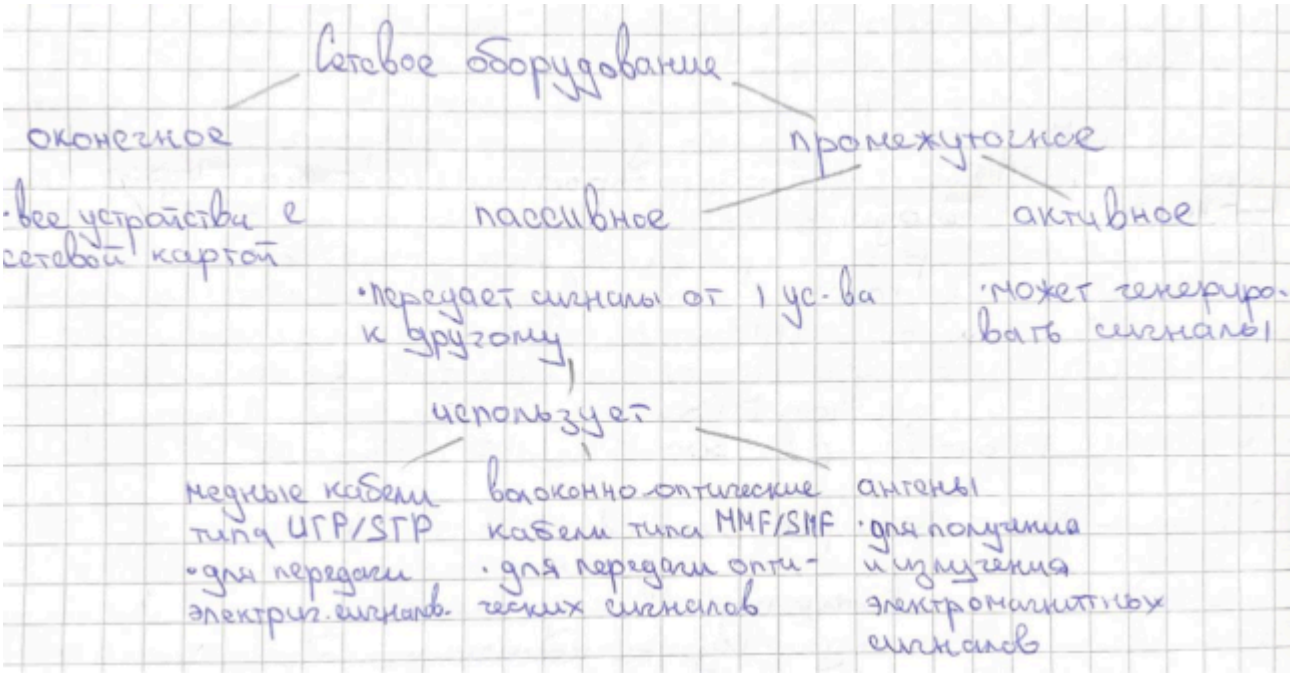
Введение в сетевые технологии

Сеть (Network) — это набор оборудования и программного обеспечения, позволяющий компьютерам и другим устройствам взаимодействовать на больших расстояниях. Кроме компьютеров к сети также можно подключать принтера, сканеры, камеры наблюдения, ip-телефоны, смартфоны и вообще любое устройство, у которого есть сетевая карта. Все это оборудование называют оконечным.

Кроме оконечного оборудования также есть промежуточное сетевое оборудование, которое разделяется на активное и пассивное. Активным называют оборудование, которое может генерировать сигналы. А пассивное оборудование передаёт эти сигналы от 1 активного устройства к другому. Тип пассивного оборудования выбирается в зависимости от типа передаваемых сигналов. Это могут быть медные кабели типа UTP/STP - для передачи электрических сигналов, волоконно-оптические кабели типа MMF/SMF — для передачи оптических сигналов и антены — для излучения и получения электромагнитных сигналов, которые передаются через окружающую среду. Кроме кабелей в обязательном порядке используются разъемы для того, чтобы согласовать кабель с сетевой картой. Типы кабелей и разъемов определяет базовая сетевая технология (БЛВС — Базовая технология Локальной Вычислительной Сети). Наиболее распространенной базовой технологией на сегодняшний день является семейство Ethernet.

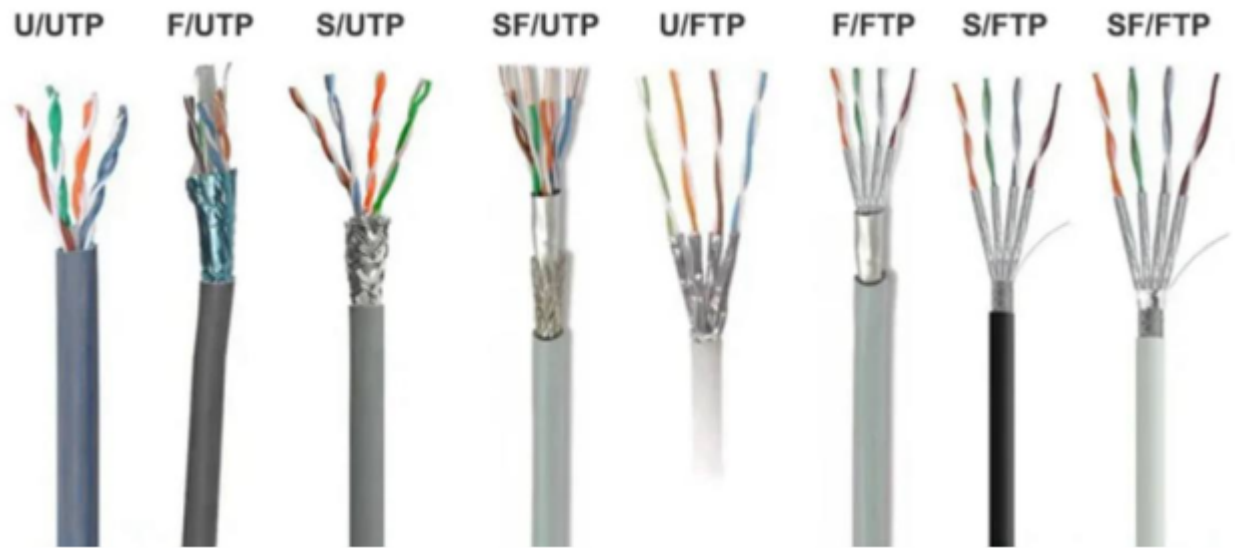


Рассмотрим пассивное оборудование более подробно.

Медные кабели

Их принято называть витая пара (Twisted Pair). Кабель витая пара представляет собой 8 попарно скрученных медных жил в одной оболочке. Эти 8 жил образуют 4 пары кабеля. Есть удешевленные варианты кабеля витая пара включающие в себя всего 4 жилы, попарно скрученных в 2 пары.
Такие кабели настоятельно не рекомендуется использовать!
Их можно использовать только, например, для низкокачественных видеокамер. Больше нигде!!!

Кабели типа витая пара могут быть неэкранированными (UTP – Unshieldede Twisted Pair (Неэкранированная витая пара)) и экранированные (STP – Shielded Twisted Pair (Экранированная витая пара), FTP – Foiled Twisted Pair (Экранированная витая Пара), SFTP – Shielded Foiled Twisted Pair, S/UTP).
Экранированные медные кабели, как правило прокладываются в помещениях с плохой электромагнитной совместимостью (промышленные помещения), где есть электромагнитное излучение, которое может помешать работе сети.

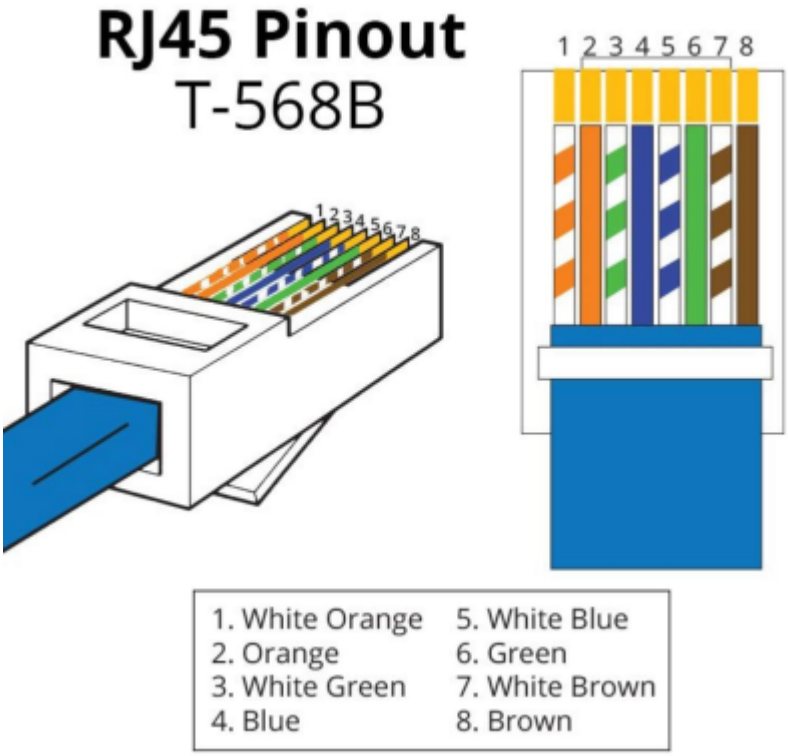


Кроме типа витой пары важнейшей её характеристикой является категория. Категория определяет полосу пропускания кабеля, которая самым прямым образом влияет на пропускную способность канала связи. На сегодняшний день наименьшей категорией витой пары является 3-я. Полоса пропускания такого кабеля 16 МГц, что позволяет увеличить скорость передачи данных до 10 МГбит / сек. На сегодня такие используются только в телефонной связи (стационарный телефон). Следующей очень распространенной категорией стала 5-я с полосой пропускания 100 МГц, что позволяло обеспечить скорость передачи данных в 100 МГбит / сек. Самой распространенной категорией витой парой на сегодня является 5е, полоса пропускания 100 МГц, до 100 МГбит / с (Mbps -mega bit per second). Также есть 6 категория 250 МГц, 1 Гбит/сек. 6А 500МГц, 10 МГбит/сек.

UTP cat 3 - 16 MHz, 10 Mbit/s;
UTP cat 5 - 100 MHz, 100 Mbps;
UTP cat 5e - 100 MHz, 100 Mbps;
UTP cat 6 - 250 MHz, 1 Gbps;
UTP cat 6a - 500 MHz, 10 Gbps;

С кабелем типа витая пара всегда используется коннекторы типа RJ-45. Раскладка пар на коннекторе определяется стандартом EIA/TIA – 568 A/B.

Главным ограничением медных кабелей типа витая пара является дальность передачи. Ни 1 витая пара не может надежно передавать сигнал на расстояние больше 100 метров без участка регенерации. Поэтому рынок захватили и продолжают захватывать волоконно-оптические кабели.



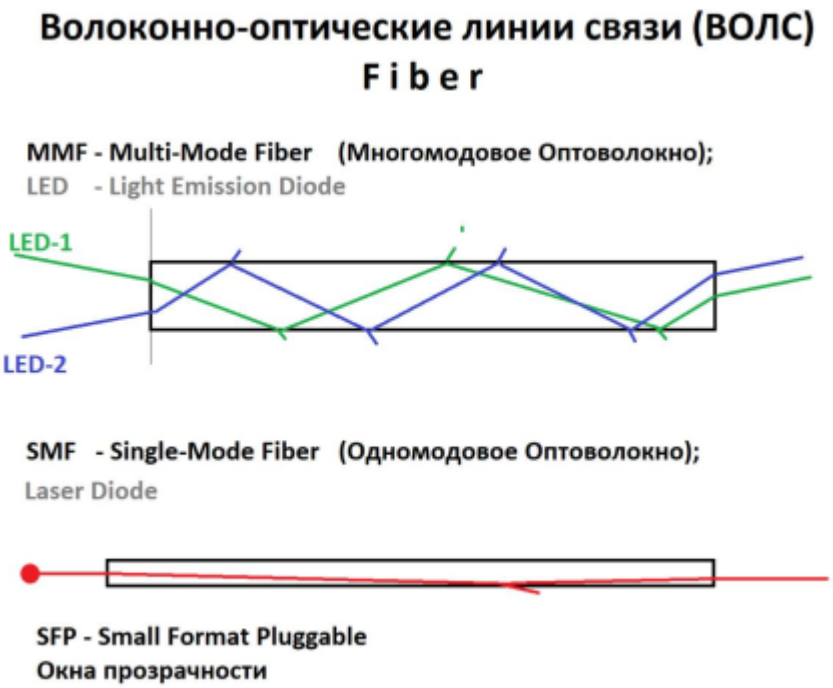
Волоконно-оптические линии связи (ВОЛС) (Fiber)

Волоконно-оптические линии связи (ВОЛС) (Fiber) бывают 2-х типов:

MMF – Multi-Mode Fiber (Многомодовое оптоволокно)
SMF – Single-Mode Fiber (Одномодовое оптоволокно)

MMF позволяет по 1 жиле передавать множества сигналов из разных источников на разной длине волны. Для ввода сигнала в волокно используются самые обычные светодиоды (LED – Light Emission Diode). Но максимальное расстояние, на которое может передавать MMF ограничивается в 500 метров. В некоторых случаях до километра без участка регенерации. Это обусловлено тем, что большое количество энергии сигнала теряется в результате отражения и преломления цвета в стенках оптического волокна.

В SMF сигнал вводится в волокно при помощи лазерного диода (лазера), мощность которого в значительной степени превышает мощность обычных светодиодов. Кроме того, сигнал вводится в волокно практически под прямым углом, что минимизирует его отражение и преломление внутри волокна, за счет чего SMF способна надежно передавать сигнал на расстояние до 10 км без участка регенерации. Но по 1 оптической жиле одновременно может передаваться только 1 сигнал от 1 источника и только в 1 направлении. Следовательно, для обеспечения полнодуплексного канала при помощи SMF нужно 2 оптические жилы, 1 передает данные в 1 направлении, другая — в другом, что негативно влияет на стоимость линии связи. Но даже такое негативное влияние несоизмеримо с тем, чтобы устанавливать участок регенерации каждые пол километра.



Как правило, активное сетевое оборудование, обеспечивающее работу по ВОЛС реализуют это через SFP (Small Format Pluggble) модули. При выборе волоконно-оптического оборудования всегда обязательно нужно учитывать, в каких окнах прозрачности оно работает. Окна прозрачности определяют длину волны светового сигнала, которое измеряется в нанометрах. Распространенными окнами прозрачности являются 850, 1310, 1550 нанометров. Также появились окна прозрачности 150 нанометров и 1400 нанометров. Окно прозрачности всегда можно узнать из базовой технологии, для которой покупается оборудование.

Базовые технологии Локальных Вычислительных Сетей (БЛВС)

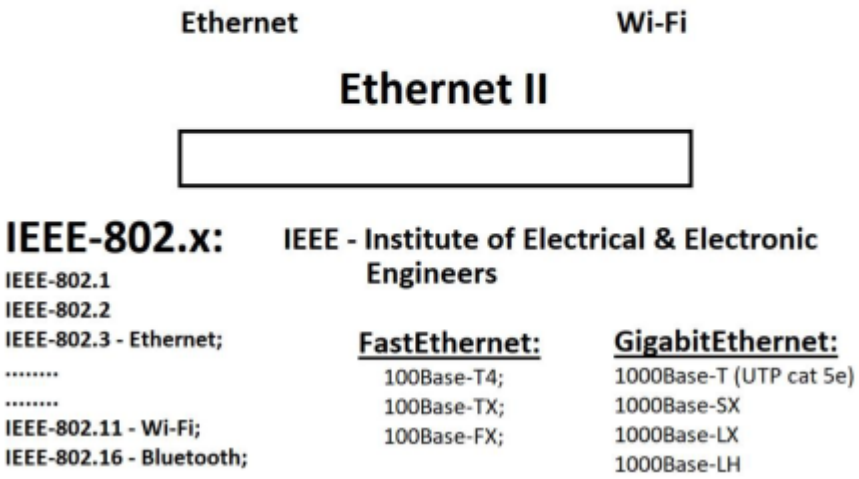
Это набор активного и пассивного оборудования, обеспечивающего работу аппаратной части сети. Существует множество базовых технологий локальных сетей (TokingRing, FDDI, 100VG-AnyLan – нигде не используются сейчас), но наиболее распространенными на сегодня являются технологии семейства Ethernet и Wi-Fi. Эти 2 технологии полностью совместимы между собой благодаря тому, что они используют одинаковые формат кадра. И там и там используется кадр формата Ethernet 2. Всего существует 4 формата кадра.

Все технологии семейства Ethernet описаны в серии стандартов IEEE-802.x , где x- номер стандарта.
IEEE-802.3 – Ethernet;
IEEE-802.11 – Wi-Fi;
IEEE – Institute of Electrical and Electronics Engineers

Каждая технология описана как минимум 1 спецификацией. FastEthernet описана следующими спецификациями: 100Base-T4, 100Base-TX, 100Base-XX;

Базовые технологии локальных вычислительных сетей (БЛВС)

TokenRing, FDDI, 100VG-AnyLan.....



Спецификация — это описание активного и пассивного оборудования для построения сети. Например, 100Base-T4 можно построить на кабелях UTP Category3; 100Base-TX для построения требует кабели UTP 5 категории; 100Base-XX строятся на волоконно-оптических кабелях.

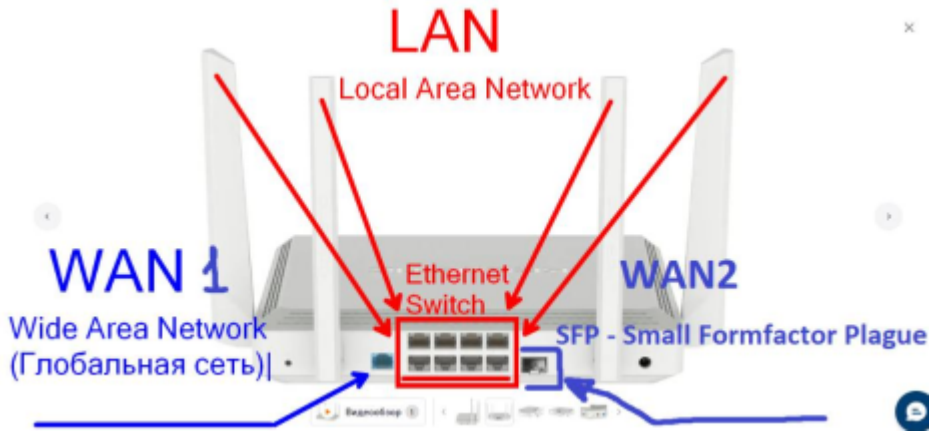
Самой распространенной спецификацией Gigabit Ethernet. Также широкое распространение получили стандарты волоконно-оптического Gigabit Ethernet: 1000Base_T, 1000Base-SX, 1000Base-LX, 1000Base-LH

Кроме спецификаций базовая технология также описывает не менее важную вещь, определяющую базовую технологию (это формат кадра)

Активное сетевое оборудование

Активным сетевым оборудованием является любое устройство, которое генерирует электрические, оптические или радио- сигналы. Все активное оборудование можно разделить на оконечное и промежуточное.

К промежуточному оборудованию относятся:
1. Коммутатор (switch) — это устройство, которое объединяет компьютеры в сеть. Коммутатор перенаправляет Ethernet кадры с 1 порта на другой по MAC-адресу.
2. Маршрутизатор (Router) – это устройство, которое объединяет сети одной или разных базовых технологий в составную сеть. Маршрутизатор перенаправляет ip-пакеты из 1 сети в другую по ip-адресу. Маршрутизаторы — это основные устройства, на которых работает сеть интернет. Именно маршрутизаторы доставляют данные из 1 сети в другую через Internet. Сам Интернет, как мы его понимаем, это 1 большая составная сеть.
Internet – составная сеть.
Intranet – составные сети меньших размеров.



3. Точка доступа Wi-Fi – это устройство, позволяющее включить беспроводные устройства в проводную сеть.
Примечание: Wi-Fi роутеры объединяют в себе все 3 устройства (коммутатор, маршрутизатор, точку доступа)
4. Повторитель (Repeater) — устройство, усиливающее и восстанавливающее сигнал для того, чтобы передать его на большее расстояние.
5. Преобразователь среды передачи (Mediaconverter) как правило используется, для того чтобы преобразовать оптический сигнал в электрический и наоборот. Дело в том, что большинство современных провайдеров заводят интернет по оптическому кабелю. Но, несмотря на это, для монтажа сети внутри здания все еще используется витая пара и большинство роутеров, несмотря на это в качестве wan-порта все еще используют RJ-45. Для того, чтобы согласовать оптическую сеть с медной сетью используются медиаконверторы.

Active Network Equipment

1. **Коммутатор (Switch)** - это устройство, которое объдиняет компьютеры в сеть;
   MAC-адрес

2. **Маршрутизатор (Router)** - это устройство, которое объединяет сети одной или разных базовых технологий в составную сеть;
   IP-пакеты из одной сети в другую по IP-адресу.
   Internet - составная сеть;
   Intranet;

3. **Точка доступа Wi-Fi** - это устройство, которое позволяет включить беспровоные устройства в проводную сеть.

4. **Повторитель (Repeater)** - это устройство, которое усиливает и восстанавливает сигнал, для того чтобы передать его на болешее расстояние.

5. **Преобразователь среды передачи (Mediaconverter)**

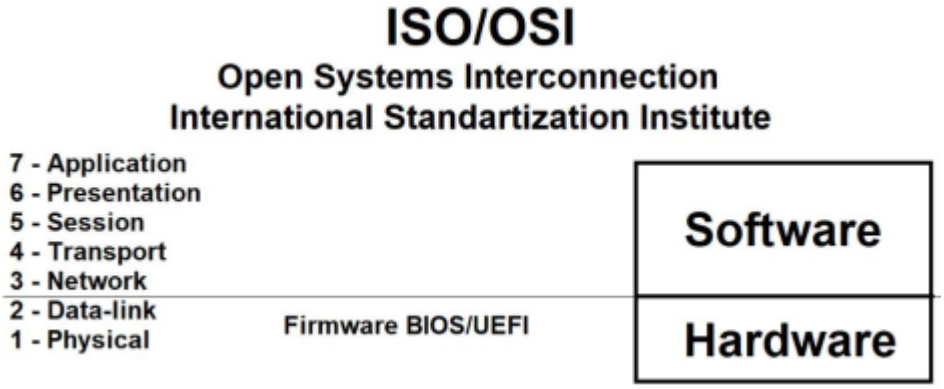
Модели сетевого взаимодействия

Задача сетевого взаимодействия является достаточно сложной. Как и любую другую сложную задачу, ее можно разделить на несколько более простых задач. Это называется декомпозиция. Декомпозицию задачи сетевого взаимодействия выполняют при помощи многоуровневых моделей. Первая из которых была ISO/OSI или модель взаимодействия открытых систем. Эту модель разработал международный институт по стандартизации. Эта модель состоит из 7 уровней, каждый из которых выполняет свои задачи.

ISO/OSI

7 уровень Прикладной (Application) выполняет задачу предоставления данных для приложений и реализован в самих приложениях в виде прикладных протоколов.

6 уровень Представительный (Presentation) представляет данные от протоколов прикладного уровня в едином формате для передачи через сеть.
5 уровень Сеансовый (Session) отвечает за установку виртуальных соединений и контроль доставки данных. Этот уровень выставляет контрольные точки в передаче и при ошибках передачи позволяет возобновить отправку данных с последней контрольной точки, а не с самого начала.
4 уровень Транспортный (Transport) Предназначен для адресации протоколов 1-го уровня в пределах одного узла
3 уровень Сетевой (Network) Отвечает за адресацию в составных сетях а также за доставку пакетов с данными до узла назначения.
2 уровень Канальный (Data-Link) Отвечает за адресацию узлов в пределах 1 локальной или глобальной сети определенной базовой технологии а также за доставку данных до узла в пределах 1 определенной сети.
1 уровень Физический (Physical) Отвечает за физическое соединение узлов в сети (типы разъемов, кабелей, антен) и за методы кодирования сигналов.



Физический уровень сугубо аппаратную реализацию. Канальный уровень — аппаратно-программную реализацию. А все остальные уровни — сугубо программную реализацию.
Любая базовая технология полностью берет на себя обязанности первых 2-х уровней — физического и канального. Именно базовая технология определяет тип разъемов и кабелей для построения сети, формат кадра, передаваемого по сети и формат адреса для нумерации узлов в сети. Обязанности всех остальных уровней выполняет стек протоколов.
Одним из ключевых понятий в сетевых технологиях является протокол.
Протокол — это формализованные правила взаимодействия сетевых компонентов разных узлов на 1 уровне. Модель OSI также вводит понятие интерфейс.
Интерфейс — это формализованные правила взаимодействия сетевых компонент одного узла на разных уровнях.

Протоколы и интерфейсы позволяют взаимодействовать оборудованию разных производителей и программам в разных операционных системах. На каждом уровне модели OSI используется свой определенный PDU (Protocol Data Unit) – блок данных с которым работают протоколы определенного уровня. На прикладном уровне PDU является сообщение (Message); на транспортном и сеансовом PDU – сегмент или датаграмма; на сетевом — пакеты; на канальном — кадры; на физическом — биты;

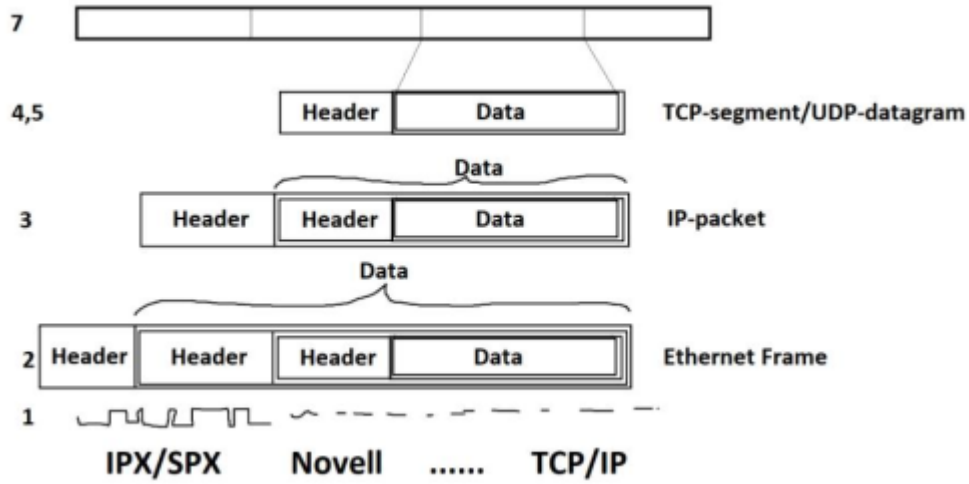
PDU

Protocol Data Unit

7 - Message
5, 4 } Segment/Datagram
3 - Packet
2 - Frame
1 - bit

Encapsulation/Decapsulation

Разнотипные сообщения от протоколов прикладного уровня преобразуются в единый формат сегмента или датаграммы представительным уровнем. После чего эти сегменты или датаграммы проходят процесс инкапсуляции. То есть, каждый следующий протокол нижнего уровня добавляет к этим данным свои служебные данные в виде заголовка. На приемной стороне происходит обратный процесс (декопсуляция). То есть каждый протокол определенного уровня при получении блока данных читает свой заголовок, удаляет его и полученные данные отправляет на следующий уровень.

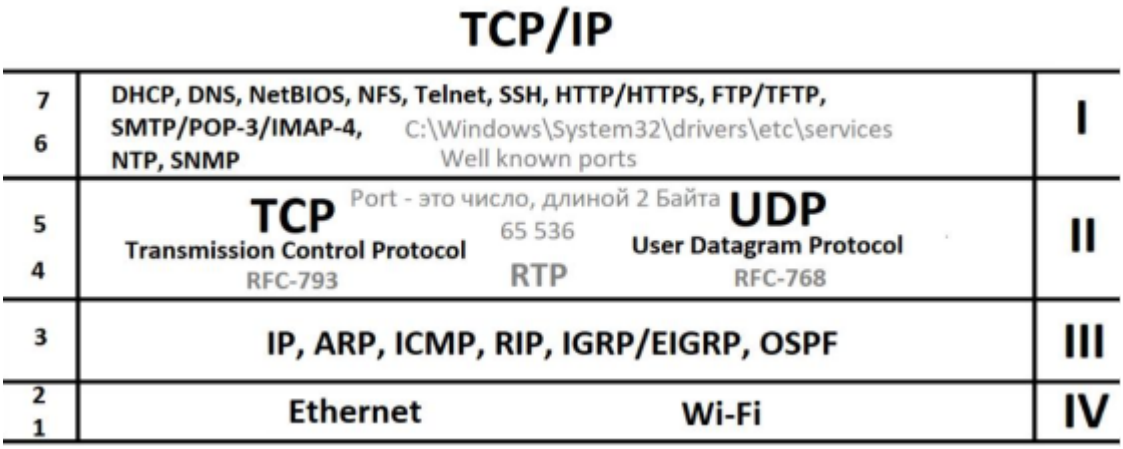


OSI является первой сетевой моделью и есть даже стек протоколов OSI, но он не получил широкого распространения, а лишь дал толчок для создания других стеков протоколов таких как IPX/SPX, Novell… Но наиболее распространенным стеком протоколов является TCP/IP. Именно на этом стеке построен интернет, каким мы его знаем.

Стек протоколов TCP/IP

Состоит из 4-х уровней, которые номеруются сверху вниз:
1) Прикладной (Application)
2) Транспортный (Main)
3) Сетевой или межсетевой(Network или Internetwork)
4) Уровень сетевых интерфейсов (Network Interface)

Каждый из этих уровней выполняет обязанности 1-го или нескольких уровней модели OSI.



Протоколы прикладного уровня

Протокол DHCP или же Dynamic Host Configuration Protocol (Протокол Динамической Настройки Узлов) отвечает за выдачу Ip-адресов в LAN-сети и других настроек протокола IP. Кроме IP-адреса это еще маска подсети, основной шлюз, DNS и тд. Протокол DHCP также может выдавать имя загрузочного файла и адрес загрузочного сервера. Для загрузки операционной системы по сети. Протокол DHCP на транспортном уровне использует порты UDP-67, UDP-68.Протокол DHCP произошел от протокола Bootp (старая версия DHCP).

Telnet – это протокол удаленного управления, который позволяет выполнять команды на удаленном компьютере через LAN (Local Area Network) или Internet. Главным недостатком протокола Telnet является то, что он передает данные по открытым каналам связи, включая логины, пароли, и вообще всю информацию. Telnet работает по 23 порту протокола TCP (TCP-23).

Недостатки протокола Telnet устраняет протокол SSH (Secure Shell). Так же как и Telnet позволяет выполнять команды на удаленном компьютере, но абсолютно всю информацию передает по зашифрованным каналам связи. SSH работает по 22 порту TCP (TCP-22).

DNS – Domain Name System (Domain Name Service) позволяет присваивать узлам а точнее IP-адресам иерархические символьные имена (google.ru, downloads.microsoft.com) FQDN – Fully Qualified Domain Name (Полностью определенное доменное имя). На транспортном уровне протокол DNS использует 53-й порт протокола TCP и UDP (TCP-53/UDP-53).

NetBIOS – это набор протоколов, в частности он включает протоколы для разрешения имен. В отличие от DNS, NetBIOS использует плоские имена (без какой-либо иерархии). Такие имена часто используют в LAN. Кроме плоского именования NetBIOS также позволяет использовать файловую систему другого компьютера как свою собственную файловую систему через локальную сеть. NetBIOS, как правило используется в сетях Windows как основной протокол для обмена файлами. Протокол NetBIOS в Unix-системах еще называют SMB (Samba).

Аналогом протокола NetBIOS в Unix-системах является NFS (Network File System). NFS также позволяет файловую систему другого компьютера использовать как локальную файловую систему. NFS и NetBIOS это немаршрутизируемые протоколы, то есть они могут работать только в пределах 1 локальной сети (без выхода в Интернет).

Для обмена файлами также существуют протоколы FTP/TFTP.
FTP (File Transfer Protocol) - протокол передачи файлов. Работает по протоколу TCP-21. FTP может передавать данные как в локальной сети, так и в Интернете.
TFTP (Trivial File Transfer Protocol) – простой протокол передачи файлов. Работает по протоколу UDP порт 67. TFTP как правило используется только в локальных сетях и предназначен для передачи образов операционных систем, резервных копий конфигураций и т.д.. При установки или загрузке Операционной Системе через сеть, передача файлов ОС производится именно по протоколу TFTP.

HTTP (Hyper-Text Transfer Protocol) – это протокол для передачи гипертекста. Используется для общения браузера с WEB-сервером. Работает по протоколу TCP-80 (протокол TCP 80-й порт).
HTTPS (HTTP Secure). В отличие от протокола HTTP, который передает данные в открытом виде, HTTPS шифрует передаваемые данные при помощи протоколов SSL/TLS. SSL - Sequre Socket Layer/Transport Layer Security. HTTPS работает по 443-му порту протокола TCP (TCP-443).
Протоколы SSL/TLS также могут использоваться для шифрования почтовых сообщений.

DHCP - Dynamic Host Configuration Protocol (Протокол Динамической Настройки Узлов) **UDP-67,UDP-68;**
Bootp - старая версия DHCP**;**
Telnet - это протокол удаленного управления, который позволяет выполнять команды на удаленном компьютере через LAN или Internet; **TCP-23**

SSH - Secure Shell **TCP-22**

DNS - Domain Name System (Service) google.ru, downloads.microsoft.com.
FQDN - Fully Qualified Domain Name (Полностью определенное доменное имя) **TCP-53/UDP-53**

NetBIOS - это набор протоколов, в частности он включает протоколы для разрешение имен. В отличие от DNS, NetBIOS использует плоские имена, такие имена часто используют в LAN; Windows
SMB - Samba
NFS - Network File System
NFS и NetBIOS - это немаршрутизируемые протоколы, т.е., они могут работать только в пределах одной локальной сети (без выхода в Интернет).
FTP/TFTP:
File Transfer Protocol - Протокол передачи файлов. **TCP-21**
Trivial File Transfer Protocol - Простой протокол передачи файлов. **UDP-67;**

HTTP - Hyper-Text Transfer Protocol (Протокол передачи гиппертекста) **TCP-80.**
HTTPS - HTTP Secure. SSL/TLS - Sequre Socket Layer/Transport Layer Security. **TCP-443.**

Почтовые протоколы

К ним относятся SMTP, POPv3, IMAPv4. (v - номер версии протоколов).

SMTP (Simple Mail transfer Protocol) — простой протокол передачи почты. Работает по 25-му порту протокола TCP и используется как почтовыми клиентами, так и и почтовыми серверами для отправки почтовых сообщений.
Протоколы POP-3 и IMAP-4 используются для получения писем с почтового ящика на сервере на локальную машину. Эту задачу выполняет почтовый клиент. (Mozila Tunder Bold…).
Popv3- Post Office Protocol. Выполняет синхронизацию с почтовым ящиком на сервере с определенным интервалом (как правило в 20 минут). Ориентирован на работу по медленному соединению.
При наличии быстрого соединения лучше использовать IMAPv4 (Internet message Access Protocol) — протокол доступа к Интернет-сообщениям. Получает письма с сервера мгновенно при их поступлении.

NTP- Network Time Protocol. Предназначен для синхронизации времени с выделенным сервером.

SNMP – Simple Network Menagment Protocol (Простой протокол управления сетью).

SMTP/POPv3/IMAPv4
SMTP - Simple Mail Transfer Protocol (Простой протокол передачи почты) **TCP-25;**
POPv3 - Post Office Protocol
IMAPv4 - Internet Message Access Protocol

SNMP - Simple Network Management Protocol

Протоколы транспортного уровня

На транспортном уровне работают всего 2 основных протокола: TCP и UDP.

TCP – Transmission Control Protocol и протокол управления передачей. Работает с установлением виртуальных соединений, благодаря чему обеспечивает надежную доставку данных (то есть выполняет обязанности сеансового уровня модели OSI). Но вносит определенную задержку при передаче данных а также тратит определенную часть пропускной способности на контроль доставки данных. Протокол TCP используется для передачи данных, чувствительных к потерям. Это, как правило, файлы. Протокол TCP описан в нормативном документе RFC-793.

UDP (User Datagram Protocol)– протокол пользовательских датаграмм работает без установления виртуальных соединений и поэтому не обеспечивает никакой надежности доставки данных, но лучше подходит для передачи трафика реального времени (аудио или видео). Описан в нормативном документе RFC-768. Основной задачей протоколов транспортного уровня как TCP, так и UDP является доставка данных до приложения в пределах узла. Для этого как TCP, так и UDP использует номера портов.
Порт — это число длиной 2 байта, означающее номер приложения, прослушевающего сеть. Всего портов 65536. Номер порта это своего рода адрес приложения в пределах узла. Номера портов с 0 по 1023 еще называют Well known ports или общеизвестные порты. Эти порты используют стандартные приложения (Web-сервер, SSH-сервер…). Well Known Ports или общеизвестные порты всегда можно найти в файле C:\Windows\System32\drivers\etc\services

Протоколы Сетевого уровня

Основным протоколом сетевого уровня является IP (Internet Protocol) — протокол межсетевого взаимодействия. Главной задачей протокола Ip является доставка данных до узла назначения составной сети. Протокол Ip работает как на оконечных узлах, так и на маршрутизаторах. Протокол IP всегда перенаправляет пакет следующему маршрутизатору, который на 1 шаг ближе к сети назначения, чем отправитель. Для того , чтобы понять на какой интерфейс переслать пакет протокол IP использует таблицу маршрутизаций. Таблица маршрутизаций есть как на оконечных узлах, так и на маршрутизаторе. Если протокол IP не знает какому следующему маршрутизатору переслать пакет, он отправляет его на маршрут по умолчанию (default route). Протокол IP Описан в нормативном документе RFC-791. Протокол IP и в коем образе не может обходиться без протокола ARP (Address Resolution Protocol) Протокол разрешения адресов.
Протокол ARP по указанному IP-адресу находит MAC- адрес узла. Этот MAC- адрес вкладывается в заголовок Ethernet-кадра, а затем используется коммутатором чтобы переслать этот кадр на соответствующий порт. Протокол ARP работает только в пределах одной локальной сети(в пределах одного широковещательного домена). Протокол ARP описан в RFC-826. Протокол ARP для поиска MAC-адресов использует широковещательные сообщения (Broadcast Message). В любой ОС также есть ARP-кэш, который хранит недавно найденные MAC-адреса. В операционной системе Windows время жизни записи ARP-кэша составляет 2 минуты. Если за эти 2 минуты к записи не было ни единого обращения, она удаляется. Отобразить ARP-кэш можно командой arp -a.
arp -d очищает кэш.

ICMP – Internet Control Message Protocol (Протокол межсетевых управляющих сообщениях). Описан в RFC-792 и предназначен для диагностики сети и отправки сообщений об ошибках.

Команды ping и tracert используют I7P сообщения.

Протоколы маршрутизации

К ним относятся
RIP (Routing Information Protocol) - Протокол передачи маршрутной информации.
IGRP (Internet Gateway Routing Protocol).
EIGRP (Extended IGRP).
OSPF (Open Shortest Path First).

Существует ошибочное мнение, о том что протоколы маршрутизации перенаправляют пакеты до узла назначения. На самом деле, это не так. Протоколы маршрутизации лишь исследуют топологии сети при помощи служебных сообщений и строят маршрутную таблицу на каждом маршрутизаторе, а протокол IP лишь использует это таблицу маршрутизации для того, чтобы переслать пакет на нужный интерфейс. Команда route print показывает таблицу маршрутизации.

Форматы PDU

Ethernet Frame (Формат Ethernet-кадра)

Заголовок состоит из 3-х полей:

1) DestinationMAC
2) Source MAC
3) Protocol
4) Data-Link
DstMAC – MAC-адрес получателя.
SrcMAC – MAC-адрес отправителя.
Protocol - тип протокола верхнего уровня. Занимает 2 байта. 0X800 означает Протокол IP. То есть в поле данных Ethernet–кадра вложен IP-пакет.

Формат IP-пакета

Version – версия протокола, всегда 4; **4 бита**

IHL - Internet Header Length; Содержит размер IP-заголовка в двойных словах (двойное слово 4 байта). Минимально возможная длина IP-заголовка, включающего в себя лишь обязательные поля составляет 20 байт. Следовательно, поле IHL, как правило, содержит значение 5. **4 бита**

TOS – Type Of Servervice содержит приоритет трафика. Всего существует 8 уровней приоритета. Это поле никогда не использовалось и не будет использоваться. **8 бит**
TotalLength – это общая длина IP-пакета, включая заголовок и поле данных. Измеряется в байтах. **16 бит**

Максимально возможная длина IP-пакета составляет 64 Килобайта. Но, как правило, в сеть передаются пакеты не больше 1500 байт. Потому что в каждой ОС определен именно такой MTU (Maximum Transfer Unit).

Следующие 3 поля (Identification, Flags, Fragment offset) отвечают за фрагментацию IP-пакета. Фрагментация выполняется в том случае, когда фактический размер пакета превышает MTU сети, через которую его нужно передать.

TTL (Time To Live) содержит время жизнь IP-пакета в так называемых Попах или Прыжках. Это поле по умолчанию содержит значение 64 или 128 в зависимости от операционной системы и декрементируется на каждом промежуточном маршрутизаторе. TTL позволяет избавляться от заблудившихся пакетов. Когда TTL равно 0, протокол IP уничтожает пакет (имеется в виду на каком-то маршрутизаторе).

Protocol – определяет тип протокола верхнего уровня (например: 0x01 — ICMP; 0x06 – TCP; 0x17 – UDP).

Header checksum – это контрольная сумма заголовка, вычисленная по алгоритму CRC-32. Это поле пересчитывается на каждом маршрутизаторе.

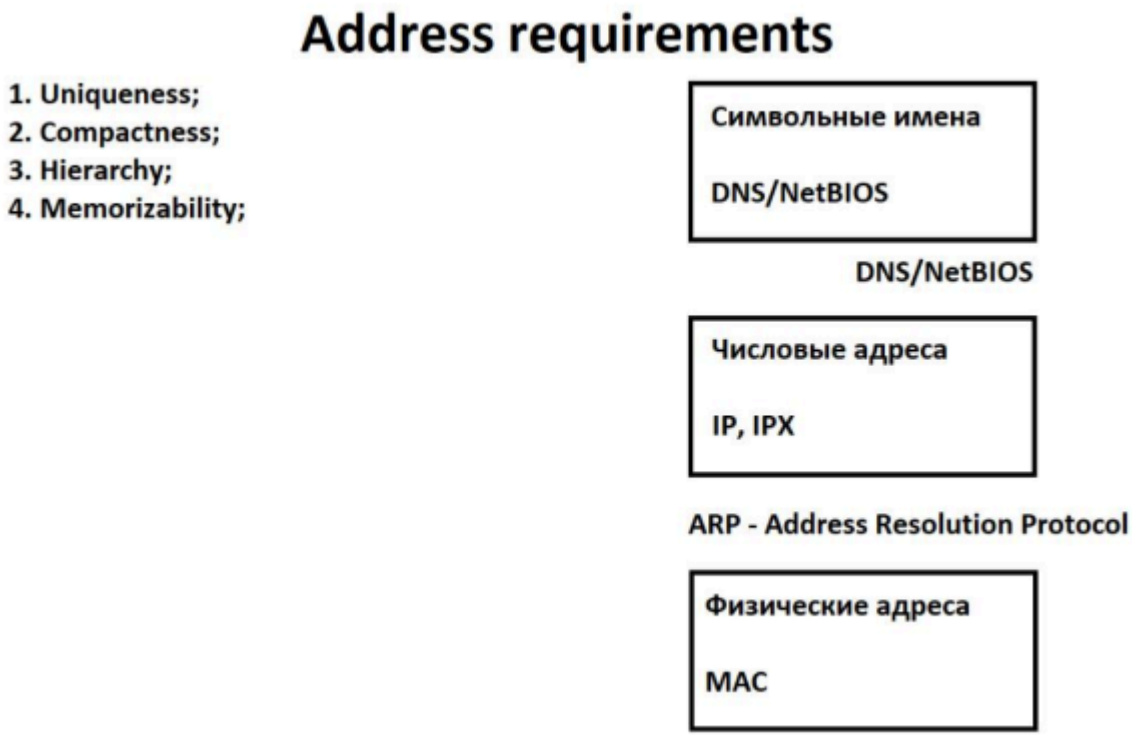
Source Address – это IP-адрес отправителя.
Destanition address – IP-адрес получателя.

Все эти поля являются обязательными. То есть, они всегда есть в любом IP-пакете. Но на этом формат IP-заголовка не заканчивается. У него есть необязательное поле Options.

Адресация

В сетевых технологиях к адресам предъявляется 4 основных требования:
1) Уникальность (Uniqueness) говорит о том, что в сети не может быть 2-х одинаковых адресов. Каждый адрес должен быть уникальным.
2) Компактность (Compactness) говорит о том, что адреса не должны занимать много памяти и чем меньше адрес, тем проще с ним работать. Это приводит к минимальным затратам ресурсов для работы с адресами.
3) Иерархичность (Hierarchy) в адресе должны выделяться различные уровни. (номер сети, номер узла и т.д.)
4) Запоминаемость (Memorizability). Адрес должен легко читаться и легко восприниматься человеком.

Адрес, одновременно отвечающий всем требованиям создать невозможно. Можно создать адрес, отвечающий как минимум 2-м требованиям, иногда 3-м. Поэтому для разных целей было разработано несколько уровней адресации. Всего существует 3 типа адреса:
1) символьные имена. Такие как DNS или же NetBIOS.
2) числовые адреса. Такие как IP, IPX.
3) физические адреса. Такие как MAC.
Каждый из этих адресов используется для решения своих задач и как правило у одного и того же узла сети присутствуют все 3 адреса (как минимум 2 — числовой и физический). Для сопоставления этих адресов используются специальные протоколы. Например, протоколы DNS и NetBIOS сопоставляют символьные имена числовым адресам. А IP-адреса с физическими адресами сопоставляются с ARP (Addess Resolution Protocol).



Физические (MAC) адреса

MAC означает MEdia Access Control (Управление доступом к среде передачи). MAC – адрес представляет собой число длинной 6 байт как правило записанной в 16-ричной системе счисления. Байты при этом разделяются либо дефисами, либо двоеточиями. Старшие 3 байта являются кодом производителя (Manufacturer ID), а младшие 3 байта обозначают серийный номер сетевой карты (Serial Number). MAC- адрес присваивается сетевой карте ее производителем. Он зашивается в BIOS сетевой карты. То есть, если на компьютере будет установлено 5 сетевых карт, то у этого компьютера будет 5 MAC-адресов. MAC-адрес VS Windows всегда можно узнать при помощи команды getmac с ключами / v /fo list. Для проводных сетевых карт драйвер также позволяет изменить MAC-адрес. В Windows это можно сделать через диспетчер устройств. MAC-адреса работают на канальном уровне модели OSI и они видны лишь коммутаторам и лишь в пределах 1 локальной сети. MAC-адреса невозможно использовать для адресации узлов в Итернете. Потому что для этого нужны числовые иерархические адреса. Именно такими являются числовые IP-адреса.