Урок 2

# Физический и канальный уровень. Технология Ethernet. Часть 2

Основные концепции технологии Ethernet. CSMA/CD. MAC - адресация. Формат Ethernet фрейма. Коммутация. Микросегментация. Диагностика канального уровня.

# Введение

На прошлом занятии мы уже начали знакомиться с физическим уровнем модели OSI/ISO на примере технологии Ethernet. Теперь же мы познакомимся с работой Ethernet на канальном уровне. В конце методички также приведен обзор разнообразных, как современных, так и перспективных, а кроме того, некоторых устаревших, но имевшем в прошлом значение технологий, работающих на физическом и канальном уровне модели OSI/ISO (соответственно относящихся к уровню сетевых интерфейсов стека TCP/IP).

В чем разница между физическим и канальным уровнем, зачем нужно такое разделение?

Предположим, что у нас имеется рации. Рации - это устройства физического уровня, настроенные на работу на одном радиоканале, имеющие кнопку или тангенту переключения «прием/передача», то есть работающие в полудуплексном режиме. Все эти вещи характеризуют наши устройства (рации), как устройства физического уровня. Но этого недостаточно, чтобы организовать полноценную связь, понадобятся определенные правила, которые нужно соблюдать.

Прежде всего отметим, что в радиосети находятся несколько абонентов. У каждого из абонентов имеется имя, а то и фамилия, но таким способом именовать по радиоканалу оказывается не удобно. А именовать надо, так как наш канал слышат все из абонентов, и даже если мы отправляем сообщение только одному абоненту, остальные должны иметь возможность определить, нужно ли это сообщение прослушать ( «оно адресовано мне» либо «всем»), или можно спокойно проигнорировать («сообщение не мне»), несмотря на то, что мы его физически слышим.

То есть первая проблема — это проблема адресации. И она решается использованием позывных ( «дуб, дуб, я сосна», «первый-первый, я второй»). Обратите внимание, что у каждого абонента присутствует два имени (два адреса). Одно – его настоящее имя (сравните с именем хоста, hostname), а второе — имя канального уровня, позывной. В разговоре по рации мы можем сказать, «Вася, скажи Пете, пусть уже спускается», «Маша, передай Василию Иванычу, мы задерживаемся», но перед этим мы используем сообщения о своих позывных. Более того, мы можем передать сообщение из нашей радиосети в другую сеть, в этом случае нас позывной конечного адресата не интересует (он может вообще не пользоваться рацией или быть доступен по телефону, то есть маршрут до него значения не имеет), но мы назовем его имя и обратимся к тому, кто может с ним связаться. Точно также обстоит дело и в сетях. Аналогами позывных являются MAC-адреса, за пределами сети (нашего радиоканала) они значения не имеют, равно как MAC-адреса для нас в других сетях. Для идентификации друг друга мы используем MAC-адреса, но для обращения к другим, в том числе и не находящимся в нашей сети мы используем имена (IP-адреса). Прежде чем выходить на связь, нам нужно знать позывные (соответствие имени и позывного, аналогия в сетях: IP-адреса и MAC-адреса). Чтобы передать данные кому-то во вне сети, мы именуем его по имени, а обращаемся к тому, кто может передать. Таким образом нас интересует не позывной адресата (его в сети нет), а позывной того, кто может передать. Также и в компьютерных сетях для передачи данных в другую сеть необходим IP-адрес адресата, а всем машинам, которые хотят передавать данные в другие сети, необходимо знать MAC-адрес шлюза (на практике используется IP-адрес шлюза в настройках TCP/IP соединения, но при передачи данных фигурирует MAC-адрес шлюза. Вот он определяется исходя из IP-адреса, сам IP-адрес шлюза в заголовках сетевого уровня не участвует).

Вторая проблема — организовать работу сети так, чтобы два абонента не пытались говорить одновременно. Когда мы общаемся по рации, мы слушаем, не говорит ли кто в данный момент, а сами начинаем говорить, дождавшись молчания. Каждый сетевой интерфейс тоже слушает канал. Тем не менее, механизм обнаружения коллизий (попытки одновременной передачи сразу двумя узлами) встречаются. Исторически было несколько попыток справиться с этой проблемой. Так в Token Ring кольцевая топология использовалась для передачи данных по кругу (передача

осуществлялась только в одном направлении, out одного устройства подключался к in другого), по очереди устройства передавали друг другу токен – маячок. Только имя маячок устройство передавало, все остальные слушали. Эта идея казалась перспективной, но проиграла историческую гонку технологии Ethernet, показавшей лучшие возможности для масштабирования. В Ethernet используется другой механизм: обнаружения коллизий. В WiFi-стандарте, похожем на Ethernet, и в отличие от «эфирной сети», действительно работающем в эфире, применяется механизм избегания коллизий.

Теперь, разобравшись с аналогией, мы можем посмотреть, как работает канальный уровень на примере Ethernet.

# Канальный уровень

Канальный уровень служит для передачи структурированного набора бит между устройствами, объединенными общей средой передачи данных и находящихся в одной локальной сети (более точно в широковещательном домене, о чем мы сегодня поговорим). Как правило, в одной физической сети (витая пара, оптоволокно, радиоканал на одной и той же частоте), но и возможен логический, «виртуальный вариант», например, в случае туннелирования. В этом случае вместо кодирования через параметры физической среды происходит дальнейшая упаковка, используя протоколы такого же (PPPOE), или вышестоящего (PPTP) уровня.

В модели OSI/ISO канальный уровень по счету – второй, после физического. В модели TCP/IP объединен с физическим под именем «Уровень сетевых интерфейсов». Определенный смысл в этом есть, потому как четкой грани провести между физическим и канальным уровнем невозможно. Например, в структуре кадра протокола Ethernet 802.3 поле преамбулы (самое первое поле, которое, фактически даже не входит в сам кадр) служит для того, чтобы синхронизировать приемник и передатчик, дать на это время, чем и определяется структура преамбулы, которая состоит из семи байт, содержащих одну и ту же битовую последовательность: 10101010. Фактически, она нужна, чтобы сформировать определенную форму сигнала, т.е. идет речь напрямую о физическом уровне. С другой стороны, устройства физического (L1) и канального уровня (L2) значительно отличаются, и если в устройствах L1, как правило, есть только физические соединения (на уровне электрической схемы или порядка подключения патч-кордов в патч-панели), то устройства канального уровня — уже «умные устройства», умеющие анализировать заголовки кадров (фреймов) канального уровня, имеющие реализацию определенного алгоритма, процессор или реализуемую на программируемой логической микросхеме логику и оперативную память. В случае, если все устройства в сети соединены топологией «шина», либо сетевым концентратором (хабом, устройством L1), то устройствами, выполняющими задачи канального уровня, будут сами сетевые карты. В дальнейшем появились сетевые мосты, а потом и сетевые коммутаторы, умеющие анализировать заголовки проходящих через них кадров и принимать решения о направлении в тот или иной порт коммутатора.

Сначала определим, как решается проблема идентификации получателя. Когда несколько устройств соединены шиной или концентратором, сигнал получают все. Если топология шина или звезда с концентратором, то сетевая карта анализирует заголовок канального уровня и определяет, ей предназначено это сообщение или не ей. Если MAC-адрес получателя совпадает с адресом сетевой карты (либо является широковещательным), то кадр принимается и отдаетстя в реализацию сетевого стека операционной системы. Если же нет, то отбрасывается.

## MAC-адрес

MAC расшифровывается как Media Access Control (управление доступом к среде). MAC-адрес или MAC-48 имеет длину 48 бит (6 байт) и иногда называется Hardware Address, аппаратный адрес. MAC-48 один из вариантов аппаратных адресов, используемых для сходных задач. (Другие варианты

EUI-48, EUI-64. Последний используется в FireWire, а также в IPv6). MAC-48 получил широкое распространение, использовался в Token Ring, FDDI, используется в Ethernet, WiFi, WiMAX и т.д.

## Структура MAC-адреса

Задача MAC-адреса – обеспечить уникальную адресацию сетевых интерфейсов устройств, работающих в одной локальной сети (использующих одну и ту же среду передачи данных).

Итак, MAC-адрес состоит из 6 октетов, т.е. из 48 бит, и имеет следующую структуру:


Рисунок 3. Структура MAC-адреса

Первый бит является признаком того, является ли получатель одиночным или данный кадр является широковещательным.

Часто используется широковещательный адрес: FF:FF:FF:FF:FF:FF

Каждый раз, когда срабатывает ARP-запрос, либо протокол DHCP или PPPoE пытается обнаружить сервер, или в других случаях броадкастного запроса, применяется этот адрес.

Существуют и другие варианты широковещательного адреса, например, при мультикастовой адресации. Все подписчики IP-телефонии будут также видеть широковещательный MAC-адрес, если попытаются проанализировать трафик через Wireshark.

Второй бит определяет, будет ли данный адрес глобально уникальным («универсальный») или он назначен локально (т.е. возможны конфликты совпадающих MAC-адресов). Стоит отметить, что и глобально уникальный адрес также можно присвоить сетевой карте во многих случаях, то есть «уникальным» он будет постольку поскольку карте не присвоили новый адрес или адрес сетевой карты не присвоили другому устройству. Отметим, что несмотря на глобальную уникальность, сама уникальность нужна только в рамках локальной сети, чтобы можно было различать соседей по используемому каналу. Хотя идеи с использованием «уникальности» MAC-адреса для сетевой идентификации тоже существовали.

## Каким образом обеспечивается «уникальность»

В случае универсального адреса следующие после первых 2 битов 22 бита – префикс производителя, зарегистрированный в IEEE. Каждый производитель ведет учет выпущенных устройств, добавляя к своему префиксу порядковый номер выпущенного устройства (нечто вроде серийного номера) или сетевого интерфейса. Таким образом мы можем считать, что никакие два устройства либо сетевых интерфейса с универсальными MAC-адресами не будут иметь один и тот же адрес.

00:0c:ad:1d:ab:11 – пример локально администрируемого адреса.

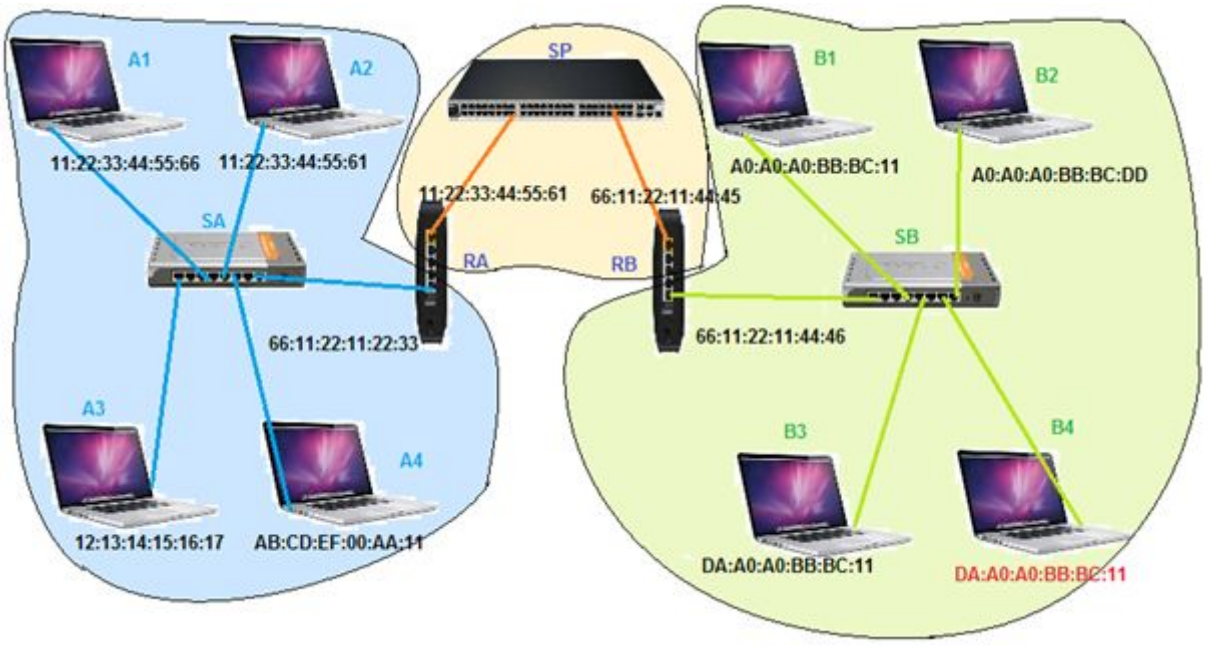
Локально администрируемые адреса выделяются для виртуальных сетевых интерфейсов (виртуальные машины, тоннели), хотя у сетевого интерфейса можно поменять прошитый заводской MAC-адрес на необходимый.

Домашние роутеры позволяют на внешнем интерфейсе (Uplink) поднимать (клонировать, привязывать) MAC-адрес сетевого интерфейса компьютера в локальной сети. Такое может понадобиться, если провайдер идентифицирует Ваш аккаунт (для биллинга, контроля трафика и журналирования) по MAC-адресу компьютера. Используя клонирование MAC-адреса, можно подключить к Интернету уже не один компьютер, а целую локальную сеть, используя домашний роутер.

## Область использования MAC-адреса

MAC-адреса должны быть уникальны среди всех адресов, которые доступны через одну и ту же среду передачи данных.

Обратите внимание на рисунок. Благодаря тому, что интерфейс Вашего компьютера и внешний интерфейс домашнего роутера находятся в разных сетях, конфликта не произойдет. Если же два сетевых интерфейса в одном сегменте будут иметь один и тот же MAC-адрес, произойдет конфликт.




Сети объединяют роутеры (RA и RB), каждый из которых имеет по два сетевых интерфейса (а, стало быть, два MAC. Это не всегда так, есть варианты, когда используется только один MAC-адрес на все устройство, но мы рассмотрим простой пример, где в качестве маршрутизатора применяется обычный домашний роутер либо компьютер с двумя сетевыми картами).

В сети SA (левой) все MAC-адреса уникальны.

В провайдерской сети SP (средней) также все MAC-адреса уникальны.. Несмотря на то, что роутер RA склонировал MAC-адрес компьютера A2 (видимо он был первоначально подключен к провайдеру, почему и была осуществлена привязка через его MAC-адрес), в «среднем» сегменте также все MAC-адреса уникальны.

В сети SB (правой) имеются два компьютера (B3 и B4) с неуникальными MAC-адресами. Конфликт MAC-адресов приведет к ошибкам в работе.

### Можно ли забанить по MAC-адресу

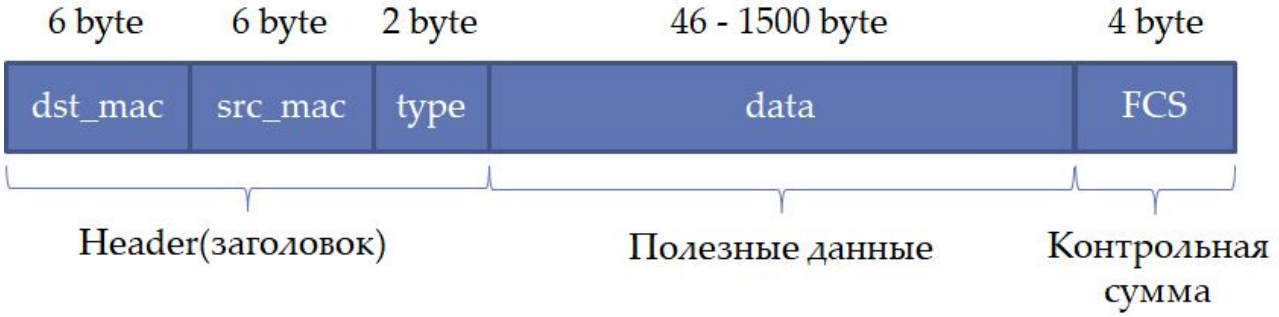
**Ответьте на вопрос.** Имеется форум. На форму злоумышленник повадился писать назойливый спам (легкий заработок, умерла тетя в Зимбабве и т.д.). Можно ли его забанить по MAC-адресу. В каких случаях.

Вариант «MAC-адрес можно сменить» в качестве корректного ответа не подойдет. Если злоумышленник работает в другой сети, мы будем видеть в приходящих кадрах в качестве MAC-адреса отправителя MAC своего шлюза доступа. Если кто-то попытается забанить злоумышленника таким образом, пожелаем ему удачи.

Если же злоумышленник работает в той же сети (если форум работает на сервере в домашней сети, и злоумышленник находится в соседнем подъезде, то есть доступен не через шлюз, либо сервер находится в серверной, и злоумышленник – сосед по серверному шкафу), то в заголовках кадра мы действительно будем видеть MAC-адрес сетевой карты (или назначенный вручную) злоумышленника. В этом случае бан по MAC-адресу технически действительно возможен.

## Формат Ethernet-кадра

На канальном уровне Ethernet-кадр выглядит следующим образом:




Первые 6 байт – MAC-адрес получателя.

Вторые 6 байт – MAC-адрес отправителя.

Следующие 2 байта — тип протокола вышестоящего уровня (предназначен для того, чтобы оборудование или операционная система могла понять, какой протокол инкапсулируется. ARP, IPX, IPv4, IPv6, MPLS и т.д. и т.п.)

Полезные данные могут иметь длину от 46 до 1500 байт. Размер данных меньшего размера не позволит эффективно посчитать контрольную сумму. Размер больше чем 46 и меньше 1500 байт был выбран исходя из особенностей работы через общую среду. Если размер данных меньше 46, такой кадр пройдет через сеть быстрее, чем успеет распространится коллизия (что создает ряд сложностей). Размер более 1500 байт напротив займет канал, не давая возможность другим узлам также отправить сообщение. В высокоскоростных сетях (как правило, при использовании оптических каналов связи) полезные данные могут быть больше, чем 1500 байт. В IPv6 такие фреймы называются jumbo-frame. На практике все еще часто используется 100 Мбит Ethernet с длиной полезных данных в 1500 байт. Стоит отметить, что фреймы-карлики (dwarf) с длиной полезной

нагрузки 46 байт иногда встречаются в сети, например, при выключении сетевого оборудования. Иногда вместо 46 может встречаться меньшее значение, например, 42, это связано с вариациями протокола Ethernet, содержащих те или иные дополнительные заголовки ( LLC – Logical Link Control, 802.1Q VLAN и т.п.)

Контрольная сумма служит для определения, были данные повреждены в ходе передачи (из-за помех, наводок и т.д.). Если контрольная сумма не совпадает со вновь посчитанной получателем, кадр отбрасывается. Это единственная услуга, которая касается целостности данных, предоставляемая канальным уровнем. Контроль порядка принятых данных, оповещение о доставке либо недоставке, повторная доставка, сборка последовательностей из принятых сообщений – все эти задачи не выполняются на канальном уровне. (Выполняются на транспортном и лишь совсем чуть-чуть на сетевом). Обратите также внимание, что контрольная сумма рассчитывается каждый раз в своей сети, то есть ничего не говорит о том, были ли повреждены данные на других участках маршрута (в других сетях). Контроль целостности самих данных, чтобы они пришли к конечному получателю от изначального отправителя, тоже не входит в задачи канального уровня.

## MTU (Maximum Transmission Unit)

В выводе ifconfig в UNIX-подобных системах можно видеть параметр MTU. На самом деле MTU является свойством любого сетевого интерфейса и означает размер полезной нагрузки кадра. Сообщение больше, чем MTU, не может быть передано одним кадром. У разных канальных технологий MTU разное. Традиционное значение для Ethernet – 1500. Для туннелирующих технологий MTU должно быть установлено меньше, чем MTU сетевого устройства, через которое данные будут передаваться физически с учетом туннелируемых заголовков.

```
user@lvm-virtual-macshine:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:1f:6b:1a
          inet addr:192.168.116.140  Bcast:192.168.116.255  Mask:255.255.255.0
          inet6 addr: fe80::bb62:f277:31cd:d92a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:737409 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3774151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:109882858 (109.8 MB)  TX bytes:9476988136 (9.4 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:540029 errors:0 dropped:0 overruns:0 frame:0
          TX packets:540029 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:4808782049 (4.8 GB)  TX bytes:4808782049 (4.8 GB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.6  P-t-P:172.16.0.5  Mask:255.255.255.255
          inet6 addr: 2002:b9c3:1ba4:cafe::1000/64 Scope:Global
          inet6 addr: fe80::6286:fa36:73dd:52d8/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1420  Metric:1
          RX packets:4756 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6234 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:3124862 (3.1 MB)  TX bytes:773195 (773.1 KB)
```

# CSMA/CD

Технология Ethernet базируется на методе управления доступом называемым CSMA/CD (Carrier Sense Multiply Access with Collision Detection) — это означает множественный доступ с контролем несущей и обнаружением коллизий. Коллизией называют столкновение информационных передач, таким образом устройства в сети постоянно прослушивают эфир и останавливают любую передачу в случае детектирования коллизий.

Каким образом осуществляется работа данного механизма?

Устройство прослушивает несущую частоту. Если обнаруживается несущая частота, следовательно, ни один из передатчиков не модулирует сигнал, значит, канал свободен. Когда узел начинает передавать информацию, он одновременно проверяет сигнал на проводнике, в который осуществляется передача. Если сигнал не совпадает, значит, кто-то другой тоже пытается передать сигнал, обнаружена коллизия (кстати, тот же способ при отсутствии коллизий позволяет в Гигабит Ethernet и выше использовать один проводник в полнодуплексном режиме. Если коллизий нет, благодаря использованию коммутаторов, мы можем отправлять сигнал в канал и вычислять разницу между сигналом, поступившим в канал и отправленным. Это будет принятый сигнал. При нескольких абонентах в одной сети, использующих общую разделяемую среду такой метод не работает, так как передать могут и несколько абонентов одновременно, а не только два).

Почему же коллизии возникают, если мы прослушиваем несущую частоту. Из-за низких скоростей в первых версиях Ethernet и задержки сигнала оба узла могли зафиксировать несущую частоту (сигнал еще не дошел) и начать передачу. Коллизия будет обнаружена, когда уже часть данных отправлена.

Если узел обнаруживает коллизию, он перестает отправлять и формирует jam-сигнал — сигнал преднамеренной помехи, призванный информировать другие станции, что возникла коллизия и узлы не должны отправлять. После этого каждым узлом, пытавшимся отправить сообщение, выдерживается псевдослучайной длины пауза, после чего передача возобновляется. Если снова возникнет коллизия, длительность паузы будет увеличена и т.д.

Стоит отметить, что если в  Ethernet используется технология обнаружения коллизии, в WiFi – технология избегания коллизий. Там jam-последовательность отправляется перед передачей и служит сигналом другим, что передавать не надо.

# Концентраторы и коммутаторы

Концентраторы (хабы) реализовали топологию типа “звезда”, но работали на физическом уровне (т.е. с точки зрения работы на канальном уровне хаб не отличается от шины). Задача обнаружения коллизий и определения того, предназначен ли данный кадр данному получателю или нет, возлагался непосредственно на сетевые интерфейсы.

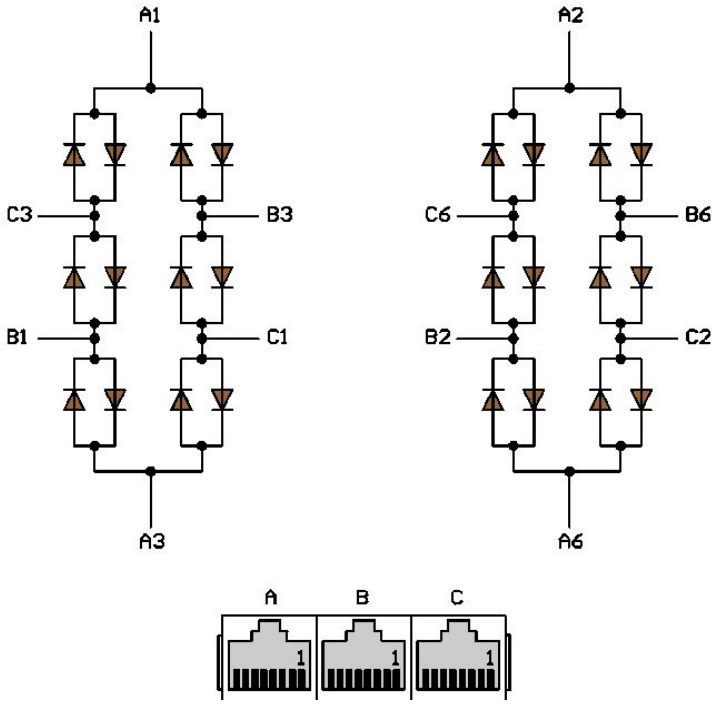
Простейший хаб возможно спаять самостоятельно. Таким образом мы видим, что хаб работает на физическом уровне. Это электронное устройство без программируемой логики.

В обычном состоянии на Ethernet-интерфейсе используется фильтрация пакетов канального уровня и если MAC-адрес в заголовке назначения принятого кадра не совпадает с MAC-адресом текущего сетевого интерфейса и не является широковещательным, то пакет отбрасывается.

Сетевая карта может работать в Promiscuous режиме (неразборчивом режиме). В этом случае будут приниматься все кадры. Это может использоваться злоумышленниками, либо сетевыми инженерами для поиска проблем в сети. Wireshark или tcpdump на компьютере, подключенном к хабу или к шине, с promiscous режимом на сетевой карте будет получать все фреймы, проходящие через данную сеть.

Стоит отметить, что Ethernet-хабы уже практически уже не встретить. Даже самые дешевые коммутаторы, если их и называют хабами, как правило, на самом деле являются простейшими коммутаторы.

Сравним схемы (и внешний вид) концентратора и коммутатора.




Простенький “самодельный” концентратор на диодах. Электрическая схема и фото готового устройства. Более того, устройства на три порта пассивное, не требует даже питания. Работает в half-duplex режиме, 10 Мбит/с.

Источник: http://www.zen22142.zen.co.uk/Circuits/Interface/pethhub.htm


48-портовый коммутатор D-Link DES-3550

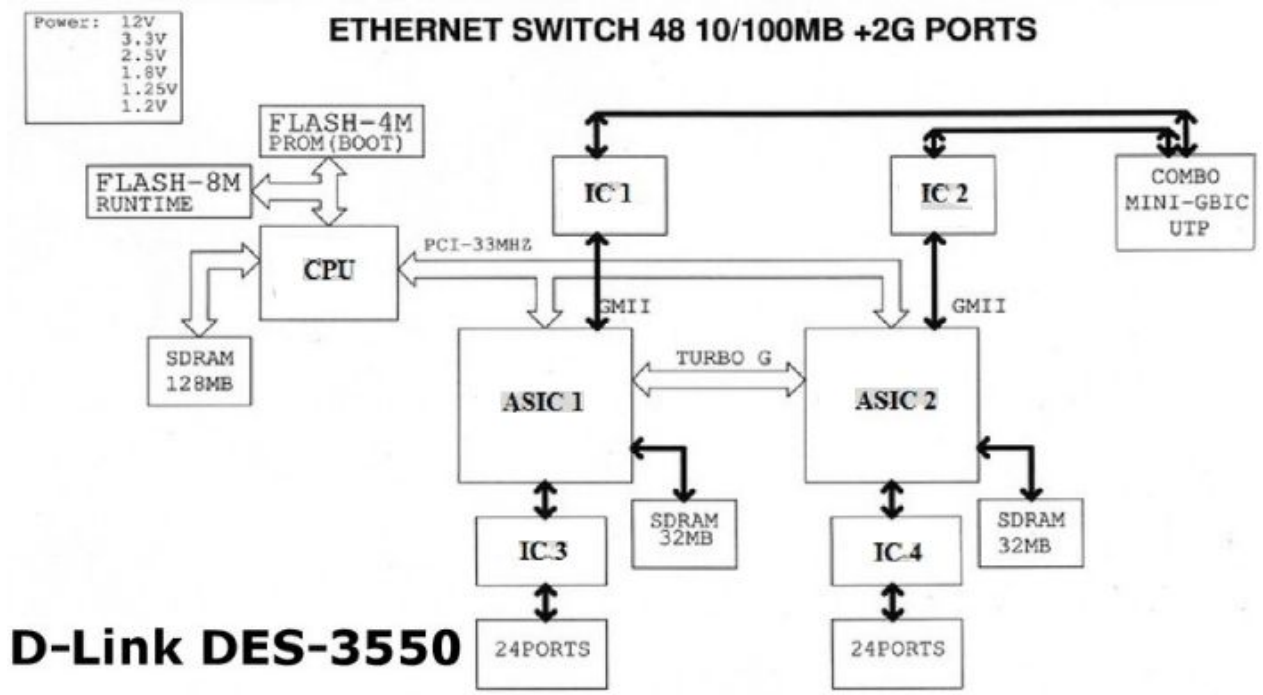



Схема коммутатора D-Link-3550

Устройство и логика работы коммутатора (свитча) совершенно иные, нежели чем у концентратора.

Коммутатор работает на канальном уровне и ведет таблицу соответствий номеров портов и MAC-адресов. Коммутатор самостоятельно с помощью одного паяльника не сделать, даже самый простейший коммутатор реализуется с помощью ПЛИС (программируемые логические интегральные схемы) или процессора, где реализуется алгоритм работы коммутатора, должна присутствовать оперативная память для хранения **таблицы коммутации** – таблицы соответствий MAC-адресов и номеров портов коммутатора и для буфера поступающих кадров.

Стоит отметить, что, как правило, порты коммутатора, в отличие от сетевых интерфейсов, не обладают собственными MAC-адресами (и, тем более, IP-адресами). Работа коммутатора, в целом, прозрачна для отправляющего и принимающего устройств.

При первом получении кадра с MAC-адресом получателя, которого нет в таблице, кадр будет отправлен широковещательно во все порты. После того, как будет получен ответ и можно будет идентифицировать соответствие MAC-адрес и порт, оно будет занесено в таблицу, и последующие кадры последуют в порт коммутатора, к которому подключен получатель непосредственно.

Таким образом решается задача идентификации, как же решается задача предотвращения коллизий?

В случае поступления нескольких фреймов одновременно устройство сможет обработать только один из фреймов, либо должно накапливать фреймы в буфере. В современных коммутаторах буферизация используется тогда, когда порт назначения занят. Буферизация может осуществляться общая на все устройство, либо для каждого порта отдельно, образуя очереди. При буферизации также возможны потери (например, когда буфер достигнет максимально допустимого размера).

С точки зрения физического уровня сегмент является доменом коллизий (верно для случая с концентратором или шиной). Устройствам приходится конкурировать за среду передачи данных.

С точки зрения канального уровня сегмент является широковещательным доменом.

Широковещательные ARP, PPPoE, DHCP-запросы ограничены широковещательным доменом.

Также возможен широковещательный ping, например, ping 192.168.0.255

Не все узлы могут отвечать на широковещательный ICMP-запрос (поэтому надежным способом поиска узлов является не ping 192.168.0.255, а последовательный перебор всех адресов в сети).

Современные коммутаторы не только объединяют домены коллизий, но и обеспечивают промежуточный контроль ошибок. По этому принципу коммутаторы выделяют на Cut-Thru и Store-And-Forward. Коммутаторы Cut-Thru буферизируют только MAC-адрес отправителя и получателя для выполнения коммутации и дальше пересылают сообщение. Кадры с неправильной контрольной суммой, карликовые кадры тоже пересылаются. Коммутаторы Cut--Thru работают быстро, опережая в скорости сетевые мосты, но не могут обработать несколько сообщений, направляемых в один и тот же порт одновременно, либо одновременно принять и отправить сообщение в один порт. Коммутаторы **Store-and-Forward** полностью буферизируют сообщение, и помимо коммутации выполняют проверку, не отправляя поврежденные кадры между сегментами.

## Домен коллизий/широковещательный

Доменом коллизий называют часть сети Ethernet, где все узлы работают с общей разделяемой средой передачи данных, и каждое устройство может создать коллизию в сети с любым другим абонентом этого домена.

Можно сказать, что домен коллизий - это один сегмент сети Ethernet, работающий с общим канальным уровнем (Data Link layer) модели OSI, в котором одновременно осуществить передачу кадра может только один узел. Задержка передачи кадров между узлами или одновременная передача кадров приводит к возникновению коллизий, которые препятствуют передаче кадров, снижают пропускную способность и требуют работы специального алгоритма снижающего вероятность возникновения коллизий в сети. С увеличением числа узлов в сегменте увеличивается вероятность возникновения коллизии. Домены коллизий отделяются между собой сетевыми мостами или коммутаторами.

На практике домен коллизий — это несколько устройств, объединенных топологией шина, либо звезда с концентратором, либо точка-точка (что имеет значение при полудуплексной передаче). В домене коллизий передача одного фрейма заставляет ожидать остальные устройства завершения передачи, либо при попытке одновременной передачи двумя или более узлами приведет к коллизии. Кроме того, в домене коллизии все слышат абсолютно весь трафик.

Широковещательным доменом (сегмент) (англ. broadcast domain) — называют группу доменов коллизий, соединенных с помощью устройств второго уровня. Иными словами, логический участок компьютерной сети, в котором все узлы могут передавать данные друг другу с помощью широковещания на канальном уровне сетевой модели OSI.

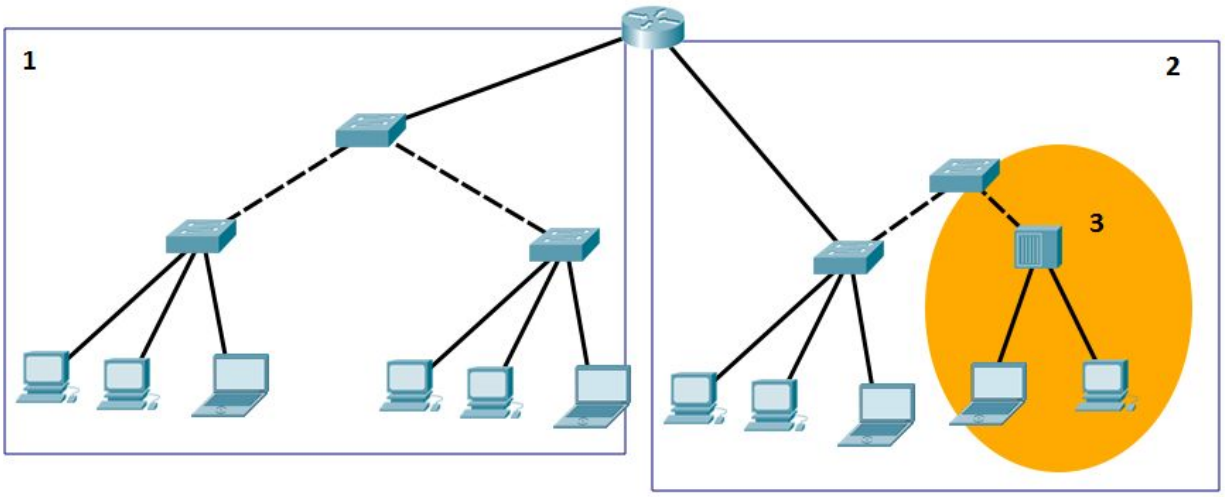
В широковещательном домене несколько доменов коллизий могут вести передачу внутри себя независимо друг от друга. В отличие от домена коллизий в широковещательном домене каждое устройство не слышит весь трафик, но только трафик своего домена коллизий. Тем не менее, широковещательный трафик распространяется по всему домену коллизий.

Чем является участок сети легко обнаружить с помощью Cisco Packet Tracer. Если ICMP-сообщение распространилось по всем узлам, то это домен коллизий. Если же ARP-сообщение распространилось по всем узлам, это широковещательный домен.

С точки зрения модели OSI/ISO домен коллизий является физическим сегментом (L1). Широковещательный домен — логическим сегментом (L2).

Зона 1 и 2 широковещательные домены, границами которых служат интерфейсы маршрутизатора.

Зона 3 – домен коллизий, границей которого является порт коммутатора.




## Чем чреват конфликт MAC-адресов

Если два устройства (B3 и B4) будут иметь один и тот же MAC-адрес, коммутатор будет постоянно перезаписывать таблицу и пытаться отправить кадр широковещательно. При этом кадр может уйти не «тому» получателю.

Кадры будут теряться, скорость падать.

Забегая вперед, отметим, что перед первой отправкой отправителю MAC-адрес не известен. Для его получения широковещательно рассылается ARP-запрос (на MAC-адрес FF:FF:FF:FF:FF:FF).

Существует несколько атак канального уровня, среди которых можно назвать атаки MAC-spoofing, DHCP-spoofing, ARP-spoofing. Рассмотрим пример ARP-spoofing. Ответив на ARP-запрос своим MAC-адресом, злоумышленник может представиться, например, маршрутизатором, и реализовать атаку человек посередине (man in the middle). Для защиты от ARP-спуфинга используют VLAN, access-листы, туннелирование (в частности, PPPoE), IPSEC и статичные ARP.

Локальные компьютеры тоже ведут таблицы соответствия arp (изучите команду arp, доступна и в Windows и в GNU/Linux). Можно фиксировано прописать MAC-адрес маршрутизатора, например, на каждой клиентской машине в сети, если он известен заранее.

## Петля коммутации

Если у нас несколько коммутаторов, к каждым подключено несколько узлов (обратите внимание, все они находятся **в одном сегменте**), то может прийти мысль увеличить надежность, замкнув коммутаторы в кольцо (Или даже выстроить более сложную топологию). Без поддержки протокола STP, в лучшем случае, таблицы коммутатора могут постоянно перезаписываться, а в худшем один кадр может передаваться по кругу… бесконечно, нарушая работу коммутаторов. Такое состояние называется **петля коммутации**.

Алгоритм STP (Spanning Tree Protocol) определяет топологию, в том числе, благодаря обмену между коммутаторами и другим признакам, в результате лишние пути отсекаются. Используются алгоритмы графов для нахождения кратчайшего пути и получения дерева без петель. Если физическая топология — кольцо, то логическая — дерево, позволяющее избежать петель коммутации.

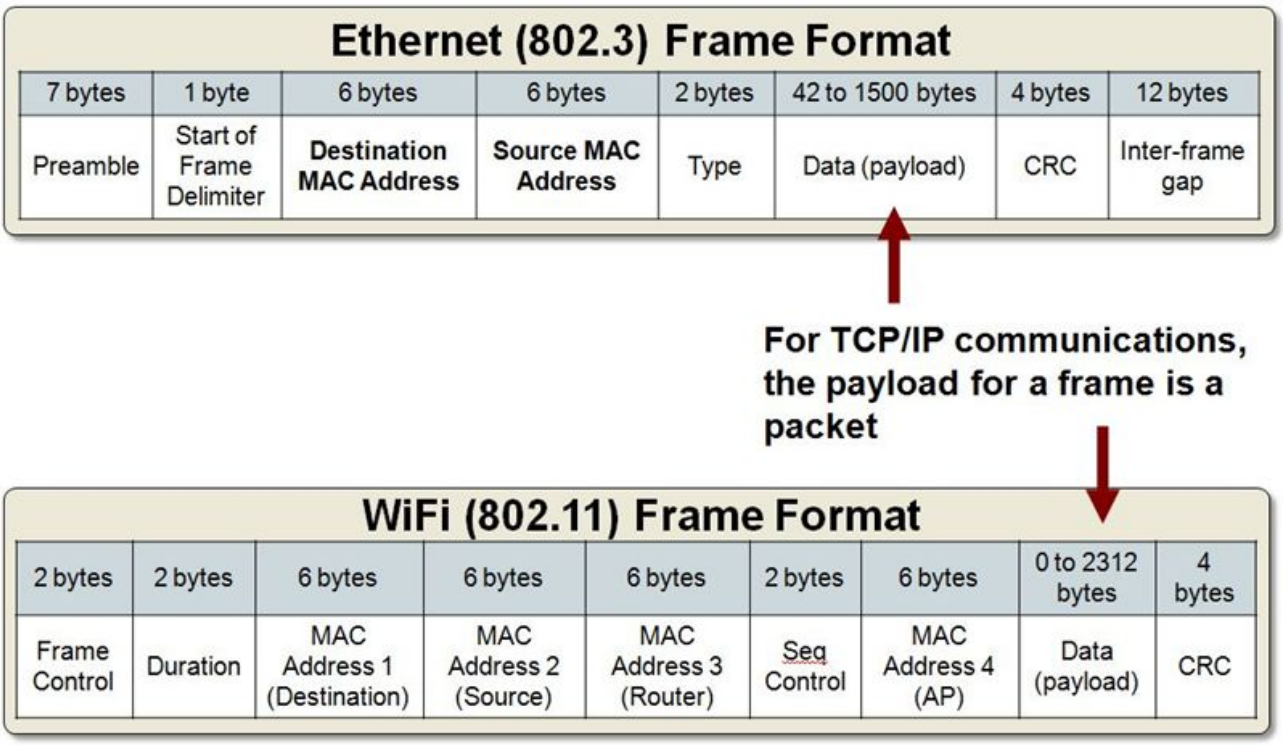
Как же решается вопрос надежности?

В случае нарушения одного из путей, он будет отсечен, а граф перестроен (включится ранее отключенный путь).

## Более подробно о формате Ethernet-кадра

Как правило, когда рассматривают Ethernet-кадр, речь идет только о канальном уровне. На самом деле, Ethernet-кадр содержит и структуры, относящиеся к физическому уровню, к ним относят преамбулу (Preambule), ограничитель начала кадра (Start of Frame Delimiter) и межкадровый интервал (Inter-Frame Gap).

Рассмотрим структуру фрейма стандарта 802.3




Формат фрейма IEEE 802.3 Ethernet. Для сравнения формат фрейма IEEE 802.11

Вначале узел, собираясь начать передачу, передает преамбулу. Семь байт вида: 10101010. На самом деле мы для себя делим эту последовательность на байты, технически это всего лишь последовательность единиц и нулей, призванная сформировать особой формы сигнал, необходимый для синхронизации передатчика и приемника.

Далее следует ограничитель начала кадра. Длиной в один байт (или, как принято говорить, октет) он содержит комбинацию из 8 бит: 10101011 – т.е. ровно на единицу отличается от последовательности преамбулы. Его значение соответствует названию, за ним следует осмысленная информация. Иногда его рассматривают, как часть преамбулы, исторически в протоколах-предшественниках стандарта, восьмой октет действительно был частью преамбулы из 8 октетов. Теперь последний байт логически

выделен в отдельный, наделен особым смыслом, и отличается на единицу от исходного значения. Этот бит, установленный в 1, вместо 0, фактически означает конец преамбулы и начало приема MAC-адреса получателя.

Следующие два поля – кодируют так называемые физические адреса, или MAC-адреса. С ними мы уже познакомились. После могут присутствовать дополнительные поля, в зависимости от используемого протокола канального уровня. В стандартном Ethernet II дополнительных вставок нет, скорее всего и вы не обнаружите их, используя Wireshark в обычном для вашего компьютера трафике.

Следующее поле Длина/Тип протокола.

> Кадры формата 802.3 содержат поле Length вместо привычного нам Type (EtherType). Исторически сложилось, что существует несколько стандартов для кадров Ethernet (помимо перечисленных).
>
> Потом DEC, Intel и Xerox доработали их до универсального красивого решения Ethernet II (Ethernet DIX по первым буквам компаний), которое стало экстремально популярным — IP работает именно поверх него.
>
> Поле Length прежде говорило о общем размере полезной нагрузки, что было в общем-то мало информативно, и тем более такой кадр мог нести только один тип вышестоящего протокола. Значения Length могут быть до 1500 (0x05dc).
>
> В кадре Ethernet II отказались от поля Length и освободившиеся 2 байта использовали под поле Type (EtherType), которое определяет тип вышестоящего протокола. Чтобы чётко отличать их от 802.3 берутся значения, выше 1536 (0x0600).
>
> Так например, если кадр несёт IPv4, то тип будет 0x0800, ARP — 0x0806, VLAN (802.1q) — 0x8100, IPv6 — 0x86DD, QinQ — 0x9100 итд.

Источник: http://pascal.tsu.ru/other/frames.html#as-h4-2325214 via https://habrahabr.ru/post/189268/

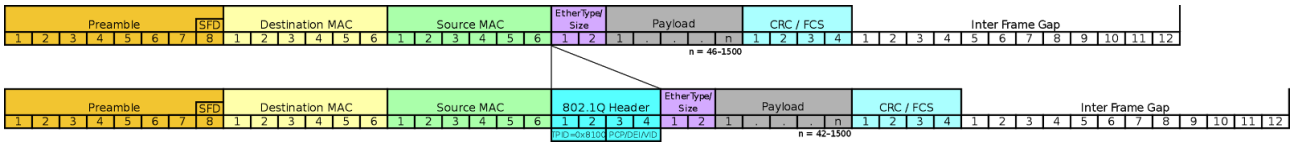
А по адресу https://habrahabr.ru/post/189268/ можно найти ответы на другие каверзные вопросы, касающиеся стека сетевых технологий для собеседований.

Следующее поле – данные. Полезная нагрузка. Как правило, это IPv4-пакет, но не обязательно. Может присутствовать пакет ARP, IPv6, IPX, MPLS.

Замыкает поле контрольной суммы, что служит для контроля за ошибками.

После чего следует межкадровый интервал (Inter-Frame Gap), также часто не упоминаемый в формате кадра канального уровня, так как относится к физическому уровню. Его длина 12 байт и служит он для механизма работы с коллизиями. Эта пауза, необходимая между передачей фреймов для того, чтобы не возникло коллизий.

Разные стандарты 802.3x и 802.X могут содержать дополнительные поля, но общая структура одна и та же.




Пример для 802.1Q, определяющий тегирование трафика для VLAN.

## Микросегментация

В настоящее время концентраторы в технологиях Ethernet практически не встречаются. На протяжении развития Ethernet попытки снизить влияние коллизий привели к созданию мостов, потом коммутаторов, а потом коммутаторов, работающих в full-duplex. Если при использовании half-duplex домен коллизий включает порт устройства, порт коммутатора и соединение между ними, при full-duplex в домене коллизий остается только порт устройства, и, фактически, число коллизий сходит на нет. Это явление называется микросегментацией, а порты устройств - микросегментами.

При этом Ethernet обратно совместим, он будет работать и со старыми стандартами. Все механизмы, такие как CSMA/CD, проверка MAC-адреса на соответствие MAC-адресу получателя, работают до сих пор. Более того, несмотря на то, что топология шина и топология звезда с концентратором ушли в прошлое, влияние тех времен до сих пор значительно в архитектуре Ethernet, и, в особенности, Fast Ethernet, который все еще довольно распространен при подключении провайдерами конечных абонентов.

## Каким образом на той же витой паре мы можем получить вместо 100 Мбит/с Гигабит, а то  и больше

При этом не только переходом на оптоволокно, но и с использованием витой пары.

Конечно, скорость упирается в качество витой пары. На кабеле категории 3 скорость Гигабит/с получить не выйдет, но на 5е уже возможно. При этом скорость во многом определяется не только улучшением характеристик  проводника, но и алгоритмически.

Какие идеи используются в Gigabit, 40Gigabit и т.д.

1) Использованием 4 пар вместо двух. Логичный и простой шаг. При этом кабель кросс уже применяться не должен, только прямой. Прирост – вместо 1 бита мы передаем 2. (2TX вместо 1). Также мы и получаем 2 бита вместо одного (2RX вместо 1)
2) Использование 4 пар одновременно для приема и передачи. Это позволит отправить сразу 4 бита, либо принять 4 бита, но в полудуплексе. Как же сделать дуплекс?
3) Отправляем сигнал и прослушиваем, если сигнал не совпадает, вычисляем разницу. Раньше это использовалось для контроля коллизий, теперь, в условиях микросегментации, еще позволяет поднять нам скорость. Теперь мы можем одновременно отправить 4 бита и еще принять 4 бита. Кстати, в таком случае для нас при измерении скорости единица 1 бод будет равен не 1 бод в секунду, а целых 4.
4) Также мы можем увеличить количество состояний сигнала. Если в компьютерах применяется 0 и 1, на практике в Ethernet применяется большее число состояний.
5) Можно увеличить частоту передачи. Таким образом в единицу времени мы будем передавать еще больше информации.

В результате получаем прирост скоростей в 10, 40, 100 раз.

# Иерархическая модель сети

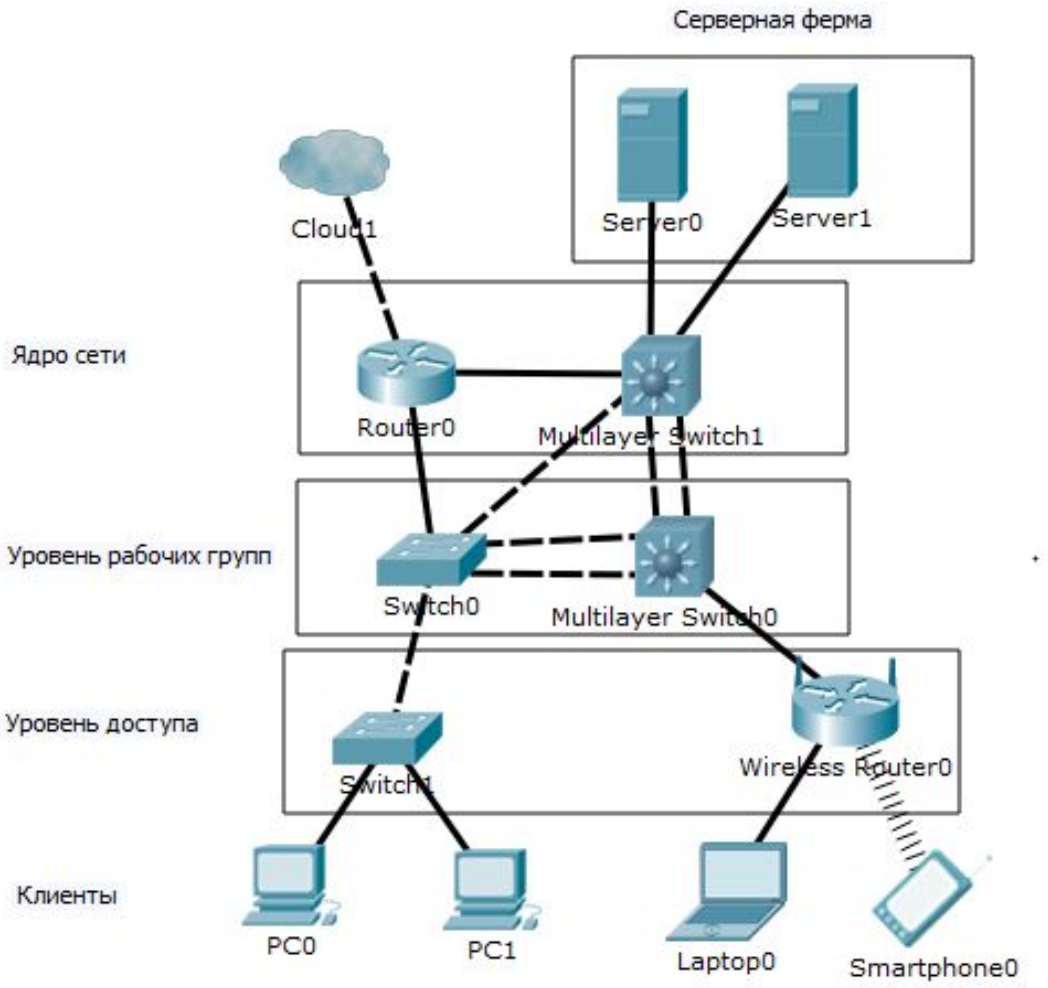
На данный момент широко используется иерархическая модель построения сети. При анализе или проектирование любой локальной сети выделяют 3 уровня. Если сеть небольшая, они могут объединяться, но логически каждый уровень выполняет свои функции.

Уровни модели:

1) уровень сетевого доступа или access layer;

2) уровень агрегации сетевых групп, также называемый уровнем распределения (distribution layer);

3) Уровень сетевого ядра (core layer).




## Уровень сетевого доступа

Уровень сетевого доступа занимается подключением абонентских устройств к сети. Объединяет клиентские устройства в рабочие группы. Основная задача уровня сетевого доступа - это обеспечение пользователя точками доступа к сети. Это могут быть как проводные, так и беспроводные решения. Основные функции выполняемые уровнем доступа:

- управление политиками сети и обеспечение доступа пользователей к ресурсам сети;
- создание отдельных широковещательных доменов (сегментов сети);
- соединение устройств, находящихся в рабочих группах с уровнем агрегации.

Уровень доступа обычно обеспечивается технологиями Wi-Fi и Fast и Gigabit Ethernet. Для уровня доступа сейчас наиболее часто используется скорости 100 и 1000 Мбит/с. Применяются технологии защиты от петель, аутентификации клиентских устройств и политики безопасности. Уровень сетевого доступа должен изолировать сервисы сети от несанкционированного доступа, поэтому вопросам безопасности здесь должно уделяться максимальное внимание.

## Уровень рабочих групп

Уровень агрегации рабочих групп или распределения является промежуточным звеном между ядром сети и уровнем доступа. В небольших сетях он может быть объединен с ядром, а в географически больших сетях этот уровень всегда присутствует. На этом уровне наиболее остро стоят вопросы отказоустойчивости и высокой пропускной способности. На этом уровне выделяют следующие основные функции:

- маршрутизация информации между сегментами сети, обеспечение QoS (заданного качество обслуживания для информационных потоков) и ACL (расширенных листов управления доступом, обеспечивающих безопасность сети);
- агрегация каналов между коммутационным оборудованием;
- использование кольцевых и многосвязных топологий;
- использование оптических высокоскоростных технологий (Gigabit Ethernet/10 Gigabit Ethernet).

## Уровень ядра сети

Уровень сетевого ядра находится в логическом центре и локальной сети. Именно сюда сходятся все информационные потоки, поэтому к ядру сети предъявляются самые высокие требования и вопросы безопасности, отказоустойчивости и высоких скоростей являются наиболее актуальными, потому что отказ незарезервированного оборудования на этом уровне может привести к отказу сетевого сервиса во всей сети и заденет всех абонентов. Примерно 90% сетевого трафика передается через ядро сети. Ядро сети имеет подключения к сети Интернет, а также серверной ферме (сегменту сети, в котором расположено оборудование, предоставляющие локальные сетевые сервисы).

# Справочная информация

## Некоторые сетевые стандарты

Наибольшее распространение получили стандарты семейства IEEE 802.X, разработанные в организации под названием Институт инженеров электротехники и электроники – IEEE (англ. Institute of Electrical and Electronics Engineers):

- IEEE 802.1Q (Ранее 802.10) – Vlan;
- IEEE 802.3 – Ethernet;
- IEEE 802.11 – WiFi;
- IEEE 802.14 – Кабельный широкополосный доступ (сети кабельного телевидения);

- IEEE 802.15.1 – Bluetooth;
- IEEE 802.16 – WiMax.

Но также сюда относятся и такие технологии, как PoE (Power Over Ethernet):

- IEEE 802.3af-2003;
- IEEE 802.3at-2009.

PoE не просто распиновка + и - питания на соответствующие пары, но и алгоритм, контролирующий потребление питающего напряжения и снимающий напряжение в случае отсутствия потребления и перегрузки. В этом случае PoE может использовать те же пары, что и для передачи данных. Также часто используется пассивное PoE (Passive PoE), когда питание просто подается на неиспользуемые пары, с помощью инжектора, а затем разделяется на питание и данные с помощью сплиттера. В пассивном PoE V+ передается по 4 и 5 жилам, V- по 7 и 8.

К слову сказать, этой же организацией разработаны и другие, не менее примечательные стандарты, например:

- IEEE 1003 – POSIX;
- IEEE 1284 – LPT (параллельный интерфейс);
- IEEE 1294 – USB;
- IEEE 1394 – FireWire.

Но есть также стандарты, реализующие протоколы канального уровня, не семейства IEEE 802.X, например:

- ITU G.992.X – асимметричный xDSL;
- ITU G.991.X – симметричный xDSL;
- ITU G.995X – HomePNA;
- FDDI;
- ISDN;
- RFC 1661 – PPP.

## Ethernet (справочная информация)

Ethernet (эзернет, от лат. aether — эфир) — сетевая технология канального уровня, использующаяся в большинстве локальных сетей. Технология осуществляет пакетную коммутацию.

Стандарты Ethernet определяют проводные и оптические соединения и электрические/волновые сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Технология, появившаяся в 70-х годах прошлого века, практически вытеснившая аналогичные сетевые технологии с рынка, на данный момент может быть использована не только для построения локальных, но и в глобальных сетях. Современные телекоммуникационные операторы связи строят свои сети на базе этой технологии. Высокая пропускная способность и надежность современных линий связи, а также дополнительные функции (VLAN / QoS / STP) позволяют данной технологии минимизировать недостатки пакетной коммутации и полностью раскрыть свои возможности для передачи голосового трафика.

Ethernet-технологию описывают стандарты 802.3 IEEE. Первоначальная версия была разработана в 1979 году Робертом Меткалфом. В качестве передающей среды используется коаксиальный кабель (устарело), витая пара (UTP-5cat) или оптоволокно.

Технология характеризуется постоянно установленным соединением.

Скорость потока 10 Мб/сек, 100 Мб/сек, 1 Гб/сек, 10 Гб/сек, 40 Гб/сек, 100 Гб/сек в обе стороны (режим полного дуплекса). Скорость определяется используемым видом стандарта.

## Виды Ethernet

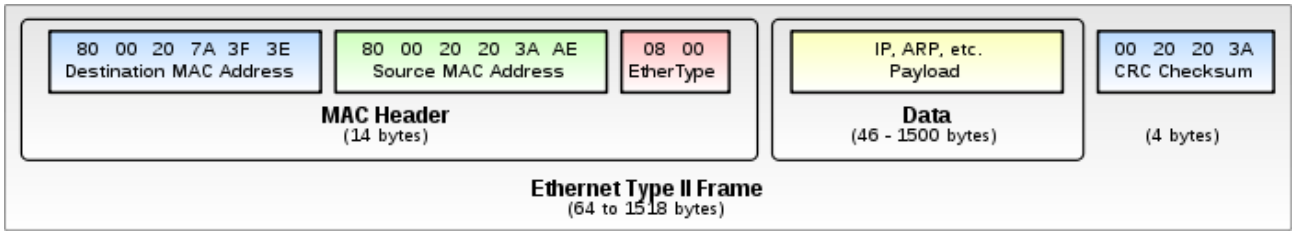
Классификация Ethernet по скорости:

- Ethernet (коаксиал/витая пара/оптика) 10 Мбит/с;
- Fast Ethernet (витая пара 4 жилы/оптика) 100 Мбит/с;
- Gigabit Ethernet (витая пара 8 жил/оптика) 1000 Мбит/с;
- 10 Gigabit Ethernet (витая пара 8 жил/оптика) 10 000 Мбит/с;
- 40 Gigabit Ethernet (оптика) 40 000 Мбит/с;
- 100 Gigabit Ethernet (оптика) 100 000 Мбит/с.

## MAC

MAC-адреса или физические адрес в сети используются для того, чтобы уникально идентифицировать каждое устройство. Сетевые устройства (компьютер, маршрутизатор, принтер и т.д.), которые оборудованы интерфейсом Ethernet, имеют физический адрес. Если бы у них не было адреса, другие устройства не смогли бы передать им информацию. Физический адрес имеет размер 48 бит и выглядит как 12 символов в шестнадцатеричной системе. Первые шесть символов определяют завод изготовитель и задаются согласно стандарту, принятому IEEE, таким образом по физическому адресу можно определить производителя устройства, эта часть данных называется (Organizationally Unique Identifier — OUI). Также определенные вендоры позволяют по mac-адресу определить и модель устройства.

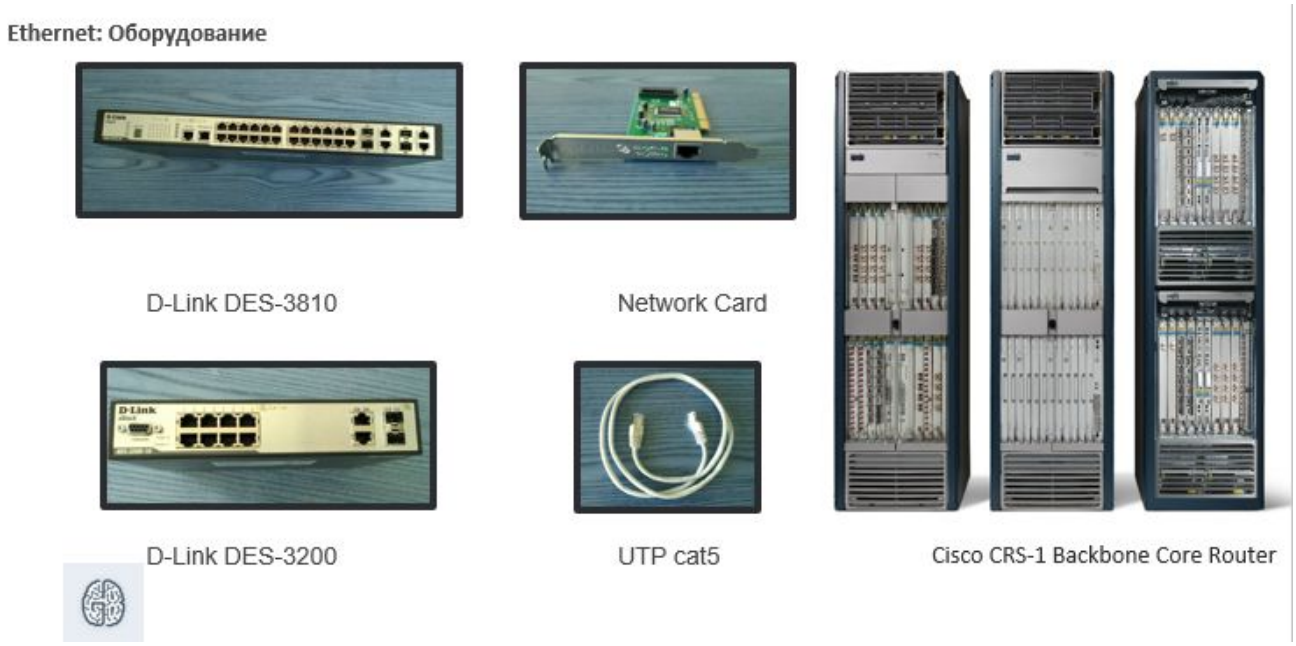

Несмотря на то, что MAC-адрес задается на заводе, существует возможность перепрограммировать MAC-адрес устройства. Поэтому привязка политик безопасности по MAC-адресу не дает гарантированной защиты, также существуют виды атак, позволяющие осуществлять временную подмену MAC-адреса. (Кроме того учтите, что MAC-адреса имеют значения только внутри одной физической сети). На рисунки ниже приведена структура кадра. Каждый кадр начинается с преамбулы. Позволяющий устройствам определить, что далее будет произведена передача кадра, далее идет передача заголовка сообщения (служебных данных), основной информации (поля Data) и завершается кадр суммой, позволяющий определить целостность кадра.




Ethernet-кадр кадр может содержать тег IEEE 802.1Q, для идентификации VLAN к которой он адресован и IEEE 802.1p для указания приоритетности. Виртуальные сети и уровень качества обслуживания помещается в поле EtherType.

### Ethernet-оборудование

В локальных сетях широко применяется технология Ethernet, основное сетевое оборудование, используемое для построения сетей, это сетевые карты, коммутаторы и маршрутизаторы. Также пассивное сетевое оборудование: сетевые розетки, патч корды и линии связи относятся к сетевому оборудованию. На слайде ниже приведены изображения оборудования, которое может быть использовано для построения сети Ethernet.



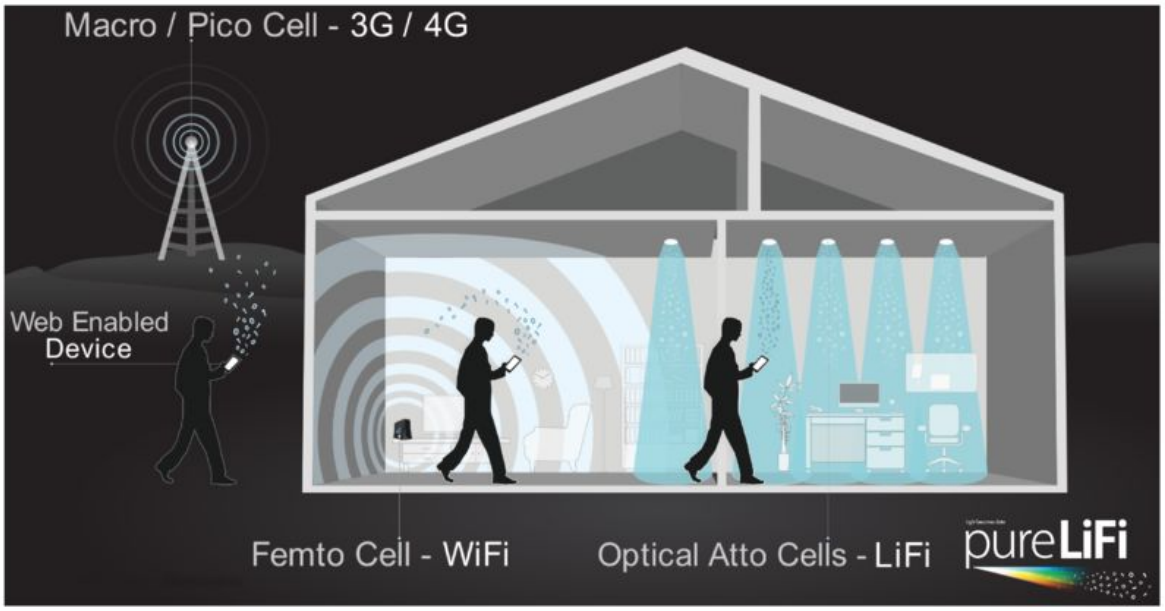

## Возможные конкуренты Ethernet в будущем

Мы подробно рассмотрели основы работы Ethernet на канальном и сетевом уровне.  Но существуют сетевые технологии, которые только развиваются или используются в узкоспециализированных областях (например, в центрах обработках данных для высокоскоростного подключения серверов к дисковым накопителям.) Технология Li-Fi - это один из примеров технологии, которая в скором времени, возможно, будет использована в каждом устройстве.

### Li-Fi

Li-Fi (Light Fidelity) - это сетевая технология канального уровня, осуществляющая двунаправленную, высокоскоростную передачу данных с использованием света.

VLC (Visible Light Communication связь через видимый свет) — сетевая технология, использующая видимый свет и позволяющая светильнику, кроме освещения, передавать информацию. Не любую технологию передачи данных можно назвать VLC (например, оптический телеграф). Обязательно, чтобы человеческий глаз не мог определить факт передачи информации.




Li-Fi может работать с уже существующими светодиодами, которые производятся и продаются сейчас для целей освещения. Однако, возможно, что однажды технология Li-Fi станет популярной и специальные светодиоды, созданные для Li-Fi, станут ключевой областью индустрии по производству светодиодов.

Один из самых больших недостатков Li-Fi – необходимость наличия постоянно включенного света для осуществления соединения. В то время, как это не является проблемой в промышленных масштабах, это проблематично в домашних условиях с практической и экологической точек зрения. Вам придется постоянно держать свет включенным для работы Li-Fi независимо от времени суток.

В ядре iOS замечен код, поддерживающий работу Li-FI.

## Infiniband

Infiniband (иногда сокр. IB) — сетевая технология пакетной передачи, используемая для создания высокоскоростных компьютерных сетей для организации систем, предназначенных для высокопроизводительных вычислениях. Отличительными особенностями являются высокая пропускная способность и минимальная задержка коммутации. Данная технология часто используется для подключения между собой серверов в центрах обработки данных. В 2014 году Infiniband являлась самой используемой сетевой технологией для построения суперкомпьютеров. На данный момент с ней конкурируют высокоскоростные стандарты технологии Ethernet. Сетевые адаптеры Infiniband (host bus adapter) и коммутаторы производятся вендорами Mellanox и Intel. При разработке технологии Infiniband в неё заложили возможность масштабирования сети. Сеть использует иерархическую сетевую топологию на основе коммутаторов, которые называются (Switched fabric).

При построении компьютерных сетей для ЦОД IB конкурирует с Gigabit Ethernet, 10 Gigabit Ethernet, и 40/100 Gigabit Ethernet.

InfiniBand в качестве метода управления средой использует соединение точка-точка, в отличие от первоначальных реализаций Ethernet, использовавших общую шину и разделение среды передачи данных. Передача информационного потока начинается и заканчивается на адаптере канала связи. Все вычислительные узлы содержат HCA-адаптер (host channel adapter хостовой адаптер канала), который подключается к процессору через интерфейс PCI Express. Адаптеры обмениваются данными и управляющей информацией (например для обеспечения QoS).

## Прочие технологии доступа к сети Интернет

Технологии доступа к сети Интернет можно разделить на три категории, в зависимости от используемой среды передачи данных. К ним относятся:

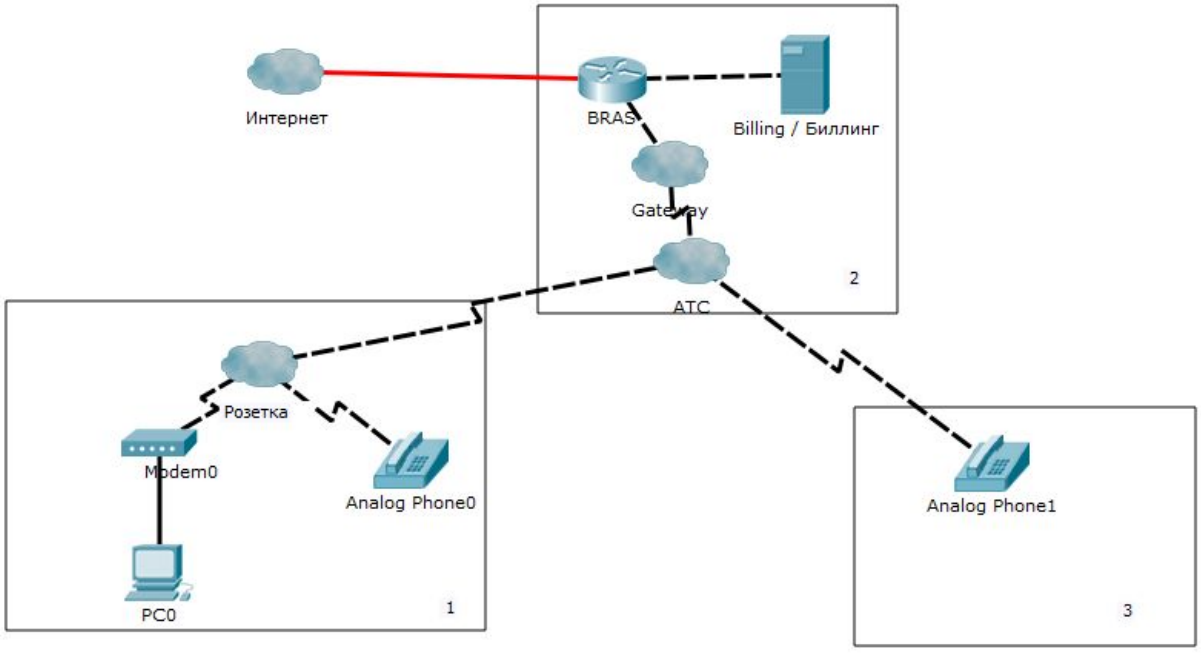
- проводные;
- беспроводные;
- оптические.

Каждый тип среды передачи несет свои плюсы и минусы. Сравнить эти технологии можно по простоте использования, доступным пропускным скоростям, безопасности, надежности, возможностям масштабирования и т.д.

### Dial-up

На данный момент данный сервис практически не используется в России, но, например, в США он до сих пор широко используется. Технология позволяет пользователю, используя компьютер и модем, подключенной к телефонной сети общего пользования (ТФоП), устанавливать соединение с другим компьютером (например, сервером доступа) для создания сеанса передачи данных (создание таких соединение может быть использовано для передачи данных между компьютерами или для доступа к сети Интернет). Обычно dial-up используют для доступа в Интернет или к модемному пулу для подключения к корпоративной сети через протокол PPP. Соединение через модем использует только телефонную сеть общего пользования. На данный момент технология практически не используется в связи с низкой пропускной способностью и занятием телефонного канала.

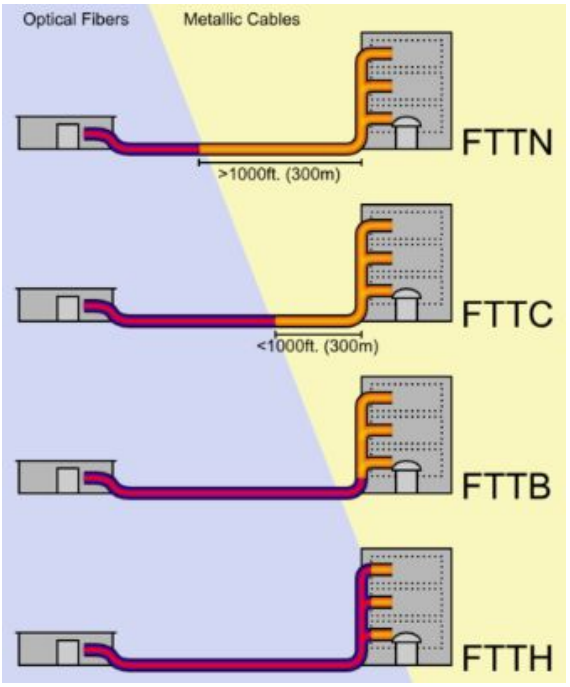
Современные модемы могут обеспечивать скорость до 56 кбит/с (при условии применения протоколов V.90 или V.92). На практике скорость составляет около 40—45 кбит/с. Это связано с низким уровнем качества линий связи.


## FTTX (Ethernet)

Fiber To The X или FTTx (оптическое волокно до точки X) — это общее название для телекоммуникационной сети, которая использует волоконно-оптическую линию связи на части участка последней мили, выполняющей подключение абонента или на протяжении всей линии связи.

Строго говоря, FTTx определяется только над физическим уровнем для передачи данных по оптическом каналу, однако на практике понятие охватывает большое число технологий на канальном уровне. Благодаря широкополосным возможностям системы, FTTx широко используются для предоставления провайдерами сетевых услуг доступа в Интернет, телефонии и кабельного телевидения.




FTTN (Fiber to the Node) — оптическое волокно до сетевого узла. Дальше до потребителей следует витая пара с доступом по Ethernet или xDSL.

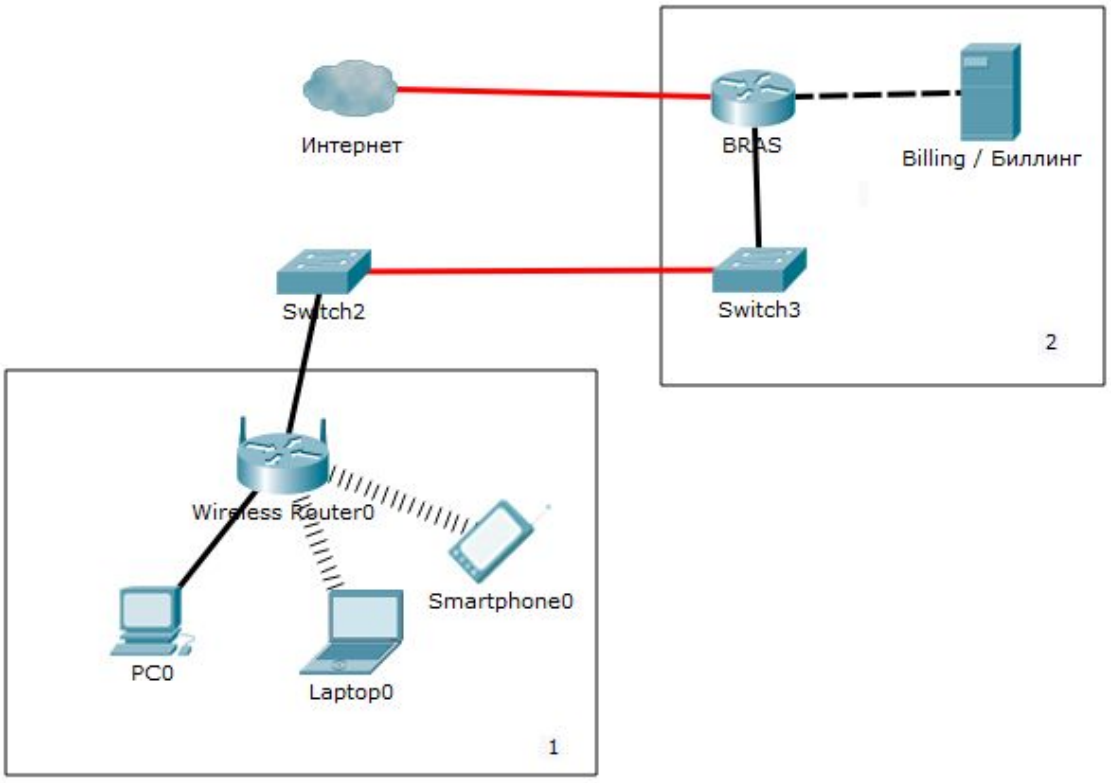
FTTC (Fiber to the Curb) — оптоволокно до группы домов/квартала/микрорайона. Для потребителя доступ организуется с использованием витой пары (Ethernet), WiFi или PLC.

FTTB (Fiber to the Building) — Большинство провайдеров подключают абонентов по технологии FTTB (fiber to the building). Оптическая линия заводится в подвал или на чердак, а к абоненту проводится витая пара, позволяющая выполнить подключение к сети провайдера на скорости до 1000 Мбит/с (но на практике все еще часто используют FastEthernet, таким образом предоставляя не более 100 Мбит/с).

FTTH (Fiber to the home) — оптическое волокно до дома. В квартире или коттедже устанавливается терминальный оптический модем ONU, а от терминала прокладывается обычный проводной кабель до компьютера или Wi-Fi.

FTTD (Fiber to the Desktop) — оптическое волокно непосредственно до рабочего места.

Оптические технологии позволяют использовать не только активные оптические сети на основе Ethernet, но также и пассивные оптические сети, которые будут рассмотрены подробнее в следующем разделе.

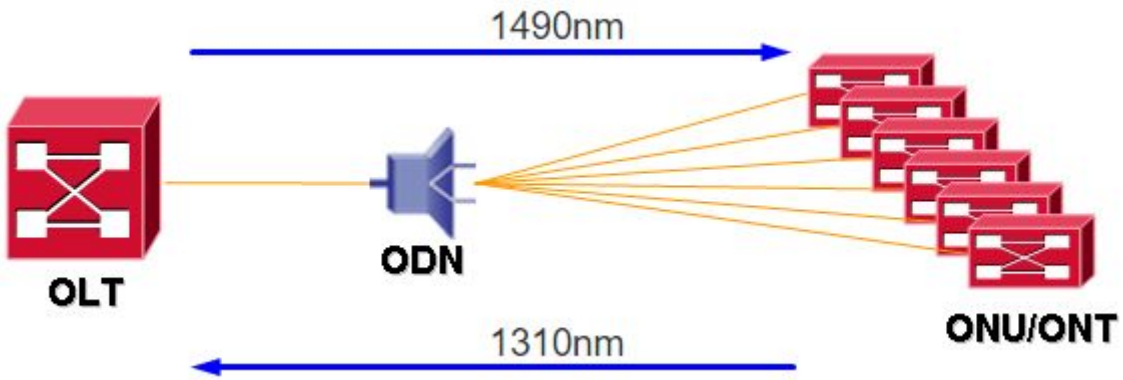



## xPON (GPON)

PON (Passive optical network, пассивная оптическая сеть) — сетевая технология, использующая пассивные оптические сети.

Существует четыре топологии, применяемые для создания оптической сети доступа:

- «кольцевая топология»;
- «соединение точка-точка»;
- «иерархическая топология с активным сетевым оборудованием»;
- «иерархическая топология с сетевым оборудованием».



Пассивная оптическая сеть (PON) доступа в основном строится с применением иерархической волоконно-оптической архитектуры с пассивными сплиттерами, выполняющими демультиплексирование сигнала на высоких скоростях, обеспечивая простое обслуживание и дешевое обслуживание для провайдеров. Архитектура PON позволяет увеличивать количество узлов в сети. Пропускная способность канала может быть увеличена путем замены оптических передатчиков и применения более эффективного спектрального уплотнения по мере роста абонентов. Минусом технологии является отсутствие возможности резервирования оптических линий связи и дорогой монтаж кабельных соединений. Особенность архитектуры оптической сети, заключается в установке у провайдера приёмопередающего модуля, называемого OLT (optical line terminal) и подключения к нему оптических линков, которые расходятся в жилые районы. В узлах коммутации устанавливаются оптические сплиттеры, не требующие питания или обслуживания, которые расшивают пришедшую оптическую линию на абонентские линии, которые уходят к абонентским устройствам ONT (optical network terminal) согласно терминологии ITU-T, или ONU (optical network unit) согласно IEEE.

Преимущества технологии PON:

- промежуточные сетевые узлы не требуют питания или настройки;
- малое количество портов на OLT обеспечивается эффективным мультиплексированием линий связи;
- эффективное использование оптических волокон.

Иерархическая топология точка-много точка предоставляет возможность использовать пере использовать оптические сплиттеры и увеличивать количество портов по мере роста количества абонентов, что значительно снижает расходы на замену оборудования.

Недостаткам технологии PON:

- высокая сложность настройки оборудования технологии PON;
- высокая стоимость OLT устройства;
- нет возможности использования многосвязной топологии для обеспечения резервирования в иерархической топологии.

Количество абонентов, подключаемых к одному модулю OLT, зависит от возможностей и максимальной скорости на одного абонента приёмопередающих портов. Последние стандарты технологии GPON позволяют поддерживать скорость до 10 Гбит/с в направлении DS от сети к пользователю и 2,5 Гбит в направлении US от пользователя к сети, обеспечивая дальность до 25 км. Есть стандарты, обеспечивающие покрытие до 40 км, но скорость на абонента меньше. Стоит понимать, что в качестве абонента может быть не один пользователь, а целый дом.

Современные провайдеры, реализуя PON, подводят оптоволокно до квартиры, вешая в прихожей розетку и (как правило, в аренду) ONT-терминал (Optical Network Terminal) с маршрутизатором, от которого по квартире уже идет либо Fast-Ethernet либо WiFi, таким образом реализуя на практике скорость, не выше все тех же 100 Мбит/с.

Пример PON  в квартире. В прихожей смонтирована PON-розетка, ONT-терминал со встроенным домашним WiFi-маршрутизаторов, розетка для питания ONT-терминала. Через кабель-канал подведено питание к розетке ONT-терминала и Ethernet-кабель для подключения домашнего компьютера. Очень удобно и инновационно.

## HFC, DOCSIS

Гибридные оптико-коаксиальные сети (HFC – Hybrid Fiber Coax). Второй термин Data Over Cable Service Interface Specifications.

Технологии сетевого доступа, использующего в качестве среды передачи коаксиальный кабель (используемый в кабельном телевидение).

Используется телевизионными провайдерами для оказания услуг доступа к сети Интернет, для своих абонентов. Работает по технологии общая шина.

Стандарт DOCSIS 3.1, предоставляет скорость 10 Гбит/с для прямого канала DS и 1 Гбит/с для обратного US.

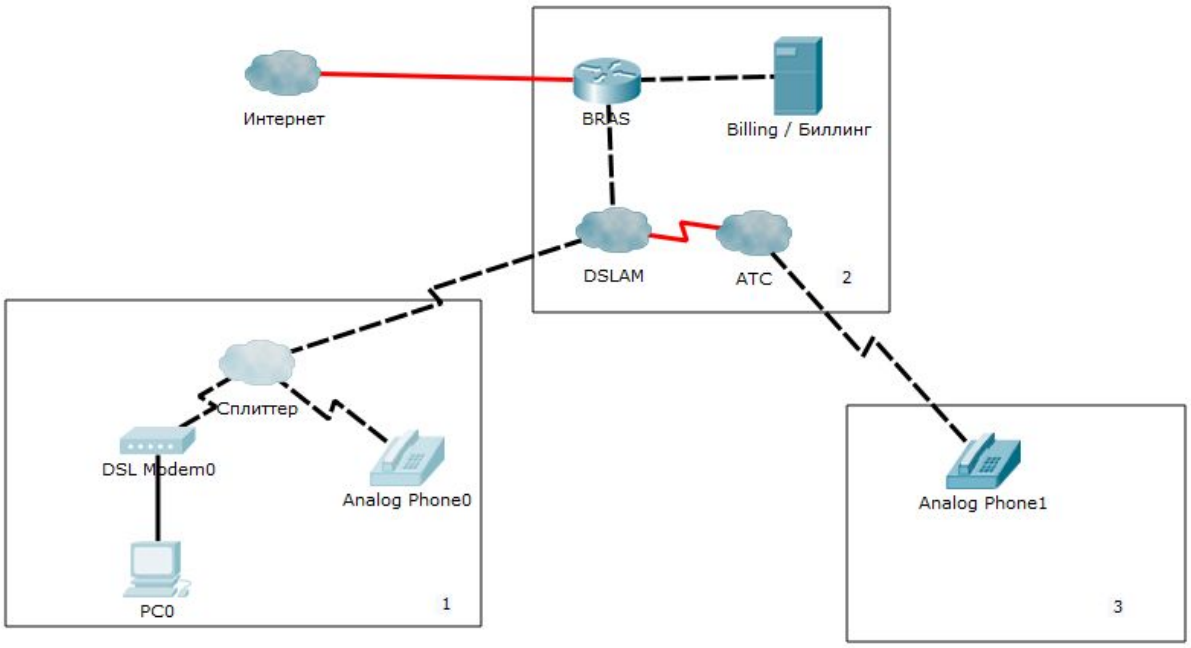
## xDSL

Технология цифровых абонентских линий используют телефонную линию связи, но значительно отличаются от технологии Dial-up. Знак **X** обозначает конкретный стандарт в технологии, а аббревиатура a DSL (digital subscriber line)  цифровую абонентскую линию.

Технология DSL включает в себя целый стек различных стандартов: ADSL, HDSL, IDSL, MSDSL, PDSL, RADSL, SDSL, SHDSL, UADSL, VDSL. Технологии отличаются используемыми алгоритмами,

частотами и, как следствие, максимальной длинной линии связи и скоростью. Все технологии используют обычный телефонный кабель.


Технология DSL разработана для решения определенных задач: они работают на проложенных телефонных линиях и не мешают работе факсимильной или телефонной аппаратуры абонента, скорость передачи данных значительно больше предела для dial-up в 54 Кбит/сек. и даже больше стандартного телефонного канала в 64 кб/с. Также данная технология обеспечивает постоянную связь. Распространение технологии DSL сопровождалось небольшой перестройкой инфраструктуры провайдеров доступа к сети Интернет и провайдеров, осуществляющих подключение к телефонным сетям, так как DSL-оборудование и телефонное работает на одних и тех же линиях связи.




Существуют варианты, когда сторонний провайдер арендует абонентские линии у традиционного оператора телефонии и выполняет подключение абонентов к сети Интернет через в DSLAM.

DSLAM (Digital Subscriber Line Access Multiplexer) — аппаратное устройство, мультиплексор (модем) доступа цифровой абонентской линии xDSL. Фактически, является промежуточным устройством, подобно сплиттеру, у абонента, который разделяет телефонную и сеть передачи данных. Для подключения к сети у него WAN-порты, а для клиента — xDSL-полукомплекты (модемы), к которым подключена телефонная линия. Со стороны абонента устанавливается аналогичный полукомплект xDSL (модем) и сплиттер, к которому подключается телефонный аппарат.

## Важно. Различия ADSL и HDSL.

Стандарт ADSL ITU G.992.1 описывает асимметричную технологию доступа.

Ассиметричный доступ (исходящая скорость значительно ниже входящей) реализуют технологии ADSL, ADSL2, ADSL2+. Это традиционный клиентский доступ, предоставляемый провайдерами большинству абонентов.

Если требуется исходящая скорость соединения при использовании технологии ADSL2+ (ITU G.992.5), можно попробовать включить в настройках ADSL-модема поддержку технологии ITU G.992.5 Annex M: это незначительно повысит исходящую скорость за счет снижения входящей.

Стандарт HDSL ITU G.991.1 описывает высокоскоростную симметричную технологию доступа. Дальнейшее развитие — SHDSL G.991.2

Как правило, такие услуги не предоставляются физическим лицам. Также можно соединить телефонным проводом два HDSL или SHDSL модема, не прибегая к провайдерам, и обеспечить связь на расстоянии до 4,5 км (HDSL) или 7,5 км (SHDSL) что иногда используется в промышленной инфраструктуре.

## PLC

Power Line Communication – или связь через ЛЭП, технология сетевого доступа интегрируемая с Ethernet-сетями. Использует в качестве среды передачи электропроводку и работает по технологии общая шина. Имеет широкое распространение в Японии. Стандарт HomePlug AV предоставляет скорость 500 Мбит/с.

Во время передачи сигнала по бытовой электросети могут возникнуть сильные искажения или затухания сигнала на определенных частотах, что приводит к искажению и потере передаваемой информации, а следовательно, и снижению пропускной способности. Технология PowerLine использует специальный алгоритм для решения данных проблем — мониторинг и динамическое переключение сигнала (dynamically turning off and on data-carrying signals). Идея технологии заключается в специальном алгоритме, в результате которого устройство выполняет прослушивание линии связи с целью детектирования помех. Если система обнаруживает искажения, то автоматически производится переход на другие частоты до улучшения помеховой обстановки.

PowerLine-технология может быть использована при реализации идеи «умного дома», где вся бытовая электроника связана в единую информационную сеть с возможностью централизованного управления.


Устройства продаются парами, но можно купить несколько пар и настроить на работу друг друга (осуществляется нажатием кнопки). Таким образом несколько устройств будут работать по топологии «шина». К достоинствам данной технологии можно отнести легкость создания сети без протягивания кабелей. К недостаткам: помехи в КВ-диапазоне, как от PLC для радиопередач, так и наоборот; нестабильность работы (влияние на качество связь помех и работы бытовых электроприборов), не будет работать, если разные PLC-адаптеры подключены к линиям, имеющим гальваническую развязку (подключены через трансформатор, ИБП и т.д.)

## Wi-Fi

Wi-Fi — торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.


Технология использует частоты 2.4 и 5 ГГц.

Сейчас наиболее популярны стандарты 802.11 g/n/ac, которые предоставляют скорость до 54/600/1300 Мбит/с соответственно.

Радиус покрытия зависит от препятствий и помех и для открытого пространства составляет до 150 метров.

Wi-Fi может быть использован не только для раздачи Интернет дома, но и для подключения конечных абонентов. По всему миру и в крупных городах России доступно большое количество бесплатных точек, где после авторизации через сеть мобильного оператора можно подключиться к сети Интернет. Обычно это крупные аэропорты, вокзалы, музеи и даже парки отдыха. В Москве беспроводной доступ к сети возможен внутри вагонов метро. Железнодорожные поезда планируется в скором времени оборудовать беспроводными точками доступа, а доступ к беспроводной сети во время межконтинентальных перелетов уже давно никого не удивляет, только услуга эта пока платная и связана с тем, что выход в Интернет самого самолета осуществляется через спутниковую связь.

Иногда технологию Wi-FI сравнивают с сотовыми сетями, что не совсем верно, потому что это технологии разного назначения. Если бы телефоны использовали только Wi-Fi, то они имели бы очень малый радиус действия. Поэтому использование Wi-FI обосновано только для локального доступа, а развёртывание крупномасштабных сетей экономически не оправдано. Тем не менее, подобные сети могут быть использованы и в коммерческих целях для осуществления звонков или безлимитного доступа на повышенных скоростях.

Сферы применения:

- кафе;
- магазины;
- аэропорты.

Постановление Правительства РФ от 31 июля 2014 г. N 758 "О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей". Данное постановление обязывает использовать средства идентификации абонентов даже для бесплатных и открытых сетей.

## WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) — сетевая технология, предназначенная для предоставления беспроводных соединений на большие расстояния для различных устройств (от обычных компьютеров или ноутбуков до мобильных телефонов). Технология описывается стандартом IEEE 802.16, который иногда называют Wireless MAN или беспроводные городские сети. Технология является переходной между WiFi и мобильными сетями. Общие принципы совпадают, но отличаются фактические скорости доступа.

## 3G/4G

3G/4G технологии относят к сотовой связи, но кроме предоставления телефонии данные сети предоставляют и широкополосный доступ в сеть Интернет. Название технологии (сотовая связь) происходит из ключевой особенности, которая заключается в том, что зона покрытия сети делится на участки в виде ячеек или сот, также называемых секторами. Каждый сектор работает на своей частоте, таким образом обеспечивается эффективное использование частот. При отсутствие помех (зданий или естественных препятствий) зона сектора – это круг, сектора пересекаются между собой,

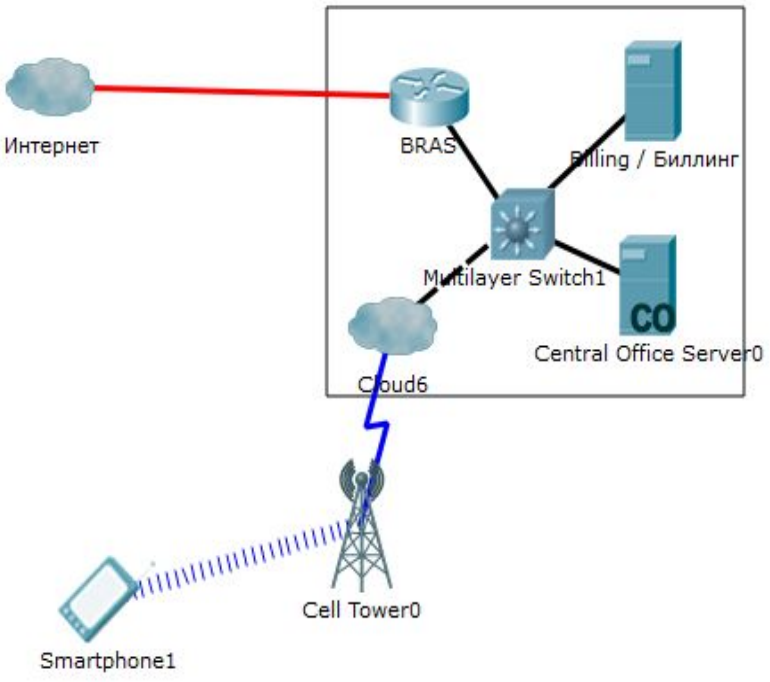
поэтому при движение абонент переключается от точки к точке – это называется роумингом, при этом обрыва связи не происходит, потому что переключением управляет контроллер сети.

3G (third generation или сети третьего поколения), сетевые технологии мобильной связи, обеспечивающие набор услуг, который включает высокоскоростной доступ в сеть Интернет и телефонию, работающую по цифровой радиосвязи. Если говорить о стандартах, то под 3G чаще всего подразумевают стандарт UMTS и его надстройку HSPA, обеспечивающую передачу данных до 42 мбит/с.

4G (fourth generation или сети четвёртого поколения) — сетевые технологии мобильной связи с широкополосным доступом и повышенными требованиями к передаче данным. Под определение сетей 4-го поколения попадают перспективные мобильные сетевые технологии, которые позволяют передавать данные на скоростях свыше 100 Мбит/с для подвижных абонентов и 1 Гбит/с для стационарных абонентов. Разные скорости для стационарных и подвижных абонентов связаны с доплеровским эффектом.

Технологии LTE Advanced (LTE-A) и WiMAX 2 (WMAN-Advanced, IEEE 802.16m) признаны беспроводными стандартами связи четвёртого поколения 4G (Международным союзом электросвязи на конференции в Женеве в 2012 году.

На данный момент идет работа над стандартами 5-го поколения, утверждение которых планируется к 2020 году.



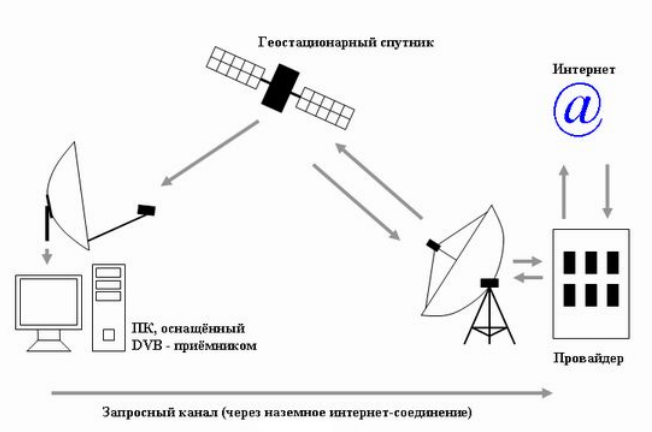

## Спутниковый Интернет

Спутниковый Интернет — это сетевая технология, использующая для доступа в интернет геостационарные спутники.

Спутниковые технологии делят два класса в зависимости от способа обмена данными со спутником:

- односторонний, также называется асимметричный — для передачи данных используется наземное или беспроводное подключение (например, мобильный телефон с низкой пропускной способностью), для отправки запросов, а для получения данных используется спутниковый канал. Таким образом пользователь посылает запрос через мобильную связь на сервер провайдера, провайдер скачивает нужную информацию и осуществляет передачу абоненту через геостационарный спутник.

- двухсторонний, также называется симметричный — абонент использует более дорогое спутниковое оборудование, осуществляющее передачу запроса и получение данных через спутник. Данный тип подключения широко используется для передачи репортажей в прямом эфире (устанавливается на крышу автомобиля и автоматически настраивается на спутник), связи на кораблях или самолетах.



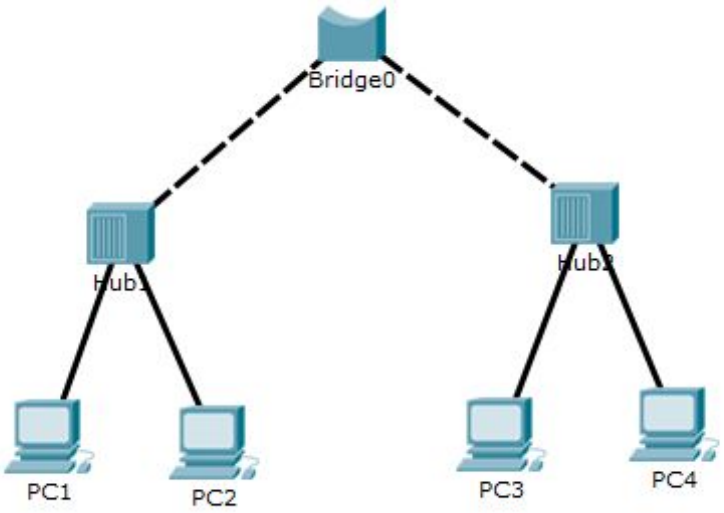

# Сетевые устройства

Мы уже рассматривали некоторые сетевые устройства физического и канального уровня. Рассмотрим еще некоторые.

## Мост

Сетевой мост или бридж (bridge) — активное сетевое устройство второго уровня модели OSI, используемое для соединения двух или нескольких сегментов (подсети) сети. Данное оборудование предназначено для структуризации сети, на данный момент практически не используется. Мост обычно объединял два участка сети, изолируя домены коллизий друг от друга. Устройство принимало кадр, буферизировало его, затем перенаправляла в другой сегмент сети. В результате развития сетевого оборудования и переход на технологию Fast Ethernet появилось многопортовое высокоскоростное (100 Мбит/с) сетевое устройство, аналогичное по функциям сетевому мосту, но которое назвали коммутатором. В настоящее время мосты, как L2-устройства, вытеснены коммутаторами и существуют только в виде программной реализации для объединения виртуальных устройств (виртуальных машин) либо нескольких сетевых интерфейсов в один виртуальный коммутатор (бриджинг).

Построив данную сетевую схему, мы можем посмотреть, как осуществляется передача данных внутри сети при использование концентратора и моста.




## Медиаконвертер (трансивер)

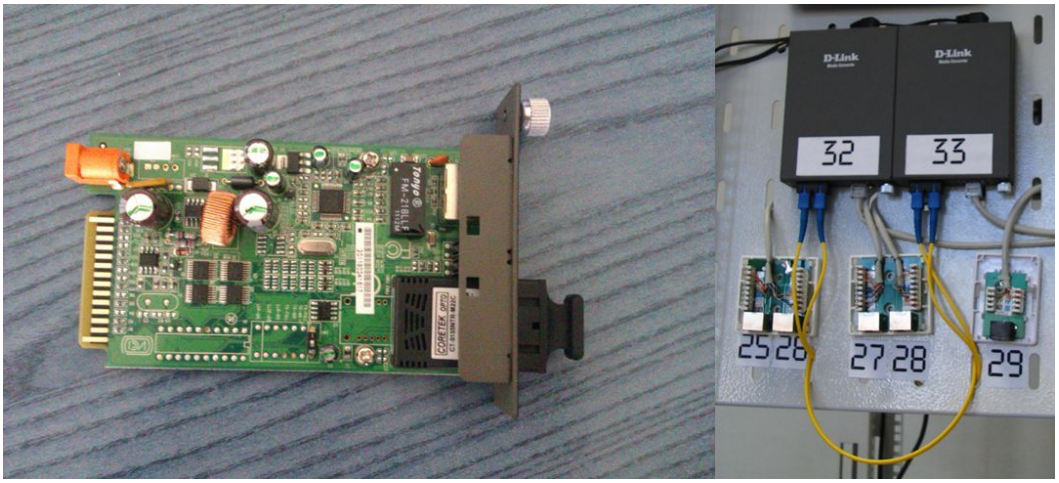
Сетевая инфраструктура обладает гетерогенной структурой, устройства могут быть значительно удалены между собой и в этом случае возникает необходимость применения устройств, которые позволяют перейти от проводных к оптическим технологиям и обратно.

Медиаконвертер – активное сетевое устройство, осуществляющее преобразование сетевого сигнала из одной среды в другую, аналогом данного устройства является беспроводная точка доступа в режиме моста.

Сейчас повсеместно используются медиаконвертеры, до их применения использовались трансиверы, отличием в работе данных устройств является возможность преобразования скорости передаваемых потоков. Например, 100 Мбит/с в 1 Гбит/с. Это осуществляется за счет буферизации кадров.

Продолжением развития медио конвертеров стали SFP/XFP модули, устанавливаемые в специализированные порты в коммутаторах/маршрутизатора/сетевых картах.

Использование отдельных плат оправдано, в связи с тем, что существует много типов оптических коннекторов и 2 типа оптического волокна. Производители оборудования предоставляют администраторам самостоятельно выбрать необходимую конфигурацию.



Оптические медиаконвертеры могут быть установлены в отдельном корпусе как на рисунке справа, так и смонтированы как платы в шасси. Данное активное сетевое устройство не имеет сетевых настроек и относится физическому и канальному уровню модели OSI. По своим функциям аналогично сетевому мосту, но отличается тем, что работает с различными сетевыми средами (оптика/медь).

## Мультиплексоры

Мультиплексор – аппаратное устройство, выполняющее объединение нескольких телекоммуникационных потоков в одну линию передачи связи. Обычно мультиплексоры используют для оптических систем и используют частотное или временное уплотнение.

Обычно применяются оптические мультиплексоры, использующие частотное и временное уплотнение совместно со сплиттерами или демультиплексорами (устройствами делителями).

Применяется в технологиях PDH/SDH/xPON для повышения эффективности использования существующих линий связи путем передачи нескольких потоков по одной линии связи.

## Точка доступа

Беспроводная точка доступа или access point – это беспроводное устройство, аналогичное по своей работе концентратору. Беспроводная точка не использует кабельные соединения для подключения абонентов, но может быть подключена к основной сетевой инфраструктуре посредством кабеля. Часто данное соединение используется также для питания устройство по технологии POE.


Точка доступа является активным сетевым оборудованием и служит для подключения устройств по топологии общая шина. Относится к физическому и канальному уровню модели OSI. Точкой доступа может выступать сетевой адаптер, поддерживающий работу в инфраструктурном режиме. Точка доступа управляет работой клиентов на канальном уровне.

Режимы работы:

- Точка доступа (точка доступа объединяет клиентов и управляет их работой).
- Репитер / повторитель (принимает сигнал от основной точки доступа и усиливает его).
- Шлюз (осуществляет подключение проводного абонента к беспроводной сети в режиме клиента, данный режим может быть использован для устройств, которые необходимо подключить к беспроводной сети, но на которых отсутствует беспроводная сетевая карта, например телевизор или проектор).
- Радио-мост (осуществляет беспроводное соединение между двумя точками доступа, за счет использования направленных антенн может осуществлять передачу сигнала на значительное расстояние).

## Wi-Fi маршрутизатор

Домашнее устройство, называемое ошибочно роутером, является комбайном из точки доступа, коммутатора и маршрутизатора.

Включает в себя или может включать:

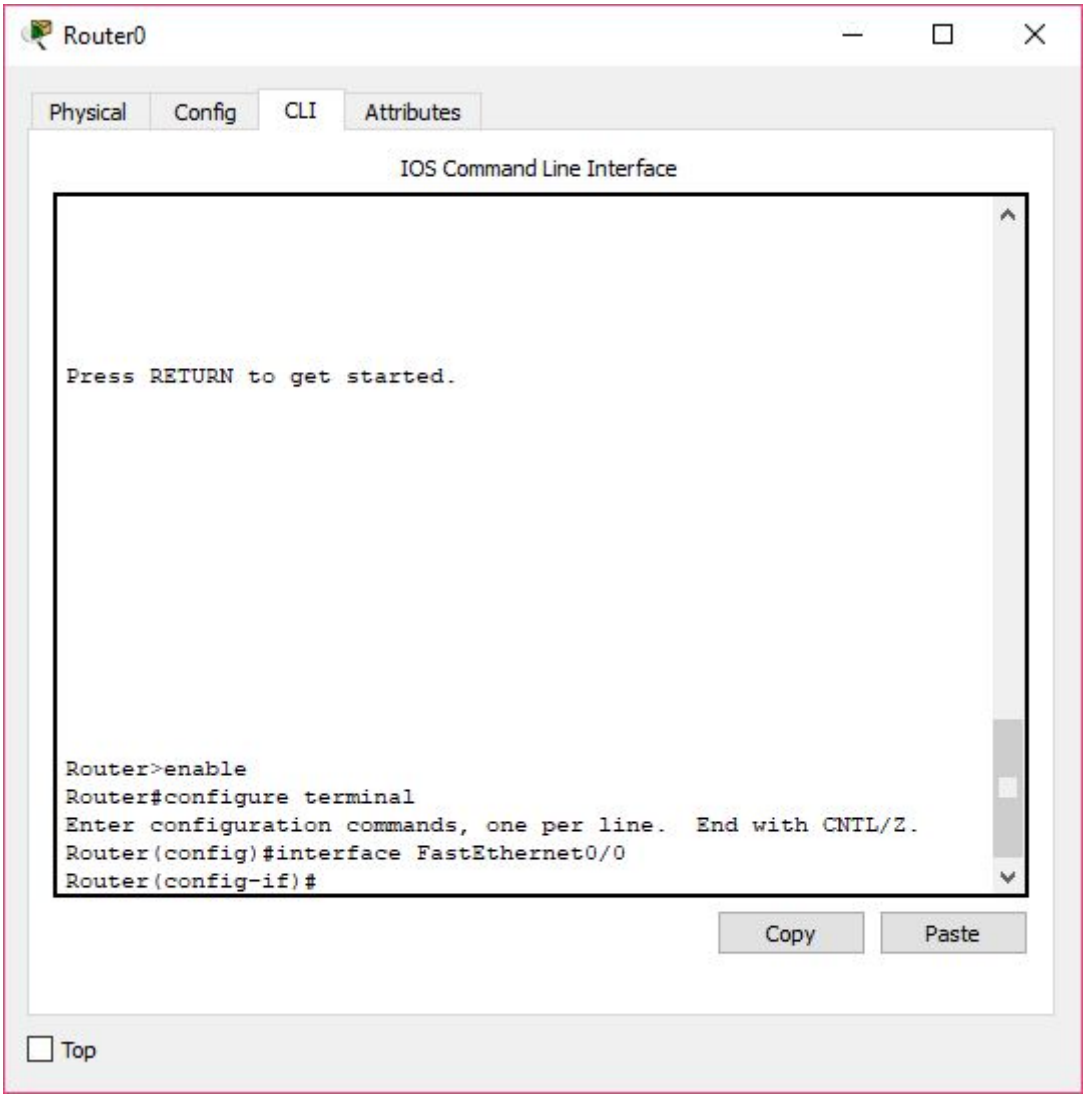
- точка доступа;
- роутер;
- коммутатор;
- сервер Linux;
- межсетевой экран;
- торрент;
- файловый сервер;
- принт-сервер.

# Работа в консоли CLI

Оборудование Cisco работает под управлением собственной операционной системы - **Cisco IOS** (от англ. Internetwork Operating System — Межсетевая Операционная Система).

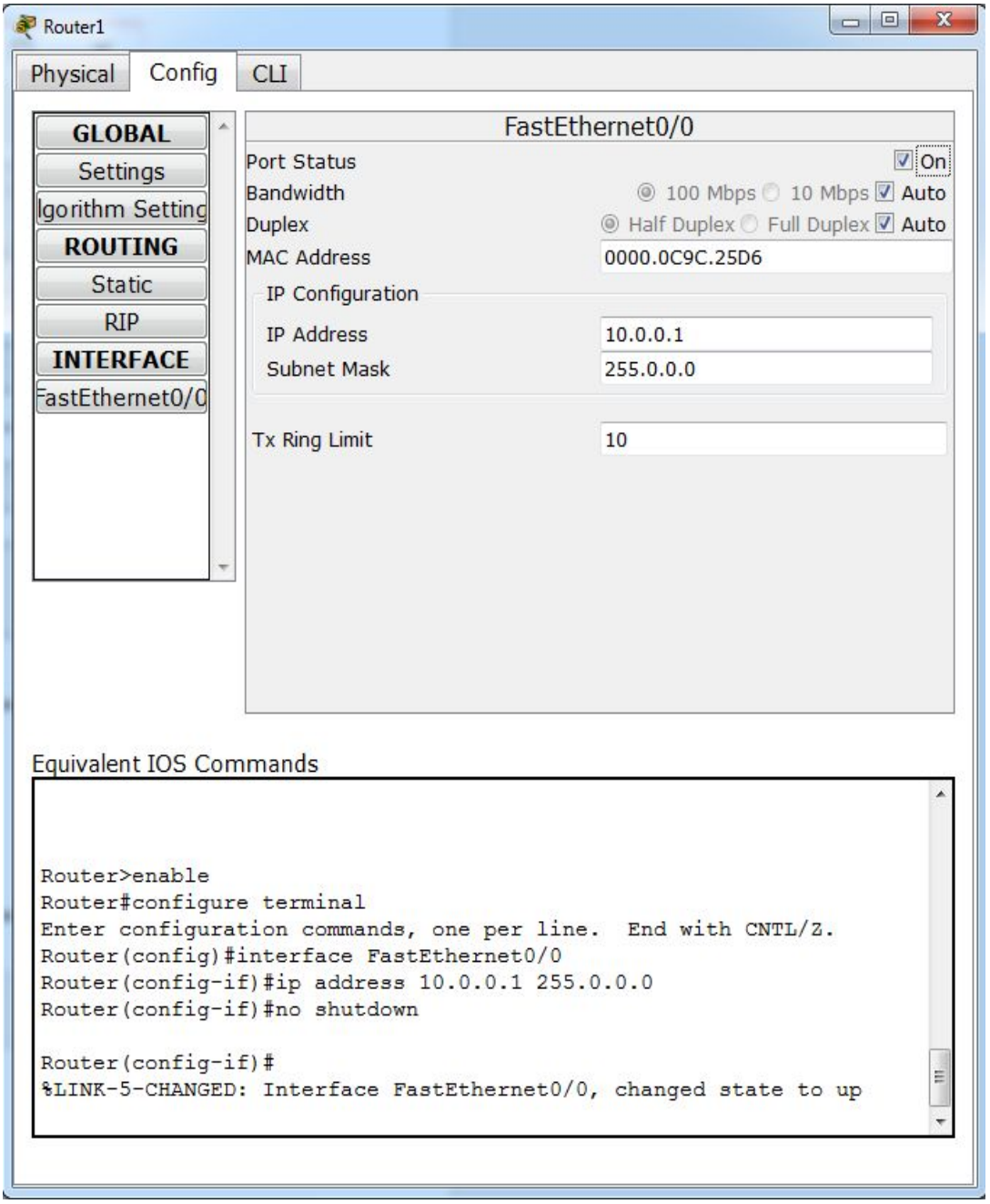
Настройка данного оборудования выполняется через **CLI** (*Command-Line* Interface, интерфейс командной строкой).

В **Cisco Packet Tracer** (далее сокращённо **PT**), консоль доступна через вкладку **CLI**




Несмотря на то, что в **PT** есть подобие графического интерфейса, позволяет он сделать не много. Кроме того, нажатие на те или иные кнопки и ввод значений, на самом деле управляет устройством через **CLI**. Обратите внимание на то, что происходит в **CLI** когда мы что-то делаем, например, с маршрутизатором. В данном примере, мы настроили на интерфейсе *FastEthernet0/0* IP адрес **10.0.0.1**

и маску подсети **255.0.0.0**, а также **включили** сам интерфейс.




Давайте разберём, что именно **PT** написал в **CLI**.

Переход в привилегированный режим:

```
Router>enable
```

Вход в режим глобальной конфигурации:

```
Router#configure terminal
```

Вход в раздел конфигурации интерфейса *FastEthernet0/0*:

```
Router(config)interface FastEthernet0/0
```

Установка IP адреса и маски подсети на интерфейсе:

```
Router(config-if)ip address 10.0.0.1 255.0.0.0
```

Включение сетевого интерфейса:

```
Router(config-if)no shutdown
```

При конфигурировании оборудования напрямую через CLI, необходимо было бы выполнять те же консольные команды.

# Основные концепции Cisco CLI

## Режимы работы командной строки

Устройства Cisco имеют несколько режимов командной строки:

1. Пользовательский режим (user mode).
2. Привилегированный режим (privileged mode).
3. Режим глобальной конфигурации (global configuration mode).
4. Режим специфической конфигурации.

Понять, в каком режиме мы находимся, очень просто, для этого надо посмотреть на приглашение в командной строке. Оно будет иметь следующий вид:

1. Для пользовательского режима ***Router>***
2. Для привилегированного режима ***Router#***
3. Для режима глобальной конфигурации ***Router(config)#***
4. Для режимов специфической конфигурации ***Router(config-*)#***, где на месте звёздочки находится название подрежима. Например, ***Router(config-if)#*** – режим настройки сетевого интерфейса.

Вместо слова Router пишется имя устройства. По умолчанию маршрутизаторы имеют имя Router, коммутаторы – Switch, но обычно при конфигурировании эти имена меняют на более конкретные.

### Пользовательский режим

В этот режим мы попадаем изначально, здесь доступен только ограниченный перечень команд, выполнение которых не должно навредить функционированию устройства. Например, из этого режима можно посмотреть версию операционной системы командой ***show version*** или запустить команду ***ping***.

### Привилегированный режим

Для перехода в этот режим необходимо из пользовательского режима выполнить команду ***enable*** и в случае необходимости ввести пароль. После перехода нам доступен полный перечень команд и возможность перехода в режим конфигурации без пароля. Таким образом, зная пароль на вход и на привилегированный режим, человек имеет полный доступ к устройству. Для перехода обратно в пользовательский режим используется команда ***disable***.

### Режим глобальной конфигурации

Этот режим позволяет вносить изменения в конфигурацию устройства. Для входа в него необходимо из привилегированного режима, выполнить команду ***configure terminal***. Ввод паролей в данном случае не потребуется. Быстрый выход из режима глобальной конфигурации выполняется командой ***end***.

### Режимы специфической конфигурации

Этих режимов множество и они являются подрежимами режима глобальной конфигурации. Например, введя в режиме глобальной конфигурации команду ***interface FastEthernet 0/0*** мы перейдём в подрежим настройки соответствующего интерфейса ***(config-if)***. Множество режимов специфической конфигурации соответствует множеству разных ветвей глобальной конфигурации. Выхода на уровень выше выполняется командой ***exit***.

## Хранение конфигурации оборудования.

В устройствах Cisco имеется по меньшей мере 2 конфигурации:

1. **Running-configuration** – это конфигурация, загруженная в данный момент в оперативную память устройства. Когда вы вносите изменения в оборудование, как раз эта конфигурация изменяется.
2. **Startup-configuration** - это конфигурация, которая храниться в энергонезависимой памяти устройства и будет прочитана и установлена в **running-configuration** при включении устройства.

**Важно! Running-configuration НЕ сохраняется автоматически и в случае перезагрузки устройства - теряется.**

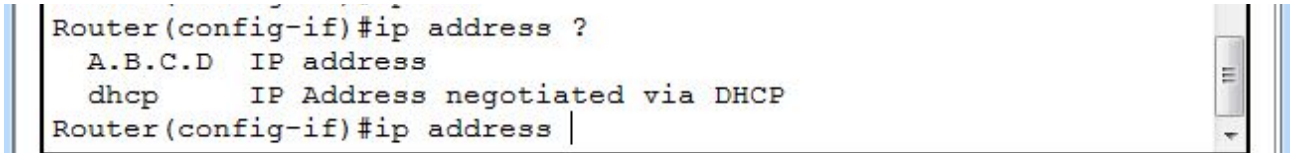
Основные команды для работы с конфигурациями:

- ***show running-config*** - отображает текущую рабочую конфигурацию;
- ***show startup-config*** - отображает текущую стартовую конфигурацию;
- ***write*** - выполняет запись **running-configuration** в **startup-configuration;**
- ***erase startup-config*** - удаляет **startup-config**, если в таком состоянии перезагрузить устройство, то оно загрузится с настройками по умолчанию.

# Общие методы работы с CLI

## Получение справки

Символ знак вопроса “**?**” можно использовать почти в любой момент, чтобы **получить справку** о возможных командах.




## Автозавершение команд

Нажатие клавиши <tab> выполняет автозавершение текущей написанной команды, если не возникает неоднозначности.

## Выполнение команд из режима конфигурации

Если на устройстве работает Cisco IOS 12.2(8) или выше, вы имеете возможность использовать команду do для запуска привилегированных команд из конфигурационного режима. Другими словами, вы имеет возможность выполнить команду show или другую команду во время конфигурирования устройства.

Для выполнения данного действия необходимо добавить do перед необходимой командой.

Например:

```
router(config)# do show interface f0/0
```

или

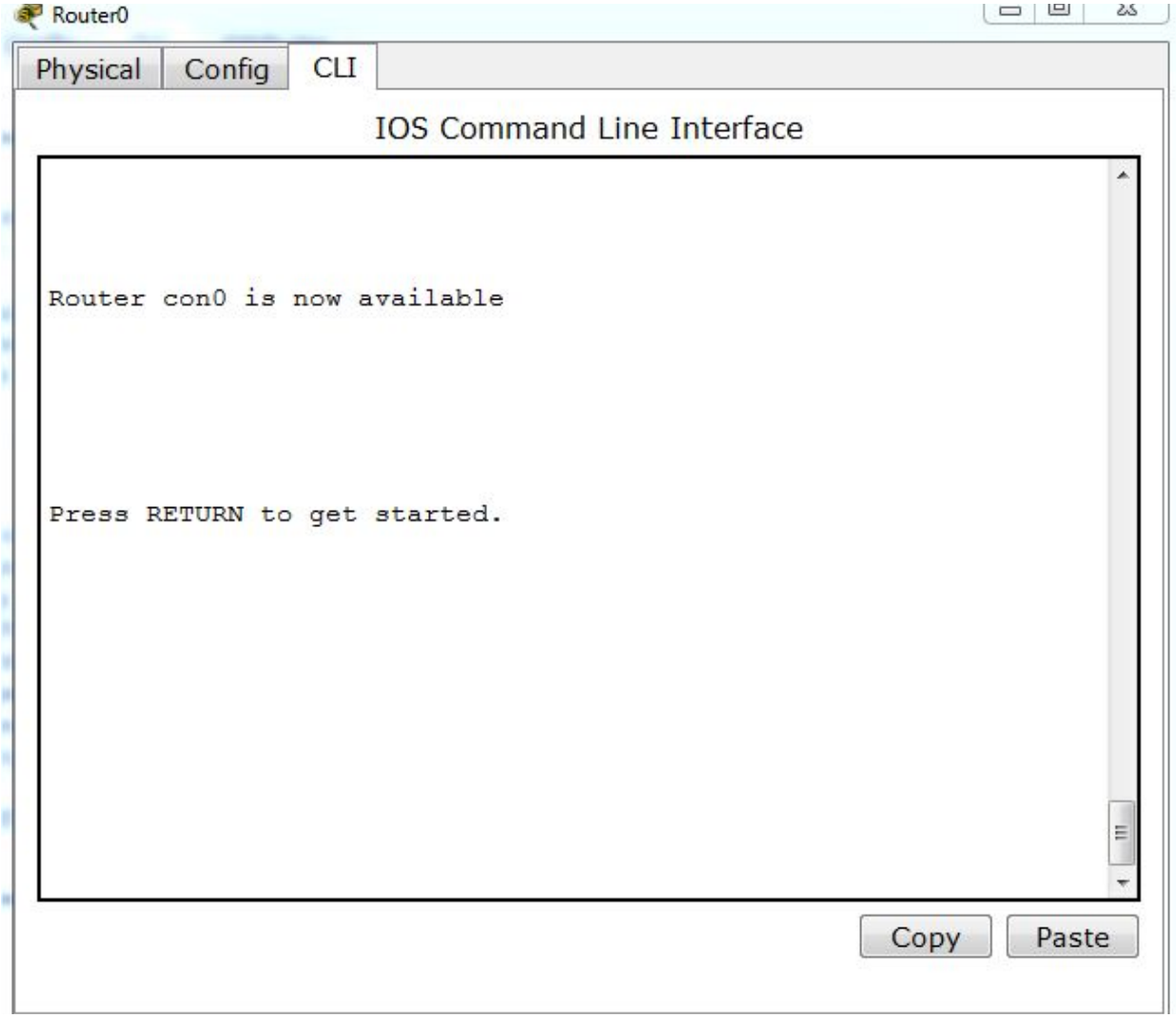
```
switch(config-if)# do show run
```

Таким же образом можно использовать команды ping, debug и пр.

## Сокращение команд

Все команды можно сокращать, если это не вызывает неоднозначности. Пример configure terminal сокращается до conf t.

# Пример ручной конфигурации сетевого интерфейса с помощью CLI




```
Router>enable
Router#configure terminal
Router(config)interface fa1/0
```

Нажатие клавиши <tab> приводит к автозавершению команды, если это возможно:

```
Router(config-if)ip addr<tab>
```

В результате:

```
Router(config-if)ip address
```

Назначаем IP адрес и маску подсети:

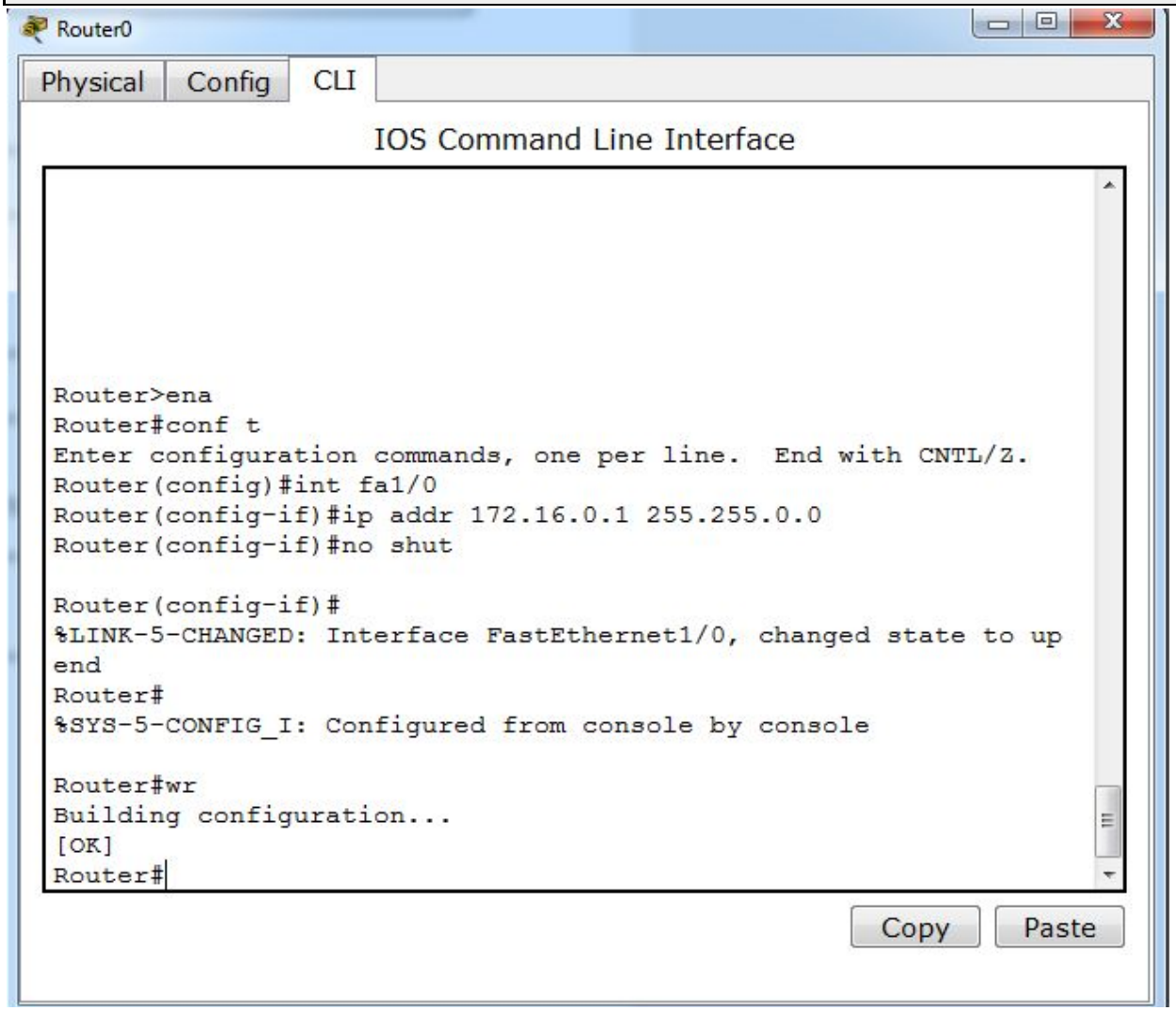
```
Router(config-if)ip address 172.16.0.1 255.255.0.0
```

Включим сетевой интерфейс (он по умолчанию выключен):

```
Router(config-if)no shutdown
```

Выходим из режима конфигурации и сохраняем текущий конфиг в стартовый:

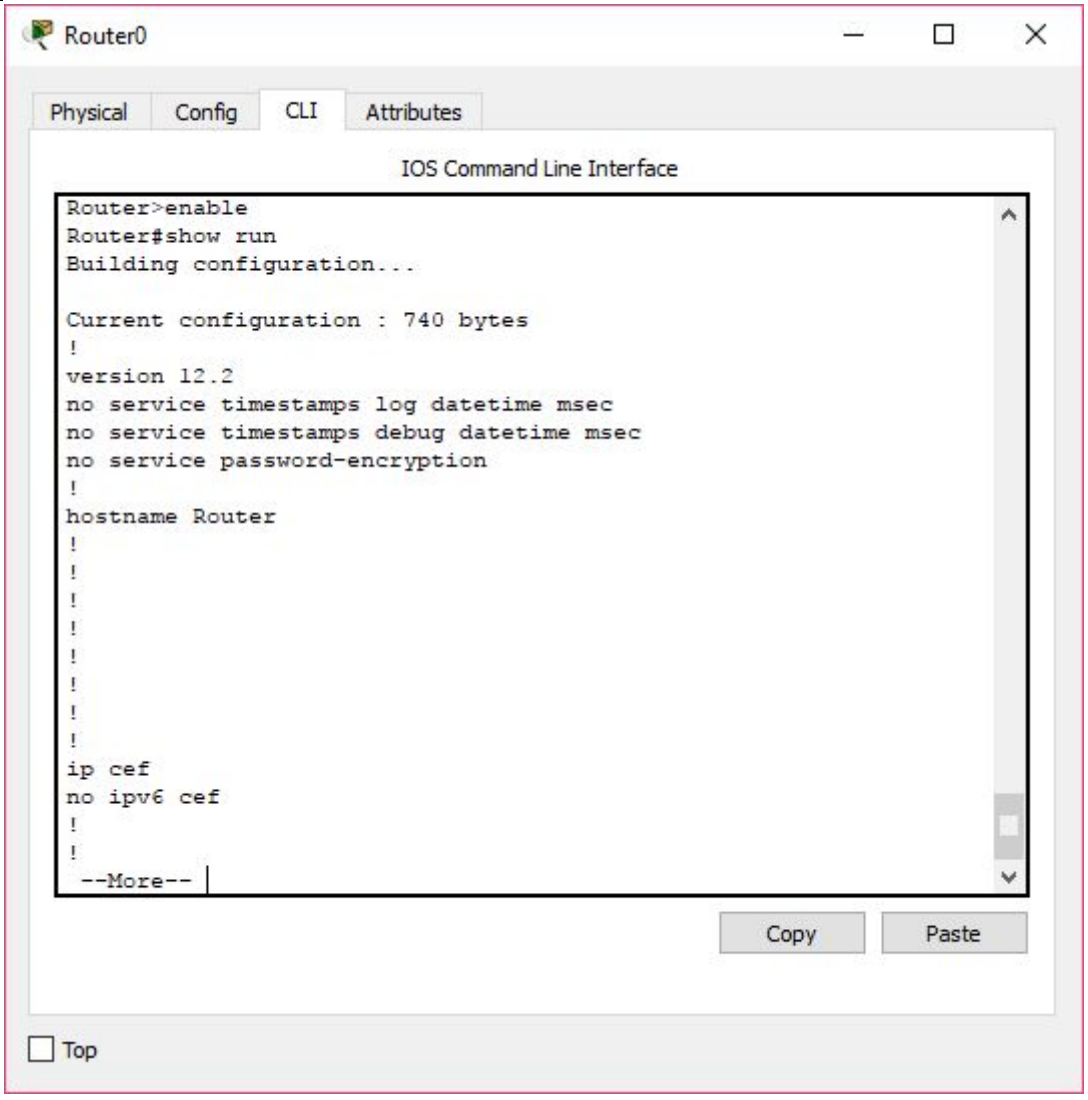
```
Router(config-if)end
Router#write
```



Мы сделали все тоже самое, что умеет делать графический интерфейс и немножко больше (сохранили конфигурацию).

Для отображения текущей рабочей конфигурации введите:

```
Router#show run
```



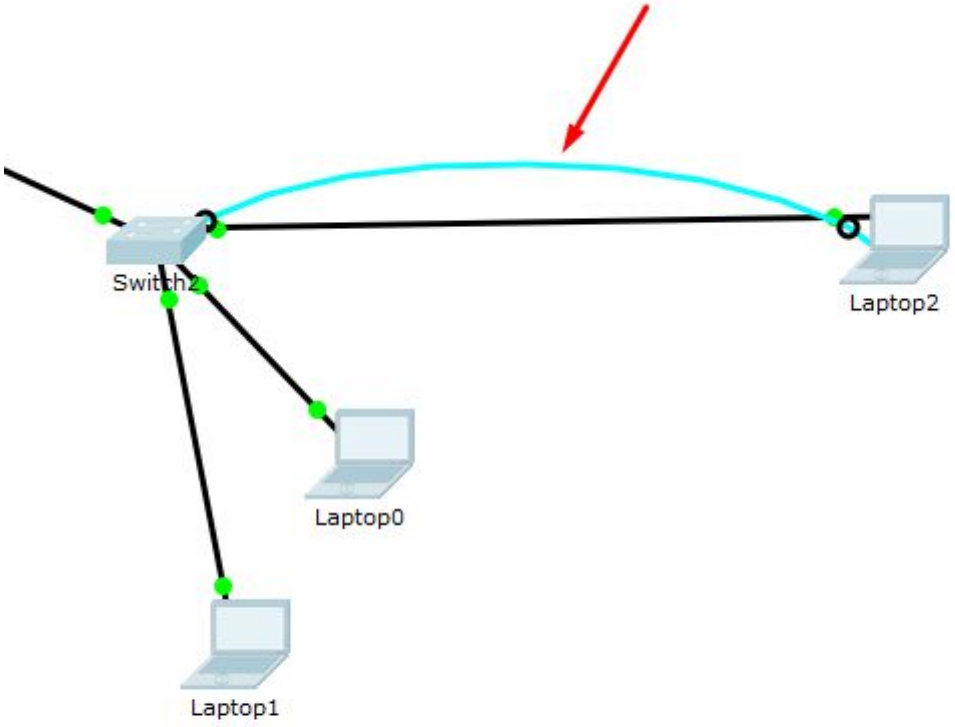

Попробуйте самостоятельно:

```
Router#show ?
```

Изучите предложенные команды.

# Настройка удалённого доступа к коммутатору через telnet

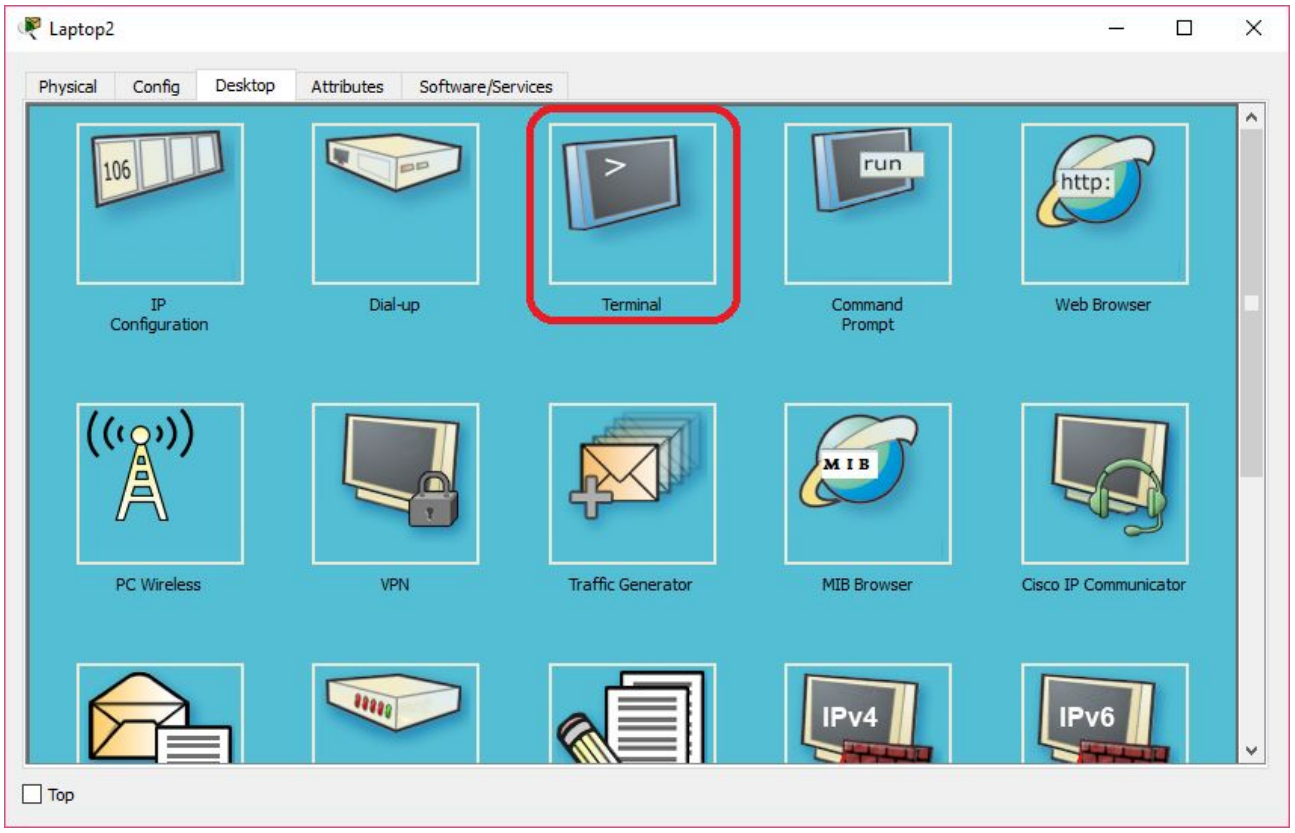
Настроим коммутатор для доступа через telnet, подключив синий консольный кабель (это мы в Cisco Packet Tracer видим терминал, а на практике надо подключить терминал через консольный кабель). После настроек можно будет подключаться к устройству по сети.



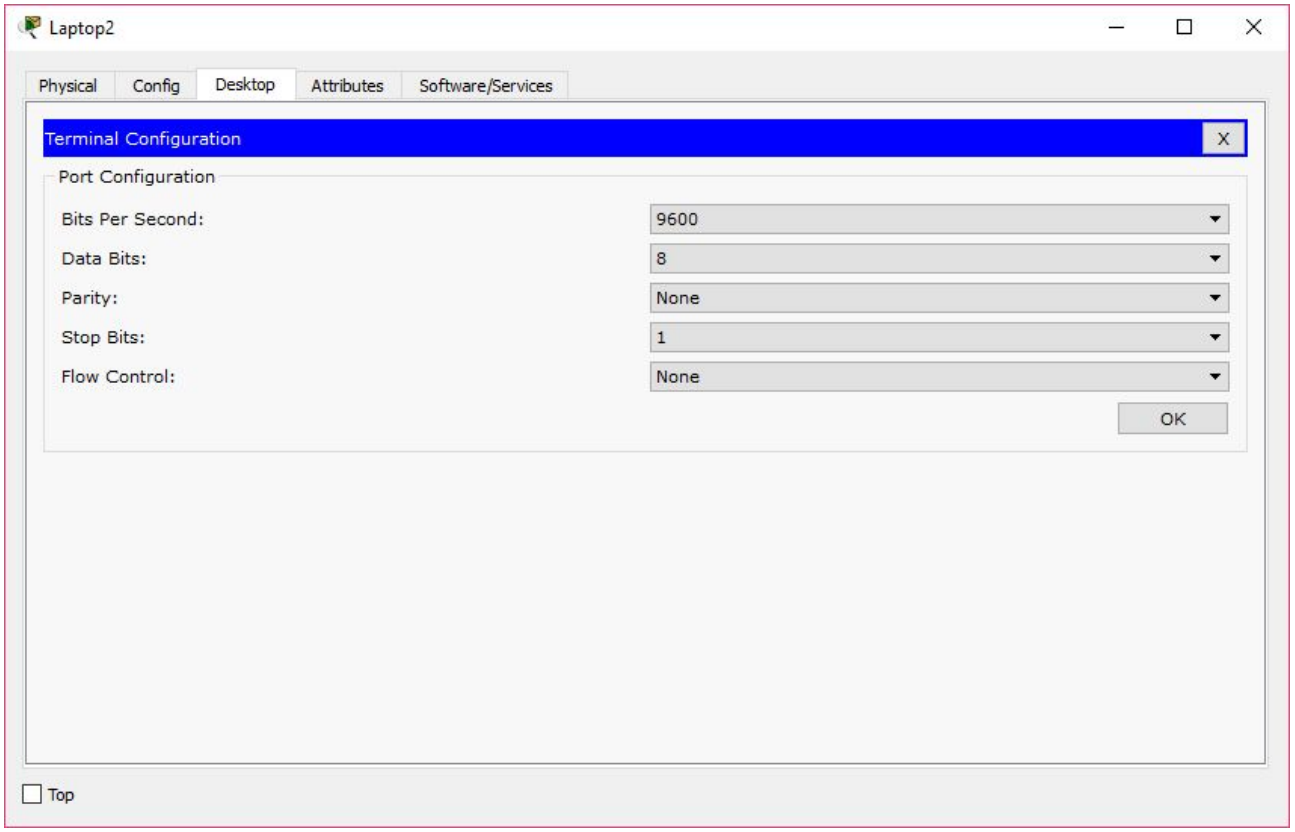


В коммутатор следует консольный кабель включить в консольный порт.

На компьютере в порт RS-232 (COM-порт, стандартный последовательный порт для работы с терминалом).

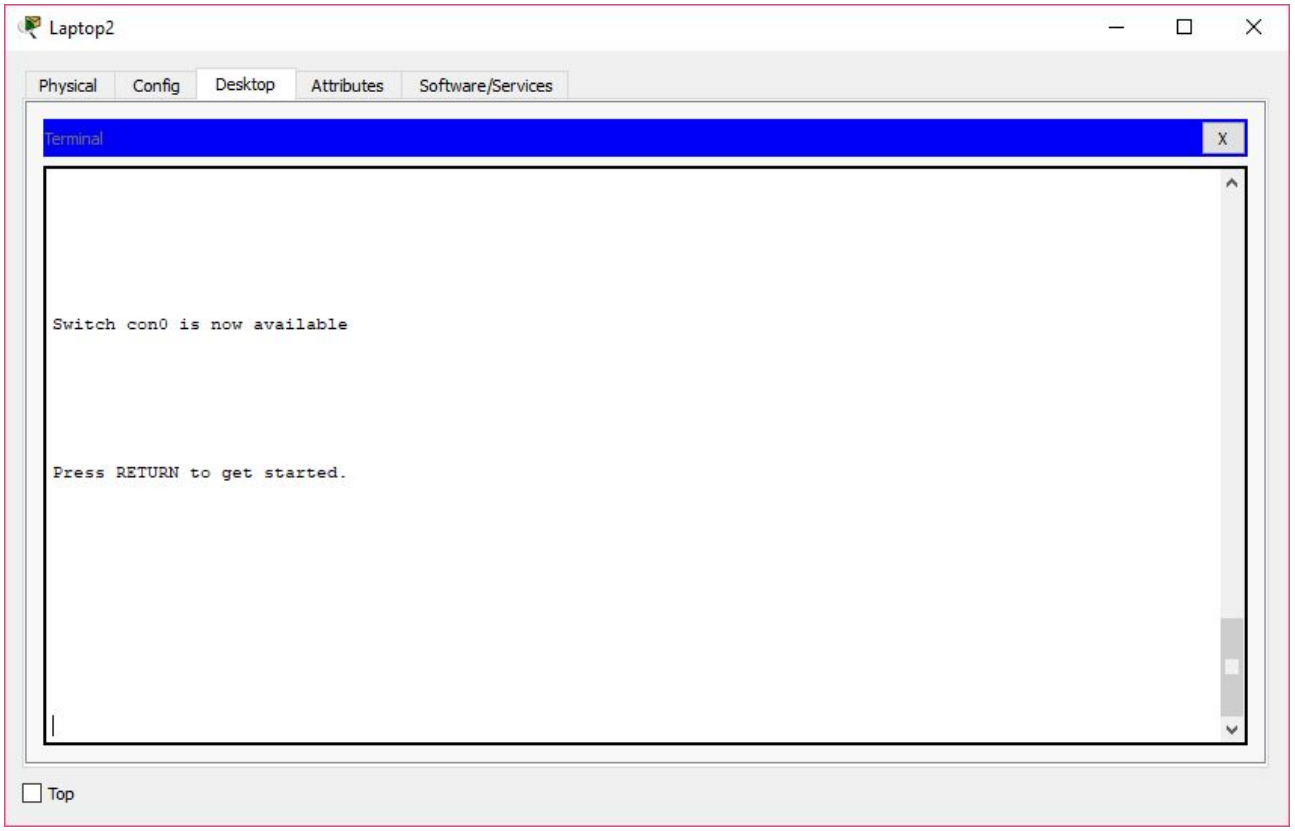



Кликаем терминал.



Стандартные настройки: 9600-8-N-1-N.

Подключаемся.




И видим ту же самую консоль, что и через Cisco Packet Tracer, только теперь ближе к реальности.

Команды можно сокращать:

```
Switch>ena
Switch#conf t
```

Задаём пароль  для привилегированного режима (enable):

```
Switch(config)#ena pass qwr
```

Настроим пять терминальных линий:

```
Switch(config)#line vty 0 4
```

Зададим пароль:

```
Switch(config-line)pass asd
```

Настроим сетевой интерфейс для доступа по сети. Он будет находиться в первом vlan и иметь IP-адрес 10.0.0.1 с маской 255.0.0.0.

```
Switch(config-line)int vlan 1
Switch(config-if)ip addr 10.0.0.1 255.0.0.0
```

Включим интерфейс:

```
Switch(config-if)no shut
```

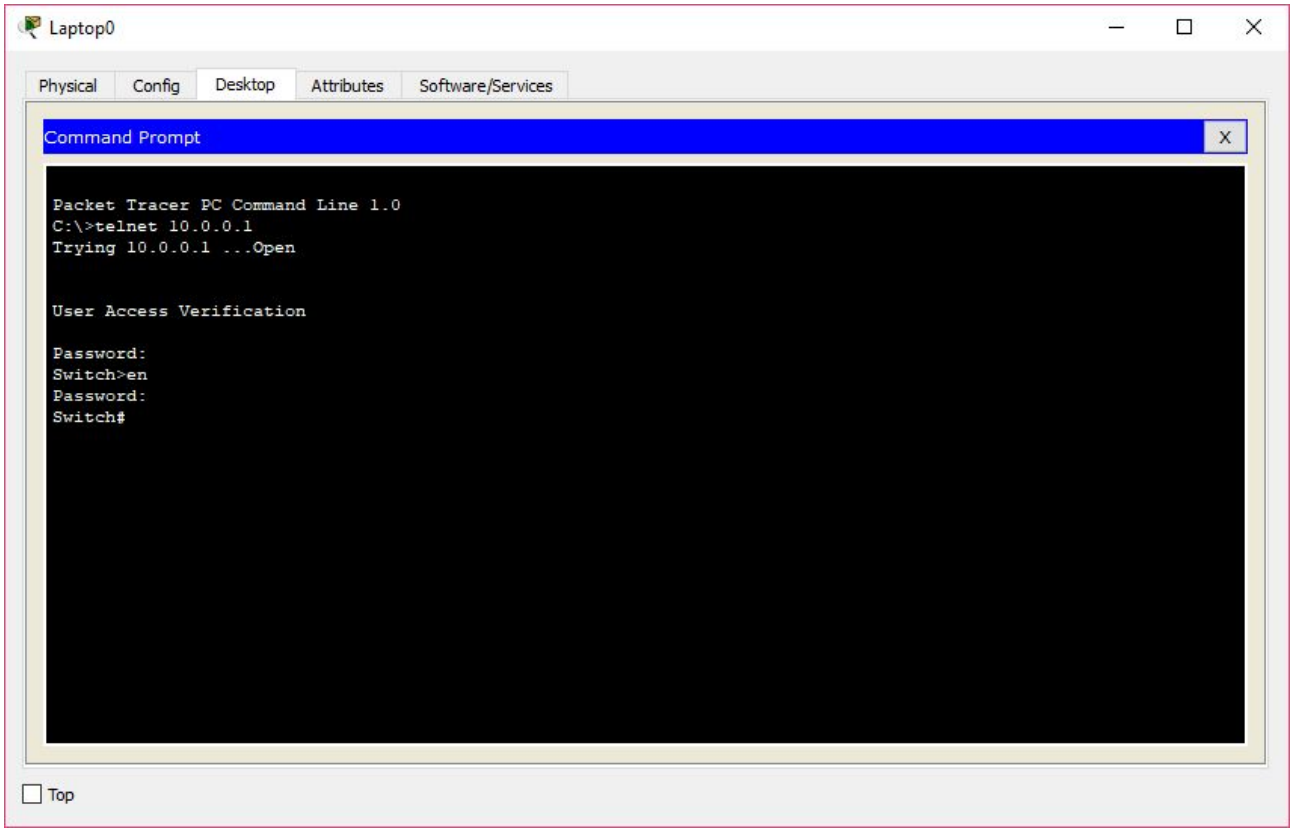
Выходим из режима конфигурации:

```
Switch#end
```

Сохраняем текущую конфигурацию:

```
Switch#wr
```

Теперь мы можем с любого другого компьютера в сети 10.0.0.0 (компьютер подключен к коммутатору, и имеет ip-адрес, например, 10.0.0.200 и маску сети 255.0.0.0) подключится данному устройству.

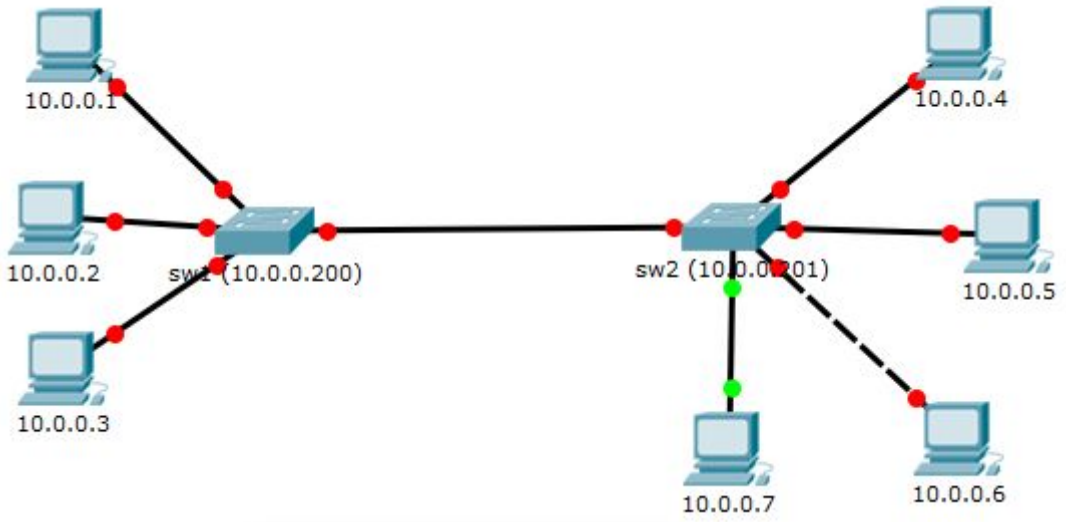



Вводим пароль, переходим в enable, снова вводим пароль. Можно настраивать.

# Домашнее задание

**Работа в CPT.** Скачать приложенный файл.

1. Исправить проблемы с линками на всех хостах.
2. Настроить сетевые интерфейсы на всех хостах и менеджмент на свитчах, используя только консольный кабель.
3. Обвести синим цветом все широковещательные домены, а красным все домены коллизий.




# Дополнительные материалы

1. Таненбаум Э., Уэзеролл Д. Т18  Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с. **(Глава 2)**

# Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы:


1. http://pascal.tsu.ru/other/frames.html#as-h4-2325214
2. https://habrahabr.ru/post/189268/
3. https://ru.wikipedia.org/wiki/Power_over_Ethernet
4. http://xgu.ru/wiki/Петля_коммутации
5. http://forum.sources.ru/index.php?showtopic=294913
6. http://www.zen22142.zen.co.uk/Circuits/Interface/pethhub.htm
7. https://tools.ietf.org/html/rfc894