Модель взаимодействия открытых систем (Модель OSI)

Международная организация стандартов (International Standards Organization – **ISO**) в 1984 году создала эталонную **модель взаимодействия открытых систем** (Open System Interconnection reference model – **OSI**), которая определяет концепцию и методологию создания сетей и систем передачи данных.

Модель OSI описывает стандартные правила функционирования устройств и программных средств при обмене данными между узлами (компьютерами) в открытой системе, определяет сетевые функции, выполняемые каждым ее уровнем.

Открытая система – любая система (компьютерная, вычислительная сеть, операционная система, аппаратная или программная продукция), которая построена в соответствии с открытыми (общедоступными) спецификациями.

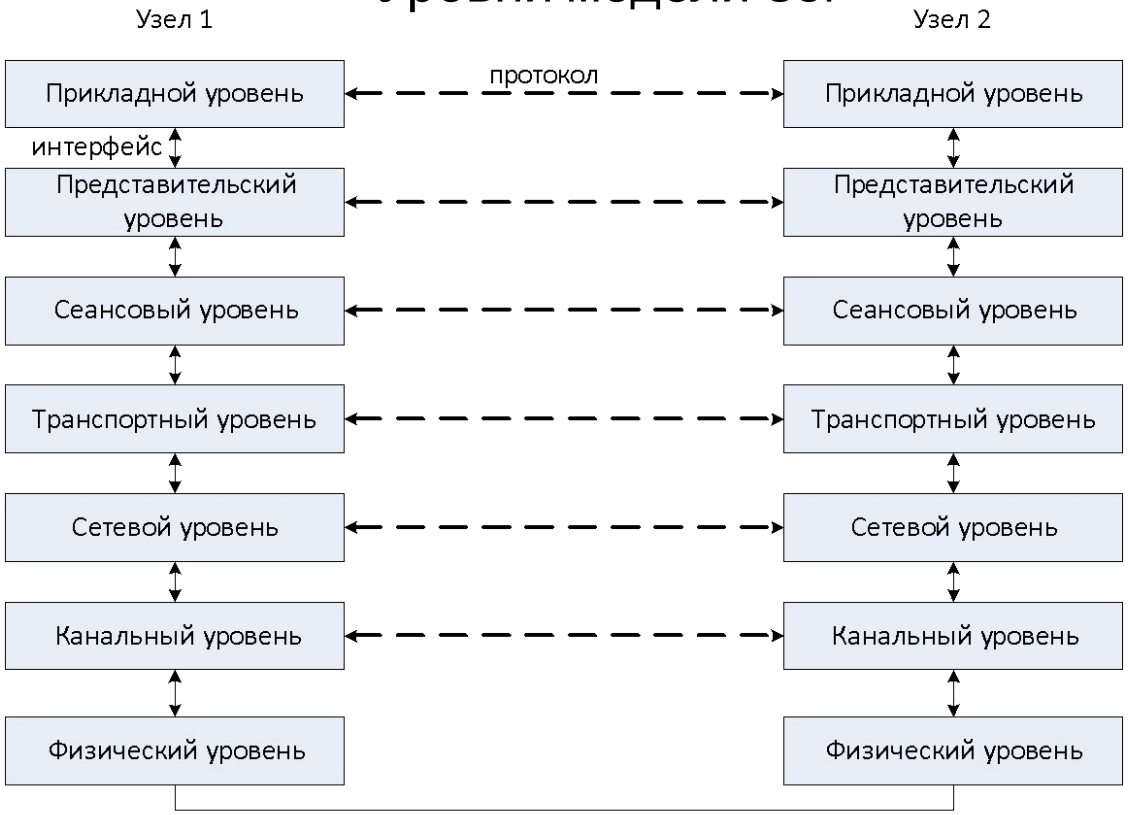
Спецификация – формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, особых характеристик.

Модель OSI включает 7 уровней.

Уровни модели OSI

Номер уровня	Наименование уровня
7	Прикладной
6	Представления
5	Сеансовый
4	Транспортный
3	Сетевой
2	Канальный
1	Физический

Уровни модели OSI

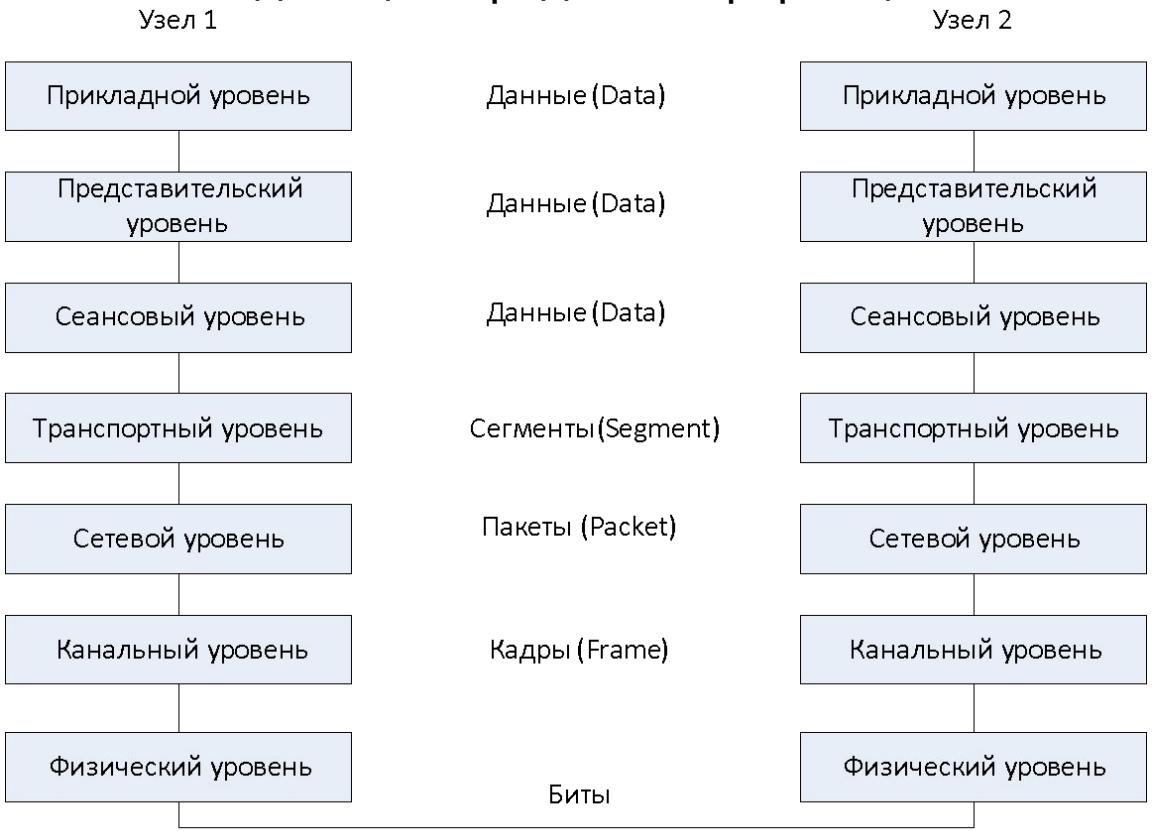


Правила, по которым происходит обмен данными между программно–аппаратными средствами, находящимися на одном уровне, называются **протоколом**.

Набор протоколов называется **стеком** протоколов и задается определенным стандартом.

Взаимодействие соответствующих уровней является **виртуальным**, за исключением физического уровня, на котором происходит обмен данными по кабелям, соединяющим компьютеры. Взаимодействие уровней между собой происходит через межуровневый **интерфейс** и каждый нижележащий уровень предоставляет услуги вышележащему.

Единицы передачи информации

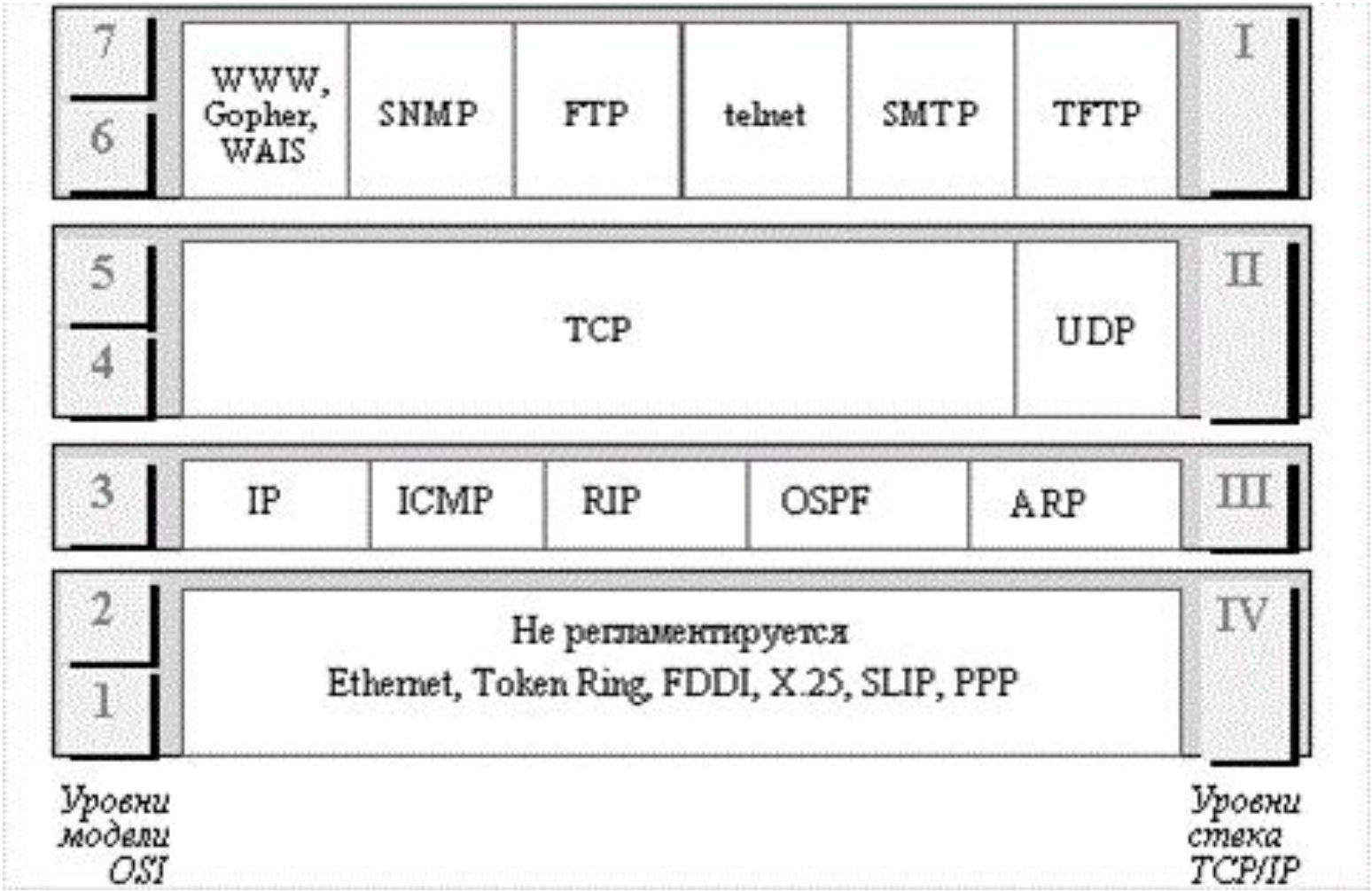


Виртуальный обмен между соответствующими уровнями узлов Узел 1 и Узел 2 происходит определенными единицами информации.

На трех верхних уровнях – это сообщения или данные (Data).
На транспортном уровне – сегменты (Segment), на сетевом уровне – пакеты (Packet), на канальном уровне – кадры (Frame) и на физическом передается последовательность битов.

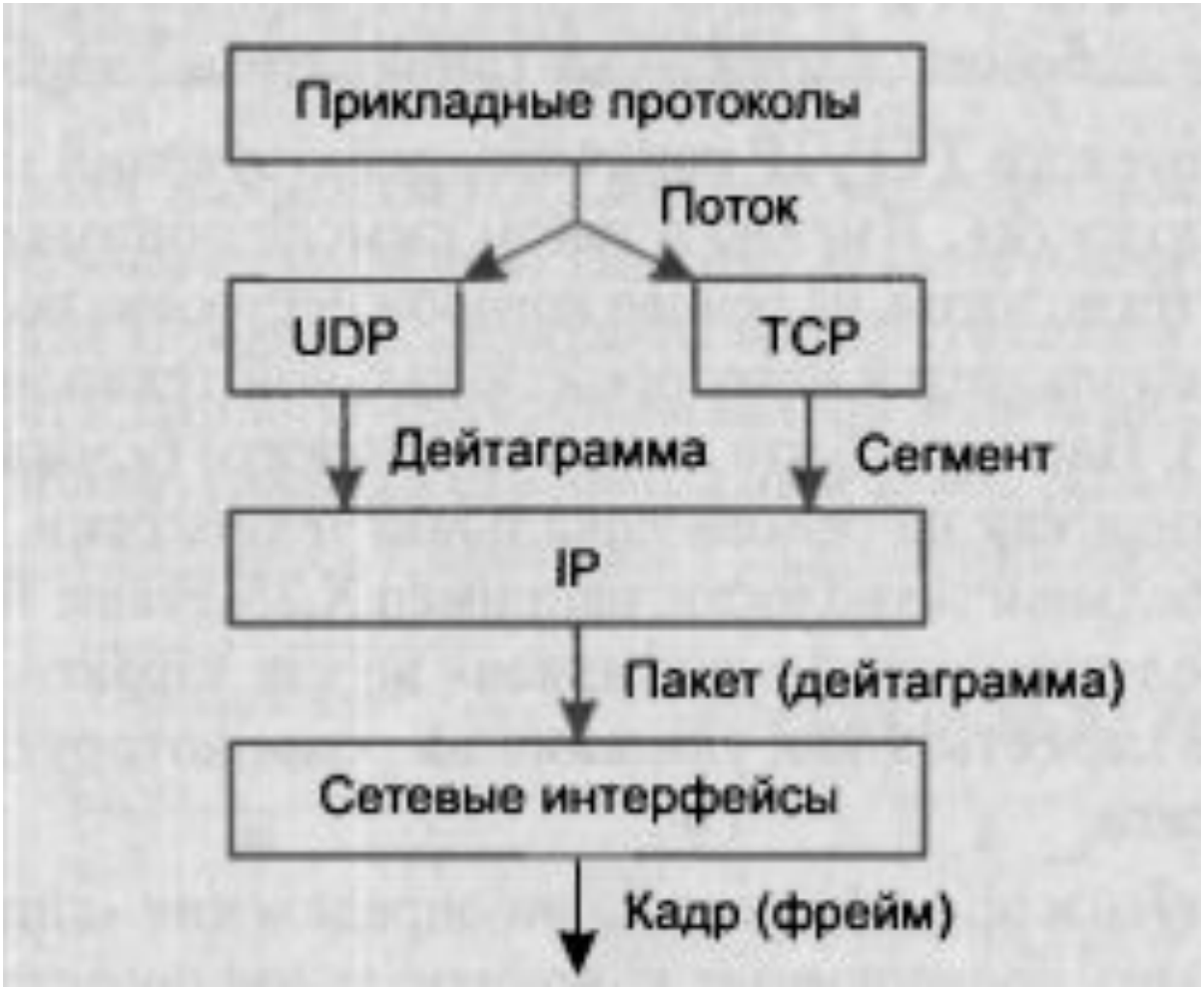
Уровень модели OSI	Функция уровня	Используемые протоколы
Уровень приложений	Обеспечивает пользовательский интерфейс.	Telnet HTTP
Уровень представления	Представление данных (чтобы информация уровня приложений, которую посылает одна система, могла быть прочитана уровнем приложений другой системы); Управление процессами, например шифрованием.	TIFF, JPEG MIDI,MPEG
Сеансовый уровень	Установление сеанса связи между двумя рабочими станциями; Разделение данных разных приложений.	NFS ASP
Транспортный уровень	Обеспечивает надежную или ненадежную доставку; Проводит коррекцию ошибок перед повторной передачей данных;	TCP UDP SPX
Сетевой уровень	Обеспечивает выбор маршрута и соединение между собой двух рабочих станций; Обеспечивает логическую адресацию, где путь определяется маршрутизаторами;	IP, IPX AppleTalk
Канальный уровень	Разделяет пакеты на байты и объединяет байты в кадры; Обеспечивает физическую адресацию на уровне носителя (например, с помощью MAC-адресов); Анализирует сетевую топологию, доступ к сети; Выполняет выявление ошибок, но не их коррекцию;	Ethernet Token Ring ATM FR
Физический	Перемещает между устройствами биты данных;	Коаксиал Витая пара

Стек TCP/IP



1ый уровень: прикладной
2ой уровень: транспортный
3ий уровень: сетевой (межсетевого взаимодействия, уровень Интернета)
4ый уровень: сетевых интерфейсов

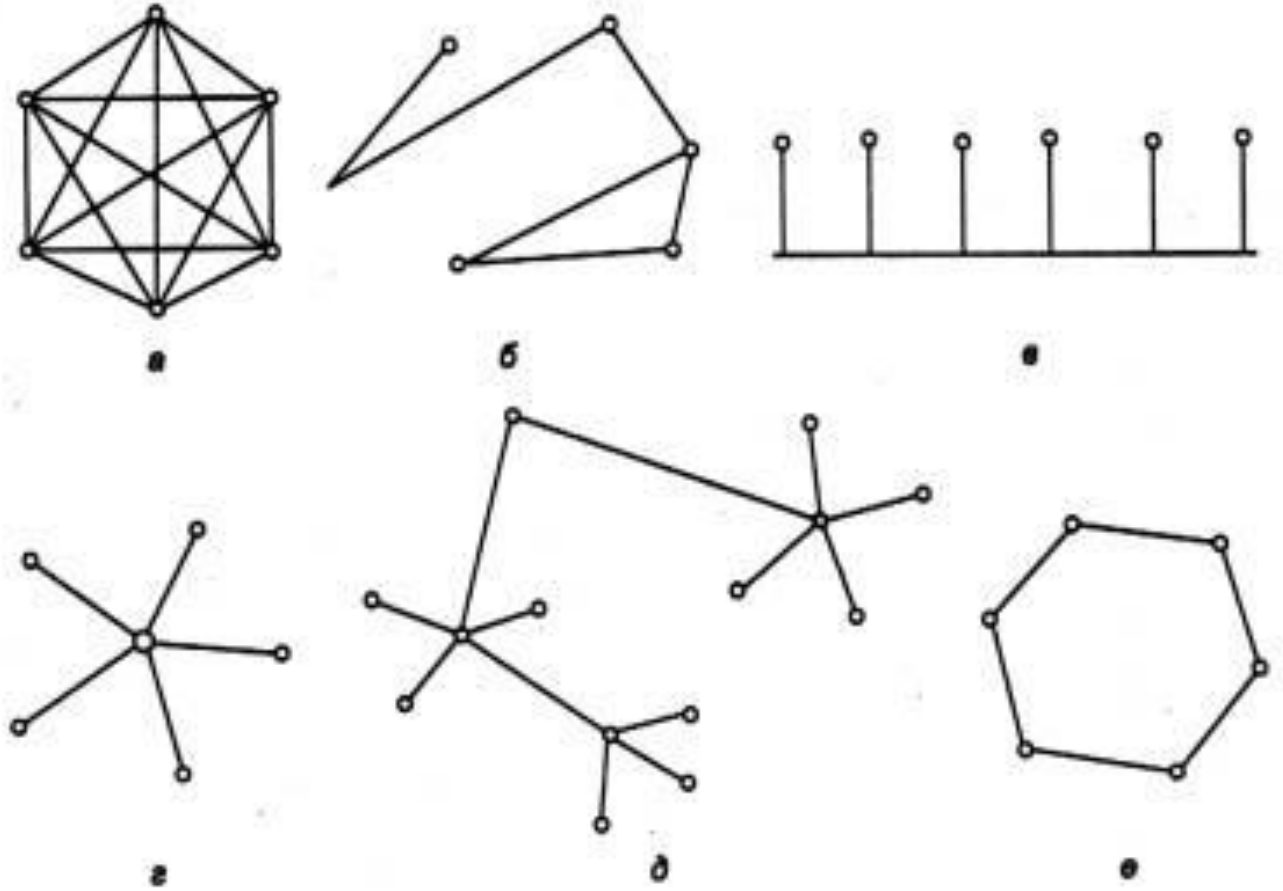
Единицы передачи данных между уровнями



№	Уровень TCP/IP	Функция уровня
I	Прикладной	Объединяет сервисы, предоставляемые системой пользовательским приложениям.
II	Транспортный	Предоставляет прикладному уровню 2 типа сервиса: Гарантированную доставку (протокол TCP) Доставку по возможности – без подтверждения доставки (протокол UDP).
III	Сетевой (межсетевого взаимодействия, уровень Интернета)	Соответствует сетевому уровню модели OSI (обеспечивает выбор маршрута и соединение между собой двух рабочих станций, обеспечивает логическую адресацию, где путь определяется маршрутизаторами).
IV	Сетевых интерфейсов	Трактовка уровня сильно отличается от трактовки канального и физического уровня модели OSI. Отвечает только за организацию взаимодействия с подсетями различных технологий, входящими в составную сеть.

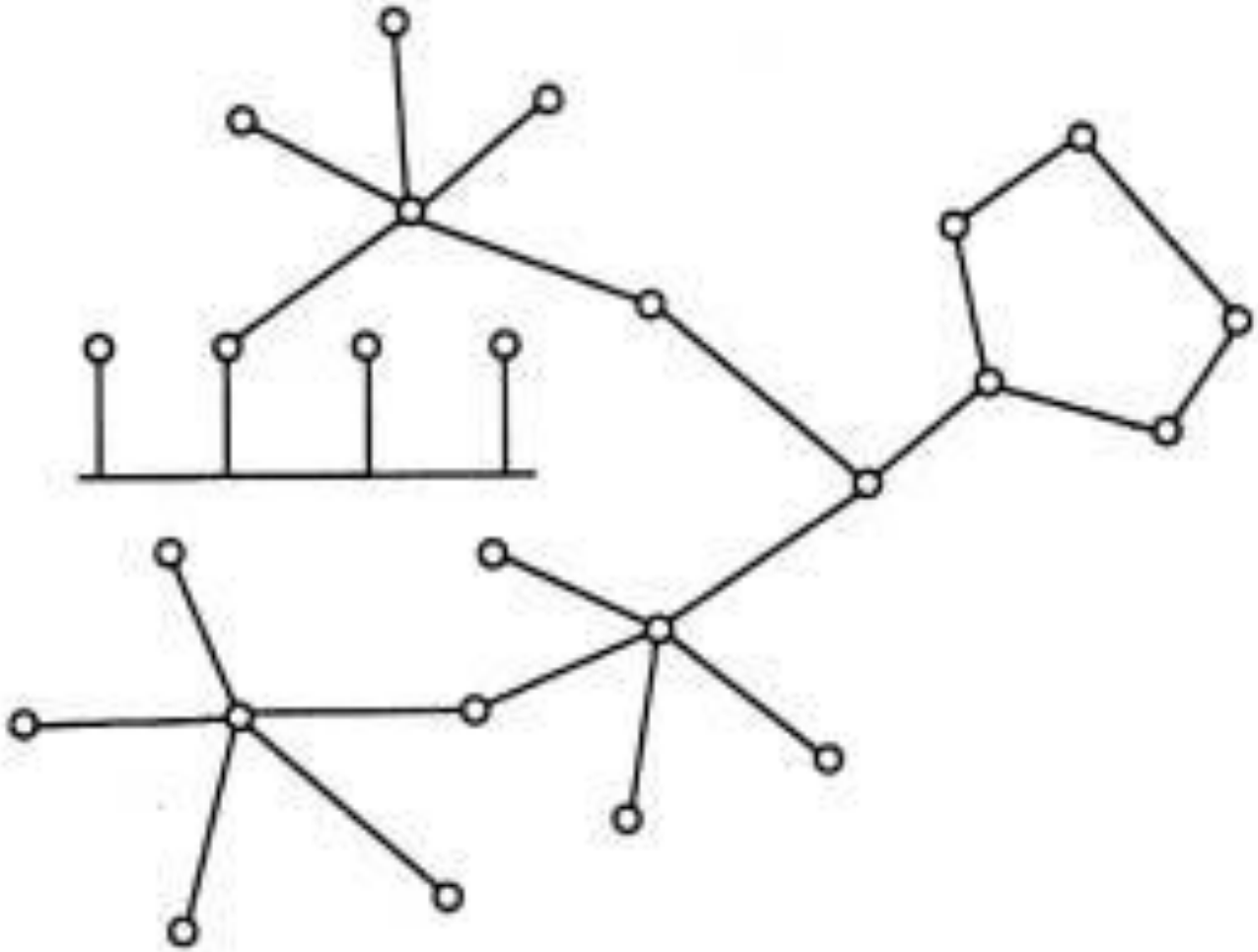
Топологии компьютерных сетей

Топология - совокупность элементов и связей между ними, «очищенных» от всех свойств, кроме свойств существования и связности; способ организации физических связей



а – полносвязная («каждый с каждым»), б – ячеистая, в – общая шина
г – звезда, д – иерархическая звезда, е – кольцевая

Смешанная топология



IEEE Project 802

802.1 – объединение сетей с помощью *мостов* и *коммутаторов*

802.2 – управление логической связью на *подуровне LLC*.

802.3 – локальная сеть с методом доступа *CSMA*/CD и топологией шина (Ethernet).

802.4 – локальная сеть с топологией шина и маркерным доступом (Token-Bus).

802.5 – локальная сеть с топологией кольцо и маркерным доступом (Token-Ring).

802.6 – городская сеть (*Metropolitan Area Network*, MAN) с расстояниями между абонентами более 5 км.

802.7 – широкополосная технология передачи данных.

802.8 – оптоволоконная технология.

802.9 – интегрированные сети с возможностью передачи речи и данных.

802.10 – безопасность сетей, шифрование данных.

802.11 – беспроводная сеть по радиоканалу (*WLAN – Wireless LAN*).

802.12 – локальная сеть с централизованным управлением доступом по *приоритетам запросов* и топологией звезда (*100VG-AnyLAN*).

Сетевое оборудование

Активное

оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников и выполняющее функции усиления, преобразования сигналов и иные.

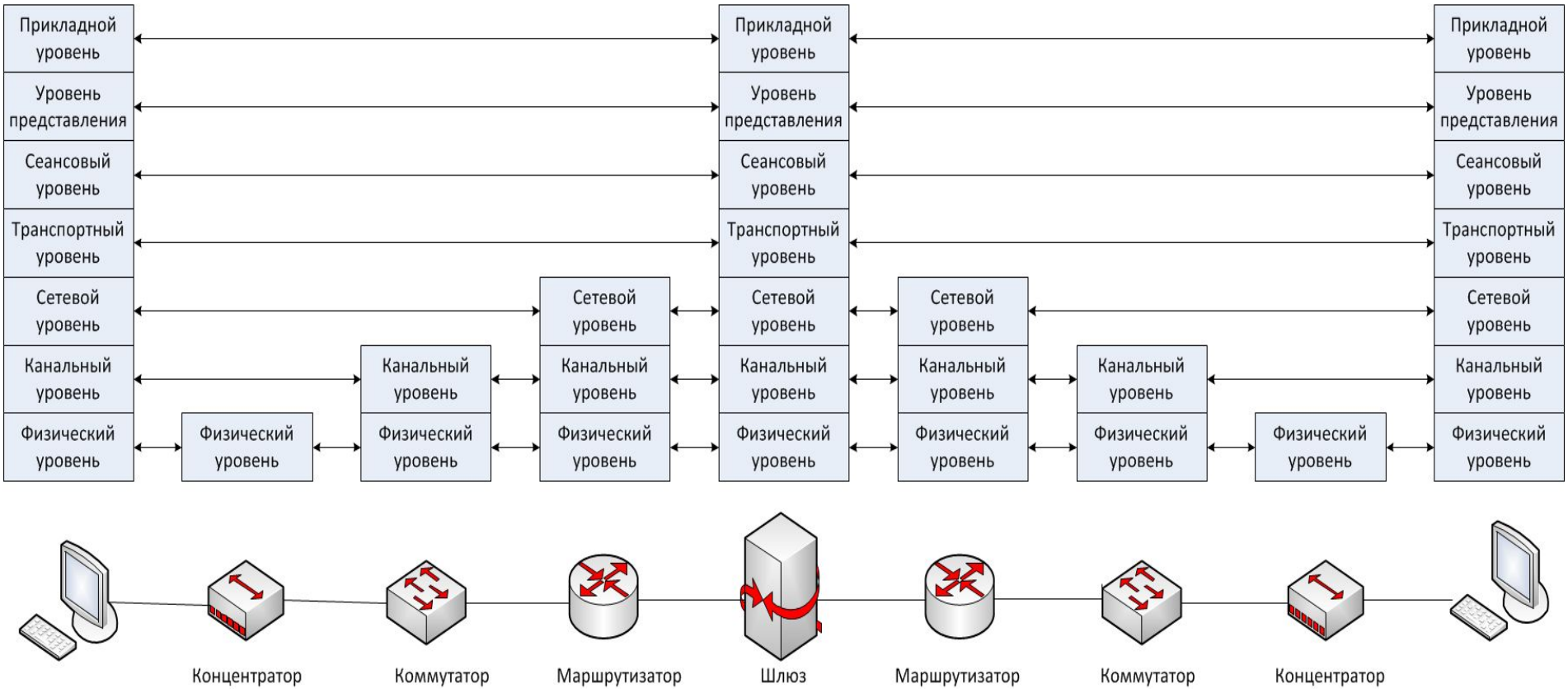
- сетевой адаптер
- репитер (повторитель)
- концентратор (активный хаб, многопортовый репитер)
- мост
- коммутатор (свитч)
- маршрутизатор (роутер)
- медиаконвертер
- сетевой трансивер

Пассивное

оборудование, не получающее питание от электрической сети или других источников, и выполняющее функции распределения или снижения уровня сигналов.

- кабель
- разъемы (вилка/розетка)
- патч-панель

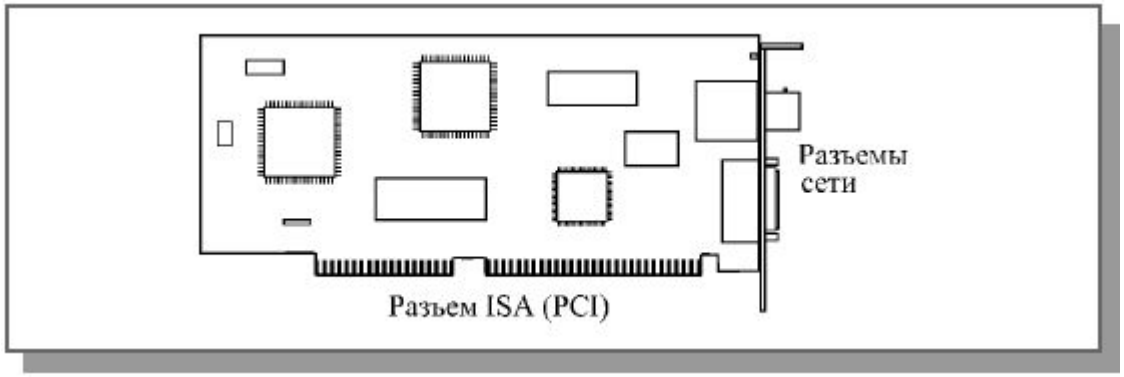
Соответствие функций различных устройств сети уровням модели OSI



Сетевые адаптеры

(они же контроллеры, карты, платы, интерфейсы, NIC – Network Interface Card)

Как правило, сетевые адаптеры выполняются в виде платы, вставляемой в слоты расширения системной магистрали (шины) компьютера (чаще всего PCI, ISA или PC-Card). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.



Для каждого типа кабеля используются свои разъемы и свой способ подключения кабеля к сетевому адаптеру. В настоящее время сетевые адаптеры могут поддерживать стандарты Ethernet/FE (например, 100 BASE-T Ethernet).

Разъемы адаптера Ethernet:

TPO – разъем RJ-45 (для кабеля на витых парах по стандарту 10BASE-T).

TPC – разъемы RJ-45 (для кабеля на витых парах 10BASE-T) и BNC (для коаксиального кабеля 10BASE2).

TP – разъем RJ-45 (10BASE-T) и трансиверный разъем AUI.

Combo – разъемы RJ-45 (10BASE-T), BNC (10BASE2), AUI.

Coax – разъемы BNC, AUI.

FL – разъем ST (для оптоволоконного кабеля 10BASE-FL).

К магистральным относятся те функции, которые осуществляют взаимодействие *адаптера* с магистралью (системной шиной) компьютера (то есть опознание своего магистрального адреса, пересылка данных в компьютер и из компьютера, выработка сигнала прерывания процессора и т.д.). Сетевые функции обеспечивают общение *адаптера* с сетью.

К основным сетевым функциям *адаптеров* относятся:

- гальваническая развязка компьютера и кабеля локальной сети
- преобразование логических сигналов в сетевые (электрические или световые) и обратно
- кодирование и декодирование сетевых сигналов
- опознание принимаемых пакетов (выбор из всех приходящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно)
- преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме
- буферизация передаваемой и принимаемой информации в буферной памяти *адаптера*
- организация доступа к сети в соответствии с принятым методом управления обменом
- подсчет контрольной суммы пакетов при передаче и приеме

Типичный *алгоритм* взаимодействия компьютера с *сетевым адаптером*

Если *компьютер* хочет передать пакет, то он сначала формирует этот пакет в своей памяти, затем пересылает его в буферную *память сетевого адаптера* и дает команду *адаптеру* на передачу. *Адаптер* анализирует текущее состояние сети и при первой же возможности выдает пакет в *сеть* (выполняет *управление доступом* к сети). При этом он производит преобразование информации из буферной памяти в последовательный вид для побитной передачи *по* сети, подсчитывает контрольную сумму, кодирует биты пакета в сетевой код и через узел гальванической развязки выдает пакет в *кабель* сети. *Буферная память* в данном случае позволяет освободить *компьютер* от контроля состояния сети, а также обеспечить требуемый для сети темп выдачи информации.

Если *по* сети приходит пакет, то *сетевой адаптер* через узел гальванической развязки принимает биты пакета, производит их *декодирование* из сетевого кода и сравнивает *сетевой адрес* приемника из пакета со своим собственным адресом. Если *адрес* совпадает, то *сетевой адаптер* записывает пришедший пакет в свою буферную *память* и сообщает компьютеру (обычно – сигналом аппаратного прерывания) о том, что пришел пакет и его надо читать. Одновременно с записью пакета производится подсчет контрольной суммы, что позволяет к концу приема сделать *вывод*, имеются ли ошибки в этом пакете. *Буферная память* в данном случае опять же позволяет освободить *компьютер* от контроля сети, а также обеспечить высокую степень готовности *сетевого адаптера* к приему пакетов.

Сетевой адаптер выполняет функции первого и второго *уровней модели OSI*

В последнее время все больше встречается компьютеров, в которых *сетевые адаптеры* встроены в системную плату. Достоинства такого подхода очевидны: пользователь не должен покупать *сетевой адаптер* и устанавливать его в компьютер. Достаточно только подключить сетевой кабель к внешнему разъему компьютера. Однако недостаток состоит в том, что пользователь не может выбрать *адаптер* с лучшими характеристиками.

Трансиверы или приемопередатчики (от английского TRANsmitter + reCEIVER) служат для передачи информации между *адаптером* и кабелем сети или между двумя сегментами (частями) сети.

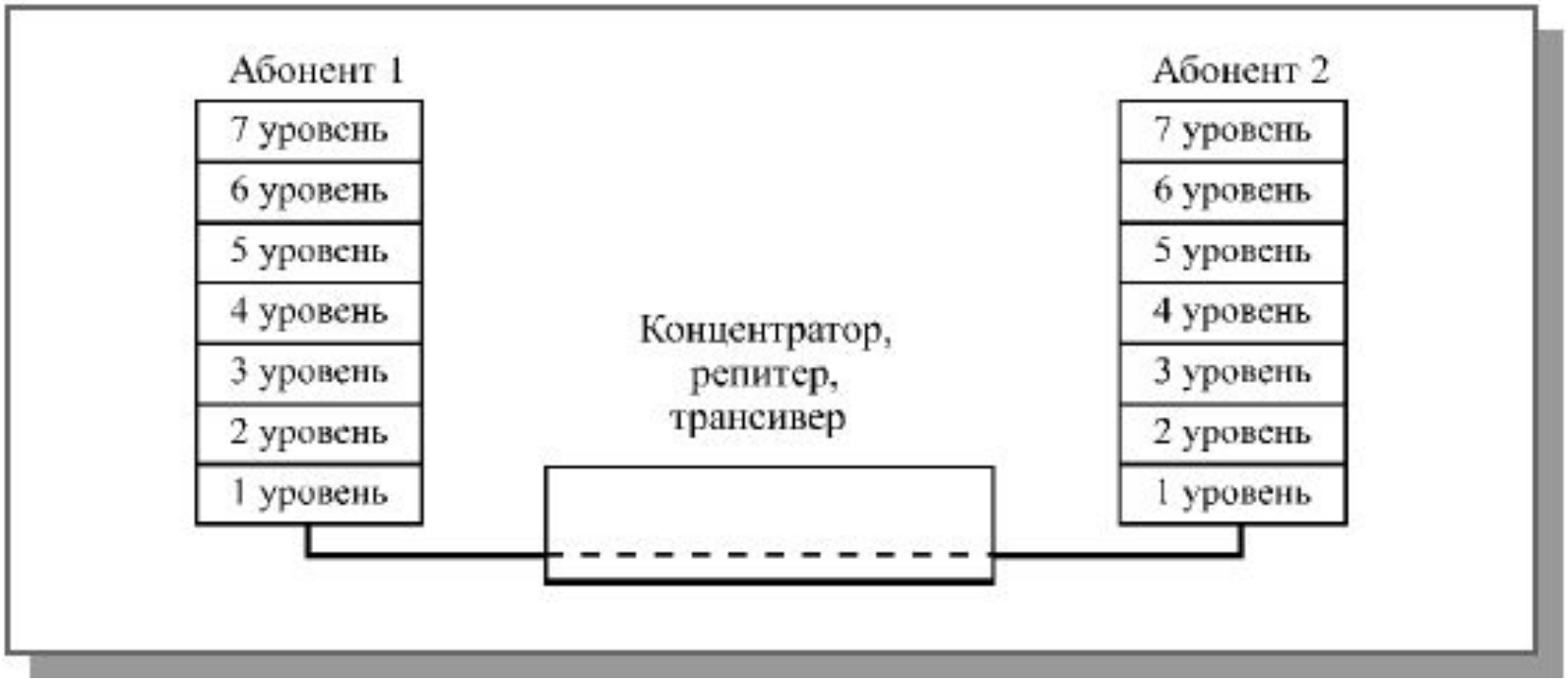
Трансиверы усиливают сигналы, преобразуют их *уровни* или преобразуют сигналы в другую форму (например, из электрической в световую и обратно).

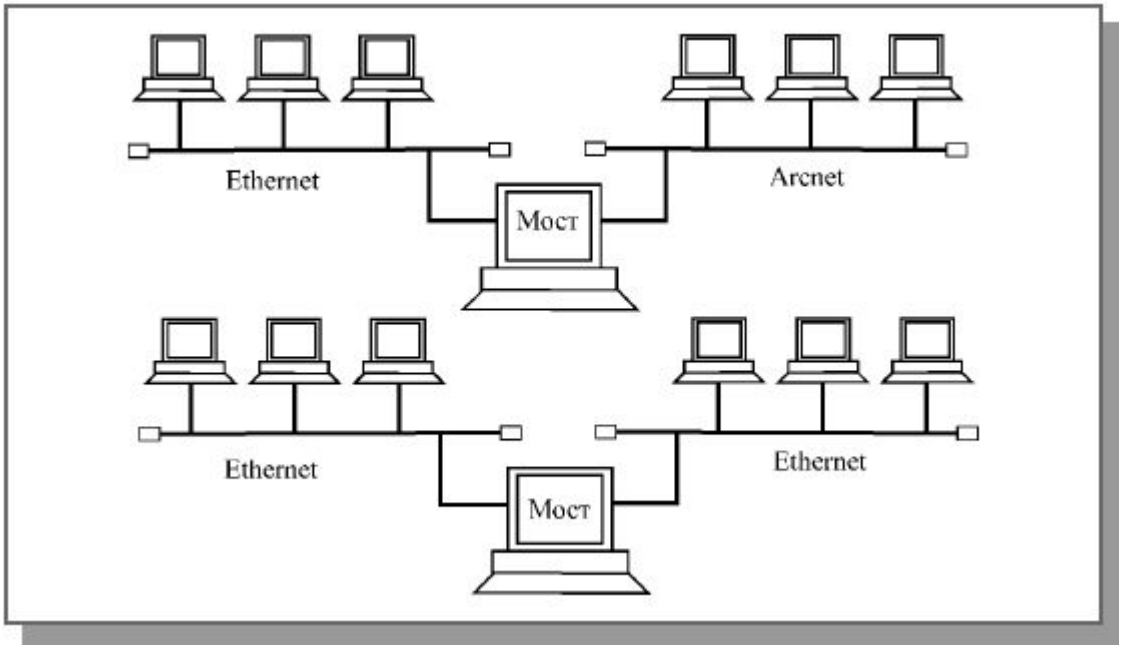
Трансиверами называют встроенные в *адаптер* приемопередатчики.

Репитеры или повторители (repeater) — приборы, как правило, с двумя портами, восстанавливают ослабленные сигналы (их амплитуду и форму), приводя их к исходному виду.

Цель такой ретрансляции сигналов состоит исключительно в увеличении длины сетевого сегмента.

Концентраторы (активный хаб, многопортовый репитер) — приборы с 4-32 портами, применяемые для объединения пользователей в сеть.


Абонент 1
7 уровень
6 уровень
5 уровень
4 уровень
3 уровень
2 уровень
1 уровень
Концентратор,
репитер,
трансивер
Абонент 2
7 уровень
6 уровень
5 уровень
4 уровень
3 уровень
2 уровень
1 уровень

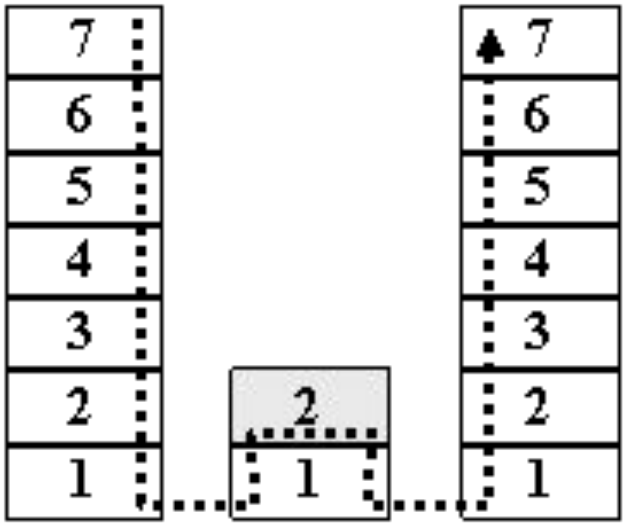


Мосты – наиболее простые устройства, служащие для объединения сетей с разными стандартами обмена, или нескольких сегментов (частей) одной и той же сети, принимают поступающие пакеты целиком и в случае необходимости производят их простейшую обработку.

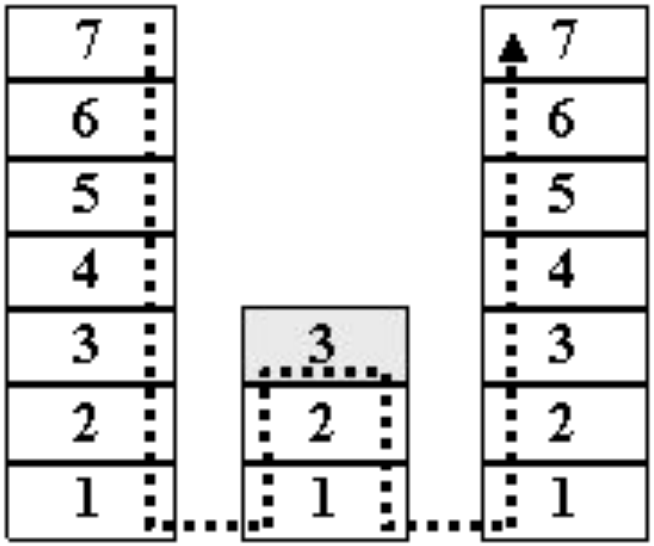
Коммутаторы (свичи, коммутирующие концентраторы, switch, иначе - многопортовый мост), как и концентраторы, служат для соединения сегментов в сеть. Они также выполняют более сложные функции, производя сортировку поступающих на них пакетов.

Коммутаторы передают из одного сегмента сети в другой не все поступающие на них пакеты, а только те, которые адресованы компьютерам из другого сегмента.

При этом сам пакет *коммутатором* не принимается, а только пересылается.

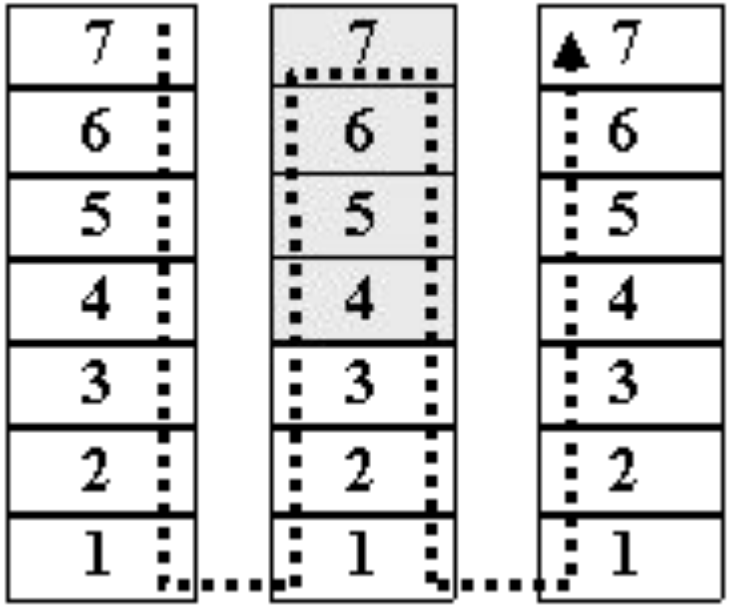


Маршрутизаторы осуществляют выбор оптимального маршрута для каждого пакета с целью избежания чрезмерной нагрузки отдельных участков сети и обхода поврежденных участков, работают на третьем *уровне модели OSI*, так как они анализируют не только MAC-адреса пакета, но и IP-адреса.



Шлюзы – это устройства для соединения сетей с сильно отличающимися протоколами, например, для соединения локальных сетей с большими компьютерами или с глобальными сетями.

Шлюзы реализуют связь между абонентами на верхних *уровнях модели OSI* (с четвертого по седьмой). Соответственно, они должны выполнять и все функции нижестоящих *уровней*.



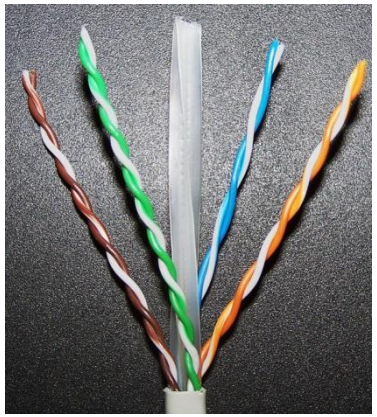
Построение систем доступа на физическом уровне модели OSI

Физический уровень отвечает за транспортировку информации непосредственно через физическую среду передачи.

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи.

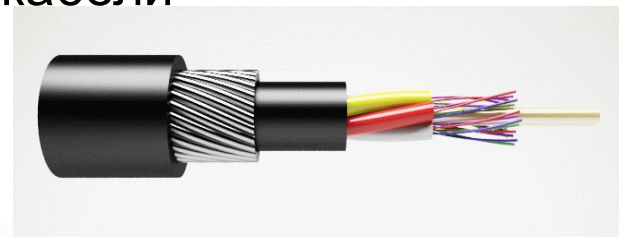
Кабели

- витая пара



- коаксиальные кабели

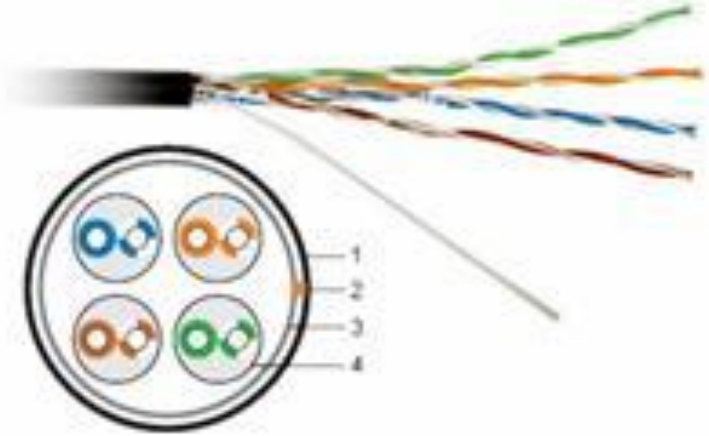
- оптоволоконные кабели



Кабельные каналы связи на основе витых пар

Витая пара (twisted pair) - вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой.

- экранированная витая пара (shielded twisted pair, STP);
- неэкранированная витая пара (unshielded twisted pair, UTP).

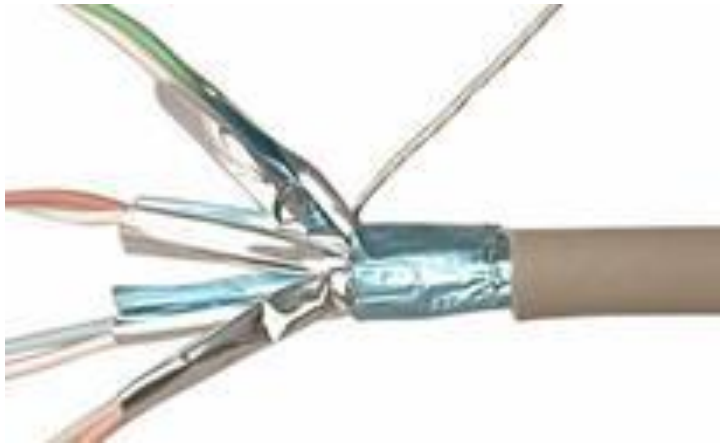


1 - Внешняя оболочка;

2 - Рип-корд;

3 - Защитная пленка;

4 - Витая пара.



Категории витой пары UTP

Обозначение	Полоса частот, МГц	Применение	Примечания
CAT1	0,1	Телефонные и старые модемные линии	1 пара. Используется только для передачи голоса или данных при помощи модема (не подходит для современных систем).
CAT2	1	Старые терминалы	2 пары проводников, старый тип кабеля, поддерживал передачу данных на скоростях до 4 Мбит/с.
CAT3	16	10BASE-T,100BASE-T4, Ethernet, token ring	4-парный кабель, поддерживает скорость передачи данных до 10Мбит/с или 100 Мбит/с по технологии 100BASE-T4 на расстоянии не дальше 100 м.
CAT4	20	token ring, сейчас не используется	4 скрученные пары, скорость передачи данных не превышает 16 Мбит/с по одной паре.
CAT5	100	100BASE-TX Ethernet (LAN, ATM,CDDI)	4-парный кабель, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар.
CAT5e	100	1000Base-T	4-парный кабель. Скорость передач данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар. Самый распространённый, используется для построения компьютерных сетей.
CAT6	250	Fast Ethernet, Gigabit Ethernet	состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 55 м.
CAT6a	500	Gigabit Ethernet (10GBASE-T Ethernet)	состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 100 метров.
CAT7	600	Gigabit Ethernet (10GBASE-T Ethernet)	скорость передачи данных до 10 Гбит/с. Кабель этой категории имеет общий экран и экраны вокруг каждой пары.

Классы сетей Ethernet

В рамках стандарта Ethernet принято различать несколько типов построения распределенной вычислительной системы (классов), отличающихся топологической структурой, используемым оборудованием, типом кабеля, скоростью передачи данных (пропускной способностью линий).

При построении разветвленной локальной сети возможна организация нескольких подсетей, построенных с использованием различных топологий. Применительно к стандарту Ethernet возможна организация локальных сетей с топологией "общая шина" или "звезда".

Каждый из классов сетей Ethernet имеет собственное обозначение, отражающее его технические характеристики. Такое обозначение имеет вид **XBase/BroadY**,
где **X** - пропускная способность сети,
обозначение **Base** или **Broad** говорит о методе передачи сигнала – однополосный (*baseband*) или широкополосный (*broadband*)
Y отображает максимальную длину сегмента сети в сотнях метров, либо обозначает тип используемого в такой системе кабеля, который и накладывает ограничения на максимально возможное расстояние между двумя узлами сети, исходя из собственных технических характеристик.

Например, сеть класса 10Base2 имеет пропускную способность 10 Мбит/с, использует метод передачи данных baseband и допускает максимальную длину сегмента в 200 м.

Разновидности Ethernet-кабеля

В зависимости от скорости передачи данных, и передающей среды существует несколько вариантов технологии. Независимо от способа передачи стек сетевого протокола и программы работают одинаково практически во всех нижеперечисленных вариантах.

10 Мбит/с Ethernet

10BASE5, IEEE 802.3 («Толстый Ethernet») – первоначальная разработка технологии со скоростью передачи данных 10 Мбит/с, использует коаксиальный кабель RG-8, с максимальной длиной сегмента 500 метров.

10BASE2, IEEE 802.3a («Тонкий Ethernet») – использует коаксиальный кабель RG-58, с максимальной длиной сегмента 185 метров. Многие годы этот стандарт был основным для технологии Ethernet.

10BASE-T, IEEE 802.3i — для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории-3 или категории-5. Максимальная длина сегмента 100 метров.

FOIRL (акроним от англ. Fiber-optic inter-repeater link) – базовый стандарт для технологии Ethernet, использующий для передачи данных оптический кабель. Максимальное расстояние передачи данных без повторителя 1 км.

10BASE-F, IEEE 802.3j – основной термин для обозначения семейства 10 Мбит/с ethernet-стандартов, использующих оптический кабель на расстоянии до 2 километров.

10BASE-FL (Fiber Link) – улучшенная версия стандарта FOIRL. Улучшение коснулось увеличения длины сегмента до 2 км.

Разновидности Ethernet-кабеля

Быстрый Ethernet (Fast Ethernet, 100 Мбит/с)

100BASE-T — общий термин для обозначения стандартов, использующих в качестве среды передачи данных витую пару. Длина сегмента до 100 метров. Включает в себя стандарты 100BASE-TX, 100BASE-T4 и 100BASE-T2.

100BASE-TX, IEEE 802.3u — развитие стандарта 10BASE-T для использования в сетях топологии «звезда». Задействована витая пара категории 5, фактически используются только две неэкранированные пары проводников, поддерживается дуплексная передача данных, расстояние до 100 м.

100BASE-T4 — стандарт, использующий витую пару категории 3. Задействованы все четыре пары проводников, передача данных идёт в полудуплексе. Практически не используется.

100BASE-FX — стандарт, использующий многомодовое волокно. Максимальная длина сегмента 400 метров в полудуплексе (для гарантированного обнаружения коллизий) или 2 километра в полном дуплексе.

Разновидности Ethernet-кабеля

Гигабитный Ethernet (Gigabit Ethernet, 1 Гбит/с)

1000BASE-T, IEEE 802.3ab – основной гигабитный стандарт, использует витую пару категории 5e. В передаче данных участвуют 4 пары, каждая пара используется одновременно для передачи по обоим направлениям со скоростью — 250 Мбит/с. Длина сегмента до 100 метров.

1000BASE-TX – спецификация физического уровня дуплексного Ethernet 1000 Мб/с симметричных кабельных систем категории 6. Распространения не получил из-за высокой стоимости кабелей, фактически устарел. Стандарт разделяет принимаемые и посылаемые сигналы по парам (две пары передают данные, каждая на 500 Мбит/с и две пары принимают), что упрощало бы конструкцию приёмопередающих устройств. На основе данного стандарта создано большое количество продуктов для промышленных сетей.

1000BASE-SX, IEEE 802.3z — стандарт, использующий многомодовое волокно в первом окне прозрачности с длиной волны равной 850 нм. Дальность прохождения сигнала составляет до 550 метров.

1000BASE-LH (Long Haul) — стандарт, использующий одномодовое волокно. Дальность прохождения сигнала без повторителя до 100 километров[10].

Разновидности Ethernet-кабеля

10-гигабитный Ethernet (Ethernet 10G, 10 Гбит/с)

Стандарт 10-гигабитного Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN. В настоящее время он описывается поправкой IEEE 802.3ae и должен войти в следующую ревизию стандарта IEEE 802.3.

10GBASE-CX4 – технология 10-гигабитного Ethernet для коротких расстояний (до 15 метров), используется медный кабель CX4 и коннекторы InfiniBand.

10GBASE-SR — технология 10-гигабитного Ethernet для коротких расстояний (до 26 или 82 метров, в зависимости от типа кабеля), используется многомодовое волокно.

10GBASE-LX4 — использует уплотнение по длине волны для поддержки расстояний от 240 до 300 метров по многомодовому волокну. Также поддерживает расстояния до 10 километров при использовании одномодового волокна.

10GBASE-T, IEEE 802.3an-2006 — принят в июне 2006 года после 4 лет разработки. Использует витую пару категории 6 (максимальное расстояние 55 метров) и 6a (максимальное расстояние 100 метров).

Общая характеристика протоколов канального уровня

Спецификация IEEE 802 разделяет канальный уровень на 2 подуровня:

- MAC (Подуровень управления доступом к среде) регулирует доступ к разделяемой физической среде,

- LLC (Подуровень логической передачи данных) обеспечивает обслуживание сетевого уровня, устанавливает виртуальный канал связи. На этом уровне работают коммутаторы, мосты.

Верхний подуровень (***LLC – Logical Link Control***) осуществляет управление логической связью, то есть устанавливает виртуальный канал связи. Функции *подуровня LLC* выполняются программой драйвера *сетевого адаптера*. *Подуровень LLC* отвечает за взаимодействие с *уровнем* 3 (сетевым).

Нижний подуровень (***MAC – Media Access Control***) обеспечивает непосредственный доступ к среде передачи информации (каналу связи). Он напрямую связан с аппаратурой сети. Именно на *подуровне MAC* осуществляется взаимодействие с физическим уровнем. Здесь производится контроль состояния сети, повторная передача пакетов заданное число раз при коллизиях, прием пакетов и проверка правильности передачи.

Формат кадра Ethernet

SFD: Start of frame Delimiter - ограничитель начала кадров

DA: Destination Address - адрес назначения; MAC-адрес получателя

SA: Source Address - адрес источника; MAC-адрес отправителя

L: длина поля данных (для кадра 802.3)

T: тип поля данных (для кадра Ethernet II)

FCS: Frame Check Sequence - контрольная последовательность кадра

Форматы кадров Ethernet

Кадр 802.3/LLC

6	6	2	1	1	1(2)	46–1497 (1496)	4
DA	SA	L	DSAP	SSAP	Control	Data	FCS
			Заголовок LLC				

Кадр Raw 802.3/Novell 802.3

6	6	2	46–1500	4
DA	SA	L	Data	FCS

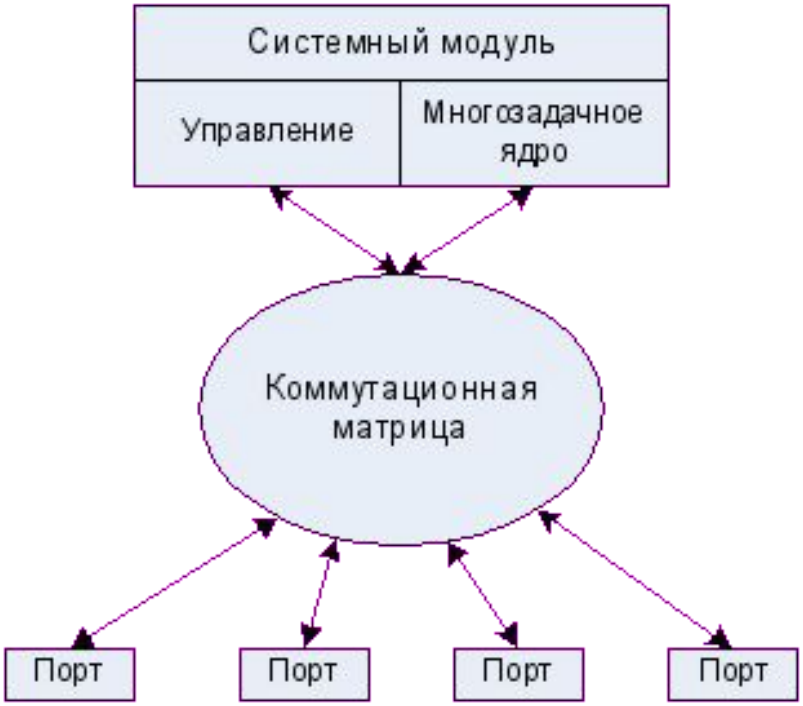
Кадр Ethernet DIX (II)

6	6	2	46–1500	4
DA	SA	T	Data	FCS

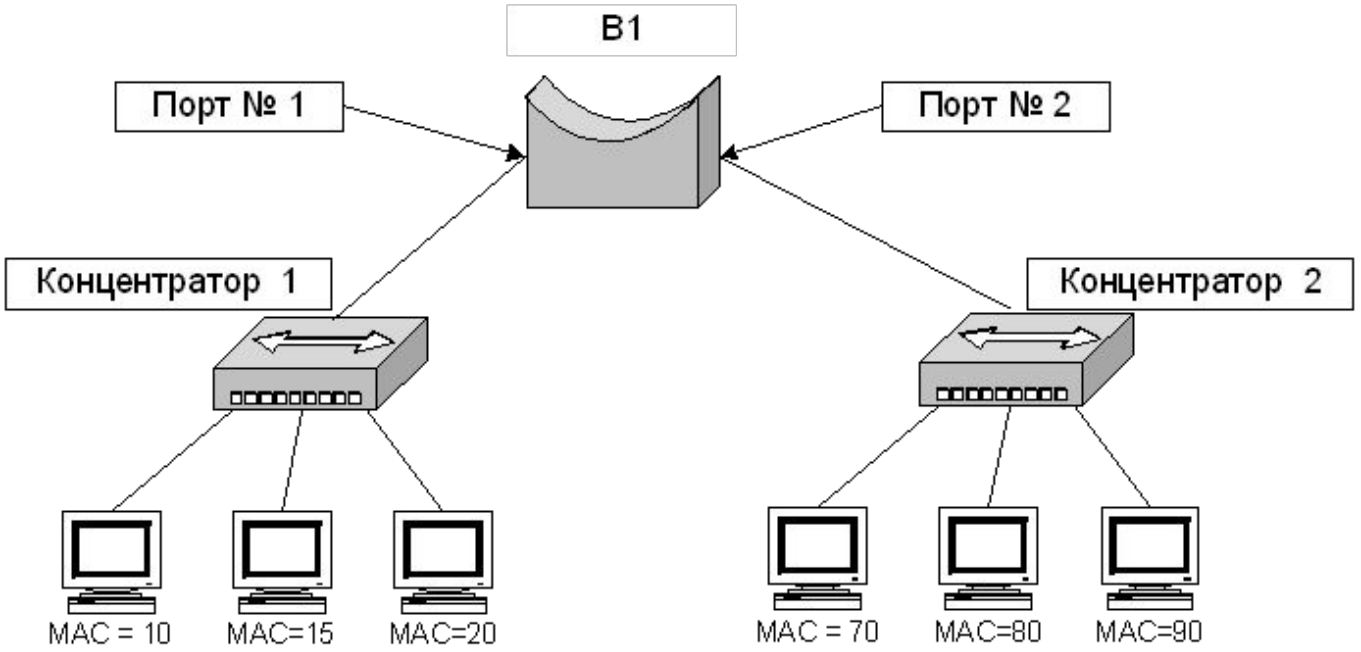
Кадр Ethernet SNAP

6	6	2	1	1	1	3	2	46–1492	4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data	FCS
			AA	AA	03	000000			
			Заголовок LLC			Заголовок SNAP			

Функциональная схема коммутатора EtherSwitch



В этом коммутаторе системный модуль поддерживает общую адресную таблицу коммутатора. Коммутационная матрица отвечает за пересылку кадров между портами. Каждый порт имеет свой процессор кадров. При поступлении кадра в один из портов его процессор отправляет в буфер несколько первых байт, чтобы прочитать адрес назначения. После определения адреса процессор принимает решение о передаче кадра, не анализируя остальные байты. По адресной таблице выбирается соответствующий выходной порт. Коммутационная матрица формирует соединение входного и выходного портов. Если полученный адрес отсутствует в адресной таблице, он записывается в новой строке, а кадр передается методом широкого вещания через все порты, за исключением принявшего.



MAC адрес	Порт
10	1
15	1
20	1
70	2
80	2
90	2

Таблица MAC адресов и портов моста B1 (база данных)

Таблица адресов и портов моста B1

Адресация узлов сети

По количеству адресуемых интерфейсов:

- уникальный адрес (unicast) – для идентификации отдельных интерфейсов;

- групповой адрес (multicast) – для идентификации сразу нескольких интерфейсов, входящих в группу;

- широковещательный адрес (broadcast) – данные направляются всем узлам сети;

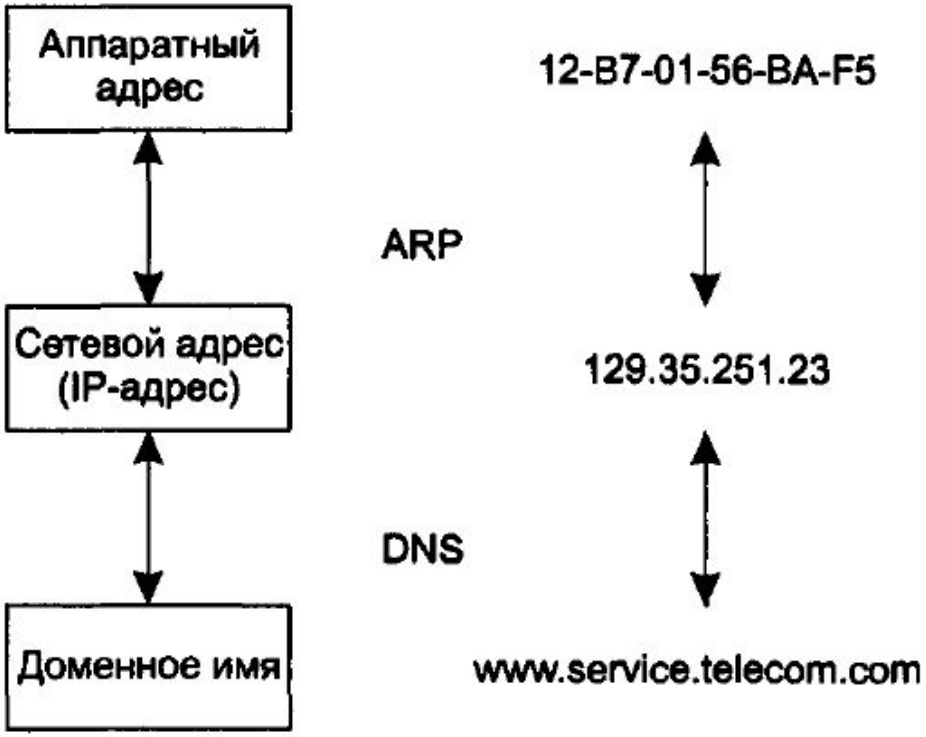
- адрес произвольной рассылки (anycast) – как и групповой адрес, задает группу адресов, но данные должны быть доставлены хотя бы одному из адресов в группе.

Адреса могут быть:

- числовыми (81.1A.FF.FF или 192.134.25.255)

- символьными (site.domen.ru, ftp-arch1.ucl.ac.uk)

Типы адресов стека TCP/IP



- Локальные (аппаратные) адреса
- Сетевые адреса (IP-адреса)
- Символьные (доменные) имена

ARP (Address Resolution Protocol) – протокол разрешения адресов, определяет на основании IP-адреса следующего устройства его локальный адрес (MAC-адрес).

DNS (Domain Name System) – система доменных имен, устанавливает соответствие между доменным именем (символьным именем) и IP-адресом узла на основании создаваемых администраторами сети таблиц соответствия.

Сетевые IP-адреса. Формат IP-адреса

IP-адрес :

- имеет фиксированную длину 4 байта (32 бита)
- состоит из 4-х частей (октетов), записанных в виде десятичных чисел с точками

Каждый октет может принимать значения:
в двоичном виде – от 00000000 до 11111111
в десятичном виде – от 0 до 255

Пример представления IP-адресов:

128.10.2.30

10000000 00001010 00000010 00011110

Подходы к разделению номера сети и номера узла

- **использование фиксированной границы.** 32-битное поле адреса заранее делится на 2 части не обязательно равной, но фиксированной длины, в одной из которых всегда будет размещаться номер сети, в другой – номер узла. Этот подход не нашёл применения, хотя и использовался на начальном этапе существования технологии TCP/IP.

- **использование маски**, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла.

Маска сети – это число, применяемое в паре с IP-адресом, причем двоичная запись маски содержит непрерывную последовательность единиц в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Граница между последовательностями единиц и нулей в маске соответствует границе между номером сети и номером узла в IP-адресе.

Например:

IP-адрес с маской сети:

128.10.2.30/16

Маска сети:

11111111 11111111 00000000 00000000

255.255.0.0

- **использование классов IP-адресов.** Вводятся 5 классов адресов: A, B, C, D, E. Три из них предназначены для адресации сетей, а два – имеют специальное значение. Для каждого класса сетевых адресов определено собственное положение границы между номером сети и номером узла.

Классы IP-адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Возможное число сетей	Возможное число узлов в сети	Маска сети
A	0	1.0.0.0	126.0.0.0	126	2^{24}, 3 байта	255.0.0.0
B	10	128.0.0.0	191.255.0.0	16382	2^{16}, 2 байта	255.255.0.0
C	110	192.0.0.0	223.255.255.0	2097150	2^{8}, 1 байт	255.255.255.0
D	1110	224.0.0.0	239.255.255.255	-	Групповые адреса	255.255.255.255
E	11110	240.0.0.0	247.255.255.255	-	Зарезервировано	-

0.0.0.0 – путь пакетов по умолчанию (default route)

127.0.0.0 – кольцевой адрес или ссылка самого на себя (loopback)

Серые (частные) адреса:

- в классе A – сеть 10.0.0.0;
- в классе B – диапазон из 16 номеров сетей (172.16.0.0 – 172.31.0.0);
- в классе C – диапазон из 255 сетей (192.168.0.0 – 192.168.255.0).

Бесклассовая адресация

Бесклассовая адресация (англ. Classless Inter-Domain Routing – ***CIDR***) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации (использование маски сети).

Число маски показывает, сколько бит в IP-адресе используется под номер сети.

IP-адрес с маской сети: 128.10.2.30/16 – 16 бит в номере сети

Маска сети (16 бит единицы, остальные - нули):

11111111 11111111 00000000 00000000

255.255.0.0

Адрес сети (16 бит IP-адреса оставляем, остальные – номер узла – в нули):

10000000 00001010 00000000 00000000

128.10.0.0

Адрес широковещания (16 бит оставляем, остальные – номер узла – в единицы):

10000000 00001010 11111111 11111111

128.10.255.255

IP-адреса между адресом сети и адресом широковещания можно использовать для адресации хостов.

IPv4 (Интернет протокол версии 4) – определяет основной тип адресов, используемый на сетевом уровне модели OSI, для осуществления передачи пакетов между сетями.

IP-адрес

статический

настраивается вручную системным администратором во время настройки вычислительной сети

динамический

настраивается автоматически с использование специальных протоколов (например, с помощью протокола ***DHCP - протокола динамической настройки хостов***)

Формат заголовка IP

Октет	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31																															
0	Версия				IHL				Тип обслуживания								Длина пакета															
4	Идентификатор																Флаги			Смещение фрагмента											
8	Время жизни (TTL)								Протокол								Контрольная сумма заголовка															
12	IP-адрес отправителя																															
16	IP-адрес получателя																															
20	Параметры от 0-я до 10-и 32-х битовых слов																															
	Данные																															

Версия – для IPv4 значение поля должно быть равно 4

IHL – длина заголовка IP-пакета в 32-битных словах. Это поле указывает на начало блока данных в пакете. Минимальное корректное значение для этого поля равно 5

Тип обслуживания (TOS) – байт, содержащий набор критериев, определяющих тип обслуживания IP-пакетов.

Длина пакета – длина пакета в октетах, включая заголовок и данные. Минимальное корректное значение для этого поля равно 20, максимальное 65535

Идентификатор – значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета. Для фрагментированного пакета все фрагменты имеют одинаковый идентификатор

Флаги (3 бита). Первый бит должен быть всегда равен нулю, второй бит DF (don't fragment) определяет возможность фрагментации пакета и третий бит MF (more fragments) показывает, не является ли этот пакет последним в цепочке пакетов

Смещение фрагмента — значение, определяющее позицию фрагмента в потоке данных

Время жизни (TTL) – число маршрутизаторов, которые должен пройти этот пакет. При прохождении маршрутизатора это число уменьшатся на единицу. Если значения этого поля равно нулю, то пакет должен быть отброшен и отправителю пакета может быть послано сообщение Time Exceeded (ICMP код 11 тип 0)

Протокол — идентификатор интернет-протокола следующего уровня указывает, данные какого протокола содержит пакет, например, TCP или ICMP

Контрольная сумма заголовка — вычисляется в соответствии с RFC 1071

Функции протокола IP:

- осуществление передачи блоков данных (дейтаграмм) от хоста-отправителя, до хоста-назначения, где отправителями и получателями выступают вычислительные машины, однозначно идентифицируемые адресами фиксированной длины (IP-адресами).

- осуществление, в случае необходимости, фрагментации и сбора отправляемых дейтаграмм для передачи данных через другие сети с меньшим размером пакетов;

Недостаток:

ненадежность протокола
(перед началом передачи не устанавливается соединение, не подтверждается доставка пакетов, не осуществляется контроль корректности полученных данных (с помощью контрольной суммы) и не выполняется обмен служебными сообщения с узлом-назначения и не определяется его готовность приема пакетов).

Протокол ICMP (Протокол межсетевых управляющих сообщений) – вспомогательный сетевой протокол стека TCP/IP, использующийся для диагностики и мониторинга сети.

Принцип работы ICMP:

Протокол передает сообщения об ошибках при передаче или исключительных ситуациях, то есть когда маршрутизатор не работает или требуемая услуга недоступна. Не может запросить послать потерянный пакет повторно, просто оповещает о несчастных случаях.

При передаче по сети, сообщения ICMP инкапсулируются в поле данных IP-пакетов.

Сетевая маршрутизация

Маршрутизация (англ. *Routing*) – процесс определения маршрута следования информации в сетях связи.

Маршрутизация в компьютерных сетях выполняется специальными программно-аппаратными средствами — маршрутизаторами; в простых конфигурациях может выполняться и компьютерами общего назначения, которые управляются специальным программным обеспечением.

Маршрутизатором, или **шлюзом**, называется узел сети с несколькими IP-интерфейсами, подключенными к разным IP-сетям, осуществляющий на основе решения задачи маршрутизации перенаправление дейтаграмм из одной сети в другую для доставки от отправителя к получателю.

Задача маршрутизации включает в себя две подзадачи:
- определение маршрута;
- оповещение сети о выбранном маршруте.

Маршрутизация

статическая	динамическая
маршруты задаются администратором	маршруты вычисляются с помощью протоколов маршрутизации (RIP, OSPF

Достоинства статической маршрутизации:

Лёгкость отладки и конфигурирования в малых сетях;

Отсутствие дополнительных накладных расходов (из-за отсутствия протоколов маршрутизации);

Мгновенная готовность (не требуется интервал для конфигурирования/подстройки);

Низкая нагрузка на процессор маршрутизатора;

Предсказуемость в каждый момент времени;

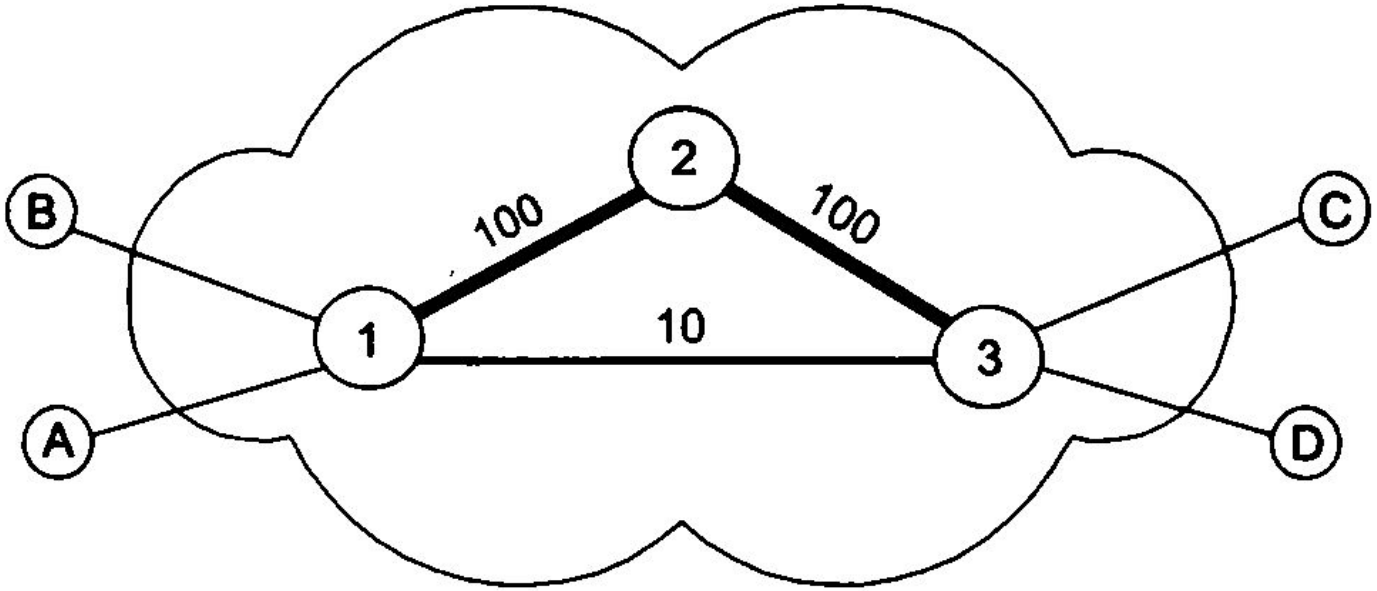
Недостатки статической маршрутизации:

Очень плохое масштабирование (добавление (N+1)-ой сети потребует сделать 2*(N+1) записей о маршрутах, при N>3-4 процесс конфигурирования становится весьма трудоёмким);

Отсутствие динамического балансирования нагрузки;

Необходимость в ведении отдельной документации к маршрутам, проблема

Определение маршрута



Параметр – число транзитных узлов (топология). Оптимальный путь: *A-1-3-C.*

Параметр – пропускная способность (над путями). Оптимальный путь: *A-1-2-3-C.*

Метрика - абстрактный способ измерения степени близости между двумя объектами

Передача информации о маршрутах другим устройствам

После того как маршрут определен (вручную или автоматически), надо оповестить о нем все устройства сети.

Сообщение о маршруте должно нести каждому транзитному устройству примерно такую информацию: «каждый раз, когда в устройство поступят данные, относящиеся к потоку n, их следует передать для дальнейшего продвижения на интерфейс F».

Каждое подобное сообщение о маршруте обрабатывается устройством, в результате создается новая запись в таблице маршрутизации.

В этой таблице локальному или глобальному признаку (признакам) потока (например, метке, номеру входного интерфейса или адресу назначения) ставится в соответствие номер интерфейса, на который устройство должно передавать данные, относящиеся к этому потоку.

Таблица маршрутизации

- электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора

Таблица маршрутизации обычно содержит:

- адрес сети или узла назначения, либо указание, что маршрут является *маршрутом по умолчанию* ***(Network Destination)***

- маску сети назначения ***(Netmask)***

- шлюз, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения ***(Gateway)***

- интерфейс (в зависимости от системы, это может быть порядковый номер, GUID или символьное имя устройства) ***(Interface)***

- метрику — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние) ***(Metric)***

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.10.0	255.255.255.0	192.168.10.4	192.168.10.4	1
192.168.10.4	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.10.255	255.255.255.255	192.168.10.4	192.168.10.4	1
224.0.0.0	240.0.0.0	192.168.10.4	192.168.10.4	1
255.255.255.255	255.255.255.255	192.168.10.4	192.168.10.4	1

Типы записей в таблице маршрутизации:

- маршрут до компьютера (хоста)
- маршрут до сети
- маршрут по умолчанию

Для посылки пакетов поиск адресата происходит в следующей последовательности:

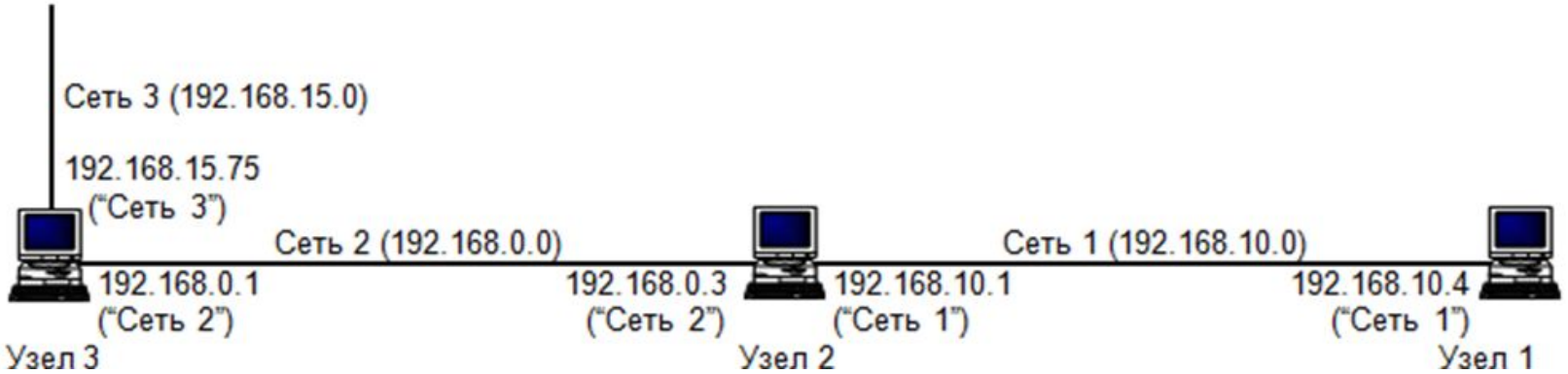
- Поиск с учетом адреса интерфейса.
- Поиск с учетом подсетей.
- Использование Шлюза по умолчанию.

Маршрут к хосту. Это маршрут по IP-адресу конкретного хоста. Маска сети для маршрута этого типа – 255.255.255.255. Наложение такой маски на IP-адрес назначения пакета позволяет проанализировать все разряды IP-адреса назначения и определить IP-адрес конкретного хоста.
Это запись со значением 192.168.10.4 в поле Сетевой адрес.

Маршрут к сети. Маршрутом к сети может быть либо маршрут к непосредственно подключенной сети (192.168.10.0 для примера). Маршрут к непосредственно подключенной сети – это маршрут к сетевому сегменту, к которому подключен интерфейс маршрутизатора (или хоста).

Маршрут по умолчанию. Это маршрут ко всем адресатам, используемый тогда, когда в таблице маршрутизации не обнаруживается никакого маршрута к хосту или маршрута к сети, соответствующего адресату. Маршрут по умолчанию имеет адрес назначения 0.0.0.0 и маску сети 0.0.0.0

Таблица маршрутизации для Узла 1



Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.10.0	255.255.255.0	192.168.10.4	192.168.10.4	1
192.168.10.4	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.10.255	255.255.255.255	192.168.10.4	192.168.10.4	1
224.0.0.0	240.0.0.0	192.168.10.4	192.168.10.4	1
255.255.255.255	255.255.255.255	192.168.10.4	192.168.10.4	1

Чтобы выяснить, соответствует ли IP-адрес назначения передаваемого пакета некоторой записи таблицы маршрутизации, на IP-адрес назначения пакета накладывается содержимое поля Netmask этой записи (выполняется операция логического И). Результат сравнивается со значением в поле Network Destination данной записи. Если результат операции логического И и значение в поле Network Destination совпадают, то IP-адрес назначения пакета соответствует данной записи, и для продвижения пакета используется IP-адрес следующего перехода (содержимое поля Gateway) этой записи.

В первой строке в качестве сетевого адреса указан адрес сети 127.0.0.0. Сеть с таким адресом является внутренней сетью модуля маршрутизации хоста и служит для тестирования программного обеспечения стека TCP/IP в пределах одного хоста.

Чтобы проверить правильность работы программного обеспечения стека TCP/IP на хосте, нужно ввести команду ping с любым IP-адресом, относящимся к сети 127.0.0.0. При выполнении такой команды данные не передаются модулем IP сетевому адаптеру для последующей передачи в сеть, а возвращаются источнику – в локальный модуль IP, т.е. образуется “петля”. Поэтому адрес 127.0.0.0 называется адресом loopback, т.е. адресом замыкания на себя, или адресом программного закольцовывания.

```
C:>\ping 127.255.150.10
Pinging 127.255.150.10 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

Во второй строке в качестве сетевого адреса указан адрес сети 192.168.10.0 . Например, если хост Notebook хочет послать пакет по адресу 192.168.10.1, т.е. на непосредственно подключенный интерфейс соседнего маршрутизатора (хоста 2), то сначала выполняется операция И для адреса 192.168.10.1 и маски сети 255.0.0.0 (из первой строки таблицы маршрутизации).
Результат – 192.0.0.0. Он не совпадает со значением 127.0.0.0, указанным в поле Network Destination первой строки таблицы маршрутизации.

Поэтому для выполнения следующей операции И используется маска сети 255.255.255.0 (из второй строки таблицы маршрутизации).
Результат операции И для адреса 192.168.10.1 и маски сети 255.255.255.0 равен 192.168.10.0. Он совпадает со значением, указанным в поле Network Destination второй строки таблицы маршрутизации.

Поэтому пакет соответствует данной записи таблицы маршрутизации и должен быть направлен по адресу шлюза 192.168.10.4 (в данном случае адрес шлюза совпадает с адресом единственного физического интерфейса хоста, так как маршрут с адресом назначения 192.168.10.1 соответствует непосредственно подключенному сегменту).

В третьей строке столбца “Network Destination” указан адрес хоста 192.168.10.4, являющийся адресом физического интерфейса хоста 1. Это адрес собственного интерфейса хоста 1, при выполнении на этом хосте, например, команды ping по адресу 192.168.10.4 для проверки локального интерфейса пакет эхо-запроса в сеть посылать не надо – ответ должен быть получен от внутреннего модуля IP. Поэтому в качестве адреса шлюза и интерфейса в третьей строке таблицы маршрутизации указаны значения 127.0.0.1.

В четвертой строке столбца “Network Destination” указан адрес 192.168.10.255. Это широковещательный адрес для сети 192.168.10.0. Запись с таким адресом нужна хосту (маршрутизатору) для того, чтобы он знал, через какой интерфейс передавать широковещательные пакеты с адресом назначения 192.168.10.255.

В пятой строке столбца “Network Destination” указан адрес 224.0.0.0. Это адрес класса D, т.е. групповой адрес. Запись с таким адресом нужна хосту (маршрутизатору) для того, чтобы он знал, через какой интерфейс передавать пакеты с групповым адресом назначения, начинающимся с 224, например, с адресом 224.0.0.9. Такой адрес назначения имеют пакеты рассылки маршрутной информации RIP версии 2, предназначенные всем маршрутизаторам RIP версии 2, находящимся в сетевом сегменте, подключенном к интерфейсу, с которого посылаются эти пакеты.

В шестой строке столбца “Network Destination” указан адрес 255.255.255.255. Запись с таким адресом нужна хосту для того, чтобы он знал, через какой интерфейс передавать широковещательные пакеты с адресом назначения 255.255.255.255. Пакеты с таким адресом назначения рассылаются всем узлам, находящимся в той же сети, что и их источник. В качестве примера таких пакетов можно указать пакет DHCP-поиска (DHCP Discover), посылаемый клиентом DHCP при загрузке, для обнаружения сервера DHCP с целью запроса у него IP-адреса.