

Теория сети





Модель OSI. Из истории...

В течение последних десятилетий наблюдался значительный рост глобальных сетей. Новые технологии и продукты внедрялись сразу после их появления, и поэтому многие сети были сформированы с использованием различных аппаратных и программных средств. Многие сети оказались несовместимыми и стало сложным организовывать обмен информацией между компьютерами, использующими различные сетевые спецификации. Компании начали испытывать трудности от развития сетей. Становилось всё сложнее объединять сети, использующие разные спецификации и исполнения. Стало понятно - пора прекращать закрытое использование сетевых систем – систем, которые отдельно развиваются, используются и управляются.

Закрытость системы значит, что только одна компания или маленькая группа компаний контролирует всё использование технологии.

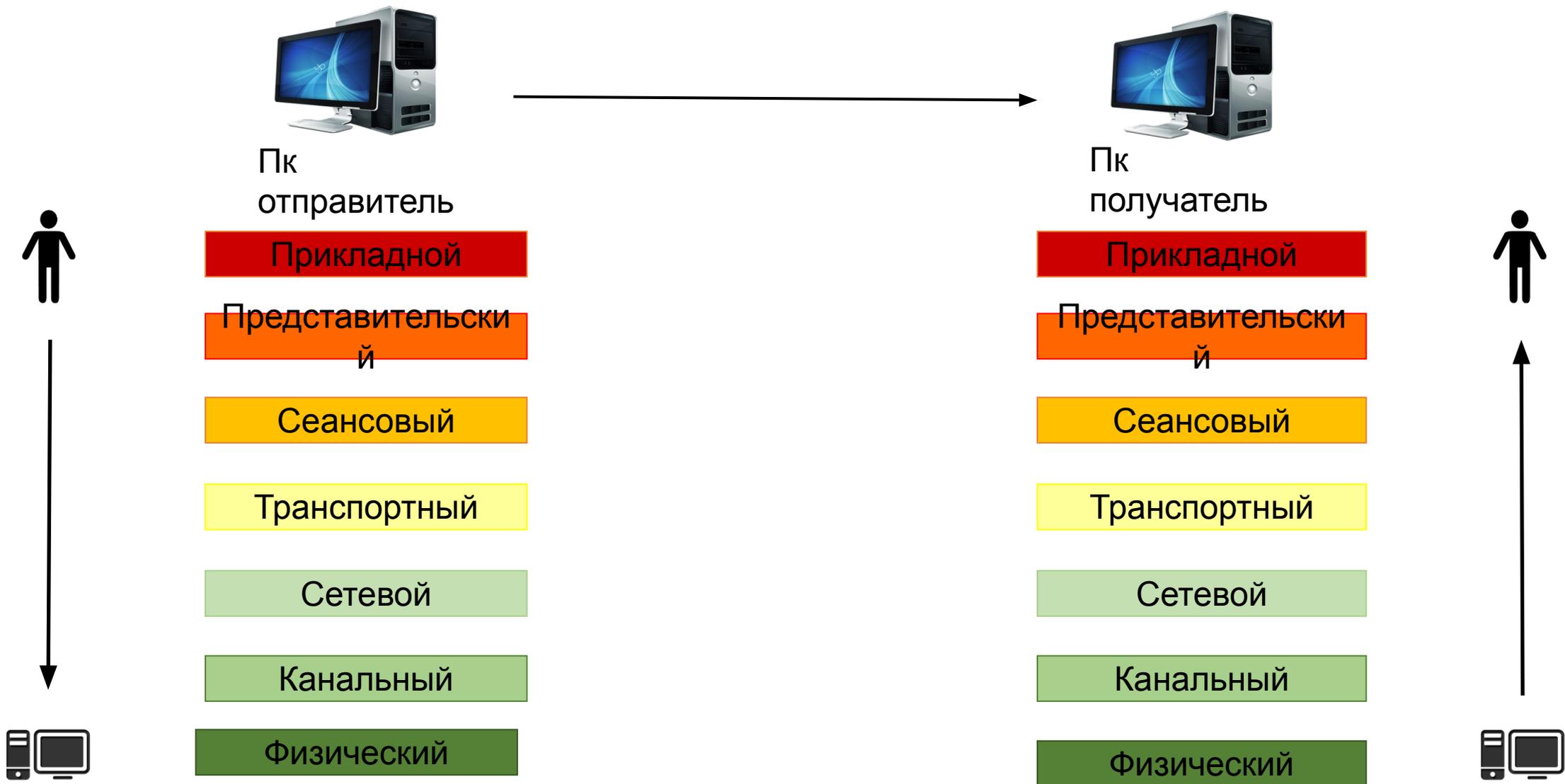
Открытость системы означает, что она доступна для использования любому желающему.

Для решения проблемы **Международная Организация Стандартизации** создала **модель OSI**, которая должна способствовать созданию совместимых сетевых технологий. Модель OSI снабдила разработчиков набором стандартов, обеспечивающих совместимость и способность соединения различных типов сетей разработанных разными компаниями по всему миру.

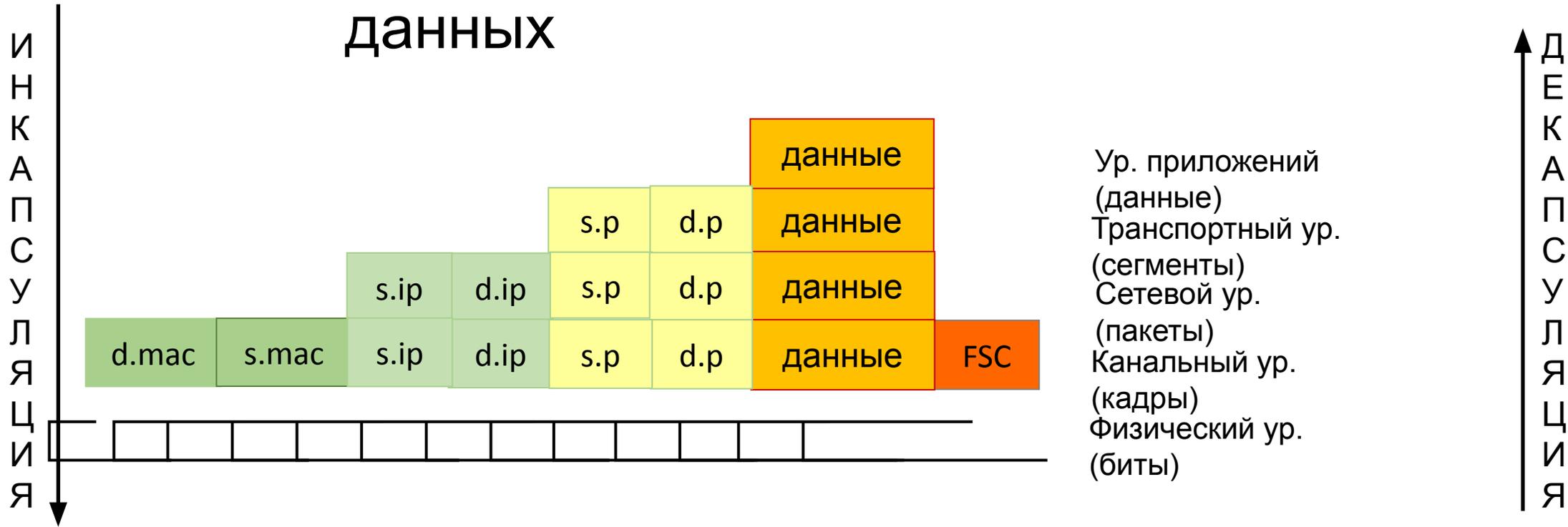
Модель OSI способствует пониманию, как информация путешествует по сети. Если смотреть глубже, модель OSI описывает, как данные путешествуют от одного приложения пользователя, через сетевые коммуникации, к



OSI (англ. *open systems interconnection basic reference model*) – это модель взаимодействия открытых систем. Данная модель делит сетевое взаимодействие на 7 уровней.



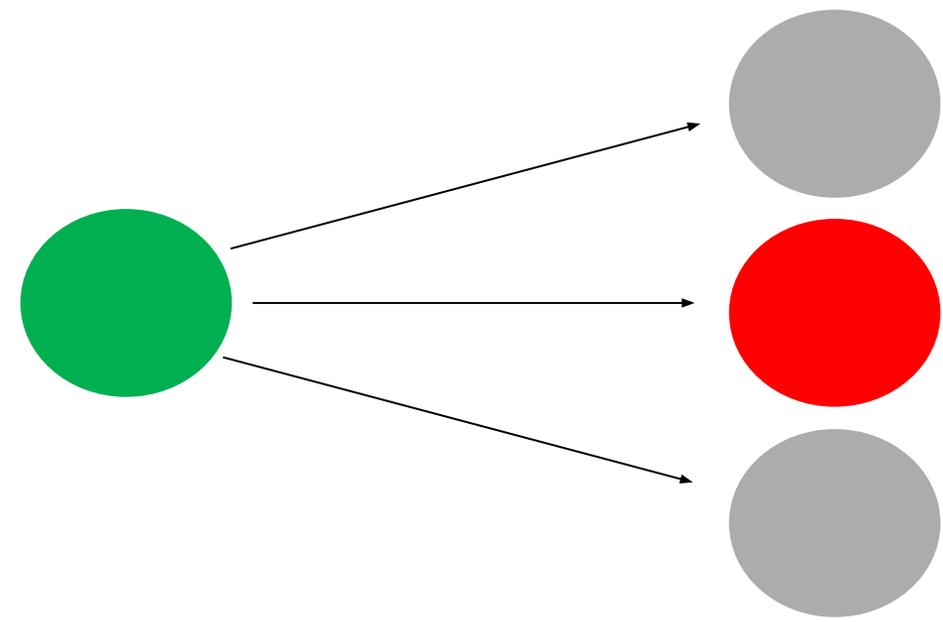
Инкапсуляция и декапсуляция данных



Декапсуляция – процесс обработки данных и их представление в виде влант (оптоволоконных/оптоволоконных) радиосигналов в виде сетевых данных по сетевой физической среде (витая пара, оптическое волокно, Wi-Fi, и др.). Причём на каждом уровне различные протоколы добавляют к передающимся данным свою информацию.

* source - отправитель; destination -

Типы трафика по критерию «Адрес Назначения»



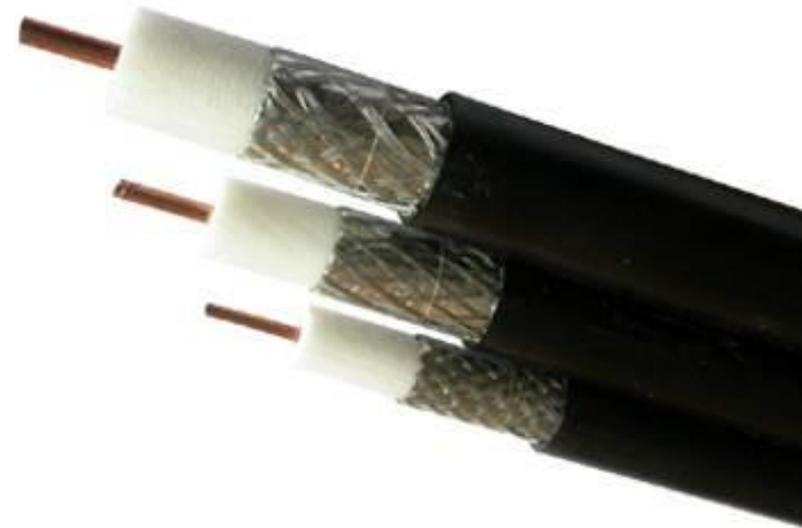
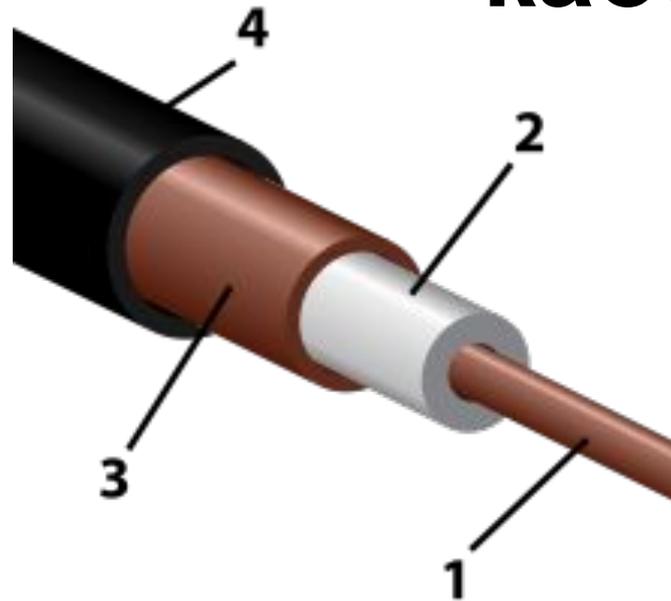
Физический уровень

— это **первый** уровень сетевой модели OSI. На данном уровне передается сигнал через различные среды передачи данных.

Единица измерения, используемая на этом слое — **Биты**.

То есть физический уровень осуществляет передачу потока битов по соответствующей физической среде через соответствующий интерфейс.

Коаксиальный кабель



Устройство коаксиального кабеля

- 1 — внутренний проводник
- 2 — изоляция (сплошной полиэтилен)
- 3 — внешний проводник
- 4 — оболочка

BNC- коннектор



Подтипы BNC

BNC — либо припаивается, либо обжимается на конце кабеля.

BNC-F — с резьбовым креплением.

BNC-T (*T-коннектор*) — соединяет сетевой кабель с сетевой платой компьютера в стандарте 10BASE2.

BNC-I и **BNC-баррел** (*I-коннектор*) — применяются для сращивания двух отрезков тонкого коаксиального кабеля.

TNC- коннектор



TNC-коннектор (Threaded Neill-Concelman) — версия BNC-коннектора с резьбой.

Витая пара

(англ. 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.



RJ-4

5

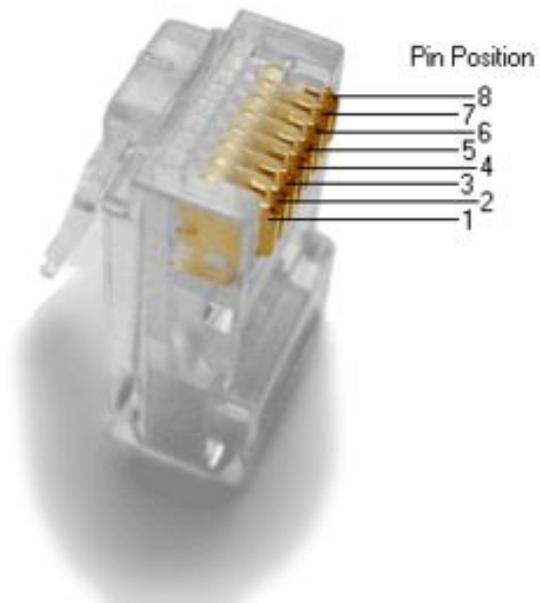
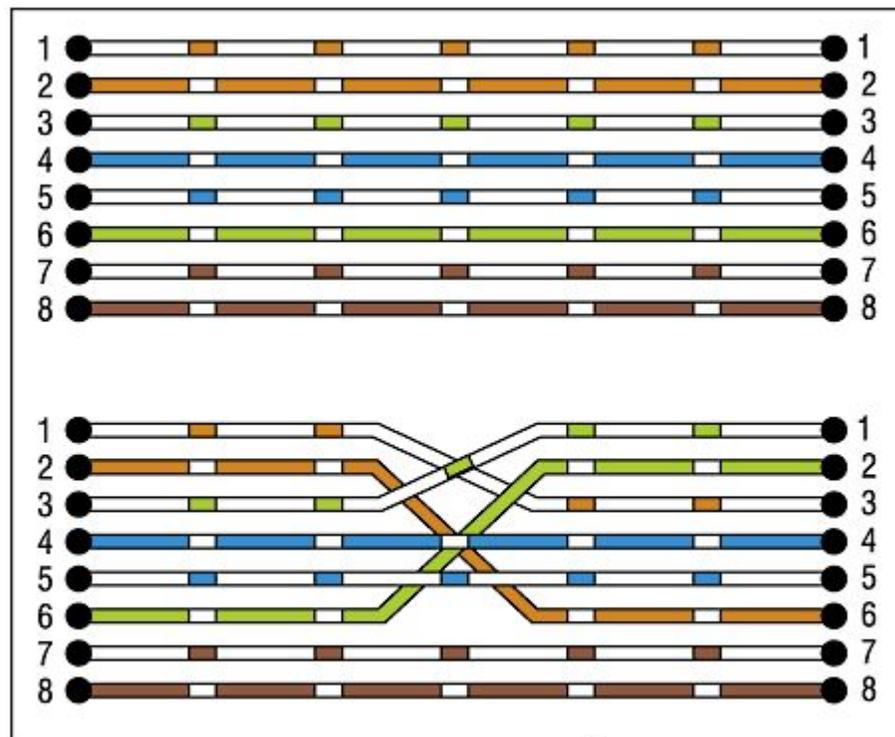


Рис.1



Коммутационные шнуры: «прямой» и Crossover

Рис.2

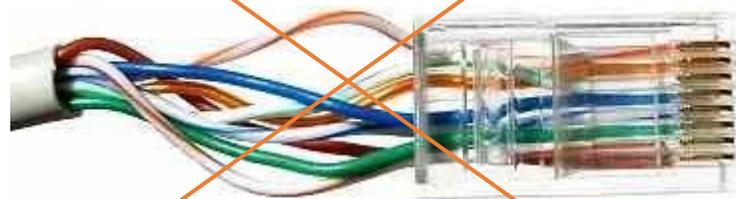


Рис.3

**Правильно
обжат**



**Неправильно
обжат**



На примере справа оставлены слишком длинные жилы, из-за чего расстояние от коннектора до оплетки остается незащищенным. Также кабель теряет прочность.

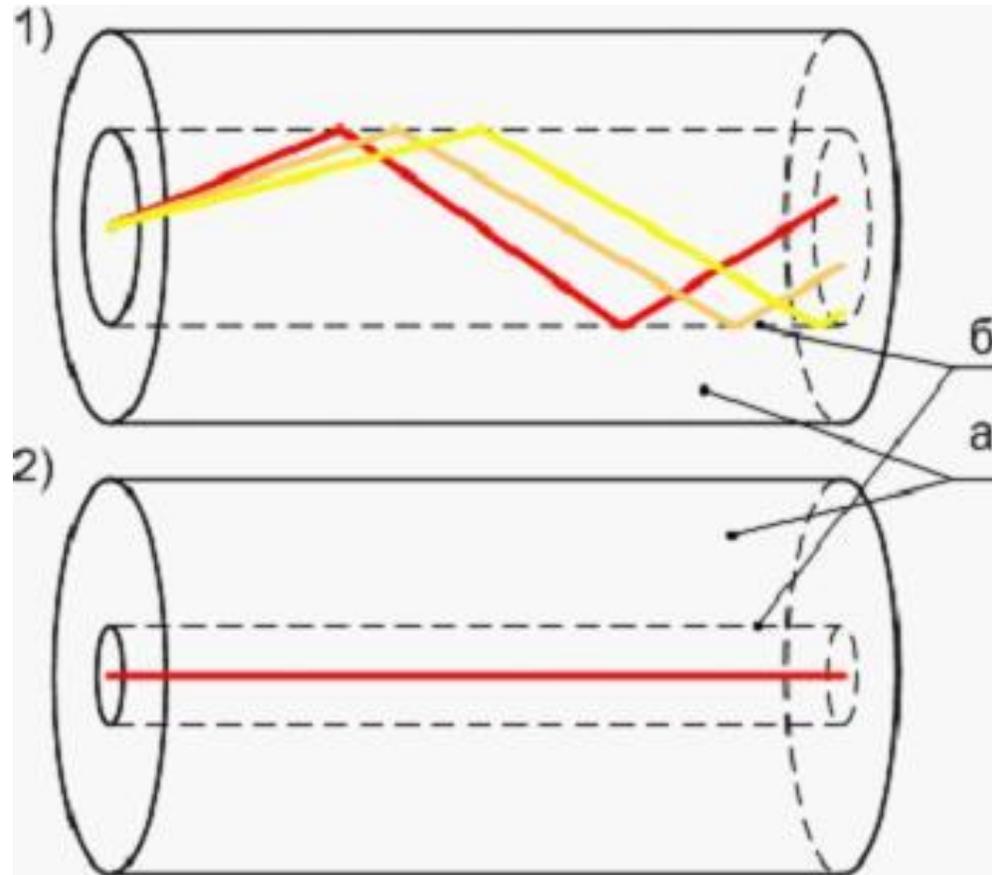
ОПТОВОЛОК НО



ОПТОВОЛОК НО

1)
МНОГОМОДОВОЕ

2)
ОДНОМОДОВОЕ



Соединение волоконно-оптического кабеля

Широко применяется три способа монтажа оптоволоконна:

- 1) сварка оптических волокон:
- 2) соединение при помощи механических разъемов
- 3) соединение при помощи сплайса.

Модуль SFP

Модули SFP используются для присоединения платы сетевого устройства (коммутатора, маршрутизатора или подобного устройства) к оптическому волокну или неэкранированной витой паре, выступающих в роли сетевого кабеля.



LinkSys 100 Base-FX Mini-GBIC SFP
Трансивер



Устройства физического уровня

Повторитель

Повторитель (репiтер, от англ. *repeater*) — сетевое оборудование. Предназначен для увеличения расстояния сетевого соединения путём повторения электрического сигнала «один в один». Бывают однопортовые повторители и многопортовые. В терминах модели OSI работает на физическом уровне.



Концентратор

Сетевой концентратор или хаб (жарг. от англ. *hub* — центр деятельности) — сетевое устройство, предназначенное для объединения нескольких устройств Ethernet в общий сегмент сети. Устройства подключаются при помощи витой пары, коаксиального кабеля или оптоволокна.

Концентратор работает на физическом уровне сетевой модели OSI, повторяет входящий на один порт сигнал на все активные порты. В случае поступления сигнала на два и более порта одновременно возникает коллизия, и передаваемые кадры данных теряются.



Канальный уровень

— это второй уровень сетевой модели OSI. Он предназначен для передачи данных узлам, находящимся в том же сегменте локальной сети. Также может использоваться для обнаружения и, возможно, исправления ошибок, возникших на физическом уровне.

Единица измерения, используемая на этом уровне — **Кадр (фрейм)**.

MAC- адрес

MAC-адрес (от англ. *Media Access Control* — управление доступом к среде, также **Hardware Address**) — это уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей.

MAC-адреса формируют основу сетей на канальном уровне, которую используют протоколы более высокого (сетевоего) уровня.

MAC-адрес

Стандарты IEEE определяют 48-разрядный (6 октетов) MAC-адрес, который разделен на четыре части.

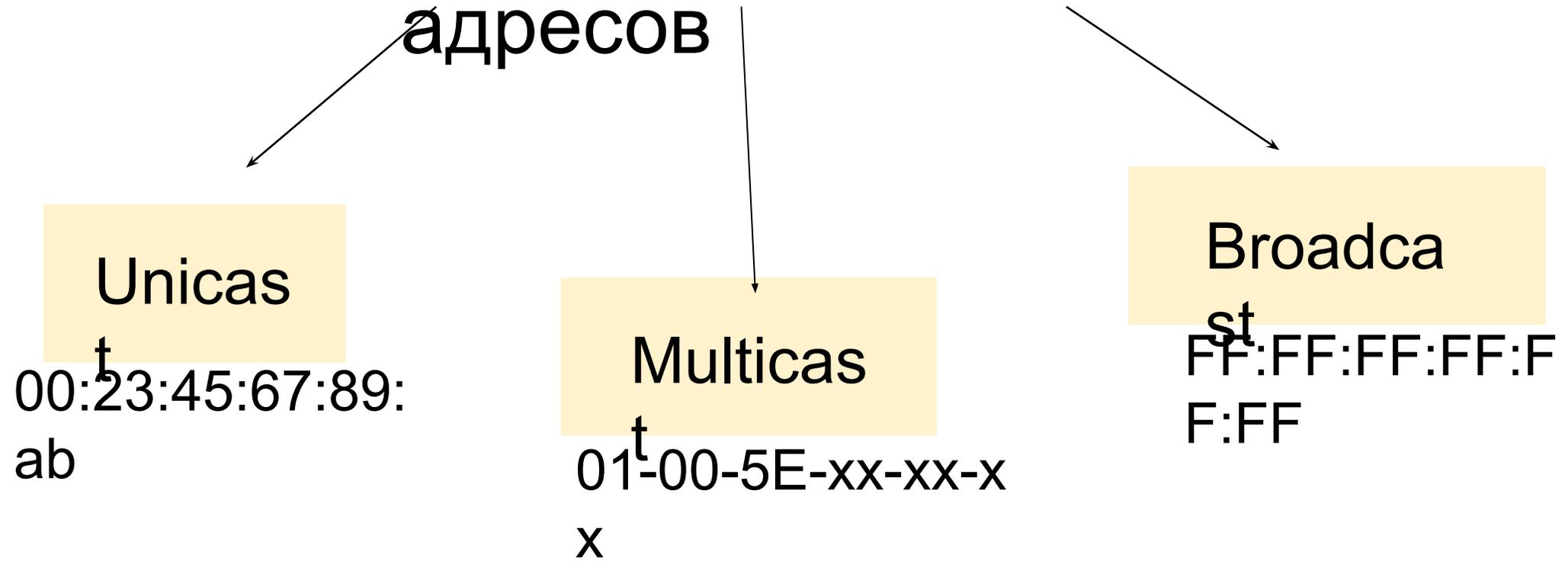
Первые 3 октета содержат 24-битный уникальный идентификатор организации (OUI), или (Код MFG — Manufacturing, производителя), который производитель получает в IEEE. При этом используются только младшие 22 разряда (бита), 2 старшие имеют специальное назначение:

- первый бит указывает, для одиночного (0) или группового (1) адресата предназначен кадр
- следующий бит указывает, является ли MAC-адрес глобально (0) или локально (1) администрируемым.

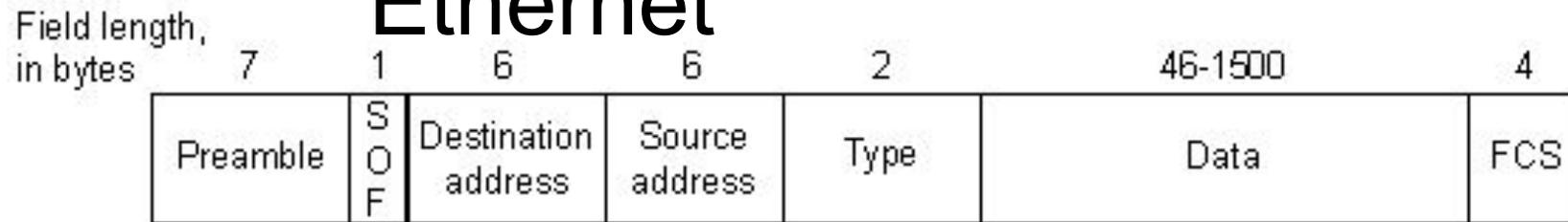
Следующие три октета выбираются изготовителем для каждого экземпляра устройства.



Виды MAC-адресов



Формат кадра Ethernet

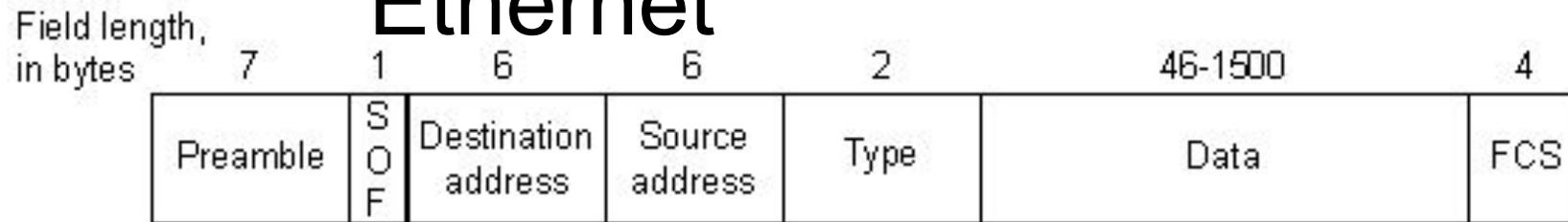


Поля "Преамбула" и "Признак начала кадра" предназначены для синхронизации отправителя и получателя. Преамбула представляет собой 7 - байтовую последовательность единиц и нулей. Поле признака начала кадра имеет размер 1 байт. Эти поля не принимаются в расчёт при вычислении длины кадра.

Поле "Адрес получателя" состоит из 6 байт и содержит физический адрес устройства в сети, которому адресован данный кадр. Значения этого и следующего поля являются уникальными.

Поле "Адрес отправителя" состоит из 6 байт и содержит физический адрес устройства в сети, которое отправило данный кадр.

Формат кадра Ethernet



Поле "Длина/тип" может содержать длину или тип кадра в зависимости от используемого кадра Ethernet. Если поле задаёт длину, она указывается в двух байтах. Если тип - то содержимое поля указывает на тип протокола верхнего уровня, которому принадлежит данный кадр. Например, при использовании протокола IPX поле имеет значение 8137, а для протокола IP - 0800.

Поле "Данные" содержит данные кадра. Чаще всего - это информация, нужная протоколам верхнего уровня. Данное поле не имеет фиксированной длины.

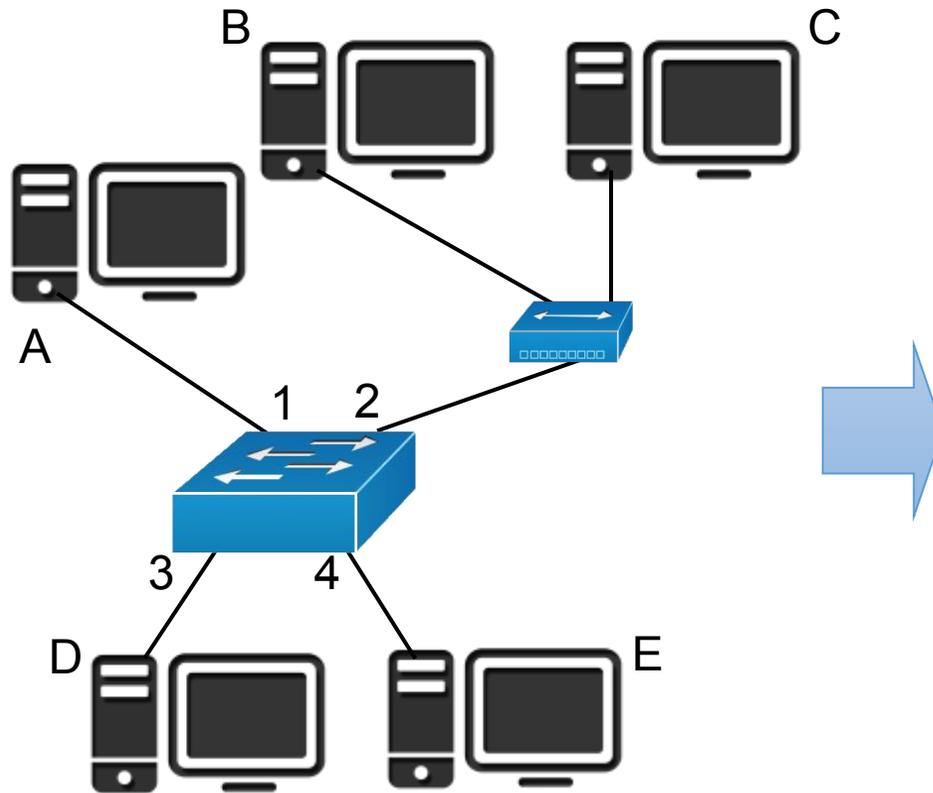
Поле "Контрольная сумма" содержит результат вычисления контрольной суммы всех полей, за исключением преамбулы, признака начала кадра и самой контрольной суммы. Вычисление выполняется отправителем и добавляется в кадр. Аналогичная процедура вычисления выполняется и на устройстве получателя. В случае, если результат вычисления не совпадает со значением данного поля, предполагается, что произошла ошибка при передаче. В этом случае кадр считается испорченным и игнорируется.

Коммутатор

Сетевой коммутатор (жарг. **свич**, **свитч** от англ. *switch* — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю, исключение составляет широковещательный трафик (на MAC-адрес FF:FF:FF:FF:FF:FF) всем узлам сети. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.



Таблица КОММУТАЦИИ



Порт	MAC - адрес
1	A
2	B
2	C
3	D
4	E

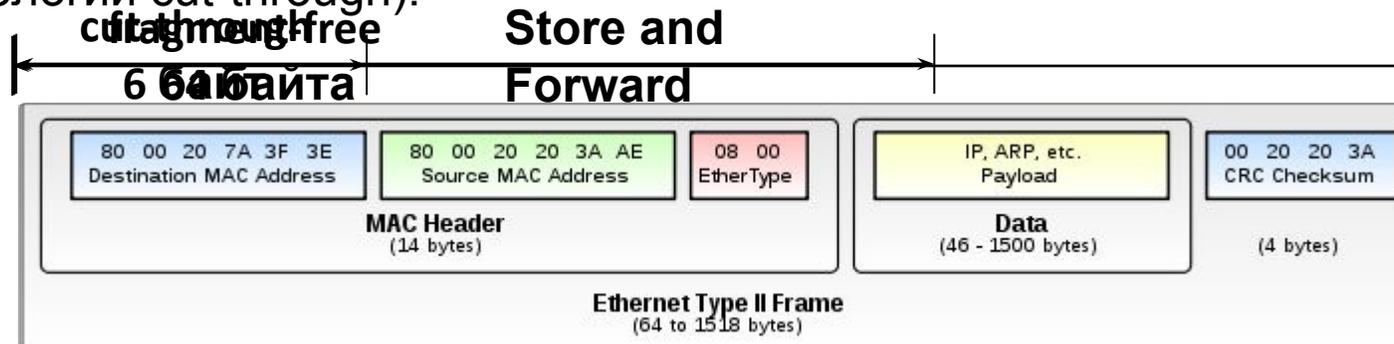
Режимы

КОММУТАЦИИ

Существует три способа коммутации. Каждый из них — это комбинация таких параметров, как время ожидания и надёжность передачи.

Безпротокольный (store-and-forward) (Store and Forward).

Коммутатор проверяет каждый кадр перед передачей. В отсутствие ошибок, выявляемых с помощью технологии full-duplex (кадровый размер 64 байта) обработка обнаружена ошибок (store-and-forward, остальные по технологии cut-through).



Сетевой уровень

— это третий уровень сетевой модели OSI. Предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов (ip) и имён в физические (MAC), определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и заторов в сети.

Единица измерения, используемая на этом слое — **Пакет**.

IPv

4

Ip –адрес – это уникальный адрес любого устройства, находящегося в компьютерной сети. Если проводить аналогию, у каждого из нас есть адрес, где мы проживаем и чтобы доставить нам письмо, почтальон идет четко на тот адрес, который указан в письме и информация доходит именно до того, кому предназначалась. Так же и в компьютерных сетях, ip – адрес, это адрес устройства в этой сети на который ему доставляется информация.

IPv4 использует 32-битные (четырёхбайтные) адреса, ограничивающие адресное пространство 4 294 967 296 (2^{32}) возможными уникальными адресами.

Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками, например, *192.168.0.1*. (или *128.10.2.30* — традиционная десятичная форма представления адреса)

Форма записи	Пример
Десятичная с точками	192.168.0.22
Двоичная с точками	11000000.10101000.00000000.00010110

Маска

подсети

- это битовая маска, которая показывает, какая часть ip-адреса относится к адресу сети, а какая часть к адресу самого узла в этой сети.

Дано

IP-адрес:

192.168.123.132

Маска: Адрес

255.255.255.0

Решени

e:

192.168.123.13	11000000.10101000.01111	0000000
2	011.111111.1111111.1111	0000000
255.255.255.0	1111.	0

11000000.10101000.01111011.00000000 – адрес подсети (192.168.123.0)

11000000.10101000.01111011.11111111 – Broadcast-адрес
(192.168.123.255)

Классовая адресация

Класс	Первый байт (2)	Первый байт (10)	Адреса хостов	Маска
A	0xxxxxx	1 – 127	10.0.0.1 – 126.255.255.254	255.0.0.0
B	10xxxxxx	128-191	128.0.0.1 – 191.255.255.254	255.255.0.0
C	110xxxxx	192 – 223	192.0.0.1 – 223.255.255.254	255.255.255.0

Класс A	0	адрес сети (7 бит)	адрес хоста (24 бита)
Класс B	10	адрес сети (14 бит)	адрес хоста (16 бит)
Класс C	110	адрес сети (21 бит)	адрес хоста (8 бит)
Класс D	1110	Адрес многоадресной рассылки	
Класс E	1111 ^[1]	Зарезервировано	

Бесклассовая

адресация

(англ. *Classless Inter-Domain Routing*, англ. *CIDR*) — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

11111111.11111111.11111111.00000000

255.255.255.0

11111111.11111111.11111111.11100000

255.255.255.224

Виды IP-адресов

Broadcast

Глобально
255.255.255.255

Локально
последний ip-адрес подсети
Например 10.1.1.255 (подсеть 10.1.1.0/24)

Multicast

Все IP-адреса из класса D
224.0.0.0 –
239.255.255.255

Unicast

Любой ip-адрес из любой подсети, который присваивается ПК в этой сети.
Например: 10.1.1.2

Статический и динамический ip-адреса

Статический - это когда за вашим компьютером привязан конкретный IP-адрес.

Динамический - это когда при включении компьютер получает произвольный IP-адрес из диапазона, определенного провайдером.

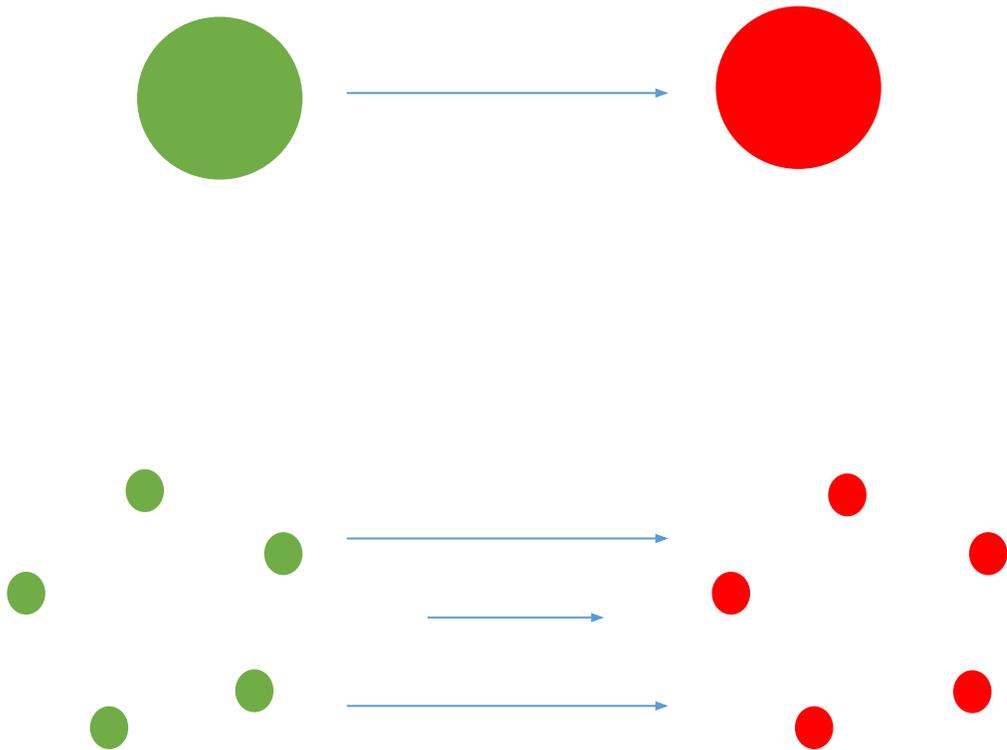
Серые и белые ip-адреса

Белый - это уникальный IP-адрес в интернете.

Серый - это внутренний IP локальной сети, напрямую доступный только внутри этой сети.

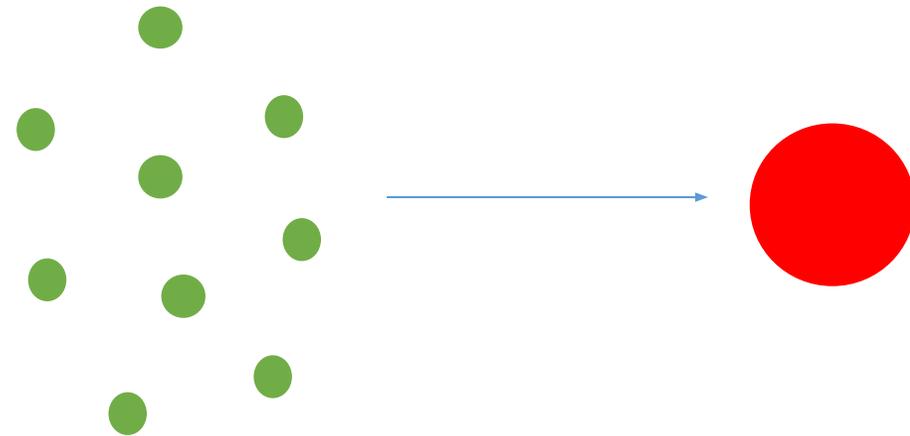
NAT

(Network Address Translation)



PAT

(Port Address Translation)



Протокол DHCP

- сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер».

- Клиент DHCP:

Компьютер, который получает IP-адрес автоматически;

- Сервер DHCP:

Компьютер, который обеспечивает назначение IP-адресов;

Ведет таблицу выданных IP-адресов, чтобы избежать дублирования.

Клиент и сервер обмениваются сообщения DHCP в режиме **запрос-ответ**.

Процесс получения IP-адреса по DHCP



DHCP
server



Процесс получения IP-адреса по DHCP

1. Обнаружение DHCP

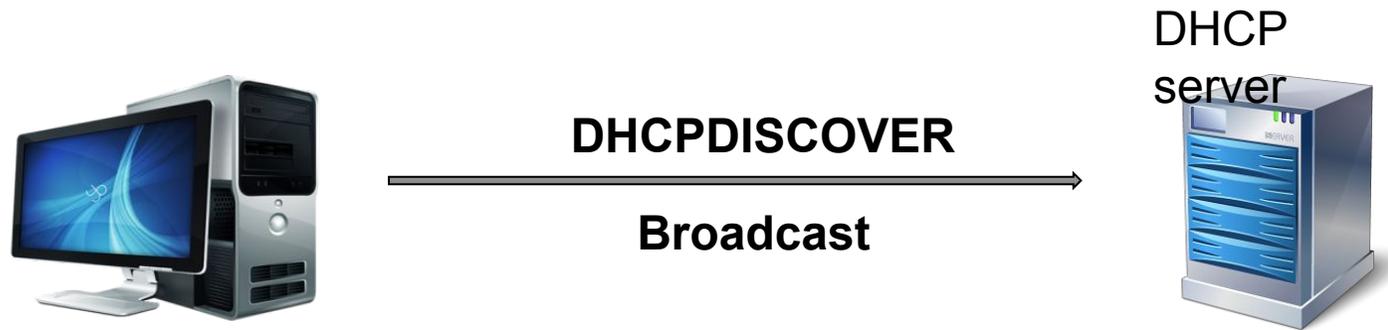


DHCP
server



Процесс получения IP-адреса по DHCP

1. Обнаружение DHCP



Клиент выполняет широковещательный (Broadcast) запрос по всей физической сети с целью обнаружить доступные DHCP-серверы.

Процесс получения IP-адреса по DHCP

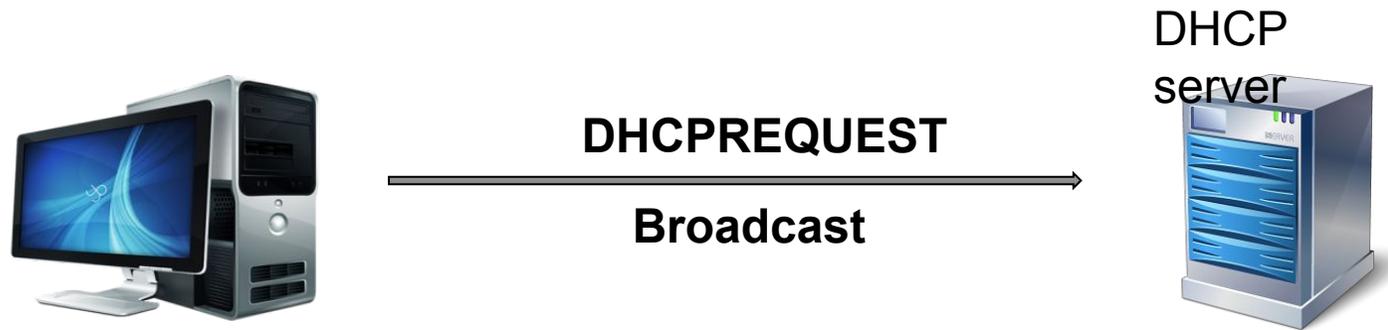
2. Предложение DHCP



Получив сообщение от клиента сервер отправляет ответ (DHCPOFFER), в котором предлагает конфигурацию.

Процесс получения IP-адреса по DHCP

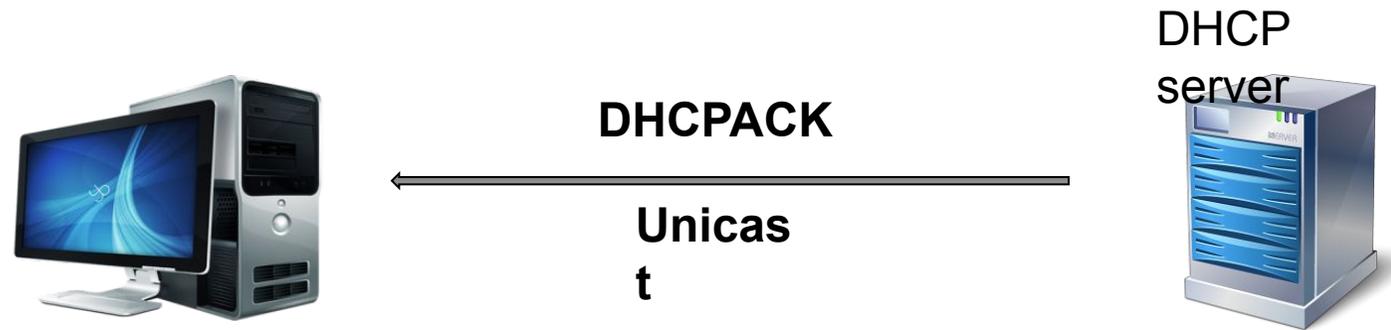
3. Запрос DHCP



Выбрав одну из конфигураций, предложенных DHCP-серверами, клиент отправляет запрос DHCP (DHCPREQUEST).

Процесс получения IP-адреса по DHCP

4. Подтверждение DHCP



Наконец, сервер подтверждает запрос и направляет это подтверждение (DHCPACK) клиенту.

Процесс получения IP-адреса проще всего запомнить через аббревиатуру:

DHCP**D**ISCOVER

DHCP**O**FFER

DHCP**R**EQUEST

DHCP**A**CK

Маршрутизатор

ор

(он же роутер) устройство, которое передает данные между различными сетями, например сетью интернет провайдера и домашней локальной сетью. Маршрутизатор также имеет разъемы для подключения к нему посредством кабеля других устройств, например компьютеров, модемов или сетевого коммутатора.

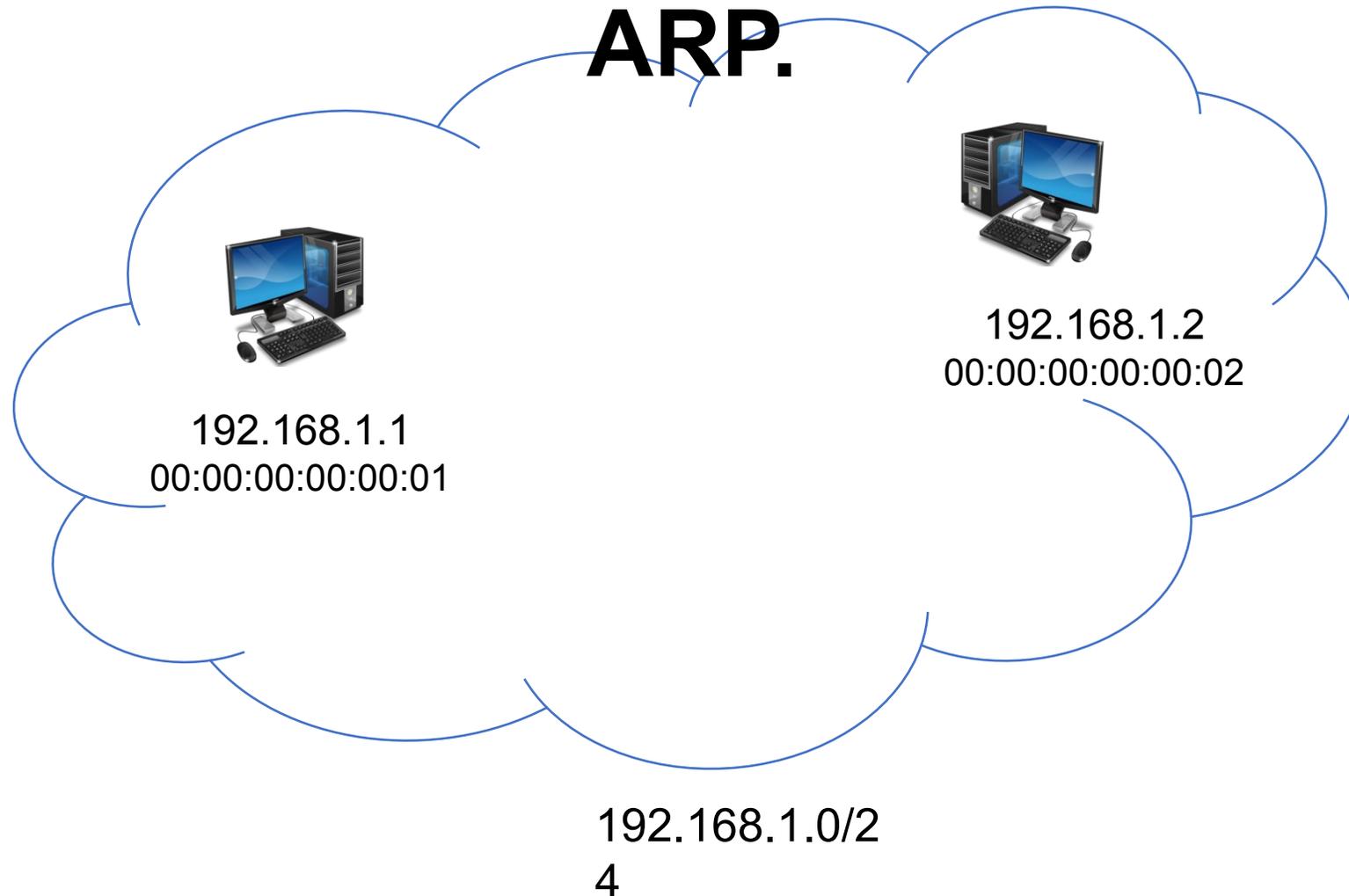
Маршрутизатор является связующим звеном между двумя различными сетями и передает данные, основываясь на определенном маршруте, указанном в его таблице маршрутизации. Эти таблицы позволяют роутеру определить, куда следует направлять пакеты. Эта таблица называется таблицей маршрутизации.



Протокол ARP

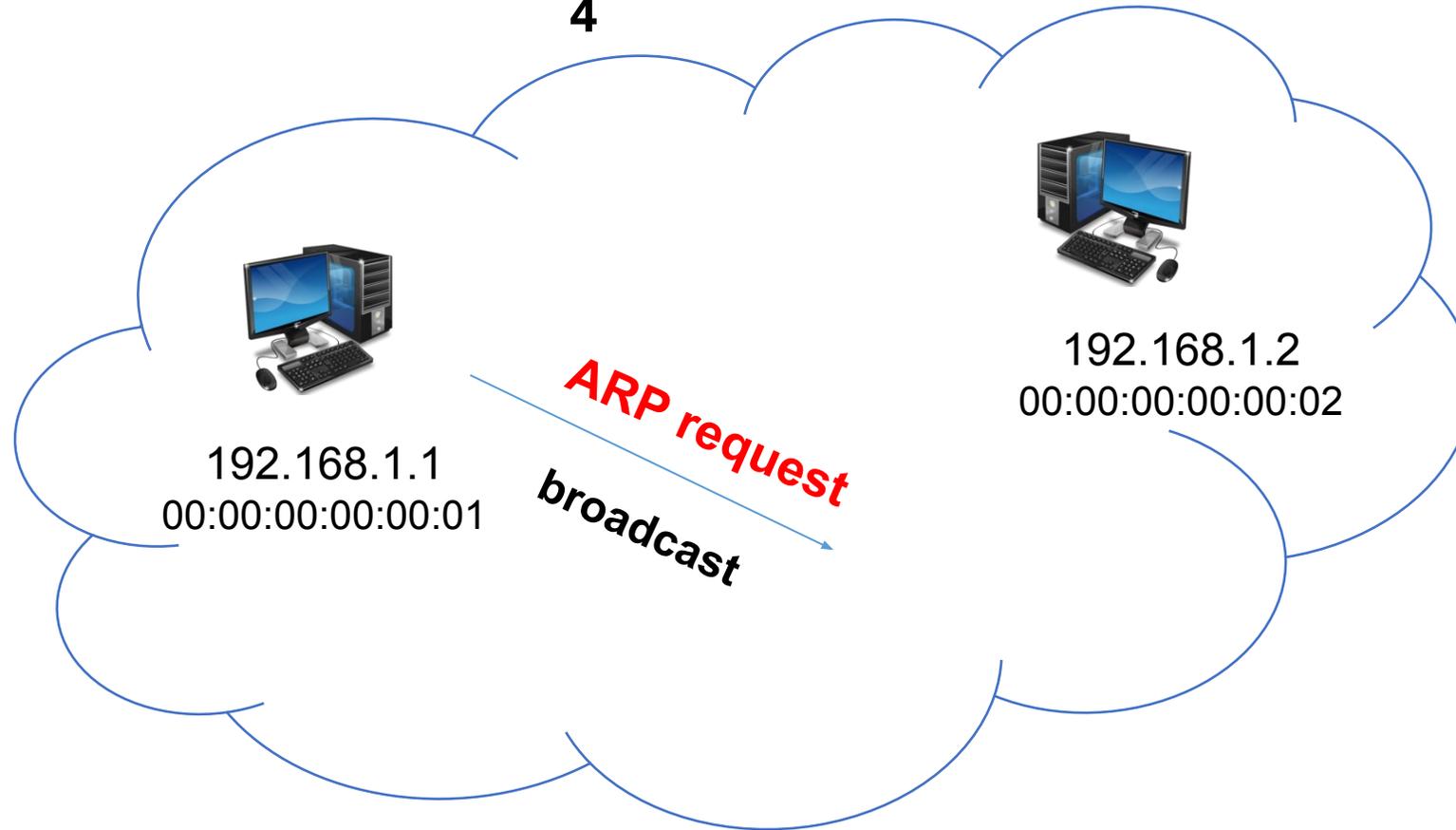
(англ. *Address Resolution Protocol* — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения *MAC-адреса* по известному IP-адресу.

Принцип работы протокола **ARP.**



AR

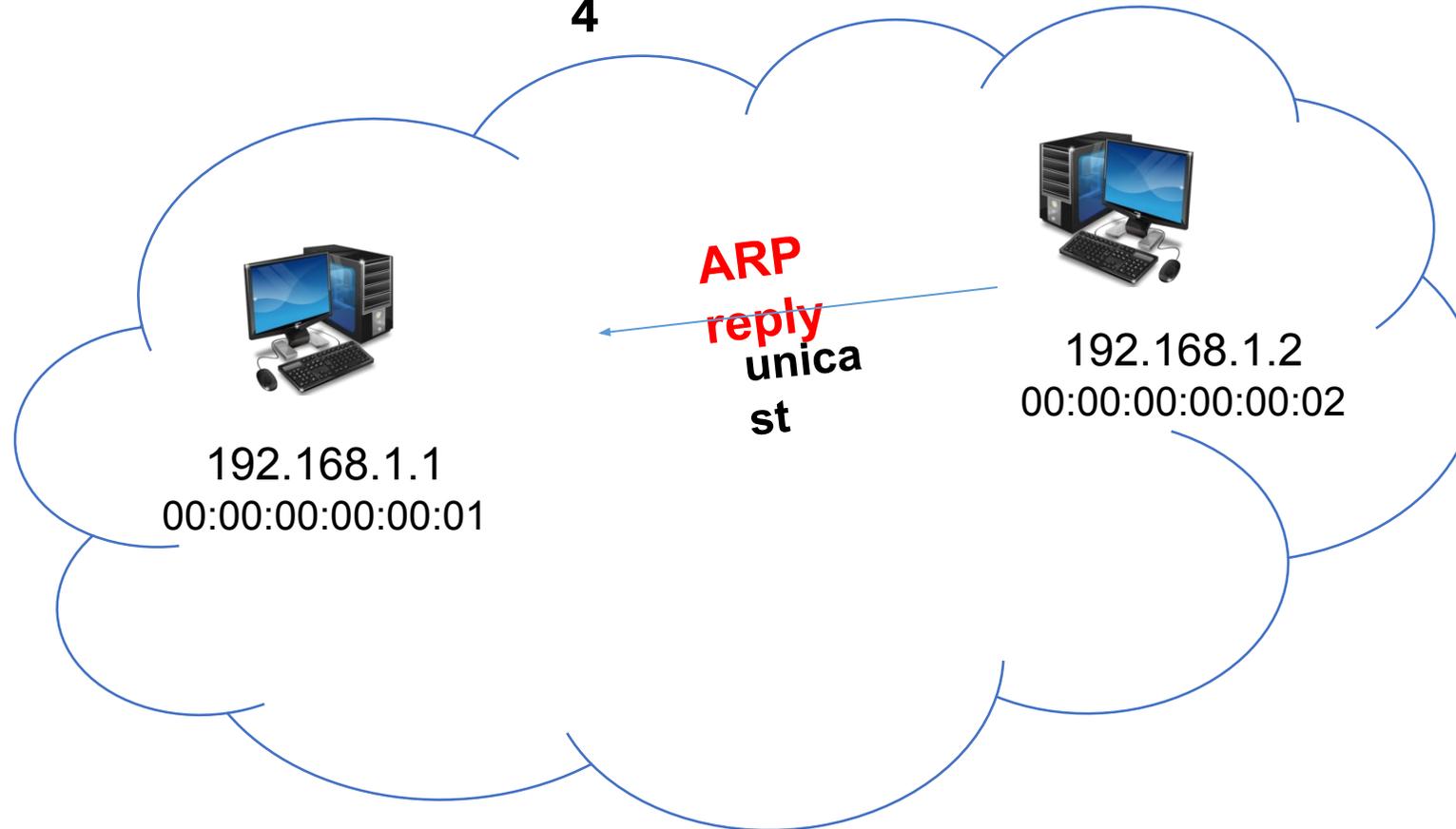
192.168.1.0/24



«Кто-нибудь знает физический адрес устройства, обладающего следующим IP-адресом: 192.168.1.2?»

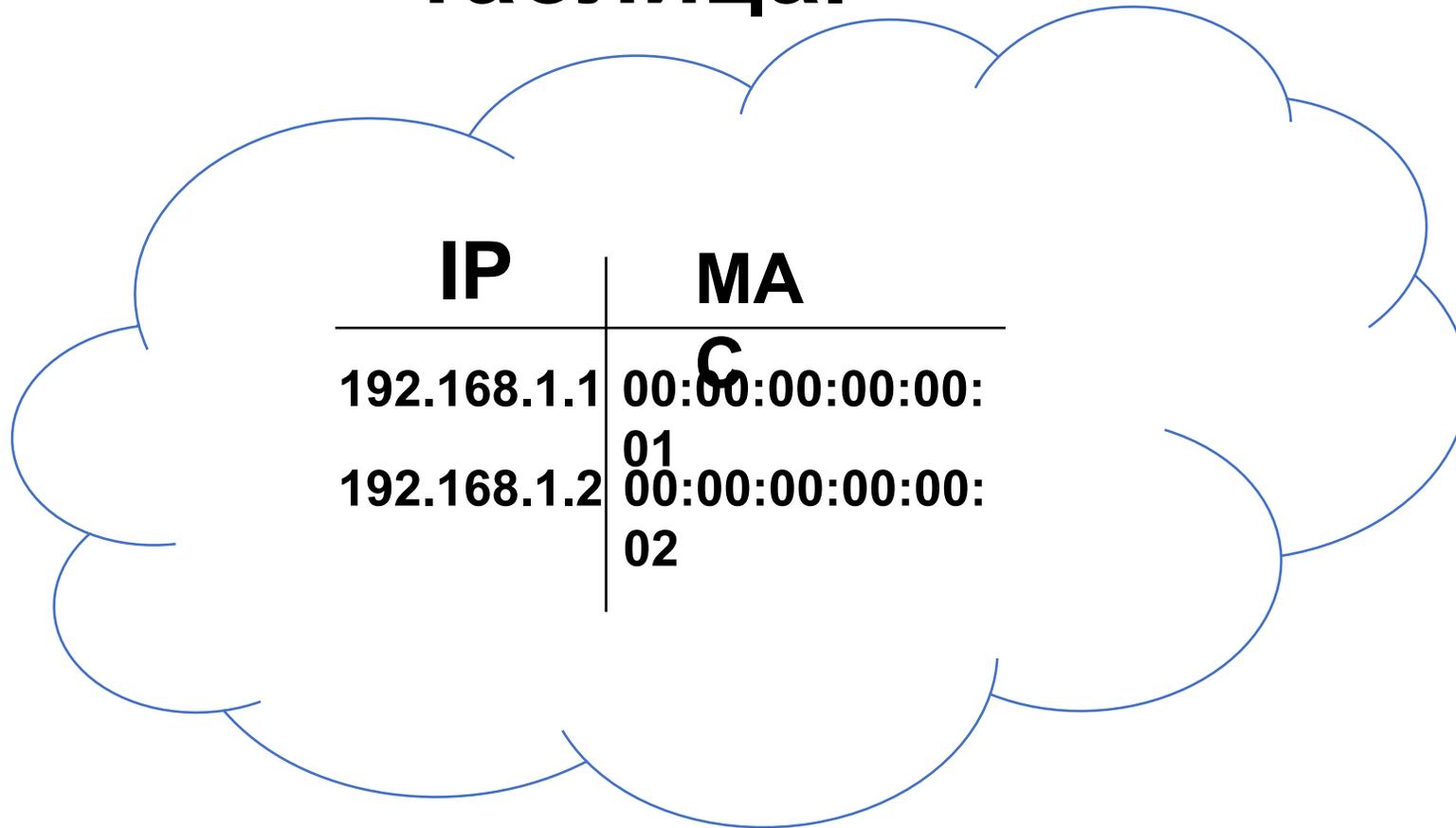
AR

192.168.1.0/24



*«Да, это мой IP-адрес. Мой физический адрес следующий: **00:00:00:00:00:02**»*

ARP – таблица.



IP	МА
192.168.1.1	00:00:00:00:00:00: 01
192.168.1.2	00:00:00:00:00:00: 02

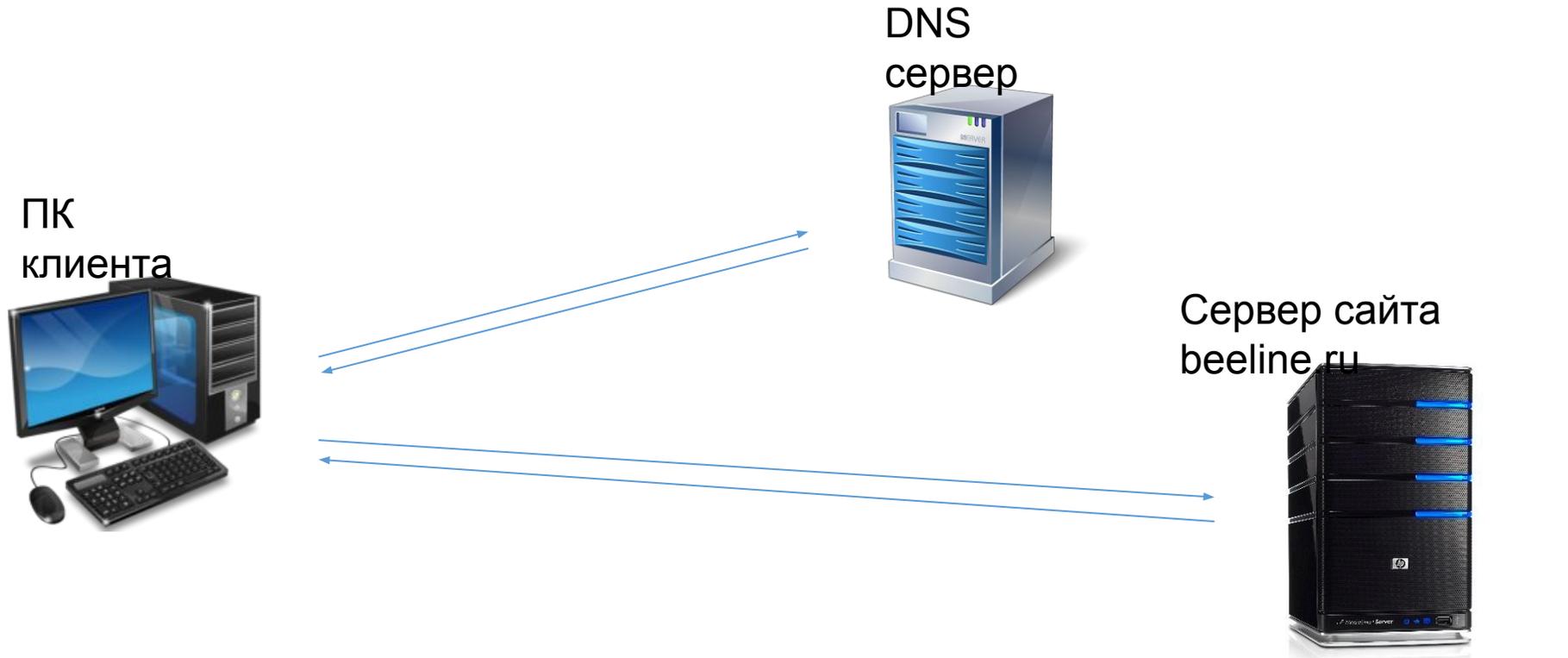
arp

Протокол DNS

(англ. *Domain Name System* — система доменных имён) — протокол в компьютерных сетях, предназначенный для определения ip-адреса хоста по известному доменному имени.

Beeline.ru 
85.21.78.93

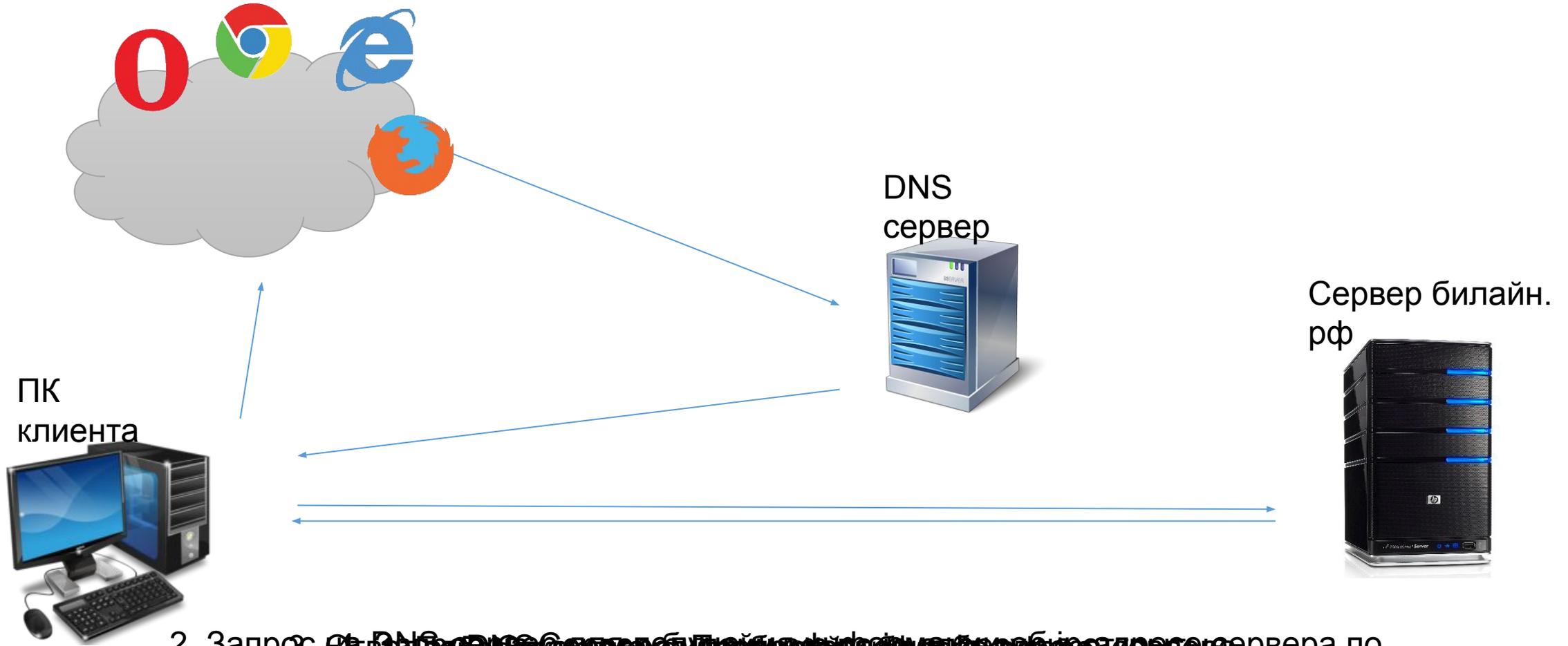
DNS



Ip
217.118.87.98

Созвонившись с сервером DNS, клиент узнает на сайте
«Какой ip-адрес ПК имеет сервер сайта beeline.ru?»
и получает ответ: «IP-адрес сервера находится сайт
beeline.ru 217.118.87.98»

Punycode

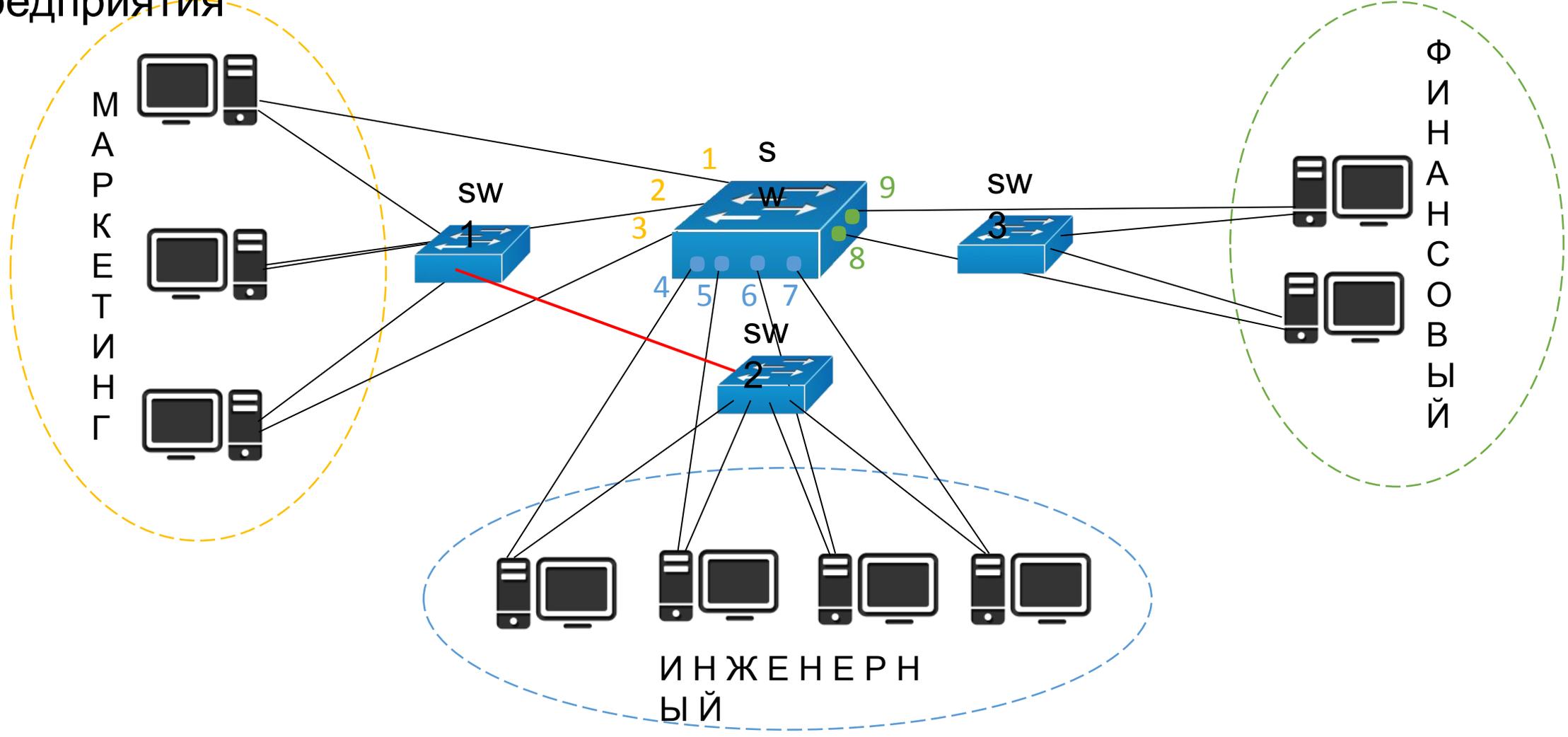


2. Запрос от ПК клиента к серверу билайн.рф по адресу сервера по punycode билайн.рф

VLAN

(от англ. *Virtual Local Area Network*) — виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения.

Сеть предприятия



Стоимость 1 свитча ~ 25000 руб