МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

РГР

ПО ДИСЦИПЛИНЕ «Информационные сети»

на тему: IP-адресация и IPv4.

Факультет: АВТ Преподаватель: Мищенко П.В.

Группа:

Студент:

Новосибирск 2023 г.

Содержание

Введение

Интернет прочно вошел в повседневную жизнь современного человека. С его помощью всегда можно отыскать нужную информацию, сделать в любое время видеозвонок, оплатить различные услуги. Благодаря Интернету появились практически безграничные возможности во всех областях жизни.

IP-адрес используется в Интернете непосредственно для связи между различными устройствами. Например, между сайтом Яндекса и вашим компьютером. Или между вами и другим игроком в Minecraft.

IP-адрес назначается каждому сетевому устройству, и делает это ваш провайдер. Разумеется, для того, чтобы назначить IP-адрес, надо как-то отличить ваше устройство от устройства вашего соседа, и вот тут как раз нам необходим MAC-адрес, который зашил в устройство производитель.

Проще говоря, IP-адрес – это надстройка над MAC-адресом, которую делает ваш оператор для обеспечения вас связью. И если в теории ваш MAC-адрес с вами навсегда (пока не смените свой ноутбук, компьютер или телефон), то ваш IP-адрес, как правило, постоянно меняется. Он меняется в зависимости от места подключения, времени подключения и условий подключения, и, конечно, вашего оператора.

Цель работы: изучить IP-адресацию и IPv4.

Задачи работы:

- изучить понятие IP-сети и их особенности и механизм адресации
- изучить маски подсети: назначение и применение;
- изучить интернет протокол версии 4, выявить основные неполадки и разработать некоторые рекомендации по их устранению.

1. IP-сети: устройство, адресация и особенности

1.1 Понятие и особенности

IP-адрес – это уникальный адрес, идентифицирующий устройство в интернете или локальной сети [4]. IP означает «Интернет-протокол» – набор правил, регулирующих формат данных, отправляемых через интернет или локальную сеть.

По сути, IP-адрес – это идентификатор, позволяющий передавать информацию между устройствами в сети: он содержит информацию о местоположении устройства и обеспечивает его доступность для связи. IP-адреса позволяют различать компьютеры, маршрутизаторы и веб-сайты в интернете и являются важным компонентом работы интернета.

IP-адрес – это строка чисел, разделенных точками. IP-адреса представляют собой набор из четырех чисел, например, 192.158.1.38. Каждое число в этом наборе принадлежит интервалу от 0 до 255. Таким образом, полный диапазон IP-адресации – это адреса от 0.0.0.0 до 255.255.255.255.

IP-адреса не случайны: они рассчитываются математически и распределяются Администрацией адресного пространства Интернета (Internet Assigned Numbers Authority, IANA), подразделением Корпорации по присвоению имен и номеров в Интернете (Internet Corporation for Assigned Names and Numbers, ICANN).

ICANN – это некоммерческая организация, основанная в США в 1998 году с целью поддержки безопасности интернета и обеспечения его доступности для всех пользователей [1]. Каждый раз, когда кто-либо регистрирует домен в интернете, он пользуется услугами регистратора доменных имен, который платит ICANN небольшой сбор за регистрацию домена.

Компьютерам, серверам и роутерам в интернете нужно понимать, куда отправлять данные, чтобы они не потерялись в паутине проводов и прочих

вайфаев по пути с какого-нибудь американского хранилища «Ютуба» в браузер в Новосибирске. Один из помощников в этом деле — IP-адрес. Он представляет собой что-то вроде дорожного указателя, маяка, который содержит данные о месте конкретного устройства в структуре Глобальной сети.

Чтобы узнать IP-адрес вашего устройства, можно открыть терминал и ввести ipconfig в Windows или ifconfig в macOS и Linux (рисунок 1).

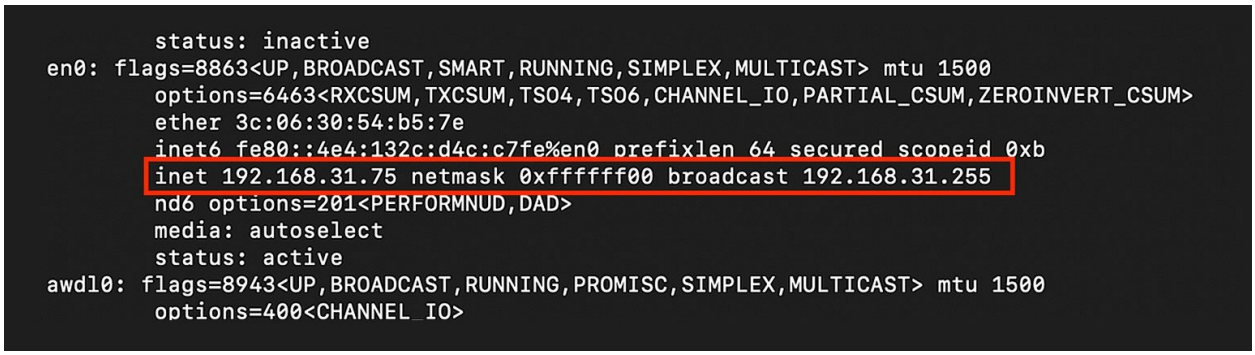

Рисунок 1 – Терминал Windows

Чаще всего это четыре числа, которые разделены между собой точками (такой формат поддерживается в протоколе IPv4).

Каждое из чисел в адресе — это восьмизначное двоичное число, или октет. Оно может принимать значения от 0000 0000 до 1111 1111. Или же от 0 до 255 в десятичной системе счисления — то есть 256 разных значений.

Получается, диапазон IP-адресов стартует с 0.0.0.0 и заканчивается 255.255.255.255. Если посчитать количество всех адресов в этом диапазоне, получится 4 294 967 296.

Формат адресов IPv4 — не единственный, хоть и один из самых популярных в интернете. Есть ещё стандарт IPv6 — его адреса состоят уже из 128 битов (в IPv4 — 32 бита). Таким образом, IPv6 позволяет пронумеровать 2128 устройств (по 300 миллионов на каждого жителя Земли).

Ниже будет говориться только об IPv4, однако эти принципы хорошо ложатся и на IPv6.

1.2 Механизм адресации

На самом деле IP-адрес — это чуть больше, чем просто набор чисел. Он всегда состоит из двух частей: номера хоста (устройства) и номера сети.

Например, IPv4-адрес 192.168.1.34 состоит из таких смысловых частей (рисунок 2).

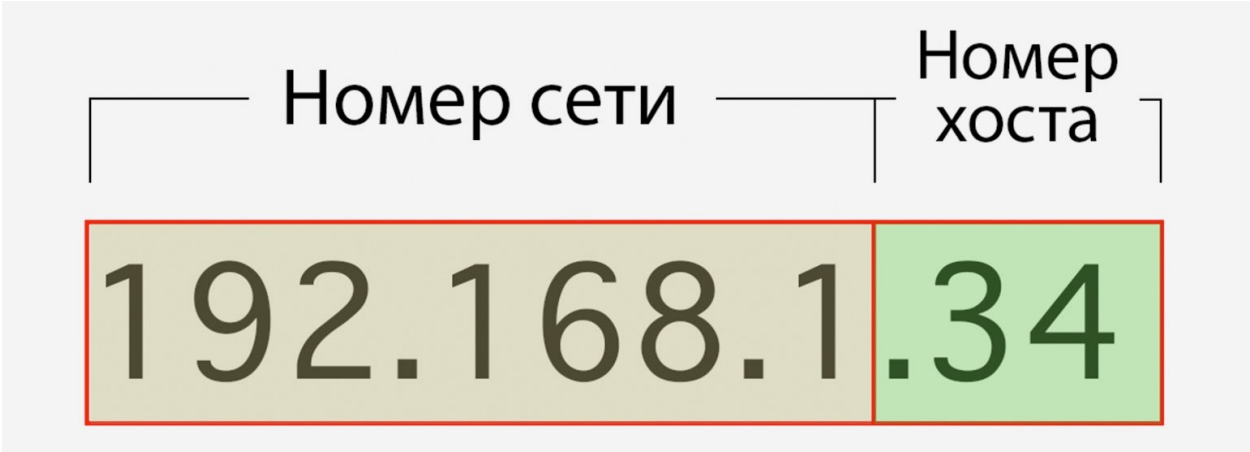

Рисунок 2 – Описание смысловой части IP

В нём первые три числа означают номер сети, а четвёртое — номер хоста (то есть вашего устройства). Все устройства, идентификаторы которых начинаются с 192.168.1, находятся в одной сети (рисунок 3).

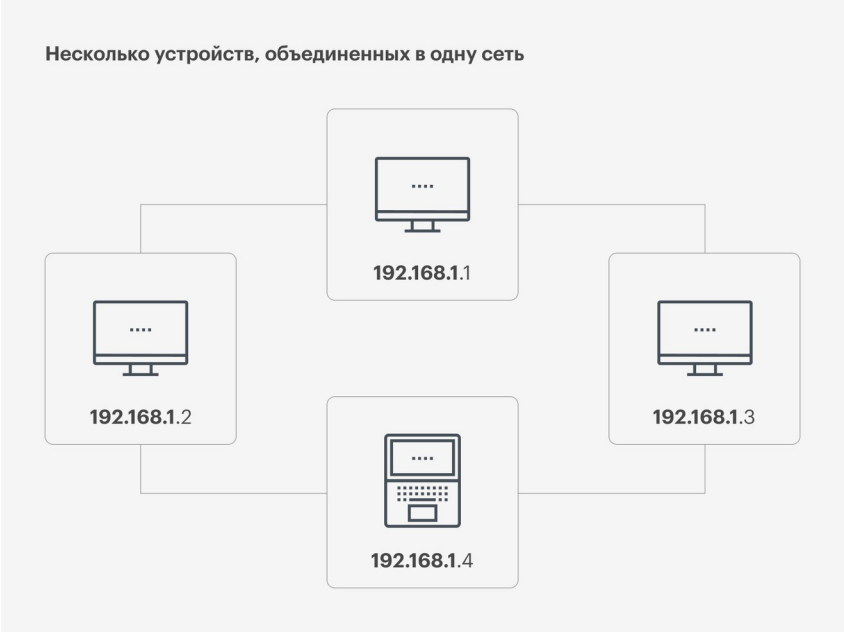

Рисунок 3 – Схема одной сети

Устройство, идентификатор которого начинается, например, с 192.168.2, будет принадлежать к другой сети и не сможет связываться с устройствами из сети 192.168.1. Чтобы это сделать, понадобится роутер, который соединит две сети между собой.

Он будет мостом, по которому данные переходят из одной сети в другую. Если же говорить техническим языком, то роутер — это сеть более высокого уровня, которая объединяет несколько подсетей. Со стороны это будет выглядеть так, будто у роутера есть устройства, которым он передаёт данные и которые могут связываться между собой (рисунок 4).

Рисунок 4 – Схема двух сетей

Номер сети может храниться не только в первых трёх октетах, но и в первых двух или даже в одном. Остальные числа — это номера устройств в сети.

Чтобы компьютер понимал, какие октеты обозначают сеть, а какие — компьютеры и роутеры, используют несложный механизм. Первые несколько битов в двоичном представлении IP-адреса фиксируются, считываются компьютером и автоматически распознаются — это похоже на конструкцию switch вязыках программирования:

1. Если первый бит — это 0, значит, компьютер имеет дело с большой сетью, на которую указывает только одно, самое первое число [11].

При этом первый бит у нас уже зарезервирован под такой «свитч», поэтому всего таких сетей может быть 128 (от нуля до 127), а устройств в них — более 16 миллионов (рисунок 5).

Рисунок 5 – IP-адреса большой сети

2. Если первые два бита — это 10 (то есть 2 в десятичной системе счисления), значит, IP-адрес принадлежит к средней сети и использует два числа как указатель на неё [11].

У такого адреса уже зарезервировано два первых бита, а значит, для номера сети остаётся только 14 битов — это более 16 тысяч сетей и более 65 тысяч устройств (рисунок 6).

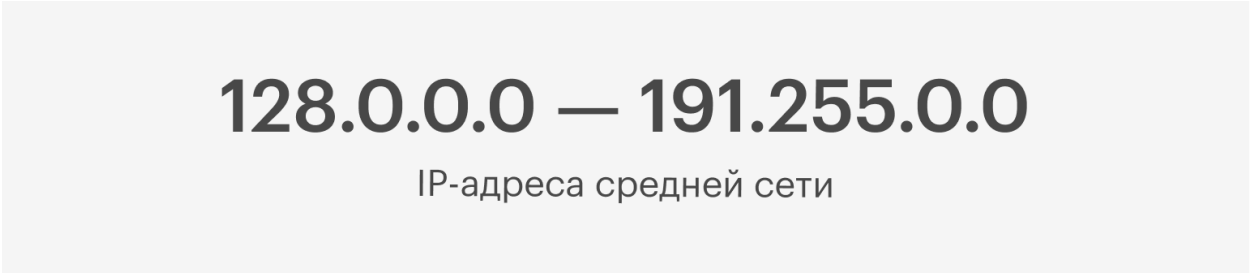

Рисунок 6 - IP-адреса средней сети

3. Если первые три бита — это 110, значит, компьютеру попался IP-адрес из маленькой сети, в качестве указателей на которую используются только три первых числа.

Всего таких сетей существует более двух миллионов, а подключаемых устройств в каждой — 256. Диапазон значений — от 192.0.0.0 и до 223.255.255.0 (223 — потому что у нас зарезервировано три бита).

Все эти виды IP-адресов имеют свои названия: класс A, B и C [10]. Класс A — это большие сети, B и C — средние и маленькие [10]. Кроме них существуют ещё сети класса D и E. В них входят зарезервированные адреса — например, 127.0.0.0 или 192.168.X.X. Первый указывает сам на себя — когда он отправляет данные по этому адресу, они тут же приходят обратно (его ещё называют localhost). А второй — это стандартный идентификатор интернет-модемов и Wi-Fi-роутеров.

Бывает, что хостов в сети больше, чем доступных IP-адресов, — в современном интернете дела обстоят именно так. В этом случае интернет-провайдеры выдают устройствам адреса формата IPv6. При этом адрес IPv4 можно легко переделать в формат IPv6, а вот в обратную сторону это уже не работает.

Однако не все интернет-провайдеры перешли на новую версию IP-адресов, и это создало новую проблему: невозможно напрямую отправлять данные с устройств, поддерживающих IPv4, на устройства с IPv6. Проблему решили с помощью туннелирования — создали специальный канал между двумя устройствами, по которому обмениваются информацией между сетями с разными версиями протокола.

2. Маска подсети: назначение и применение

Маска подсети — это более удобный способ разделить IP-адрес на номер сети и номер хоста [3]. Она пришла на смену алгоритму, который был

описан выше. Маска подсети состоит из тех же четырёх чисел и похожа на IP-адрес (рисунок 7).

Рисунок 7 – Пример маски подсети

В двоичном представлении такая маска выглядит как 1111 1111 0000 0000. Нули показывают, где находится номер хоста, а единицы — номер сети.

Чтобы применить маску, нужно воспользоваться логическими операторами «И» и «НЕ». Первый работает по следующим правилам (рисунок 8).

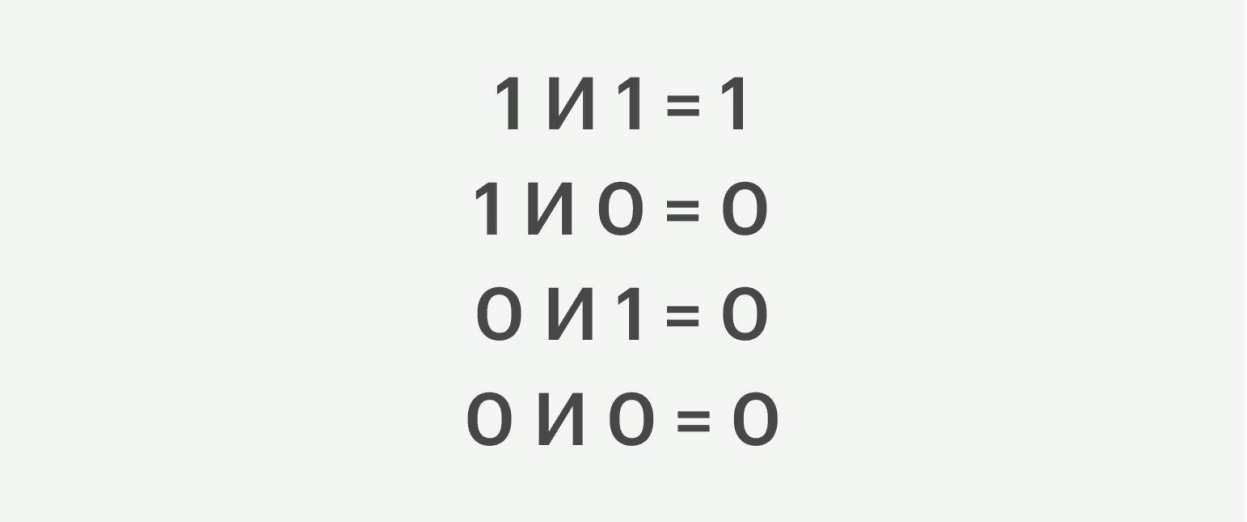

Рисунок 8 – Правила логического оператора «И» и «НЕ»

Оператор «НЕ» просто меняет все нули на единицы, а единицы на нули. И делает он это справа налево (рисунок 9).

НЕ 1 = 0

НЕ 0 = 1

Рисунок 9 – Пример работы логического оператора «НЕ»

Применим к IP-адресу 192.168.1.34 маску подсети 255.255.255.0 (рисунок 10).

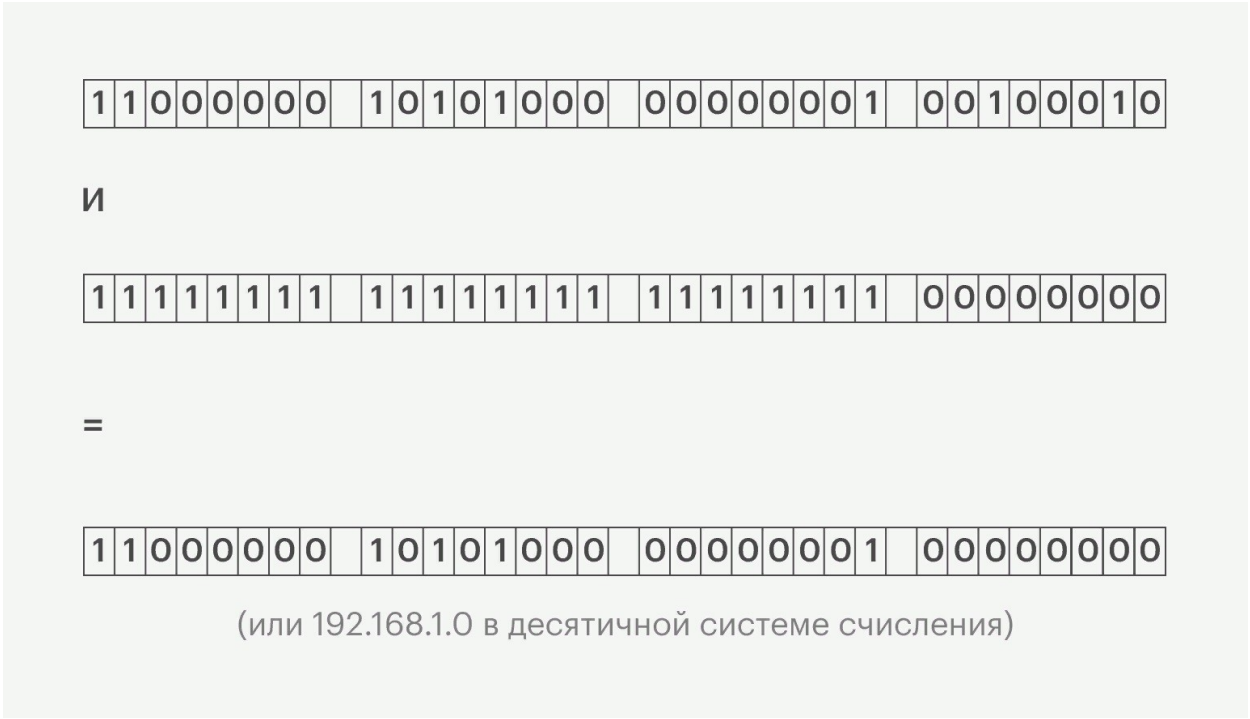

Рисунок 10 – Пример работы маски подсети

На рисунке 10 показано, как мы сначала перевели IP-адрес и маску подсети в двоичную систему счисления. А затем побитово справа налево применили операцию логического «И». Маска помогла удалить ненужную часть адреса, и мы выделили номер сети — 192.168.1.0.

Чтобы выделить номер хоста, нужно сначала применить операцию логического «НЕ» к маске подсети, а затем — операцию логического «И» к IP-адресу и полученной маске (рисунок 11).

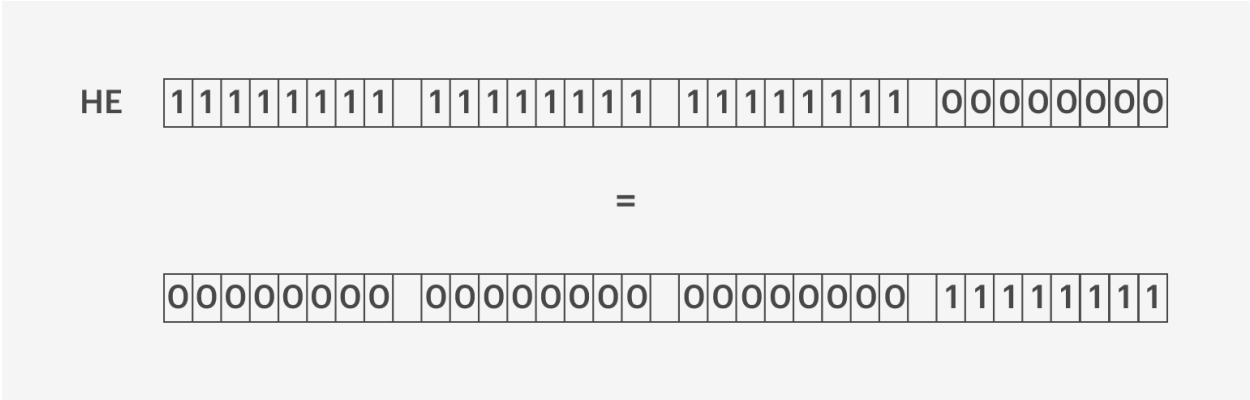

Рисунок 11 – Применение логического «НЕ» к маске подсети

Так мы получили маску для выделения номера устройства. А теперь применим операцию логического «И» (рисунок 12). У нас получился адрес 0.0.0.34. Это и есть номер хоста.

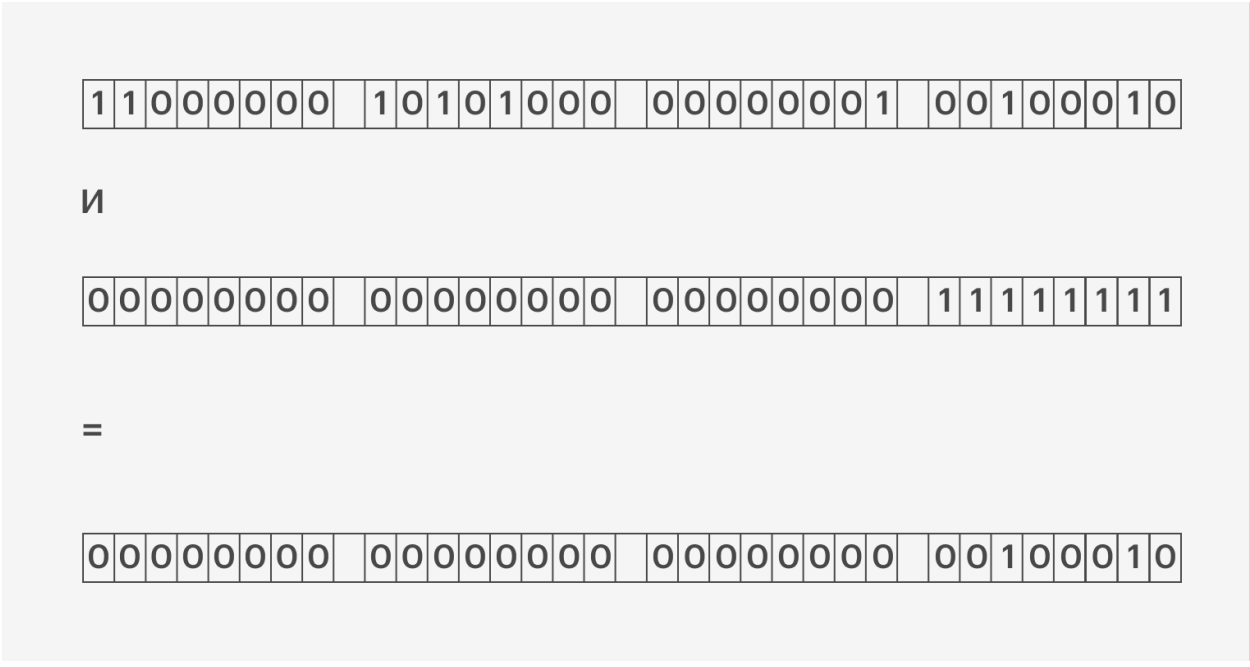

Рисунок 12 - Применение логического «И» к маске подсети

Обычно маска задаётся программистами в настройках серверов или пользователями в настройках системы. Например, на MacBook маску подсети

можно посмотреть в разделе «Сеть» → «Дополнительные настройки» (рисунок 13).

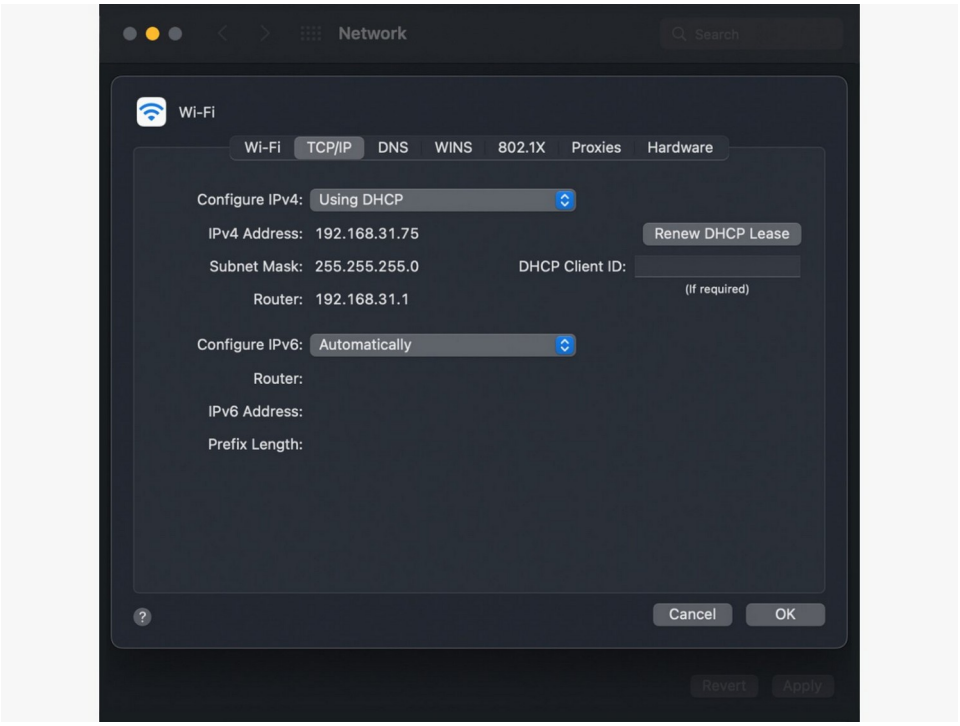

Рисунок 12 – Маска подсети на MacBook

Маска показывает, сколько битов включает в себя номер сети. Например, у большой сети номером будет только первое число (8 битов), а маска будет состоять из восьми единиц и 24 нулей: 255.0.0.0.

Если IP-адрес принадлежит к маленькой сети, то первые три числа в нём будут представлять номер сети. Значит, маска будет выглядеть так: 255.255.255.0.

Есть и слегка необычные маски подсетей — например, 255.255.254.0. Они тоже означают, сколько битов используется в номере сети. Только в данном случае их будет 23 — по 8 в первых двух числах и 7 в третьем. Остальные биты будут принадлежать номеру хоста.

Выделять номера хостов и сетей удобно, но это не самая интересная часть использования масок. Их главная «суперсила» — умение разделять большие сети на несколько маленьких.

Допустим, у нас есть номер сети 185.12.0.0 с маской 255.255.0.0. В такой сети может быть более 65 тысяч устройств, чего вполне хватит, чтобы вместить все компьютеры в одном большом офисе.

Но что если у нас есть несколько маленьких офисов в одном здании, и мы хотим их все подключить к сети? Создавать новую сеть с 65 тысячами IP-адресов для каждого офиса нерационально. Поэтому мы можем разбить сеть 185.12.0.0 на подсети.

Для этого вместо маски 255.255.0.0 мы возьмём маску 255.255.255.0. Так у нас появится 256 новых подсетей внутри одной большой. При этом в каждой подсети будет по 256 устройств.

Если в офисе понадобится больше устройств, мы можем взять другую маску — например, 255.255.254.0. И теперь нам будет доступно 512 устройств, а количество подсетей сократится до 128.

3. Интернет протокол версии 4 (IPv4)

3.1 Особенности работы IPv4

Клиентам нужны IP-адреса для идентификации, так же, как и серверам. Серверам также требуются имена хостов. У веб-серверов есть доменное имя (имя хоста), как Google.com, и когда захотите добраться до него, то увидите содержимое страницы.

Контент каждого веб-сайта размещается на веб-серверах в центрах обработки данных. Веб-сайтам и приложениям нужны серверы для размещения служб, чтобы вы могли получить к ним доступ.

Всё и началось с ARPAnet (Агентство перспективных исследовательских проектов Министерства обороны США) предоставило финансирование исследовательской сети, известной как ARPAnet.

Впервые он стал доступен в 1969 году и разрешал соединения между 4 хостами [5]. У каждого хоста был свой определённый адрес для онлайн-

общения. Сеть со временем росла, и в 1981 году к ней было подключено 213 хостов [5]. ARPA оказала значительное влияние на университеты и исследовательские центры в Соединённых Штатах.

Цель состояла в том, чтобы сохранить неоднородность каждой сети, обеспечивая при этом возможность взаимодействия пользователей между сетями. Чтобы добиться этого, Винт Серф (NCP) и Роберт Хан (DARPA) работали над программой управления передачей в первой половине 1970-х годов и опубликовали свою первую статью в 1974 году.

Протокол управления передачей (TCP) и интернет-протокол (IP) были разделены на отдельные версии в третьей из четырёх его реализаций. Первоначальный проект TCP/IP v4 был выпущен в 1978 г. К 1981 г. он стал нормой, а 1 января 1983 г. ARPANET заменила NCP протоколом TCP/IP IPv4 [12].

Адрес IPv4 — это 32-битный адрес, который идентифицирует устройство в сети (рисунок 13) [6]. Он состоит из 4 групп цифр (октетов) по 3 цифры в каждой.

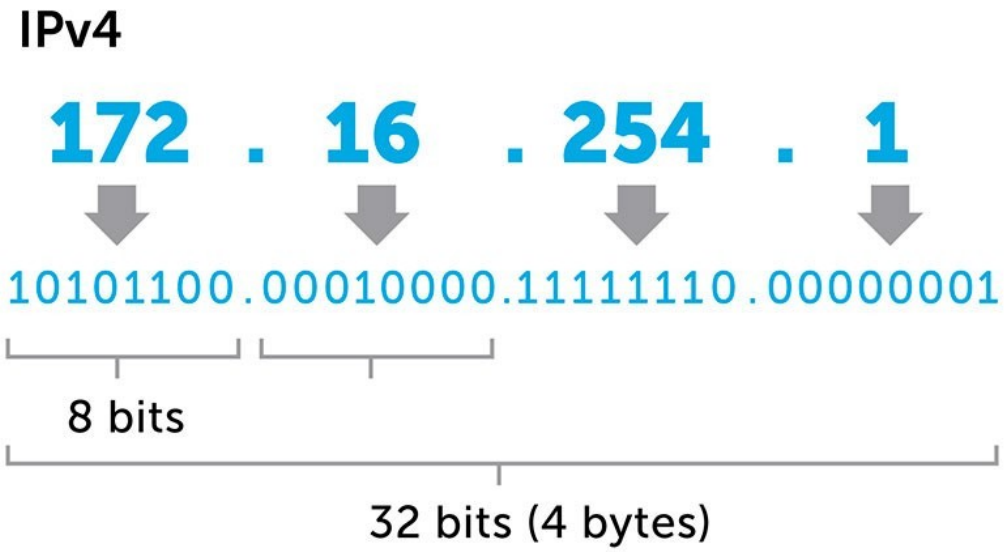

Рисунок 13 - Адрес IPv4

Мы можем выделить пять классов IPv4: A, B, C, D и E, каждый имеет собственный набор IP-адресов (рисунок 14).

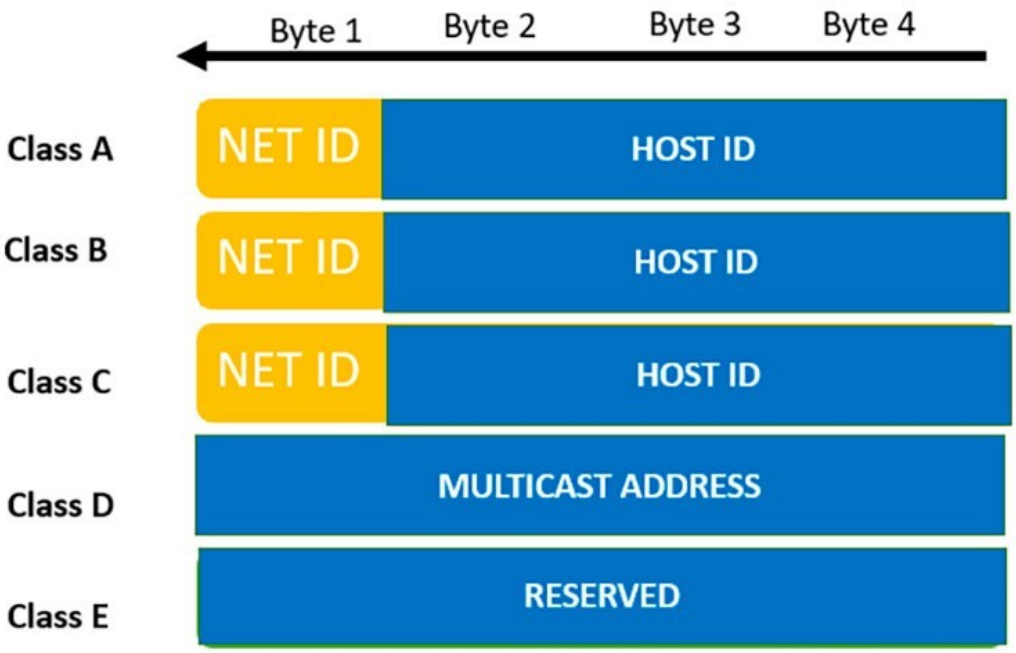

Рисунок 14 - Классы IPv4

Выделим их [5,8,9]:

- Класс A – первый бит, равный 0, охватывает значения от 0.0.0.0 до 127.255.255.255. Этот класс, имеющий 8 бит для сети и 24 бита для хостов, предназначен для больших сетей;
- Класс B – предназначен для сетей среднего и крупного размера. Первые два бита, равные 10, находятся между 128.0.0.0 и 191.255.255.255. Он также содержит 16 бит для хостов и 16 бит для сети;
- Класс C – мы используем его для небольших локальных сетей (LAN). Сеть в этом классе имеет отступ в три октета. И IP-адрес имеет диапазон от 192.0.0.0 до 223.255.255.255, 24 бита сети и 8 бит хоста;
- Класс D – используют только программы, требующие многоадресной рассылки. Это означает, что мы не используем класс D для стандартных сетевых функций. Вместо этого первые три бита устанавливаются в «1», а четвёртый бит используется для «0». Кроме того, 32-битные сетевые адреса составляют адреса класса D;

- Класс E — мы используем его для экспериментов или исследований. Этот класс IP-адресов охватывает значения первого октета от 240.0.0.0 до 255.255.255.255. Первые четыре бита IP-адреса класса E, равны единице в двоичном формате.

Между старым IPv4 и новым IPv6 есть несколько важных различий (рисунок 15):

- 32-битные адреса по сравнению со 128-битными адресами, что обеспечивает гораздо больше адресов в случае IPv6;
- 4 294 967 296 IP-адресов против 340 282 366 920 938 463 463 374 607 431 768 211 456 IP-адресов;
- Конфигурация адресов вручную или с помощью DHCP по сравнению с SLAAC или DHCP6;
- Опциональный IPsec или часть стандарта. IPv6 поддерживает сквозное шифрование и позволяет избежать атак «человек посередине»;
- Трансляция NAT по сравнению с отсутствием необходимости в IPv6.

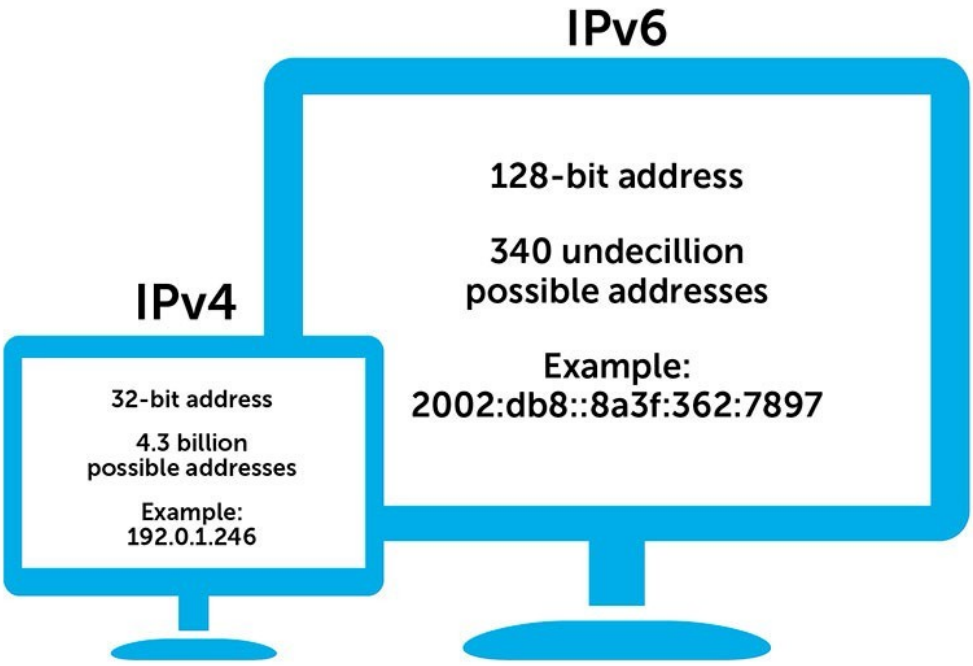

Рисунок 15 – Различия интернет протоколов 4 и 6

Основной целью IPv4 является подключение устройств по сети. Миллионы устройств поддерживают этот протокол. Это делает его самым простым совместимым интернет-протоколом.

Вот ещё несколько преимуществ протокола:

- отличная поддержка системы – IPv4 поддерживается на всех сетевых устройствах;
- простая топология – проще настроить и управлять сетью IPv4;
- длина IP-адреса короткая – это облегчает их запись и даже запоминание;
- совместимость с любым устройством.

Проблемы протокол интернета версии 4 tcp IPv4:

- исчерпание IP-адресов. Потребности в IP-адресах не могут быть удовлетворены только адресами IPv4, поэтому они уже переходят на IPv6;
- нет поддержки IPsec по умолчанию. Вы можете включить его, но с более новым IP-адресом это намного проще;
- ограниченный заголовок, в который нельзя добавлять дополнительные параметры;
- это становится слишком дорогим с ценами выше 25 долларов за IP-адрес.

Теоретически IPv6 по части скорости сети идёт впереди старого протокола. Но на практике всё не так просто, потому что современный протокол ещё нуждается в шлифовке. Это приводит к тому, что нередко IPv4 лучше по скорости.

В 1993 году было введено огромное улучшение распределения адресов IPv4, которое получило название бесклассовой междоменной адресации (CIDR).

Благодаря CIDR, теперь у нас есть суффикс, который представляет собой число от 0 до 32 и показывает, сколько бит представляет сеть. Выглядит так: 192.168.100.14/24. CIDR позволяет использовать подсеть переменной длины, адаптирующаяся к текущим потребностям.

Уменьшив количество неиспользуемых адресов, которые мешали системе классов, CIDR задержал расширение таблиц маршрутизации и продлил срок службы IPv4. Этот трюк очень помог с исчерпанием адресов IPv4, но больше похож на временное исправление, чем на окончательное решение.

Мы живём во время перехода от IPv4 к IPv6. Это небыстрая миграция, и многие компании пока решают придерживаться модели с двумя стеками. Им сложнее управлять, но он надёжнее, чем просто IPv6.

Из-за исчерпания адресов IPv4 в итоге мы движемся к будущему с одним IPv6, что займёт некоторое время. Ведущими странами в этом отношении являются Индия, Бельгия, Германия, Малайзия и Греция.

3.3 Основные неполадки

Если компьютеру TCP/IP необходимо связаться с хостом в другой сети, он обычно связывается с помощью устройства, которое называется маршрутизатор. В терминах TCP/IP маршрутизатор, указанный в хосте, который связывает подсеть хостов с другими сетями, называется шлюзом по умолчанию. В этом разделе объясняется, как TCP/IP определяет, отправлять ли пакеты в шлюз по умолчанию для достижения другого компьютера или устройства в сети.

Когда хост пытается взаимодействовать с другим устройством с помощью TCP/IP, он выполняет процесс сравнения с помощью определенной маски подсети и IP-адреса назначения по сравнению с маской подсети и собственным IP-адресом. В результате этого сравнения компьютеру сообщается, является ли назначение локальным хостом или удаленным хостом.

Если в результате этого процесса назначение определяется как локальный хост, компьютер отправляет пакет в локальную подсеть. Если в результате сравнения назначение определяется как удаленный хост,

компьютер перенаправит пакет в шлюз по умолчанию, определенный в свойствах TCP/IP. После этого маршрутизатор несет ответственность за перенаправление пакета в соответствующую подсеть.

Проблемы сети TCP/IP часто возникают из-за неправильной конфигурации трех основных записей в свойствах TCP/IP компьютера. Понимая, как ошибки в конфигурации TCP/IP влияют на сетевые операции, можно решить множество распространенных проблем TCP/IP.

Неправильная маска подсети: если сеть использует другую маску подсети, чем маска по умолчанию для своего класса адресов, и клиент по-прежнему настроен с помощью маски подсети по умолчанию для класса адресов, связь не будет работать с некоторыми соседними сетями, но не с удаленными.

Например, если вы создаете четыре подсети (например, в примере подсетей), но используете неправильную маску подсети 255.255.255.0 в конфигурации TCP/IP, хосты не смогут определить, что некоторые компьютеры находятся в других подсетях, чем их собственные. В этой ситуации пакеты, предназначенные для хостов различных физических сетей, которые являются частью одного и того же адреса класса C, не будут отправлены в шлюз по умолчанию для доставки.

Распространенным симптомом этой проблемы является то, что компьютер может связываться с хостами, которые находятся в локальной сети, и может общаться со всеми удаленными сетями, за исключением тех сетей, которые находятся поблизости и имеют один и тот же адрес класса A, B или C. Чтобы устранить эту проблему, просто введите правильную маску подсети в конфигурацию TCP/IP для этого хоста.

Неправильный IP-адрес: если компьютеры с IP-адресами, которые должны быть в отдельных подсетях, размещаются в локальной сети рядом друг с другом, они не смогут связывается. Они будут пытаться отправлять пакеты друг другу с помощью маршрутизатора, который не может переадресовать их правильно. Симптомом этой проблемы является

компьютер, который может связываться с хостами в удаленных сетях, но не может связываться с некоторыми или всеми компьютерами в локальной сети. Чтобы устранить эту проблему, убедитесь, что все компьютеры одной физической сети имеют IP-адреса в одной подсети IP. Если в одном сегменте сети закончились IP-адреса, существуют решения, которые выходят за рамки этой статьи.

Неправильный шлюз по умолчанию: компьютер, настроенный с неправильным шлюзом по умолчанию, может связываться с хостами в своем сетевом сегменте. Но он не сможет связываться с хостами в некоторых или всех удаленных сетях. Хост может связываться с некоторыми удаленными сетями, но не с другими, если верны следующие условия:

- одна физическая сеть имеет несколько маршрутизаторов;
- неправильный маршрутизатор настроен как шлюз по умолчанию.

Эта проблема распространена, если в организации есть маршрутизатор к внутренней сети TCP/IP и другой маршрутизатор, подключенный к Интернету.

3.3 Рекомендации по настройке IPv4 на примере Windows

Если в окне «Состояние» сетевого подключения вижу надпись «IPv4-подключение: без доступа к интернету», или «IPv4-подключение: без доступа к сети» и интернет на вашем компьютере, или ноутбуке не работает, то следуя советам из этой статьи, вы сможете исправить эту проблему. Или хотя бы попытаться все починить, и разобраться в чем дело.

На самом деле, проблема очень популярная и статус «без доступа к интернету, или сети» возле протокола TCP/IPv4 может появится из-за множества разных причин.

В том числе проблемы с Wi-Fi роутером (если у вас подключение через роутер), какие-то ошибки в Windows, или даже проблемы у вашего интернет-провайдера. Сейчас мы постараемся найти причину и устранить ее. Главная

проблема – не работает интернет на компьютере. И нам нужно сделать так, чтобы он заработал.

С этой проблемой можем столкнутся при подключении как по Wi-Fi сети, так и по сетевому кабелю через маршрутизатор, или напрямую к интернет-провайдеру. Так же отсутствие интернета для IPv4 можно наблюдать как в новой Windows 10, так и в Windows 8 и Windows 7. Решения будут универсальными для всех ОС, компьютеров, ноутбуков. Открыв «Состояние» своего подключения к интернету (беспроводное соединение, или Ethernet), скорее всего увидим статус без доступа к интернету, или сети (рисунок 16).

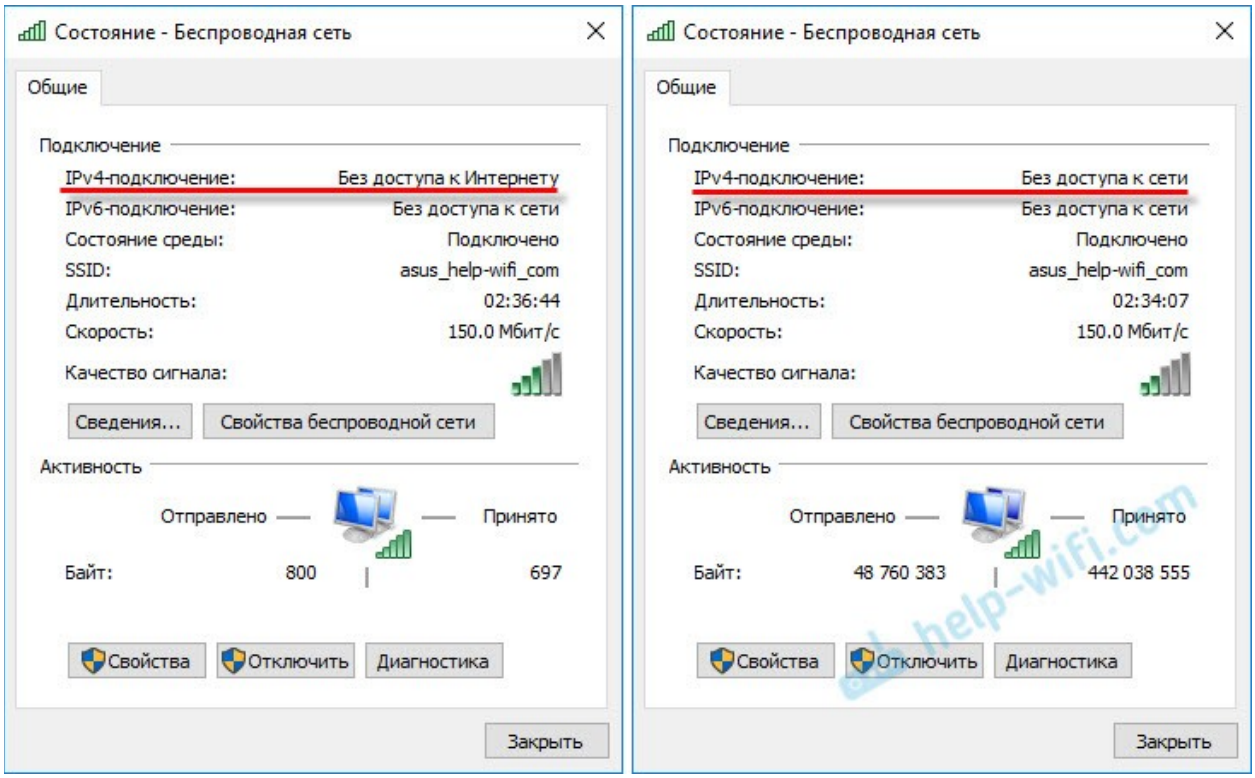

Рисунок 16 - «Состояние» подключения к интернету

Для начала выполним несколько несложных рекомендаций, и попытаюсь определить причину:

- перезагрузка компьютера, или ноутбука. Именно перезагрузка, а не выключение;

- если подключение через роутер, то перезагружаем роутер, полностью отключив питание на минуту;
- вспоминаю, что делал перед тем, как интернет перестал работать, а возле IPv4 появился статус без доступа к интернету. Это очень важно. Может менял какие-то настройки, или что-то установил;
- если интернет подключен напрямую к компьютеру (без маршрутизатора и модема), то при возможности подключаем его к другому компьютеру. Не исключено, что проблема у интернет-провайдера;
- если установлен роутер, и интернет не работает ни на одном устройстве, которое подключено через него, то причина в самом роутере, или провайдере. Если же интернет не работает только на одном компьютере, значит ищем причину на нем;
- временно отключаем антивирус.

Прямо в окне «Состояние» нажмите на кнопку «Диагностика» (рисунок 17).

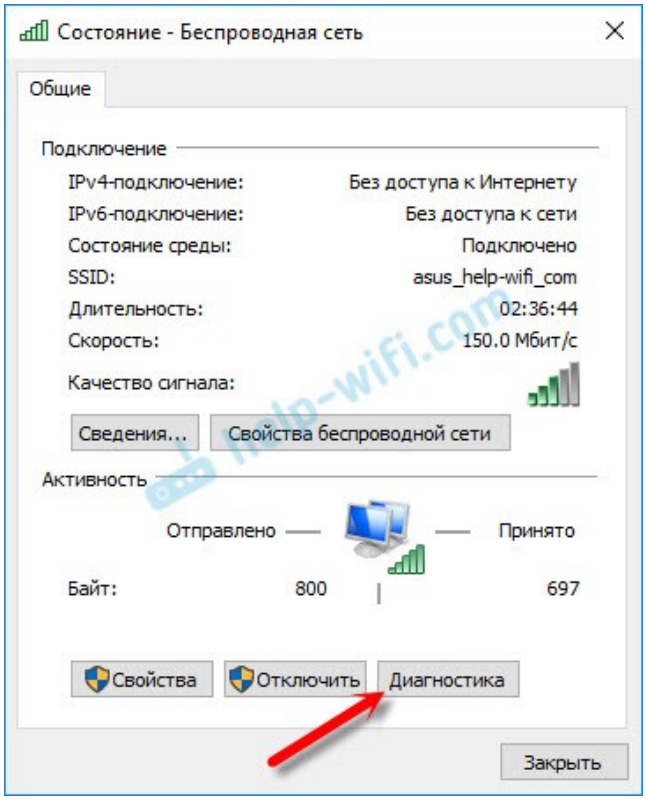

Рисунок 17 – Окно «Состояние»

Начнется «Диагностика неполадок», затем появится результат. Чаще всего удается найти вот такие ошибки (рисунок 18).

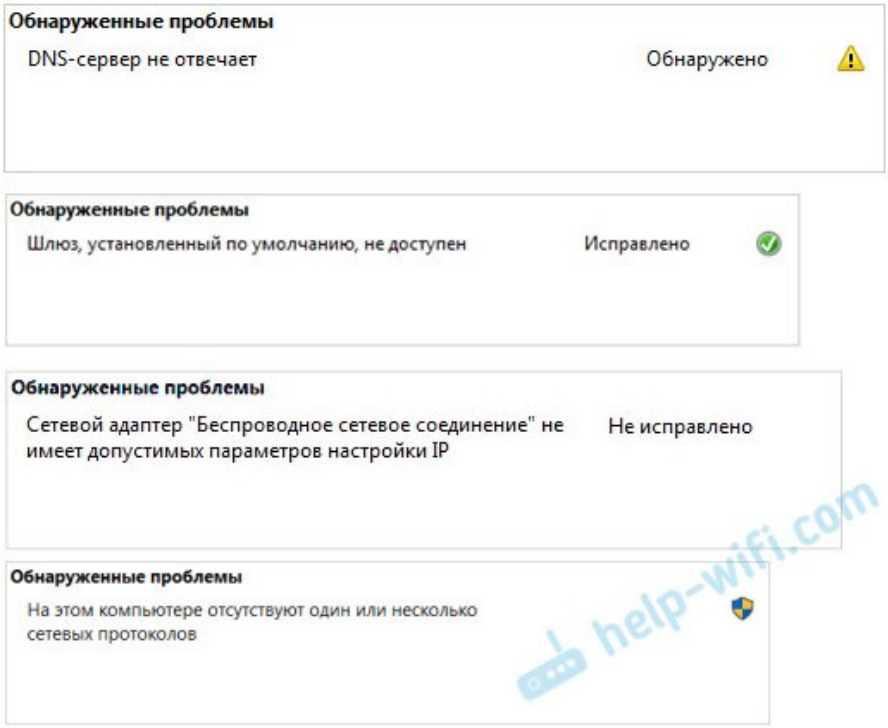

Рисунок 18 – Основные ошибки

В зависимости от найденной проблемы, можно применить решения:

- DNS-сервер не отвечает, или «Параметры компьютера настроены правильно, но устройство или ресурс (DNS-сервер) не отвечает»;
- шлюз, установленный по умолчанию, не доступен;
- сетевой адаптер не имеет допустимых параметров настройки IP;
- на этом компьютере отсутствуют один или несколько сетевых протоколов.

Если ошибка не была обнаружена, можно еще проверить настройки протокола TCP/IPv4.

Заходим в «Сетевые подключения»: можно нажать правой кнопкой мыши на значок подключения (на панели уведомлений) и выбрать «Центр управления сетями и общим доступом». Затем, в новом окне слева выбрать «Изменение параметров адаптера».

Дальше, нажимаем правой кнопкой мыши на тот адаптер, через который подключаюсь к интернету, и выберите «Свойства». Если по Wi-Fi, то это «Беспроводная сеть». Если по кабелю, то это «Ethernet» (подключение по локальной сети).

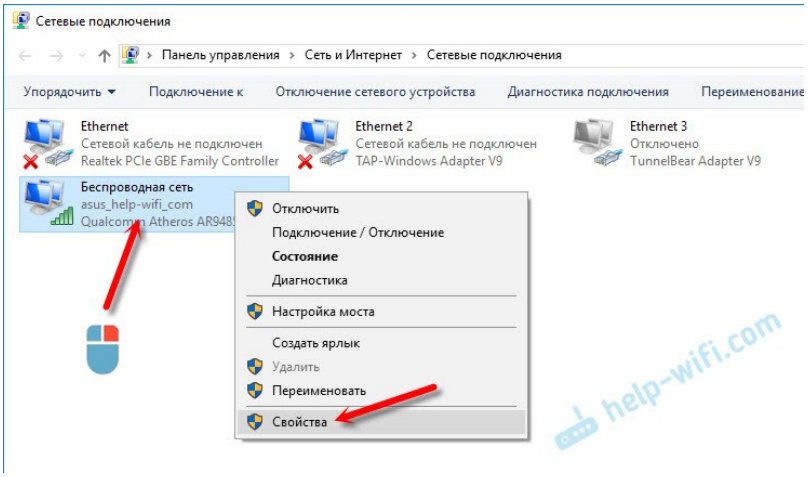

Рисунок 19 – Окно сетевых подключений

В окне «Свойства» выделяем пункт IP версии 4 (TCP/IPv4), и нажимаем на кнопку «Свойства». В большинстве случаев, компьютер получает настройки автоматически от роутера, или провайдера. Поэтому, получение IP-адреса оставляем автоматически (если провайдер, или администратор вашей сети не требует статических настроек), а DNS прописываю вручную и нажимаю Ok. Указываю такие адреса: 8.8.8.8 / 8.8.4.4. Как на скриншоте ниже (рисунок 20).

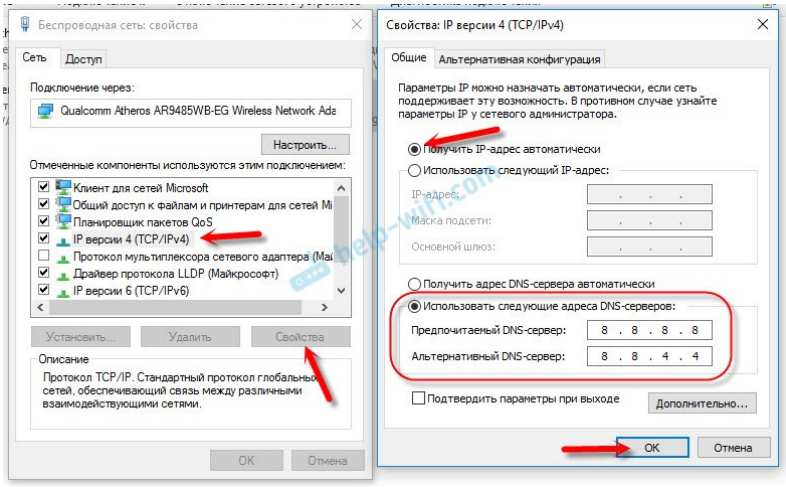

Рисунок 20 – Свойства IPv4

Компьютер желательно перезагрузить. Если это не помогло, и подключение через маршрутизатор, то можно попробовать вручную задать настройки IP.

Задаем статические адреса для IPv4: нужно узнать IP-адрес своего роутера. Скорее всего, это 192.168.1.1, или 192.168.0.1. Он должен быть указан на самом маршрутизаторе.

В поле IP-адрес прописываем адрес роутера и меняем последнюю цифру. Например: 192.168.1.10. Маска подсети – будет выставлена автоматически. Основной шлюз – IP-ёадрес роутера. DNS можно оставить «получать автоматически», или прописать свои (рисунок 21).

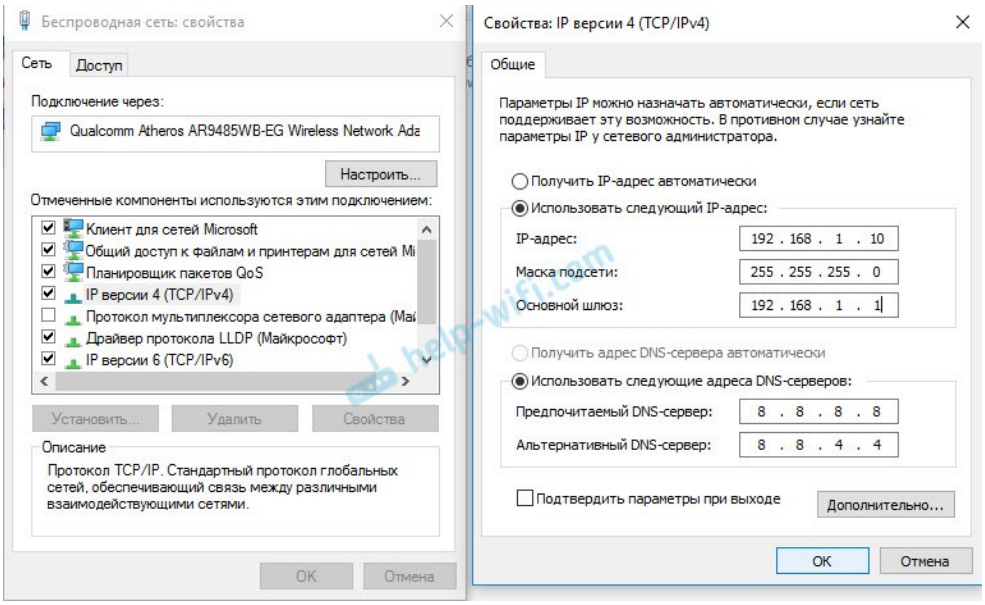

Рисунок 21 – Свойства IPv4

Если рекомендации не помогли, и выяснилось, что проблем на стороне интернет-провайдера нет, или интернет работает на других устройства от этого же маршрутизатора, то можно попробовать сделать сброс настроек сети.

В том случае, если проблема в маршрутизаторе, то можно проверить его настройки, или сбросить их к заводским, и выполнить поворотную настройку.

Отсутствие доступа к интернету, или сети для IPv4, это практически та же проблема, что без доступа к интернету в Windows 7, и Ограничено в Windows 10.

Заключение

IP-адреса нужны, чтобы передавать данные внутри сетей. Их делят на классы A, B и C — для больших, средних и маленьких сетей. Ещё есть классы D и E, но они нужны для служебных задач.

Логически IP-адрес поделён на номер сети и номер хоста (устройства). Эти части позволяют определить, к какой сети подключено устройство и какой у него номер.

Маска подсети помогает удобно выделять из IP-адреса номер сети и номер хоста. Она выглядит как обычный IP-адрес, но на самом деле представляет собой набор последовательных единиц и нулей. Первые показывают, сколько битов занимает номер сети в IP-адресе, а второй — сколько битов принадлежит номеру хоста.

Ещё маски позволяют создавать подсети внутри одной сети. В этом случае подсети будут соединены одним компьютером, который похож на роутер. Он помогает хостам из разных сетей общаться между собой.

По сей день самым популярным протоколом является IPv4. Когда впервые появился IPv4, оказалось, что адресов хватает для всех устройств, подключённых к сети. Однако население мира быстро растёт вместе с числом устройств, имеющих доступ к интернету, что увеличивает потребность в IP-адресах.

Кроме того, в результате продолжающихся технологических достижений почти во всех сферах общества выросло больше сетей. Следовательно, это подразумевает увеличение количества IP-адресов. Это привело к разработке нового типа IP-адреса, такого как IPv6, который обладает более выдающимися характеристиками и ёмкостью.

Список используемой литературы

1. Березин, С.В. Internet у вас дома / С.В. Березин, С.В. Раков. - М.: СПб: БХВ-Петербург; Издание 2-е, перераб. и доп., 2018. - 752 с.
2. Богданов-Катьков, Н.В. Интернет: Новейший справочник / Н.В. Богданов-Катьков, А.А. Орлов. - М.: Эксмо, 2015. - 928 с.
3. Ватаманюк А. Домашняя и офисная сеть. Самоучитель. - СПб.: Питер, 2017;
4. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 1 : учебник и практикум для СПО / М. В. Дибров. — М.: Издательство Юрайт, 2019. — 333 с.
5. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей : учеб. пособие для магистратуры / О. М. Замятина. — М. : Издательство Юрайт, 2017. — 159 с.
6. Иванова Т.И., Корпоративные сети связи, Изд.:Эко-Тренд, 2012, 284с.
7. Кенин, А.М. Самоучитель системного администратора / А.М. Кенин. - М.: БХВ-Петербург, 2018. - 560 с.
8. Райс, Л. Эксперименты с локальными сетями микро-ЭВМ / Л. Райс. - М.: Мир, 2018. - 268 с.
9. Сети и телекоммуникации: учебник и практикум для академического бакалавриата / К. Е. Самуйлов [и др.]; под ред. К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — М.: Издательство Юрайт, 2019. — 363 с.
10. Хаит Крейг. Персональные компьютеры в сетях TCP/IP / Перев. с англ. - BHV-Киев, 2014.
11. Хиллс, М.Т. Программирование для электронных систем коммутации / М.Т. Хиллс, С. Кано. - М.: Связь, 2014. - 248 с.
12. Microsoft TCP/IP. Учебный курс. - М.: Microsoft Press. Русская Редакция; Издание 3-е, испр., 2015. - 400 с.