Урок 7

Углубленное изучение сетевых технологий. Часть 2

Семейство технологий Wi-Fi. Технологии VLAN (802.1Q). Введение в IPv6

Технологии, применяемые в сетях Ethernet

- Виртуальные локальные сети VLAN
- STP
- Агрегация каналов
- Port Security
- 802.1x
- ACL
- QoS
- LLDP

VLAN

Технология Wi-Fi

Особенности работы Wi-Fi

- Безопасность в Wi-Fi
- Формат кадра IEEE 802.11

- CSMA/CA
- RTS/CTS
- Ad Hoc – маршрутизация

Введение в IPv6

- Недостатки и ограничения протокола IPv4
- IPX как предшественник IPv6
- Идеи IPv6
- IPv6
- Особенности адресации IPv6
- Сравнение IPv4 и IPv6
- Формат IPv6 пакета
- Популярность IPv6 адресов
- 6to4

Практическое задание

Дополнительные материалы

Используемая литература

Технологии, применяемые в сетях Ethernet

Виртуальные локальные сети VLAN

Виртуальные локальные сети используются для объединения узлов сети в логические группы, чей трафик изолируется друг от друга, включая широковещательную рассылку. Иными словами, передача кадров между абонентами разных виртуальных сетей с использованием физической адресации становится невозможна вне зависимости от используемого типа адреса (индивидуальный, групповой или широковещательный). В виртуальной локальной сети кадры транслируются между устройствами согласно таблица коммутации (только на порт, который соответствует адресу назначения для передаваемого кадра). Благодаря технологии VLAN уменьшается размер широковещательного домена и уменьшаются проблемы передачи широковещательных кадров и вызываемые ими явления, например, широковещательный шторм, который может возникнуть в результате неправильной коммутации оборудования и привести к сбою передачи данных в пределах широковещательного домена.

IEEE 802.1Q — это открытый стандарт виртуальных локальных сетей, который описывает процесс тегирования кадров для добавления служебной информации о том, что кадр относится к определенному VLAN.

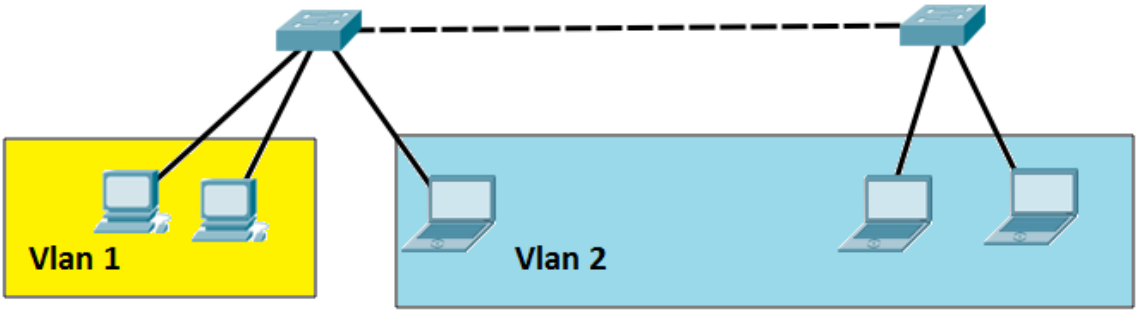
Технология VLAN обладает рядом преимуществ.

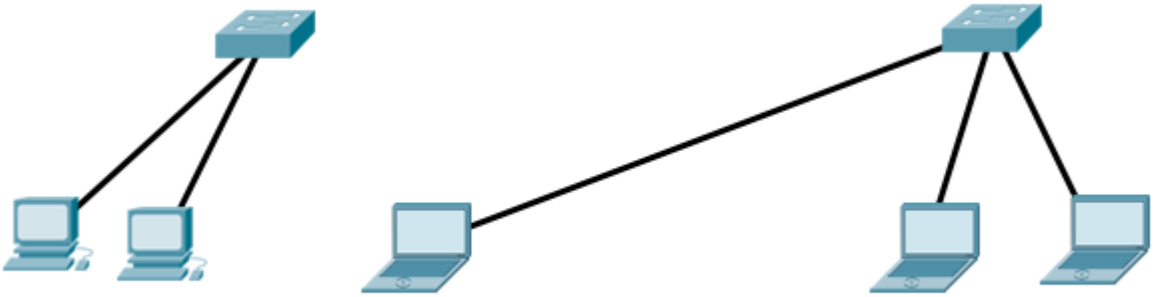
VLAN позволяют эффективно логически группировать сетевых пользователей в виртуальные рабочие группы независимо от их физического местоположения в сети.

VLAN уменьшает границы широковещательного домена, что позволяет лучше контролировать широковещательные сообщения и, как следствие, увеличивает эффективную полосу пропускания, доступную пользователям.

VLAN повышает безопасность сети, изолировав абонентов в разных локальных сетях с помощью листов доступа на коммутаторах или маршрутизаторах, системный администратор может задать политику передачи данных и взаимодействия хостов из разных виртуальных сетей.

VLAN совместим с устройствами, которые не поддерживают этот стандарт. 802.1Q не изменяет стандартную служебную информацию в кадре, а пользуется специализированным полем, поэтому сетевые устройства, которые не знают про этот стандарт, могут передать кадр без обработки информации о VLAN.





QinQ (IEEE 802.1QinQ) — расширение к стандарту IEEE 802.1Q, описывающее как тегированный трафик, может передаваться внутри уже тегированного по 802.1Q трафика. Эта технология имеет большое значение для построения Metro Ethernet-сетей. Для использования QinQ-инкапсуляции требуется поддержка со стороны коммутатора.

Типы VLAN.

- По порту (Port-based, 802.1Q).
- По MAC-адресу (MAC-based).
- По протоколу (Protocol-based).
- Методом аутентификации 802.1x.

Преимущества VLAN.

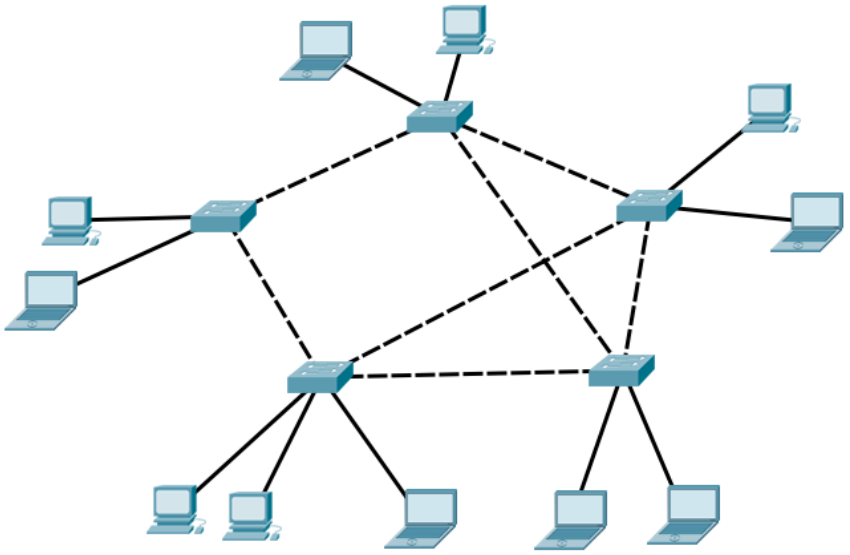
- Увеличение мобильности устройств и быстрое создание логических групп.
- Гибкие возможности создания политики безопасности и контроля трафика со стороны администратора благодаря изоляции сетевых сегментов между собой и возможности контроля пакетов на сетевом уровне при маршрутизации между сетями.
- Снижение размеров широковещательного домена и, как следствие, уменьшение количества широковещательного трафика.

- Снижение нагрузки на процессоры коммутационного оборудования за счет уменьшения количества широковещательных кадров.
- Снижение влияния широковещательного шторма в случае возникновения петли и уменьшение потерь трафика.

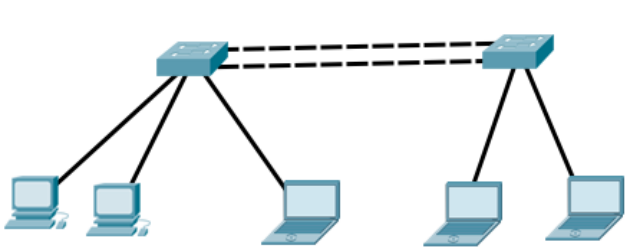
STP

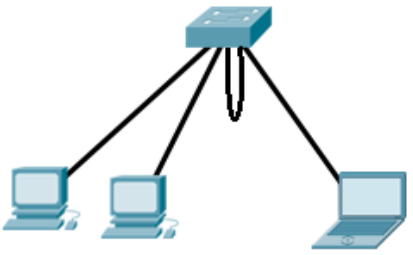
Spanning Tree Protocol (STP, семейство протоколов покрывающего или связующего дерева) — протокол канального уровня. Основная функция протоколов STP - предотвращение широковещательных штормов путем устранения колец в сетях Ethernet, возникающих вследствие избыточных соединений между коммутаторами. STP в автоматическом режиме анализирует топологию сети и при возникновении кольцевой или многосвязной топологии блокирует избыточные соединения, образуя иерархическую топологию во главе с корневым коммутатором.

Протокол описан в стандарте IEEE 802.1d. STP основан на одноимённом алгоритме, который разработала Радья Перлман. Сейчас повсеместно используется следующая версия IEEE 802.1w-2001 RSTP, отличающаяся малым временем вычисления топологии.



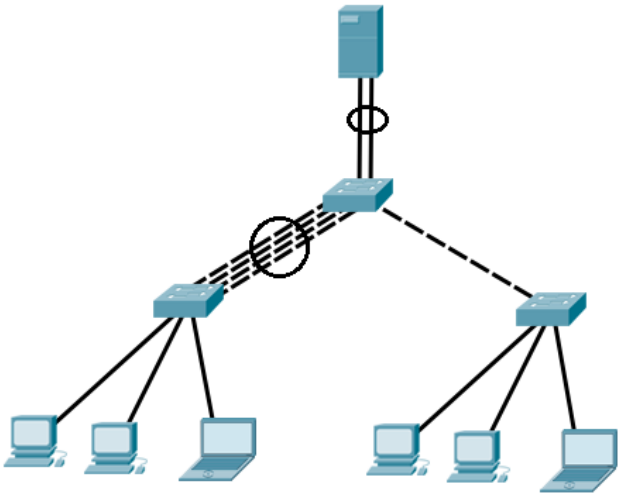
Петля коммутации (Bridging loop, Switching loop) - состояние в сети, при котором происходит бесконечная пересылка фреймов между коммутаторами, подключенными в один и тот же сегмент сети.





Агрегация каналов

Агрегирование каналов (агрегация каналов, англ. link aggregation) — технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором, между коммутатором и хостом.



Агрегирование каналов позволяет решить две задачи.

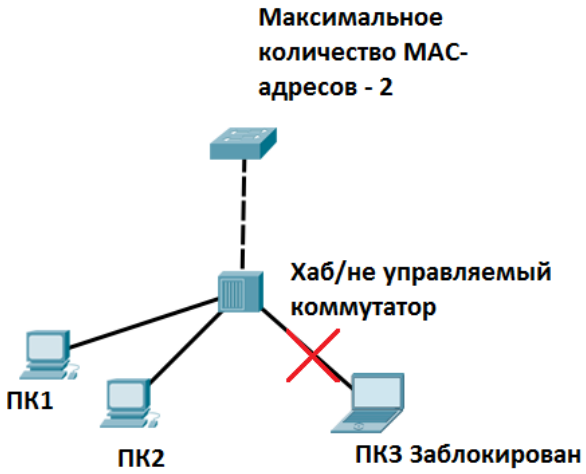
- Повысить пропускную способность канала.
- Обеспечить резерв на случай выхода из строя одного из каналов.

Link Aggregation Control Protocol (LACP) — протокол канального уровня, обеспечивающий работу нескольких физических соединений как один логический канал. Данная технология обеспечивает резервирование, повышение отказоустойчивости и пропускной способности. Используется между двумя устройствами канального уровня, может быть настроена между двумя коммутаторами или коммутатором и сервером.

Протокол LACP используются для управления и мониторинга канальной группы. Существует несколько технологий агрегации Ethernet-каналов. Применение протокола LACP может помочь в диагностике линии связи и определить обрыв в канале, который не будет обнаружен при работе статической агрегации. Протокол в некоторых случаях позволяет обнаружить повреждённый канал, который бы при использовании обычной статической агрегации обнаружен бы не был. Технология агрегации описана в стандарте IEEE 802.3ad.

Port Security

Функция безопасности портов или port security позволяет зафиксировать один или несколько физических адресов, закрепленных за портом коммутатора. При включенной функции port security коммутатор перестает изучать поступившие кадры и добавлять их в ARP таблицу. Все кадры, поступившие от MAC-адреса, не внесенного в разрешенный список, отбрасываются. Также существует возможность указать количество хостов на один порт, таким образом ограничив количество изучаемых MAC-адресов.



Данная функция обеспечивает безопасность сети на канальном уровне сети.

- Запрещается несанкционированная смена MAC-адреса компьютера или подключение нового устройства.
- ARP таблица коммутаторов защищена от переполнения вызванных сетевыми атаками.

802.1x

Протокол 802.1X работает на канальном уровне и определяет механизм контроля доступа к сети на основе принадлежности к порту (в контексте стандарта порт — точка подключения к сети).

Наибольшее распространение протокол получил в беспроводных сетях.

Согласно протоколу 802.1X доступ к сети получают только клиенты, прошедшие аутентификацию, если аутентификация не была пройдена, доступ с соответствующего порта будет запрещен.

802.1X предполагает использование модели точка-точка. То есть он не может быть применен в ситуациях, когда несколько хостов соединяются с коммутатором (на котором настроена аутентификация 802.1X) через хаб или через другой коммутатор.

ACL

Access Control List или сокращенно ACL — списки контроля доступа, описывающие действия, которые необходимо выполнить с полученными кадрами или пакетами. Листы доступа позволяют запрещать или разрешать доступ определенным абонентам, помечать трафик как приоритетный или наоборот, блокировать его.

ACL широко используются не только в сетях, но и в файловых системах для настройки политик доступа.

Доступные опции для канального уровня.

- MAC-адрес получателя и отправителя.
- Port.
- VLAN.
- QoS.

Коммутаторы сетевого уровня дополнительно анализируют пакеты и могут использовать информацию сетевого уровня: IP-адрес получателя и отправителя, порты и протоколы.

QoS

Quality of Service, QoS, качество обслуживания.

Type of Service (ToS) — поле в IP-заголовке (1 байт). Предназначено для маркировки трафика на сетевом уровне.

Class of Service (CoS) — поле из 3 бит в теге 802.1Q Ethernet-кадра.

Значения поля IP Precedence и соответствующие названия.

Имя	Десятичное значение	Двоичное значение
Routine	Precedence 0	000
Priority	Precedence 1	001
Immediate	Precedence 2	010
Flash	Precedence 3	011
Flash Override	Precedence 4	100
Critic/Critical	Precedence 5	101
Internetwork Control	Precedence 6	110
Network Control	Precedence 7	111

LLDP

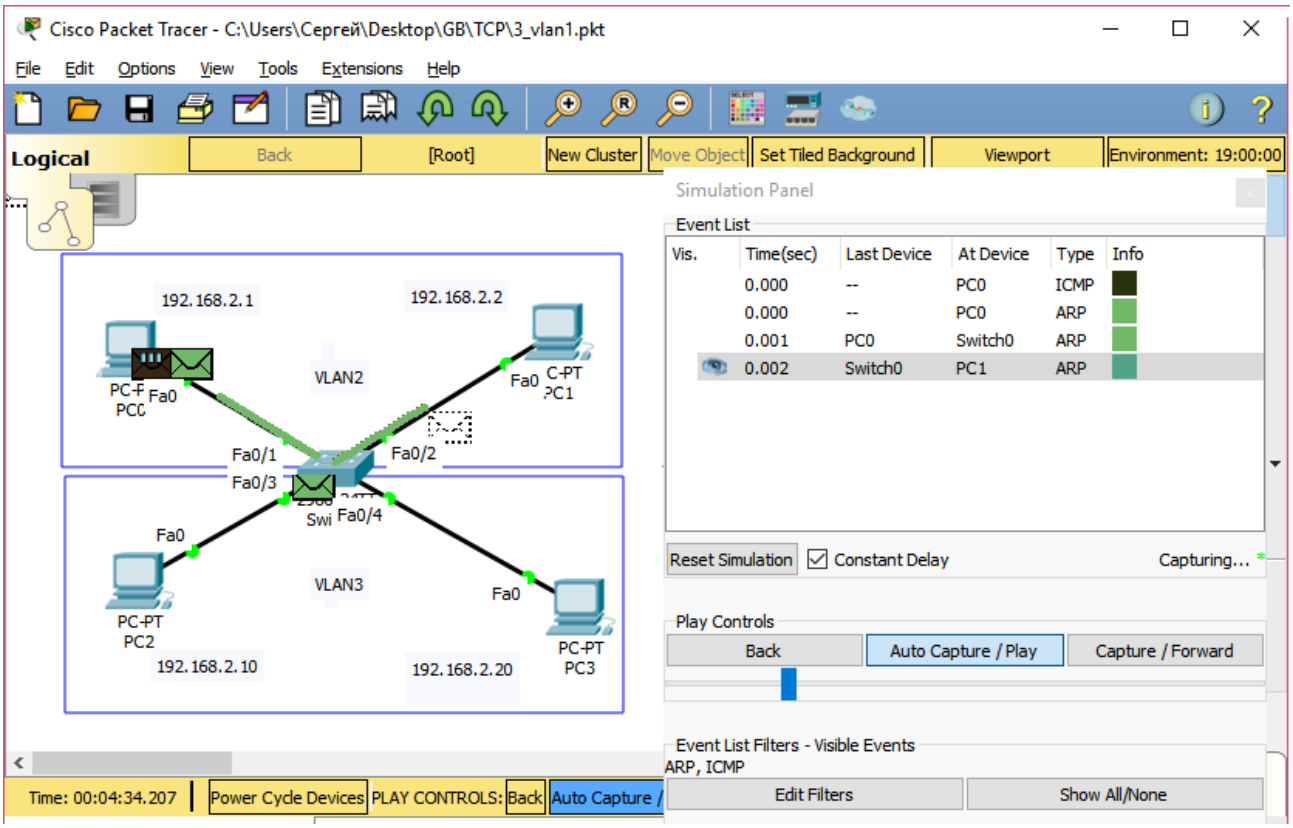
Link Layer Discovery Protocol (LLDP) — протокол канального уровня, который позволяет сетевым устройствам анонсировать в сеть информацию о себе и о своих возможностях, а также собирать эту информацию о соседних устройствах.

LLDP - это стандартный протокол, который описан в IEEE 802.1AB.

VLAN

Более подробная информация о VLAN http://xgu.ru/wiki/VLAN.

VLAN (Virtual LAN) описывается стандартом IEEE 802.1Q и определяет организацию нескольких виртуальных сетей на канальном уровне. VLAN позволяет группировать порты маршрутизатора с поддержкой VLAN, создавая своего рода “виртуальные коммутаторы”. При этом каждому порту задается принадлежность номеру соответствующей VLAN и трафик из одной VLAN в другую не попадет.

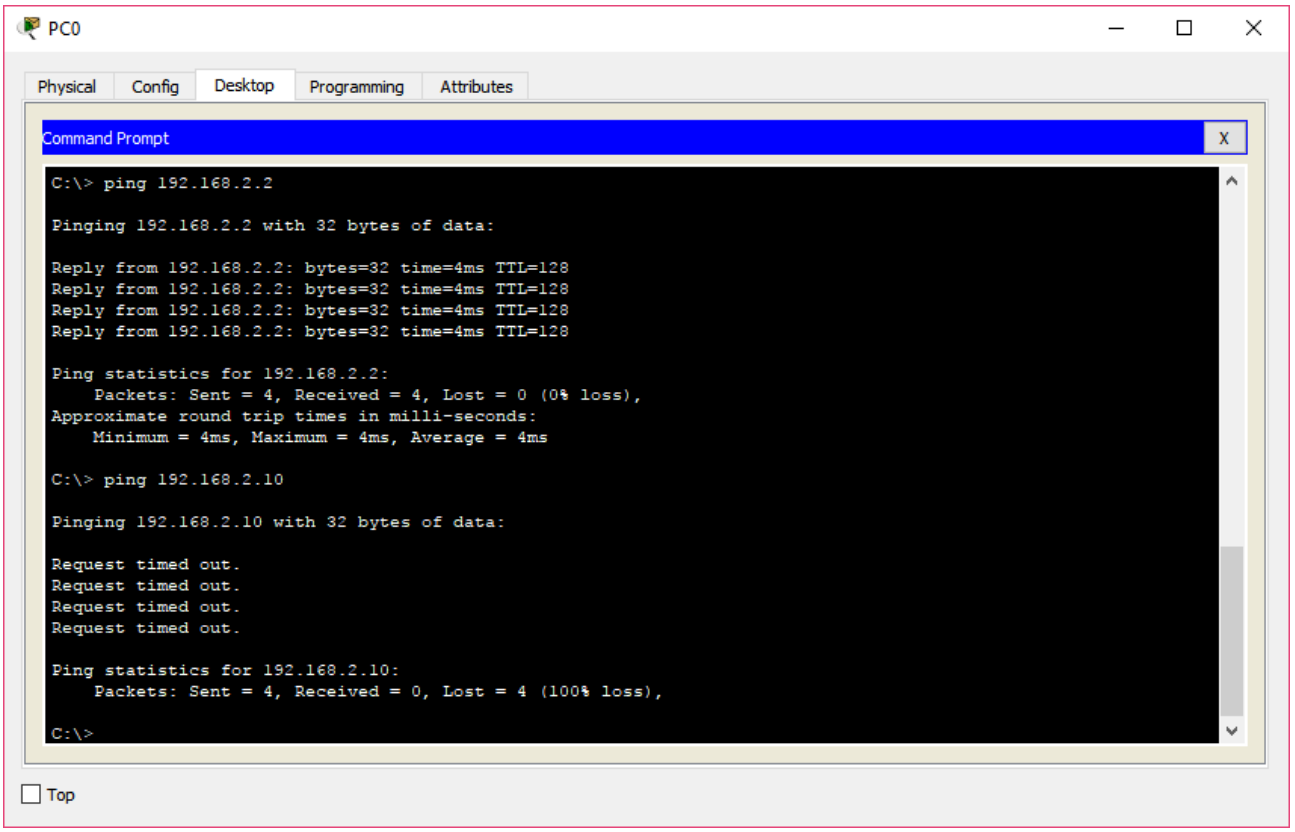


При прохождении кадров коммутатор проверяет, принадлежат ли исходящий и входящий порт одному VLAN (порт может принадлежать только одному VLAN, если он не является транковым, об этом позже). При этом получатели не знают, что работают с VLAN, формат кадров ничем не изменяется.

На схеме мы видим, что ARP-запрос не тиражируется во все порты, а отправляется только в порт, принадлежащий VLAN2. Таким образом VLAN ограничивает броадкаст-домен.

Это может быть полезным для обеспечения большей безопасности сегментов сети, исключения атаки канального уровня (ARP-spoofing, DHCP-spoofing, DDOS) и вышестоящих уровней.

Мы можем убедиться, что узлы не из нашего VLAN недоступны.



Конфигурация для коммутатора.

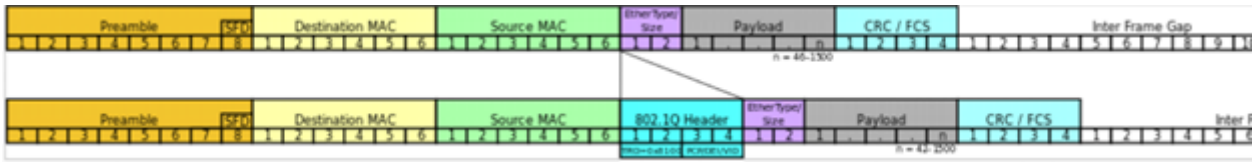
```
Switch>
Switch>ena
Switch#show run
Building configuration...

Current configuration : 1276 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/2
```

```
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
```

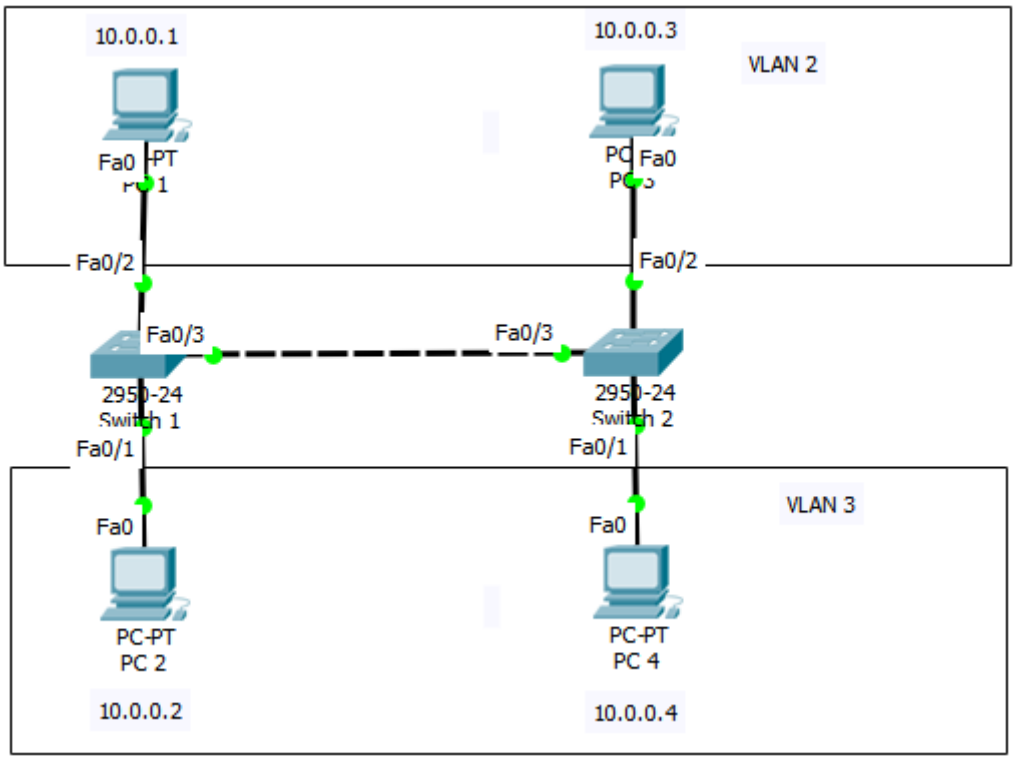
```
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
end
```

Схожей схемы работы можно было бы добиться без VLAN, используя два не связанных между собой коммутатора.

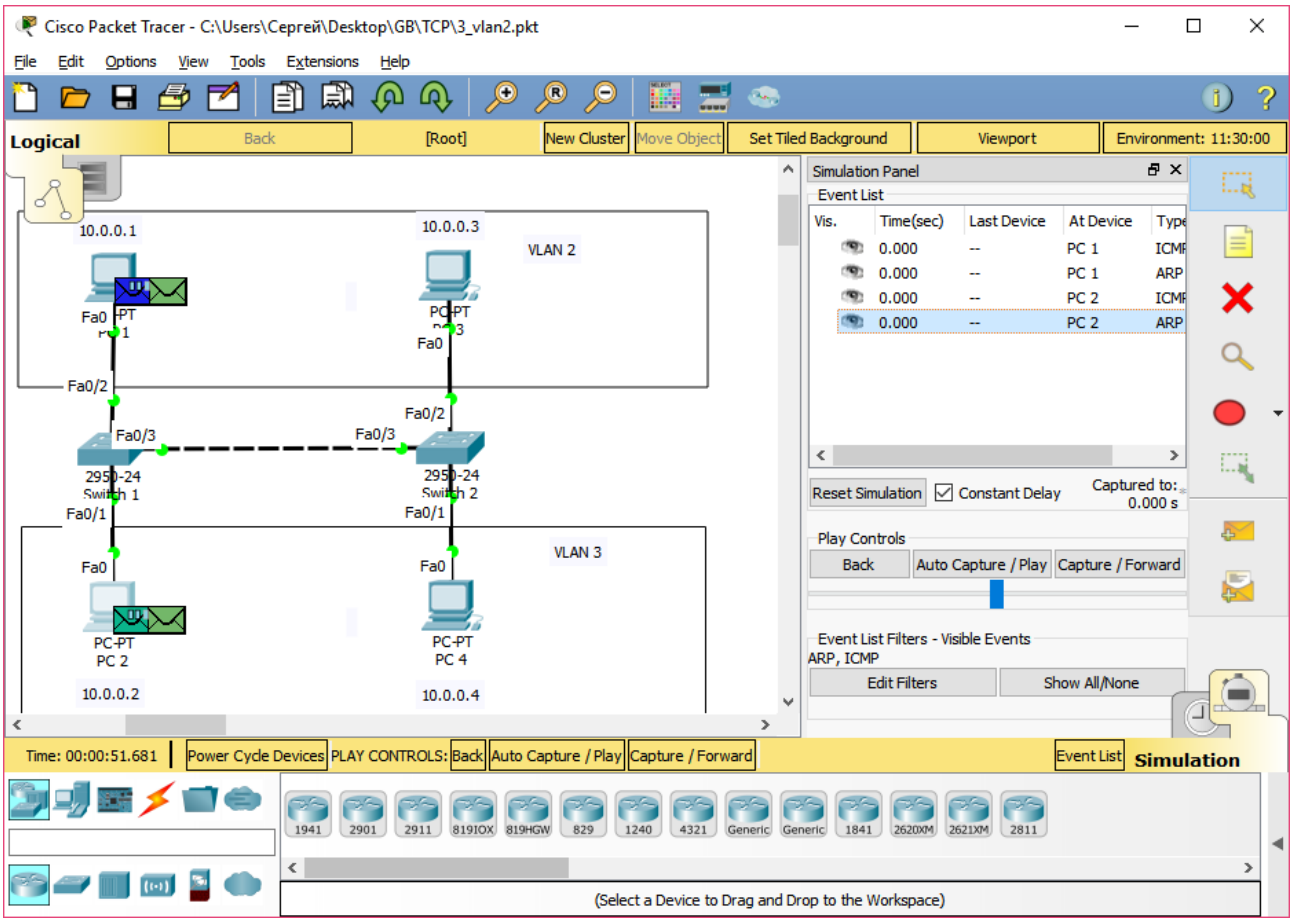
Но это не сильно гибко, как быть, если имеется несколько коммутаторов и на каждом будут присутствовать порты из каждой VLAN. Для этого используется тегированный трафик. Один и тот же канал используется для передачи трафика разных VLAN, но принадлежность VLAN будет обозначаться вставкой. Такой порт называется тегированным, в терминологии Cisco – транковым. Он может входить в несколько VLAN (фактически в одном физическом канале осуществляется мультиплексирования нескольких логических VLAN-каналов). Достигается это добавление в формат кадра еще одного поля: 802.1Q Header.



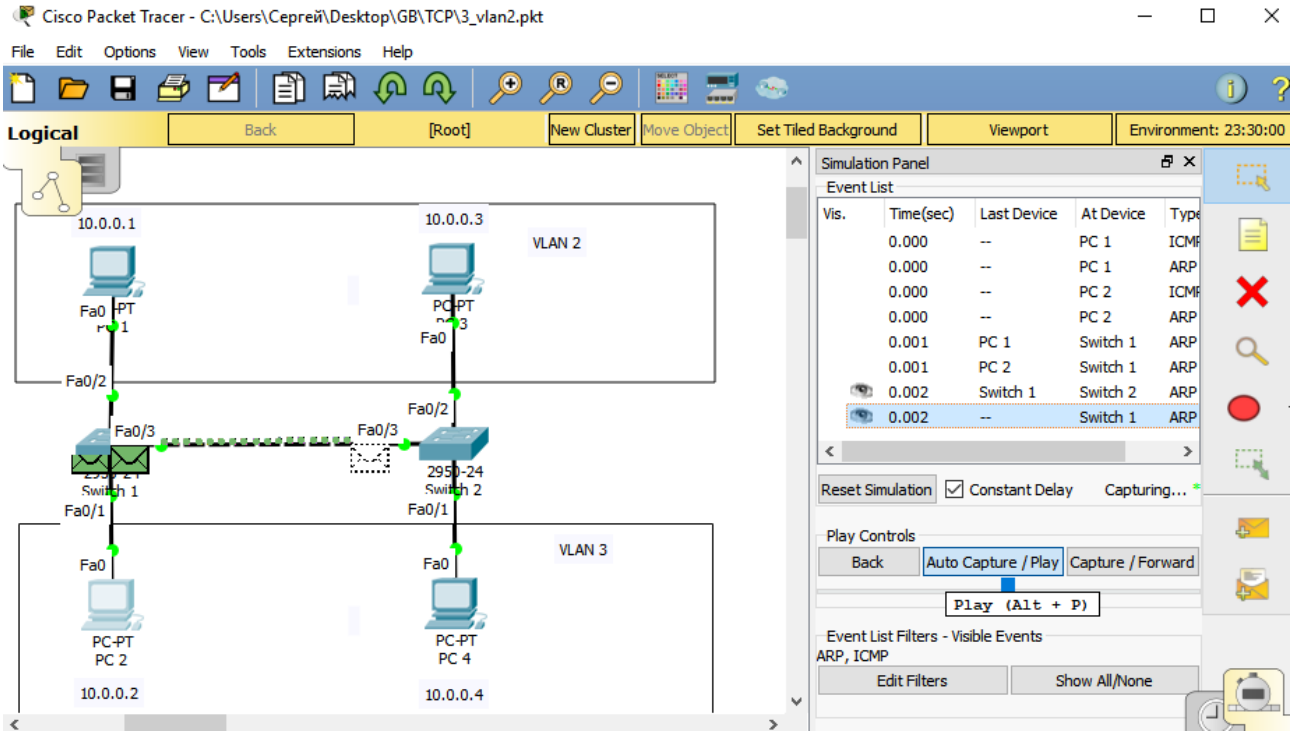
Формат кадра для IEEE 802.3 и IEEE 802.Q.



Ситуация вроде бы похожая, но теперь у нас два коммутатора. Чтобы реализовать такую технологию без VLAN, пришлось бы использовать уже четыре коммутатора. Два в первой сети и два во второй. Чтобы реализовать такую технологию без тегирования трафика, пришлось бы использовать два соединения между коммутаторами, что избыточно. Порт Fa0/3 в Switch1 и порт Fa0/3 в Switch2 — транковые. Они пропускают трафик и VLAN1 и VLAN2, но трафик помечен благодаря заголовку 8021.Q.



Попробуем отправить ping с 10.0.0.1 на 10.0.0.3 и с 10.0.0.2 на 10.0.0.4. Сначала будут отправлены ARP-запросы. ARP-запросы не попадают в чужие VLAN, но транслируются по одному и тому же транковому порту.



Настройки Switch1.

```
Switch>
Switch>ena
Switch#show run
Building configuration...

Current configuration : 1137 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 2
switchport mode access
!
```

```
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
```

```
login
line vty 5 15
login
!
!
!
end


Switch#
```

Особое значение в сетевых устройствах Cisco имеет Native port. Обычно он принадлежит VLAN1. Это нетегированный порт, в который будет отправляться по умолчанию нетегированный трафик, пришедший на тегрированный порт.

Подробнее: http://xgu.ru/wiki/Native_VLAN

Стоит отметить, что поддержку VLAN можно включить и в Linux, FreeBSD и других сетевых ОС.

Технология Wi-Fi

Особенности работы Wi-Fi

Wi-Fi — популярная технология для беспроводного обмена данными компьютерами, (некоторыми) мобильными телефонами и прочими устройствами. Фактически является обобщающим термином для множества технологий и протоколов, описанных в стандартах IEEE 802.11. Особенностями данной технологии является: ограниченный радиус действия, высокие скорости, простое подключение к сети без прокладки сетевых проводов.

Сферы применения.

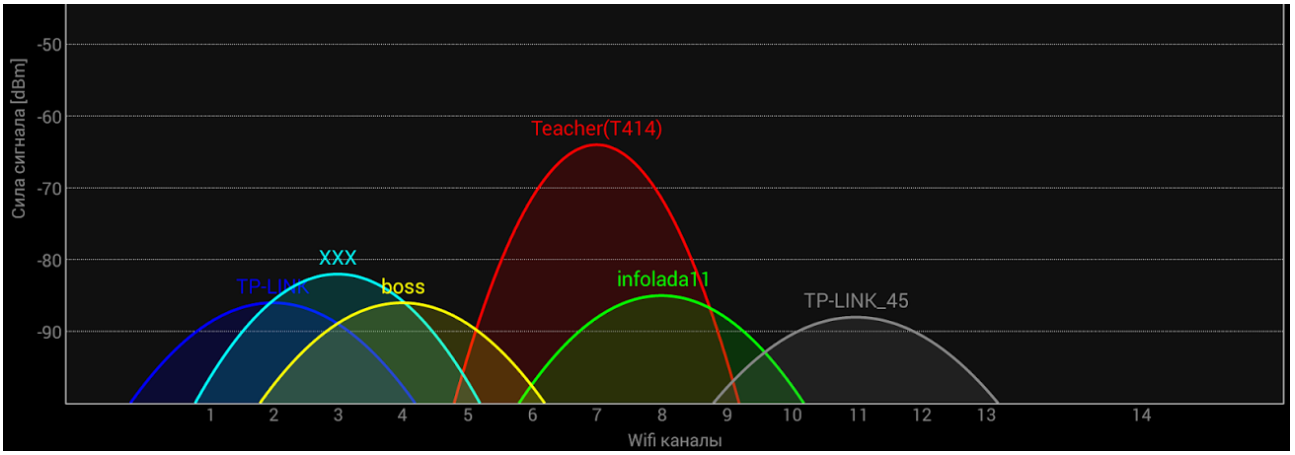
- Доступ в интернет.
- Домашняя сеть.
- Радиомосты.
- Корпоративные сети.

На данный момент сетевые популярные стандарты wifi: 802.11 g/n/ac.

Стандарты IEEE 802.11 работают на физическом и канальном (1 и 2) уровнях сетевой модели и используют диапазоны 2,4 и 5 ГГц.

Стандарт G работает в диапазоне 2,4 ГГц, стандарт N поддерживает работу в обоих диапазонах. Стандарт AC работает только в 5 ГГц диапазоне. Диапазон 2,4 ГГц характеризуется меньшим количеством каналов, но большим радиусом покрытия в связи с большим размером длины волны.

Стандарт AC эффективно применять внутри одного помещения, благодаря этой технологии можно добиться очень высоких скоростей передачи, при этом сети, находящиеся в соседних помещениях, не будут оказывать значительного влияния. При работе в диапазоне 2,4 ГГц необходимо исходить из реальной загрузки каналов. На рисунке ниже приведено сканирование радиоэфира. 1



В настройках точки доступа вы можете указать 20 или 40 mhz. При высоком уровне помех от других сетей расширение канала приведет к увеличению количества повторных передач и, как следствие, к снижению производительности канала.

802.11-B – 2 ггц. Скорости до 11 мбит. – В настоящее время протокол устарел.

802.11-G – 2 ггц. Скорости до 54 мбит.

802.11-A – 5 ггц. Скорости до 54 мбит.

802.11-N – 2/5 ггц. Скорости до 450 мбит. – Наиболее распространенная сейчас версия.

802.11-AC – 5 ггц. Скорости до 6 гбит. – Набирающая популярность и работающая в флагманских моделях телефонов версия.

Реальные скорости, которые можно получить в канале, значительно ниже теоретических и зависят от целого ряда условий: чистоты радиоэфира, количества используемых приемопередатчиков, удаления абонентов. Кроме основных данных большую часть занимает служебная информация, а скорость всего канала делится между всеми абонентами.

Ниже приведена реальные пропускные способности, которые можно получить.

802.11-B – 2 ггц. Пропускная способность менее 5 мбит.

802.11-G – 2 ггц. Пропускная способность менее 22 мбит.

802.11-A – 5 ггц. Пропускная способность менее 22 мбит.

802.11-N – 2/5 ггц. Пропускная способность менее 150 мбит.

Некоторые стандарты предусматривают работу на нескольких диапазонах. Для частоты 2.4ггц это 802.11 B/G/N. На этой частоте работают рации, Bluetooth, микроволновки. Данная частота эффективно огибает препятствия и наиболее распространена.

Частота 5 ггц используется 802.11 A/N/AC. Работа устройства (роутера) на всех стандартах снижает эффективность работы и пропускную способность, в связи с тем, что служебная информация передается со скоростью работы самых медленных абонентов в сети, поэтому желательно указывать используемый стандарт беспроводной сети.

Существует стандартная сетка каналов диапазона 2.4ггц.

2412 = 1

2417 = 2

2422 = 3

2427 = 4

2432 = 5

2437 = 6

2442 = 7

2447 = 8

2452 = 9

2457 = 10

2462 = 11

2467 = 12

2472 = 13

2484 = 14

Стоит заметить, что непересекающихся каналов всего 3: первый, шестой и двенадцатый. Это связано с тем, что спектр сигнала распространяется на соседние каналы. Сейчас точки доступа обладают возможностью автоматического выбора канала, но не всегда могут работать оптимально. Также анализ радиоэфира может помочь при диагностике и выявлении таких проблем, как низкая производительность сети или нестабильная работа.

Стандартная сетка каналов диапазона 5 ггц.

36 = 5180

38 = 5190

40 = 5200

42 = 5210

44 = 5220

46 = 5230

48 = 5240

52 = 5260

56 = 5280

60 = 5300

64 = 5320

149 = 5745

151 = 5755

153 = 5765

155 = 5775

157 = 5785

159 = 5795

161 = 5805

163 = 5815

165 = 5825

Для построения беспроводной локальной сети обычно применяется 2 типа.

- Клиентское устройство – это может быть компьютер, оснащенный беспроводным адаптером, ноутбук, планшет или телефон. Современные модели телевизоров, принтеров и даже проекторов также комплектуются беспроводными адаптерами и могут быть подключены к беспроводной сети.

- Точка доступа - устройство, выполняющее роль беспроводного коммутатора между клиентами, а также роль моста, соединяя беспроводную и проводную сеть между собой.

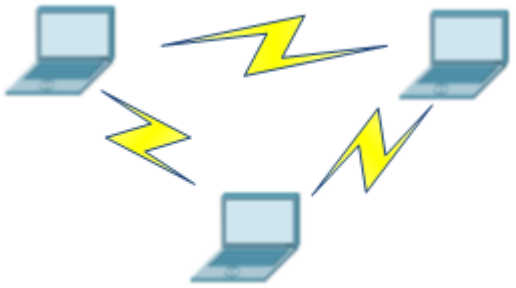
Точка доступа состоит из следующих элементов.

- Антенна. Современные точки доступа комплектуются 2 или более (до 8) антеннам.

- Приемопередатчик, подключаемые к антенне.

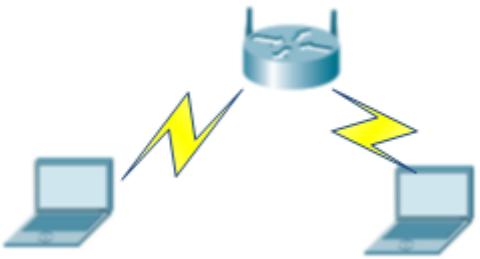
- Адаптер проводной сети, иногда выполняется в виде коммутатора, установленного в точку доступа (обычно от 1 до 5 портов).
- Материнская плата с встроенным ЦП, оперативной памятью и блоком ПЗУ.
- Программное обеспечение. Обычно это прошивка на базе embedded linux.

1. Соединение Ad-Hoc (точка-точка).
   Особенностью данного режима работы является отсутствие единого устройства для подключения. Максимальная скорость работы устройств в данном режиме ограничена 11 Мбит/с, это связано с тем, что отсутствует устройство, обеспечивающее передачу сообщений без коллизий и централизованно управляющее работой остальных устройств.

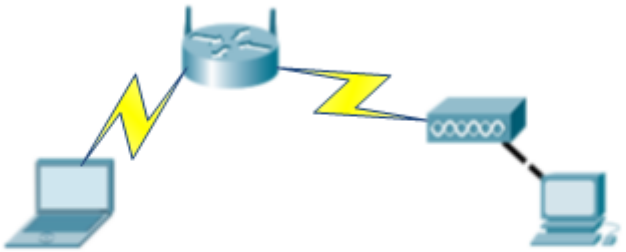


.

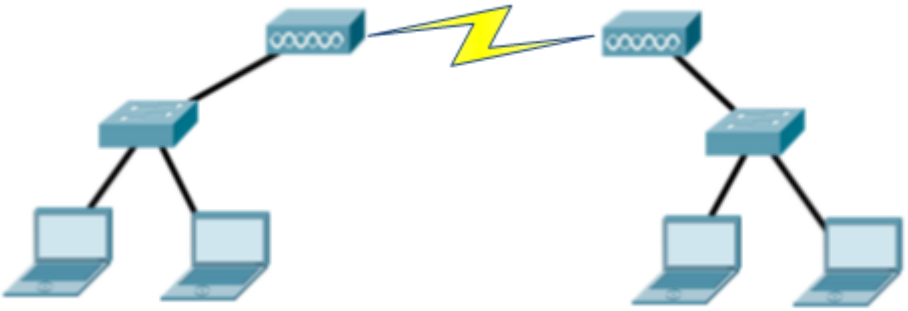
2. Точка доступа с использованием роутера или модема.
   Классический режим работы точки доступа. Используется по умолчанию в домашних роутерах для подключения абонентов беспроводной сети к сети провайдера или локальной сети.



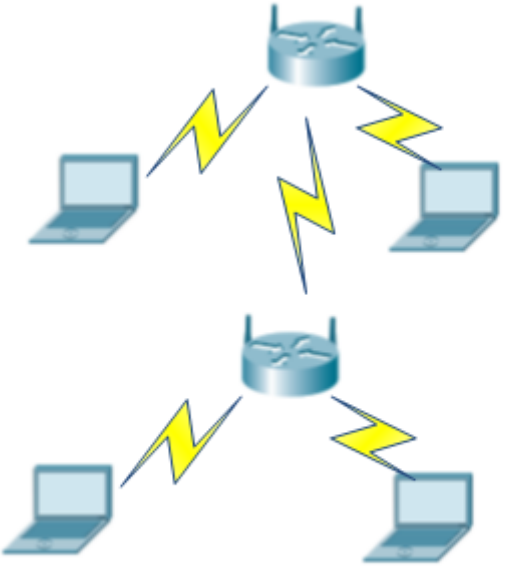
3. Клиентская точка.
   Данный режим работы нужен для подключения устройств, на которые физически нет возможности установить беспроводную сетевую карту, но их необходимо подключить к сети с использованием беспроводной технологии. Например, сетевой принтер, в котором есть только Ethernet порт или телевизор.



4. Соединение мост.
   Соединение типа мост позволяет соединить проводные сети между собой, соединение которых с использованием проводных технологий невозможно. Например: река, железнодорожные пути и т.п.
   Прямой видимости недостаточно для выбора установки места антенны. Необходимо, чтобы между передающими устройствами не было препятствий, в случае наличия на пути домов/деревьев или других препятствий необходимо рассчитать зону между антеннами.



5. Репитер.
   Репитер устанавливают для расширения зоны покрытия беспроводной сети. Стоит заметить, что при этом скорость работы в основной сети значительно снижается, поэтому для увеличения радиуса покрытия более эффективно использовать независимые точки доступа.



Безопасность в Wi-Fi

Безопасность в беспроводной сети – это понятие, включающее в себя достоверность передаваемых данных, ограничение доступа к этим данным только доверенным пользователям. Возможность использования сети только доверенными устройствами и защищенность от внешнего влияния также относится к безопасности.

В отличие от проводных сетей к обеспечению защиты и безопасности в беспроводных сетях нужно подходить более ответственно, потому что в качестве среды передачи данных используется радиоэфир, доступный для любого пользователя, находящегося в зоне действия антенны. Обязательно использование шифрования и прочих технологий, обеспечивающих безопасность.

Основные элементы, которые могут использованы для построения безопасной беспроводной сети.

- Контроль доступа.
- Аутентификация пользователей.
- Шифрование трафика.
- Система предотвращения вторжений в беспроводную сеть.
- Система обнаружения чужих устройств и возможности их активного подавления.
- Мониторинг радио интерференции и DoS-атак.
- Мониторинг уязвимостей в беспроводной сети и возможности аудита уязвимостей.

Применяемые стандарты шифрования: WEP, WPA, WPA2.

На данный момент рекомендуемым видом шифрования является WPA2 и AES соответственно.

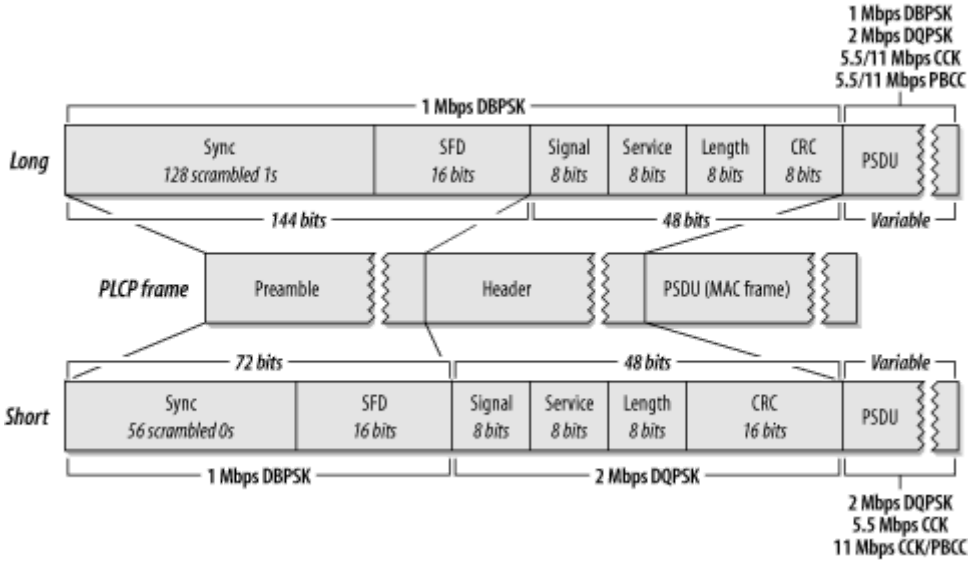
Пароль для доступа к сети необходимо задать не менее 8 символов с использованием цифр, букв и символов. Только такие настройки политики безопасности могут гарантировать защищенность вашей домашней сети.

Также рекомендуется отключить функции WPS авторизации по пин коду, так как она содержит в себе потенциальную уязвимость.

Формат кадра IEEE 802.11

IEEE 802.11 является стандартом физического и канального уровня, родственным Ethernet, при этом имеющим как сходства, так и отличия.

Вначале передается преамбула так же, как и в Ethernet, являющаяся признаком кадра. Длина поля зависит от реализации протокола.



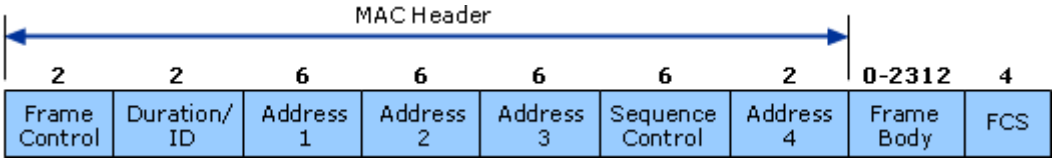
Существует длинная преамбула (в ранних версиях стандарта) и короткая преамбула (в более новых версиях стандарта.

Далее следует заголовок PLCP (Physical Layer Convergence Protocol), всегда передается на скорости 1 Мбит/с и содержит информацию для физического уровня.

- Длину фрейма.
- Скорость передачи.
- Контрольную сумму заголовка.

Поле «CRC» служит для контроля целостности фрейма. При приеме фрейма значение этого поля сравнивается с результатами расчета контрольной суммы на приемной стороне.

Затем следует заголовок MAC-подуровня.



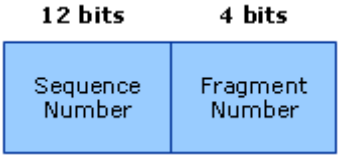
Кадр 802.11 состоит из следующих полей.

1. Frame Control — содержит управляющую информацию.
2. Duration/ID — содержит либо идентификатор станции (BSS), если при передаче используется функция энергосбережения (Power Save), либо предполагаемое время занятия канала.
3. Address 1 — Address 4 могут иметь разное значение в зависимости от структуры сети и направления передачи.
    a. Address 1 — Destination Address — всегда содержит адрес непосредственного получателя кадра (конечного получателя). Если бит «To DS» в поле Frame Control установлен в единицу, то в этом поле указан адрес точки доступа. В этом случае он называется идентификатором базового набора обслуживания (BSSID). Во всех остальных случаях – это адрес станции-получателя кадра.
    b. Address 2 — Source Address — всегда указывает адрес непосредственного отправителя. Если бит «From DS» установлен в единицу, то в этом поле задается адрес точки доступа (BSSID), в противном случае – это адрес абонента.
    c. Address 3 — Receiver Address — указывает адрес получателя (расположенного в DS), если бит «To DS» имеет значение, равное единице, или адрес отправителя (из DS), если установлен в единицу бит «From DS». В случае использования одноранговой сети или передачи служебных кадров от точки доступа, это поле содержит значение BSSID.
4. Address 4 — Transmitter Address — адрес отправителя. Используется только в случае, если DS представляет собой беспроводную сеть.

Примеры использования полей адресации.

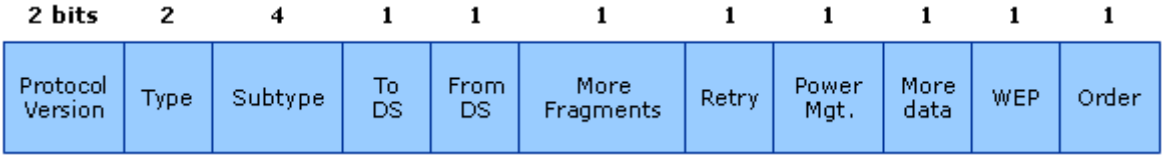
ToDS	From DS	Адрес 1	Адрес 2	Адрес 3	Адрес 4
0	0	DA	SA	BSSID	–
0	1	DA	BSSID	SA	–
1	0	BSSID	SA	DA	–
1	1	RA	TA	DA	SA

5. Sequence Control состоит из двух полей.



- Sequence Number — содержит номер кадра.
- Fragment Number — содержит номер каждой части фрагментированного кадра.

Отдельно отметим поле Frame Control.



1. Protocol Version указывает текущую версию используемого 802.11 протокола.
2. Type — тип кадра. Может принимать значения.
    a. Management (00) – фреймы для передачи служебной информации (Beacon, Probe Request, Authentication и т.д.).
    b. Control (01) – используются для контроля доступа к среде передачи, например, RTS, CTS, ACK.
    c. Data (02) – служат для передачи полезной информации.
3. Subtype — используется для деления типы на подтипы.
4. To DS и From DS — используются только для указания, отправляется кадр или приходит из распределенной системы DS (distributed system). DS установлен в единицу, если кадр адресован точке доступа для передачи его в обычную сеть (с точки зрения стандарта – DS) или другому абоненту из данного BSS. Бит «From DS» установлен в единицу, соответственно, если кадр направлен из DS.
5. More Fragments — если установлен в единицу, указывает, что кадр фрагментирован и за ним последуют еще фрагменты кадра (похоже на механизм фрагментирования в IPv4).
6. Retry — указывает на то, что данный фрейм – повторная передача предыдущего фрейма (ретрансмиссия), что позволяет принимающей станции распознавать повторяющиеся фреймы, возникающие из-за потери подтверждений.
7. Power Management — означает, что после передачи данного фрейма станция переходит в режим энергосбережения из активного режима или наоборот.
8. More Data — используется точкой доступа для того, чтобы сообщить станции, что для нее имеются данные (в буфере в точке доступа).
9. WEP — указывает на то, что фрейм зашифрован по протоколу WEP (ненадежный и взломостойкий протокол шифрования).
10. Order — указывает, что все полученные кадры данных должны быть обработаны по порядку.

CSMA/CA

CSMA/CA Carrier Sense Multiple Access With Collision Avoidance — «множественный доступ с контролем несущей и избеганием коллизий» — это сетевой протокол (рекомендация ITU-R M.1450), схожий с CSMA/CD, но вместо детектирования коллизии применяется механизм избегания коллизий. Также используется механизм прослушивания несущей волны, но при этом станция, которая собирается начать передачу, посылает jam signal (сигнал преднамеренной помехи) после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу фрейма. Если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку.

CSMA/CA отличается от CSMA/CD тем, что коллизиям подвержены не пакеты данных, а только jam-сигналы. Отсюда и название «Collision Avoidance» — предотвращение коллизий (имеется в виду предотвращение коллизий при передаче данных). Избегание коллизий используется для того, чтобы улучшить производительность CSMA, отдав сеть единственному передающему устройству. Эта функция возлагается на «jamming signal» в CSMA/CA. Улучшение производительности достигается за счёт снижения вероятности коллизий и повторных попыток передачи. Но ожидание jam signal создаёт дополнительные задержки, поэтому другие методики позволяют достичь лучших результатов. Избегание коллизий полезно на практике в тех ситуациях, когда своевременное обнаружение коллизии невозможно, например, при использовании радиопередатчиков.

Среди примеров применения CSMA/CA можно отметить Apple LocalTalk, использующий трёхбайтный jam signal и Wi-Fi IEEE 802.11 RTS/CTS, реализует CSMA/CA, используя короткие сообщения: Request to Send (запрос на отправку) и Clear to Send (готовность к отправке).

RTS/CTS

RTS/CTS (англ. Request To Send/Clear To Send — запрос на отправку/разрешение отправки) — механизм CSMA/CA, используемый в беспроводных сетях стандарта IEEE 802.11 для исключения коллизий кадров; способ решения проблем «скрытого узла» (когда два или несколько узлов сети (абонентов) пытаются получить доступ к базовой станции (точке доступа) сети, но при этом не видят друг друга, т.к. физически не могут принимать сигналы в эфире друг от друга (например, из-за большой дальности, условий распространения сигналов и т. д.) и «незащищенного узла» (когда узел слышит RTS (запрос на передачу) с соседнего узла, но не слышит соответствующего CTS (разрешения на передачу) от принимающего узла, этот узел может считать себя незащищенным узлом и иметь возможность передавать на другие узлы).

Узел, желающий отправить информацию, посылает RTS-кадр. Целевой узел отвечает CTS-кадром. Любой другой узел, получивший CTS-кадр, должен воздержаться от отправки информации на заданное время (решение Проблемы скрытого узла). Любой другой узел, получивший RTS-кадр, но не CTS-кадр от передачи информации воздерживаться не должен (решение проблемы незащищенного узла). Количество времени, которое должен ожидать другой узел перед попыткой доступа к эфиру, записано и в RTS-кадре, и в CTS-кадре.

Ad Hoc – маршрутизация

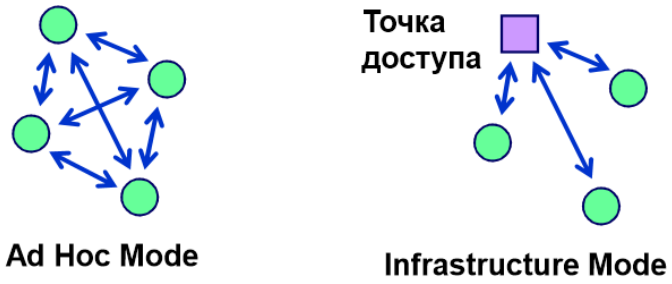
Беспроводные ячеистые сети представляют ссобой топологию, представленной маршрутизаторов, лишенной проводов между узлами. Mesh топология позволяет передавать данные на большие расстояния путём разбиения длинного маршрута на серию коротких переходов между узлами - хопов/hops. Промежуточные узлы не только усиливают сигнал, но и совместно передают его от точки A до точки B — осуществляют переадресацию, основываясь на их знании о сети в целом. Таким образом каждый узел не только является конечной точкой, но и сам осуществляет маршрутизацию.

Топология беспроводной ячеистой сети относительно постоянна. Только в случаях внезапного отключения или добавления новых узлов могут быть инициированы процессы изменения структуры сети. Маршрут движения трафика, будучи сформированным большим числом конечных пользователей, редко меняется. Практически весь трафик в топологии ячеистой сети либо направлен

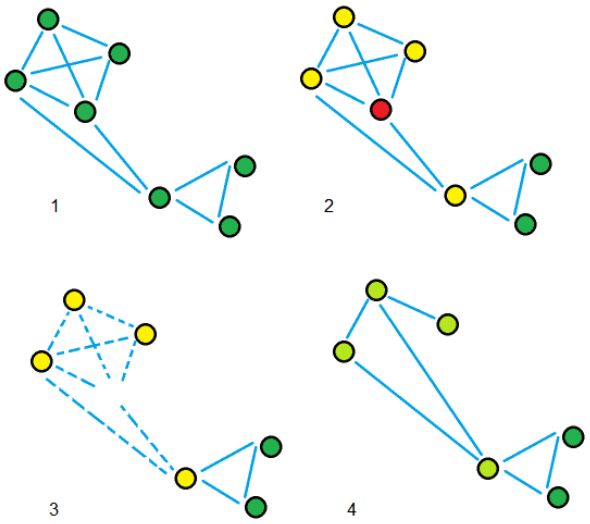
через шлюз, либо исходит из него, в то время как в беспроводных ad-hoc сетях трафик течет между произвольной парой узлов.

Беспроводная ad-hoc-сеть (беспроводная динамическая сеть, беспроводная самоорганизующаяся сеть) — децентрализованная беспроводная сеть, не имеющая постоянной структуры. Клиентские устройства соединяются «на лету», образуя собой сеть. Каждый узел сети пытается переслать данные, предназначенные другим узлам. При этом определение того, какому узлу пересылать данные, производится динамически на основании связности сети. Это является отличием от проводных сетей и управляемых беспроводных сетей, в которых задачу управления потоками данных выполняют маршрутизаторы (в проводных сетях) или точки доступа (в управляемых беспроводных сетях). Первыми беспроводными самоорганизующимися сетями были сети «packet radio», начиная с 1970-х годов, финансируемые DARPA после проекта ALOHAnet.

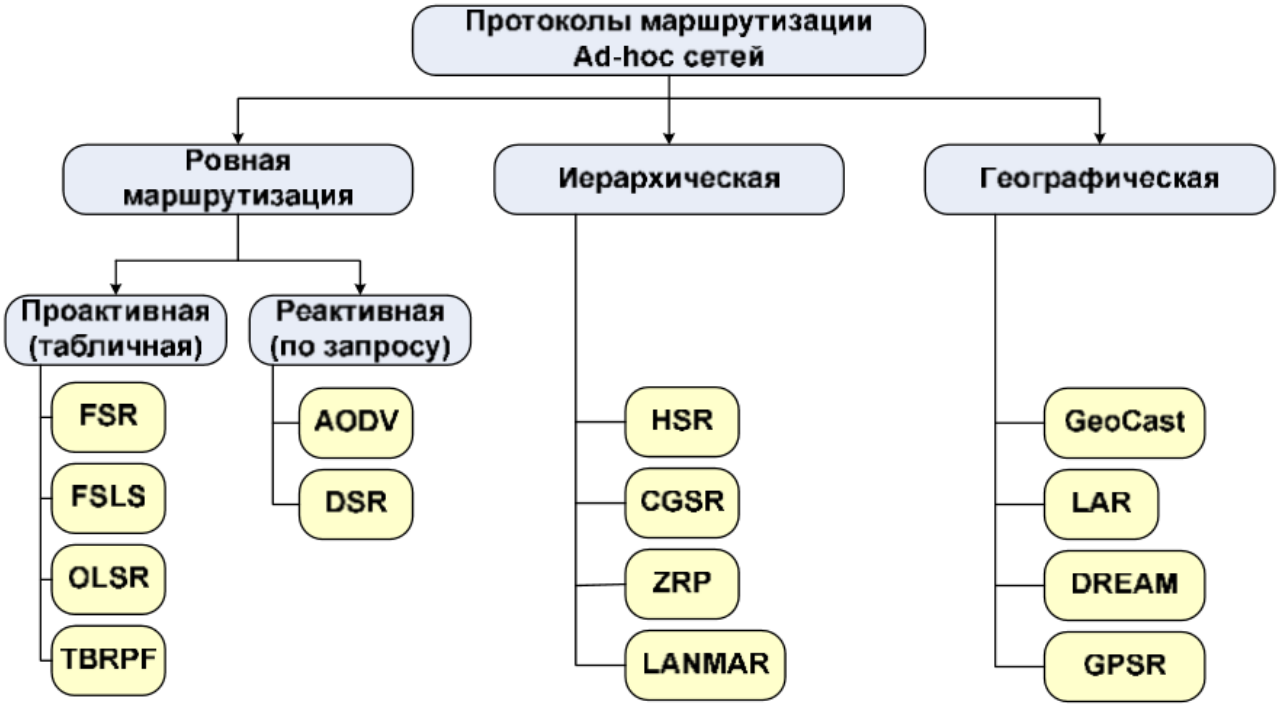
Примерами использования ad hoc сетей могут быть сенсорные сети (распределённая, самоорганизующаяся сеть множества датчиков и исполнительных устройств, объединённых между собой посредством радиоканала), мобильные сети транспортных средства (VANET — vehicular ad hoc networks), мобильные самоорганизующиеся сети (MANET).



Сравнение Ad Hoc-сетей и сетей с точкой доступа.



Пример самовосстановления сети. После выключения промежуточного узла автоматически строятся новые маршруты. Анимированная gif-картинка: https://upload.wikimedia.org/wikipedia/commons/0/06/Mesh_network_self_healing.gif.



Протоколы ad hoc маршрутизации (источник: Терновой М. Ю. «Мобильные сети: IP маршрутизация и алгоритмы MANET маршрутизации»).

В качестве примеров ad hoc маршрутизации можно привести OLSR и AODV.

OLSR (англ. Optimized Link-State Routing) — протокол маршрутизации для MANET, который также может использоваться в других беспроводных сетях. OLSR — проактивный протокол маршрутизации, использующий обмен сообщениями приветствия и контроля для получения информации о топологии сети. Узлы используют эту информацию для определения следующего прыжка в пути маршрутизируемого пакета. Является одним из наиболее популярных протоколов, которые используются для маршрутизации в беспроводных сетях MANET.

Необходимый маршрут доступен немедленно, протокол базируется на алгоритме состояния каналов. Узлы распространяют информацию о каналах с соседними узлами.

Особенности протокола: эффективен для сетей с небольшой мобильностью, хранит новейшие данные о всей сети, время нахождения нового пути меньше.

AODV (англ. Ad hoc On-Demand Distance Vector) — протокол динамической маршрутизации для мобильных ad-hoc сетей (MANET) и других беспроводных сетей. Является реактивным протоколом маршрутизации, то есть устанавливает маршрут до адресата по требованию, чем отличается от классических протоколов маршрутизации Интернета, являющихся превентивными (находящих пути

маршрутизации независимо от использования маршрутов). Как следует из названия, для вычисления маршрутов используется дистанционно-векторный алгоритм маршрутизации.

Протокол хранит данные только об активных путях, за счет чего меньше обработка служебной информации, но больше время нахождения нового пути по сравнению с OLSR. Более эффективен для сетей с высокой мобильностью.

Подробнее примеры работы OLSR и AODV см. Терновой М. Ю. «Мобильные сети: IP маршрутизация и алгоритмы MANET маршрутизации»

Введение в IPv6

IPv6 — перспективная сетевая технология, которая призвана решить проблему нехватки сетевых адресов. Адресов в IPv6 больше, чем атомов во Вселенной!

Это раньше не каждая семья могла похвастаться не только доступом в Интернет, но даже компьютером, сейчас в каждом доме найдется пара компьютеров (десктоп и ноутбук), планшетов и смартфонов. Плюс роутер, файловое хранилище, Time-капсула. А еще IP-TV и прочие IP-утюги и холодильники.

Одной из перспективных технологий считается Интернет вещей (англ. Internet of Things, IoT) — концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей, как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека. Там, где IoT, находится и IPv6. Хорошо с IPv6 будут работать и беспроводные сенсорные сети (есть стандарт 6LoWPAN (англ. IPv6 over Low power Wireless Personal Area Networks) — стандарт взаимодействия по протоколу IPv6 поверх маломощных беспроводных персональных сетей стандарта IEEE 802.15.4).

Более того, IPv6 уже в полной мере успешно применяют современные Интернет-сервисы такие, как Яндекс, Google, социальные сети.

Переход с IPv4 на IPv6 в сегменте домашнего Интернета пока тормозится провайдерами, но и он однажды случится. Потому ознакомиться с технологий IPv6 обязательно надо.

Недостатки и ограничения протокола IPv4

Главный минус существующего протокола IPv4 - это ограниченный размер адресного пространства. Адрес в протоколе IPv4 имеет размер 4 байта, что равно 32 битам. Возведя 2^32, получаем максимальный размер адресов, равный 4.294.967.296. В 70-х годах, когда протокол разрабатывался, никто не мог представить, что даже чайник будет иметь свой IP-адрес.

Нет встроенного механизма группировки адресов. Суммаризация маршрутов частично решает эту проблему, но в целом это приводит к очень большому размеру таблиц маршрутизации, которые должны находиться в памяти маршрутизирующего оборудования. На данный момент благодаря росту вычислительных возможностей данная проблема уходит на второй план, но остаются минусы, описанные в разделе про суммаризацию.

Используемый сейчас механизм автоматического конфигурирования адресов является надстройкой и выполняется за счет службы DHCP. В протокол IPv4 не был внедрен механизм автоматической

конфигурации адреса хоста в сети. Сейчас данная проблема решается либо ручной конфигурацией либо запуском службы DHCP на одном из хостов сети.

Фрагментация передаваемых данных. Существующий механизм при передаче дейтаграмм, размер которых превышает максимальный размер пакета, фрагментирует дейтаграмму на несколько пакетов. Минусом является то, что фрагментировать может не только отправитель, но и любой маршрутизатор на пути следования пакета. Фрагментация передаваемых пакетов снижает производительность и эффективность передачи в связи с увеличением количества служебной информации.

Целый ряд проблем, связанных с безопасностью коммуникации. Протокол IPv4 не предусматривает наличия встроенных механизмов обеспечения безопасности и шифрования передачи данных.

IPX как предшественник IPv6

Протокол IPX стека IPX/SPX практически можно отнести к историческим. Но мы рассмотрим протокол IPX, так как его идеи во многом повлияли на разработку IPv6. Разработчики IPX вошли в состав рабочей группы IPng (IP Next Gen), сформированной в 1992 году, чтобы в 1996 представить первую версию стандарта IPv6. Новый протокол получил название IPv6 после IPv4, потому что существовала разработка IPv5, работающая с адресами IPv4, но предназначенная для потокового вещания. Дальнейшее ее развитие (такое же «успешное» ST — Stream protocol).

IPX – не IP версии 10, как можно было бы подумать, и не принадлежит к семейству IP. Разработанный компанией Novell протокол расшифровывается как Internetwork Pocket eXchange. Работал он так же, как и IPv4, поверх Ethernet.

Адрес IPX состоял фактически из трех частей и представлял собой 12 октетов.

Первые 4 октета обозначали адрес сети. Использовался диапазон от 00:00:00:01 до FF:FF:FF:FE. Специальные адреса 00.00.00.00 и FF.FF.FF.FF использовались для специальных целей.

00:00:00:00 – текущая сеть.

FF:FF:FF:FF – широковещательная рассылка.

Следующие 6 октетов – обозначали адрес хоста.

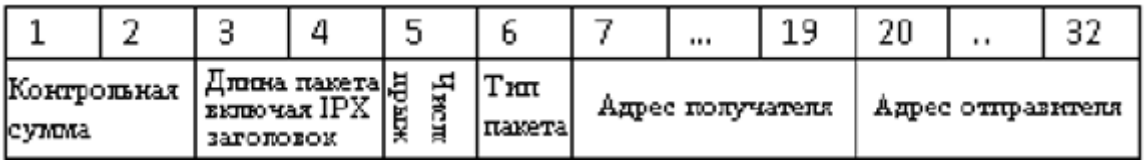
Обратите внимание, что в качестве них использовался MAC-адрес сетевого устройства.

Это тот самый случай, когда упоминалось, что MAC-адреса, в принципе, могут использоваться на сетевом уровне, хотя не сами по себе и вовсе не обязательно.

Осталось еще 2 октета. А вот они использовались для идентификации сокета (отправителя или получателя).

Фактически пакет IPX (или дейтаграмма) являлся неким аналогом дейтаграммы UDP (заголовок которой, собственно говоря, и содержит порты получателя и отправителя для идентификации программного обеспечения, работающего с полученными/отправленными сообщениями).

Формат заголовка IPX имел следующий вид.



Решение IPX кажется элегантным, но проиграло битву в конкурентной борьбе IPv4. Тем не менее, наработки IPX оказались задействованы в разработке IPv6 (по аналогии можно было использовать такой вариант: первые 8 октетов – адрес сети, следующие 8 – адрес хоста, также полученный из MAC-адреса. Впрочем, от такой практики было принято отказаться из-за небезопасности такого решения).

Идеи IPv6

Возьмем формат IPv4 адреса. Запишем в 16-ричном виде.

00:00:00:00/MASK

Стандартный 32-битный адрес плюс маска.

Где 00 — четыре октета, распределение между которыми, где адрес сети, где адрес хоста, задается маской.

Берем формат адреса IPX: FF:FF:FF:FF: 00:00:00:00:00:00: CC:CC.

Вместо FF:FF:FF:FF: — адрес сети.

Вместо 00:00:00:00:00:00: — адрес хоста (MAC-адрес).

Вместо CC:CC — номер сокета.

Видим, что всего сетей в IPX столько же, сколько всевозможных адресов сетей, броадкаст-адресов хостов в IPv4 вместе взятых.

Давайте в будущем IP удвоим число октетов, таким образом, чтобы в IPX было сетей столько же, сколько сейчас всего адресов, а для хостов тоже хватило пространство. Получаем следующее.

FF:FF:FF:FF: 00:00:00:00

Где FF:FF:FF:FF — идентифицирует сеть, 00:00:00:00 — хост.

Имем адрес длиной 64 бита.

Давайте подумаем, как избавиться от необходимости в DHCP. Что будет, если добавить в качестве адреса хоста MAC-адрес? Он же глобально уникальный (а если и не глобально уникальный, то с адресом сети все равно адрес будет уникальным). Но MAC — 6 байт. Добавлять в чистом виде не красиво и не симметрично, число 6 не кратно 4. Давайте удвоим число октетов и сгруппируем по два, получив вместо октетов хекстеты.

Получаем.

FFFF:FFFF:FFFF:FFFF: 0000:0000:0000:0000

Всего 128 бит, из них 64 бита на сеть, 64 бита на хост.

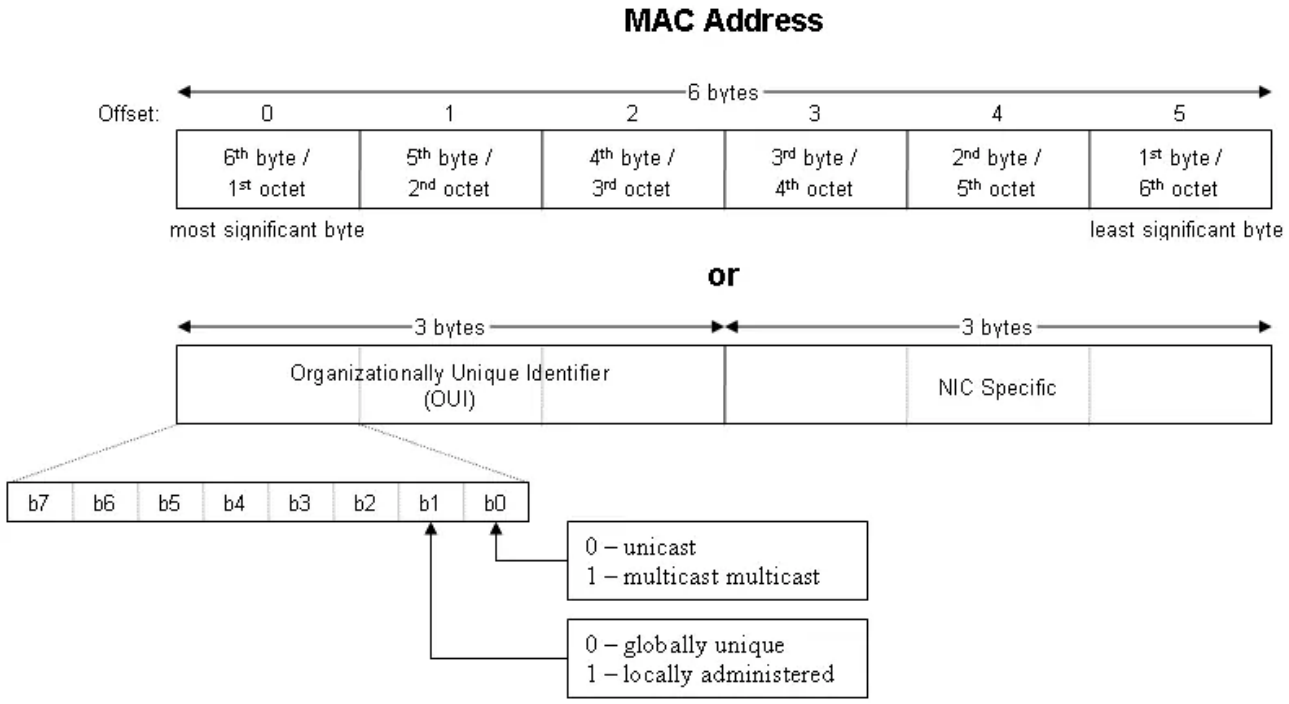
Как теперь поместить 48 битный MAC в 64-битный хост. Было принято решение транслировать 48-битный аппаратный MAC-адрес в 64-битный аппаратный EUI-64 адрес. Делается это так.

Берем исходный MAC-адрес.

Обратите внимание на OUI — уникальный идентификатор организации, NIC Specific — фактически уникальный идентификатор сетевого интерфейса в пространстве адресов OUI на два бита.

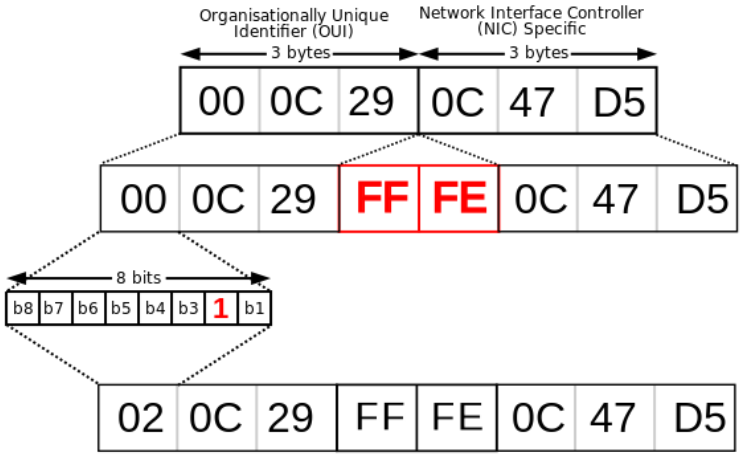
Первые два бита первого байта OUI (в некоторых источниках говорят, что последние, но это то же самое, так как биты передаются в инвертированном порядке).

MAC-48 необходимо привести к формат EUI-64, который тоже имеет префикс производителя в первых трех байтах.



Это достигается следующим алгоритмом.

Добавляется FFFE в середину, разделяющую идентификатор организации и уникальный идентификатор интерфейса для данной организации, а поле, отвечающее за тип адреса (глобально уникальный или локально администрируемый), устанавливается в единицу.



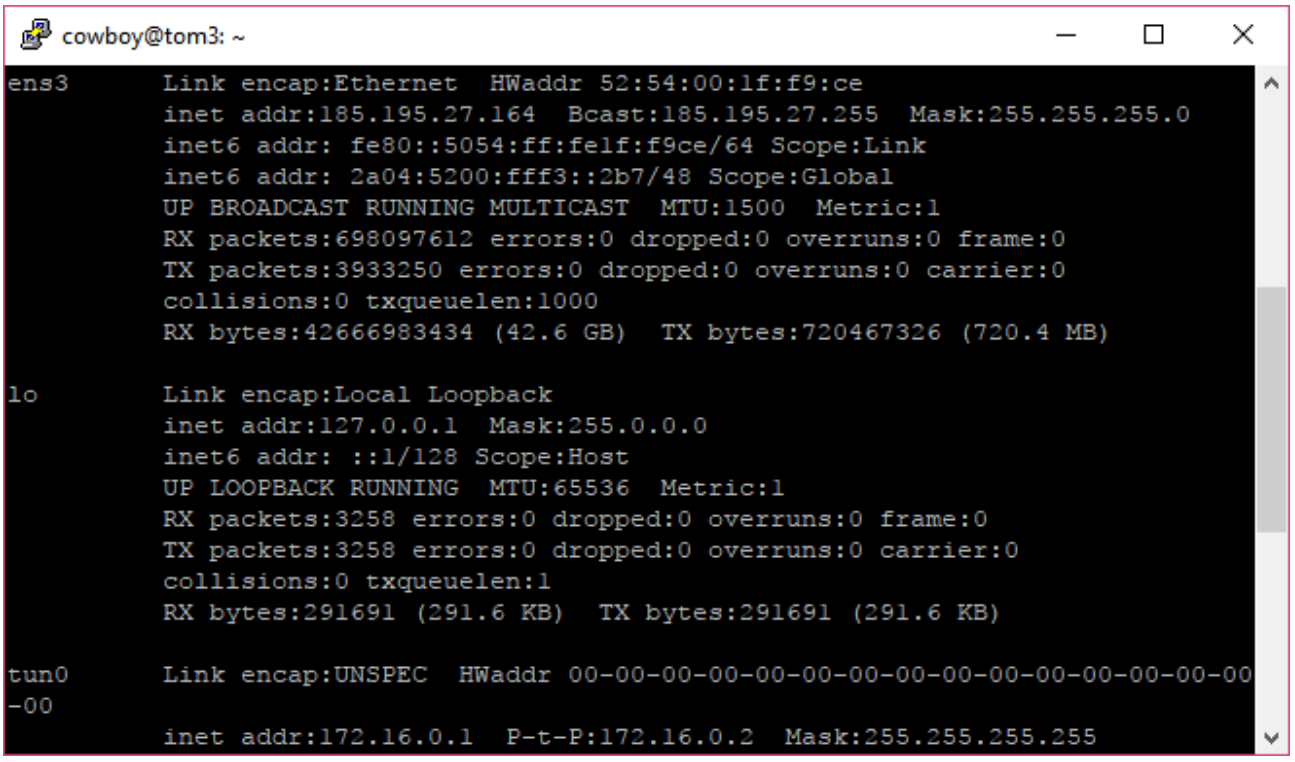
Задача инвертирования бита может быть не совсем понятна. По одной из версий она служит для того, чтобы локально-установленные адреса, состоящие из первых октетов 0000, но содержащие бит признака “локально администрируемый”, будут иметь вид 02:00:00:00:11:22, а IPv6-адрес: fe80::0200:00ff:fe00:1122 (группу нулей один раз можно сократить). Инвертирование бита для локально администрируемых адресов позволит упростить их до вида 00:00:00:00:11:22, а IPv6 до fe80::ff:fe00:1122.

Подробнее https://habrahabr.ru/post/245323/.

Достоинство такого подхода получения IPv6-адресов в том, что каждый хост сразу может начинать работу в сети. Но такие адрес по сети распространять было бы небезопасно. Во-первых, сторонние лица могут узнать о перемещении вашего устройства и вас, во-вторых, по MAC-адресу можно вычислить производителя устройства и определить возможные уязвимости. Такие адреса используются только как локальные и не маршрутизируются (это аналог link-local 169.254.0.0/16 адресов, но получаемых из MAC-адреса). С помощью ICMPv6 объявлений маршрутизатора вы уже можете получить белые IPv6-адреса.

А вот идею по передаче номера порта в сетевом адресе из IPX в IPv6 добавлять не стали. Причиной тому стала традиция использовать двух разных диапазонов портов и двух разных протоколов UDP и TCP.

Посмотрите на адреса в выдаче ifconfig.



Мы видим MAC-адрес, полученный из него link local адрес fe80, и видим белый IPv6 адрес, полученный от маршрутизатора. Обратите внимание на маски сетей /64 и /48 — это стандартные маски для IPv6 адресов, позволяющие выделять большие диапазоны так, что их хватит на все утюги, кофемолки и IP-ТВ в вашем доме.

IPv6

IPv6 — развитие протокола IPv4, который решает перечисленные проблемы путем увеличения длины адреса с 32 до 128 бит. В настоящее время протокол IPv6 широко используется внутри дата-центров, такими гигантами, как Google, Facebook, Yandex. Постепенно происходит внедрение 6 версии в сети провайдеров по всему миру, но пока протокол не получил широкое распространения в Интернете, как IPv4. Это связано с проблемами поддержки протокола оборудованием и сложностью администрирования. Протокол был разработан IETF и сейчас поддерживается всем новым телекоммуникационным оборудованием.

Особенности адресации IPv6

128-битный в шестнадцатеричном формате (0-9, A-F).

Используются 16-битные шестнадцатеричные числа, разделенные двоеточиями (:).

Каждая четверка шестнадцатеричных цифр эквивалентна 16 битам (двум байтам).

Состоит из восьми четверок, каждая из которых эквивалентна 16 битам.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64.

2001 в шестнадцатеричном виде это 0010 0000 0000 0001 в двоичном.

Структура адресов IPv6.

Префикс сайта или Префикс глобальной маршрутизации - это первые три четверки (или 48 бит) адреса. Он назначается Интернет-провайдером.

ID подсети - это 4-ая четверка адреса.

ID интерфейс - это последние 4 четверки (64 бита) адреса. Он может вручную или динамически назначаться с помощью механизма EUI-64 (Extended Unique Identifier).

Первые 3 бита фиксированы: 001(двоич), что дает 200::/12 (IANA Global Routing Number).

Биты 16-24 идентифицируют регионального регистратора.

2001:0000::/23 – IANA.

2001:0200::/23 – APNIC (Азиатско-Тихоокеанский регион).

2001:0400::/23 – ARIN (Североамериканский регион).

2001:0600::/23 – RIPE (Европа, Ближний Восток, Россия и СНГ).

Оставшиеся 8 бит до /32 идентифицируют ISP.

3-я четверка представляет идентификатор сайта/компании.

4-я четверка представляет идентификатор подсети.

- Позволяет адресовать 65,536 подсетей с 18,446,744,073,709,551,616 (18 квинтиллионов) адресов в каждой подсети.

- Не является частью хостового поля адреса.

Идентификатор интерфейса - это оставшиеся 64 бита адреса.

Может быть сконфигурирован вручную или динамически с использованием EUI-64 (Extended Unique Identifier).

Механизм EUI-64 использует 48-битный MAC адрес устройства и конвертирует его в 64-битный путем вставки значения FF:FE в середину адреса.

Первый (сетевой) и последний (широковещательный) адреса могут быть назначены интерфейсам. Интерфейсу можно назначить более одного IPv6 адреса.

Нет широковещательных адресов, вместо этого используется мультикастинг.

IPv6 использует тот же метод разделения на подсети, что и IPv4.

/127 дает 2 адреса.

/124 дает 16 адресов.

/120 дает 256 адресов.

Первый адрес в подсети полностью состоит из 0, последний – полностью из F.

Для простоты и единства структуры рекомендуется везде использовать /64. Использование чего-либо меньшего, чем /64, может потенциально привести к сбою некоторых функций IPv6 и неоправданному усложнению структуры адресации.

Нули в старших разрядах любой 16-битной секции могут быть опущены.

Адрес до упрощения: 2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64.

Адрес после упрощения: 2001:DB8:1:5270:127:AB:CAFE:E1F /64.

Это правило применимо только к нулям в старших разрядах. Если опустить нули в младших разрядах, адрес будет неверен.

Link-Local адреса предназначены для использования только в локальном канале.

Адреса Link-Local автоматически конфигурируются на всех интерфейсах.

Префикс, используемый Link-Local адресами – FE80::X/10.

Маршрутизаторы не перенаправляют пакеты с Link-local адресом источника или назначения.

Адрес Loopback - функция схожа с IPv4 адресом 127.0.0.1.

Адрес Loopback 0:0:0:0:0:0:0:1 может быть сокращен до ::1.

Используется устройством для посылки пакета себе самому.

Сравнение IPv4 и IPv6

Ниже приведены ключевые отличия версий протоколов.

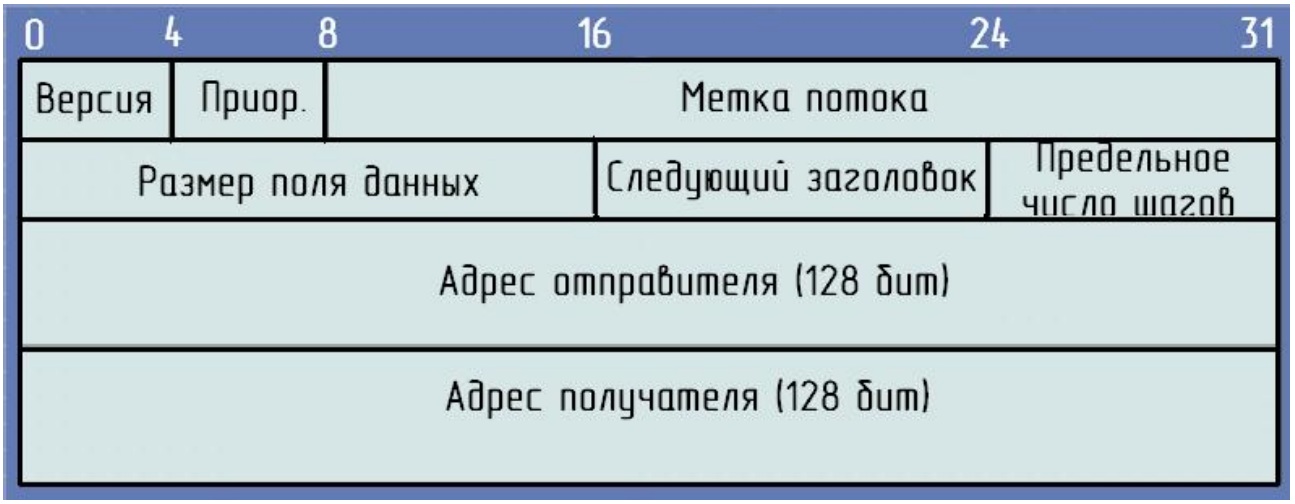
IPv6

- 128-битный адрес состоит из префикса глобальной маршрутизации, ID подсети и ID интерфейса.
- Используется 16-ричный формат 0-9, A-F.
- Минимальный размер максимального пакета 1280 байт.
- Сетевой и широковещательный адреса могут быть назначены интерфейсам конечных устройств.
- Встроенное шифрование IPsec.

IPv4

- 32-битный адрес, состоящий из сетевой и хостовой части.
- Используется десятичная запись через точку.
- Минимальный размер максимального пакета 576 байт.
- Сетевой и широковещательный адреса нельзя назначать интерфейсам конечных устройств.
- Для шифрования IPv4 пакетов нужно применять технологии VPN.

Формат IPv6 пакета



Описание полей.

- Версия: версия протокола; для IPv6 - это значение равно 6 (значение в битах — 0110).
- Класс трафика (приоритет): приоритет пакета (8 бит).
- Метка потока служит для упрощения маршрутизации однородных потоков пакетов.
- Размер поля данных (16 бит) — размер поля данных в октетах, не включает данный заголовок, но включает все расширенные заголовки.
- Следующий заголовок: задаёт тип расширенного заголовка, который идёт следующим. В последнем расширенном заголовке поле Next Header задаёт тип транспортного протокола (TCP, UDP, SCTP, DCCP, ICMPv6).
- Число прыжков (8 бит). Аналог TTL, но теперь называется в соответствии с назначением.
- Source Address и Destination Address: адрес отправителя и получателя соответственно; по 128 бит.

В IPv6 отсутствует контрольная сумма, не используемая уже в IPv4, так как считается на транспортном уровне. В расширенных заголовках может содержаться информация о требуемом

маршруте, о фрагментации, о том, что передается джамбограмма (пакет с большим MTU), заголовки IPX AH и ESP.

Популярность IPv6 адресов

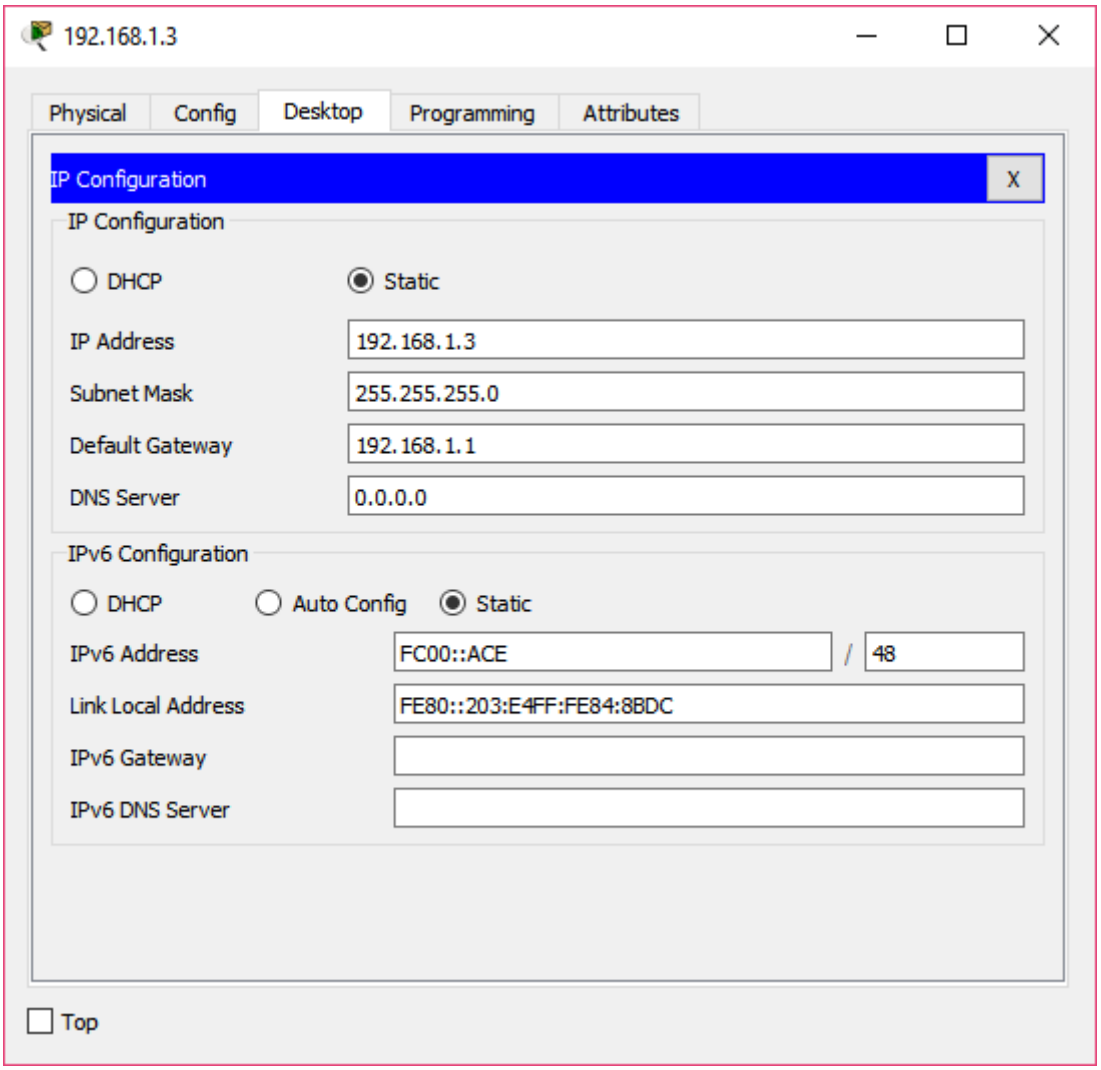
Есть мнение, что IPv6-адреса никогда не станут популярными. Этому способствует позиция провайдеров, которые освоили технологию перегруженного NAT и не спешат внедрять IPv6-адреса (и так же работает!) Но в дата-центрах уже давно используются IPv6-адреса, и, купив VDS, вы можете увидеть (например, отследив через tcpdump), что при обновлениях пакетов в Ubuntu вы работаете в IPv6 по умолчанию. Существенным недостатком является то, что большинство VDS-хостеров нарушают рекомендации, выдавая на хост всего лишь один IPv6-адрес вместо выделения 48 или 64 сети. Но если забанят вашего соседа, забанят всю сеть. В IPv6 банятся именно /64 сети.

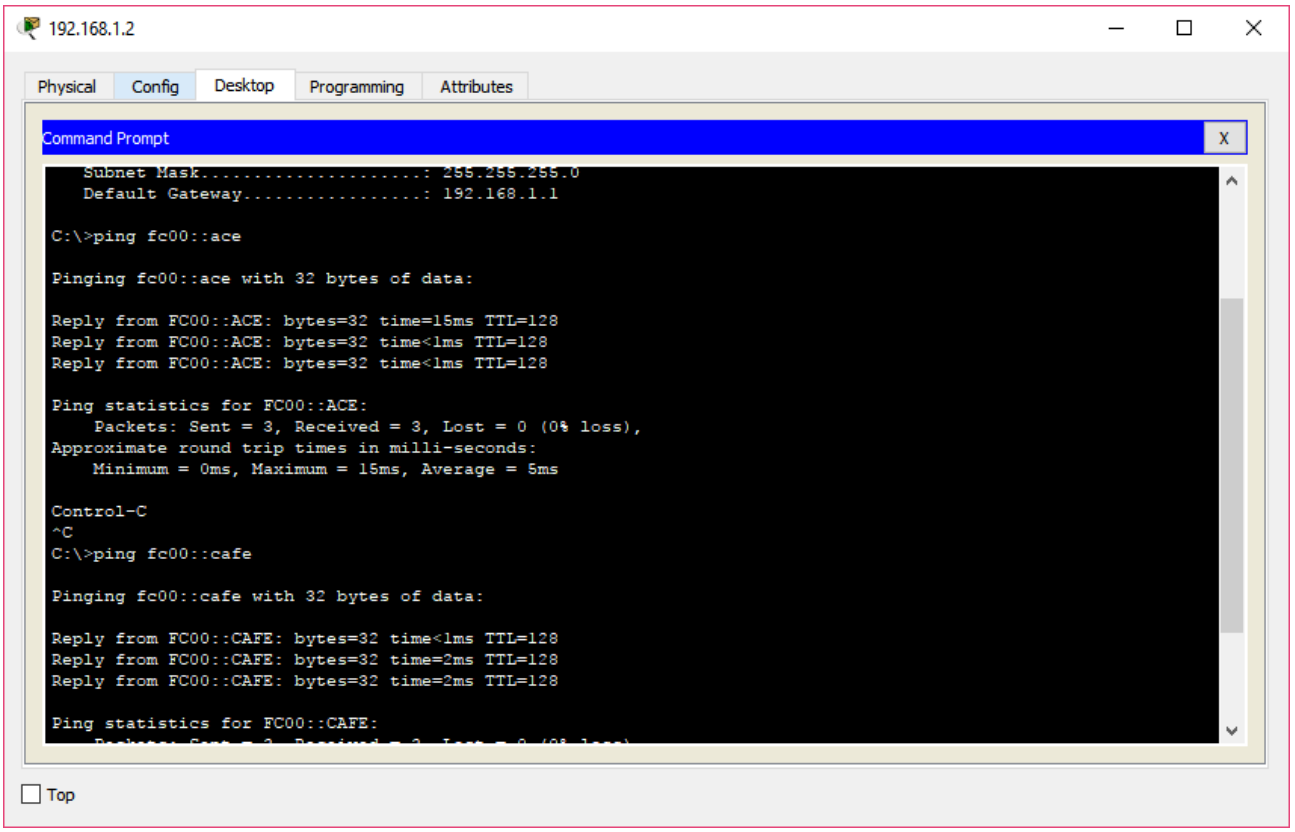
Если у вас нет возможности получить белый IPv6-адрес от провайдера, вы все равно можете испытать IPv6, если хотя бы имеется возможность получить белый IPv4-адрес благодаря туннелированию 6to4. 6to4 дает возможность получить из белого IPv4-адреса целую сеть /48 IPv6 адресов. Единственный недостатокв том, что из-за туннелированию и ненадежности работы множества туннельных 6to4-адресов такой способ работы будет хуже, чем по IPv4.

Один из аргументов, что IPv6 адреса не найдут применение, - они слишком сложные.

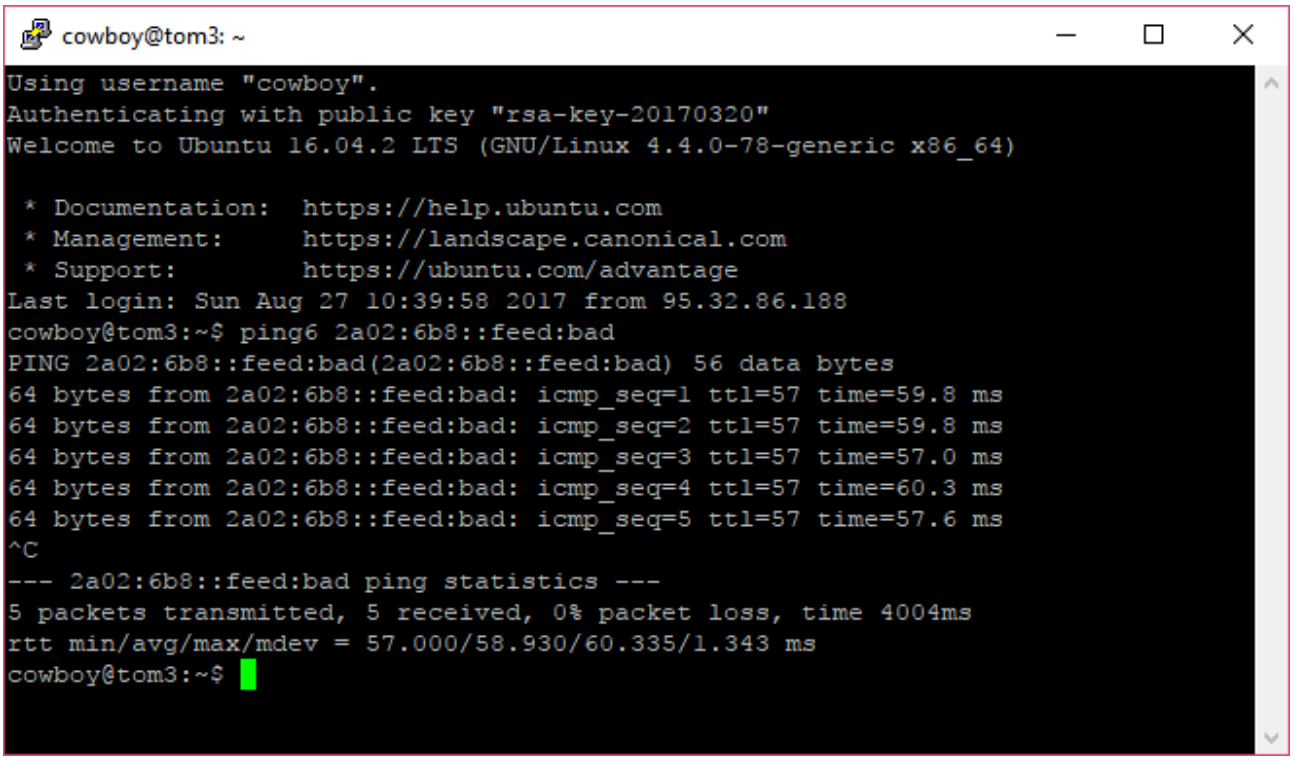
На это есть ряд контраргументов.

1. Для многих не только IPv4-адреса сложные, но даже и доменные имена. Поэтому поисковые машины даже доменные имена стремятся скрыть от пользователей, заменяя адресную строку поисковой. Многие не знают, что такое odnoklassniki.ru, они знают, что такое одноклассники. Все равно поисковая система найдет домен и подставит.
2. В IPv6 в основном используются домены. Записи вида AAAA в DNS позволяют устанавливать соответствие доменное имя — IPv6-адрес.
3. IPv6-адреса сокращаются. Хекстет можно сократить, убрав начальные нули. Группу нулевых хекстетов (но только одну можно убрать). Потому, например, аналог 127.0.0.1 в IPv6 даже короче, он выглядет как ::1.
4. Из символов a-f и цифр, похожих на буквы (0 как o, 1 как l), можно собирать аббревиатуры и короткие слова: a11 (all), beef, face, cafe, babe, c00l (cool) и т.д.
5. Последние два хекстета можно записать в формате традиционного IP-адреса. То есть если у вас были на машинах адреса вида 10.0.0.1, при получении префикса IPv6 вы можете добавить этот адрес в качестве хоста. Если используем локальный адрес (в отличие от link local, назначаемый, т.е. аналог 10.0.0.0/8 и т.д.) сетей, например, fc00::10.0.0.2, fc00::10.0.0.3, а новые хосты могут сразу получить имена fc00::ace, fc00::cafe.


192.168.1.3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
FC00::ACE
/
48
Link Local Address
FE80::203:E4FF:FE84:8BDC
IPv6 Gateway
IPv6 DNS Server
Top



В Linux для работы с IPv6 нужно использовать соответствующие утилиты ping6, traceroute6.

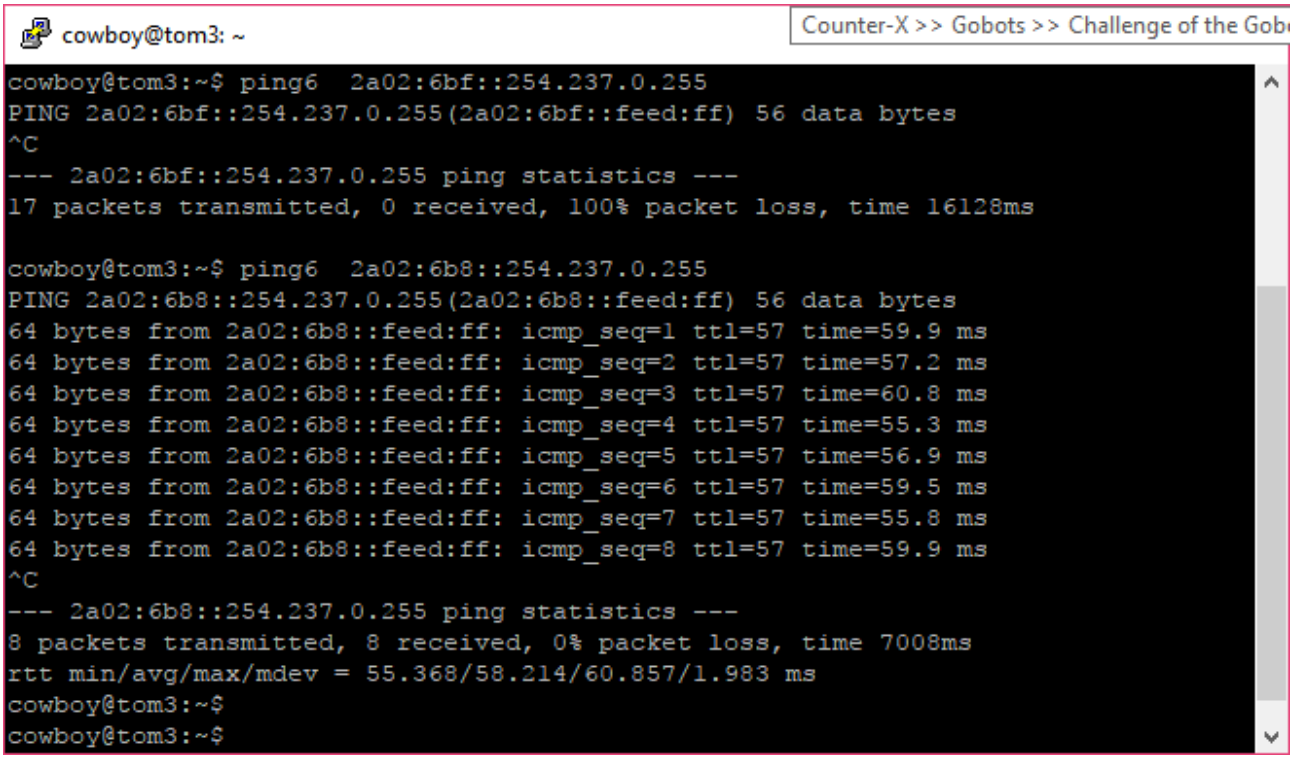


Видим, как Яндекс придумал IP-адреса для своих публичных DNS.

Вид режима	Primary IPv4 DNS	Secondary IPv4 DNS	Primary IPv6 DNS	Secondary IPv6 DNS
Базовый	77.88.8.8	77.88.8.1	2a02:6b8::feed:0ff	2a02:6b8:0:1::feed:0ff
Безопасный	77.88.8.88	77.88.8.2	2a02:6b8::feed:bad	2a02:6b8:0:1::feed:bad
Семейный	77.88.8.7	77.88.8.3	2a02:6b8::feed:a11	2a02:6b8:0:1::feed:a11

По материалам https://ru.wikipedia.org/wiki/Яндекс.DNS

Можно для примера при обращении 2a02:6b8::feed:0ff представить последние два хекстета в виде, совместимом с IPv4-записью. Получим 2a02:6bf::254.237.0.255.



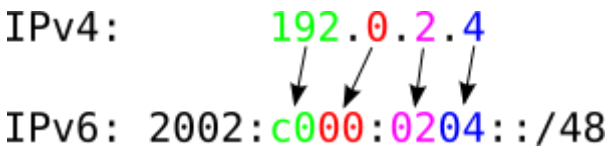
Обратите внимание, 0ff в шестнадцатеричной записи используется только для удобства (off), в записи IPv6 начальный 0 отбрасывается (а на самом деле там два нуля, так как по факту хекстет имеет вид 00ff).

На данный момент все корневые сервера поддерживают AAAA ресурсные записи (для IPv6). Почтовые службы, Yandex и Google, обмениваются IPv6 трафиком. IPv6 — безальтернативное будущее для компьютерных сетей.

6to4

Если нет IPv6 адреса, но есть белый IPv4, можно получить тоннельные IPv6-адреса, причем целую сеть /48.

Первый хекстет для адресов 6to4 имеет значение 2002, следующие два преобразуются из IPv4 адреса по схеме.



Дальше нужно использовать механизм туннелирования 6to4, IPv6 пакету будут отправляться в туннельный интерфейс tun6to4, который будет инкапсулировать IPv6 пакеты в IPv4 и отправлять на адрес туннельного шлюза 6to4 192.88.99.1. Это anycast адрес, и многие компании используют свои 6to4 шлюзы для того, чтобы ближайшие узлы могли использовать услугу IPv6.

Подключить IPv6 механизм 6to4 можно в Linux с помощью утилиты iproute2.

Предположим, наш IPv4 адрес 185.195.27.164. Адрес 6to4 сети для нас 2002:B9C3:1BA4::/48. Мы можем выбрать любой адрес в этой сети для нашего интерфейса. Пусть это будет 2002:B9C3:1BA4::FACE/128.

Шлюз 192.88.99.1 внутри IPv6 сети для нас будет выглядеть как ::192.88.99.1 (механизм трансляциии IPv4 адресов в IPv6 адресов). На него мы укажем маршрут. Внутри тоннеля это будет один хоп, снаружи — нет.

```
ip tunnel add tun6to4 mode sit remote any local 185.195.27.164 ttl 64
ip link set dev tun6to4 up
ip -6 addr add 2002:B9C3:1BA4::FACE/128 dev tun6to4
ip -6 route add 2000::/3 via ::192.88.99.1 dev tun6to4 metric 1
```

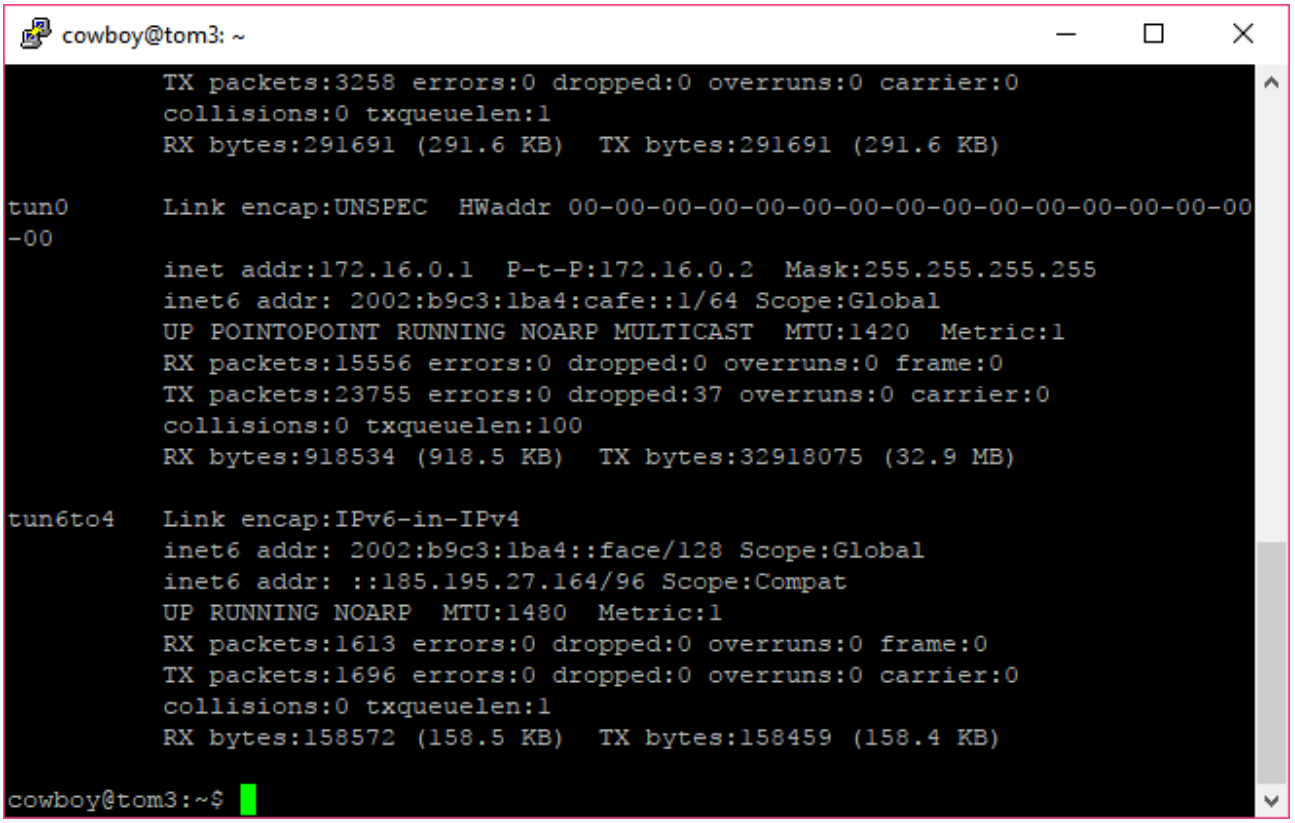
Мы укажем маршрут для сети 2000:/3 через шлюз. Это вариант совместимости, другой вариант ::/0
После этого у нас есть IPv6, причем не один адрес, а целая сеть. Но через тоннель.
Если у нас есть OpenVPN, мы можем пробросить сеть и внутрь клиентских подключений с VDS.
Для OpenVPN. Для клиента ничего изменять не надо.

Для сервера OpenVPN добавим в /etc/openvpn/server.conf строки.

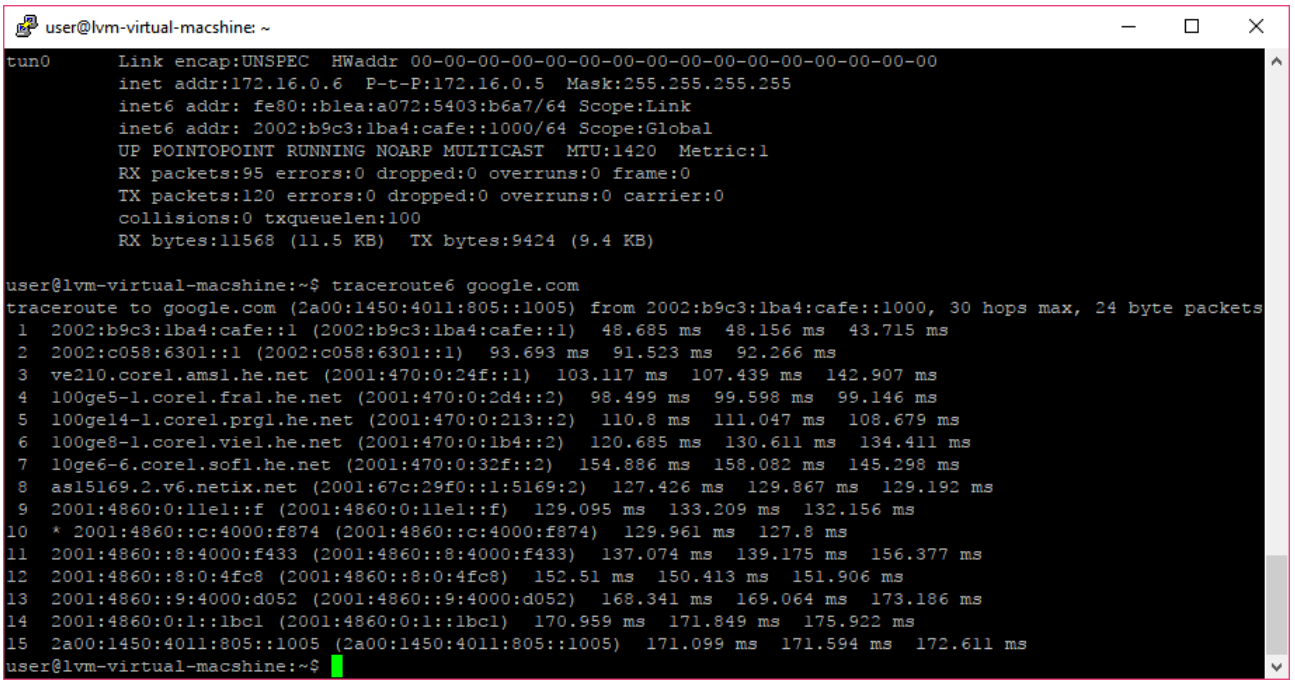
```
server-ipv6 2002:B9C3:1BA4:CAFE::/64
tun-ipv6
push tun-ipv6
push "route-ipv6 2000::/3"
push "dhcp-options DNS 2001:4860:4860::8888"
```

Выделим подсеть 2002:B9C3:1BA4:CAFE::/64 для туннельных подключений. Отправим (push)

настройки IPv6 маршрутизации и адрес DNS-сервера для IPv6 каждому подключаемому клиенту.



Два тоннеля. Один OpenVPN (безопасный), второй 6to4 (только шифрование).



Более того, наша виртуальная машина, с которой выполнено подключение, пингуется с других машин VDS по IPv6.

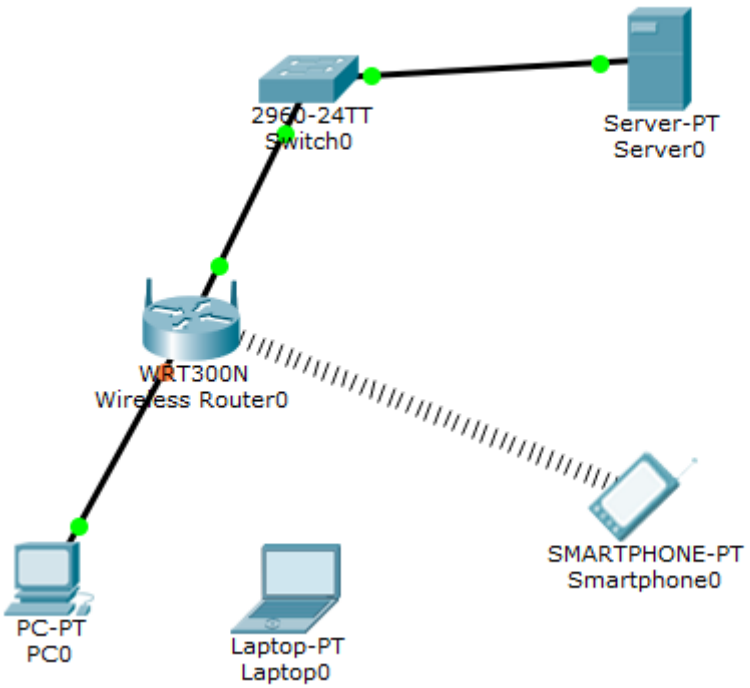
```
root@tom0:~
[root@tom0 ~]# ping6  2002:b9c3:1ba4:cafe::1000
PING 2002:b9c3:1ba4:cafe::1000(2002:b9c3:1ba4:cafe::1000) 56 data bytes
64 bytes from 2002:b9c3:1ba4:cafe::1000: icmp_seq=1 ttl=53 time=116 ms
64 bytes from 2002:b9c3:1ba4:cafe::1000: icmp_seq=2 ttl=53 time=114 ms
64 bytes from 2002:b9c3:1ba4:cafe::1000: icmp_seq=3 ttl=53 time=116 ms
64 bytes from 2002:b9c3:1ba4:cafe::1000: icmp_seq=4 ttl=53 time=114 ms
64 bytes from 2002:b9c3:1ba4:cafe::1000: icmp_seq=5 ttl=53 time=120 ms
^C
--- 2002:b9c3:1ba4:cafe::1000 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 114.601/116.408/120.629/2.232 ms
[root@tom0 ~]#
```

Практическое задание

1. Домашняя работа на закрепление принципов работы с беспроводной точкой доступа.

Разворачиваем сеть Wi-Fi.

Откройте файл с заданием.



Проверьте доступность сайта geekbrains.ru через смартфон.

Подключитесь к маршрутизатору используя пк, через веб-интерфейс.

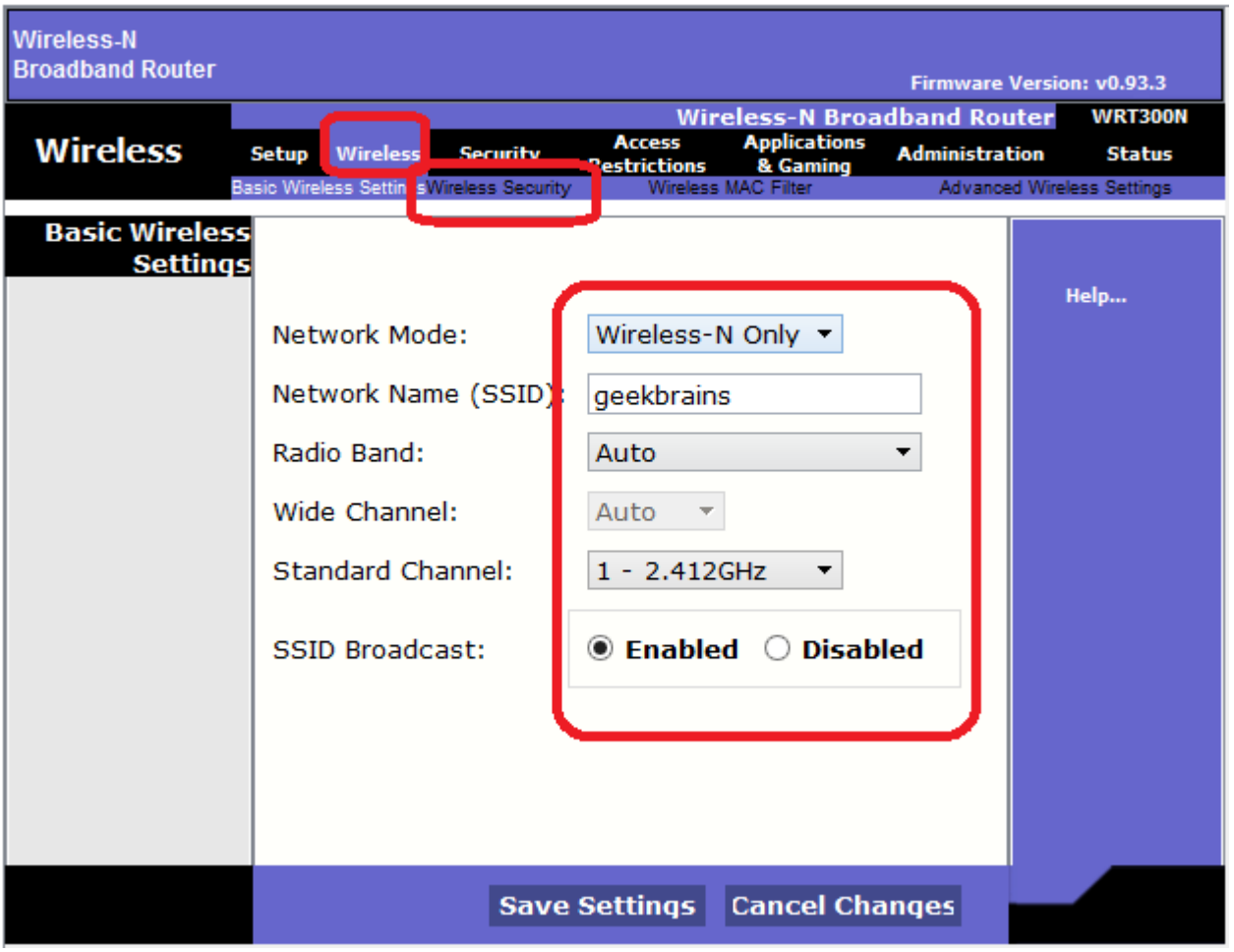
Настройте безопасную беспроводную сеть.

Для этого установите шифрование сети и смените стандартное название сети.

ssid – geekbrains.

тип шифрования:WPA2.

пароль: Geekbrain$.

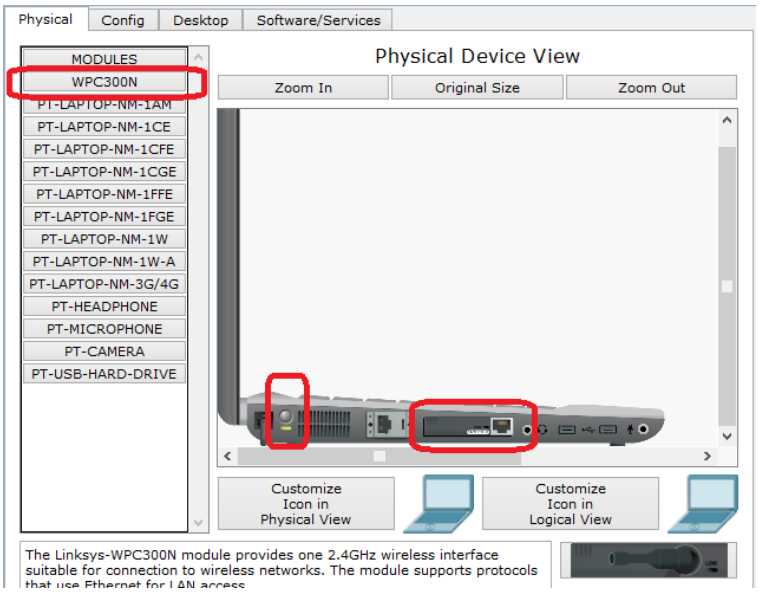


Проверьте работоспособность сайта через смартфон.

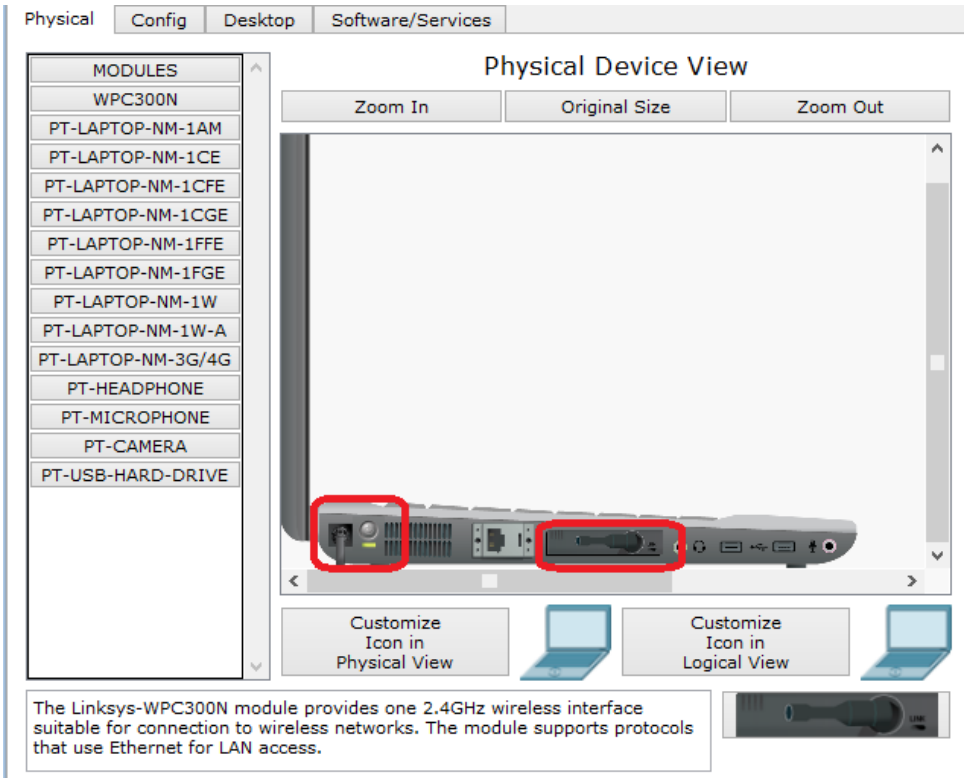
Восстановите работу беспроводной сети на телефоне, применив корректные настройки.

Проверьте доступность сервера с ноутбука.

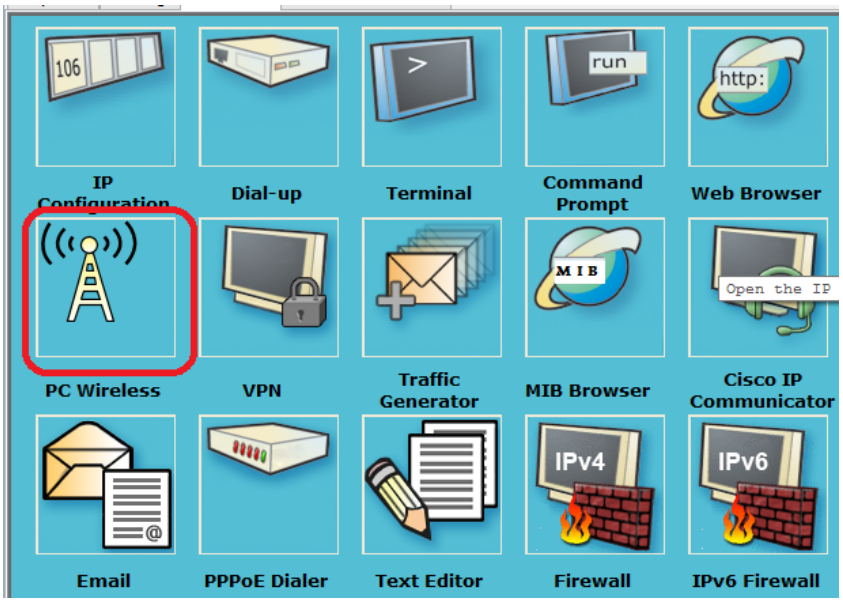
Произведите замену сетевой карты ноутбука. Для этого отключите устройство, замените плату.



После замены платы повторно включите устройство.



Перейдите в раздел сетевых настроек и произведите конфигурацию беспроводной сети согласно заданным параметрам.



Для этого перейдите в раздел профиль и создайте новое сетевое подключение с необходимым именем сети, паролем и типом шифрования. После установления соединения с точкой доступа вы увидите во вкладке Link Information сообщение об успешном установление связи.

После подключения настройте сетевой адрес устройство на работу в автоматическом режиме (DHCP).

После получения адреса проверьте связь с сервером и убедитесь в работоспособности сайта.

Дополнительные материалы

1. http://xgu.ru/wiki/VLAN
2. http://xgu.ru/wiki/Native_VLAN
3. http://xgu.ru/wiki/Безопасность_канального_уровня
4. http://www.thg.ru/network/20030311/wireless_ntk1-03.html

5. Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с. (Главы 4,5)
6. https://ru.wikipedia.org/wiki/CSMA/CA
7. https://ru.wikipedia.org/wiki/Проблема_скрытого_узла
8. https://ru.wikipedia.org/wiki/Проблема_незащищённого_узла
9. http://book.itep.ru/4/41/zigbee.htm
10. Терновой М. Ю. «Мобильные сети: IP маршрутизация и алгоритмы MANET маршрутизации» [Электронный ресурс]. – Режим доступа: URL: http://www.its.kpi.ua/itm/ternovoy; http://www.its.kpi.ua/itm/ternovoy/discipline/Інформаційне%20забезпечення%20мобільних%20систем%20ТК/Лекція %204.pdf
11. https://ru.wikipedia.org/wiki/Ячеистая_топология
12. https://ru.wikipedia.org/wiki/Беспроводная_ad-hoc-сеть
13. https://ru.wikipedia.org/wiki/Интернет_вещей
14. https://ru.wikipedia.org/wiki/Беспроводная_сенсорная_сеть

Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы.

1. https://ru.wikipedia.org/wiki/Яндекс.DNS
2. https://habrahabr.ru/post/245323/
3. https://ru.wikipedia.org/wiki/Уникальный_идентификатор_организации#EUI-64
4. http://it.mmcs.sfedu.ru/wiki/Сетевой_уровень
5. https://ru.wikipedia.org/wiki/IPv6
6. https://ru.wikipedia.org/wiki/Пакет_IPv6
7. ru.wikipedia.org/wiki/6to4
8. http://catamobile.org.ua/format-frejma-802-11.html
9. http://podokaro.blogspot.ru/2011/10/ieee-80211-jaringan-area-lokal-nirkabel.html
10. https://ru.wikipedia.org/wiki/AODV
11. https://ru.wikipedia.org/wiki/OLSR
12. https://ru.wikipedia.org/wiki/6LoWPAN