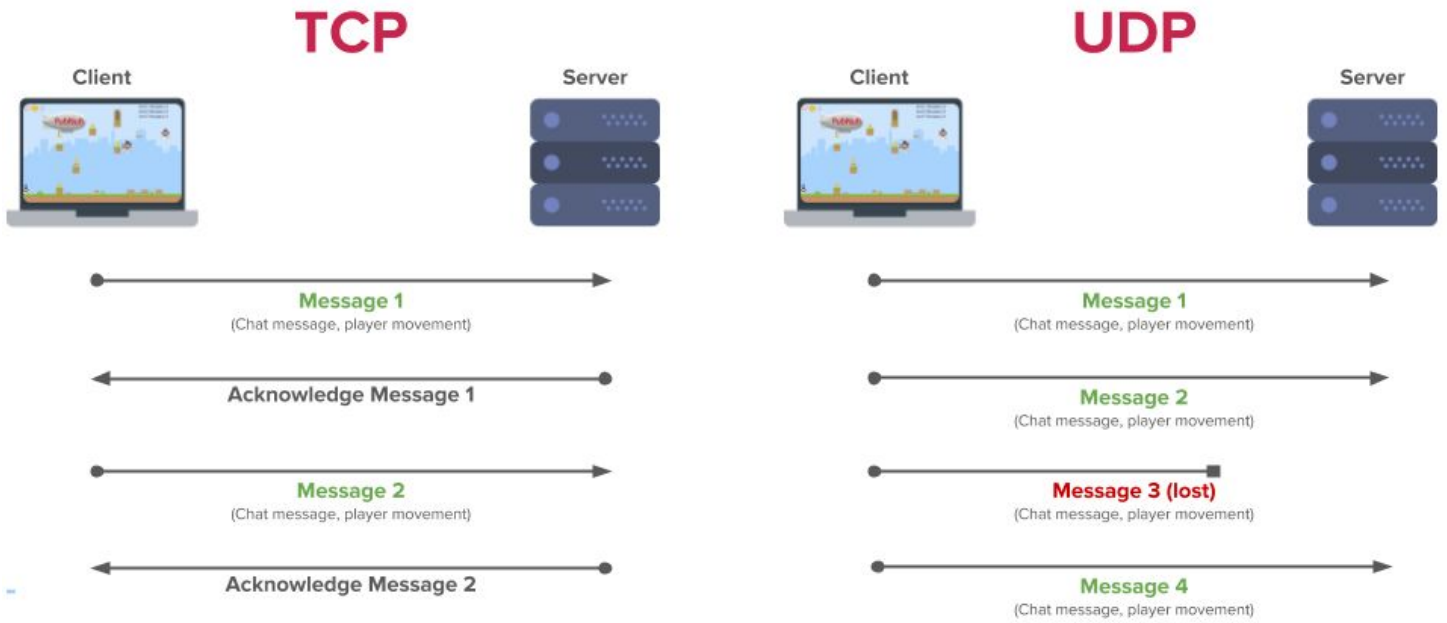
- **Ip**-Принимает сегменты сообщений с транспортного уровня.Формирует из них пакеты.Добавляет в пакеты адресную информацию для доставки конечному получателю по сети.
- **NAT**-Преобразует IP-адреса частной сети в глобальные уникальные публичные IP-адреса
- **ICMP**-Обеспечивает обратную связь от узла назначения к исходному узлу, чтобы сообщать об ошибках доставки пакетов протокол ICMP не может запросить послать потерянный пакет повторно, а просто оповещает о несчастных случаях.
- OSPF,EIGRP-протоколы маршрутизации использующий для нахождения кратчайшего пути алгоритм Дейкстры



Транспортный уровень

UDP

TCP



Свойства TCP и UDP

TCP

SMTP/POP (электронная почта)

HTTP

Требуемые свойства протокола:

- Надежность
- Подтверждение данных
- Повторная отправка потерянных данных
- Доставка данных в заданной последовательности

UDP

IP-телефония

Потоковая передача видео

Требуемые свойства протокола:

- Высокая скорость
- Низкая нагрузка
- Не требует подтверждений
- Не выполняет повторную отправку потерянных данных
- Доставка данных по мере их получения

Уровень приложений

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

DHSP-Динамически присваивает IP-адреса клиентским станциям при запуске

SMTP-Позволяет клиентам отправлять электронные сообщения на почтовый сервер

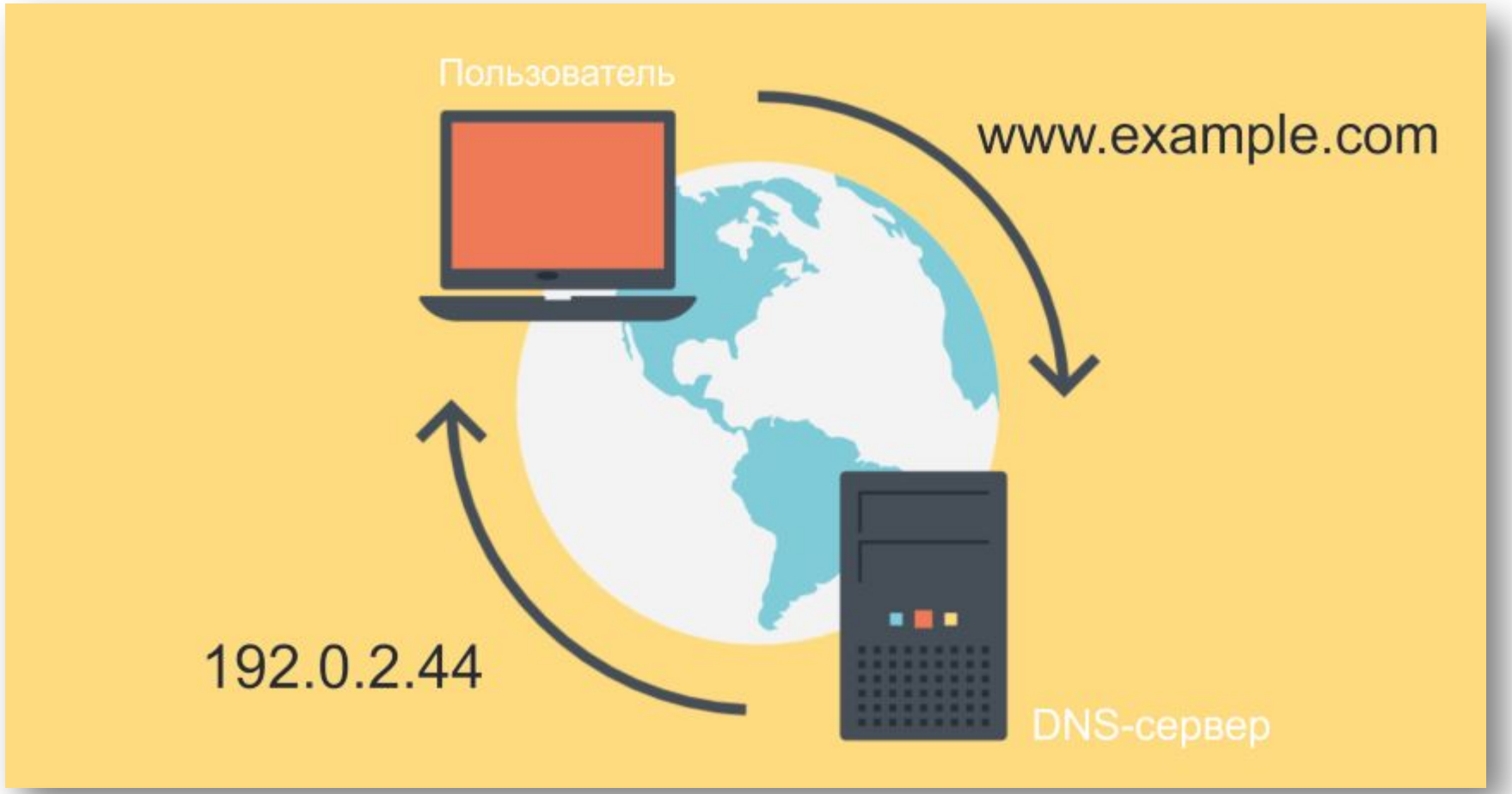
POP-Позволяет клиентам получать электронные сообщения с почтового сервера

IMAP-Позволяет клиентам получать доступ к электронным сообщениям, которые хранятся на почтовом сервере

FTP-Надежный протокол доставки файлов с подтверждением и установлением соединения

HTTP-Задает правила обмена в Интернете текстом, графическими изображениями, звуковыми, видео и другими файлами мультимедиа

DNS



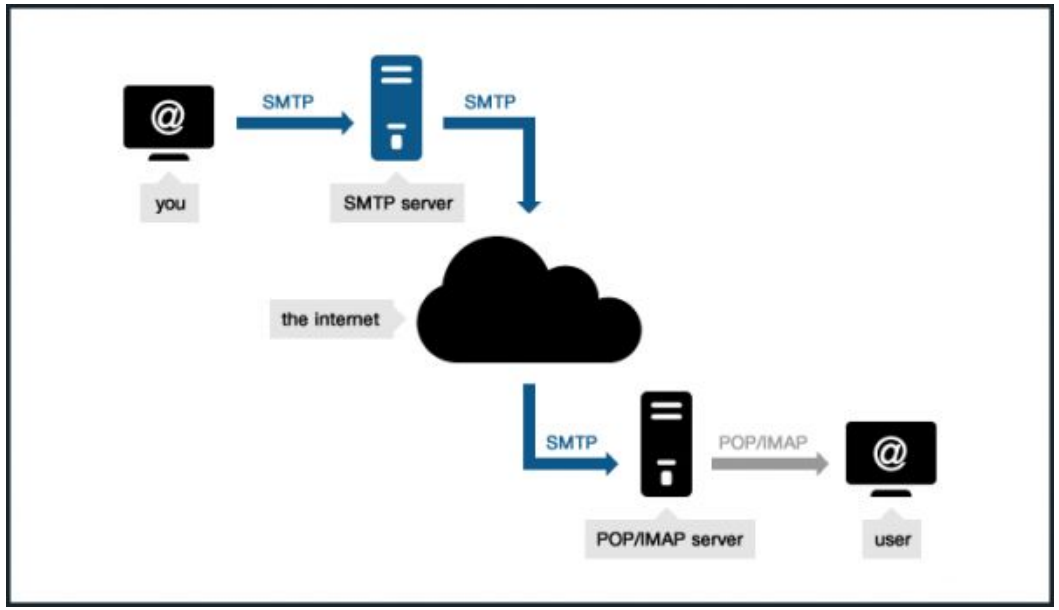
DHSP


Server
Access Point
Switch
Wi-Fi
Ethernet connection
Internet

SMTP, протокол для исходящей связи по электронной почте

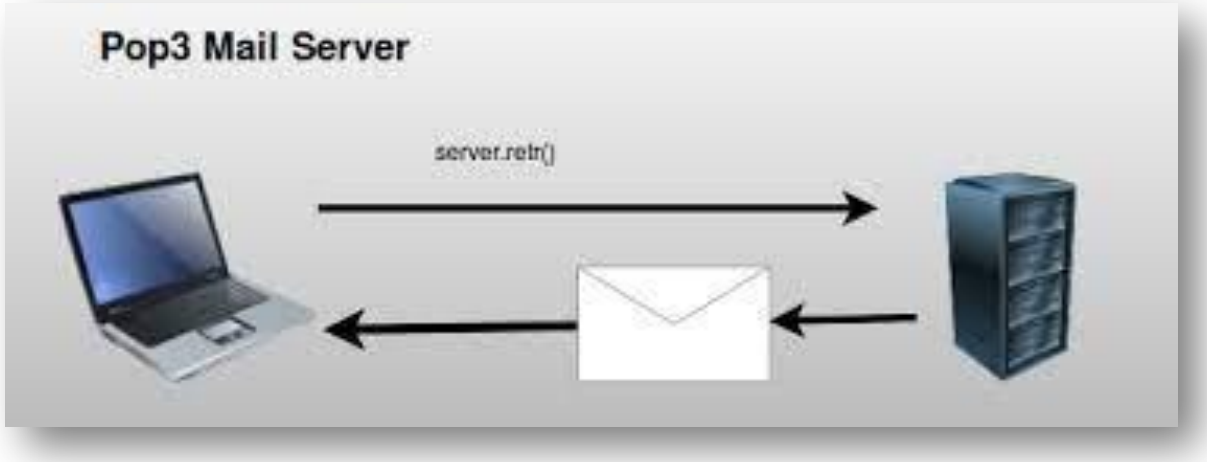
Порты SMTP:

- Порт 25 – порт без шифрования
- Порт 465 – порт SSL/TLS, также известный как **SMTPS**



POP3 (протокол почтового отделения версия 3) часто используется для связи с удаленным сервером электронной почты и загрузки сообщений на локальный почтовый клиент с последующим удалением его на сервере

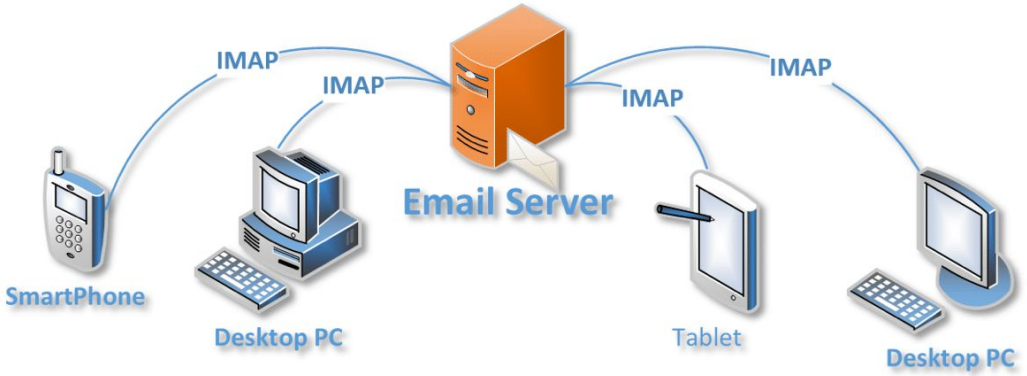
Порты POP3, по умолчанию являются такими:
Порт 110 – порт без шифрования
Порт 995 – порт SSL/TLS, также известный как **POP3S**



IMAP (протокол прикладного уровня для доступа к электронной почте), также как и POP3 используется для получения сообщений электронной почты на локальный клиент, однако, он имеет существенное отличие – загружаются только лишь заголовки электронных сообщений, сам текст письма остается на сервере.

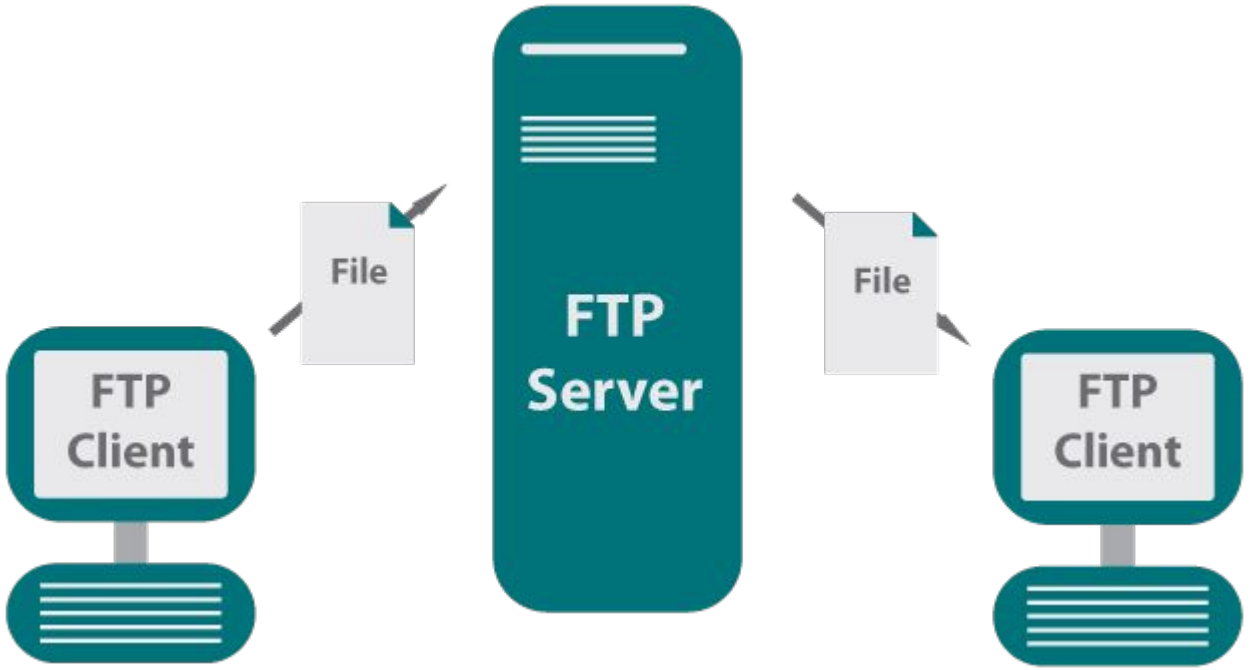
Порты IMAP, по умолчанию являются такими:

- Порт 143 – порт без шифрования
- Порт 993 – порт SSL/TLS, также известный как **IMAPS**



FTP

File Transfer Protocol — протокол передачи файлов. Он отличается от других протоколов тем, что если в процессе передачи возникает какая-то ошибка, то процесс останавливается и выводится сообщение для пользователя. Если ошибок не было, значит, пользователь получил именно тот файл, который нужен, в целости и без недостающих элементов.



HTTP

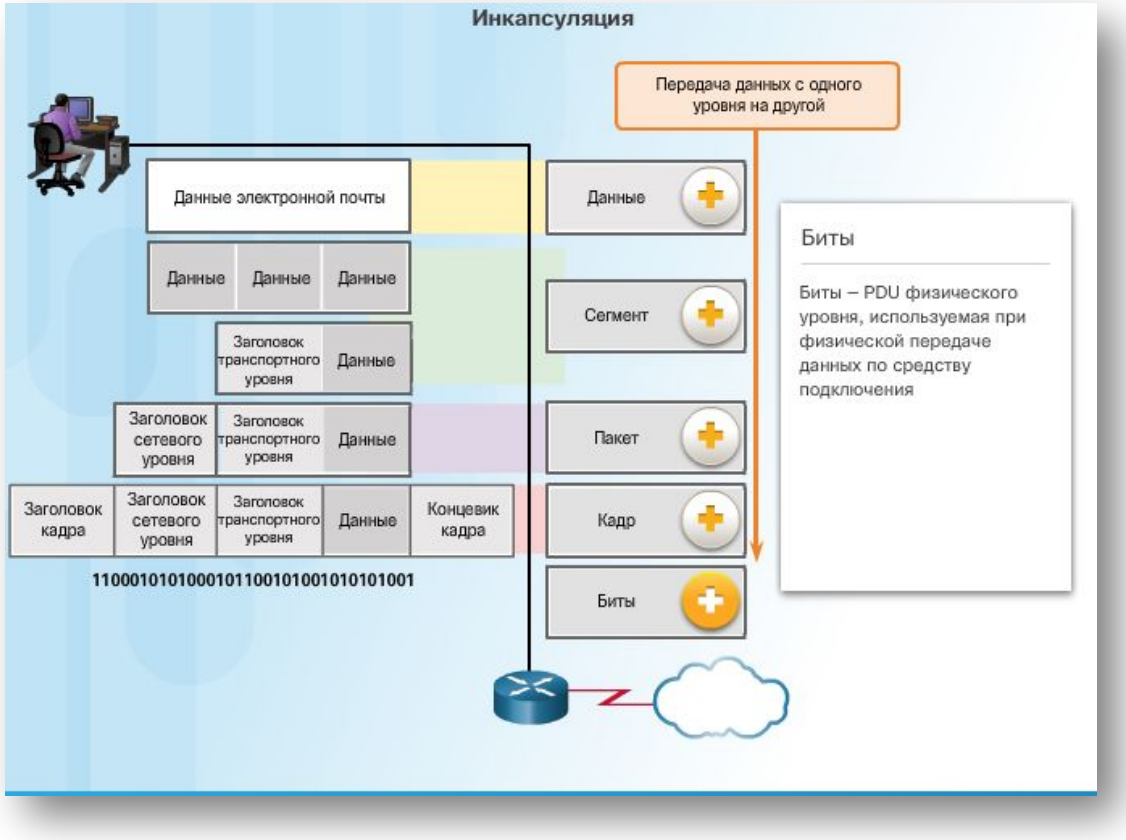
HTTP — широко распространённый протокол передачи данных, изначально предназначенный для передачи гипертекстовых документов (то есть документов, которые могут содержать ссылки, позволяющие организовать переход к другим документам)

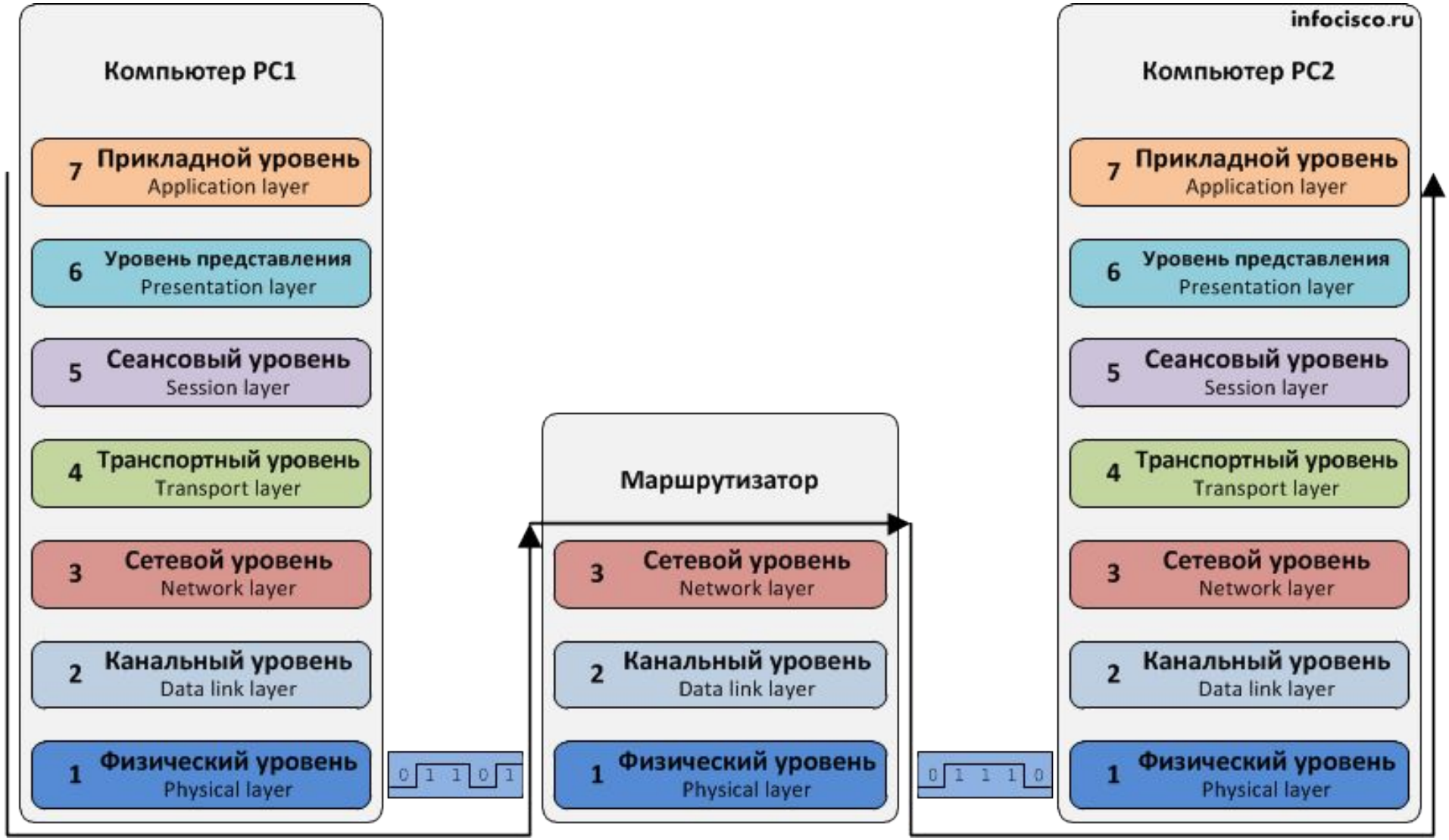
HTTP порт 80,
для **HTTPS** по умолчанию
используется порт 443

Основа для сравнения	Модель TCP / IP	Модель OSI
Расширяется до	Протокол управления передачей / Интернет-протокол	Открытая система Interconnect
Смысл	Это модель клиент-сервер, используемая для передачи данных через Интернет.	Это теоретическая модель, которая используется для вычислительной системы.
Количество слоев	4 слоя	7 слоев
Разработан	Министерство обороны (DoD)	ISO (Международная организация по стандартизации)
осязаемый	да	нет
использование	В основном используется	Никогда не использовался
подчиняющийся	Горизонтальный подход	Вертикальный подход

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.




Компьютер PC1
7 Прикладной уровень
Application layer
6 Уровень представления
Presentation layer
5 Сеансовый уровень
Session layer
4 Транспортный уровень
Transport layer
3 Сетевой уровень
Network layer
2 Канальный уровень
Data link layer
1 Физический уровень
Physical layer
0 1 1 0 1
Маршрутизатор
3 Сетевой уровень
Network layer
2 Канальный уровень
Data link layer
1 Физический уровень
Physical layer
0 1 1 1 0
infocisco.ru
Компьютер PC2
7 Прикладной уровень
Application layer
6 Уровень представления
Presentation layer
5 Сеансовый уровень
Session layer
4 Транспортный уровень
Transport layer
3 Сетевой уровень
Network layer
2 Канальный уровень
Data link layer
1 Физический уровень
Physical layer

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.

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.

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.

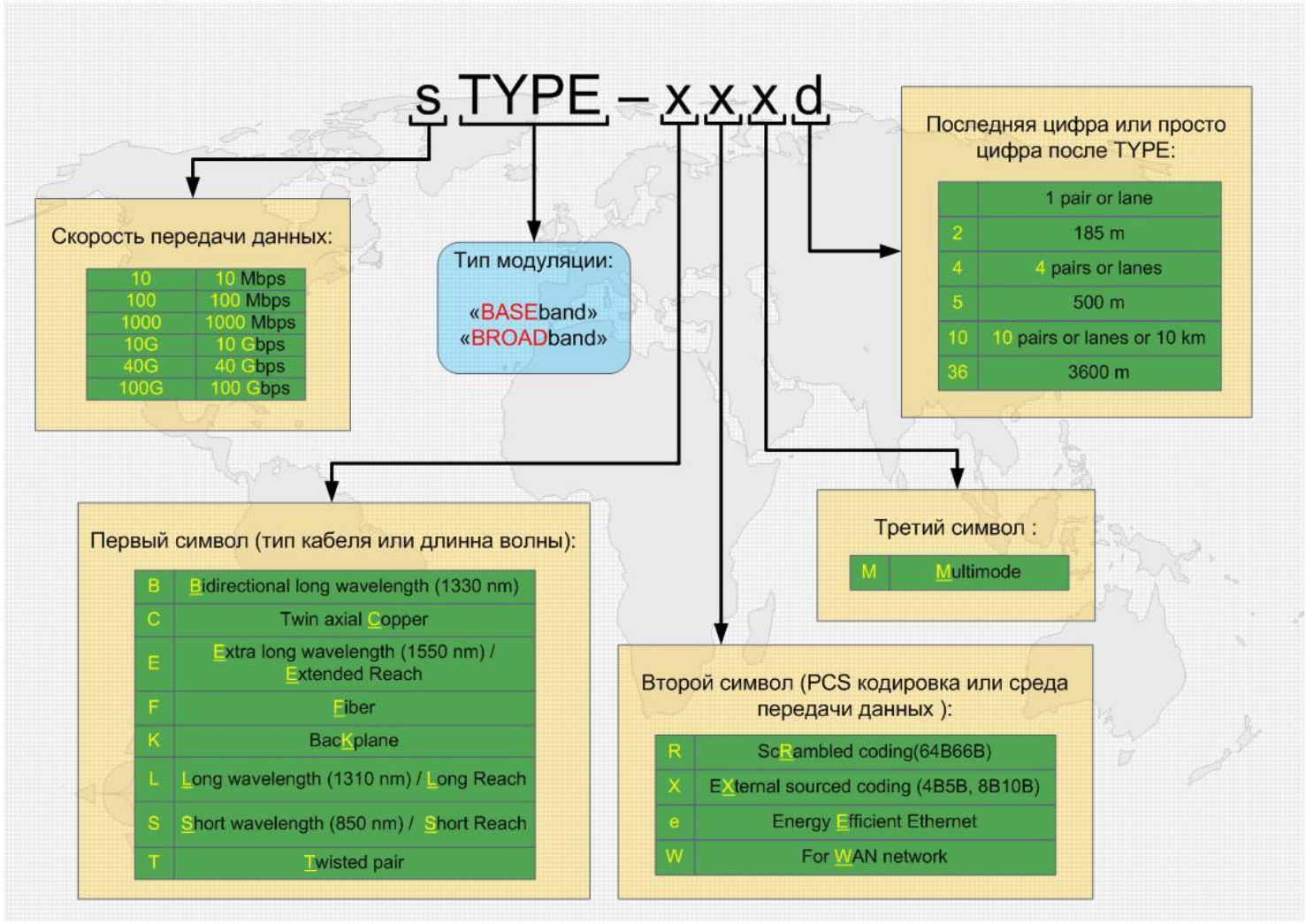
Примечание. Большинство сетей Ethernet работает в настоящее время в полнодуплексном режиме. В таком режиме Ethernet конфликты возникают редко, поскольку устройства могут выполнять отправку и прием данных одновременно.

Стандарты кабелей Ethernet

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.

Расшифровка кабелей



Расшифровка кабелей

10 Мбит/с Ethernet	
Номенклатура	**Расшифровка**
10BASE-T	Электрическая связь через витую пару, использующая прямую (немодулированную) модуляцию для передачи сигнала со скоростью до 10 Мбит/с
10BROAD36	Электрическая связь через коаксиальный кабель, использующая широкополосную модуляцию для передачи сигнала со скоростью до 10 Мбит/с
100 Мбит/с Ethernet	
100Base-T4	Электрическая связь через четыре витые пары, использующая прямую модуляцию для передачи сигнала со скоростью до 100 Мбит/с
100Base-LX10	Оптическая связь через длинноволновой оптоволоконный кабель, использующая внешнее кодирование для передачи сигнала со скоростью до 100 Мбит/с
1000 Мбит/с Ethernet	
1000Base-SX	Оптическая связь через коротковолновой оптоволоконный кабель, использующая внешнее кодирование для передачи сигнала со скоростью до 1 Гбит/с
1000Base-EX	Оптическая связь через улучшенный длинноволновой оптоволоконный кабель, использующая внешнее кодирование для передачи сигнала со скоростью до 1 Гбит/с

10 Гбит/с Ethernet	
10GBASE-LRM	Оптическая связь через длинноволновой многомодовый оптоволоконный кабель, использующая 64B66B кодирование для передачи сигнала со скоростью до 10 Гбит/с
10GBASE-SW	Оптическая связь через коротковолновой оптоволоконный кабель, использующая прямую кодировку для передачи сигнала со скоростью до 10 Гбит/с по WAN сетям
40 и 100 Гбит/с Ethernet	
40GBase-KR4	Связь через объединительную плату с использованием 64B66B схеми кодирования для передачи сигнала по 4-м параллельным проводникам со скоростью до 40 Гбит/с
100GBase-CR10	Электрическая связь через биаксиальный кабель, использующая 64B66B схему кодирования для передачи сигнала по 10 параллельным проводникам со скоростью до 100 Гбит/с

Первые версии Ethernet

10 Мбит/с Ethernet (Thick ethernet)								
Стандарт	IEEE 802.3	IEEE 802.3a	IEEE 802.3b	IEEE 802.3e	IEEE 802.3e	IEEE 802.3d	IEEE 802.3i	IEEE 802.3j
Год выхода стандарта	1983	1985	1985	1987	1987	1987	1990	1993
Тип	10Base5	10Base2	10Broad36	1Base5	StarLan 10	FOIRL	10Base-T	10Base-F
Скорость передачи (Mbps)	10	10	10	1	10	10	10	10
Максимальная длина сегмента в метрах	500 м	185 м	3600 м	250 м	250 м	1000	100 м	2км
Тип кабеля	коаксиальный			UTP	UTP	оптоволоконный	UTP cat 3,5	оптоволоконный

Fast Ethernet — общее название для набора стандартов передачи данных в компьютерных сетях по технологии Ethernet со скоростью до 100 Мбит/с

100 Мбит/с Ethernet (Fast Ethernet)									
Стандарт	IEEE 802.3u				IEEE 802.12	IEEE 802.3y	TIA/EIA-785	IEEE 802.3ah	IEEE 802.3ah
Год выхода стандарта	1995				1995	1998	2001	2004	2004
Тип	100Base-FX	100Base-T	100Base-T4	100Base-TX	100Base-VG	100Base-T2	100Base-SX	100Base-LX10	100Base-BX10
Скорость передачи (Mbps)	100	100	100	100	100	100	100	100	100
Максимальная длина сегмента в метрах	Одномод — 2 км Многомод — 400 м	100 м	100 м	100 м	100 м	100 м	300 м	10 км	10 км
Тип кабеля	оптоволоконный	UTP/STP cat 5	UTP/STP cat >= 3	UTP/STP cat 5	UTP cat 3	UTP cat 3	оптоволоконный		

Gigabit Ethernet (GbE) — термин, описывающий набор технологий для передачи пакетов Ethernet со скоростью 1 Гбит / с.

1000 Мбит/с (Gigabit Ethernet)										
Стандарт	IEEE 802.3z			IEEE 802.3ab	TIA 854	IEEE 802.3ah	IEEE 802.3ah	IEEE 802.3ap	non-standard	non-standard
Год выхода стандарта	1998			1999	2001	2004	2004	2007	?	?
Тип	1000Base-CX	1000Base-LX	1000Base-SX	1000Base-T	1000BASE-TX	1000BASE-LX10	1000BASE-BX10	1000BASE-KX	1000BASE-EX	1000BASE-ZX
Скорость передачи (Mbps)	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Максимальная длина сегмента в метрах	25 м	Одномод — 5 км Многомод — 550 м	550 м	100 м	100 м	10 км	10 км	1 m	40 км	70 км
Тип кабеля	STP cat 5,5e,6	оптоволоконный		UTP/STP cat 5,5e,6,7	UTP/STP cat 6,7	оптоволоконный		для объединительной платы	оптоволоконный	

10 Gigabit Ethernet или 10GbE являлся новейшим (на 2006 год) и самым быстрым из существующих стандартов Ethernet. Он определяет версию Ethernet с номинальной скоростью передачи данных 10 Гбит/с, что в 10 раз быстрее Gigabit Ethernet. Стандарт для оптоволокна специфицирован в IEEE 802.3-2005, а для витой пары в IEEE 802.3an-2006

10 Гбит/с Ethernet (10 GbE)							
Стандарт	IEEE 802.3ae						
Год выхода стандарта	2003	2003	2003	2003	2003	2003	2003
Тип	10GBASE-SR	10GBASE-LX4	10GBASE-LR	10GBASE-ER	10GBASE-SW	10GBASE-LW	10GBASE-EW
Скорость передачи (Gbps)	10	10	10	10	10	10	10
Максимальная длина сегмента в метрах	26-300 м	Одномод — 10 км Многомод — 300 м	10 км	40 км	26 м — 40 км		
Тип кабеля	оптоволоконный						

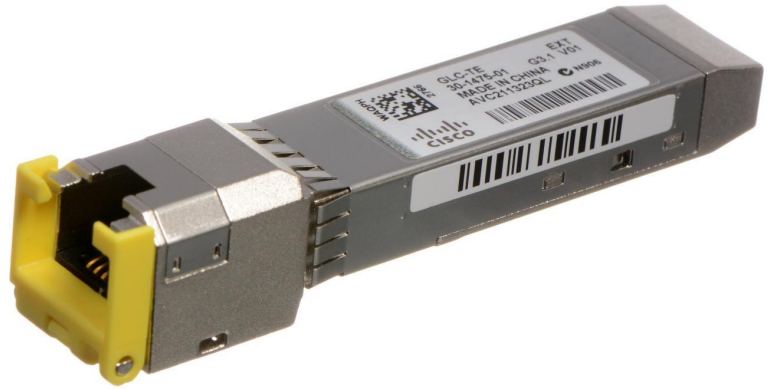
10 Гбит/с Ethernet (10 GbE)						
Стандарт	IEEE 802.3ak	IEEE 802.3an	IEEE 802.3aq	IEEE 802.3ap	IEEE 802.3ap	IEEE 802.3av
Год выхода стандарта	2004	2006	2006	2007	2007	2009
Тип	10GBASE-CX4	10GBASE-T	10GBASE-LRM	10GBASE-KX4	10GBASE-KR	10GBASE-PR
Скорость передачи (Gbps)	10	10	10	10	10	10
Максимальная длина сегмента в метрах	15м	100 м	220 м	1 м	1 м	20 км
Тип кабеля	медный кабель CX4	UTP/STP cat 6,6a,7	оптоволоконный	для объединительной платы		оптоволоконный

40-гигабитный Ethernet (или 40GbE) и **100-гигабитный Ethernet** (или 100GbE) — стандарты Ethernet, разработанные группой IEEE P802.3ba Ethernet Task Force в период с 2007 по 2011 год. Эти стандарты являются следующим этапом развития группы стандартов Ethernet, имевших до 2010 года наибольшую скорость в 10 гигабит/с. В новых стандартах обеспечивается скорость передачи данных в 40 и 100 гигабит в секунду.

40 и 100 Гбит/с Ethernet (40GbE или 100GbE)								
Стандарт	IEEE 802.3ba							IEEE 802.3bg
Год выхода стандарта	2010							2011
Тип	40GBase-KR4 100GBase-KP4	100GBase-KR4	40GBase-CR4 100GBase-CR10	40GBase-T	40GBase-SR4 100GBase-SR10	40GBase-LR4 100GBase-LR4	100GBase-ER4	40GBase-FR
Скорость передачи (Gbps)	40 100	100	40 100	40	40 100	40 100	100	40
Максимальная длина сегмента в метрах	1 м	1 м	7 м	30 м	100 м 125 м	10 км	40 км	2 км
Тип кабеля	для объединительной платы	для улучшенной объединительной платы	медный биаксиальный кабель	UTP cat 8	оптоволоконный			

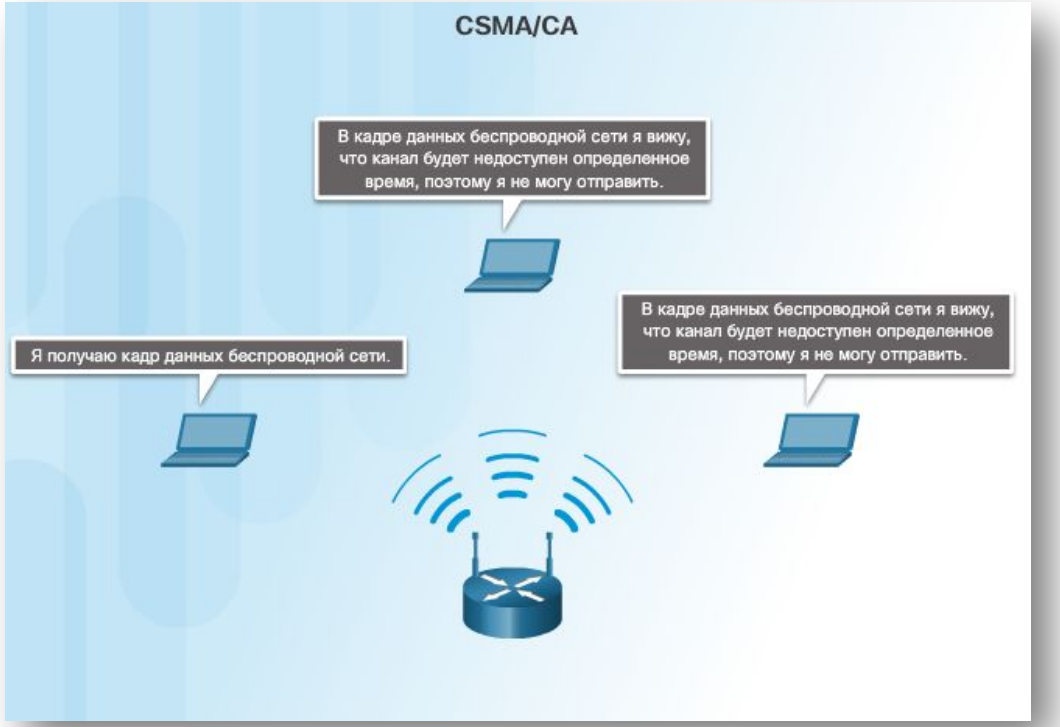
1000BASE-T — в настоящее время наиболее часто реализуемая архитектура Ethernet. Ее название включает в себя характеристики стандарта:

- 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 пр способность кабеля используется для одн
- T означает медный кабель (Twisted pair).



CSMA/CA-IEEE 802.11 — это стандарт, определяющий связь для беспроводных сетей

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 устройств.



Стандарты беспроводной передачи данных

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.

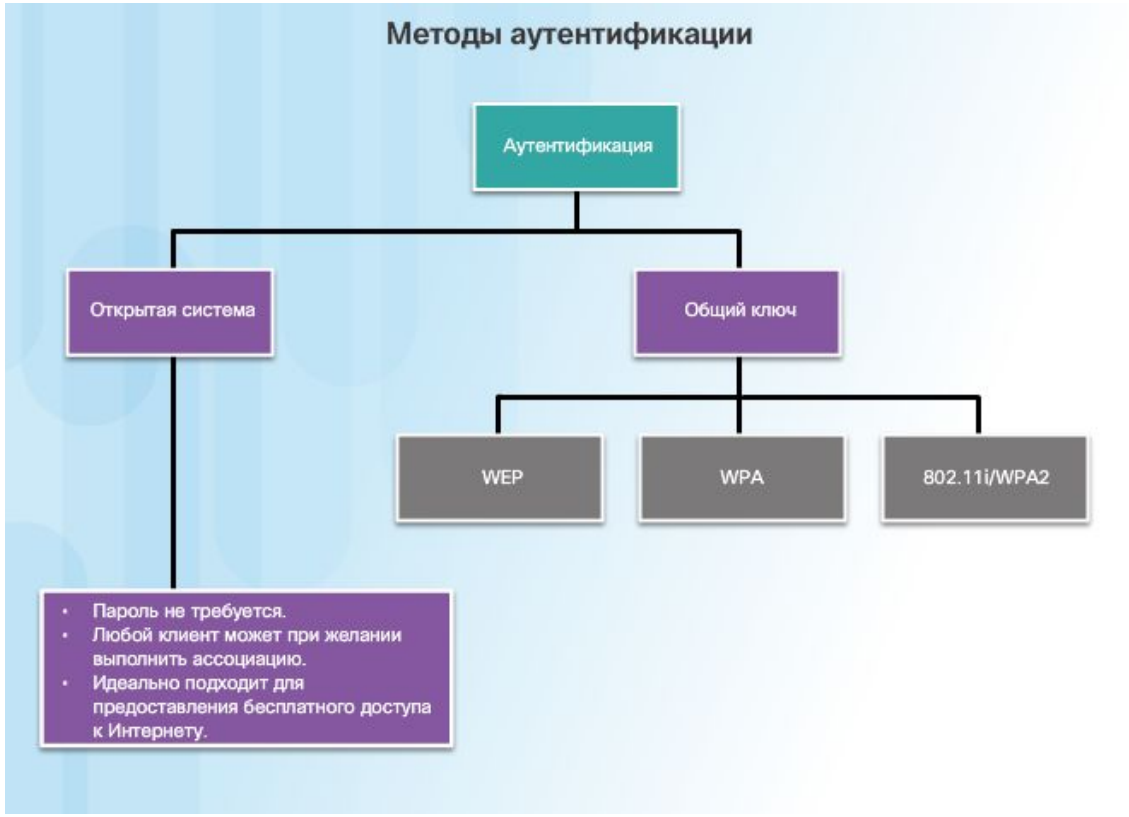
Сравнение стандартов 802.11

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,

- **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.

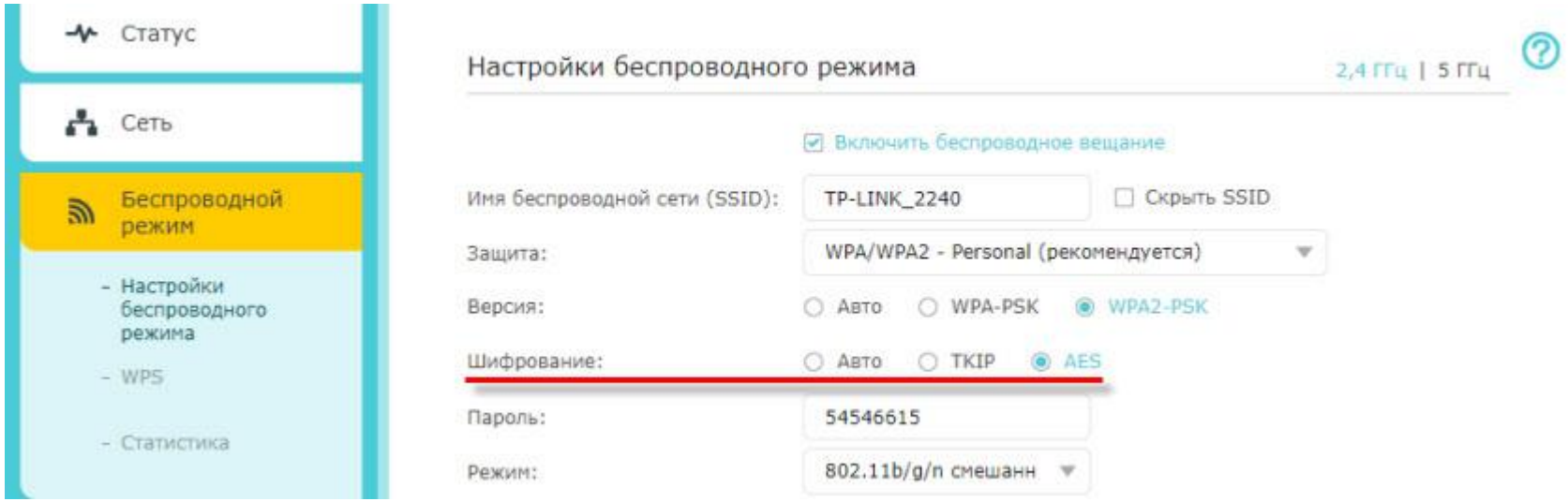
- **Эквивалент секретности проводной сети (Wired Equivalent Privacy, WEP)** — спецификация обеспечения безопасности WLAN, определенная в первоначальном стандарте 802.11. Однако при передаче пакетов ключ не меняется, поэтому его достаточно легко взломать.
- **Защищенный доступ к Wi-Fi (Wi-Fi Protected 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.
- **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 протоколом шифрования.

WPA/WPA2 может быть двух видов:

- **WPA/WPA2** - Personal (PSK) – это обычный способ аутентификации. Когда нужно задать только пароль (ключ) и потом использовать его для подключения к Wi-Fi сети. Используется один пароль для всех устройств. Сам пароль хранится на устройствах. Где его при необходимости можно посмотреть, или сменить. Рекомендуется использовать именно этот вариант.
- **WPA/WPA2** - Enterprise – более сложный метод, который используется в основном для защиты беспроводных сетей в офисах и разных заведениях. Позволяет обеспечить более высокий уровень защиты. Используется только в том случае, когда для авторизации устройств установлен RADIUS-сервер (который выдает пароли).

RADIUS — сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта пользователей, подключающихся к различным сетевым службам. Используется, например, при аутентификации пользователей WiFi, VPN

Шифрование беспроводной сети



Рекомендуется использовать AES. Если у вас в сети есть старые устройства, которые не поддерживают шифрование AES (а только TKIP) и будут проблемы с их подключением к беспроводной сети, то установите "Авто". Тип шифрования TKIP не поддерживается в режиме 802.11n.

Если вы устанавливаете строго WPA2 - Personal (рекомендуется), то будет доступно только шифрование по AES.

Модемы

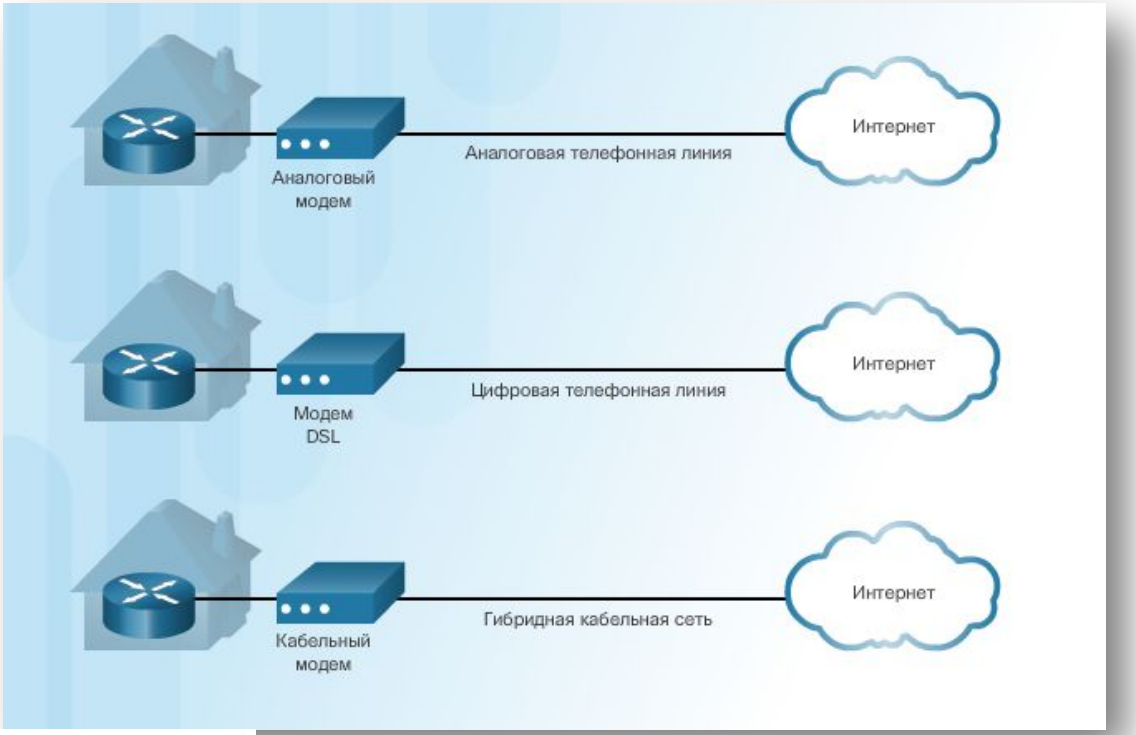
Модемы преобразуют цифровые компьютерные данные в формат, который можно передавать в сеть интернет-провайдера.

Существуют три основных типа модемов.

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

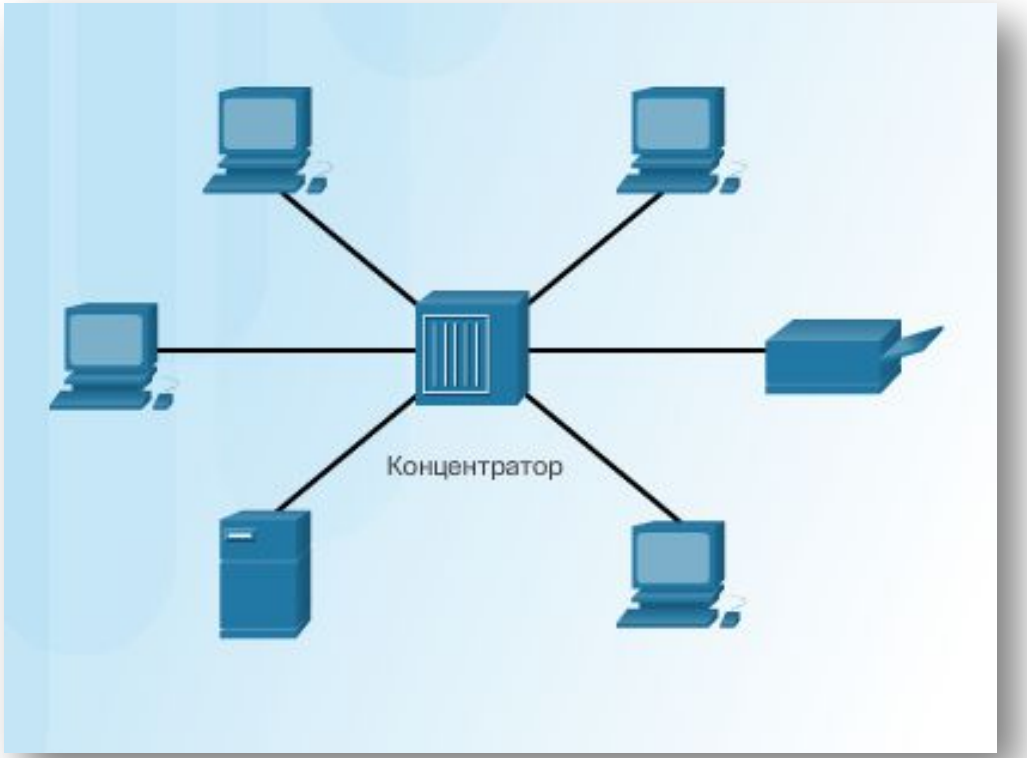
Модем цифровой абонентской линии (DSL) соединяет сеть пользователя непосредственно с инфраструктурой цифровой сети телефонной компании.

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



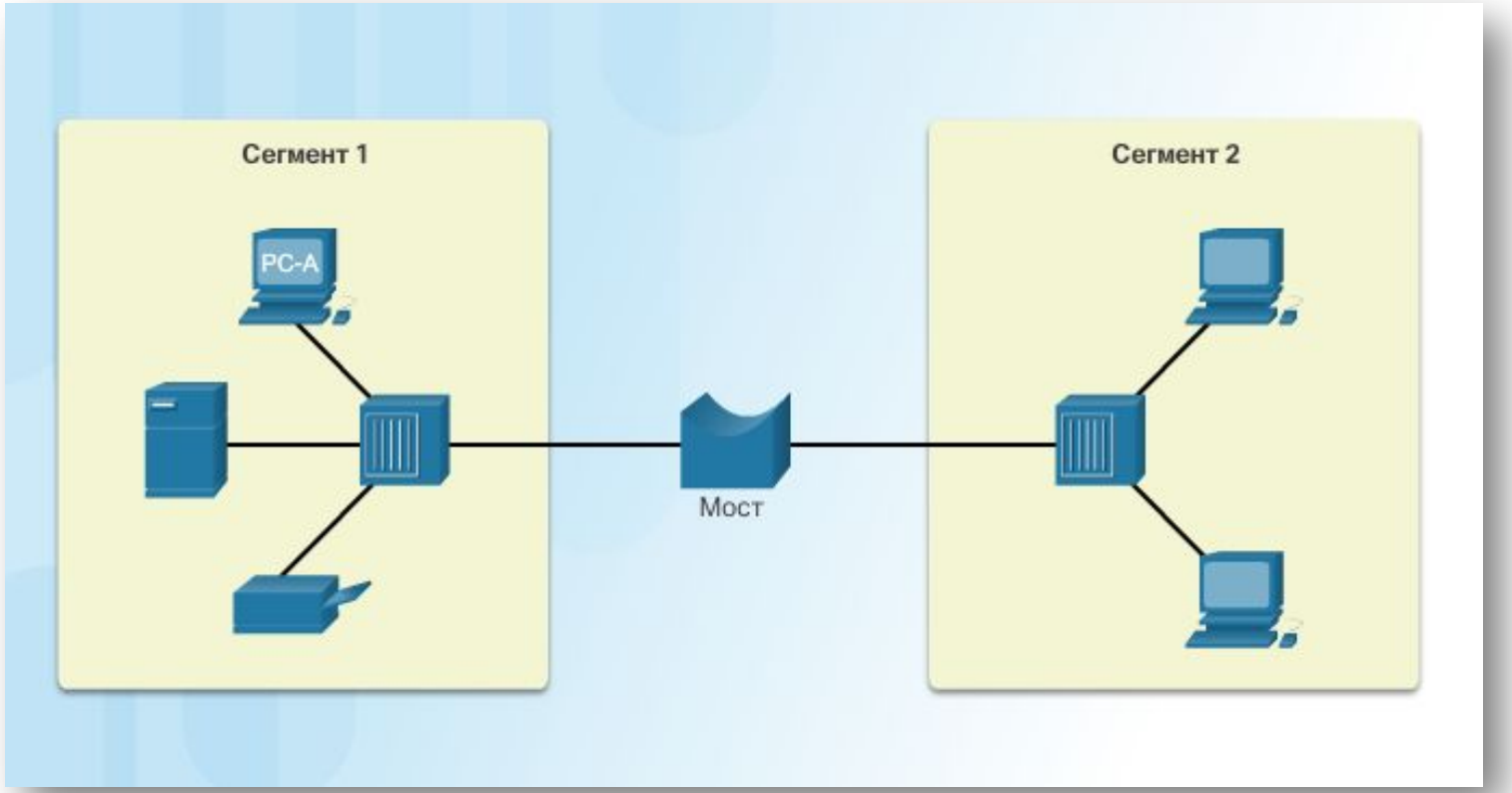
Концентраторы

Концентраторы (hub), принимают данные на одном порте, затем отправляют их на все другие порты.



Мосты

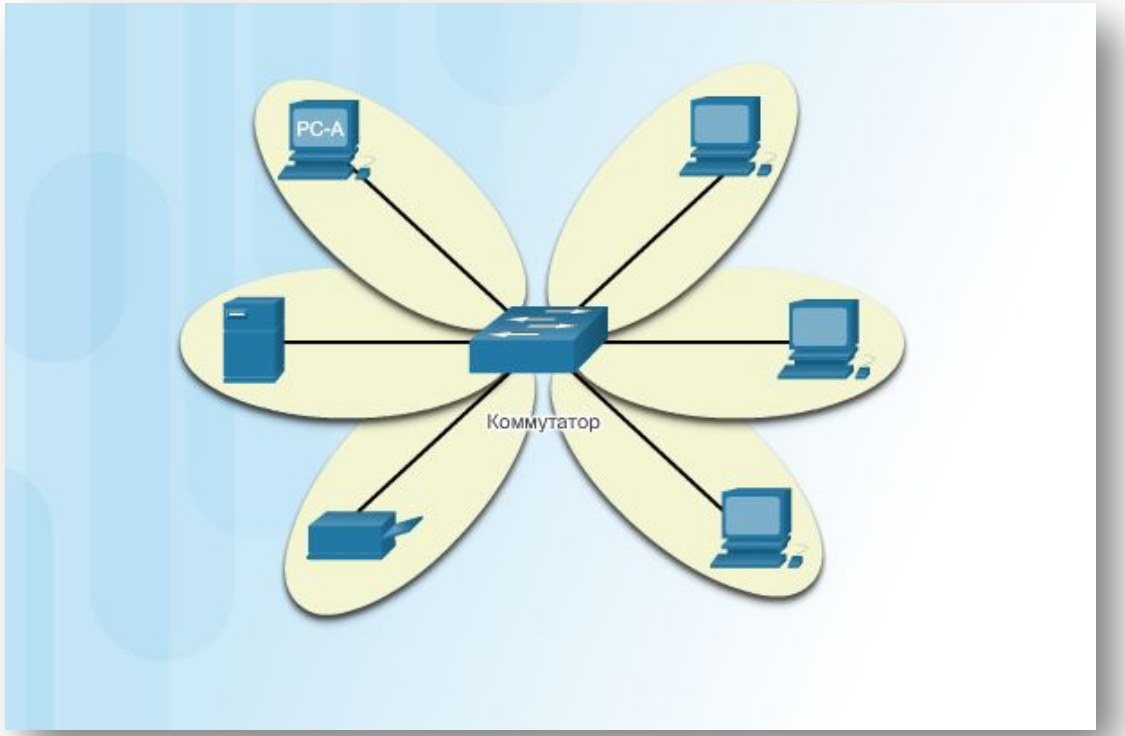
Мосты (bridge) были изобретены для разделения локальных сетей на сегменты.



Мосты запоминают, какие устройства находятся в каждом сегменте. Поэтому мост может выполнять фильтрацию сетевого трафика между сегментами локальной сети.

Коммутаторы

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.



Маршрутизаторы

Маршрутизаторы используют IP-адреса для пересылки трафика в другие сети.

Важное о роутерах, маршрутизаторах и модемах

- Роутер и маршрутизатор – два названия одного устройства.
- Роутер распределяет сигнал между участниками сети, а модем только расшифровывает его и передает на одно устройство.
- У роутера есть собственный IP-адрес, а у модема – нет.
- Роутер – многофункциональное устройство, которое поддерживает тонкую настройку, модем выполняет одну функцию.
- Роутеры (маршрутизаторы) и мобильные модемы могут работать вместе, раздавая Интернет на несколько устройств.

Модем

Роутер

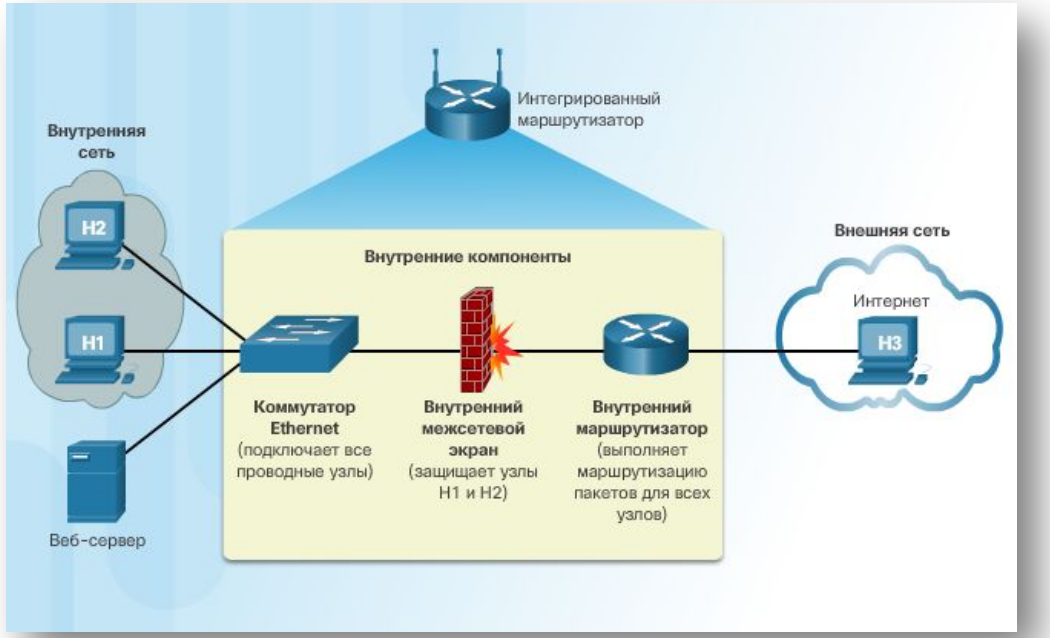
Точки беспроводного доступа и маршрутизаторы

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.

Точки беспроводного доступа обеспечивают только подключение к сети, в то время как беспроводной маршрутизатор предоставляет дополнительные возможности.

Аппаратные межсетевые экраны

Интегрированный маршрутизатор может также служить аппаратным межсетевым экраном. Аппаратные межсетевые экраны защищают данные и оборудование в сети от несанкционированного доступа. Он не использует ресурсы компьютеров, которые защищает, следовательно, не влияет на производительность обработки данных.



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 компьютеров.

Примечание. В защищенной сети, если производительность компьютеров не является проблемой, включите встроенный межсетевой экран операционной системы, чтобы обеспечить дополнительную безопасность

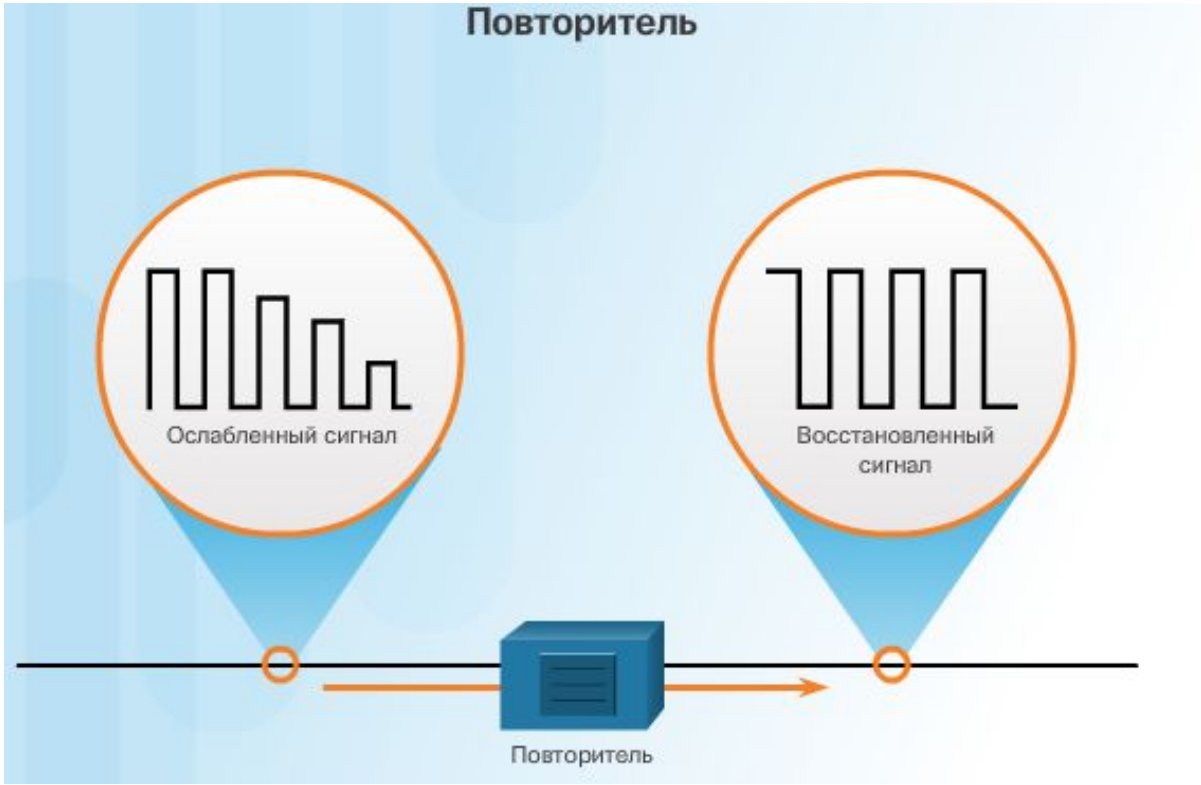
Коммутационные панели

Коммутационная панель (или патч-панель), обычно используется, чтобы собрать в одном месте входящие кабели от различных сетевых устройств.

Коммутационная панель может иметь или не иметь питание. Коммутационная панель с питанием может регенерировать слабые сигналы перед отправкой их на следующее устройство.

Повторители(репиторы)

Регенерация слабых сигналов, является основной функцией повторителей (repeater).

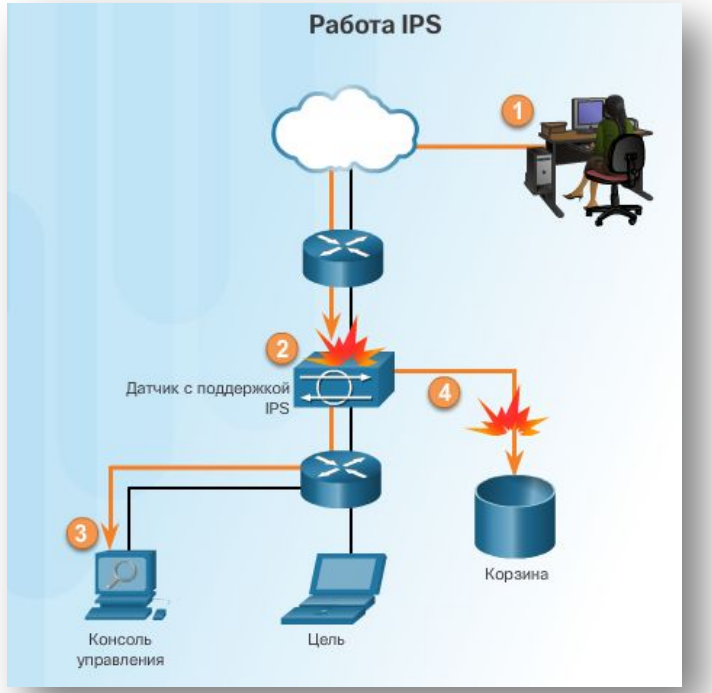


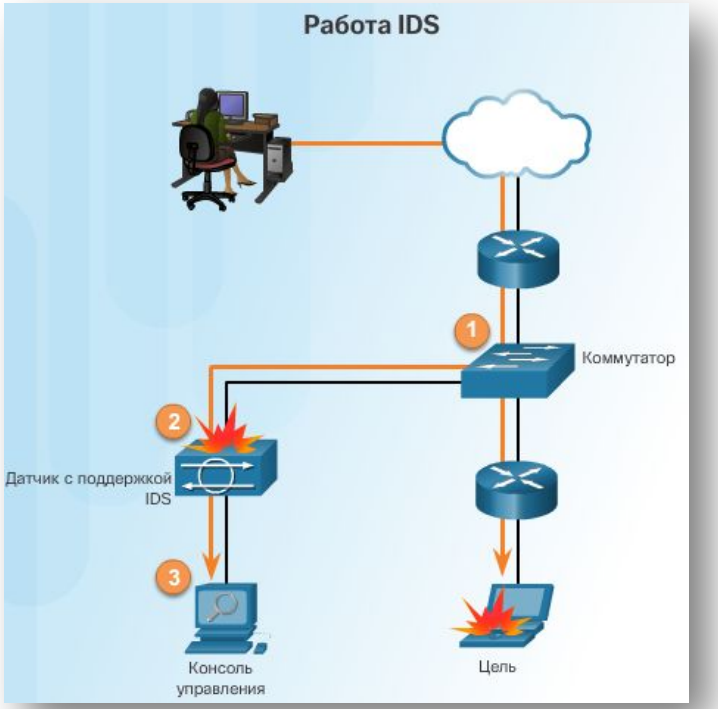
Питание через Ethernet (PoE)

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.

Системы IDS и IPS

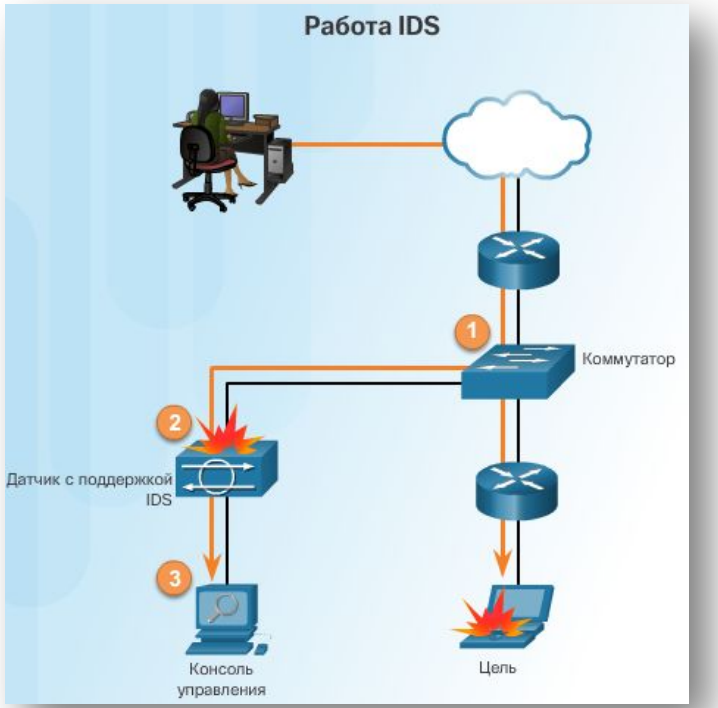
IDS/IPS системы — это уникальные инструменты, созданные для защиты сетей от неавторизованного доступа. Они представляют собой аппаратные или компьютерные средства, которые способны оперативно обнаруживать и эффективно предотвращать вторжения.





Системы IDS

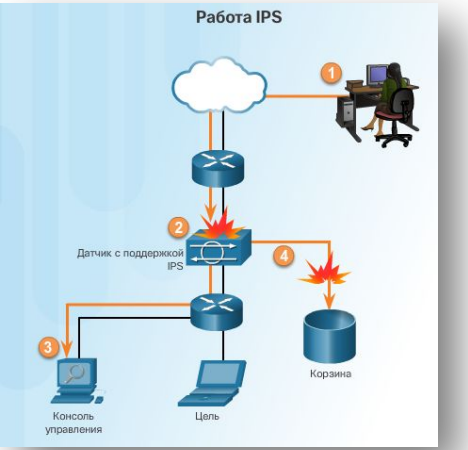
Система обнаружения вторжений (Intrusion Detection System, IDS) выполняет пассивный мониторинг сетевого трафика. Отдельные системы IDS в основном были вытеснены системами предотвращения вторжений (Intrusion Prevention System, IPS). При этом функция обнаружения, выполняемая системами IDS, по-прежнему интегрирована в любую IPS-систему



Системы предотвращения вторжений (IPS)

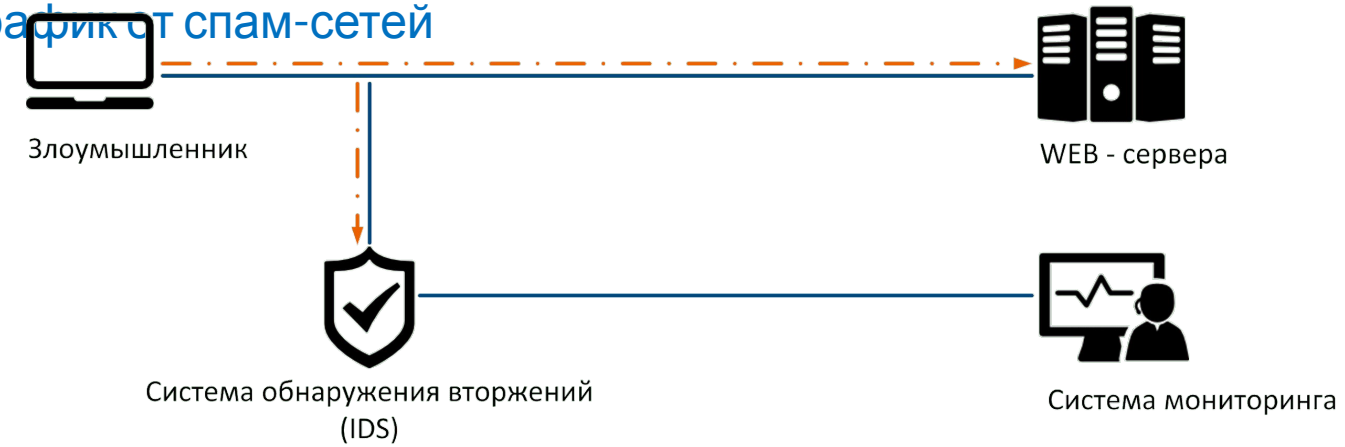
Системы предотвращения вторжений (IPS) основаны на технологиях систем обнаружения вторжений (IDS). Однако устройства IPS реализуются во встроенном (inline) режиме. Это означает, что для обработки весь входящий и исходящий трафик должен проходить непосредственно через это устройство. IPS не допускает попадания пакетов в целевую систему без выполнения их анализа.

Самым существенным отличием между системами IDS и IPS является то, что IPS реагирует на угрозы незамедлительно и не допускает распространение вредоносного трафика, в то время как IDS пропускает такой трафик до принятия специальных мер. Следует отметить, что неправильная настройка IPS может отрицательно сказываться на обмен трафиком в сети.



Использование системы IDS/IPS значительно улучшает безопасность сети. Система IDS/IPS способна:

- предупредить и предотвратить использование скомпрометированных SSL-сертификатов
- предупредить и предотвратить эксплуатирование уязвимостей в протоколах DNS, FTP, ICMP, IMAP, POP3, HTTP, NetBIOS, DCERPC, SNMP, TFTP, VOIP-протоколы
- предупредить и предотвратить использование эксплойтов и уязвимостей сетевых приложений
- предупредить и заблокировать DOS-атаки
- предупредить и заблокировать случаи сетевого сканирования
- заблокировать трафик ботнетов
- заблокировать трафик от скомпрометированных хостов
- заблокировать трафик от хостов, зараженных троянским ПО и сетевыми червями
- заблокировать трафик от спам-сетей



Системы унифицированного управления угрозами (UTM)

Системы унифицированного управления угрозами - это общее название для систем безопасности, выполненных по принципу «все в одном». Системы унифицированного управления угрозами (UTM) выполняют все функции IDS/IPS, а также межсетевого экрана с сохранением состояний

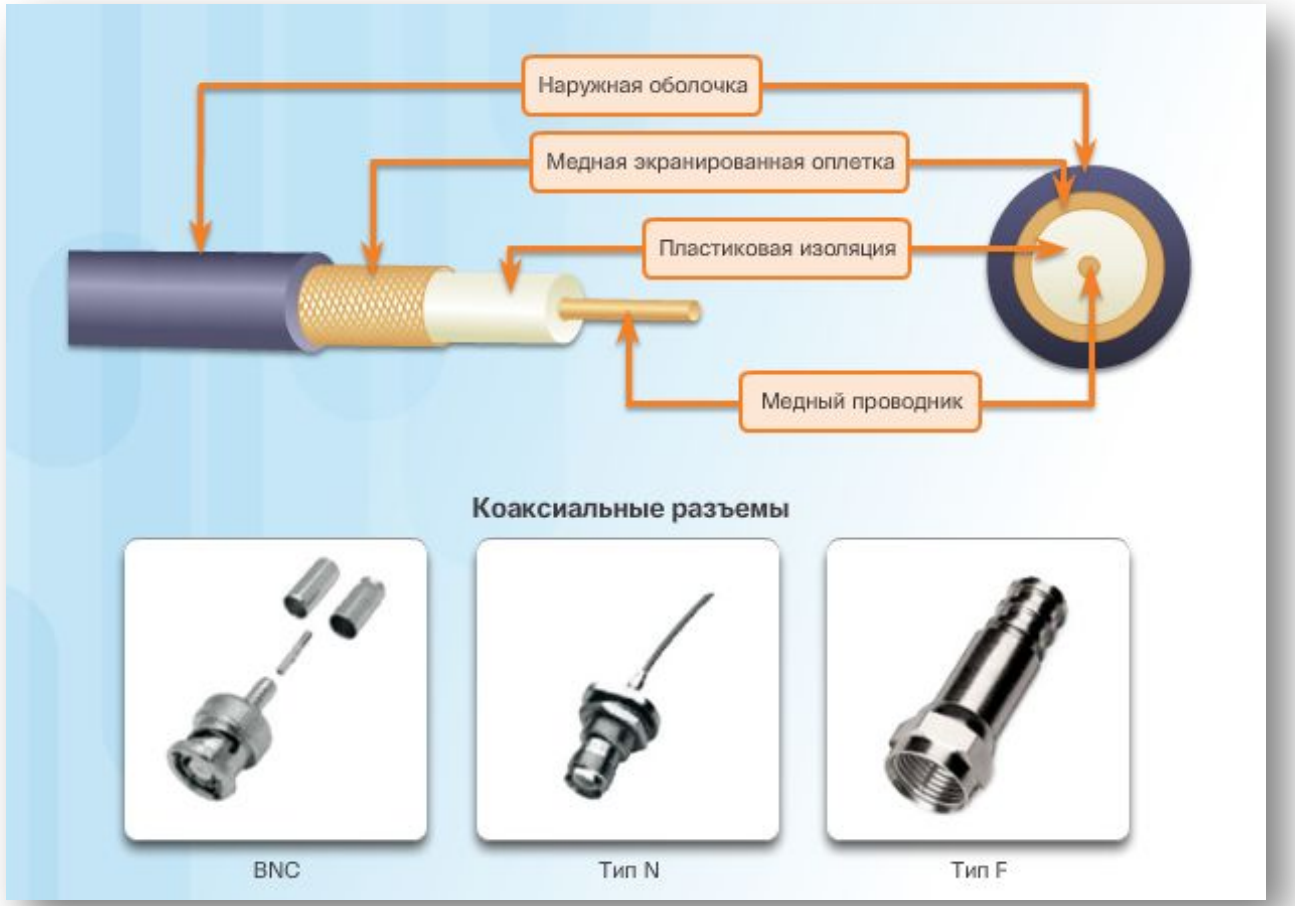
В дополнение к функциям IDS/IPS и межсетевого экрана с сохранением состояний UTM обычно выполняют и другие функции безопасности.

- Защита от новых угроз
- Защита от DoS-атак и DDoS-атак
- Прокси-фильтрация приложений
- Фильтрация электронной почты для защиты от спама и фишинговых атак
- Антишпионское ПО
- Управление доступом к сети
- VPN-сервисы

В зависимости от марки UTM объем доступных функций может существенно отличаться.

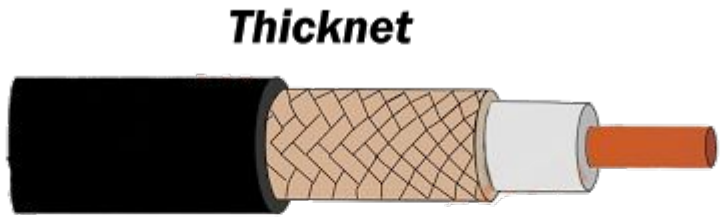
Коаксиальный кабель(DOCSIS)

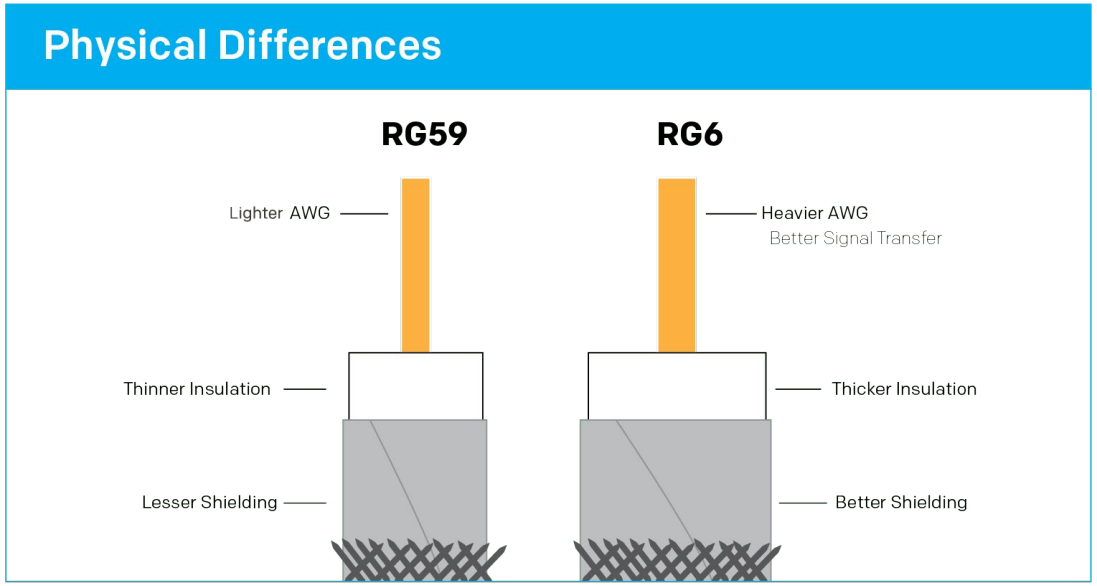
По коаксиальному кабелю проходят данные в форме электрических сигналов. Экранирование у него лучше, чем у неэкранированной витой пары (UTP), отношение сигнала к шуму выше, и данных передается больше.



Существует несколько типов коаксиальных кабелей.

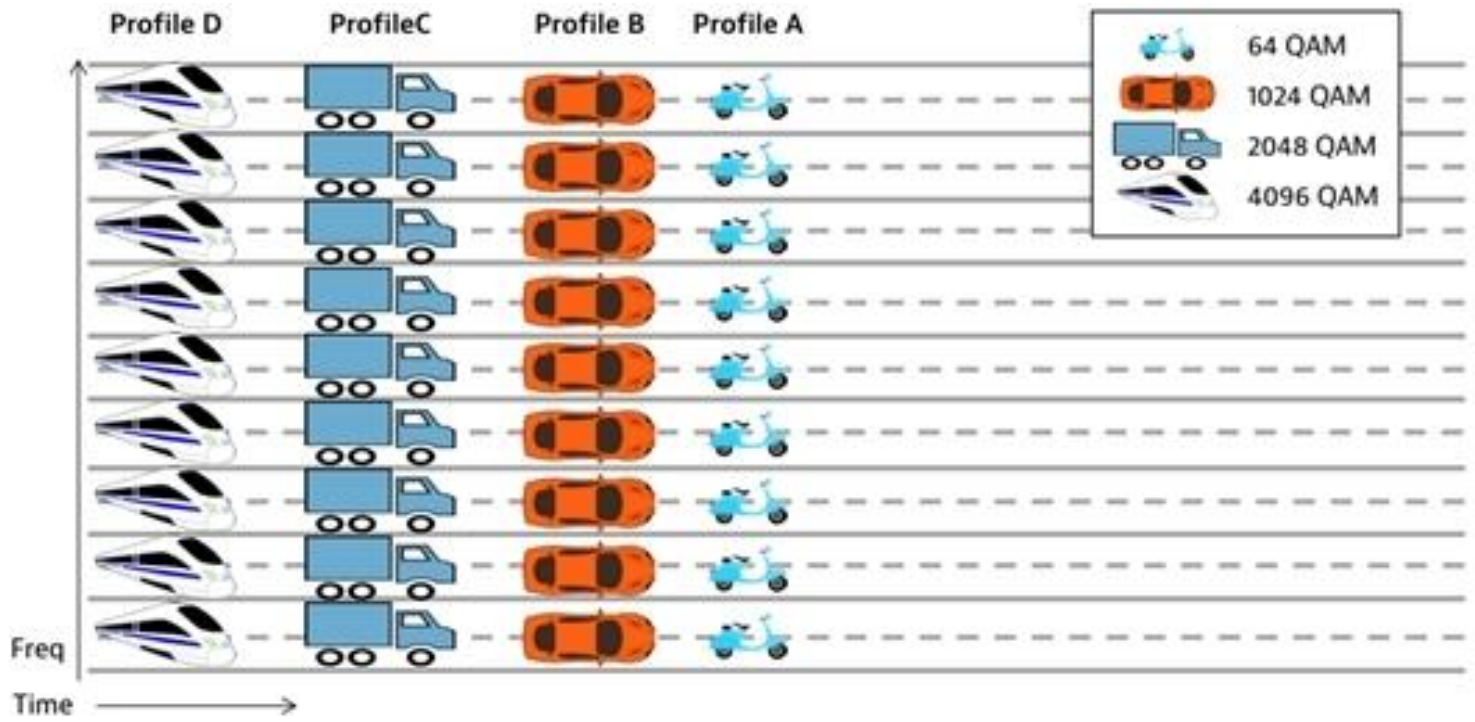
- **Thicknet или 10BASE5** — используется в сетях и работает на скорости 10 Мбит/с с максимальной длиной 500 м.
- **Thinnet 10BASE2** — используется в сетях и работает на скорости 10 Мбит/с с максимальной длиной 185 м.
- **RG-59** — чаще всего используется для кабельного телевидения в США.
- **RG-6** — кабель более высокого качества, чем RG-59, с большой пропускной способностью и менее подверженный помехам.





Американский исследовательский консорциум CableLabs разработал новую поправку к стандарту высокоскоростной передачи данных **DOCSIS 3.1**, определяющему стандарты передачи информации по коаксиальному, то есть телевизионному кабелю

После введения поправки в стандарте DOCSIS отправка и прием данных будут возможны на скорости до десяти гигабит в секунду.

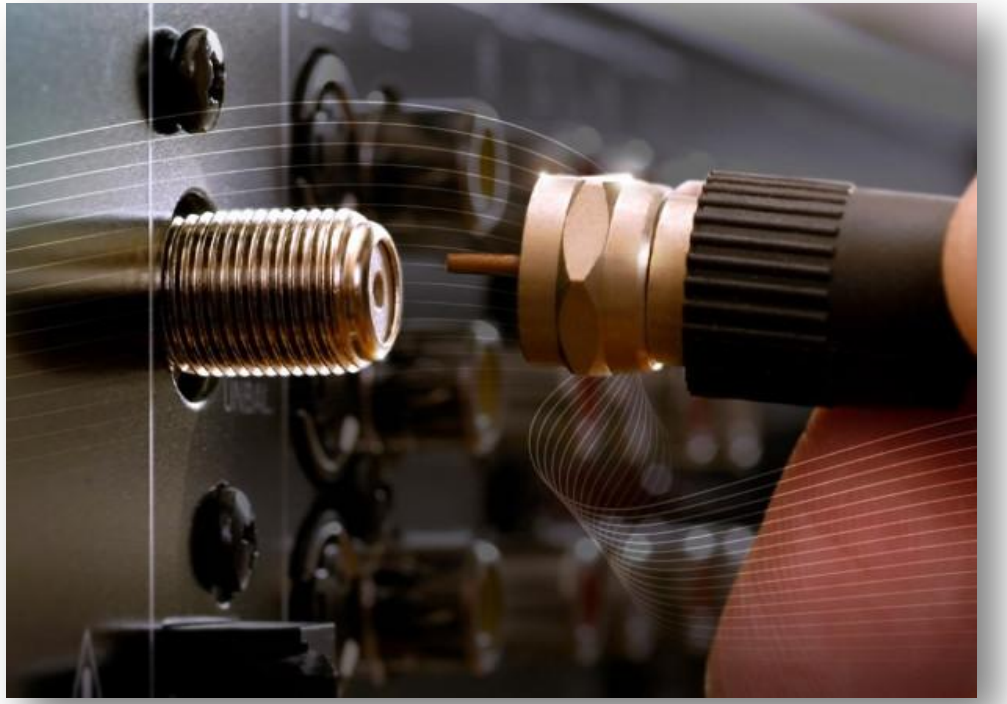


Стандарт DOCSIS был разработан и введен консорциумом CableLabs в 1998 году в рамках масштабной программы по увеличению количества абонентов, подключенных к интернету

Первая версия нового стандарта в США оговаривала возможность передачи данных абоненту (прямой канал) на скорости до 42 мегабит в секунду и приема (обратный) на скорости до 10,4 мегабит в секунду. Для обмена информацией использовались каналы шириной шесть мегагерц. Чуть позже в Европе была разработана локализованная версия стандарта, получившая название EuroDOCSIS. Она использует для передачи данных каналы шириной восемь мегагерц. В европейском стандарте первой версии скорость прямого канала 55,6 мегабита в секунду, а обратного — только 10,2.

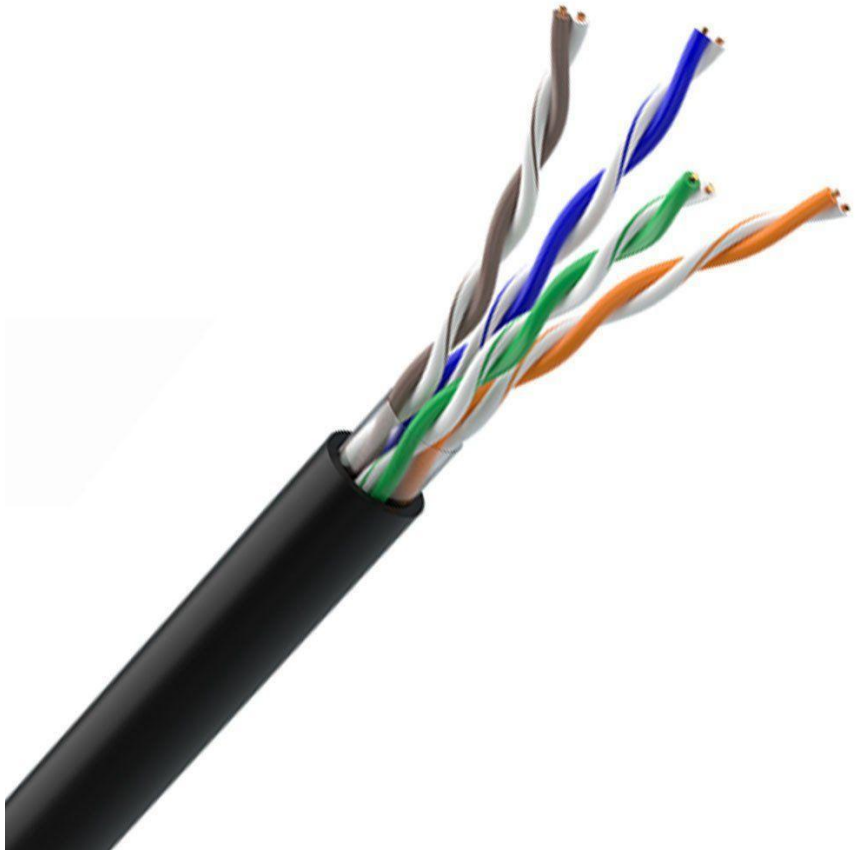
В 2013 году CableLabs представила новейший стандарт DOCSIS 3.1. В этом стандарте, если говорить упрощенно, впервые было решено отказаться от передачи данных по каналам шириной шесть и восемь мегагерц и использовать так называемые поднесущие частоты шириной от 20 до 50 килогерц. При этом новый стандарт разрешает множественное объединение этих поднесущих, что, в конечном итоге, позволяет обеспечить скорость прямого канала в десять гигабит в секунду, а обратного — в один гигабит в секунду.

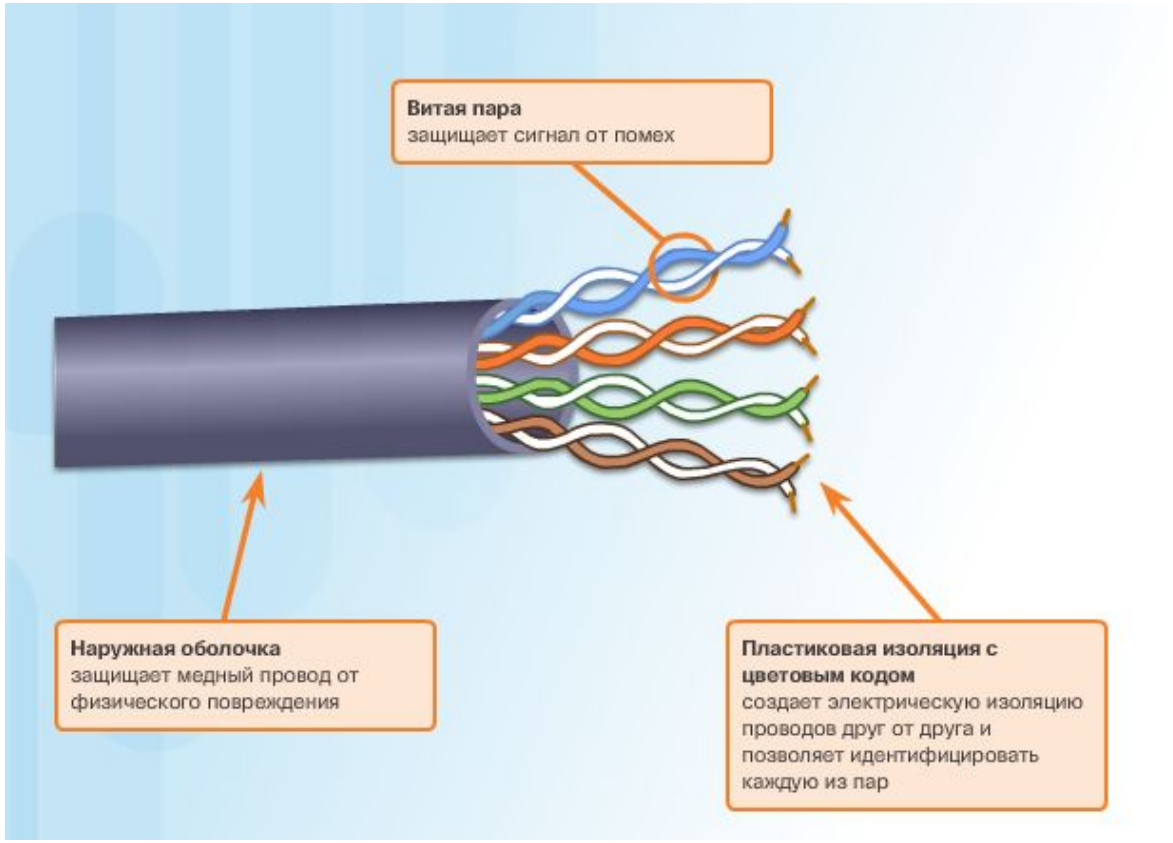
Как ожидается, коммерческое внедрение нового стандарта, получившего название DOCSIS 3.1 FD (Full Duplex, полный дуплекс) начнется в 2019 году. Ранее некоторые производители кабельных модемов для работы в сетях стандарта DOCSIS представили устройства, способные работать с полнодуплексным протоколом. В частности, компания Cisco в мае текущего года провела демонстрацию кабельного модема с равноскоростными прямым и обратным каналами. Это устройство для совместной отправки и приема данных позволяет использовать 576 мегагерц из всего кабельного спектра.



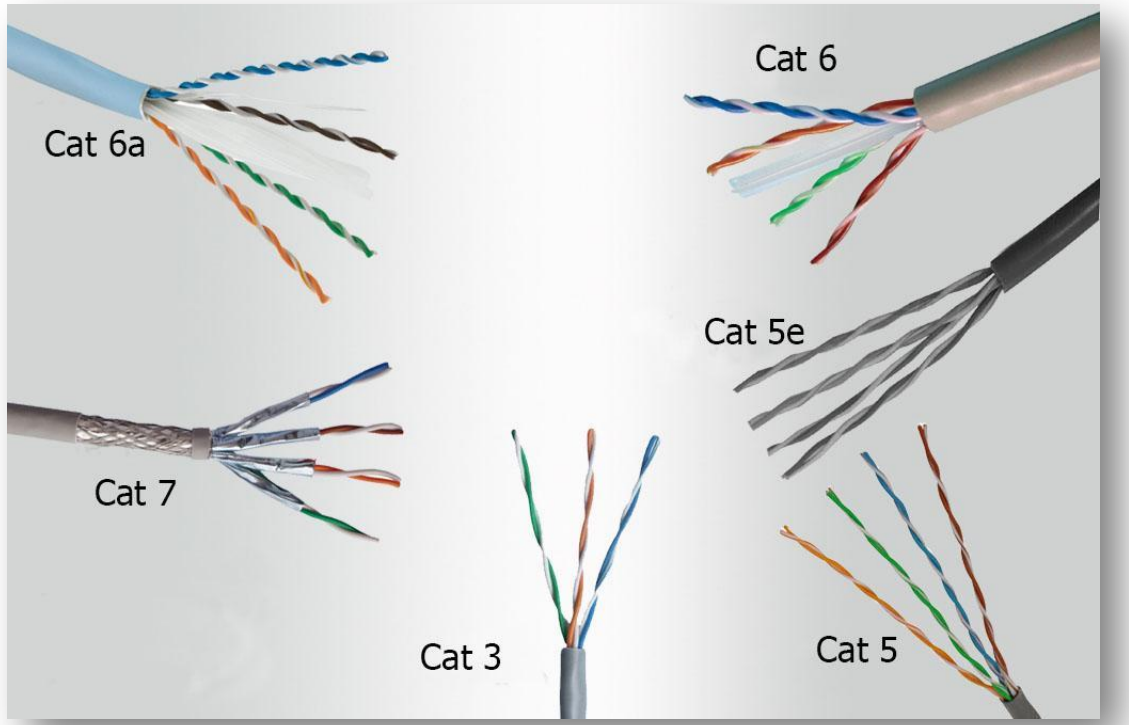
Кабели «витая пара»

Витая пара — это тип медного кабеля, используемый для телефонной связи и большинства сетей Ethernet. Витая пара обеспечивает защиту от взаимных или перекрестных наводок, т. е. от шума, создаваемого соседними парами проводов в кабеле.





Характеристики категорий витых пар



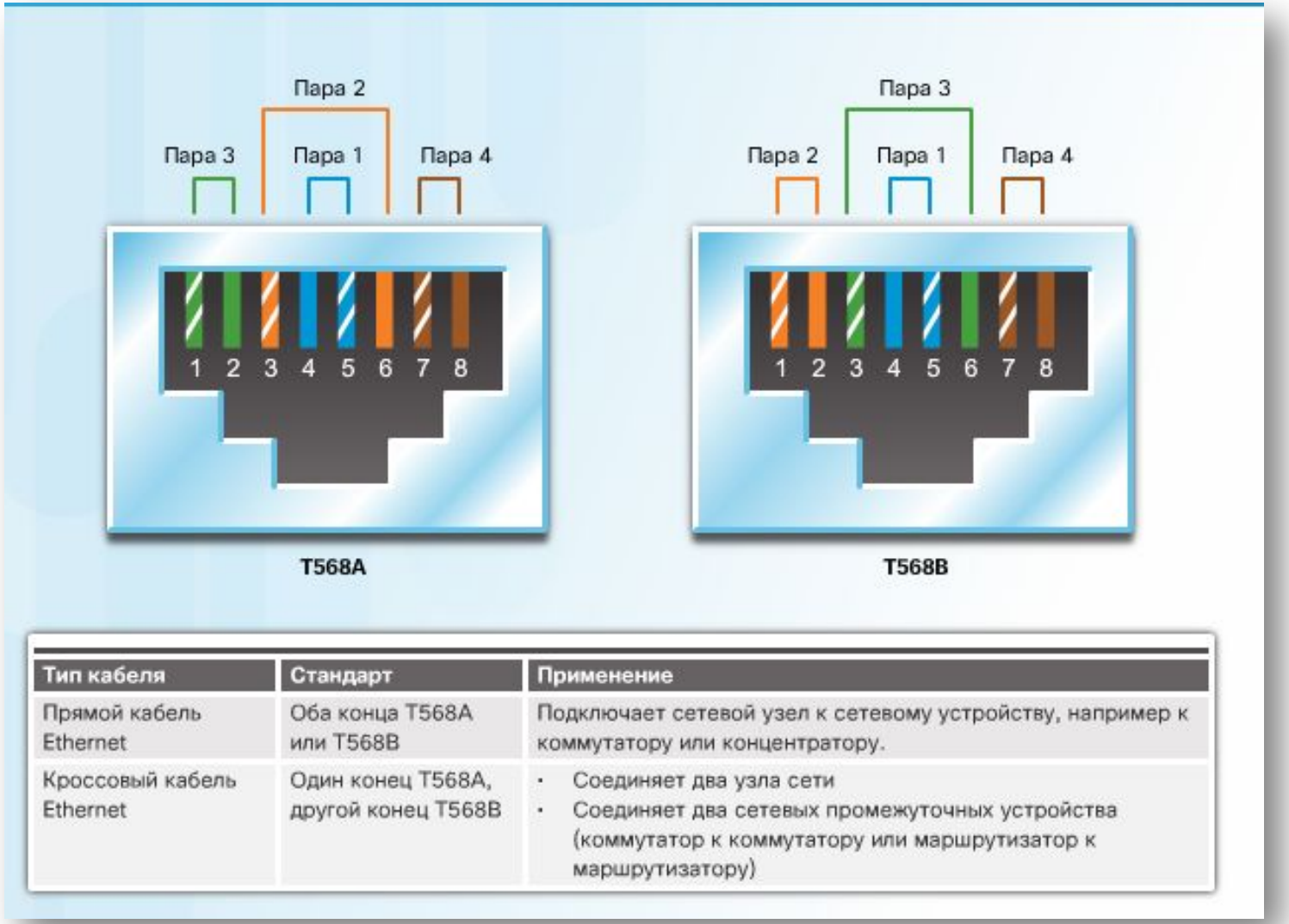
Характеристики кабеля «витая пара»

	Скорость	Функции
UTP категории 3	10 Мбит/с при частоте 16 МГц	• Подходит для локальной сеть Ethernet. • Наиболее часто используется для телефонных линий.
UTP категории 5	100 Мбит/с при частоте 100 МГц	Изготавливается по более строгим стандартам, чем категория 3, для обеспечения более высоких скоростей передачи данных.
UTP категории 5e	1000 Мбит/с при частоте 100 МГц	• Изготавливается по более строгим стандартам, чем категория 5, для обеспечения более высоких скоростей передачи данных. • Меньше число витков на единицу длины, чем у категории 5. Это обеспечивает более эффективную защиту от электромагнитных и радиочастотных помех от внешних источников.
UTP категории 6	1000 Мбит/с при частоте 250 МГц	• Изготавливается по ещё более строгим стандартам, чем категория 5e. • Меньше число витков на единицу длины, чем категория 5e. Это обеспечивает более эффективную защиту от электромагнитных и радиочастотных помех от внешних источников. • Кабель категории 6a имеет лучшую изоляцию и
Неэкранированная витая пара категории 6a	1000 Мбит/с при частоте 500 МГц	
Экранированная витая пара	10 Мбит/с при частоте 600 МГц	

В основу определения категории витой пары положен максимально пропускаемый частотный диапазон. Это обусловлено количеством витков на одну единицу длины кабеля. То бишь, чем выше категория, тем больше пропускаемый частотный диапазон в следствии увеличения витков каждой витой пары.

UTP — (Unshielded twisted pair — неэкранированная витая пара) — кабель не имеет защитного экрана.
FTP или F/UTP — (Foiled twisted pair — фольгированная витая пара) — кабель имеет один внешний общий защитный слой из фольги.
STP (Shielded twisted pair — экранированная витая пара) — кабель имеет экран для каждой пары и внешнюю защиту наподобие сетки .
S/FTP или SSTP (Screened Foiled twisted pair — фольгированная экранированная витая пара) — данный кабель имеет фольгированную защиту каждой пары, а также внешний экран.
U/STP (Unshielded Screened twisted pair — незащищенный кабель с экранированием витой пары) — кабель не имеет общего экрана, но каждая пара имеет фольгированную защиту.
SF/UTP или SFTP (Screened Foiled Unshielded twisted pair — экранированная витая пара с защитой) — имеет два внешних экрана. Один из медной сетки, а второй из экран-фольги. Между ними дренажный провод.

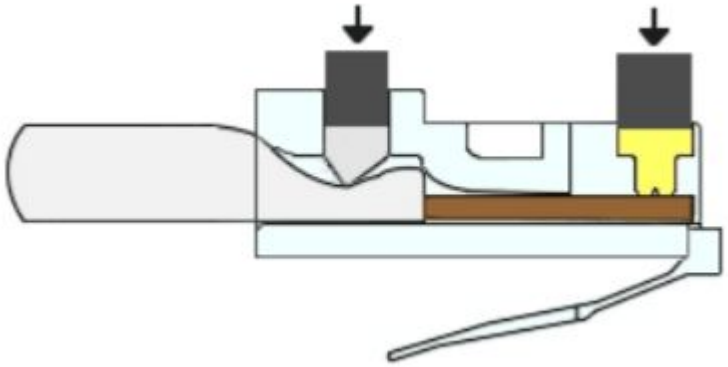
Схемы соединения проводников витой пары



Тип кабеля	Стандарт	Применение
Прямой кабель Ethernet	Оба конца T568A или T568B	Подключает сетевой узел к сетевому устройству, например к коммутатору или концентратору.
Кроссовый кабель Ethernet	Один конец T568A, другой конец T568B	• Соединяет два узла сети • Соединяет два сетевых промежуточных устройства (коммутатор к коммутатору или маршрутизатор к маршрутизатору)

Инструменты для витой пары

Лабораторная работа. Создание и тестирование сетевого кабеля 5.4.2.8



Волоконно-оптические кабели

Волоконно-оптический кабель для передачи сигнала использует свет, поэтому он нечувствителен к электромагнитным и радиочастотным помехам.

Внешняя оболочка

Оболочка, обычно из ПВХ, защищает оптическое волокна от истирания, влаги и загрязняющих веществ. Состав внешней оболочки зависит от области применения кабеля.

Уплотняющий слой

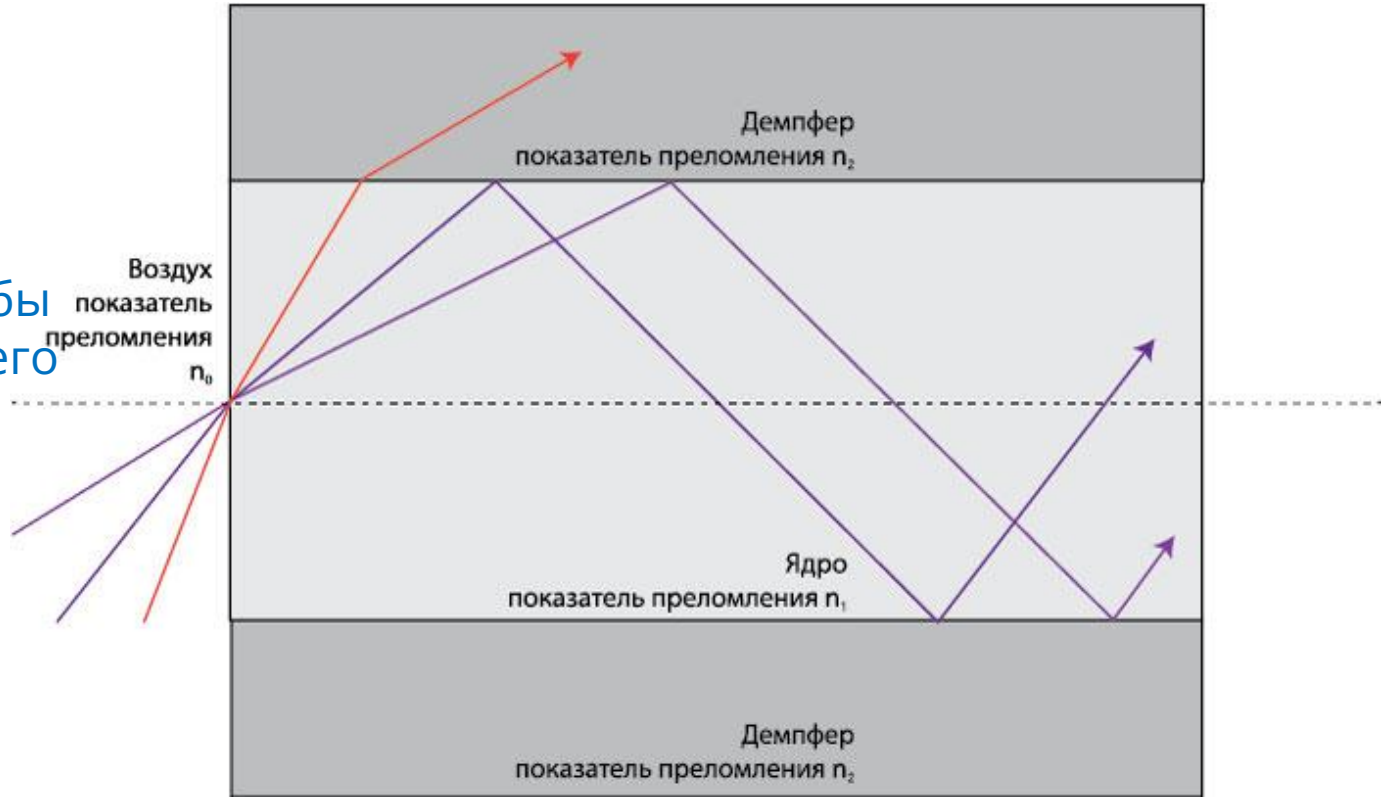
Окружает буфер и защищает оптоволоконный кабель от растяжения при вытягивании. Для уплотняющего слоя часто используют тот же материал, что и для изготовления бронежилетов.

Буфер

Используется для защиты сердечника кабеля и оболочки оптического волокна от повреждений.

Преломления ядра несколько выше, чем показатель преломления демпфера

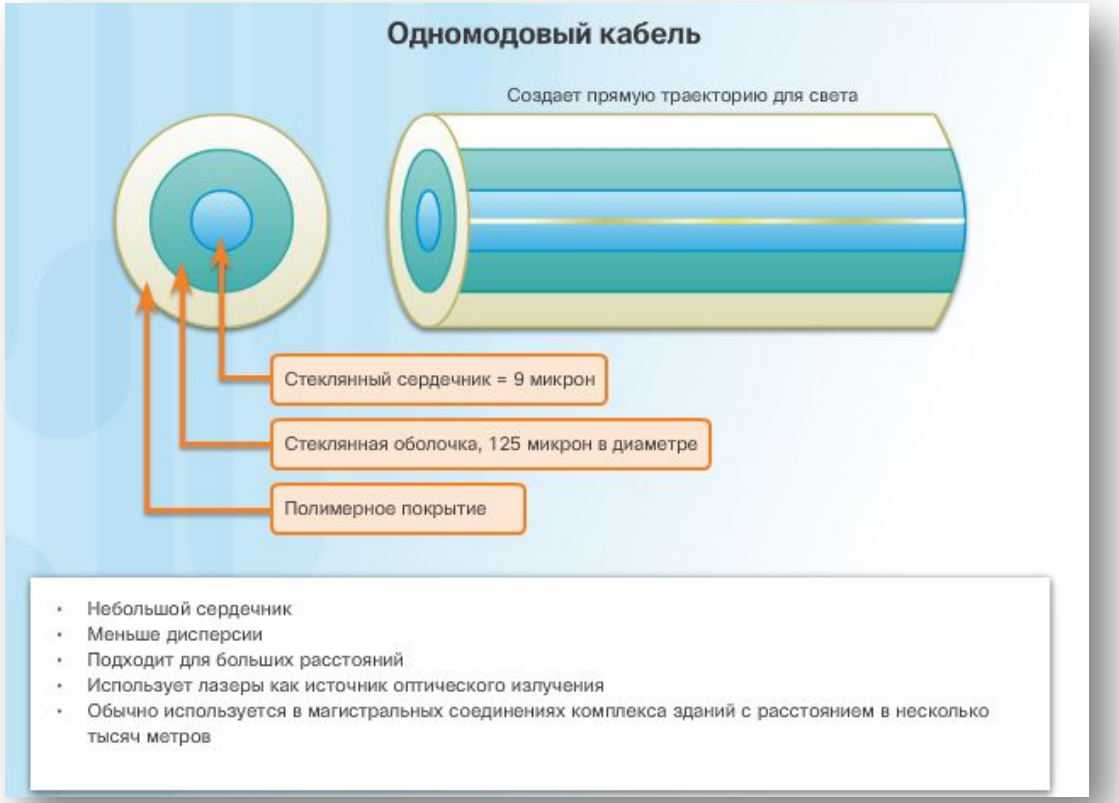
И ядро, и демпфер изготавливаются из кварцевого стекла, при этом показатель преломления ядра несколько выше, чем показатель преломления демпфера, чтобы реализовать явление полного внутреннего отражения.



Одномодовый оптоволоконный кабель (single-mode fiber, SMF)

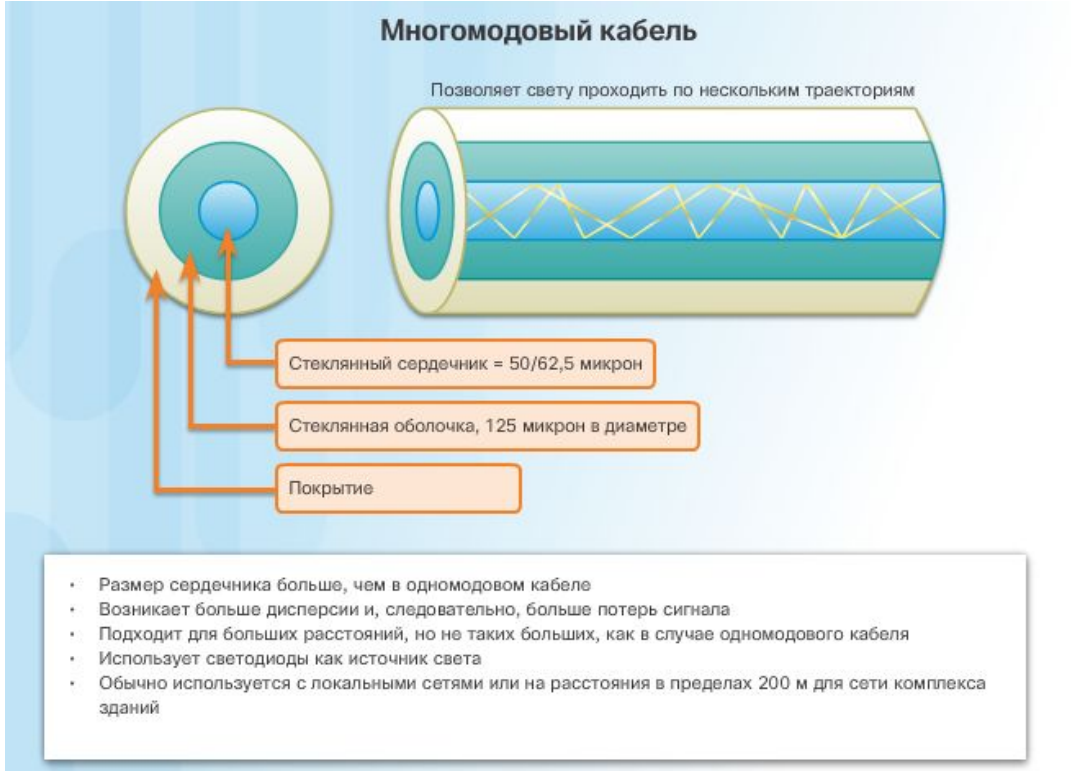
Одномодовый оптоволоконный кабель (single-mode fiber, SMF). Имеет сердечник очень малого диаметра. Для передачи луча света требуется лазерная технология. Широко используется для организации линий связи протяженностью несколько сот километров, например для дальней телефонии и кабельного телевидения.

Одномодовые волокна делятся на классы OS1 (обычные световоды, используемые для передачи на длинах волн либо 1310 нм, либо 1550 нм) и OS2,



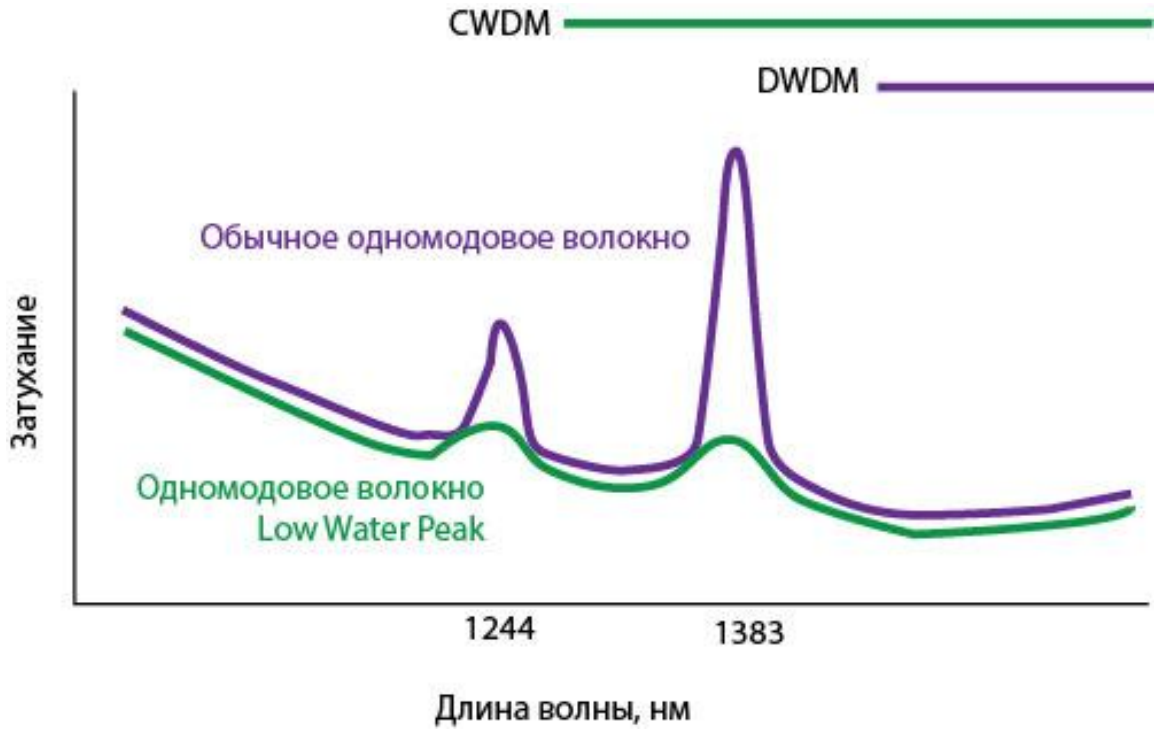
Многомодовый оптоволоконный кабель (Multi-mode fiber, MMF)

Имеет сердечник большего диаметра. Для передачи световых импульсов используются светодиодные излучатели. Как показано на рисунке, свет, излучаемый светодиодом, входит в многомодовое волокно под разными углами. Такие кабели популярны в локальных сетях, поскольку позволяют использовать для работы недорогие светодиоды. Многомодовый кабель обеспечивает пропускную способность до 10 Гбит/с на расстоянии до 550 метров.



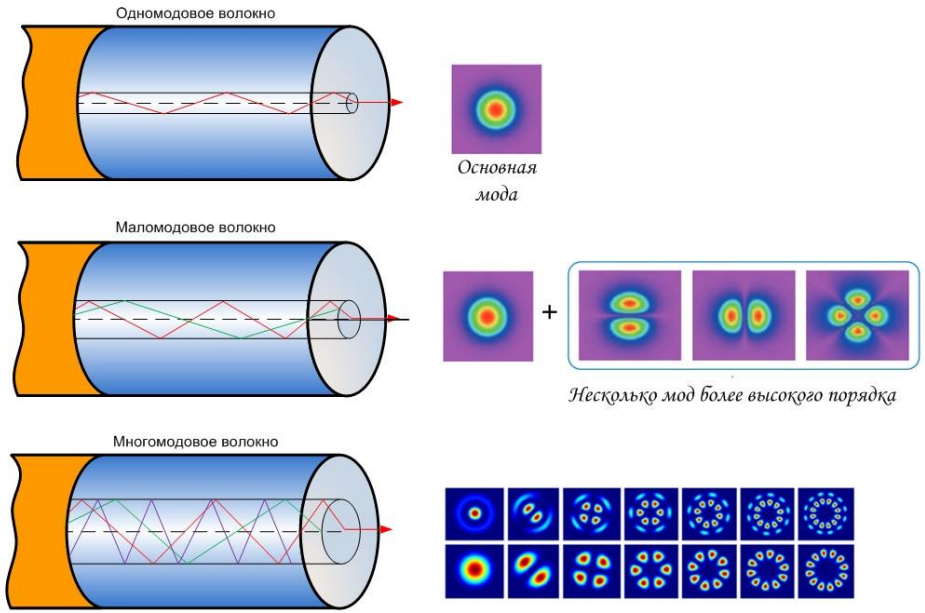
Одномодовый и многомодовый волоконно-оптический кабель: правила выбора

Диаметр ядра одномодовых волокон составляет 9 мкм, многомодовых – 50 или 62.5 мкм, при этом диаметр демпфера у всех волокон одинаков и составляет 125 мкм



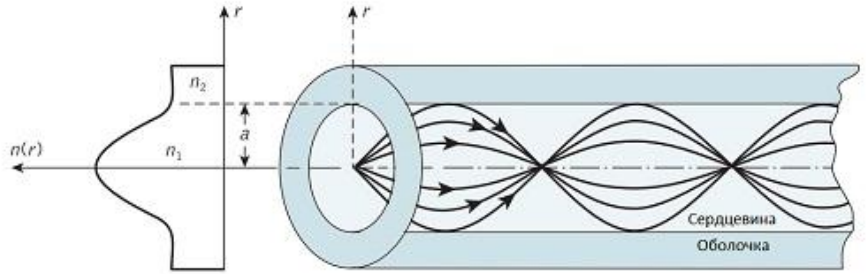
Одномодовое волокно используется:

- в морских и трансокеанских кабельных линиях связи;
- в наземных магистральных линиях дальней связи;
- в провайдерских линиях, линиях связи между городскими узлами, в выделенных оптических каналах большой протяженности, в магистралях к оборудованию операторов мобильной связи;
- в системах кабельного телевидения (в первую очередь OS2, широкополосная передача);
- в системах GPON с доведением волокна до оптического модема, размещаемого у конечного пользователя;
- в СКС в магистралях длиной более 550 м (как правило, между зданиями);
- в СКС, обслуживающих центры обработки данных, независимо от расстояния.



Многомодовое волокно в основном используется:

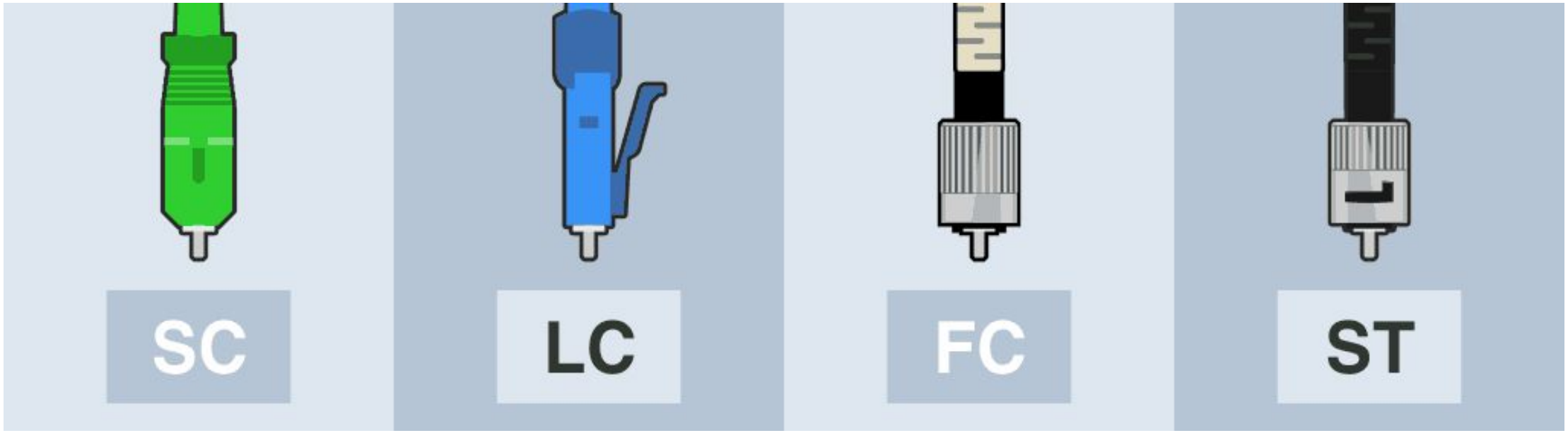
- в СКС в магистралях внутри здания (где, как правило, расстояния укладываются в 300 м) и в магистралях между зданиями, если расстояние не превышает 300-550 м;
- в горизонтальных сегментах СКС и в системах FTTD (*fiber-to-the-desk*), где пользователям устанавливаются рабочие станции с многомодовыми оптическими сетевыми картами;
- в центрах обработки данных в дополнение к одномодовому волокну;
- во всех случаях, где расстояние позволяет применять многомодовые кабели. Хотя сами кабели обходятся дороже, экономия на активном оборудовании покрывает эти затраты.



Оптоволоконные разъемы

Оптоволоконный разъем монтируется на конце оптического волокна. Существуют различные типы оптоволоконных разъемов. Основные отличия между этими типами заключаются в размерах и методах механических соединений

Наиболее распространенные типы оптических разъемов



РАЗЪЕМ FC

РАЗЪЕМ FC

- **«FC» означает...** Ferrule Connector.
- **Краткая история**: Это был первый оптический разъем с использованием керамического наконечника, разработанный Nippon Telephone and Telegraph. Его использование становится все менее распространенным в пользу разъемов SC и LC.
- **Особенности**: резьбовое соединение разъема является виброустойчивым; поэтому он используется в приложениях в движении. Он также используется в точных приборах (таких как рефлектометры) и очень популярен в кабельном телевидении.
- **Оптические характеристики**: для одномодовых волокон. Его вносимые потери достигают 0,3 дБ.

ST CONNECTOR

ST CONNECTOR

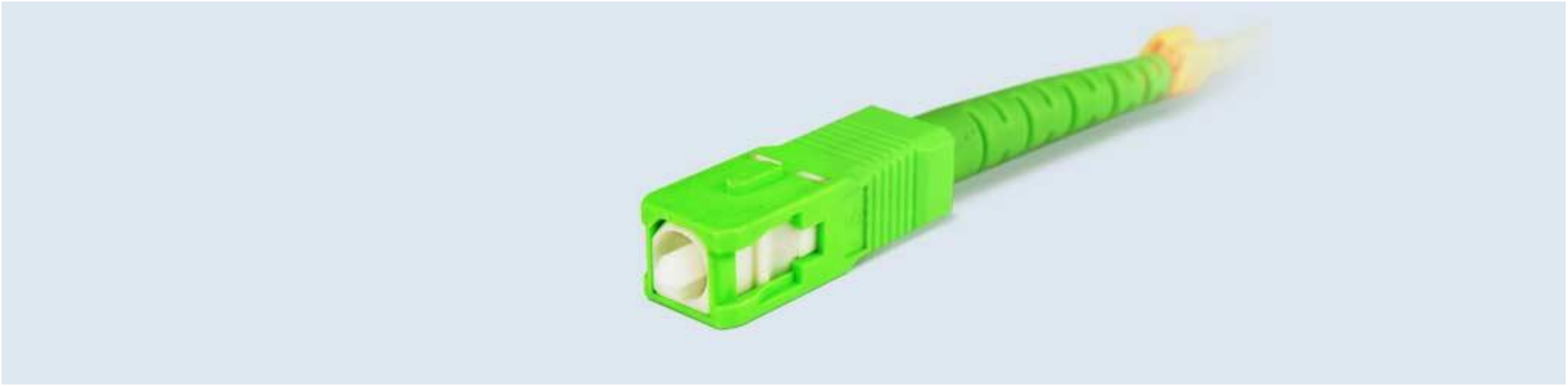
- **«ST» означает...** Straight Tip.
- **Краткая история**: разработан в США компанией AT&T и используется в профессиональной среде, такой как корпоративные сети, а также в военной области.
- **Особенности**: Его форма напоминает японский соединитель FC, за исключением его фитингов BNC-типа (поворотный замок, также называемый байонетным фитингом).
- **Оптические характеристики**: для многомодовых волокон. Его вносимые потери достигают 0,25 дБ.

РАЗЪЕМ LC

РАЗЪЕМ LC

- **«LC» означает...** Lucent Connector или Little Connector.
- **Краткая история**: Разработано Lucent Technologies и выпущено в 1997 году.
- **Особенности**: Фитинг двухтактный (напоминает RJ45). Надежнее и компактнее, чем у типа SC, что позволяет еще большую плотность разъемов в стойках, панелях и FTTH.
- **Оптические характеристики**: для одномодовых и многомодовых волокон. Потери 0,10 дБ.

РАЗЪЕМ SC

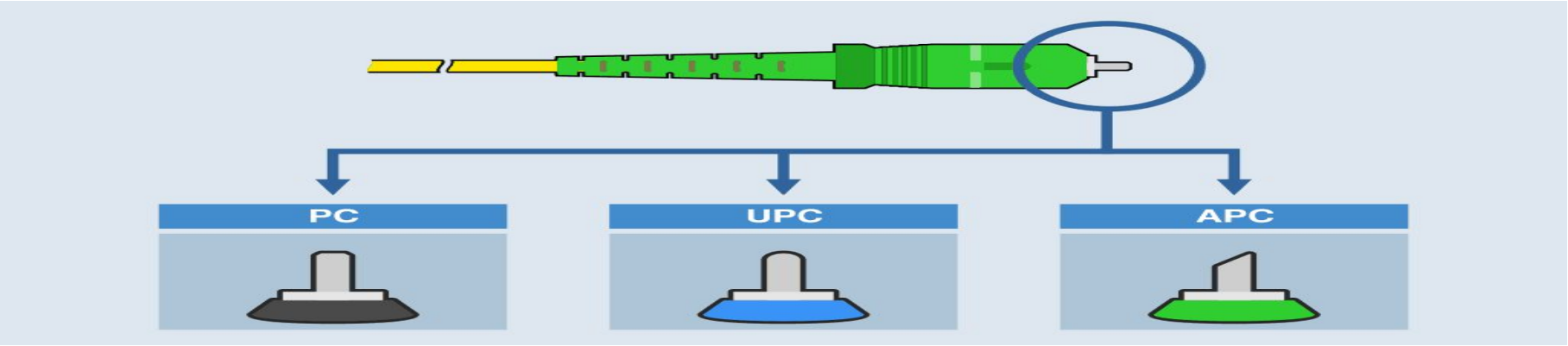


РАЗЪЕМ SC

- **“SC” stands for...** Subscriptor Connector или Square Connector
- **Краткая история**: Разработано Nippon Telegraph and Telephone, оно стало самым популярным из-за снижения производственных затрат.
- **Особенности**: Быстроразъемная установка. Он компактен, что позволяет большую плотность разъемов на инструмент. Используется в FTTH, телефонии, кабельном телевидении и т. д.
- **Оптические характеристики**: для одномодовых и многомодовых волокон. Потери 0,25 дБ.

Типы полировки

- **PC**: Physical Contact (Физический контакт). Обойма скошена и обработана на ровной поверхности. Это позволяет избежать пустых пространств между наконечниками соединяемых разъемов и обеспечивает вносимые потери в диапазоне от -30 дБ до -40 дБ. Его использование все чаще выпадает.
- **UPC**: Ultra Physical contact (Ультра физический контакт). Они аналогичны PC разъемам, что позволяет снизить возвратные потери до предела от -40 до -55 дБ благодаря более четкой кривой скоса. Текущий тренд использует его в мертвых строках, чтобы позволить операторам выполнять тесты сетей, например, с помощью рефлектометра.
- **APC**: Angled Physical Contact (Угловой физический контакт). Наконечник заканчивается плоской наклонной поверхностью под углом 8 градусов, что делает его разъемом, обеспечивающим наилучшую оптическую связь, поскольку он снижает возвратные потери до -60 дБ, что позволяет увеличить количество пользователей в одномодовых волокнах. По этой причине, в сочетании с постоянно снижающимися производственными затратами, APC стал наиболее часто используемым видом полировки.



Цветовая схема оптических разъемов

ТИП ОПТИЧЕСКОГО ВОЛОКНА	ЦВЕТ СОЕДИНИТЕЛЯ
62.5/125	Бежевый
50/125	Черный
50/125 laser optimized	Аквамарин
OM5	Лайм
Одномодовый режим	Синий
Одномодовый режим с полировкой APC	Зеленый

Инструменты для оптоволокна

Стриппер

Тестер

Сварка

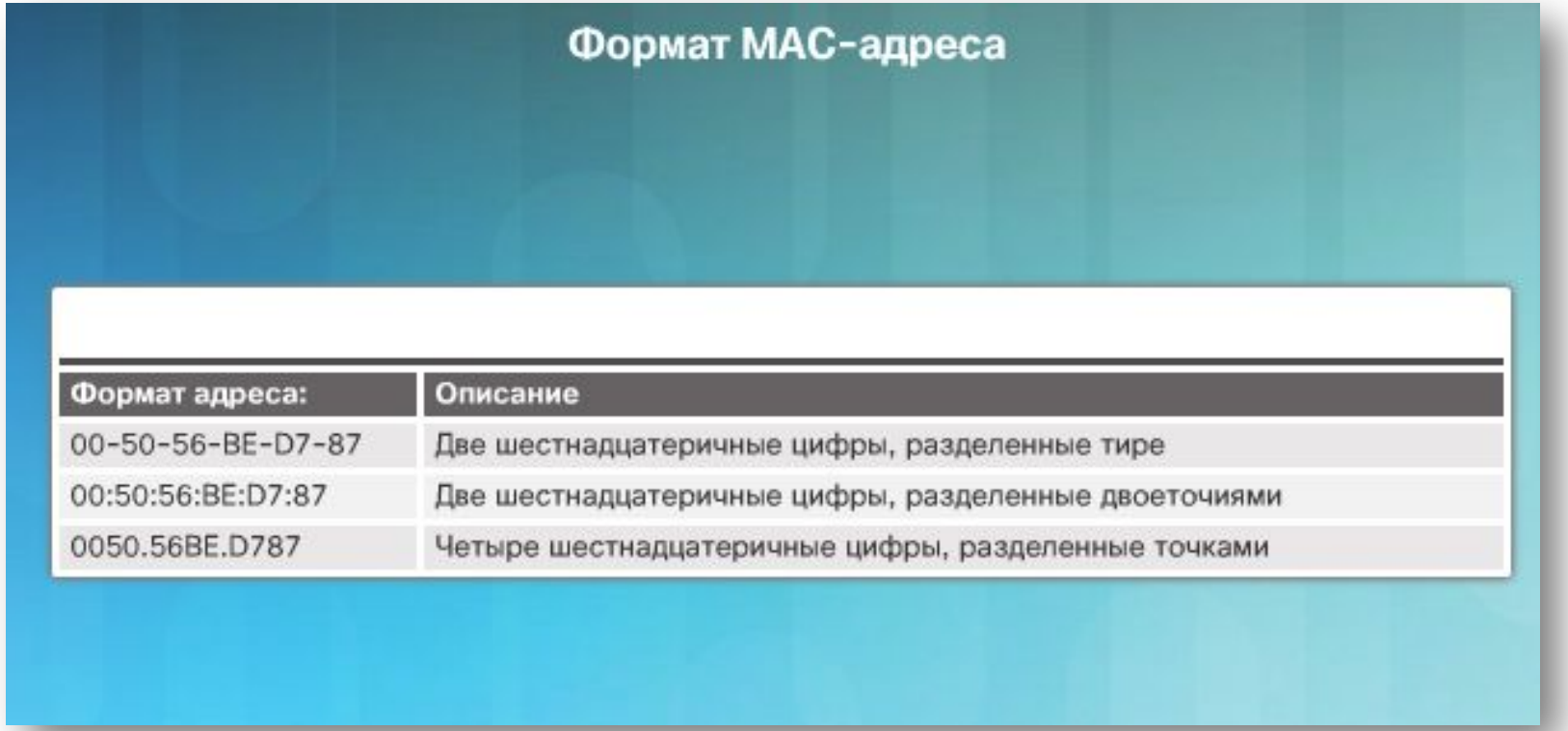
Скалыватель

Сетевая адресация

MAC-адрес (сокращение от Media Access Control – управление доступом к среде передачи) и IP-адрес. MAC-адрес прошит на сетевой интерфейсной плате (NIC) производителем

Сетевая адресация

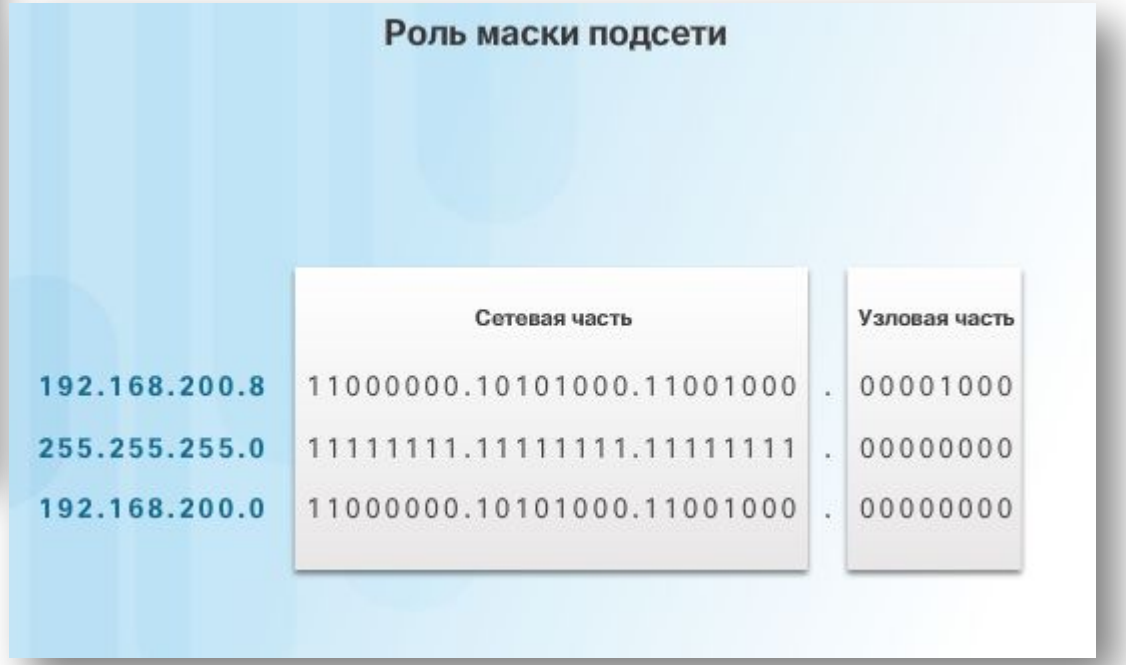
MAC-адрес имеет длину 48 бит и может быть представлен в одном из трех шестнадцатеричных форматов



IP-адреса

Адрес IPv4 состоит из 32 бит и представляется в десятичном формате с разделением точкой. Длина адреса IPv6 составляет 128 бит, и он представляется в шестнадцатеричном формате

Формат адреса IPv4



Классовая и бесклассовая адресация IPv4

Когда адресация IPv4 была впервые определена в 1981 году, адреса были разделены на три класса. Значение первого октета в адресе IPv4 отражает, к какому классу он принадлежит. Каждому классу была назначена маска подсети по умолчанию.

Классы адресов в первоначальной схеме IP-адресации.

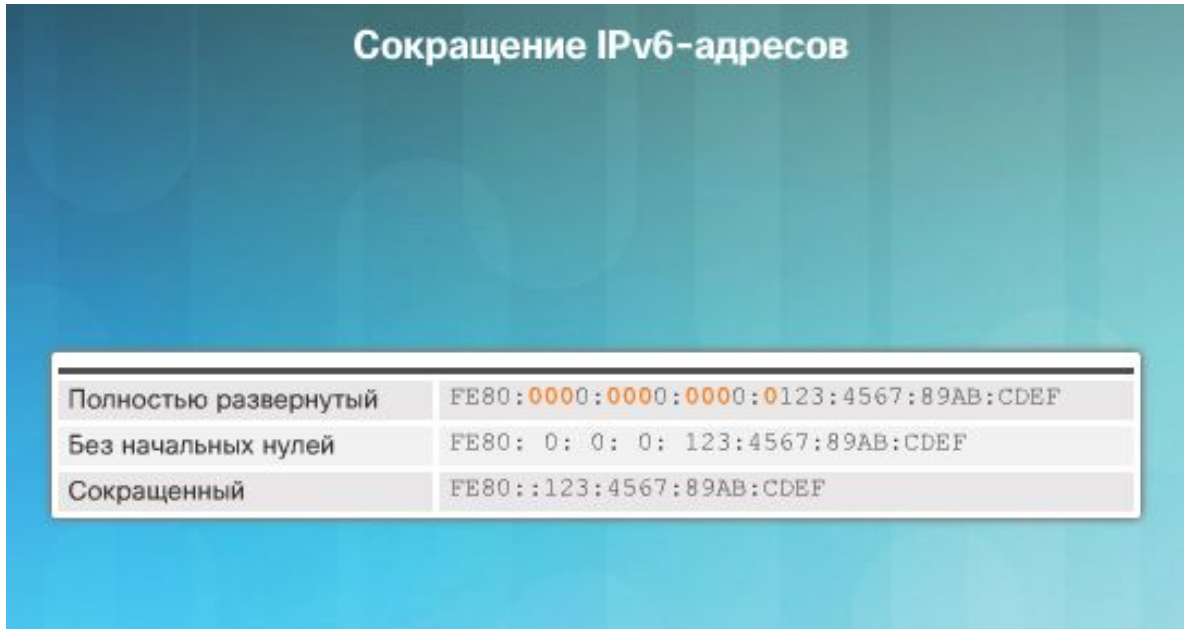
Класс	Первые биты в октете	Возможные значения первого октета	Возможное число сетей	Возможное Число узлов в сети
A	0	1-126	126	16777214
B	10	128-191	16384	65534
C	110	192-223	2097152	254
D	1110	224-239	Используется для многоадресной рассылки (multicast)	
E	1111	240-254	Зарезервирован как экспериментальный	

Количество IPv6-адресов

Название числа	Научное представление	Количество нулей
1 тысяча	10^3	1 000
1 млн	10^6	1 000 000
1 млрд	**10^9**	**1 000 000 000**
1 триллион	10^12	1 000 000 000 000
1 квадриллион	10^15	1 000 000 000 000 000
1 квинтиллион	10^18	1 000 000 000 000 000 000
1 секстиллион	10^21	1 000 000 000 000 000 000 000
1 септиллион	10^24	1 000 000 000 000 000 000 000 000
1 октиллион	10^27	1 000 000 000 000 000 000 000 000 000
1 ниниллион	10^30	1 000 000 000 000 000 000 000 000 000 000
1 дециллион	10^33	1 000 000 000 000 000 000 000 000 000 000 000
1 ундециллион	**10^36**	**1 000 000 000 000 000 000 000 000 000 000 000 000**

Форматы адресов IPv6

Первое правило для сокращения записи IPv6-адресов — пропуск всех начальных нулей в каждой четверке шестнадцатеричных цифр.



Второе правило для сокращения записи адресов IPv6 заключается в том, что двойное двоеточие (::) может заменить любую группу последовательно идущих нулей. Двойное двоеточие (::) может использоваться в адресе только один раз, иначе возникнет двусмысленность и данной записи будут соответствовать несколько возможных адресов.

Полностью развернутый	2001:0db8:0000:1111:0000:0000:0000:0200
Без начальных нулей	2001: db8: 0:1111: 0: 0: 0: 200
Сокращенный	2001:DB8:0:1111::200

Полностью развернутый	fe80:0000:0000:0000:0123:4567:89ab:cdef
Без начальных нулей	fe80: 0: 0: 0: 123:4567:89ab:cdef
Сокращенный	fe80::123:4567:89ab:cdef

Полностью развернутый	ff02:0000:0000:0000:0000:0000:0000:0001
Без начальных нулей	ff02: 0: 0: 0: 0: 0: 0: 1
Сокращенный	ff02::1

Маска подсети является числом, и она определяет диапазон IP-адресов, которые может использовать сеть. С ее помощью сети могут делиться на небольшие подсети, которые подключаются к Интернету.

Маска подсети	Маска в двоичной системе	Префикс	Количество адресов
255.255.255.255	11111111.11111111.11111111.11111111	/32	1
255.255.255.254	11111111.11111111.11111111.11111110	/31	2
255.255.255.252	11111111.11111111.11111111.11111100	/30	4
255.255.255.248	11111111.11111111.11111111.11111000	/29	8
255.255.255.240	11111111.11111111.11111111.11110000	/28	16
255.255.255.224	11111111.11111111.11111111.11100000	/27	32
255.255.255.192	11111111.11111111.11111111.11000000	/26	64
255.255.255.128	11111111.11111111.11111111.10000000	/25	128
255.255.255.0	11111111.11111111.11111111.00000000	/24	256
255.255.254.0	11111111.11111111.11111110.00000000	/23	512
255.255.252.0	11111111.11111111.11111100.00000000	/22	1024
255.255.248.0	11111111.11111111.11111000.00000000	/21	2048
255.255.240.0	11111111.11111111.11110000.00000000	/20	4096
255.255.224.0	11111111.11111111.11100000.00000000	/19	8192
255.255.192.0	11111111.11111111.11000000.00000000	/18	16384
255.255.128.0	11111111.11111111.10000000.00000000	/17	32768
255.255.0.0	11111111.11111111.00000000.00000000	/16	65536
255.254.0.0	11111111.11111110.00000000.00000000	/15	131072
255.252.0.0	11111111.11111100.00000000.00000000	/14	262144
255.248.0.0	11111111.11111000.00000000.00000000	/13	524288
255.240.0.0	11111111.11110000.00000000.00000000	/12	1048576
255.224.0.0	11111111.11100000.00000000.00000000	/11	2097152
255.192.0.0	11111111.11000000.00000000.00000000	/10	4194304
255.128.0.0	11111111.10000000.00000000.00000000	/9	8388608
255.0.0.0	11111111.00000000.00000000.00000000	/8	16777216
254.0.0.0	11111110.00000000.00000000.00000000	/7	33554432
252.0.0.0	11111100.00000000.00000000.00000000	/6	67108864
248.0.0.0	11111000.00000000.00000000.00000000	/5	134217728
240.0.0.0	11110000.00000000.00000000.00000000	/4	268435456
224.0.0.0	11100000.00000000.00000000.00000000	/3	536870912
192.0.0.0	11000000.00000000.00000000.00000000	/2	1073741824
128.0.0.0	10000000.00000000.00000000.00000000	/1	2147483648
0.0.0.0	00000000.00000000.00000000.00000000	/0	4294967296

Маска подсети	Размер адреса хоста	Макс. кол-во хостов
255.0.0.0 (8 бит)	24 бит	16777214 (2^{24} - 2)
255.255.0.0 (16 бит)	16 бит	65534 (2^{16} - 2)
255.255.255.0 (24 бит)	8 бит	254 (2^{8} - 2)
255.255.255.252 (30 бит)	2 бит	2 (2^{2} - 2)

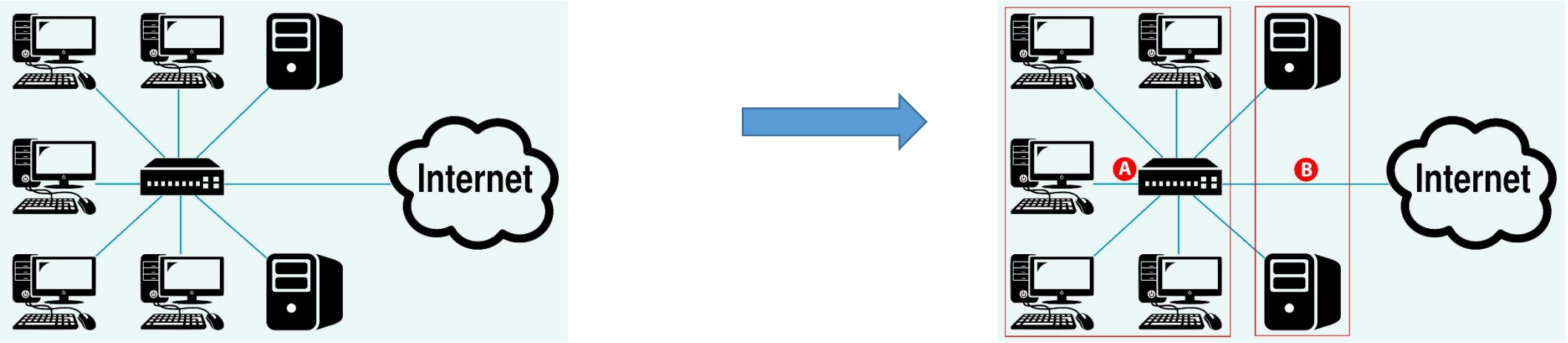
Маска подсети	Альтернативный формат	Размер адреса хоста	Макс. кол-во хостов
255.255.255.0	xxx.xxx.xxx.xxx/24	8 бит	254
255.255.255.128	xxx.xxx.xxx.xxx/25	7 бит	126
255.255.255.192	xxx.xxx.xxx.xxx/26	6 бит	62
255.255.255.224	xxx.xxx.xxx.xxx/27	5 бит	30
255.255.255.240	xxx.xxx.xxx.xxx/28	4 бит	14
255.255.255.248	xxx.xxx.xxx.xxx/29	3 бит	6
255.255.255.252	xxx.xxx.xxx.xxx/30	2 бит	2

Количество разрядов в адресе сети определяет максимальное количество хостов, которые могут находиться в такой сети. Чем больше бит в адресе сети, тем меньше бит остается на адрес хоста в адресе.

- IP-адрес с адресом хоста из всех нулей представляет собой IP-адрес сети (например 192.168.1.0/24).
- IP-адрес с адресом хоста из всех единиц представляет собой широковещательный адрес данной сети (например 192.168.1.255/24).

Маска подсети	Альтернативный формат	Размер адреса хоста	Макс. кол-во хостов
255.255.255.0	xxx.xxx.xxx.xxx/24	8 бит	254
255.255.255.128	xxx.xxx.xxx.xxx/25	7 бит	126
255.255.255.192	xxx.xxx.xxx.xxx/26	6 бит	62
255.255.255.224	xxx.xxx.xxx.xxx/27	5 бит	30
255.255.255.240	xxx.xxx.xxx.xxx/28	4 бит	14
255.255.255.248	xxx.xxx.xxx.xxx/29	3 бит	6
255.255.255.252	xxx.xxx.xxx.xxx/30	2 бит	2

В этом примере сеть компании имеет адрес 192.168.1.0. Первые три октета адреса (192.168.1) представляют собой адрес сети, а оставшийся октет — адрес хоста, что позволяет использовать в сети максимум 2^8 - 2 = 254 хостов.



Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, нужно «позаимствовать» один бит из адреса хоста. В этом случае маска подсети станет 25-битной (255.255.255.128 или /25). «Одолженный» бит адреса хоста может быть либо нулем, либо единицей, что дает нам две подсети: 192.168.1.0/25 и 192.168.1.128/25.

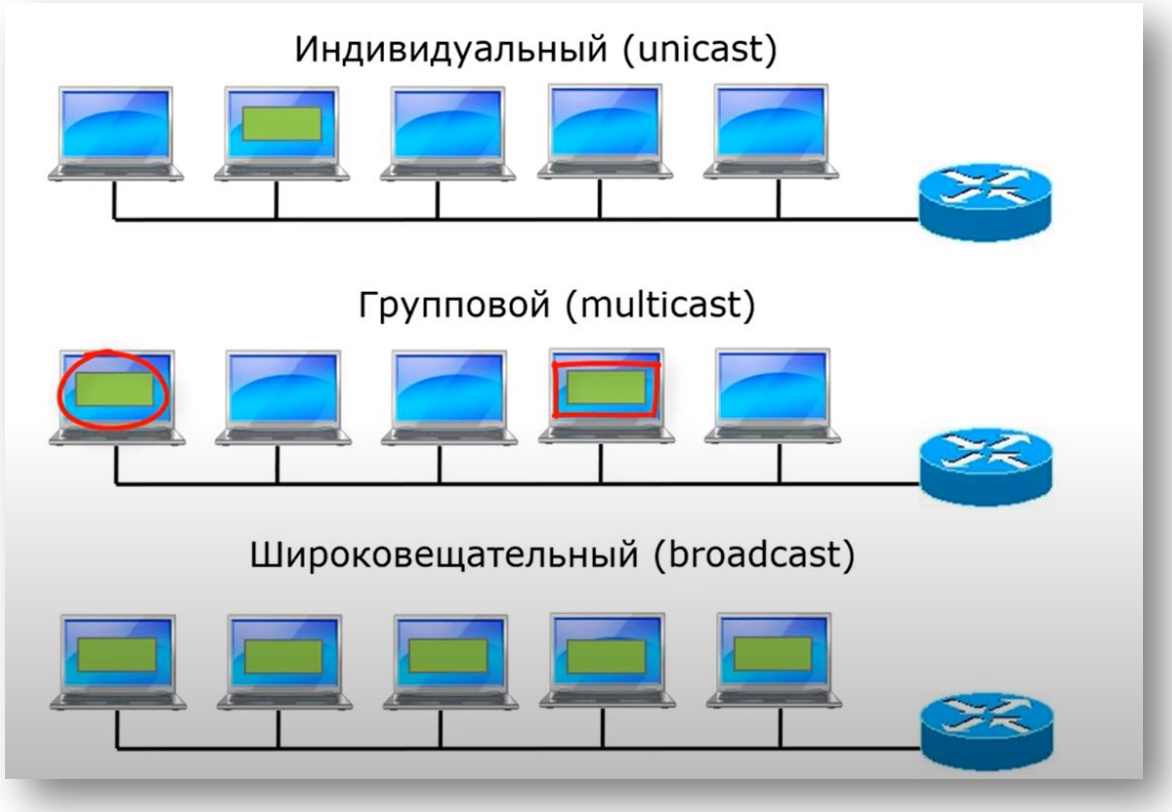
	Сеть A	Сеть B
IP-адрес подсети	192.168.1.0/25	192.168.1.128/25
Маска подсети	255.255.255.128	255.255.255.128
Широковещательный адрес	192.168.1.127	192.168.1.255
Минимальный IP-адрес хоста	192.168.1.1	192.168.1.129
Максимальный IP-адрес хоста	192.168.1.126	192.168.1.254

Аналогичным образом для разделения 24-битного адреса на четыре подсети потребуется «одолжить» два бита идентификатора хоста, чтобы получить четыре возможные комбинации (00, 01, 10 и 11). Маска подсети состоит из 26 бит (11111111.11111111.11111111.11000000), то есть **255.255.255.192.**
Каждая подсеть содержит 6 битов адреса хоста, что в сумме дает 2^6 - 2 = 62 хоста для каждой подсети (адрес хоста из всех нулей — это сама подсеть, а из всех единиц — широковещательный адрес для подсети).

	Первая подсеть	Вторая подсеть	Третья подсеть	Четвертая подсеть
IP-адрес подсети	192.168.1.0/26	192.168.1.64/26	192.168.1.128/26	192.168.1.192/26
Маска подсети	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192
Широковещательный адрес	192.168.1.63	192.168.1.127	192.168.1.191	192.168.1.255
Минимальный IP-адрес хоста	192.168.1.1	192.168.1.65	192.168.1.129	192.168.1.193
Максимальный IP-адрес хоста	192.168.1.62	192.168.1.126	192.168.1.190	192.168.1.254

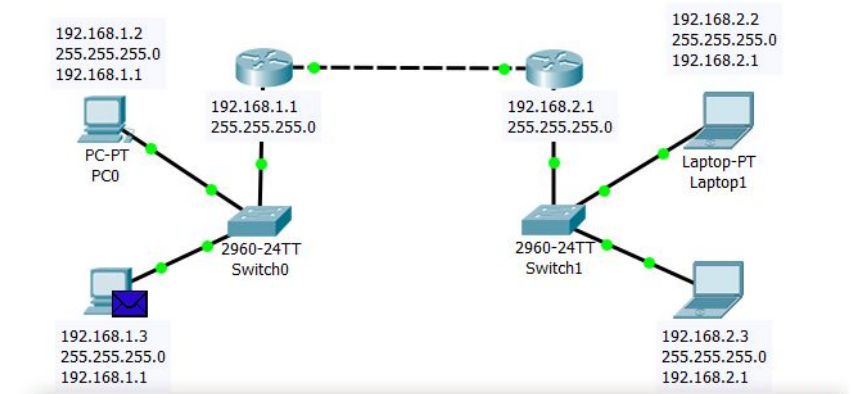
Типы IP адресов

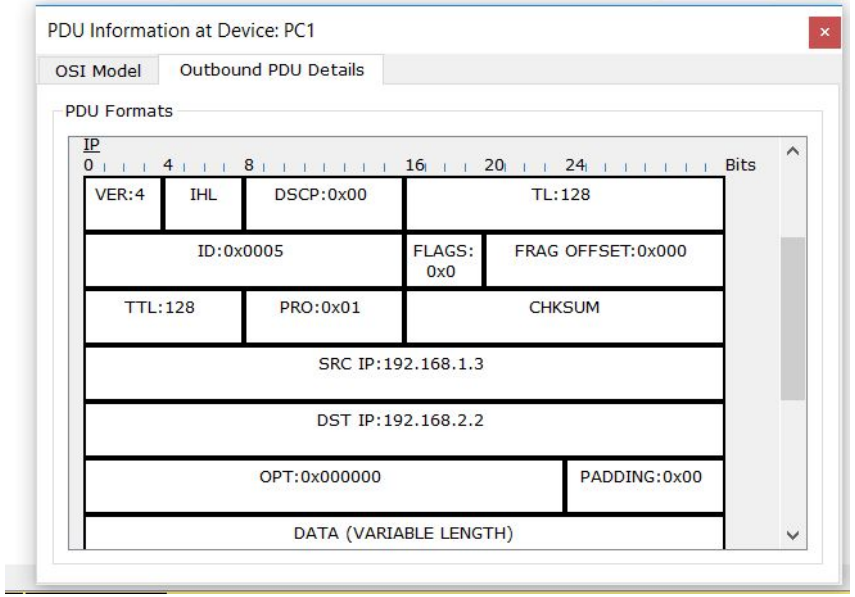
Unicast — одноадресная рассылка — один отправитель, один получатель. (*Пример: запрос HTTP-странички у WEB-сервера*).
Broadcast — широковещательная рассылка — один отправитель, получатели — все устройства в широковещательном сегменте. (*Пример: ARP-запрос*).
Multicast — многоадресная рассылка — один отправитель, много получателей. (*Пример: IPTV*).



Internet Protocol television (IPTV) - это протокол передачи телевизионного контента по IP-сети.

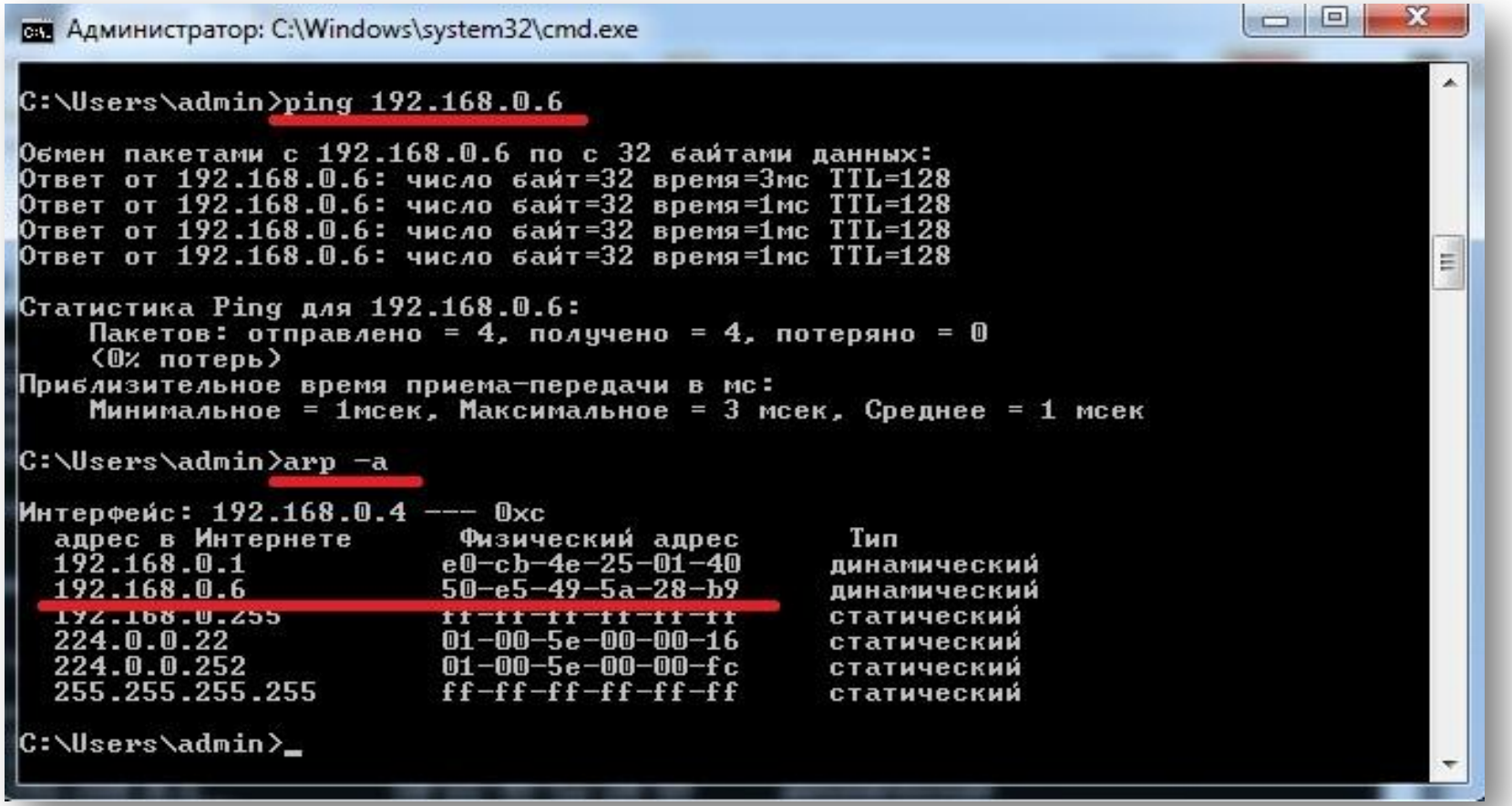
Вы легко можете убедиться в том, что unicast означает, что пакет пойдет одному конкретному адресату, если соберете схему, как показано на Рисунке, а затем выполните команду Ping от одного узла до другого в режиме симуляции.





ARP-запрос

netsh interface ip delete arpcache – очистка кеша



arp -a — будет выведена таблица соответствий IP-адреса и физического адреса сетевого интерфейса соседнего устройства(MAC-адрес).

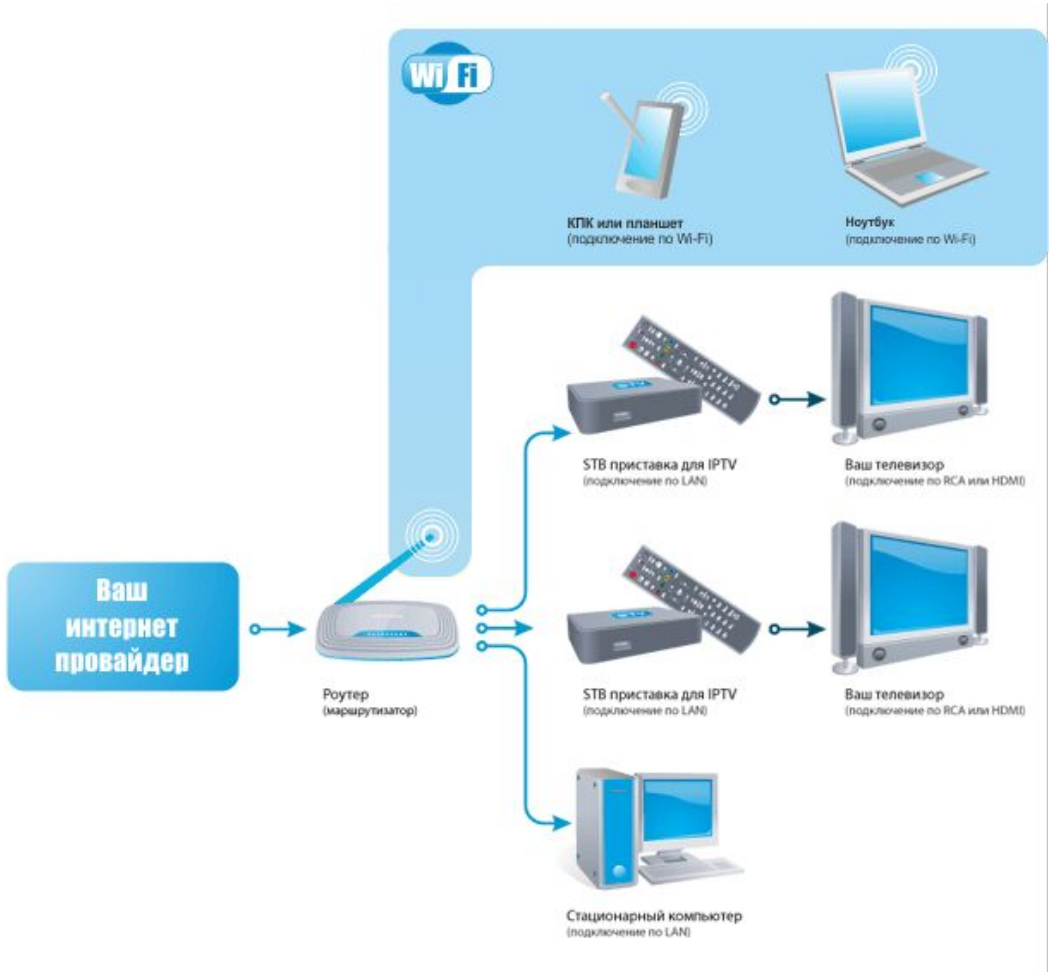
Широковещательный канал, широковещание (англ. broadcasting) — метод передачи данных в компьютерных сетях, при котором поток данных (каждый переданный пакет в случае пакетной передачи) предназначен для приёма всеми участниками сети.

Широковещательная передача используется для обнаружения специальных служб/устройств, для которых адрес не известен, или когда узел должен передать информацию всем узлам в сети.

Некоторые примеры использования широковещательных сообщений:

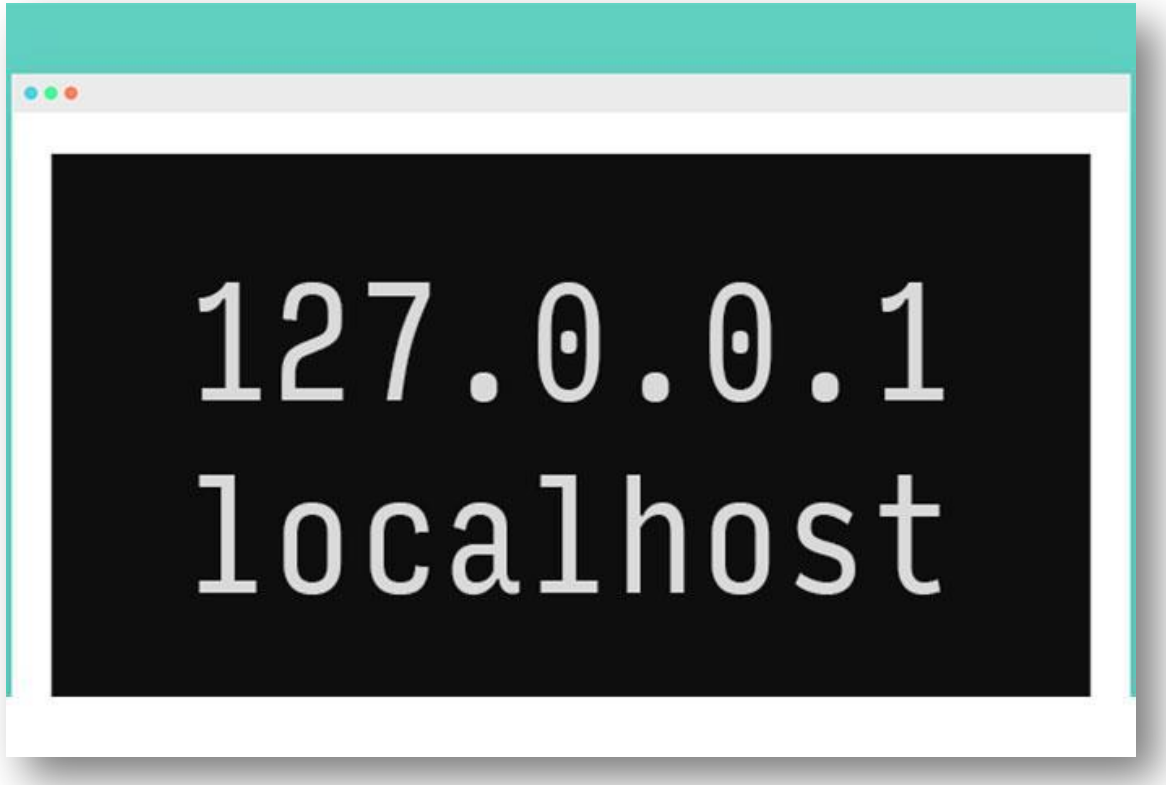
- Отображение адресов верхнего уровня к адресам нижнего уровня
- Запрос адреса
- Обмен информацией о маршрутах между протоколами маршрутизации

Multicast (*Пример: IPTV*).

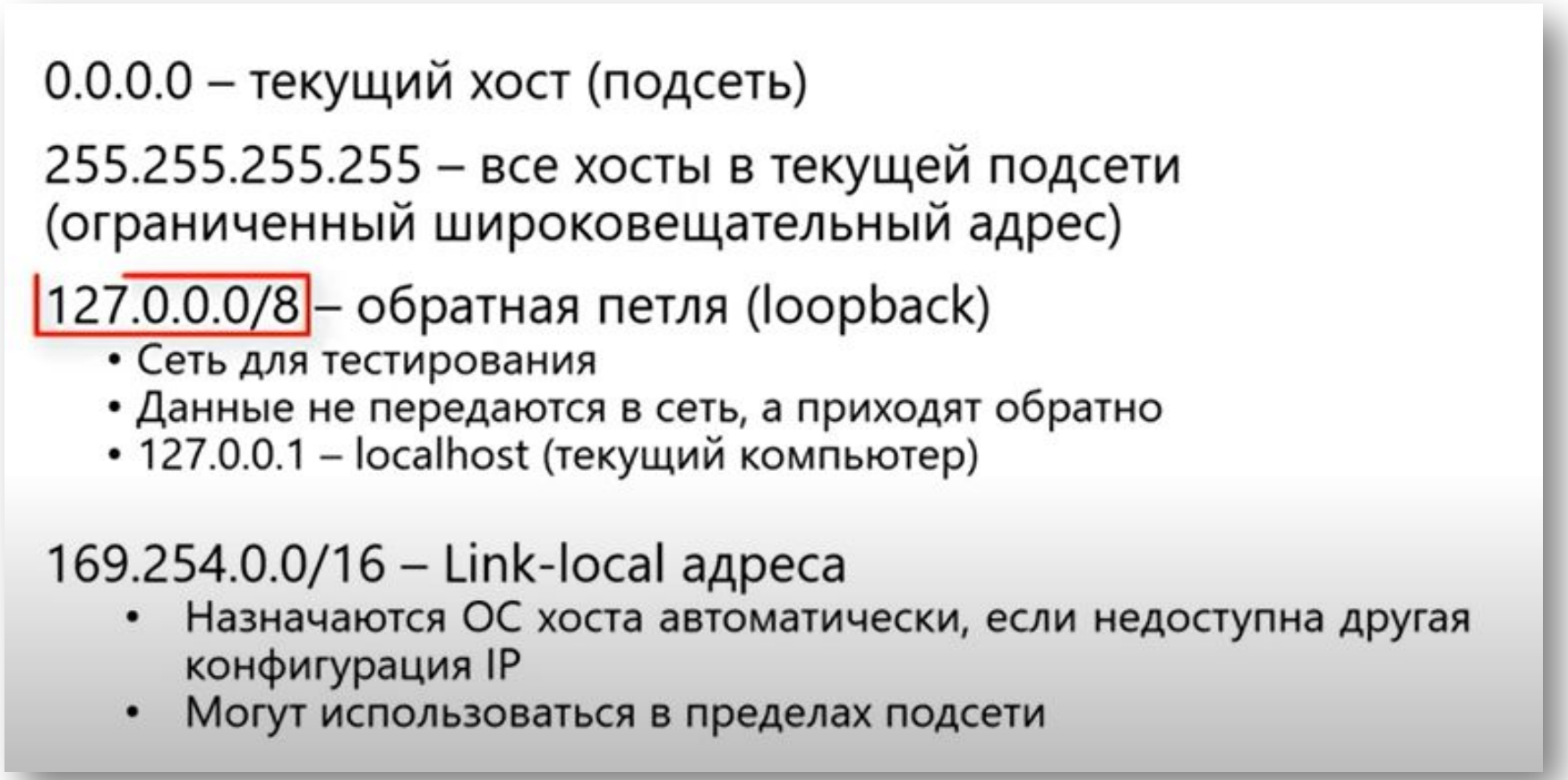


Так что же значит localhost?

Localhost — это не только термин, но и доменное имя,
например **google.com** или **wikipedia.org**. Это адрес. Если при вводе **google.com** в браузере вы попадете на главную страницу Google, куда вас доставит localhost? Он приведёт вас к вашему компьютеру.



Адрес 127.0.0.1 зарезервирован как адрес обратной связи. Если пользователь передаёт сообщение на адрес 127.0.0.1, оно должно вернуться к нему, если не произойдет сбоев в программном обеспечении. Сообщения с этим адресом не выходят из сети, а остаются на компьютере, на котором работает программа протокола IP

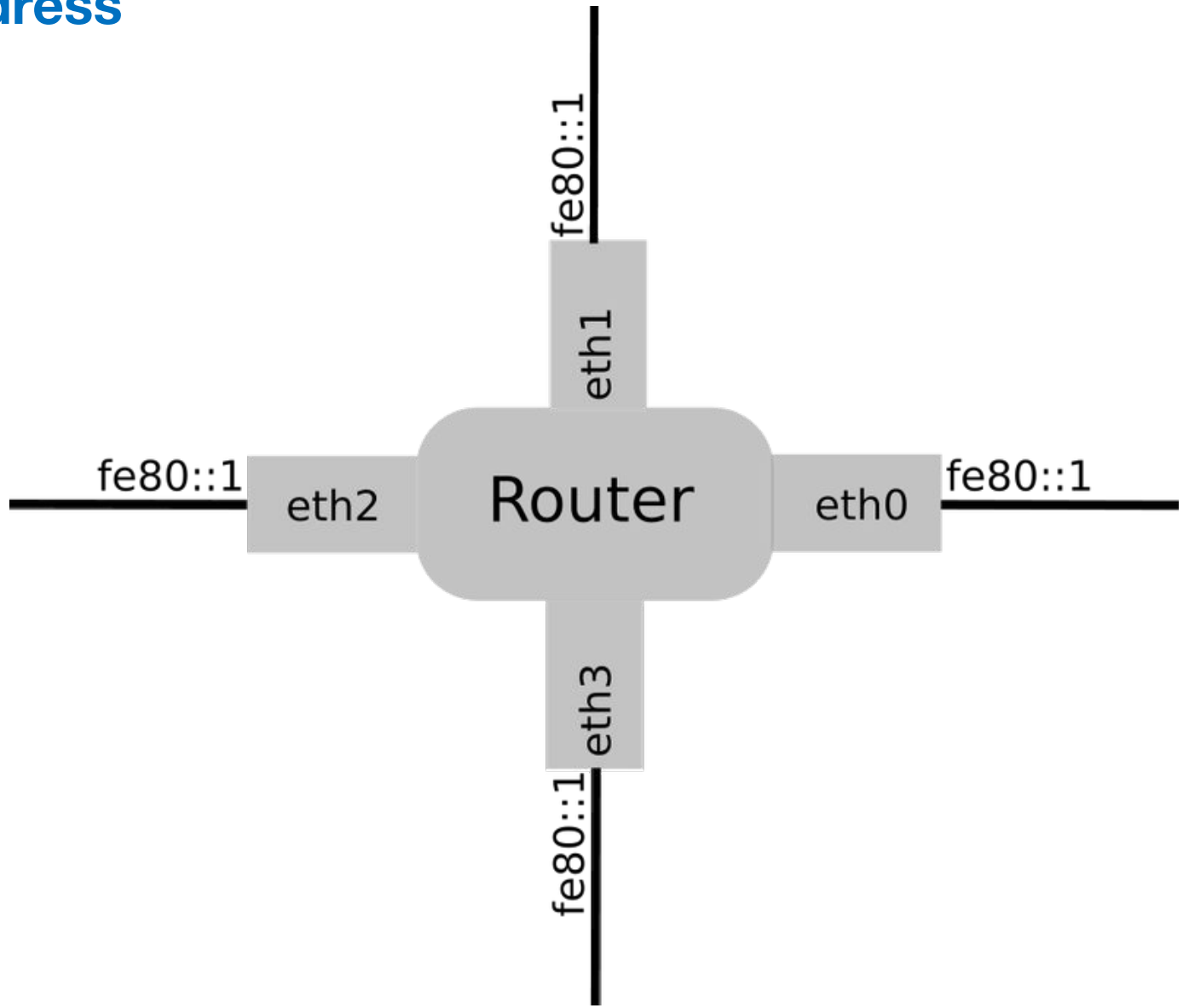


Какова цель localhost?

Тест скорости

Тест программы или веб-приложения

Link-local address



Внутренние IP адреса

Зарезервированные диапазоны адресов (RFC 1918):

- 10.0.0.0 /8
- 172.16.0.0 /12
- 192.168.0.0 /16

Не маршрутизируются в Интернет

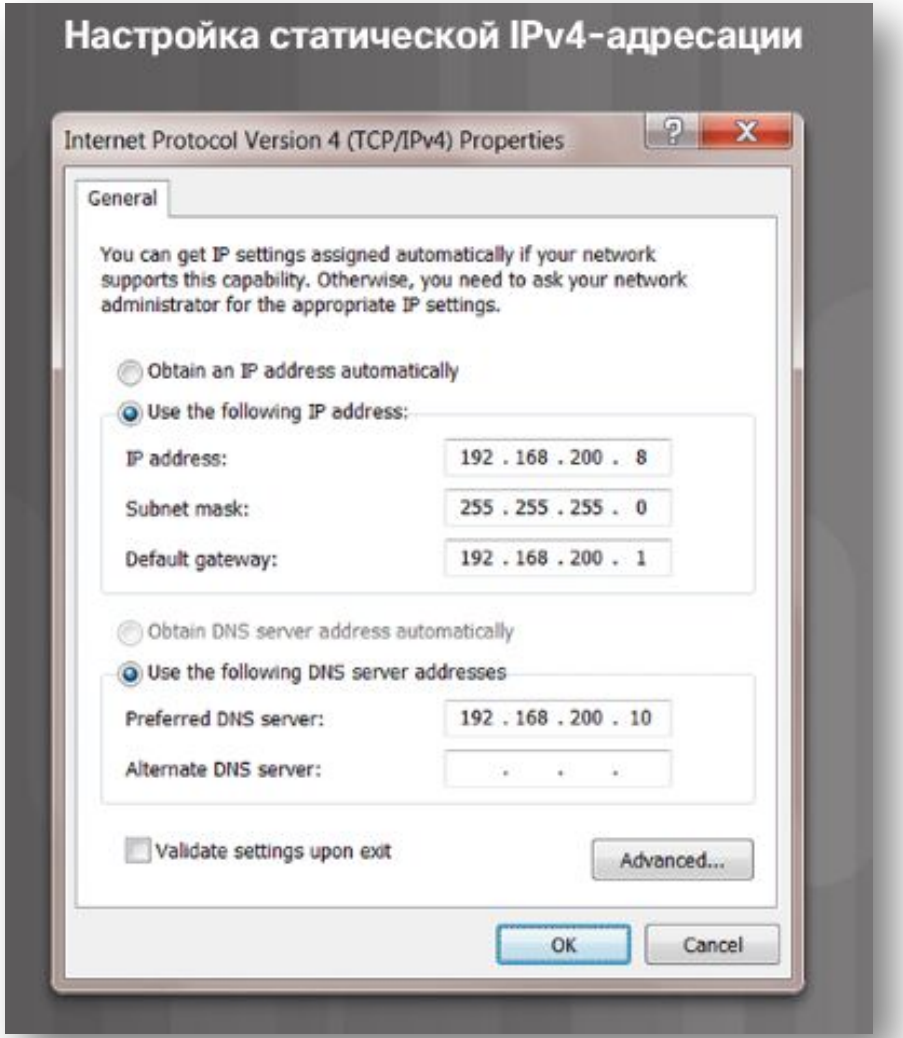
Могут использоваться внутри организации без обращения в IANA

Подключение к Интернет с использованием технологии NAT (Network Address Translation)

Статическая адресация

- **IP-адрес** — идентифицирует компьютер в глобальной сети.
- **Маска подсети** — параметр, позволяющий определить сеть, к которой он подключен.
- **Шлюз по умолчанию** — устройство, через которое компьютер подключается к Интернету или к другим сетям.

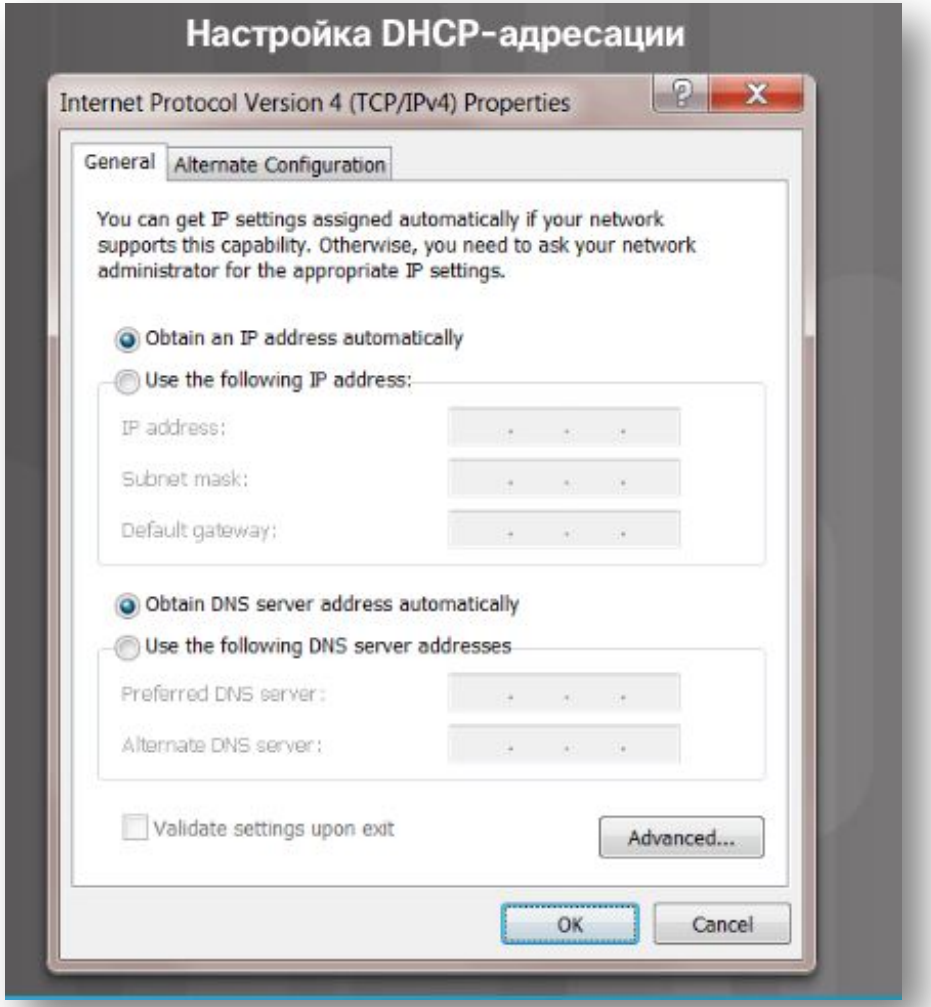
Необязательные параметры — например, адрес предпочитаемого сервера DNS и адрес дополнительного сервера DNS



Динамическая адресация

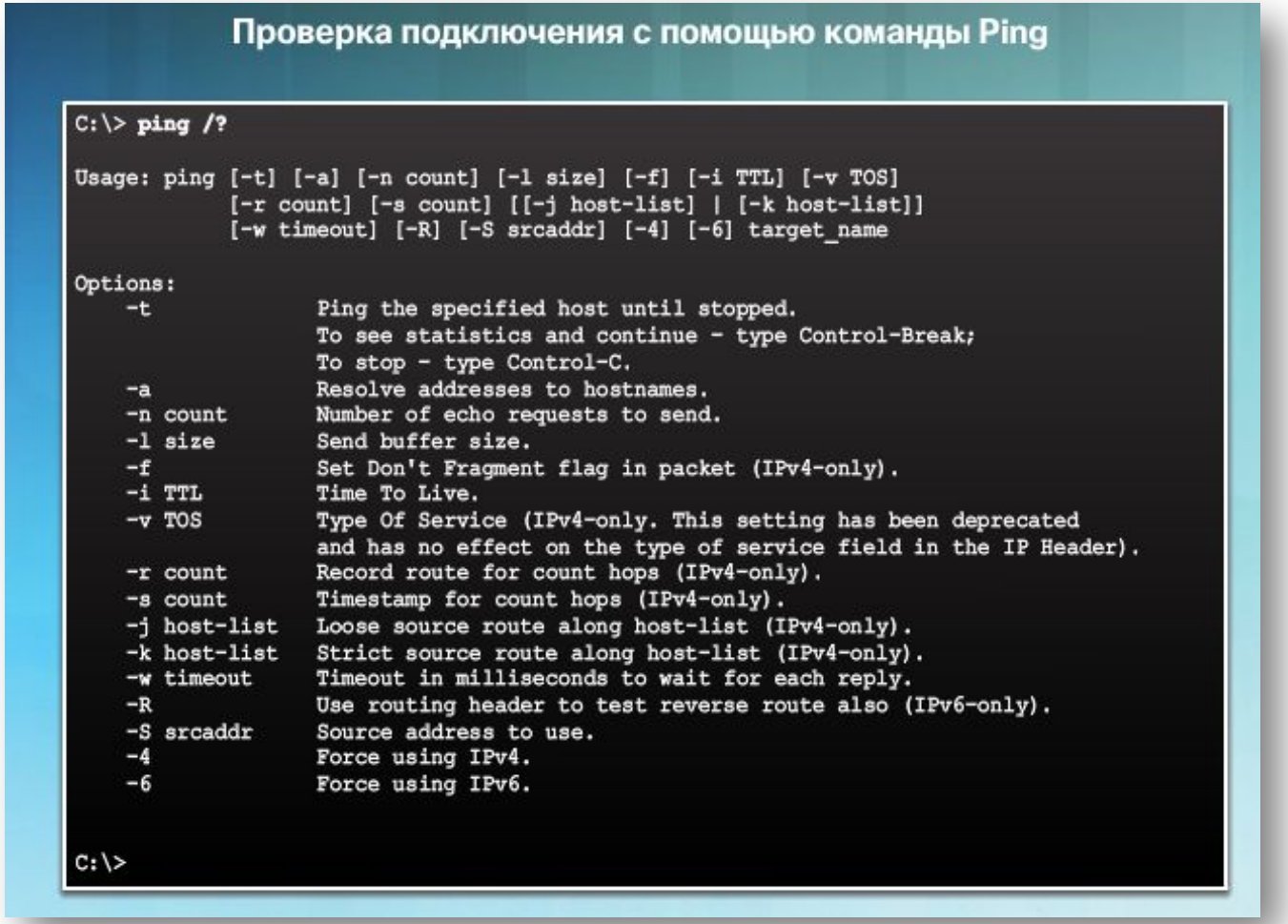
Сервер DHCP может автоматически назначить узлу следующие сведения о настройке IP-адреса:

- IP-адрес
- Маска подсети
- Шлюз по умолчанию
- Дополнительные значения, например адрес сервера DNS



ICMP

Протокол ICMP используется устройствами в сети для отправки на компьютеры и серверы управляющих сообщений и сообщений об ошибках. Существует несколько способов использования ICMP, например: объявление об ошибках сети, объявление о перегрузке сети и устранение неисправностей.



Что такое порт?

Порт - это числовой идентификатор программы или процесса, которые обслуживают сетевые соединения на заданном сетевом адресе (IP-адресе).

Протоколы всемирной паутины

Порт	Транспортный протокол	Прикладной протокол	Описание
53	TCP, UDP	DNS	Протокол службы доменных имен (DNS)
80	TCP	HTTP	Протокол передачи гипертекста (HTTP) устанавливает набор правил для обмена тестом, графическими изображениями, звуковыми, видео и прочими мультимедийными файлами во всемирной паутине
443	TCP, UDP	HTTPS	Браузер использует шифрование и выполняет аутентификацию вашего подключения к веб-серверу.

Номера портов представлены как беззнаковое целое число длинной 16 бит, и могут принимать значения от 0 до 65535 (в сумме 65536 доступных номеров портов). Организация IANA (Internet Assigned Numbers Authority), которая ответственна за ресурсы Интернет-протоколов, определила и зарезервировала номера общеиспользуемых портов, имеющих номера от 0 до 1023 (в сумме 1024 номеров портов).

Протокол электронной почты и управления идентификацией

Порт	Транспортный протокол	Прикладной протокол	Описание
25	TCP	SMTP	Простой протокол передачи почты (SMTP) используется для отправки электронных сообщений от клиентов на почтовый сервер. Он также может использоваться для ретрансляции сообщений электронной почты с между почтовыми серверами отправителя и адресата.
110	TCP	POP3	Почтовый протокол 3 используется клиентами электронной почты для получения сообщений с почтового сервера.
143	TCP	Протокол доступа к сообщениям в Интернете (IMAP)	используется для получения сообщений с почтового сервера. Это более сложный протокол в сравнении с POP3, он также дает ряд преимуществ.
389	TCP, UDP	LDAP	Облегченный протокол доступа к каталогам используется для управления информацией об учетных данных пользователей в каталоге, которая может использоваться различными сетями и системами. С его помощью можно управлять информацией о пользователях и сетевых ресурсах. Этот протокол можно использовать для идентификации пользователей на нескольких компьютерах.

Протоколы TCP и UDP используют нумерацию портов источника и адресата для отслеживания обмена данными приложений. Номер порта источника связан с инициирующим приложением на локальном устройстве. Номер порта назначения связан с целевым приложением на удаленном устройстве

Протоколы передачи файлов и управления

TCP

Протоколы передачи файлов и управления файлами

Порт	Транспортный протокол	Прикладной протокол	Описание
20	FTP		Протокол передачи файлов. Используется для передачи файлов между компьютерами. Этот протокол считается незащищенным, следует использовать протокол передачи файлов SSH (SFTP, порт TCP 22).
21	TCP	FTP	FTP использует TCP-порт 21 для создания подключения между клиентом и FTP-сервером, чтобы начать сеанс передачи данных.
69	UDP	TFTP	Простой протокол передачи файлов создает меньше нагрузки в сравнении с протоколом FTP.
445	TCP	SMB/CIFS	Протокол обмена блоками серверных сообщений (SMB) или общая файловая система Интернета (CIFS) позволяют организовать совместное использование файлов, принтеров и прочих ресурсов разными узлами в сети.
548	TCP, UDP	AFP	Apple Filing Protocol представляет собой проприетарный протокол компании Apple для файловых служб macOS и классической системы Mac OS.

Протоколы удаленного доступа

Протоколы удаленного доступа

Порт	Транспортный протокол	Прикладной протокол	Описание
22	TCP	SSH	Secure Shell или Secure Socket Shell обеспечивает строгую аутентификацию и зашифрованный обмен данными между клиентом и удаленным компьютером. По аналогии с Telnet, он предоставляет командную строку на удаленном компьютере.
23	TCP	Telnet	Telnet представляет собой незащищенный протокол удаленного доступа, предлагающий командную строку на удаленном компьютере. Из соображений безопасности предпочтение отдается протоколу SSH.
3389	TCP, UDP	RDP	Протокол удаленного рабочего стола разработан компанией Майкрософт для удаленного доступа к графическим рабочим столам на удаленных машинах. Его удобно использовать для технической поддержки, однако при этом следует соблюдать осторожность, поскольку этот протокол предоставляет удаленному пользователю все права доступа к целевому компьютеру.

Протоколы управления сетью

Протоколы управления сетью

Порт	Транспортный протокол	Прикладной протокол	Описание
67/68	UDP	DHCP	Протокол динамической конфигурации сетевого узла автоматически предоставляет IP-адреса сетевым узлам и позволяет управлять этими адресами. DHCP-сервер использует порт UDP 67, а хост клиента использует порт UDP 68.
137-139	UDP, TCP	NetBIOS (NetBT)	NetBIOS поверх TCP/IP создает систему, посредством которой устаревшие компьютерные приложения могут обмениваться данными по крупным сетям TCP/IP. Для разных функций NetBT используются разные протоколы и порты в указанном диапазоне.
161/162	UDP	SNMP	Простой протокол управлению сетью (SNMP) позволяет администраторам централизованно отслеживать работу сети.
427	UDP, TCP	SLP	Протокол обнаружения сервисов позволяет компьютерам и другим устройствам находить сервисы в локальной сети без предварительной настройки. Обычно использует UDP, но также может работать и через TCP.

Прикладные протоколы в порядке следования номеров портов

Номер порта	Протокол	Приложение
20	TCP	FTP (данные)
21	TCP	FTP (управление)
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP, UDP	DNS
67	UDP	DHCP (сервер)
68	UDP	DHCP (клиент)
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
137-139	TCP, UDP	NetBIOS NetBT
143	TCP	IMAP
161/162	UDP	SNMP
389	TCP, UDP	LDAP
427	TCP, UDP	SLP
443	TCP	HTTPS
445	TCP	SMB/CIFS
548	TCP	AFP
3389	TCP, UDP	RDP

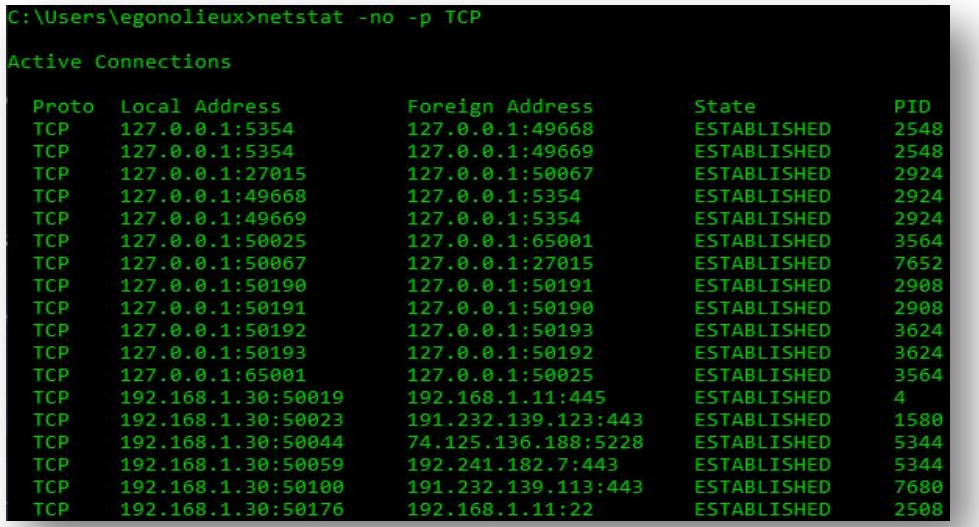
Номера портов

Номер порта	Протокол	Применение	Сокращение
20	TCP	File Transfer Protocol (Протокол передачи файлов) (данные)	FTP
21	TCP	File Transfer Protocol (Протокол передачи файлов) (управление)	FTP
22	TCP	Протокол Secure Shell	SSH
23	TCP	Программа Telnet	–
25	TCP	Simple Mail Transfer Protocol (Протокол простого обмена электронной почтой)	SMTP
53	UDP, TCP	Domain Name Service (Служба доменных имен) (DNS)	DNS
67	UDP	Dynamic Host Configuration Protocol (Протокол динамической настройки узла) (сервер)	DHCP
68	UDP	Dynamic Host Configuration Protocol (Протокол динамической настройки узла) (клиент)	DHCP
69	UDP	Trivial File Transfer Protocol (Простейший протокол передачи файлов)	TFTP
80	TCP	Hypertext Transfer Protocol (Протокол передачи гипертекста)	HTTP
110	TCP	Post Office Protocol (Протокол почтового отделения) (версия 3)	POP3
137–139	UDP, TCP	NetBIOS/NetBT	–
143	TCP	Internet Message Access Protocol (Протокол доступа к сообщениям в Интернете)	IMAP
161	UDP	Simple Network Management Protocol (Простой протокол управления сетью)	SNMP
427	UDP, TCP	Протокол поиска службы	SLP
443	TCP	Hypertext Transfer Protocol Secure (Протокол защищенной передачи гипертекста)	HTTPS
445	TCP	Протокол обмена блоками серверных сообщений/Общая файловая система Интернет	SMB/CIFS
548	Протокол TCP	Apple Filing Protocol	AFP
3389	UDP, TCP	Remote Desktop Protocol (Протокол удаленного рабочего стола)	RDP

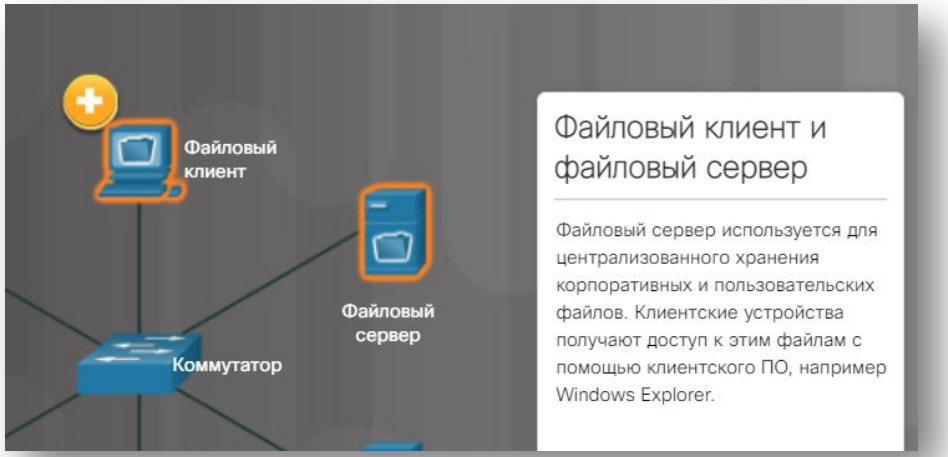
Проблемы безопасности

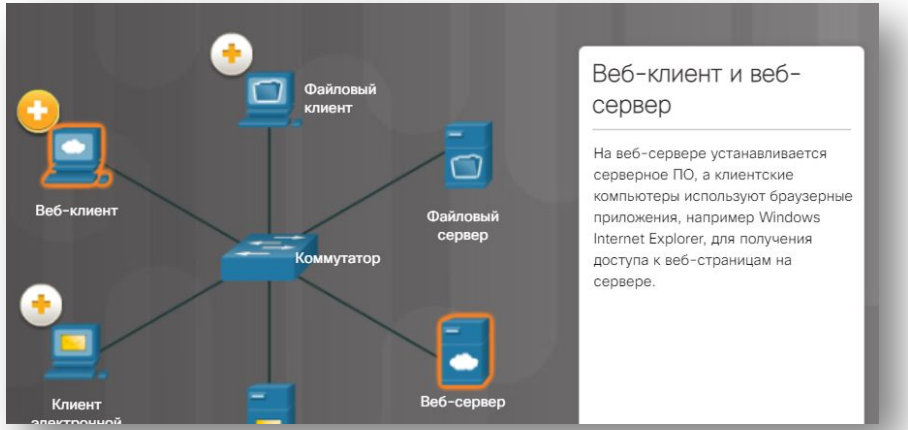
Так как на сетевом порту работает программа, а, как мы знаем, многие программы имеют ошибки, в том числе, связанные с безопасностью, открытый доступ к портам на компьютере потенциально небезопасен. Поэтому, во избежание проблем взлома, необходимо контролировать доступные порты и работающие программы на компьютере и разумно управлять ими.

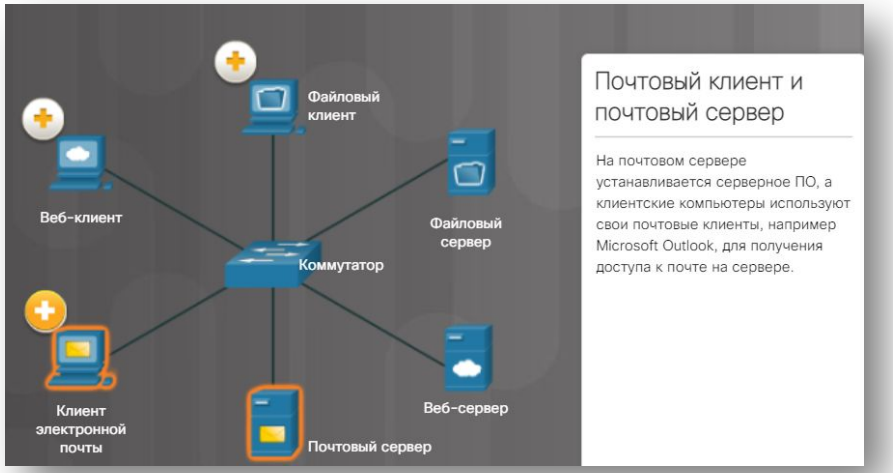
Если вы работаете в Windows, **`netstat -no -p TCP`** команда покажет вам все активные сокеты TCP и соответствующие им идентификаторы процессов, в том числе вашего браузера:



Роли клиента и сервера

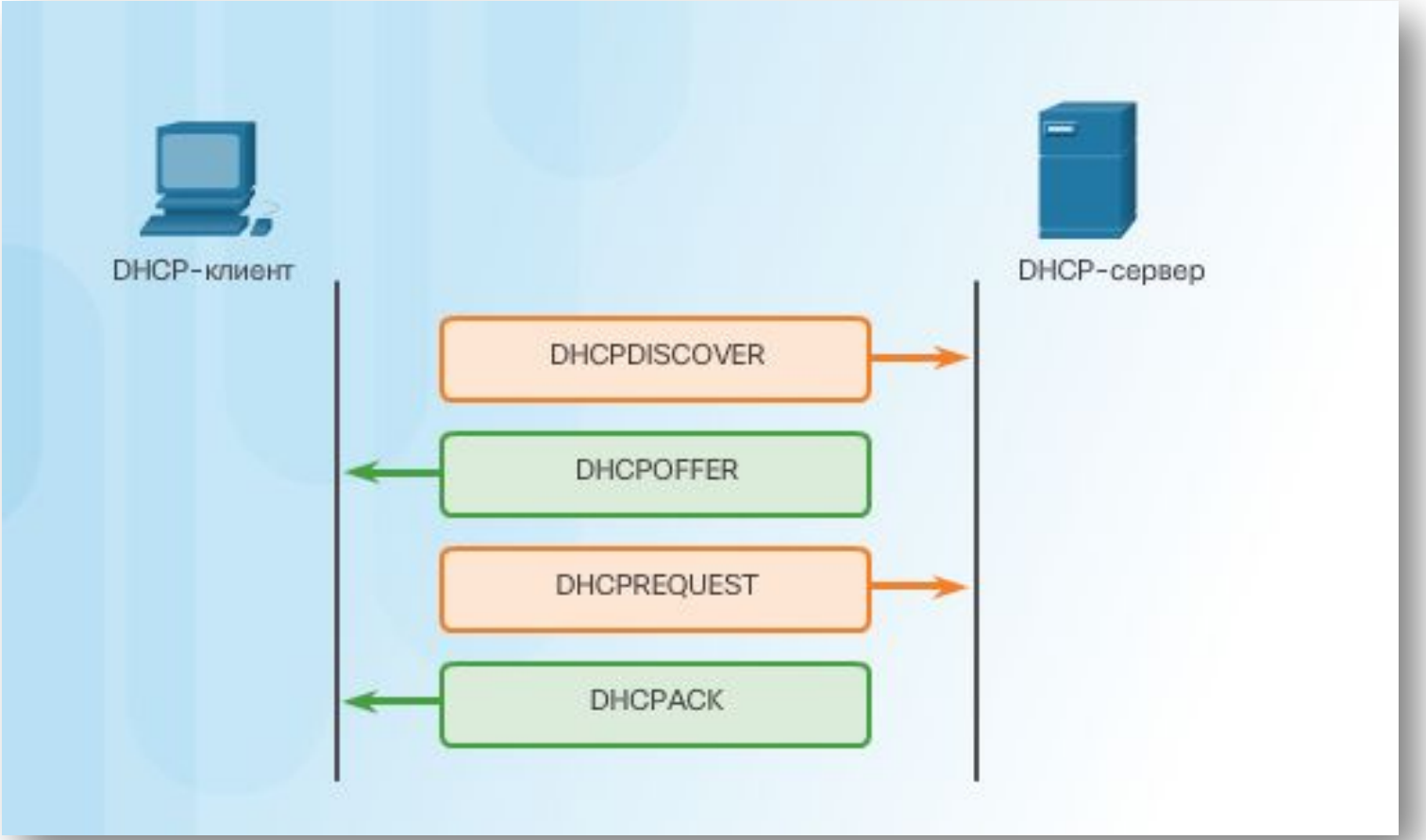






DHCP-сервер

DHCP представляет собой службу, используемую провайдерами, сетевыми администраторами и беспроводными маршрутизаторами для автоматического назначения IP-адресов хостам



1. Когда клиент загружается (или хочет присоединиться к сети), он начинает четырехэтапный процесс для получения аренды. Он запускает процесс с широковещательным (**broadcast**) сообщением **DHCPDISCOVER** со своим собственным MAC-адресом для обнаружения доступных серверов DHCPv4. Поскольку у клиента нет способа узнать подсеть, к которой он принадлежит, у сообщения **DHCPDISCOVER** адрес назначения IPv4 адреса -**255.255.255.255**. А поскольку у клиента еще нет настроенного адреса IPv4, то исходный IPv4-адрес - **0.0.0.0**.

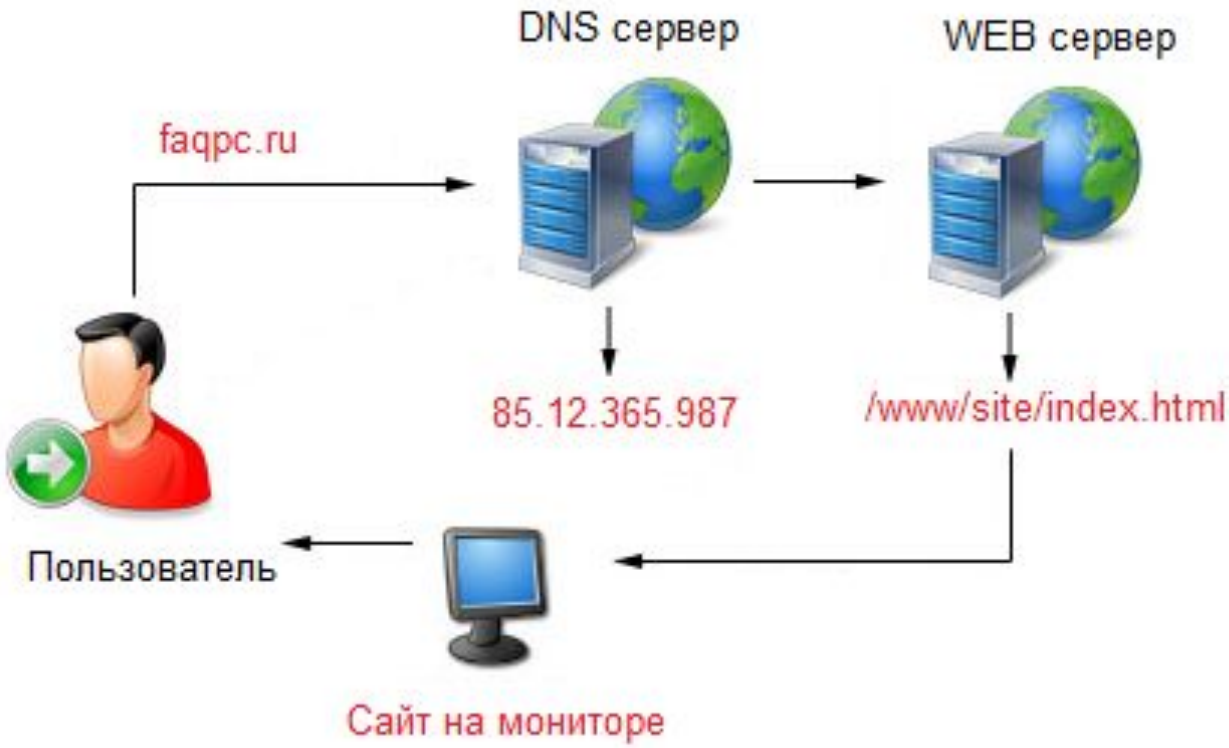
2. Сообщение **DHCPDISCOVER** находит серверы DHCPv4 в сети. Поскольку клиент не имеет IPv4 информации при загрузке, он использует широковещательные адреса 2 и 3 уровня для связи с сервером.
3. Когда DHCPv4-сервер получает сообщение **DHCPDISCOVER**, он резервирует доступный IPv4-адрес для аренды клиенту. Сервер также создает запись ARP, состоящую из MAC-адреса клиента и арендованного IPv4-адреса DHCP сервер отправляет связанное сообщение **DHCPOFFER** запрашивающему клиенту, как одноадресная передача (**unicast**), используя MAC-адрес сервера в качестве исходного адреса и MAC-адрес клиента в качестве адреса доставки.

4. Когда клиент получает **DHCPOFFER** с сервера, он отправляет обратно сообщение **DHCPREQUEST**. Это сообщение используется как для получения, так и для продления аренды. Когда используется для получения аренды, **DHCPREQUEST** служит в качестве уведомления о принятии выбранных сервером параметров, которые он предложил, и отклонении предложения от других серверов. Многие корпоративные сети используют несколько DHCP серверов, и сообщение **DHCPREQUEST** отправляется в виде широковещательной передачи, чтобы информировать все серверы о принятом предложении.

5. При получении сообщения **DHCPREQUEST** сервер проверяет информацию об аренде с помощью ICMP-запроса на этот адрес, чтобы убедиться, что он уже не используется и создает новую **ARP** запись для аренды клиента, а затем отвечает одноадресным DHCPACK-сообщением. Это сообщение является дубликатом **DHCPOFFER**, за исключением изменения поля типа сообщения. Когда клиент получает сообщение **DHCPACK**, он регистрирует информацию и выполняет поиск ARP для назначенного адреса. Если ответа на ARP нет, клиент знает, что адрес IPv4 действителен и начинает использовать его как свой собственный.

Сервер DNS

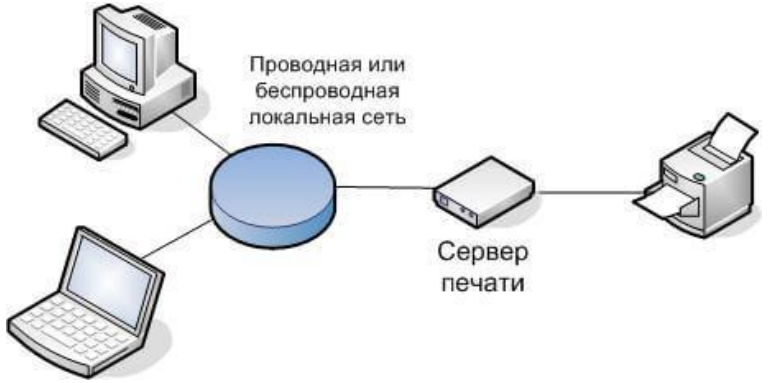
Компьютеры используют DNS для преобразования доменных имен в IP-адреса.



Сервер печати

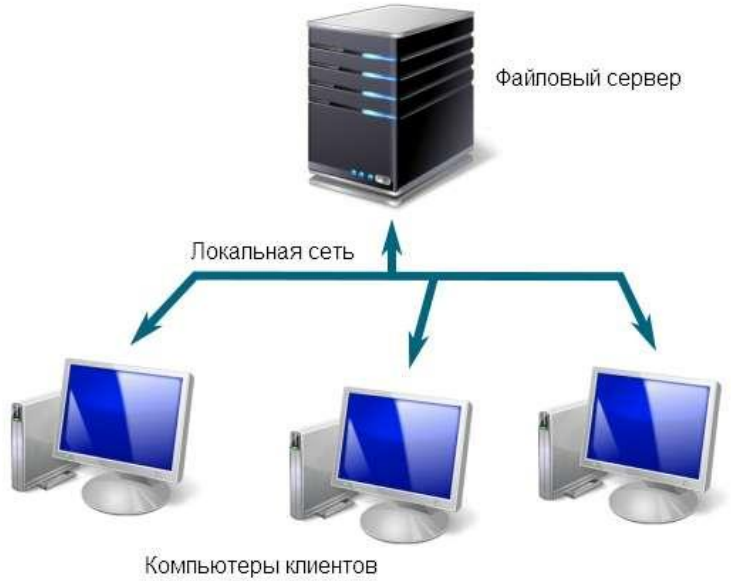
Серверы печати позволяют нескольким компьютерам получать доступ к одному принтеру. Сервер печати имеет три функции:

- Предоставлять клиентский доступ к ресурсам печати.
- Управлять заданиями печати, формируя очередь печати, и в момент готовности принтера передавать на него нужную информацию.
- Предоставлять пользователям обратную связь.



Файловый сервер

Протокол передачи файлов (File Transfer Protocol, FTP) используется для обмена файлами между клиентом и сервером. FTP-клиент представляет собой компьютерное приложение для выгрузки и загрузки файлов через сервер, на котором работает служба FTP.

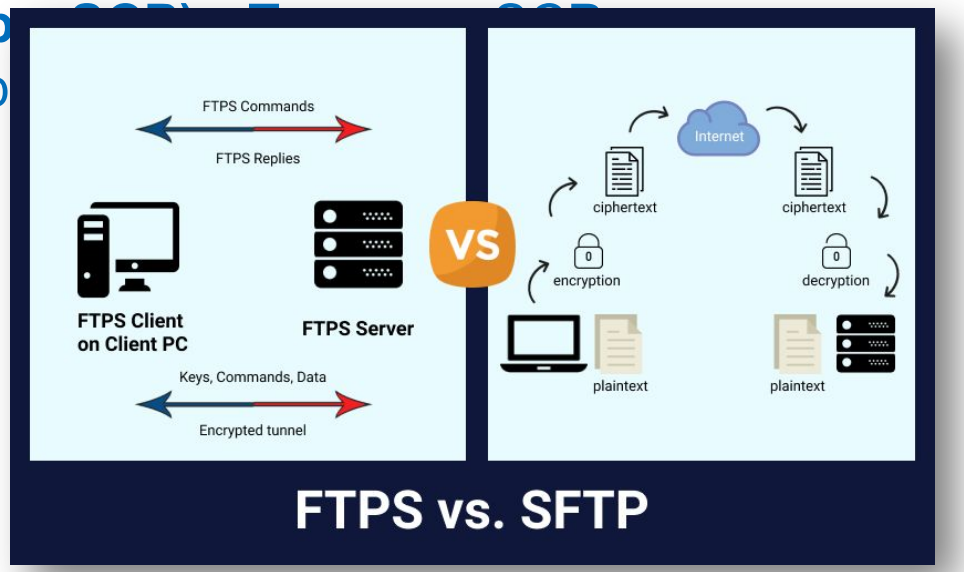


Протокол FTP имеет множество недостатков в плане безопасности. В этой связи рекомендуется использовать более защищенный протокол передачи файлов, например:

- **Защищенный протокол передачи файлов (File Transfer Protocol Secure, FTPS)** - Клиент FTP может запрашивать создание зашифрованного сеанса передачи файлов. Файловый сервер может принять или отклонить такой запрос.
- **Протокол передачи файлов с использованием SSH (SSH File Transfer Protocol, SFTP)** - Протокол SFTP, представляющий собой расширение протокола Secure Shell (SSH), можно использовать для создания защищенного сеанса передачи файлов.
- **Защищенный протокол копирования (Secure Cop**

SSL поддерживает разные криптографические
также использует SSH для защищенной передачи ф
алгоритмы. В ходе установления связи используется криптосистема открытого ключа RSA.

Главное, что отличает SFTP от стандартного FTP и FTPS, это то, что SFTP шифрует абсолютно все команды, имена пользователей, пароли и другую конфиденциальную информацию.



Различия между SCP и SFTP

Существует несколько сходств между обеими программами передачи файлов, поскольку обе используют TCP-порт 22 и работают по SSH, что делает их равными с точки зрения безопасности.

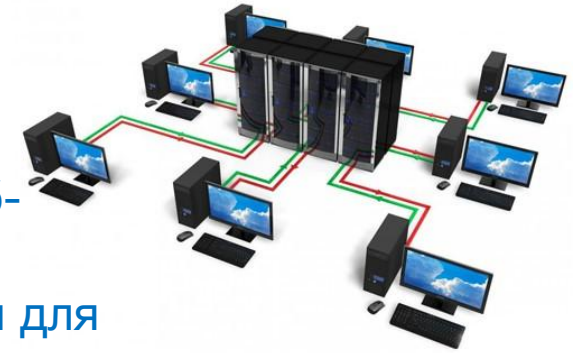
SCP передает данные с защитой от перехвата, а **SFTP** выполняет функции доступа к файлам, их передачи и управления.

Таким образом, в то время как **SCP** лучше спроектирован для одноразовой передачи файлов между двумя сетевыми компьютерами или удаленно через Интернет, **SFTP** делает это, а также управляет этими данными.

SCP не может выполнять некоторые операции, такие как удаленный просмотр каталога или удаление файла; он может только передавать файлы. **SFTP**, с другой стороны, выполняет все, в том числе задачи удаления файлов и перечисления каталогов.

SFTP предлагает компонент с графическим интерфейсом для более удаленного администрирования и больше похож на файловую систему с удаленным доступом, но **SCP** этого не предлагает.

Веб-сервер



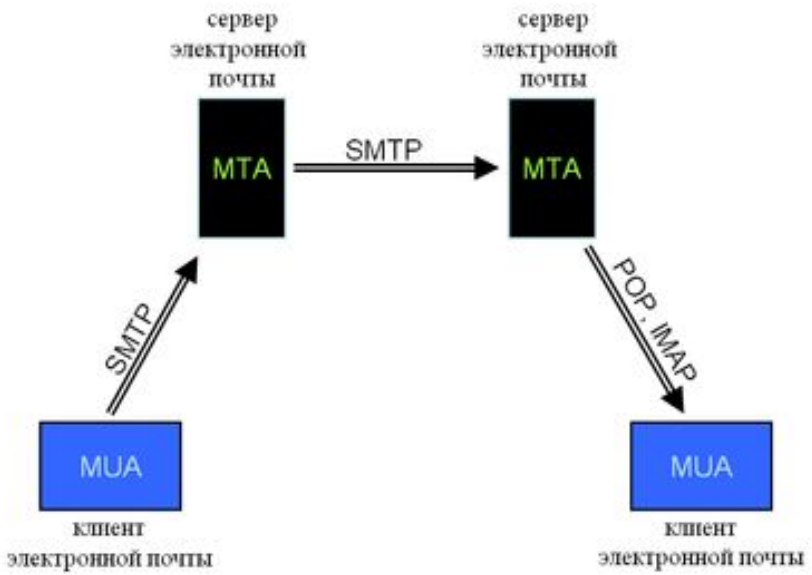
Веб-ресурсы располагаются на веб-сервере. Хост получает доступ к веб-ресурсам с использованием протокола передачи гипертекста (HTTP) или защищенного протокола HTTPS. HTTP представляет собой набор правил для обмена текстом, графическими изображениями, звуковыми и видео файлами во всемирной паутине. HTTPS дополнительно использует шифрование и аутентификацию через протокол Secure Sockets Layer (SSL) или более новый протокол Transport Layer Security (TLS). HTTP использует порт 80. HTTPS использует порт 443.

браузер обрабатывает три сегмента URL:

1. **http** (протокол или схема)
2. **www.cisco.com** (имя сервера)
3. **index.html** (имя запрашиваемого файла)

Почтовый сервер

Клиенты электронной почты для отправки и получения сообщений обращаются к серверам электронной почты. Серверы электронной почты взаимодействуют с другими серверами электронной почты для обмена сообщениями между доменами. Почтовый клиент не соединяется непосредственно с другим почтовым клиентом для отправки сообщения. Вместо этого оба клиента пользуются услугами почтового сервера.



Прокси-сервер

Прокси-сервер — это дополнительное звено между вами и интернетом. Некий посредник, который отделяет человека от посещаемого сайта. Создает условия, при которых сайт думает, что прокси — это и есть реальный человек.

Такие посредники довольно многофункциональны и используются в нескольких сценариях:

1. Для обеспечения конфиденциальности. Чтобы сайты не знали, кто именно их посещает.
2. Для повышения уровня безопасности при выходе в сеть. Базовые атаки будут направлены именно на прокси.
3. Еще он нужен, чтобы получать доступ к контенту, который существует только в определенной локации.
4. Чтобы ускорить доступ к некоторым ресурсам в интернете.
5. Ну и для того, чтобы получить доступ к заблокированным страницам. Сайтам, мессенджерам и так далее.

Все за счет того, что прокси подменяет IP-адрес, а трафик проходит через дополнительный сервер, на котором могут быть кэшированные данные или организованы дополнительные механизмы защиты данных.

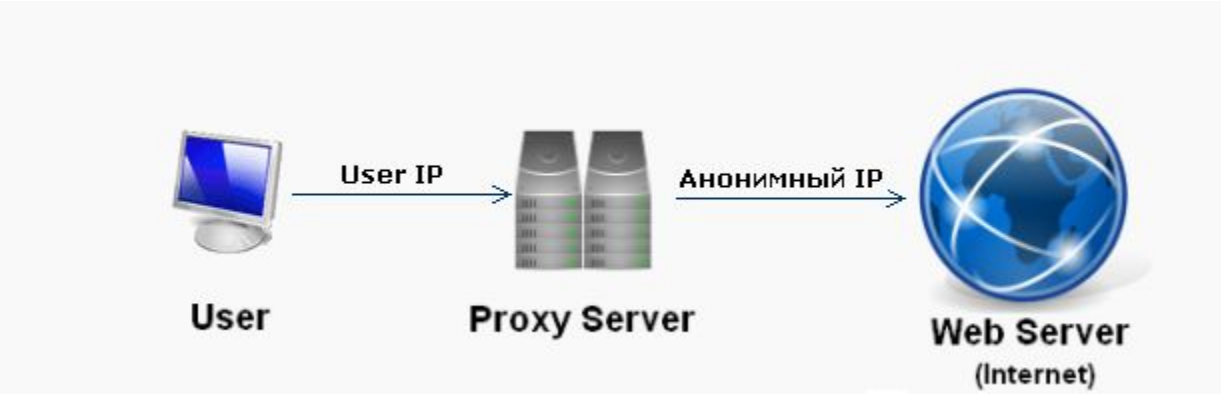
Типы прокси-серверов

Прозрачные

Такой прокси-сервер не утаивает от посещаемого сайта никакой информации. Во-первых, он честно сообщит ему о том, что является прокси, а во-вторых, передаст сайту IP-адрес пользователя по ту сторону сервера. С подобным типом можно встретиться в публичных заведениях, школах.

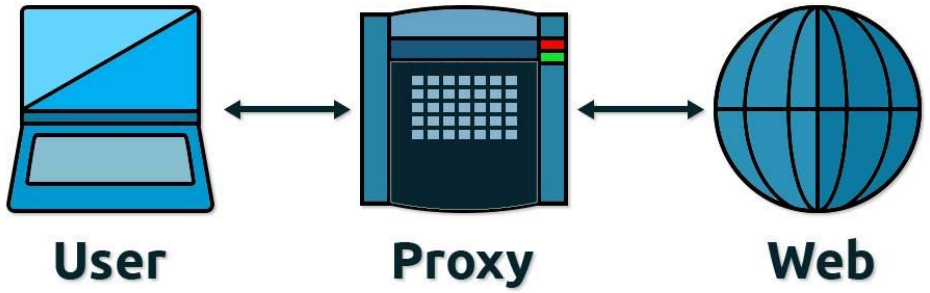
Анонимные

Более востребованный тип прокси. В отличие от первого, он тоже заявляет посещаемому ресурсу о своей proxy-сущности, но личные данные клиента не передает. То есть будет предоставлять обезличенную информацию для обеих сторон. Правда, неизвестно, как поведет себя сайт, который на 100% знает, что общается с proxy.



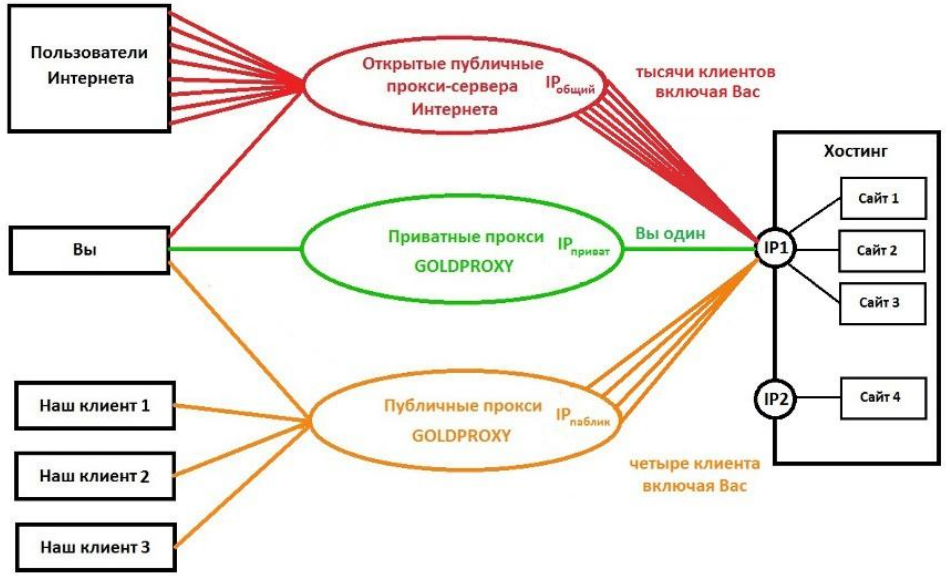
Искажающие

Такие прокси тоже идентифицируют себя честно, но вместо реальных пользовательских данных передают подставные. В таком случае сайты подумают, что это вполне себе реальный человек, и будут вести себя соответствующе. Например, предоставлять контент, доступный только в конкретном регионе.



Приватные

Вариант для параноиков. Такие прокси регулярно меняют IP-адреса, постоянно выдают фальшивые данные и заметно сокращают шансы веб-ресурсов отследить трафик и как-то связать его с клиентом.



Зачем нужен прокси-сервер?

Фильтрация доступных ресурсов

Это как родительский контроль. Только масштабы иные. Подобный proxy запросто могут поднять в крупной компании, чтобы сотрудники не лезли в Твиттер, пока занимаются делами

Ускорение работы интернета

На прокси-серверах могут храниться кэшированные копии сайтов. То есть при входе на определенный сайт вы получите данные именно с proxy

Сжатие данных

На некоторых прокси установлены инструменты, которые сжимают весь запрашиваемый контент перед тем, как перенаправить его к конечному пользователю. По такому принципу работает «Турбо-режим» в браузерах

Безопасность

Прокси может обезопасить не только частную жизнь, но и защитить от реальных угроз вроде вирусов. Можно настроить шлюз таким образом, чтобы он не принимал запросы с вредоносных ресурсов

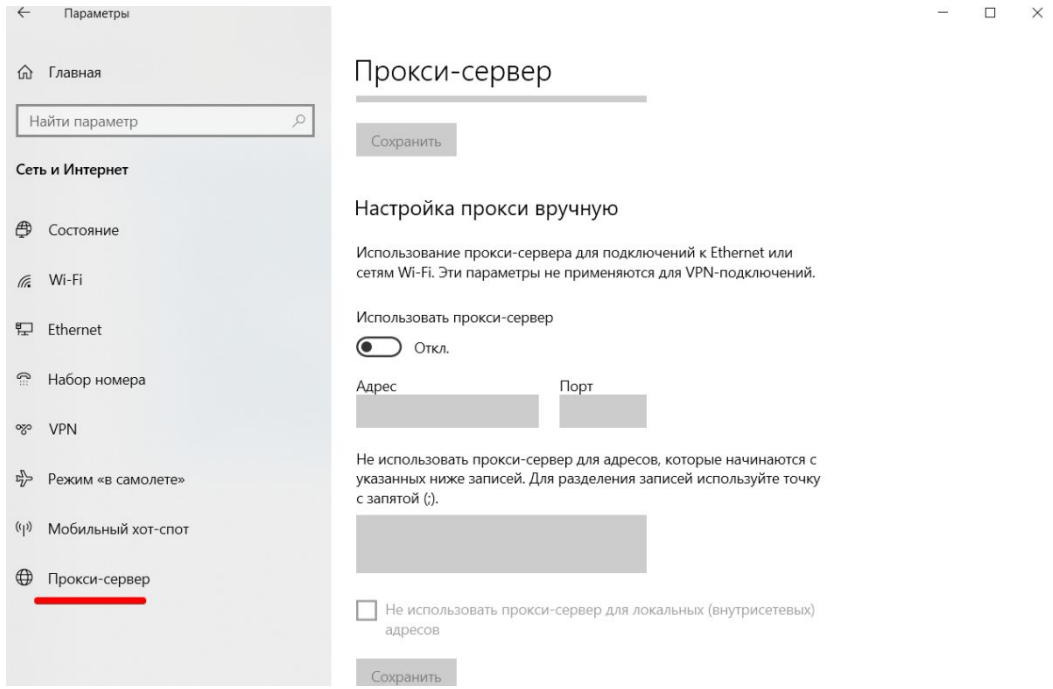
Конфиденциальность

Доступ к запрещенному контенту

Настраиваем прокси-сервер

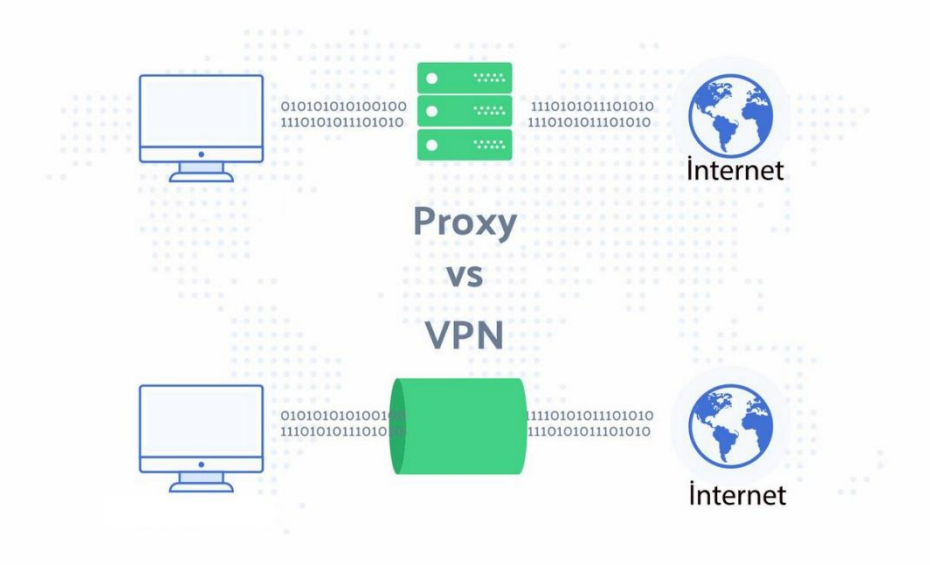
Открываем основные настройки системы.

- Выбираем пункт настроек «Сеть и интернет».
- Затем переходим в подпункт «Прокси».
- Спускаемся до блока настроек «Настройка прокси вручную».
- Переводим тумблер «Использовать прокси-сервер в положение «Вкл.».
- Вводим адрес прокси-сервер и порт в соответствующие поля.
- Затем нажимаем на кнопку «Сохранить»



Сравнение прокси с VPN

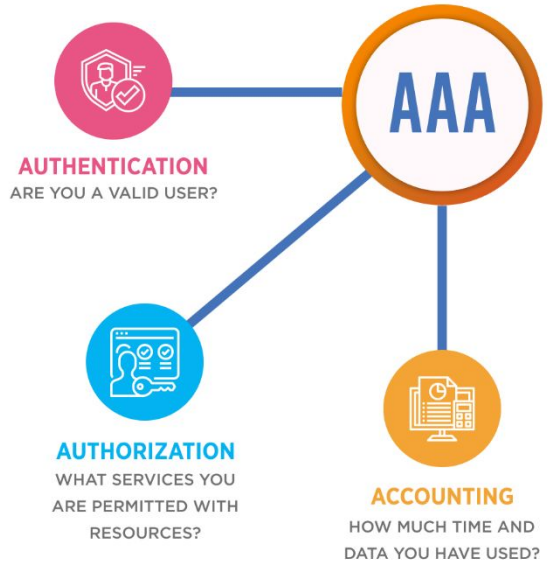
VPN лучше как в плане безопасности, так и в плане удобства, но такая сеть чаще стоит приличных денег. Зачастую VPN сложнее в настройке и работают не так быстро. Через proxy же можно подключаться, не устанавливая на компьютер ничего.



Также стоит понимать: использование прокси-сервера равняется передаче личных данных третьему лицу. Обычно с ними знакомятся только провайдер связи и владельцы страниц, которые вы посещаете. Теперь появится еще одна сторона, у которой будет доступ ко всему вашему трафику. Не факт, что он будет шифроваться или храниться в безопасности. И неизвестно, на каких условиях proxy-сервер может взаимодействовать с государством.

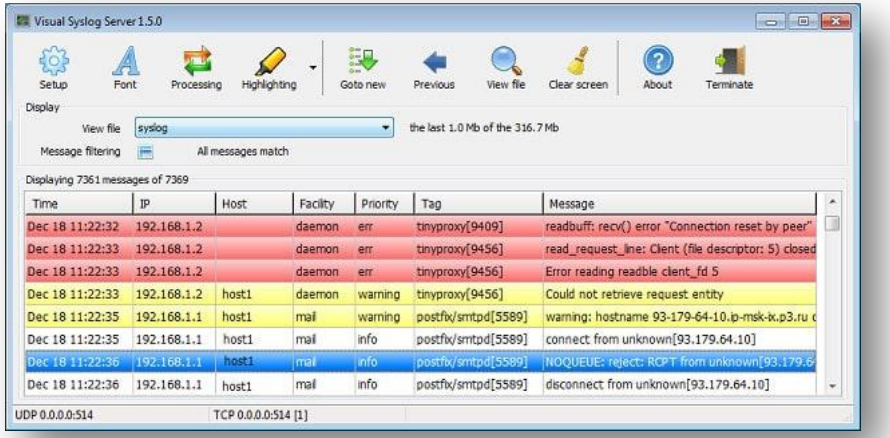
Сервер аутентификации

Для контроля доступа к сетевым устройствам обычно используют службы аутентификации, авторизации и учета (Authentication, Authorization, Accounting).



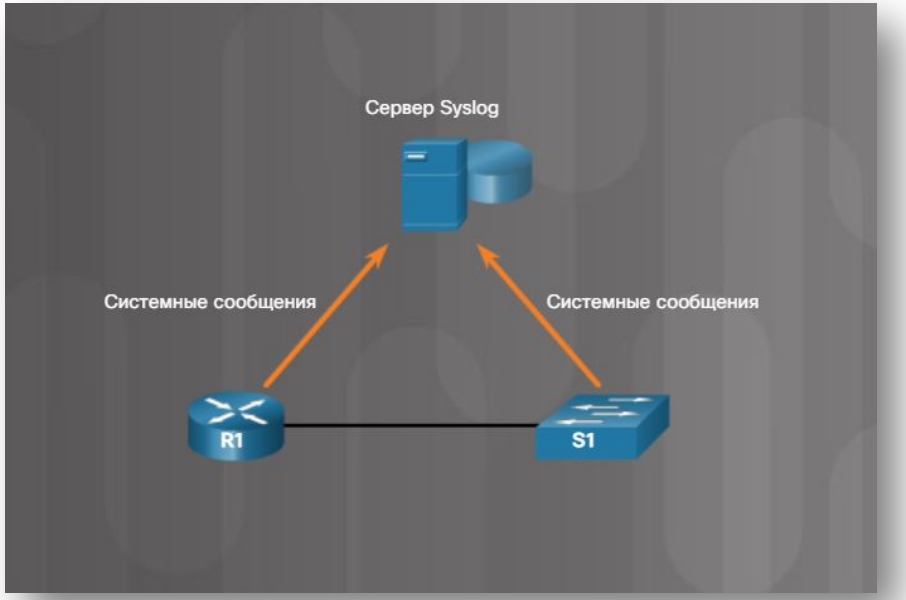
Сервер Syslog

Протокол syslog поддерживают большинство сетевых устройств, включая маршрутизаторы, коммутаторы, серверы приложений, межсетевые экраны и другие сетевые устройства. Этот протокол дает возможность сетевым службам отправлять по сети системные сообщения на серверы syslog.



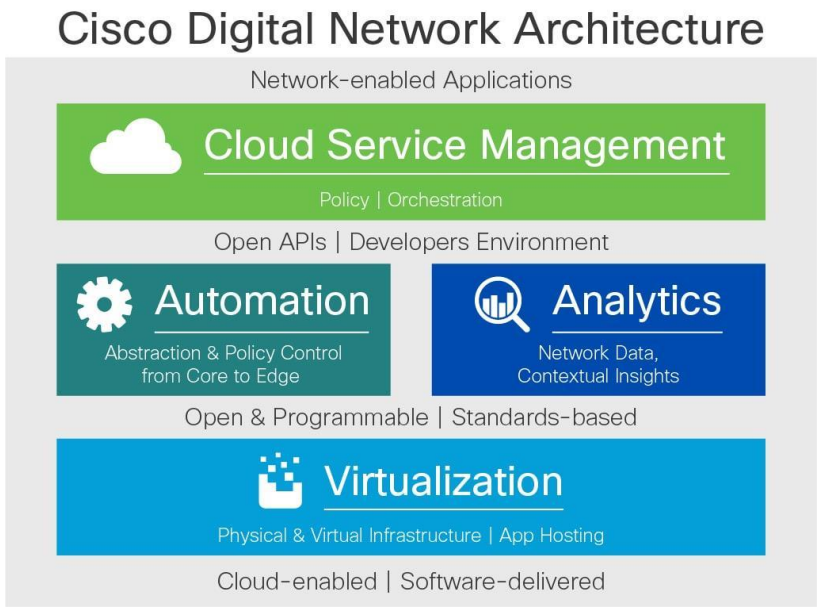
Сервис ведения системного журнала (syslog) обеспечивает три основных функции:

- Возможность собирать информацию из системных журналов с целью мониторинга и устранения неисправностей
- Возможность выбирать тип информации из системных журналов, которую нужно собрать
- Возможность указывать место назначения для отправки захваченных syslog-сообщений



Сервер управления оконечными устройствами

Сервер управления оконечными устройствами обычно отвечает за мониторинг всех оконечных устройств в сети, включая стационарные ПК, ноутбуки, серверы, планшеты и любые другие устройства, подключенные к сети. Сервер управления оконечными устройствами может ограничивать подключение оконечных устройств к сети, если такие устройства не отвечают заранее установленным критериям. Например, он может проверять, установлены ли на устройстве последние обновления ОС и антивирусного ПО.



Унаследованные и встроенные системы

Унаследованные системы - это компьютерные и сетевые системы, которые больше не поддерживаются, но продолжают использоваться в имеющихся сетях. К ним относятся самые разные системы: от промышленных систем управления до компьютерных мейнфреймов и различных сетевых устройств, таких как концентраторы и мосты. Унаследованные системы по своей сути уязвимы к угрозам безопасности, т. к. их нельзя обновить или установить для них исправления. Для защиты от некоторых рисков, связанных с такими системами, их можно изолировать.

Облачный сетевой контроллер

Облачный сетевой контроллер - это облачное устройство, которое позволяет сетевому администратору управлять сетевыми устройствами. Например, компания среднего размера, у которой есть несколько филиалов, может использовать сотни точек беспроводного доступа. Без специального контроллера управление этими устройствами может быть затруднено.

Сетевой администратор может управлять беспроводными устройствами, расположенными в разных точках, простым щелчком мышью.

- Профессиональное централизованное управление сетью Wi-Fi
- Бесплатный облачный доступ к управлению сетью откуда и когда угодно