МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра *Радиоприемные и радиопередающие устройства*
(полное название кафедры)

Утверждаю

Зав. кафедрой РП и РПУ

Киселев А.В.
(подпись, инициалы, фамилия)

«___» _____ 2017 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

Сысоев Олег Владимирович
(фамилия, имя, отчество студента – автора работы)

Исследование принципа работы блокирования клиентов по mac адресу на Wi-Fi точке доступа
(тема работы)

Факультет радиотехники и электроники
(полное название факультета)

Направление подготовки *11.03.02 – Инфокоммуникационные технологии и системы связи*
(код и наименование направления подготовки бакалавра)

Руководитель от НГТУ

Степанов М.А.
(фамилия, имя, отчество)

к.т.н.
(ученая степень, ученое звание)

_____
(подпись, дата)

Автор выпускной квалификационной работы

Сысоев О.В.
(фамилия, имя, отчество)

РЭФ, РТВ14-31
(факультет, группа)

_____
(подпись, дата)

Новосибирск 2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра *Радиоприемные и радиопередающие устройства*
(полное название кафедры)

УТВЕРЖДАЮ

Зав. кафедрой РП и РПУ
Киселев А.В.
(фамилия, имя, отчество)

_____
(подпись, дата)

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ БАКАЛАВРА

студенту *Сысоев Олег Владимирович*
(фамилия, имя, отчество)

Направление подготовки *11.03.02 – Инфокоммуникационные технологии и системы связи*
(код и наименование направления подготовки бакалавра)

Факультет радиотехники и электроники
(полное название факультета)

Тема *Исследование принципа работы блокирования клиентов по mac адресу на Wi-Fi точке доступа*
(полное название темы выпускной квалификационной работы бакалавра)

Исходные данные (или цель работы) *Исследовать алгоритм работы блокирования клиентов по mac-адресу и модернизировать его для использования различных списков доступа и политик безопасности на виртуальных точках доступа*

Структурные части работы *1) Оглавление*
2) Введение
3) Исследование и доработка алгоритма фильтрации клиентов
4) Заключение
5) Экономический раздел
6) Раздел охраны труда
7) Список используемых источников

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Задание согласовано и принято к исполнению.

Руководитель от НГТУ	**Студент**
Степанов М.А.	*Сысоев О.В.*
(фамилия, имя, отчество)	(фамилия, имя, отчество)
к.т.н.	*РЭФ, РТВ14-31*
(ученая степень, ученое звание)	(факультет, группа)
_____	_____
(подпись, дата)	(подпись, дата)

Тема утверждена приказом по НГТУ № _____ от «____» _____ 2017 г.

ВКР сдана в ГЭК № _____, тема сверена с данными приказа

_____
(подпись секретаря государственной экзаменационной комиссии по защите ВКР, дата)

_____
(фамилия, имя, отчество секретаря государственной
экзаменационной комиссии по защите ВКР)

Аннотация

В данной работе была рассмотрена модель OSI и стек протоколов TCP/IP. Также была рассмотрена внутренняя структура Ethernet фреймов, IP пакетов и TCP сегментов. Был исследован исходный алгоритм фильтрации пакетов на Wi-Fi точке доступа и по условиям технического задания изменен на новый. Были внесены изменения в WEB интерфейс управления.

Ключевые слова: модель OSI, TCP/IP, физический уровень, канальный уровень, сетевой уровень, транспортный уровень, сеансовый уровень, уровень представления, прикладной уровень, Wi-Fi точка доступа.

Abstract

In the current work, we reviewed the OSI model and TCP/IP stack. We reviewed the internal structure Ethernet frames, IP packets and TCP segments. Investigated original algorithm of packet filtering on Wi-Fi access point. By specification, the original algorithm was changed. Changes were made to the web interface.

Key words: model OSI, TCP/IP stack, physical layer, data link layer, network layer, transport layer, session layer, presentation layer, application layer, Wi-Fi access point.

Оглавление:

Введение

Тема моей работы: «Исследование принципа работы блокирования клиентов по MAC адресу на Wi-Fi точке доступа» для того чтобы понять для чего это вообще нужно следует рассмотреть историю развития Wi-Fi точек доступа, а для того чтобы разобраться почему блокировка идет по MAC, для этого нужно рассмотреть устройство сетевого протокола обмена информацией.

Развитие беспроводных технологий началось в конце 19 века. В 20-е годы 20 века были созданы приемники, основанные на принципе амплитудной модуляции, в 30-е годы была уже освоена частотная модуляция радио и появление телевидения, в 70-е создана система беспроводной передачи голоса в виде аналогового сигнала, а в 80-е уже был разработан стандарт GSM, который положил начало переходу к цифровым стандартам[1].

Начало развития стандартов беспроводных сетей было положено в 1990 году, в этом году организация под названием IEEE (Институт инженеров по электричеству и электронике) образовала комитет 802.11. Невозможно преувеличить значение World Wide Web в развитии беспроводных технологий. Изначально беспроводные технологии пользовались низким спросом в основном из-за своей дороговизны. Но со временем цены падали, а интерес и количество пользователей росли и к середине первого десятилетия 21 века счет клиентов беспроводного интернета исчислялся в десятках миллионов. Так же влияние на развитие беспроводных сетей оказало использование интернета пользователями дома. С увеличением числа устройств в доме встает проблема большого количества проводов, что наталкивает на переход к беспроводной связи.

Что такое Wi-Fi? Wi-Fi это вид беспроводной связи позволяющий подключать в одну локальную сеть множество устройств и подключать их к интернету. Сама же аббревиатура Wi-Fi расшифровывается как Wireless Fidelity, при дословном переводе означает "высокая точность беспроводной передачи данных".

Чтобы понять почему фильтрация идет именно по mac адресу, для этого нам нужно рассмотреть сетевую модель OSI, описывающую стек сетевых протоколов.

В конце 70 существовало множество протоколов связи, и они были разнообразные, что и привело к проблеме совместимости устройств, работающих на этих протоколах. Чтобы решить эту проблему решили создать общий для всех систем стек протоколов. Протокол разрабатывался семь лет с 1977 по 1984 год. Модель разрабатывалась как универсальный язык сетевых специалистов, по этой причине модель часто называют справочной. Модель OSI, в первую очередь, описывает уровни взаимодействия для систем с коммутацией пакетов, во вторую очередь дает определенные названия для этих уровней, а также определяет назначения всех уровней. Модель OSI это не реализация какого-либо протокола, это теоретическое описание модели, на которую опираются при проектировании собственного протокола, а также при изучении сетевых технологий.

Обзор модели OSI

Модель OSI состоит из семи уровней (снизу вверх): физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной. Каждый уровень отвечает за определенный, описанный в стандарте, функционал.

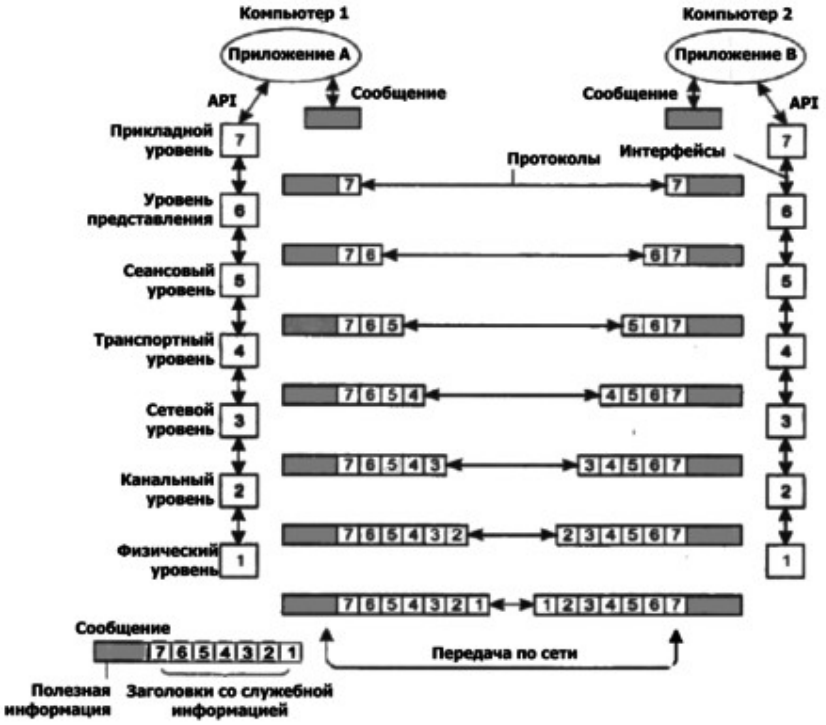

Рис. 1. Модель взаимодействия открытых систем ISO/OSI.

Физический уровень (physical layer).[2] Этот уровень отвечает за передачу потока битов (0 и 1) по физической линии передачи, например Wi-Fi, оптоволокно или витая пара. На физическом уровне заканчивается передача, а также начинается прием, поэтому этот уровень реализован на всех устройствах, находящихся в сети. Физический уровень не ведет никакой обработки информации, его задача заключается в том, чтобы без искажения передать однородный поток битов на передающем устройстве и правильно распознать этот же поток на принимающей стороне.

Канальный уровень (data link layer).[2] Второй уровень обеспечивает прозрачное соединение для сетевого уровня. Чтобы предоставить свои услуги сетевому уровню, канальный уровень должен уметь:

- Устанавливать логическое соединение между приемником и передатчиком
- Согласовывать скорость передачи

Чтобы решать эти задачи, канальный уровень формирует собственные единицы данных – кадры (фреймы). Кадр состоит из заголовка и поля данных. В поле данных, канальный уровень, помещает пакет, а заголовок заполняет своей служебной информацией. Для передачи данных, канальному уровню требуется адрес получателя, на этом уровне им является mac адрес. Мас адрес отправителя и получателя относится к служебной информации. Протокол канального уровня может работать только в плоских сетях. Плоские сети - это когда каждый компьютер от каждого находится в прямом доступе.

Сетевой уровень (network layer).[2] Этот уровень требуется для создания в сети единой транспортного пространства, которое может объединять плоские сети.

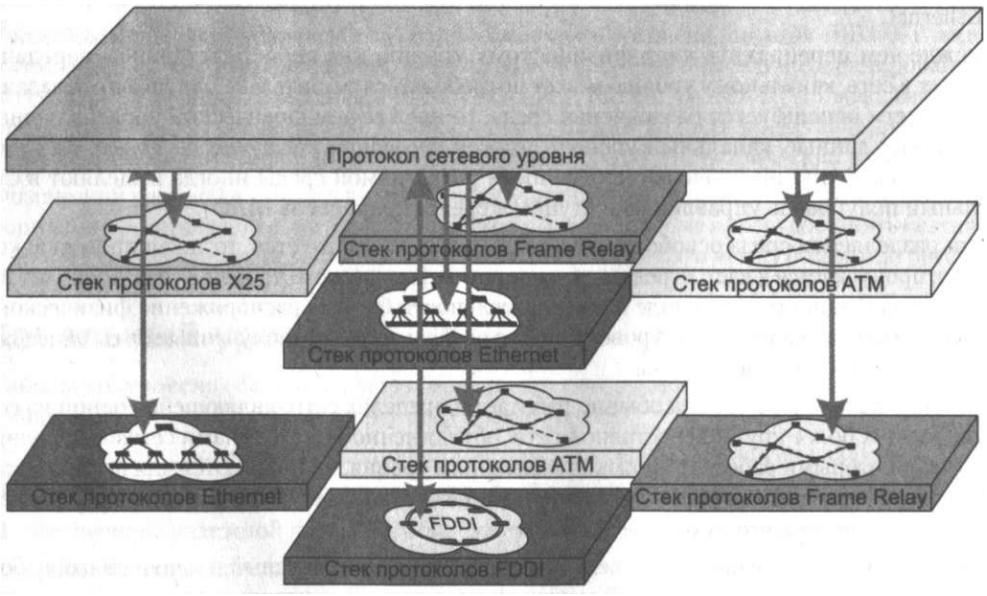

Рис. 2. Взаимодействие различных физических уровней через сетевой.

На рисунке отображено некоторое количество различных сетей, которые могут существовать и позволять им обмениваться информацией, но проблема в том, что эта сеть не сможет взаимодействовать с другой сетью. Для решения этой проблемы используется сетевой уровень, он позволяет связывать пользователей из разных сетей для обмена данными.

Для возможности связи клиентов различных сетей сетевой уровень должен уметь обеспечивать определенный набор функций. Эти функции реализуются:

- Группой протоколов
- Специальными устройствами – маршрутизаторами (роутерами)

Для маршрутизатора стоит задача физического соединения сетей. Маршрутизатор должен иметь как минимум два сетевых интерфейса, для соединения двух плоских сетей в одну общую. В таком случае каждый интерфейс маршрутизатора будет находиться в отдельной сети. Таким образом можно соединять различное количество сетей как показано на рисунке.

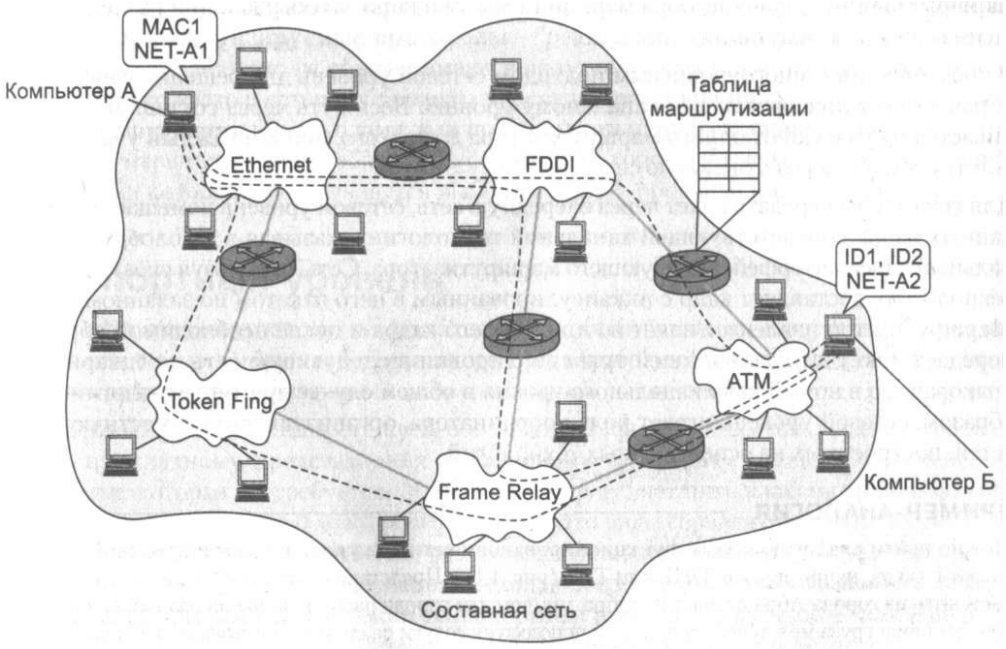

Рис. 3. Пример составной сети.

В сети маршрутизатор работает на сетевом уровне для связи компьютеров, это отлично иллюстрирует следующий рисунок.[3]

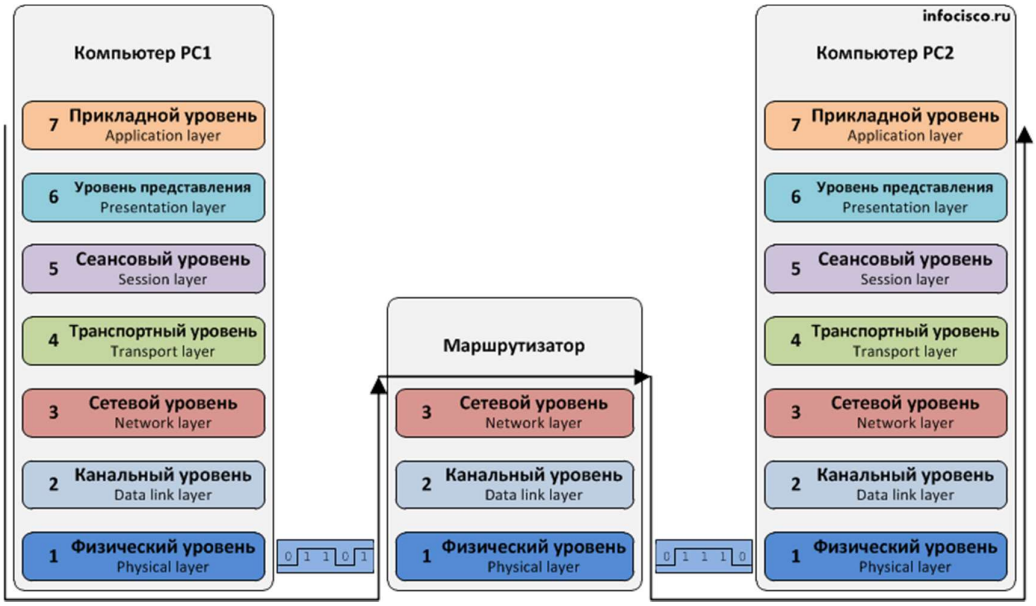

Рис. 4. Отображение уровня взаимодействия маршрутизатора с пакетом от одного устройства другому.

На сетевом уровне идет оперирование такими единицами данных, как пакеты. В пакет входят как данные верхнего уровня, так и заголовки сетевого уровня. Формат пакет имеет стандартизированный вид и не зависит от типа сети в которой он работает, что и позволяет общаться клиентам разных сетей. Так же в состав служебной информации пакета входит IP адрес получателя и отправителя. Для того чтобы маршрутизатор точно знал кому доставлять данные, каждое устройство сети должно обладать уникальным глобальным адресом. На основании указанного адреса получателя уже строится маршрут пакета.

На сетевой уровень ложится важная и сложная задача определения и описания последовательности сетей и маршрутизаторов, через которые должен пройти пакет для доставки его получателю. Весь путь прохождения пакета разделяется на отдельные участки от одного маршрутизатора до другого через сети.

Транспортный уровень (transport layer).[2] Линия передачи не идеальна и данные которые были переданы от одного источника приемнику могут исказится в процессе передачи или вовсе быть утеряны, чтобы обеспечить надежное соединение используется транспортный уровень.

Транспортный уровень может обеспечить требуемый уровень надежности. В модели OSI определяется 5 уровней надежности от 0 до 4, все они отличаются по надежности передачи, срочности, возможностью восстановить разорванное соединение, способностью обнаружения и исправления ошибок.

Транспортный уровень работает с сегментами. На транспортном уровне реализован алгоритм проверки верности данных и восстановления ошибок при помощи контрольной суммы, находящейся в заголовках сегмента. На транспортном уровне определяется приложение отправитель и приложение получатель по номеру порта, который присваивается каждому приложения при создании им сетевого соединения. Так же есть стандартные порты для определенных услуг, например, для получения обыкновенной HTTP страницы в браузере используется 80 порт, а для защищенного соединения по HTTPS используется 443 порт.

Принцип выбора уровня защищенности соединения зависит от многих факторов: от того обеспечивают ли защищенность протоколы верхнего уровня, на сколько требуется качество доставки сегментов, на сколько канал передачи неидеален.

Сеансовый уровень (session layer).[2] Предоставляет средство создания и поддержания сеанса связи, определения какая из сторон, в данный момент, является активной, а также обеспечивает синхронизацию сеанса. Он позволяет создавать некоторые контрольные точки, чтобы в случае отказа соединения продолжить передачу с этого момента, а не с самого начала.

*Уровень представления (presentation layer)***.**[2] Этот уровень занимается тем, чтобы уровни приложения понимали друг друга. Он преобразует один тип информации к другому чтобы принимающему устройству было понятно. Примером можно привести передача информации из системы с кодировкой ASCII в систему с кодировкой UTF-8, по сути эти кодировки символов, но из-за того, что они имеют разный принцип кодирования, то при простой передаче будет нарушен текст, поэтому нужно при приеме не просто принять данные,

но и преобразовать их к UTF-8. Так же на этом уровне может выполняться функции шифрования данных, чтобы обеспечить безопасность.

Прикладной уровень (application layer).[2] На этом уровне уже работают сами приложения. На этом уровне работают протоколы гипертекста, доступа к данным, работа с сетевыми принтерами, электронная почта и прочее. Три верхних уровня работают просто с данными.

Процесс инкапсуляции и декапсуляции

Теперь важным этапом будет рассмотрение таких понятий как инкапсуляция и декапсуляция.

Инкапсуляция следует с самого верхнего уровня представления последовательно проходя через все семь уровней вниз до физического.

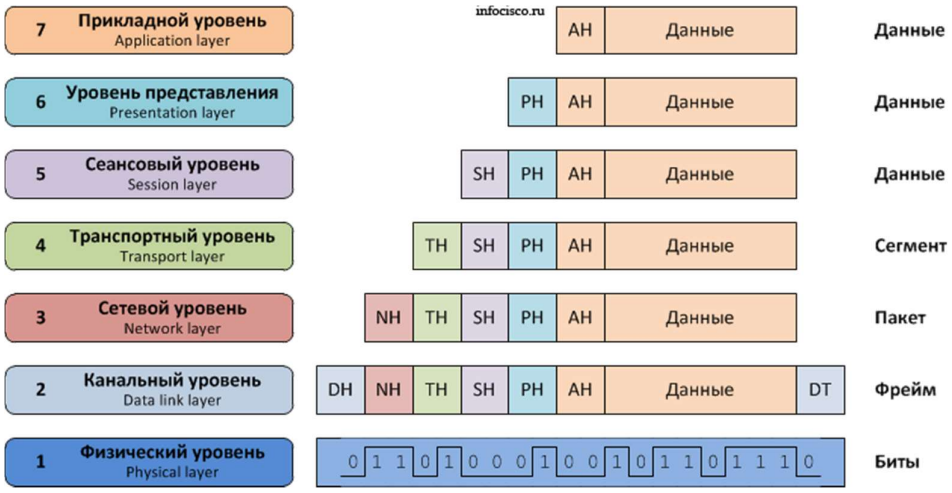

Рис. 5. Принцип инкапсуляции.

Рассмотрим процесс инкапсуляции, например, почтового письма. После того как данные были сформированы и была нажата кнопка отправки данные были помещены в поле данных на уровне приложения и были прикреплены заголовки уровня L7 (уровни сетевой модели так же принято обозначать при помощи буквы L обозначающей level и номера этого уровня, отсчет идет снизу вверх). На уровне представления все данные пришедшие от уровня приложения были помещены в поле данных и прикреплены заголовки L6 и отправлены ниже. Уровень сессии аналогично данные пришедшие от верхнего уровня помещает в поле данных и прикрепляет свои заголовки L5. На транспортном уровне уже формируются сегменты, в случае если данных

больше чем максимальный размер сегмента, то они бьются на несколько сегментов и им присваиваются порядковые номера, чтобы принимающая сторона смогла собрать на своей стороне исходное сообщение. Так же на этом уровень будет отвечать за то, требуется ли надежность доставки сообщения в случае если требуется, уровень будет отслеживать доставку сообщения и в случае неудачи будет повторно отсылать неподтвержденные сегменты. Так разбитые данные на сегменты будут помещены в поля данных и в заголовках L4 будет указан порт отправителя и получателя. На сетевом уровне в заголовках L3 будет указан IP адрес получателя и отправителя, адрес получателя нужен для маршрутизации пакетов в сети, а адрес отправителя нужен для того, чтобы получатель мог ответить на этот пакет. На канальном уровне образуется фрейм с заголовками L2 уровня. На физическом уровне тоже будут добавлены свои заголовки уровня L1 и биты пойдут в среду распространения до своего пункта назначения. В общем-то на этом процесс инкапсуляции и заканчивается, декапсуляция является обратным процессом на принимающей стороне, принятые данные идут снизу вверх попутно каждый уровень читает свои заголовки, убирает их и передает данные вверх по цепочке до уровня приложения.[4]

Стек протоколов TCP/IP

На практике модель OSI не используется и в момент развития сетей де факто стандартом стал стек протоколов TCP/IP, который и по сей день используется для передачи данных. В стеке TCP/IP, в отличии от OSI, всего 4 уровня.[5]

Вышеописанная модель OSI используется лишь для теоретического описания принципа работы сетей, на практике же используется стек протоколов TCP/IP. В момент развития сетей он де факто стал стандартом. В отличии от модели OSI в стеке протоколов TCP/IP всего 4 уровня. Меньшее количество уровней было по причине, их ненадобности в реальных системах. Реализация модели OSI будет работать заметно медленнее TCP/IP, этой причиной является то, что некоторые задачи из OSI были объединены в один блок. Уровни сеансовый, представления и прикладной были объединены в один прикладной и все требуемые задачи реализуются теперь на одном уровне, например, если потребуется шифрование данных, не потребуется взаимодействовать с дополнительным уровнем, все будет производится в пользовательском пространстве приложением. Так же были объединены канальный и физический уровень в физический.

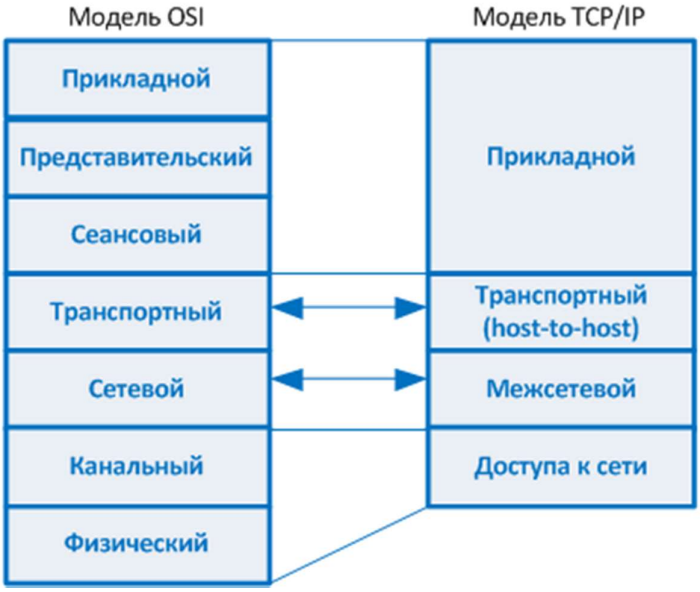

Рис. 6. Разница модели OSI и стека TCP/IP.

Структура передаваемых сообщений

Рассмотрим строение сообщения на различных уровнях:

Структура Ethernet фрейма. **[6]**

6 байт	6 байт	2 байта	46-1500 байт	4 байт
DA	SA	T	Data	FCS

DA (Destination Address) – mac адрес устройства назначения

SA (Source Address) – mac адрес отправляющего устройства

T (Type, EtherType) – в данном поле содержится тип протокола верхнего уровня.

Data – в этом поле содержатся передаваемые данные вместе с заголовками верхних уровней.

FCS (Frame Check Sequence) – поле содержащее контрольную сумму, вычисляемую по алгоритму CRC-32.

Структура IP пакета. **[7]**

<table>
<tr><td>4 бита
Version</td><td>4 бита
IHL</td><td colspan="5">8 бит
ToS</td><td colspan="2">16 бит
Total Length</td></tr>
<tr><td></td><td></td><td>3
PR</td><td>1
D</td><td>1
T</td><td>1
R</td><td>2</td><td colspan="2"></td></tr>
<tr><td colspan="4">16 бит
Identification</td><td colspan="2">3 бита
Flags</td><td colspan="2">13 бит
Fragment Offset</td></tr>
<tr><td colspan="4"></td><td></td><td>DF</td><td>MF</td><td colspan="2"></td></tr>
<tr><td colspan="2">8 бит
TTL</td><td colspan="3">8 бит
Protocol</td><td colspan="3">16 бит
Header checksum</td></tr>
<tr><td colspan="8">32 бита
Source IP Address</td></tr>
<tr><td colspan="8">32 бита
Destination IP Address</td></tr>
<tr><td colspan="8">Options</td></tr>
</table>

Version - номер версии показывает версию протокола IPv4 или IPv6.

IHL (Internet Header Length) - Содержит величину длины заголовка, обычно это 20 байт, но при добавлении служебной информации размер заголовка может расти, максимальный объем заголовка может расти до 60 байт.

ToS (Type of Service) – байт дифференцированного обслуживания, или DS-байт. Предназначение этого поля, хранить признак требуемого качества обслуживания. PR (Priority) – 3 бита приоритета пакета от 0 до 7. D (Delay) – бит задержки, если бит задан в 1, то пакет должен доставляться с минимальной задержкой. T (Throughput) – пропускная способность при 1 выбирается максимальная пропускная способность. R (Reliability) – надежность при 1 выбирается максимальная. Остальные 2 бита выставляются в 0.

Total Length - поле характеризующее полную длину пакета с данными и заголовками.

Identification - идентификатор пакета требуется для сборки единого файла, который был разбит на стороне сервера и у всех частей одного файла поле должно быть одинаковым.

Flags – флаги, поле содержит признаки фрагментации пакета. DF (Do not Fragment) – не фрагментировать, если этот бит выставлен в 1 то этот пакет запрещается фрагментировать. MF (More Fragments) – больше фрагментов, выставленный бит дает понять что этот пакет промежуточный (не является последним). 3 бит зарезервирован.

Fragment Offset - смещение фрагмента относительно начала нефрагментированных данных.

TTL (Time to Live) – время жизни устанавливает через сколько хопов пакет будет отброшен как устаревший (хопом считается переход от одного устройства до другого с уровнями L3 или выше).

Protocol – протокол который используется на вышестоящем уровне для поля дата.

Header checksum – контрольная сумма заголовка рассчитываемая только для IP заголовка.

Source IP Address – IP адрес источника сообщения.

Destination IP Address – IP адрес получателя сообщения.

Options – опции, является необязательным полем.

Структура TCP сегмента. **[8]**

Source Port								Destination Port
Sequence number								
Acknowledgment number								
Header length		URG	ACK	PSH	RST	SYN	FIN	Window
Checksum								Urgent pointer
Options								
Padding								

Source port – порт источника сообщения.

Destination port – порт назначения.

Sequence number – последовательный номер, при разбиение сообщения на сегменты, определяет порядковый номер сегмента.

Acknowledgment number – подтвержденный номер указывает на последний байт в сегменте увеличенный на единицу.

Header length – длина заголовка.

Флаги URG, ACK, PSH, RST, SYN, FIN используются для обозначения намерений пакета, например, SYN для запроса установки соединения.

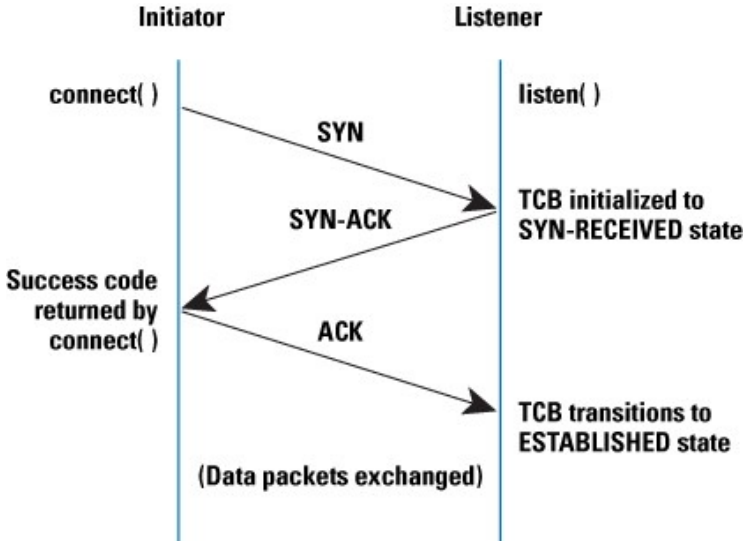

Рис. 7. Пример использования флагов SYN, ACK при создании соединения (TCP Handshake – TCP рукопожатие).

На рис. 7 показан процесс создания соединения между клиентом и сервером. Для инициализации канала клиент отправляет серверу пакет с флагом SYN, если сервер не занят, то в ответ он шлет TCP пакет с флагами SYN, ACK тем самым подтверждая создание соединения и в конце клиент подтверждает создание канала TCP пакетом с флагом ACK. Этот процесс называется TCP handshake.

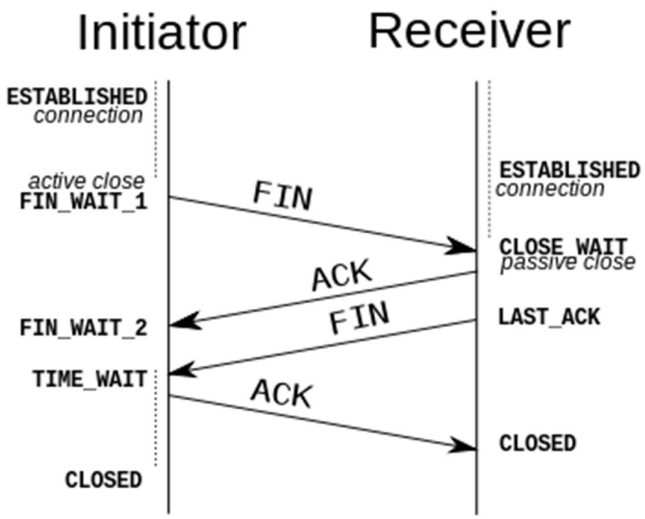

Рис. 8. Пример использования флагов FIN, ACK при разрыве соединения.

На рис. 8 отображен пример использования TCP флагов для разрыва соединения. Закрыть соединение может как сторона сервера, так и сторона клиента. Верхние две стрелки отображают закрытие соединения со стороны клиента, он шлет на сервер пакет с флагом FIN, на что сервер отвечает пакетом с флагом ACK, с этого момента соединение считается законченным. Аналогично соединение может разорвать и сервер, нижние две стрелки.

Window – окно, это поле характеризует размер окна которое устанавливает отправитель для принимаемых данных.

Checksum – контрольная сумма заголовка.

Urgent pointer – указатель срочности, указывает через сколько сегментов закончатся важные данные.

Options – параметры, необязательный параметр.

Padding – заполнение, выравнивает сегмент чтобы он нацело делился на 32 бита.

Исследование и доработка алгоритма фильтрации клиентов

Теперь, когда рассмотрен принцип работы сети можно понять почему фильтрация будет осуществляться именно по MAC адресу. Как было рассмотрено ранее при принятии пакета на маршрутизаторе он по стеку декапсулируется.

Для написания нашего алгоритма мы используем маршрутизатор, который по модели OSI работает на L3 уровне, т.е. при декапсуляции он максимум раскрывает пакет по сетевого уровня, следовательно, всего возможных уровней для выбора фильтрации у нас 3: физический, канальный и сетевой. На физическом мы не можем взаимодействовать с данным, т.к. этого нам не позволяет система, значит уже остается два уровня: канальный и сетевой. На канальном уровне мы можем оперировать с source MAC и destination MAC, а на сетевом с source IP и destination IP. Для скорости обработки мы будем фильтровать пакет по первому доступному уровню: канальному.

Так как мы рассматриваем реальное физическое устройство, то взаимодействие идет по стеку протоколов TCP/IP, а в стеке протоколов физический и канальный уровень объединены в один, следовательно, мы работает с физическим уровнем. При приеме пакета, на физическом уровне мы можем работать только с destination mac address и source mac address. Так как пакет назначается нам, то поле destination mac address проверяется на приеме, иначе по правилам пакет сразу отбрасывается. Следовательно, нам остается только поле source mac address. Плюсы фильтрации по mac адресу заключаются в некоторых моментах, первый это то, что физический уровень будет проверяться самым первым, тем самым обеспечивать минимальную задержку обработки пакета, так же удобство заключается в том, что все mac адреса принадлежат плоской локальной сети, т.е. мы точно знаем, что блокируемый клиент находится с нами в одной сети в шаговой доступности. Так же по стандарту у любого устройства, имеющего доступ в сеть, имеется уникальный mac адрес, что позволяет нам быть уверенным в том, что при

блокировке определенного mac адреса, мы случайно не закроем доступ другому устройству.

Целью моей работы является переработка существующего алгоритма фильтрации клиентов по MAC `адресу. Для тестов и проверок в наличии имеется Wi-Fi точка доступа WEP12-ac.

Рис. 9. WEP-12ac вид сбоку.

Рис. 10. WEP-12ac вид сверху.

Технические характеристики WEP-12ac[9]

Интерфейсы

- 2 порта Ethernet 10/100/1000 Base-T (RJ-45)
- Console (RJ-45)

Возможности WLAN

- Поддержка стандартов IEEE 802.11a/b/g/n/ac
- Агрегация данных, включая A-MPDU (Tx/Rx) и A-MSDU (Rx)
- Приоритеты и планирование пакетов на основе WMM
- Динамический выбор частоты (DFS)
- Поддержка скрытого SSID
- 32 виртуальные точки доступа
- Обнаружение сторонних точек доступа
- Поддержка APSD
- Поддержка WDS

Сетевые функции

- Автоматическое согласование скорости, дуплексного режима и переключения между режимами MDI и MDI-X
- Поддержка VLAN
- Поддержка аутентификации 802.1X
- DHCP-клиент
- Поддержка LLDP
- Поддержка ACL
- Поддержка IPv6

Работа в режиме кластера

- Организация кластера емкостью до 64 точек доступа
- Балансировка нагрузки между точками доступа
- Автоматическая синхронизация конфигураций точек доступа в кластере
- Single Management IP - единый адрес для управления точками доступа в кластере

- Автоматическое распределение частотных каналов между точками доступа
- Аутентификация через RADIUS-сервер

Функции QoS

- Приоритет и планирование пакетов на основе профилей
- Ограничение пропускной способности для каждого SSID
- Изменение параметров WMM для каждого радиоинтерфейса

Безопасность

- Централизованная авторизация через RADIUS-сервер (WPA Enterprise)
- Шифрование WPA/WPA2
- Поддержка Captive Portal
- E-mail информирование о системных событиях

Параметры беспроводного интерфейса

- Частотный диапазон 2400 - 2480 МГц, 5150 - 5850 МГц
- Модуляция CCK, BPSK, QPSK, 16QAM, 64QAM, 256QAM
- Внутренние всенаправленные антенны
- Поддержка 3x3 MIMO
- Два встроенных чипа Broadcom BCM43460 (IEEE 802.11a/b/g/n/ac)

Рабочие каналы

802.11b/g/n:

- 1-13 (2412 - 2472 МГц)1

802.11a/n/ac:

- 36-64 (5180 - 5320 МГц)
- 100-144 (5500 - 5720 МГц)
- 149-165 (5745 - 5825 МГц)

Скорость передачи данных

- 802.11n: 450 Мбит/с
- 802.11ac: 1300 Мбит/с

Чувствительность приемника

- 2.4 ГГц: до -98 дБм
- 5 ГГц: до -94 дБм

Максимальная выходная мощность передатчика

- 2.4 ГГц: до 19 дБм
- 5 ГГц: до 19 дБм

Физические характеристики

- Потребляемая мощность не более 14 Вт
- Процессор Broadcom BCM53016/BCM58522
- 128 МБ NAND Flash
- 256 МБ RAM DDR3
- Питание:
    - PoE+ 48В/54В (IEEE 802.3at-2009)
    - 12 В DC
- Рабочая температура от +5°C до +40°C
- Размеры (ШхВхГ): 224x42x235 мм

Конфигурирование

- Обновление ПО и конфигурирование посредством DHCP Autoprovisioning
- Удаленное управление по Telnet, SSH
- Web-интерфейс
- SNMP

Так же эта прошивка будет работать на моделях WEP-2ac, WOP-12ac, но на них мною тесты не проводились.

Рис. 11. WEP-2ac.

Рис. 12. WOP-12ac.

Все эти Wi-Fi точки доступа (AP – access point) умеют создавать виртуальные точки доступа (VAP – virtual access point), тем самым позволяют поднимать более одной Wi-Fi сети с одного устройства. Сейчас в прошивке алгоритм фильтрации клиентов по MAC адресу не удовлетворяет требованиям

потребителей, тем что этот список действует на все VAP сразу и не имеет возможности настраивать его индивидуально.

Принцип работы исходного алгоритма фильтрации

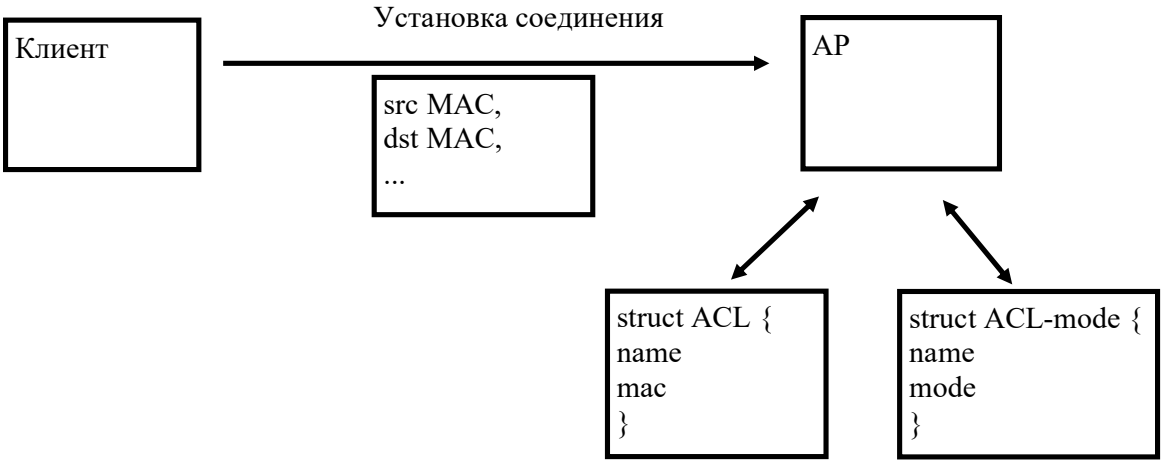

Рис. 13. Принцип работы исходного алгоритма фильтрации клиентов.

Текущий принцип фильтрации схематично можно отобразить таким образом. От клиента приходит пакет на создание соединения, в этом пакете хранятся MAC адрес отправителя, MAC адрес получателя и другая служебная информация. При принятии пакета точка сначала берет значение из структуры ACL-mode (access control list – mode), в ней хранится политика точки, она может быть в двух состояниях deny-list или accept-list, в поле name всегда стоит default. После получения политики фильтрации в цикле начинают сверяться все объекты структуры ACL с полем принятого пакета src MAC. В структуре ACL имеется два поля, поле name всегда в значении default, а в поле mac один mac списка фильтрации, таких объектов структур может быть много, они то и составляют список фильтрации. Затем в зависимости от политики принимается решение что делать с принятым пакетом. Если политика deny-list, то пакет будет пропущен в случае если ни один mac из списка ACL не совпал с src MAC, иначе он будет отброшен. Если выбранная политика access-list, то пакет будет пропущен в случае если src MAC совпал хотя бы с один из списка ACL, иначе он будет отброшен. Будем называть deny-list и access-list черными и белым списком соответственно. Единственным удобным способом управления списками на данный момент, является управление через web интерфейс.

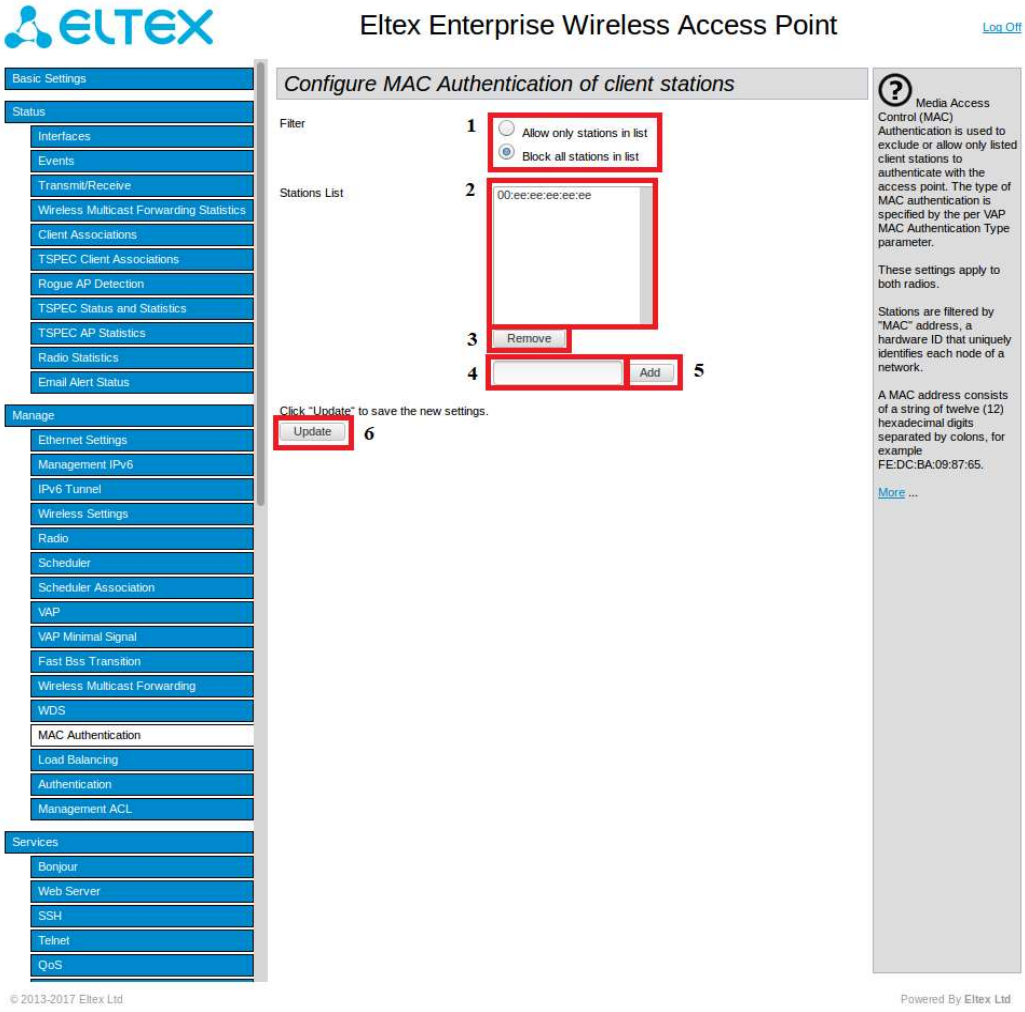

Рис. 14. Web интерфейс управления списками фильтрации.

На рис. 14 мы видим выделенные блоки:

1) Отвечает за управление политикой.

2) Уже добавленные MAC адреса в список.

3) Кнопка удаления выделенного MAC адреса из списка.

4) Поле ввода MAC адреса.

5) Кнопка добавления введенного MAC адреса в список.

6) Кнопка синхронизации настроек.

Доработка алгоритма фильтрации

Моя задача заключается в том, чтобы у каждой VAP был свой ACL и ACL-mode, и реализовать инструменты управление этим в Web интерфейсе и в CLI (command line interface). Так как я не писал все сам с чистого листа, а мне предоставили прошивки, в которой я доделывал свой функционал, то предоставить исходный код я не могу, он является интеллектуальной собственностью компании Eltex. У представленных структур на рис. 13 ACL и ACL-mode есть такое поле как name и у каждого VAP есть такой параметр как mac-acl-name, по умолчанию они все равны default, поэтому список и политика применяется ко всем VAP одни и те же.

Немного переработаем систему фильтрации. До этого у каждого VAP стоял параметр mac-acl-name в значении default, оставим это для совместимости со старыми файлами конфигурации, но реализуем изменение списка фильтрации для отдельного VAP.

set bss [VAP name] mac-acl-name [ACL name]

Просто меняет у класса поле mac-acl-name на введенное, но после изменения этого значения, после этого он будет использовать mac адреса с таким же именем. Теперь реализуем добавление mac адреса в какой-нибудь список фильтрации.

add mac-acl [ACL name] mac [mac устройства]

Теперь указывая одинаковое ACL name при добавления mac и у VAP, он будет использовать только их. Также нужно сделать индивидуальную политику при фильтрации.

set bss [VAP name] mac-acl-mode [deny-list/accept-list]

Теперь мы можем менять политику. Так же у нас имеется возможность назначить один и тот же ACL на разные VAP, но выставить у них разные политики, если это потребуется. Так же у нас имеется параметр mac-aclist-mode, в нем выставляется глобальная политика для все VAP одновременно. На данном моменте она нам мешает, т.к. она перебивает наши установки локальной политики. Убрать мы его не можем, из-за сохранения

совместимости со старыми конфигурациями. Чтобы избежать конфликтов ведем у каждой VAP такой параметр как mac-acl-global, он будет указывать на то, нужно ли применять к данной VAP глобальную политику или сохранять локальную. В случае если mac-acl-global выставлено в значение on, то в цикле установки локальных политик на глобальную они будут выставляться, в случае если mac-acl-global будет выставлено в off, то глобальная политика будет игнорироваться и сохраняться локальная.

set bss [VAP name] mac-acl-global [on/off]

Также чтобы изменить глобальную политику требуется выполнить

set mac-aclist-mode [deny-list/accept-list]

На этом реализацию всех возможностей и управление в CLI считаю выполненной, приступим к реализации управления через Web интерфейс.

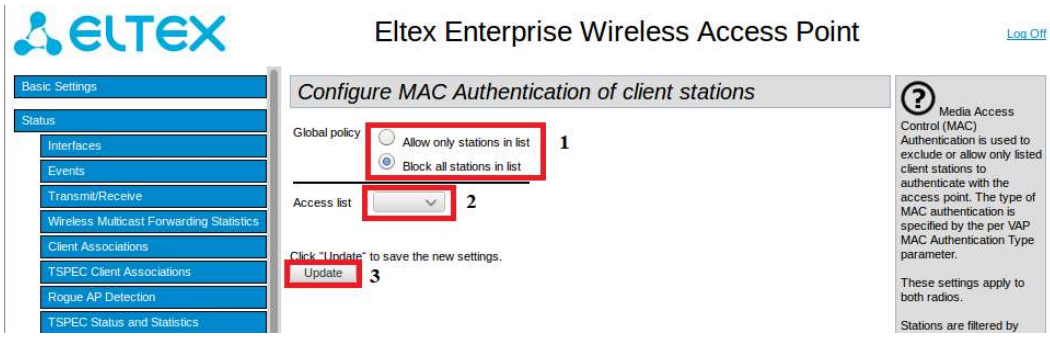

Рис. 15. Управление через Web интерфейс. Стартовая страница.

Как видно из рис. 15 наш Web интерфейс претерпел небольшие изменения.

1) Сохранился блок управления глобальной политикой.
2) Выпадающий список для дальнейшей работы со списками.
3) Синхронизация настроек.

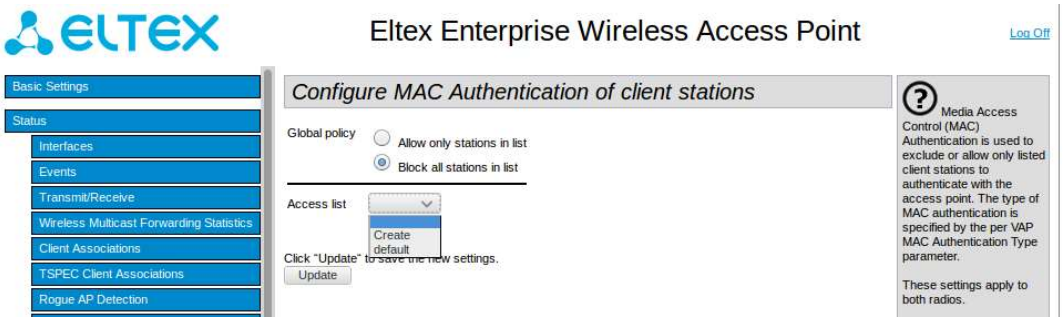

Рис. 16. Управление через Web интерфейс. Демонстрация выпадающего списка.

Как видно из рис. 16 при нажатии на выпадающий список изначально у нас есть два пункта меню:

Create – для создания нового списка фильтрации.

default – это первоначальный список который применен для всех VAP, сохранен для совместимости.

Выберем пункт Create, для того чтобы посмотреть как создается новый ACL.

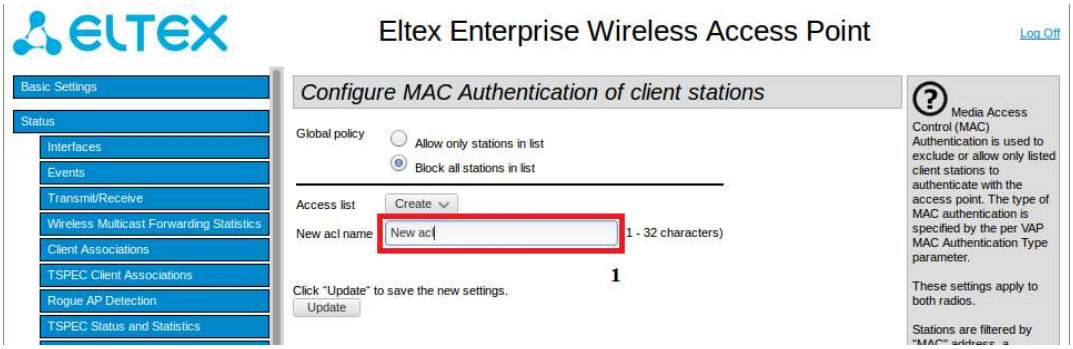

Рис. 17. Управление через Web интерфейс. Создание нового списка фильтрации.

1) Поле для ввода имени нового списка фильтрации.

После нажатия кнопки Update нас переведет в режим управления созданным списком.

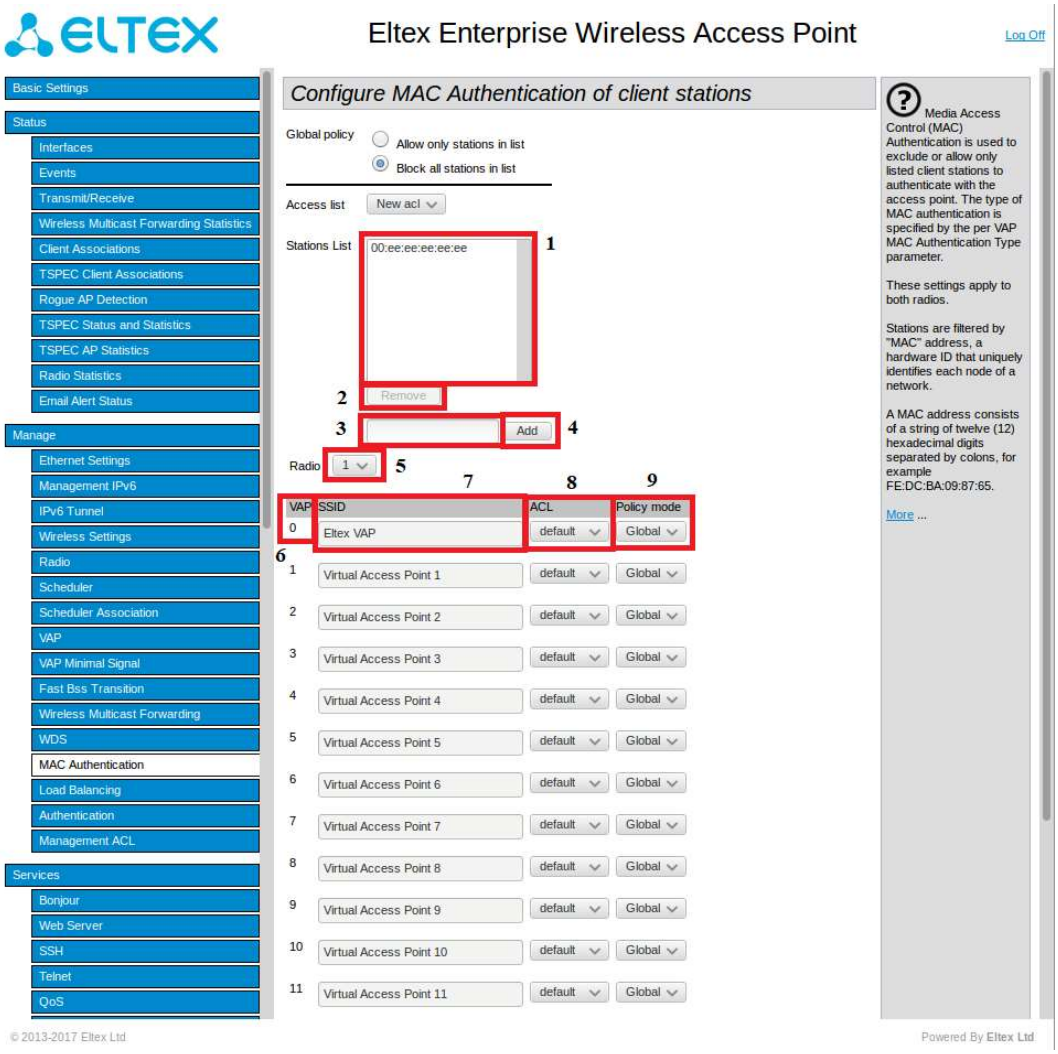

Рис. 18. Управление через Web интерфейс. Настройка созданного списка.

1) Список MAC адресов в текущем ACL.
2) Удаление выделенного MAC из списка.
3) Поле для ввода MAC адреса.
4) Добавление MAC адреса в список.
5) Выбор радио модуля (на одной ТД может быть более одного радио модуля, следовательно и VAP нужно настраивать на них отдельно).
6) Столбец в котором отображается номер VAP.
7) Столбец отображающий имя VAP.
8) Столбец для настройки ACL для VAP.
9) Столбец для настройки политики для VAP.

Рис. 19. Управление через Web интерфейс. Настройка созданного списка, продолжение.

Рассмотрим содержимое выпадающих списков.

Рис. 20. Управление через Web интерфейс. Содержание выпадающего списка Radio.

Как видно на WEP-12ac 2 радио модуля, при смене на другой нижняя таблица с настройками VAP изменится на новые значения.

Рис. 21. Управление через Web интерфейс. Содержание выпадающего списка ACL.

Сейчас у нас в ACL содержится два пункта меню, это default, стандартный список фильтрации и New acl, это наш только что созданный список.

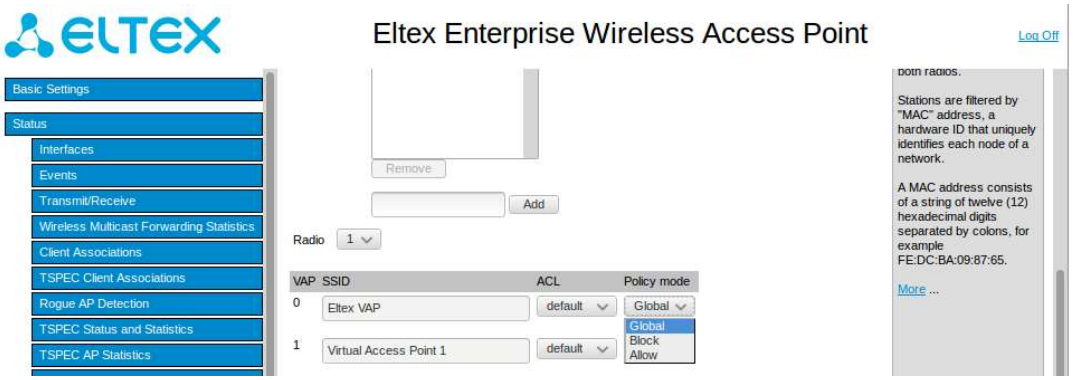

Рис. 22. Управление через Web интерфейс. Содержание выпадающего списка Policy mode.

Тут настраивается политика конкретного VAP, существует три режима:

Global – в этом случае к VAP применяется политика установленная вверху страницы.

Block – активирована локальная политика черного списка.

Allow – активирована локальная политика белого списка.

Заключение

В результате выполнения работы поставленное техническое задание было выполнено в полном объеме. В данный момент этот функционал используется в новых версиях прошивок для WEP-12ac, WOP-12ac и WEP-2ac.

Экономический раздел

Себестоимость - это стоимостная оценка используемых в процессе производства продукции (работ, услуг) природных ресурсов, сырья, материалов, топлива, энергии, основных фондов, трудовых ресурсов и других затрат на её производство и реализацию.

Таблица 1. Стоимость материалов

Наименования	Количество, шт	Стоимость, р
Системный блок	1	30299
Монитор	1	6299
Клавиатура	1	690
Мышь	1	350
Компьютерный стол	1	14999
Стул	1	725
Суммарная стоимость оборудования		53362

Рассчитаем оклад программиста. Оклад программиста составляет 22600р. Вычтем подоходный налог 13% чтобы найти зарплату.

Зарплата = оклад – 13% = 22600 – 13% = 20000(р), за месяц

Срок выполнения работы составляет три месяца.

Общая зарплата = 20000 * 3 = 60000(р)

Амортизация рассчитывается для товар стоимостью более 10000р. Рассчитаем амортизацию для системного блока и стола.

A = K * C

A – размер месячных амортизационных отчислений

K – норма амортизации

C – первичная стоимость продукта

K = 1 / n * 100%

n – срок эксплуатации продукта в месяцах

Компьютер относится ко второй амортизационной группе поэтому принимаем его срок эксплуатации равным 5 лет

$К_{компьютера} = 1 / 60 * 100\% = 1.67\%$

$А_{компьютера} = 1.67\% * 30299 = 505.9р$, ежемесячные амортизационные отчисления за системный блок.

Компьютерный стол относится к 4 амортизационной группе, следовательно, срок эксплуатации принимаем равным 7 лет.

$К_{стол} = 1 / 84 * 100\% = 1.19\%$

$А_{стол} = 1.19\% * 14999 = 178.5р$, ежемесячные амортизационные отчисления за компьютерный стол.

Таблица 2. Амортизационные отчисления

Наименование	Амортизация за месяц, р
Системный блок	505.9
Компьютерный стол	178.5
Амортизация за месяц	684.4
Общая амортизация, за весь срок работы	2053.2

Рассчитаем затраты на электроэнергию.

$З_{с.эл} = М_{пр} * Ф_{д} * С_{квт/ч}$

$З_{с.эл}$ – затраты на силовую электроэнергию

$М_{пр}$ – электроэнергия, потребляемая ПК кВт/ч

$Ф_{д}$ – фонд рабочего времени оборудования, час

$С_{квт/ч}$ – стоимость 1 кВт/ч

По текущим тарифам стоимость одного кВт/ч в Новосибирске составляет 2.49р. Электроэнергия потребляемая ПК составляет 250Вт/ч.

$З_{с.эл} = 250 * 240 * 2.49 = 149.4р$

Рассчитаем себестоимость.

Таблица 3. Себестоимость.

Наименование	Стоимость, р
Общая стоимость оборудования	53362
Зарплата программиста	60000
Общая амортизация	2053.2
Затраты на электроэнергию	149.9
Себестоимость	115565.1

Раздел охраны труда

Основные термины и понятия:

Пользователь ПК – сотрудник, который использует ПК в целях решения данных ему задач по долгу службы.

Компьютер – рабочая станция, предназначенная для сбора, накопления, передачи и обработки информации, в состав компьютера входят системный блок, монитор и другое периферийное оборудование.

Рабочее место пользователя ПК – место, где сотрудник находится в течении всего рабочего времени, для выполнения обязанностей, предполагающее работу за компьютером.

Использование ПК на рабочем месте приводит к повышению эффективности сотрудника, так и к вредным влияющим факторам на этого сотрудника.

В соответствии с СанПиН: 2.2.2.542-96 «Гигиенические требования к ВДТ и ПЭВМ. Организация работы» все вредные факторы можно поделить на 3 группы:

1) Параметры рабочего места и рабочей зоны.
2) Визуальные факторы (яркость, контрастность, мерцание изображения, блики).
3) Излучения (рентгеновские, электромагнитное излучение ВЧ и СВЧ диапазона, гамма-излучение, электростатические поля).

Расположение рабочих мест сотрудников относительно оконных проемов:

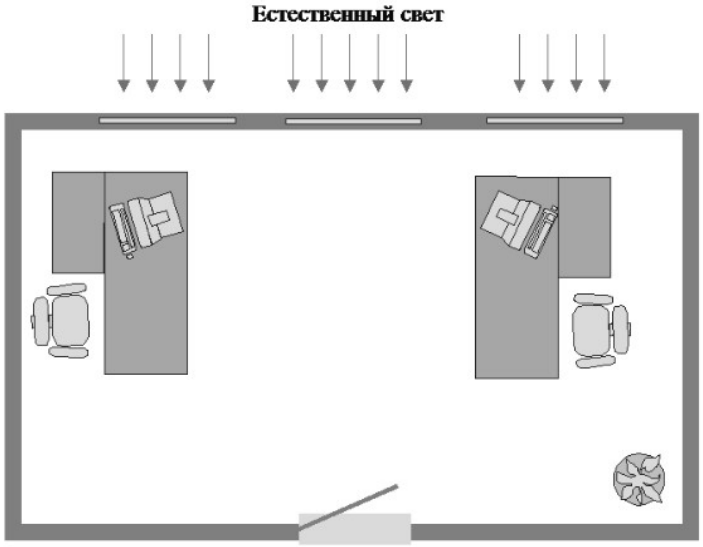

Рис. 23. Пример правильного расположения рабочих мест относительно оконных проемов.

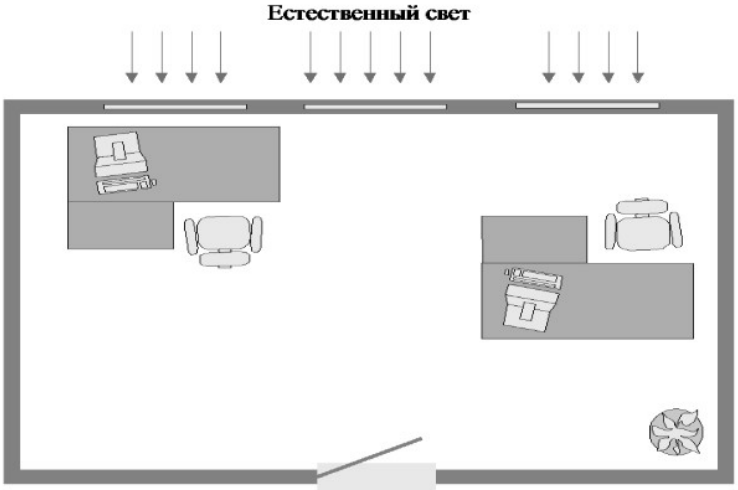

Рис. 24. Пример неправильного расположения рабочих мест относительно оконных проемов.

Необходимое свободное место вокруг монитора:

Рис. 25. Свободное пространство вокруг монитора.

Размеры рабочего стула для работы за ПК:

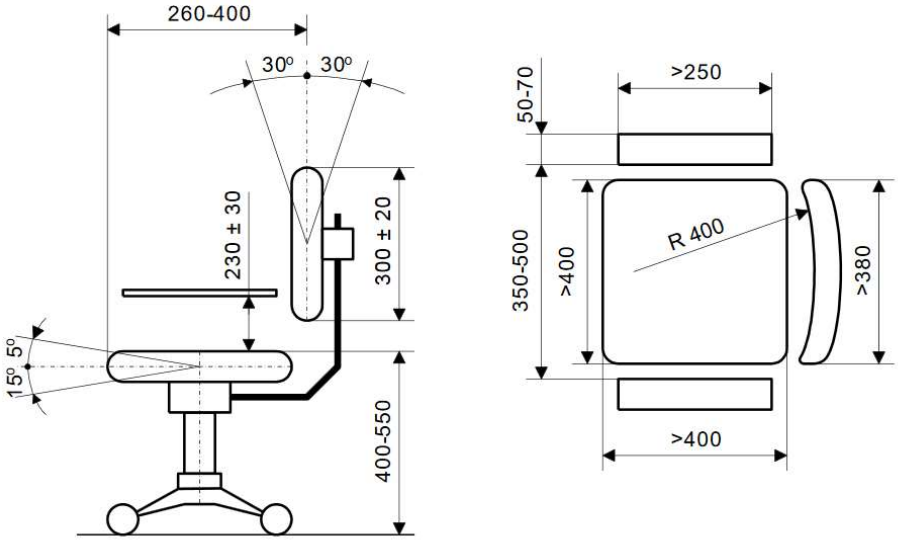

Рис. 26. Размеры рабочего стула.

Размеры рабочего стола:

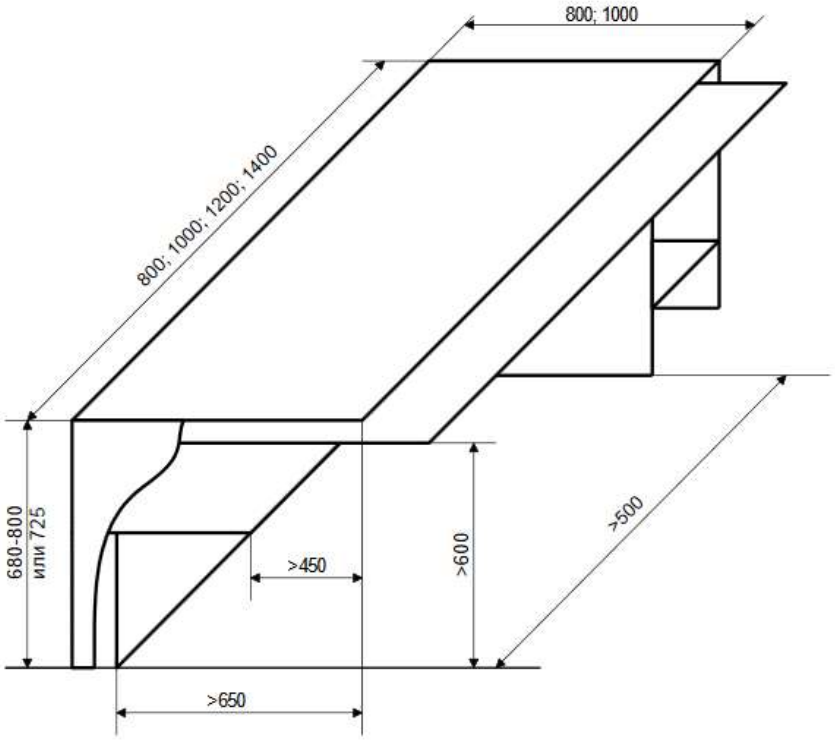

Рис. 27. Размеры рабочего стола.

Список используемых источников

1) Столлингс В. Беспроводные линии связи и сети.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 640 с.
2) Олифер В. Г., Олифер Н. А. О-54 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. СПБ.: Питер, 2010. 944 с. : ил.
3) https://www.youtube.com/watch?v=Afvm-laWfbM&index=9&list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9
4) Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети. 5-е изд. СПБ.: Питер, 2012. 960 с.: ил.
5) Ногл М. Н76 TCP/IP. Иллюстрированный учебник М.: ДМК Пресс, 2001. 408 с.:ил.
6) http://www.ieee802.org/3/as/public/0607/802.3as_overview.pdf
7) https://tools.ietf.org/html/rfc791
8) https://tools.ietf.org/html/rfc793
9) http://eltex-co.ru/catalog/wep-12ac.php