EWS Engenius

Все знают компанию Ubiquiti с точками доступа UniFi, но мало кто слышал о таком производителе, как Engenius, и его серию Neutron. В данной статье мы расскажем о новых устройствах от Engenius, и сравним их с UniFi.

Решения на базе устройств от Ubiquiti и Engenius применяются для построения беспроводных сетей в офисах, ТРЦ и других подобных местах.

Почему именно они? Преимущества:

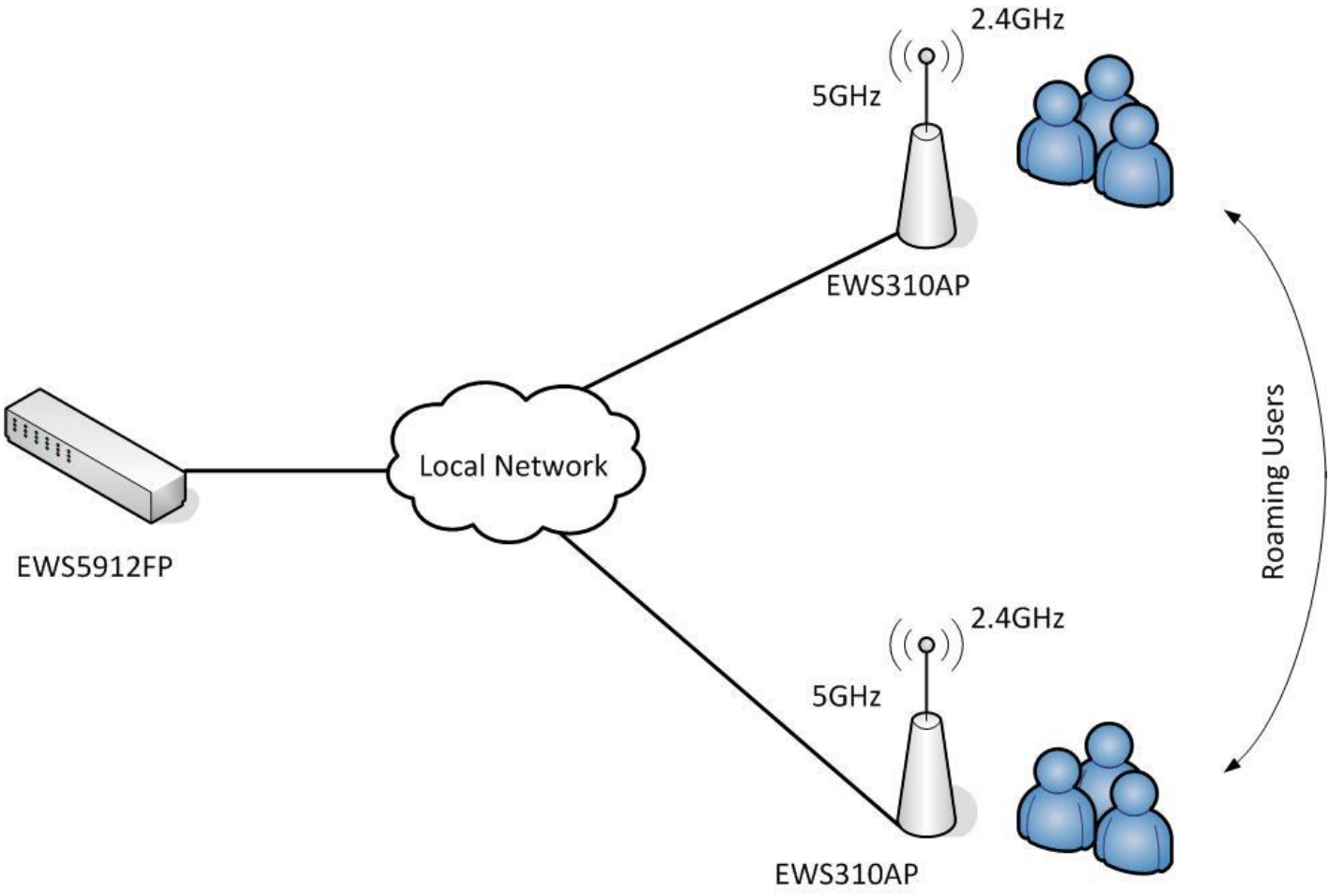
- Поддержка современных беспроводных стандартов;
- Централизованное управление всеми устройствами (обновление, конфигурирование, мониторинг и др.);
- Организация роуминга при движении между точками доступа;
- Бюджет;
- И, наконец, стильный дизайн, который впишется практически в любой интерьер.

В ходе тестирования мы определяли:

- возможность использования решения Engenius серии EWS Neutron в корпоративных сетях малого/среднего бизнеса;
- имея штатный функционал, строили бесшовный роуминг на оборудовании Engenius.

На демонстрационном стенде мы использовали ноутбук с Windows7, контроллер беспроводных сетей EWS5912FP (FW Version: 1.0.4), точки доступа EWS310AP (2.0.7 + 1.0.3), FreeRADIUS, Wi-fi-клиент (Android Phone).

Схема тестирования:



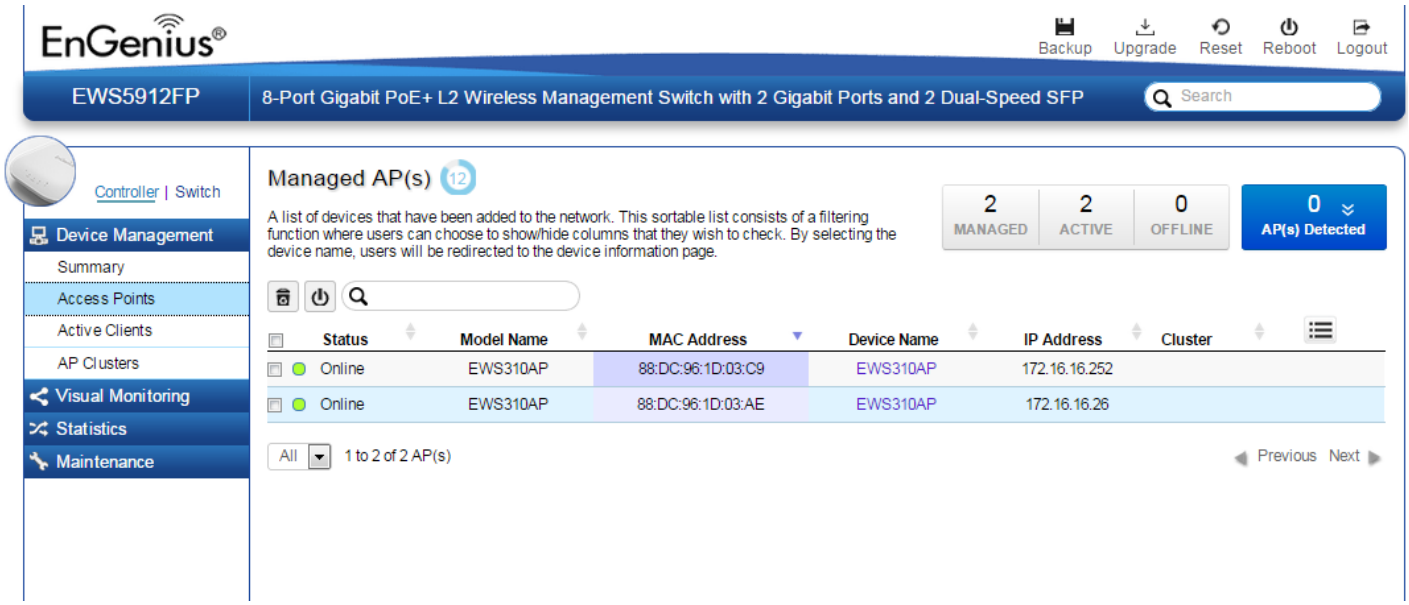
Первый запуск

Процессы запуска устройств Engenius и Unifi схожи: при первоначальном конфигурировании необходимо наличие контроллера и всех устройств в одном сегменте сети.

При запуске точки доступа контроллер автоматически определит ее наличие в сети и добавит в

меню управления для дальнейшего конфигурирования.

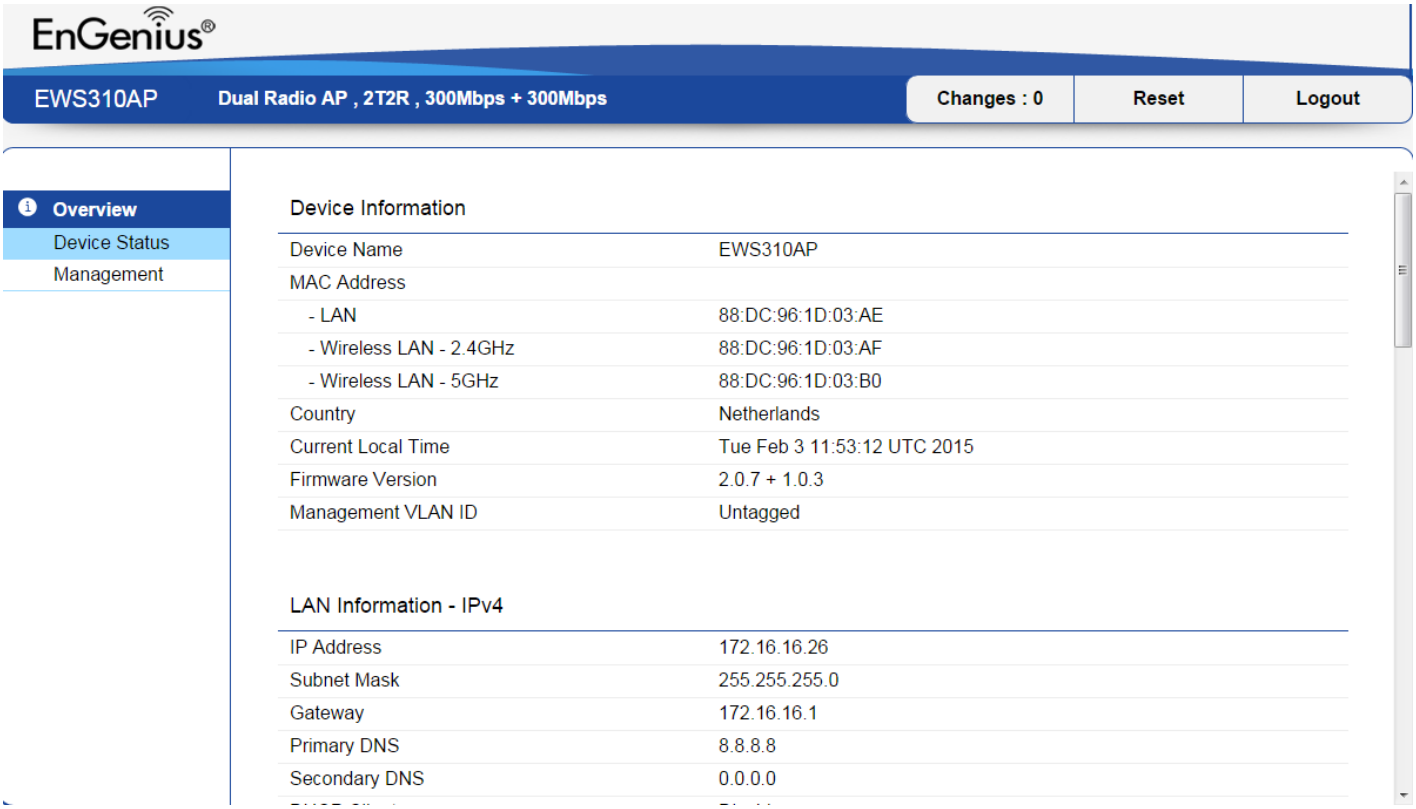
Из минусов следует отметить следующий факт. Процесс "изучения" контроллером локальной сети на наличие доступных точек доступа может затянуться, поскольку одну точку доступа контроллер может определить сразу, а вторую - через произвольное время, причем в логе контроллера этот процесс никакой дополнительной информацией не сопровождается.



Точки доступа Engenius, в отличие от Unifi, имеют собственный веб-интерфейс, через который, согласно документации, можно выполнить некоторый минимум конфигурации для работы в сети. Однако при запуске EWS310AP доступно, фактически, только две опции:

- Device Status – можно посмотреть статус текущей конфигурации;
- Management - сброс конфигурации и перезагрузка точки доступа.

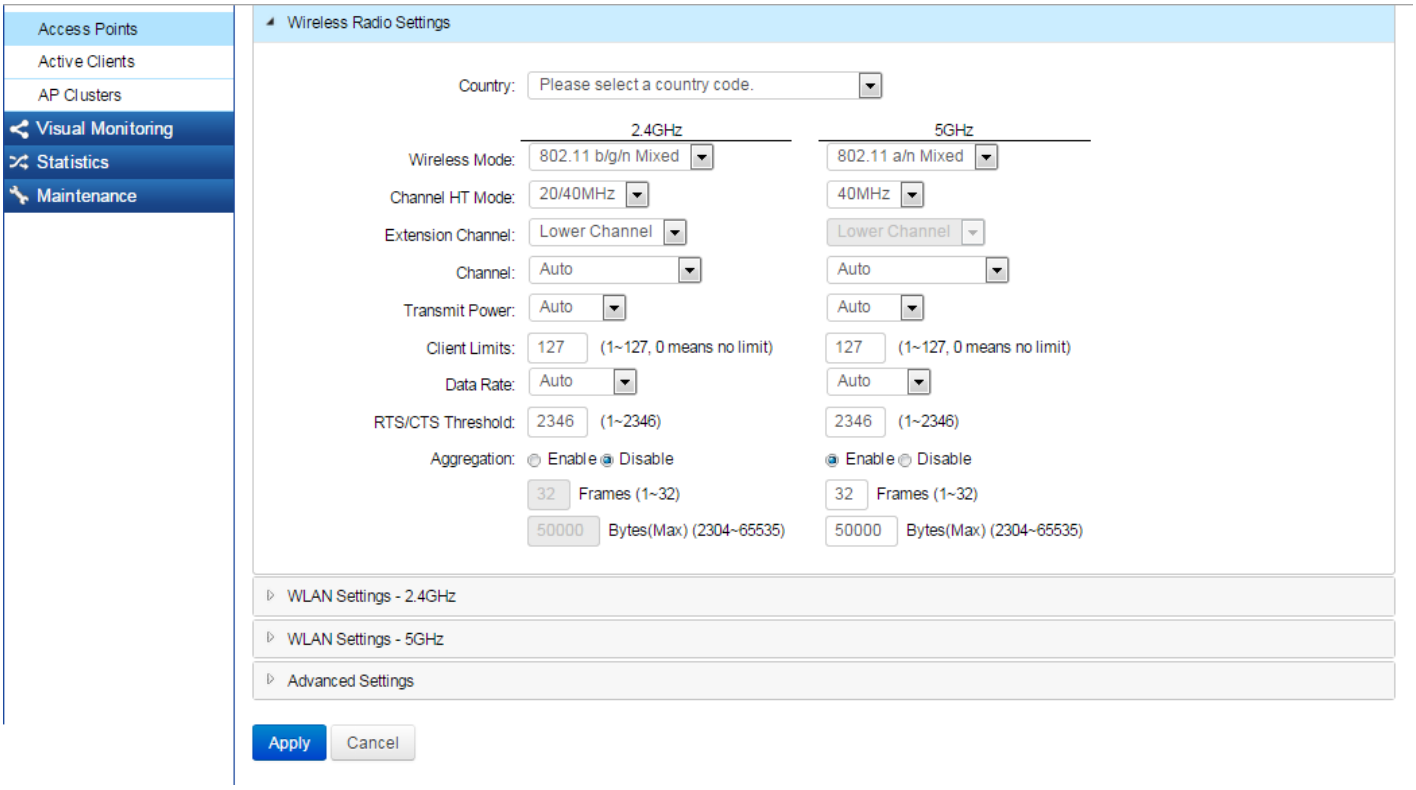
Также, согласно документации, на точке доступа можно сконфигурировать логирование, что позволит детально наблюдать за всем происходящим. Однако эта функция недоступна, поскольку управление точкой доступа ограничено статусом и менеджментом. Доступны лишь сброс точки доступа в заводские конфигурации или перезагрузка устройства.



Кроме EWS310AP, мы планировали использовать EWS210AP, но, в ходе подготовительных работ, он был исключен из схемы, так как долгие попытки определить точку доступа на контроллере так и не увенчались успехом. Зато его веб-интерфейс, в отличие от EWS310AP, соответствует документации (вне контроллера работает как штатная точка доступа).

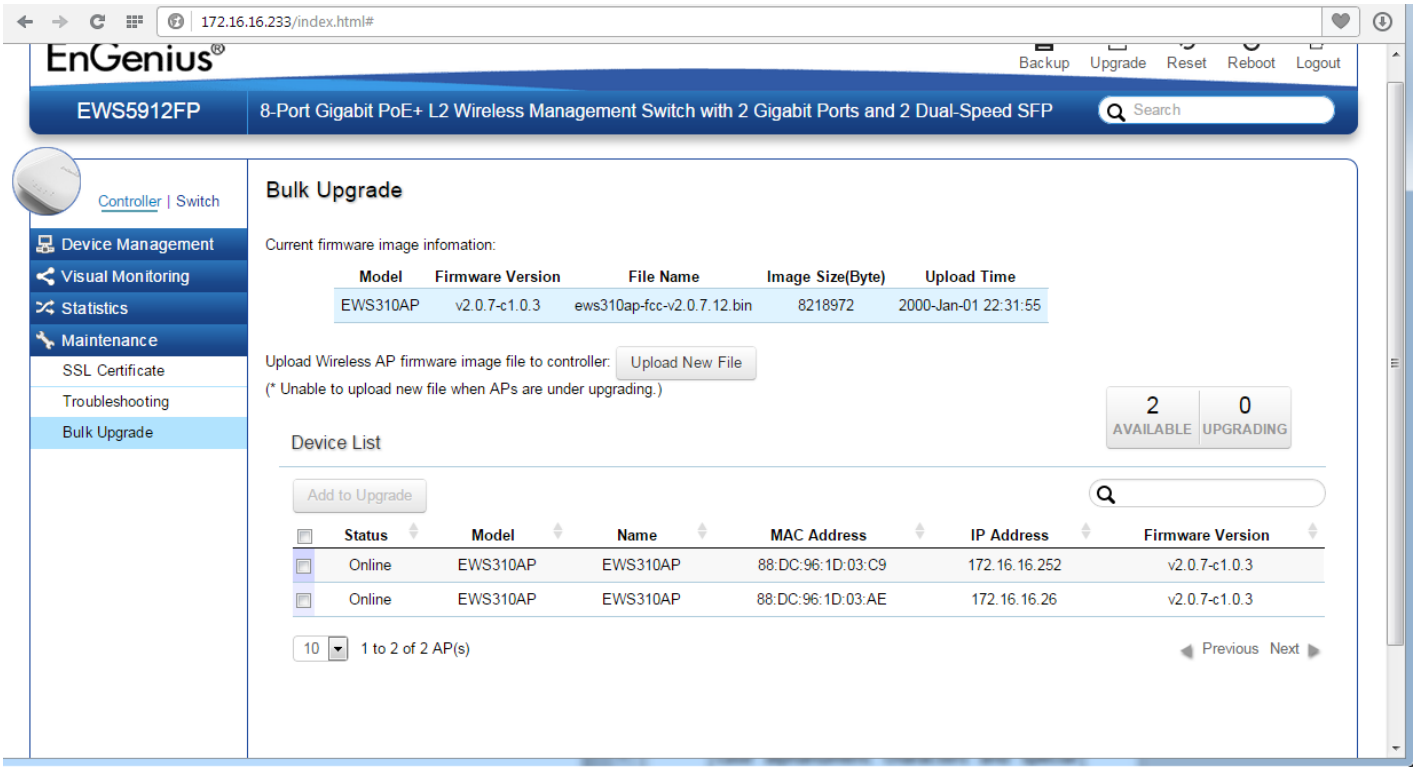
Конфигурация

Процесс конфигурации достаточно тривиальный: достаточно указать SSID, ключи, частотный канал, ширину и прочие опции по желанию.



Bulk Upgrade

Как и UniFi, Engenius имеет возможность массового обновления ПО прямо через контроллер. Можно посмотреть текущую версию ПО, и обновить либо все, либо отдельные точки доступа.



Процесс прост: загружаем ПО на контроллер, отмечаем птичками нужные точки доступа и нажимаем обновить. После перезагрузки ПО, загруженное на контроллер, удаляется (судя по всему, хранится в /tmp).

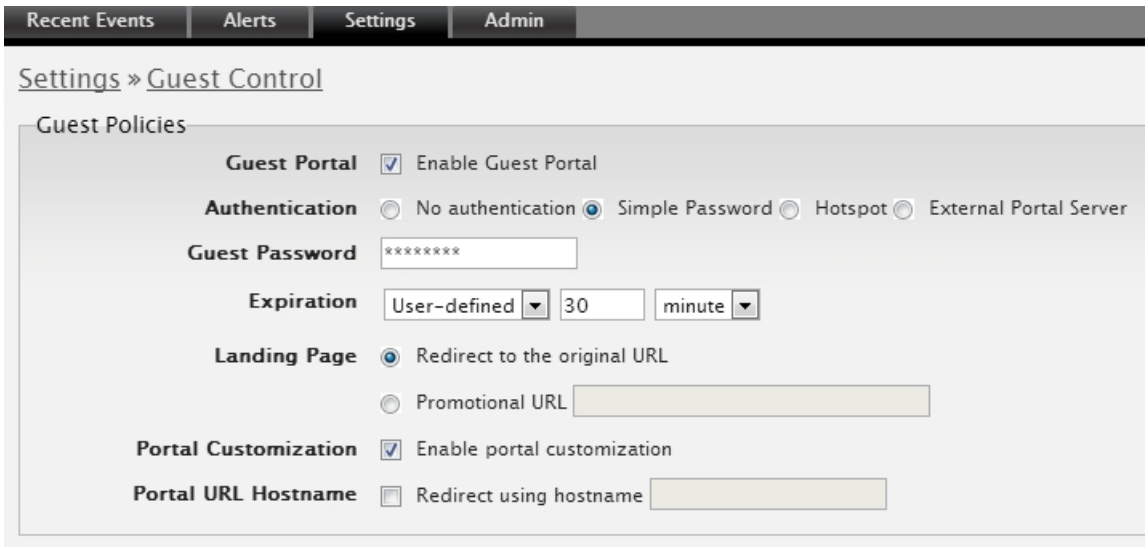
Кластер

Опция, позволяет объединить все точки доступа в группу и конфигурировать группу как единую точку доступа.

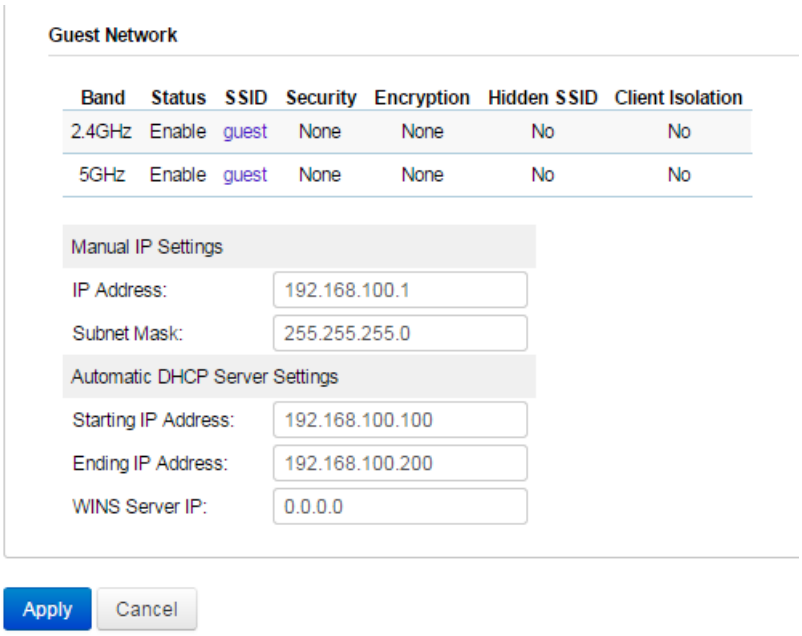
Guest Network

Думаю, что этот параметр в комментариях не нуждается. Но, если в двух словах, то это гостевая сеть. Ничем примечательным она не отличается. Все, что она может - это выдавать IP-адреса из заданного администратором пула. Жирный минус, как считают многие, заключается в том, что на ней нельзя развернуть веб-портал и авторизовать пользователей удобным для нас способом, как это можно было реализовать штатно в UniFi или MikroTik. Но Engenius поддерживает работу Vlan, поэтому ничто не мешает развернуть веб-портал на MikroTik в отдельном vlan.

Пример конфигурации на UniFi:



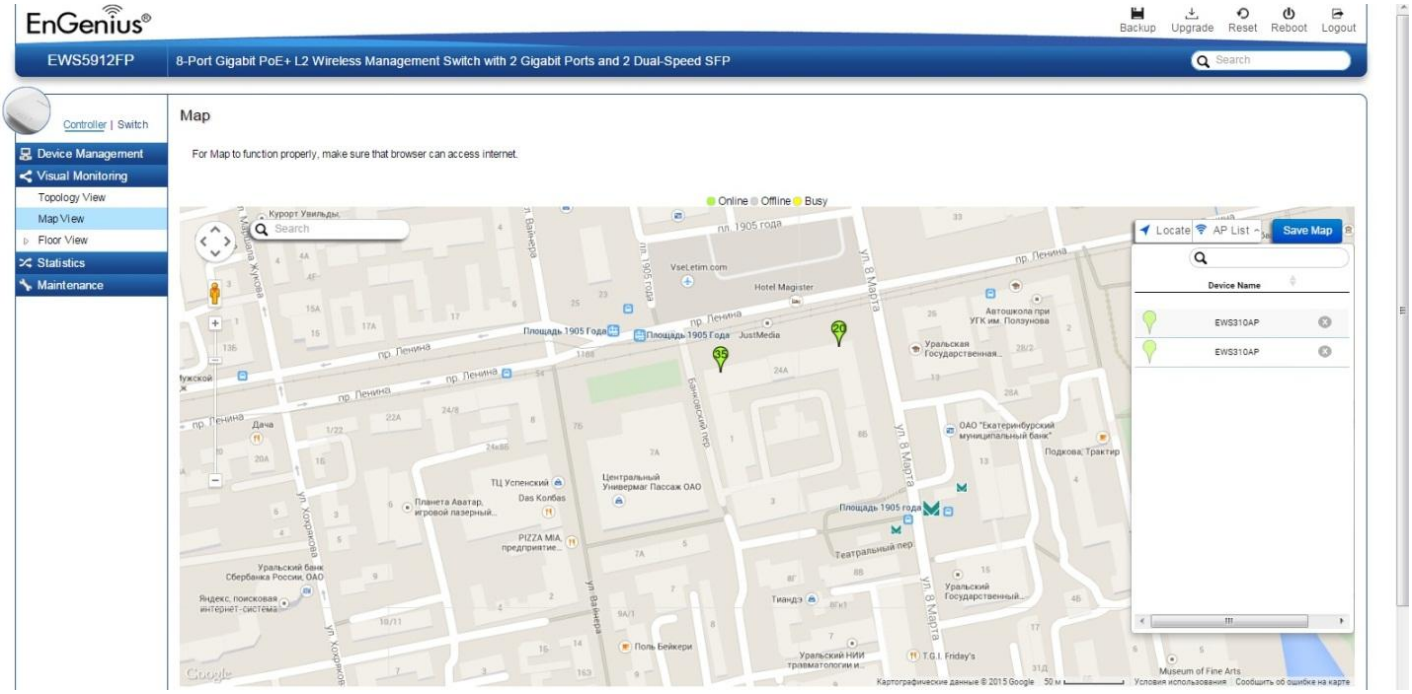
Пример конфигурации на Engenius:



Maps

Engenius, как и UniFi, поддерживает возможность загрузки своего плана местности. Кроме того, Engenius в штатном ПО имеет в себе карту от Google, на которой можно смело разместить свою

точку доступа.



Перейдем к вкусному

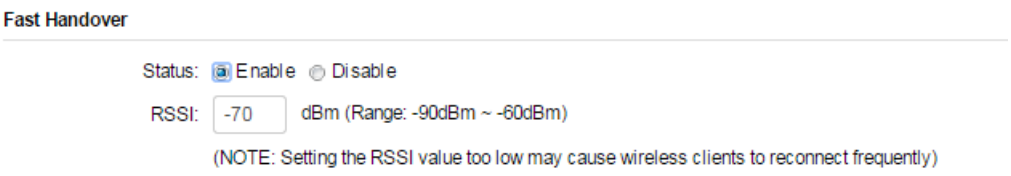
Весь штатный функционал, за исключением guest portal, схож с функционалом UniFi. Но как быть с роумингом? Как заставить пользователей максимально быстро мигрировать между точками доступа?

Для этого Engenius, в отличие от UniFi, где непонятно на основе чего происходит миграция пользователей между точками доступа, реализовал необходимый для этого функционал. А именно Fast Handover и Fast Roaming. Обе опции при совместной работе могут дать достаточно приличный роуминг в корпоративной сети.

Что такое роуминг? Чаще всего, роумингом называется процесс переподключения устройства к беспроводной сети при перемещении его в пространстве. Происходит это тогда, когда принимаемая мощность радиосигнала ослабевает с расстоянием до передатчика, в результате чего падает эффективная скорость передачи информации, а также растут канальные ошибки вплоть до обрыва беспроводного соединения. При наличии в радио-сети с одним именем (SSID) более чем одной точки доступа, перемещение мобильного абонента из зоны уверенной работы в пределах первой точки доступа в зону, где сигнал от второй точки доступа качественнее (выше мощность, больше отношение сигнал/шум) может произойти такое переподключение.

Рассмотрим обе опции отдельно.

Fast Handover. При включении данной опции для одной из точек доступа, администратору необходимо указать уровень сигнала, при котором устройство будет отключать пользователя, тем самым заставляя его переключиться к точке доступа с более уверенным уровнем сигнала. Без этой опции хорошего Wi-Fi-доступа, как и адекватного роуминга, не добиться, поскольку ВСЕГДА только клиентское устройство принимает решение об осуществлении переподключения. Fast Handover лишь помогает клиенту принять решение о переподключении в тот момент, когда уровень сигнала для клиента достаточно мал.



В UniFi подобной опции, как оговаривалось ранее, просто нет, поэтому не совсем понятно на основе чего происходит миграция пользователей между точками доступа.

Таким образом, для осуществления роуминга достаточно выделить для каждой точки доступа свою зону обслуживания по уровню сигнала. Для подобного теста необходимо, чтобы беспроводной клиент, подключенный к существующей сети, имел сигнал существенно худший, чем от другой точки

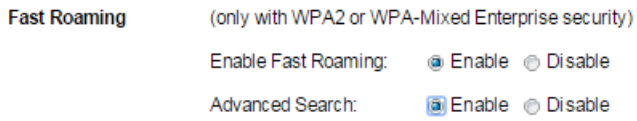
доступа.

Для переключения мобильного устройства можно либо отдаляться от одной точки доступа к другой, что в свою очередь повлечет за собой изменения уровня сигнала, либо просто накрыть точку доступа железной кастрюлей (если точки доступа лежат на столе) и наблюдать за тем как клиентский ноутбук автоматически переключается на точку доступа с более уверенным уровнем сигнала. При подобном тесте можно запустить ping, после чего, имитируя переключения между точками, наблюдать за потерями.

В среднем, при таком переключении обычно происходят незначительные потери – 1-2 пакета, при которых ssh-сессии или активные загрузки не прерываются.

Еще одна интересная опция, это **Fast Roaming**. Опция доступна при авторизации пользователей (WPA2 или WPA-Mixed Enterprise) через Radius(802.1x). Можно использовать FreeRADIUS-сервер или любой другой. В качестве базы пользователей можно использовать текстовый файл с паролями.

Как это работает? При работе с fast roaming, клиент, подключаясь к точке доступа, содержит в себе PMKSA-ключ-идентификатор беспроводной сети. Если на точках доступах, работающих в одном сегменте через единый контроллер, такой ключ закэширован, то во время переассоциации, точка доступа пропускает повторный этап авторизации, позволяя тем самым продолжить работу в сети без потери соединения. В отличие от выключенного Fast Roaming, когда устройство каждый раз проходит процесс авторизации с самого начала.

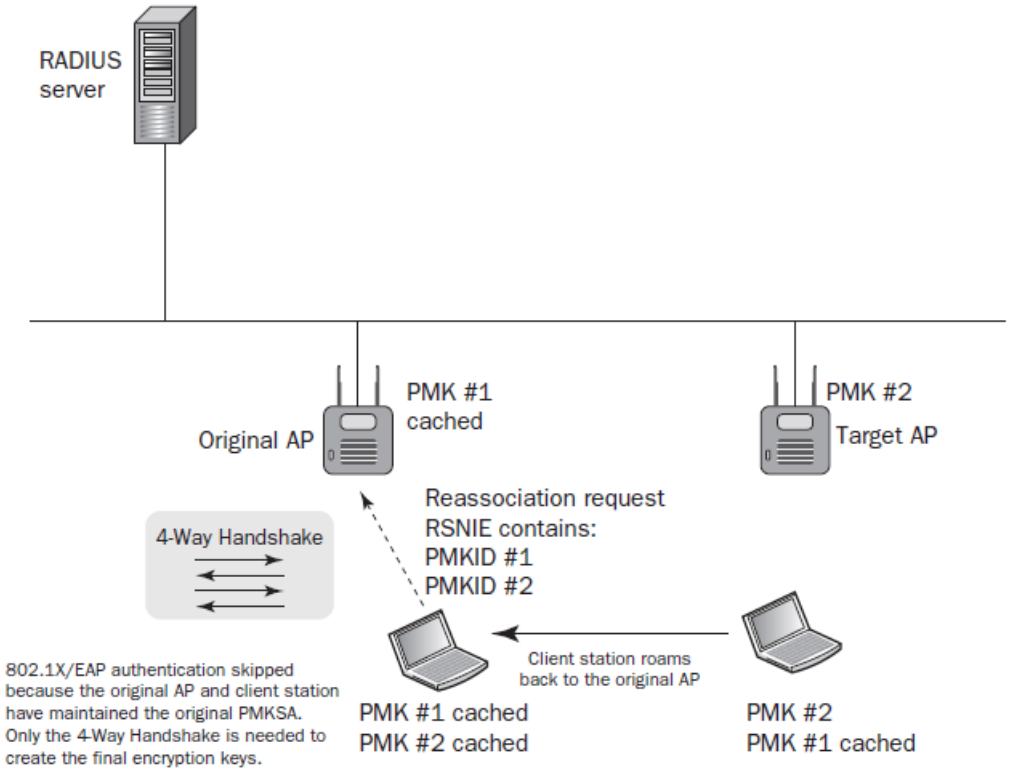


Для реализации роуминга на основе Fast Roaming нам необходимо авторизовывать пользователей на основе WPA2 Enterprise по механизму 802.1x. Поэтому для авторизации абонентов мы будем использовать FreeRADIUS-сервер. Ставится этот RADIUS в один пакет.

Для теста, одна из точек находится на некотором удалении, и сконфигурирована так, чтобы не "кикать" пользователей по уровню сигнала. Вторая точка "кикает" пользователей по уровню сигнала -60dBi и находится в непосредственной близости с беспроводным клиентом (Android Phone).

Для проверки работоспособности роуминга необходимо, чтобы клиент в какой-то период времени стал получать от точки доступа, с которой он ассоциирован, меньший сигнал, чем от другой точки с идентичными параметрами. Для того чтобы добиться этого эффекта, можно либо ходить от одной точки к другой и ждать когда уровень сигнала будет ниже чем -60 dBi, либо имитировать ситуацию, положив мобильное с Андроид, в металлическую банку (например, из-под чая). В результате, клиент соскакивал с ассоциированной ранее точки доступа на другую.

В момент, когда беспроводной клиент теряет соединение, он начинает искать более предпочтительную по уровню сигнала сеть, посылая Probe request-фрейм. После того, как клиент находит предпочтительную для себя сеть, происходит авторизация, реассоциация и обмен eapol по 802.1x.



Пример:

Packet	Source	Destination	BSSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol
79086	laptop	Ethernet B...	Eth...	*	11	73%	1,0	46	0:12:36,118860000	802.11 Probe Req
79088	ap2	laptop	ap2	*P+	11	23%	2,0	288	0:12:36,129231000	802.11 Probe Rsp
79089	ap2	laptop	ap2	*PC	11	23%	2,0	288	0:12:36,130727000	802.11 Probe Rsp
79090	ap2	laptop	ap2	*P+	11	26%	2,0	288	0:12:36,132107000	802.11 Probe Rsp
79091	ap1	laptop	ap1	*PC	11	63%	2,0	288	0:12:36,133729000	802.11 Probe Rsp
79092	laptop	ap2	ap2		11	100%	1,0	30	0:12:36,150371000	802.11 QoS Null Data
79094	linux64	laptop	ap2	W	11	31%	48,0	1082	0:12:36,150994000	802.11 Encrypted ...
79096	laptop	linux64	ap2	W	11	100%	54,0	1082	0:12:36,151501000	802.11 Encrypted ...
79101	linux64	laptop	ap2	W	11	37%	54,0	1082	0:12:36,235678000	802.11 Encrypted ...
79103	laptop	linux64	ap2	W	11	100%	54,0	1082	0:12:36,236252000	802.11 Encrypted ...
79120	laptop	ap2	ap2	+	11	100%	1,0	30	0:12:36,300363000	802.11 QoS Null Data
79122	laptop	ap1	ap1	*	11	100%	6,0	34	0:12:36,302632000	802.11 Auth
79124	ap1	laptop	ap1	*	11	63%	2,0	34	0:12:36,303095000	802.11 Auth
79126	laptop	ap1	ap1	*	11	100%	6,0	110	0:12:36,303753000	802.11 Reassoc Req
79128	ap1	laptop	ap1	*	11	57%	2,0	76	0:12:36,306223000	802.11 Reassoc Rsp
79130	ap1	laptop	ap1		11	57%	2,0	159	0:12:36,314358000	EAPOL-Key
79132	laptop	ap1	ap1		11	100%	6,0	177	0:12:36,315114000	EAPOL-Key
79134	ap1	laptop	ap1		11	63%	2,0	193	0:12:36,323120000	EAPOL-Key
79136	laptop	ap1	ap1		11	100%	6,0	137	0:12:36,324028000	EAPOL-Key
79138	laptop	Ethernet B...	ap1	W	11	100%	54,0	82	0:12:36,325749000	802.11 Encrypted ...
79140	laptop	Ethernet B...	ap1	W+	11	100%	48,0	82	0:12:36,326108000	802.11 Encrypted ...
79142	laptop	Ethernet B...	ap1	W	11	100%	54,0	386	0:12:36,329626000	802.11 Encrypted ...
79143	laptop	Ethernet B...	ap1	W+	11	100%	48,0	386	0:12:36,329866000	802.11 Encrypted ...
79147	laptop	Ethernet B...	ap1	W	11	100%	54,0	82	0:12:36,380197000	802.11 Encrypted ...
79149	laptop	Mcast IP I...	ap1	W	11	100%	54,0	110	0:12:36,380369000	802.11 Encrypted ...
79162	linux64	laptop	ap1	W	11	63%	12,0	1082	0:12:36,447569000	802.11 Encrypted ...
79165	laptop	Ethernet B...	ap1	W	11	63%	54,0	120	0:12:36,469578000	802.11 Encrypted ...
79166	laptop	Ethernet B...	ap1	W	11	63%	54,0	80	0:12:36,469946000	802.11 Encrypted ...

В запросе на реассоциацию содержится ключ PMK, который определяет идентификатор беспроводной сессии. Таким образом, точки работающие коллективно под управлением одного контроллера содержат таблицу с идентификаторами, и если во время повторной ассоциации для клиента найден такой ключ, то повторный этап авторизации на точке доступа игнорируется, и точка доступа сразу разрешает обмен данными.

Время реассоциации во время миграции между точками доступа, при работе с данными и трафиком, чувствительным к потерям (VoIP):

Data Roaming

№	Типы шифрования	Шифрование	Режим 802.11	Время миграции
1	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.022181
2	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.00645
3	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.005579
4	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.01626
5	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.005745

Voice Roaming				
№	Типы шифрования	Шифрование	Режим 802.11	Время миграции
1	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.006609
2	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.005683
3	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.005753
4	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.006424
5	WPA-Mixed Enterprise	Both(TKIP+AES)	802.11N	0.005627

Все данные получены с помощью утилиты Omnipeek Packet Sniffer.

Тесты по производительности Engenius и Unifi :

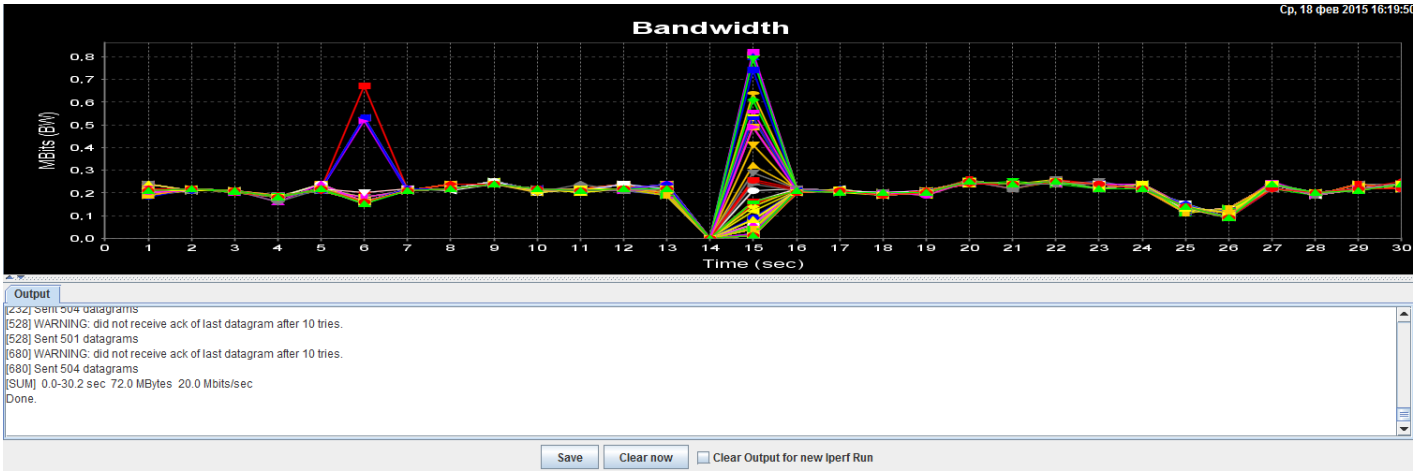
Client MAC Address	AP Device Name	AP MAC Address	Model Name	SSID	Band	RSSI
0C:8B:FD:58:E3:B4	EWS310AP	88:DC:96:1D:03:AE	EWS310AP	NAG	2.4GHz	-66

Тест в TCP 100 потоков при подключении в G-стандарте:



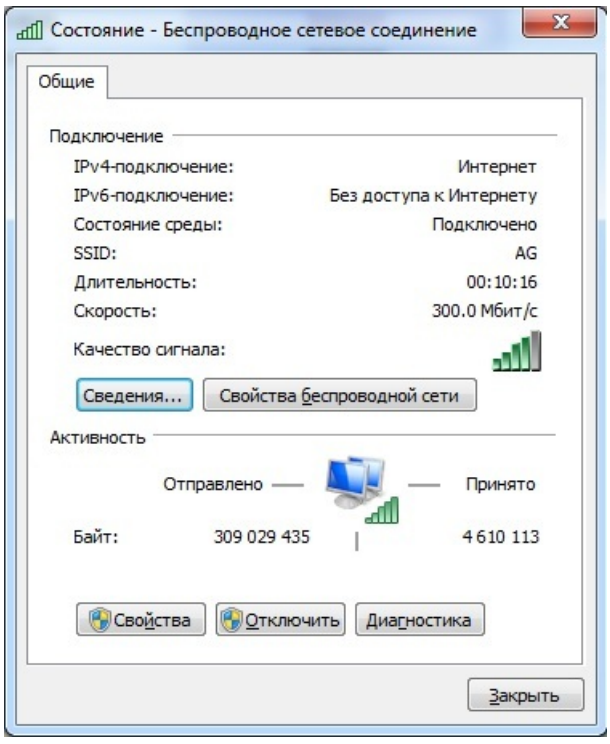
Итого: 17,9 Мбит/с FD.

Тест в UDP 100 потоков при подключении в G-стандарте:

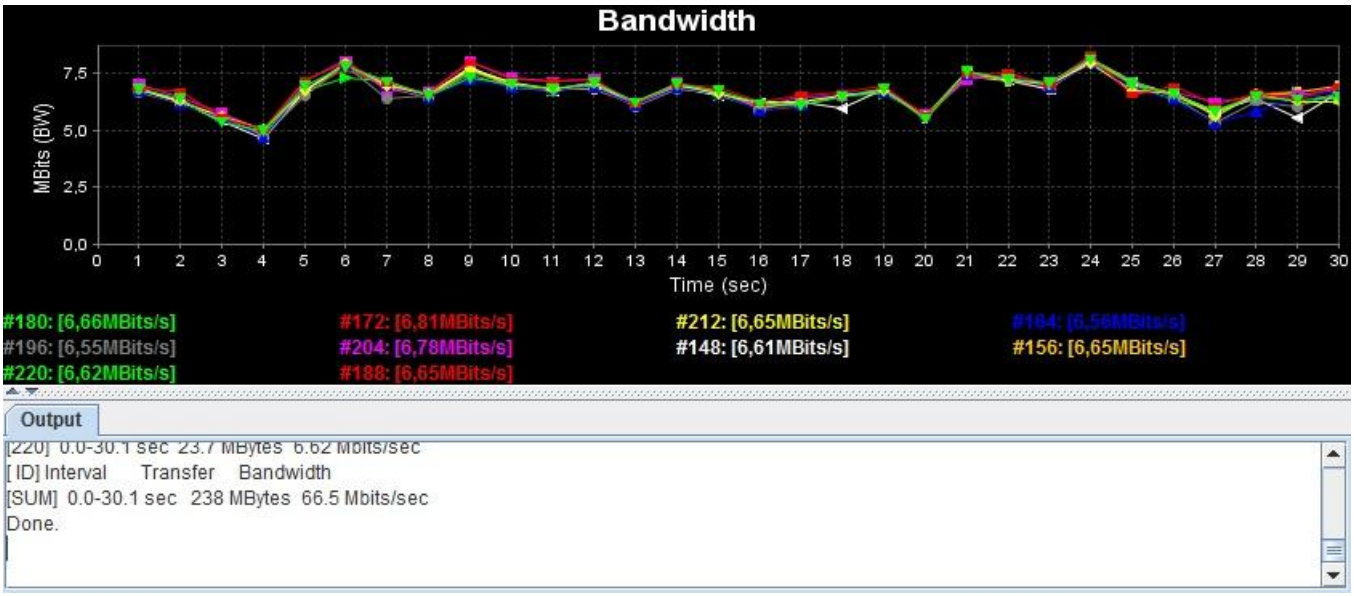


Итого: 20 Мбит/с FD.

Можно считать, что это потолок для 802.11g-стандарта. Посмотрим, как поведет себя точка доступа при аналогичном тесте для стандарта 802.11N

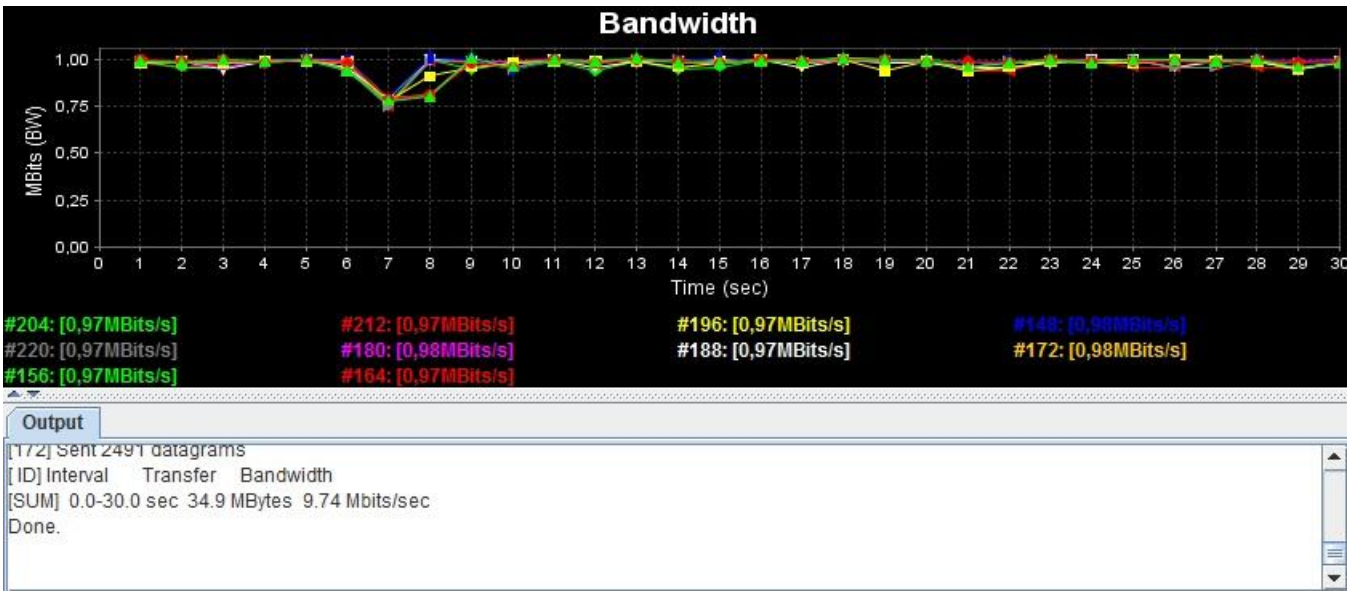


1. TCP в 10 потоков:



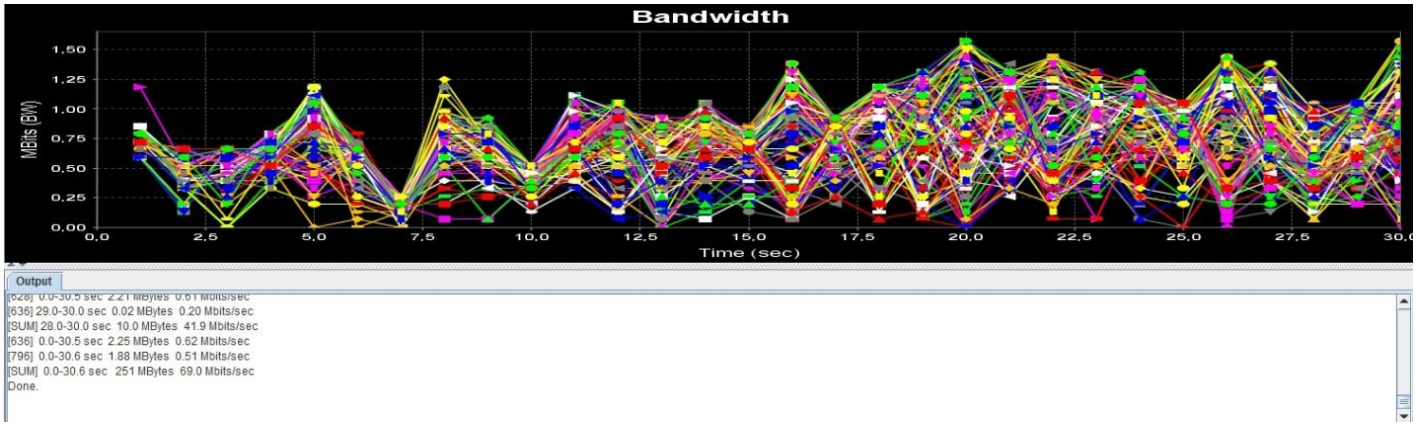
Итого: 66-70 Мбит/с.

1. UDP в 10 потоков:



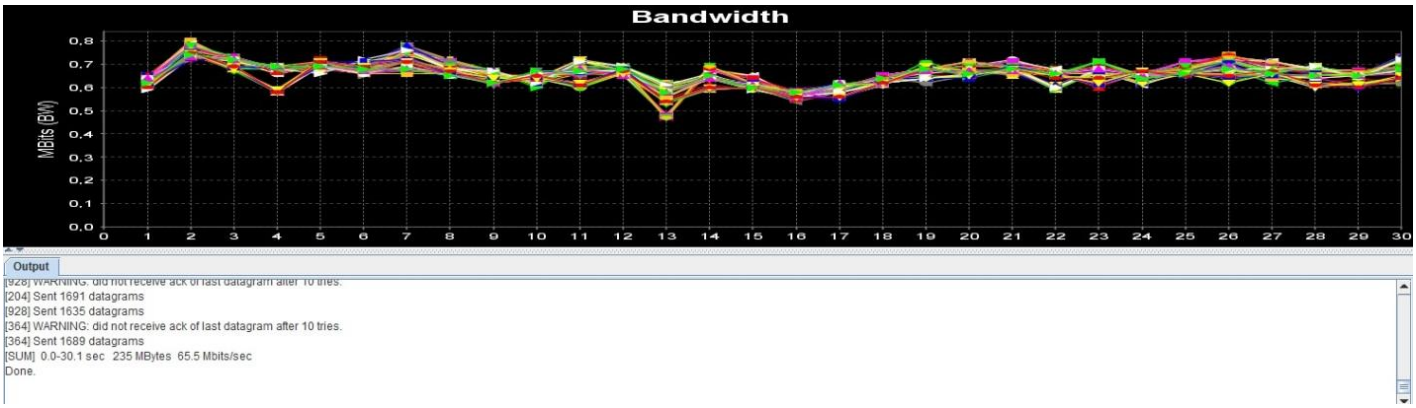
Картина немного иная. При UDP больше 10Мбит/с, точка доступа не справляется. На графике видно, что при продолжительности генерации трафика в течение 30 с, поток стабильный, без потерь и серьезных провалов. Скорее всего, софтовый недодел.

1. TCP в 100 потоков:



Всего 70Мбит/с, что равно ~140 Мбит/с из заявленных 300 Мбит/с. Не очень хороший результат для N-стандарта.

1. Udp в 100 потоков:



UDP на "N" показал сравнительно лучший результат, но все равно нет заявленных скоростей. Напомню, что тестируемые точки доступа работают в режиме бриджа и выполняют функции NAT. Фильтрации и прочие возможности - недоступны.

Немного о Unifi

- TCP в 10 потоков - ~52 - 58 Мбит/с.
- UDP в 10 потоков - ~10 Мбит/с.
- TCP в 100 потоков - ~30-35 Мбит/с.
- UDP в 100 потоков - ~49 Мбит/с.

В ходе неоднократного тестирования были выбраны средние показатели для обоих вендоров. На момент тестирования, ПО контроллеров и точек доступа было обновлено до последних версий.

Резюме

- Домашние маршрутизаторы, работающие независимо друг от друга, и независимо от единого SSID, заставляют пользователя тянуться за ними столько, насколько хватает сигнала. Как следствие, наблюдаются задержки в передаче полезного трафика, потери и прочие проблемы вплоть до разрывов соединения. Кроме того, большинство точек доступа/маршрутизаторов заставляют пользователя проходить полный цикл авторизации при миграции между станциями.

- Решение на базе UniFi хоть и имеет штатный контроллер, но способен он лишь выполнять централизованную настройку точек доступа. Функционала для решения конкретных задач по роумингу у него нет, или он скрыт от глаз администратора. В Engenius функционал нацеленный на решение вопроса касаемо миграции пользователей решен с помощью, рассмотренных ранее, опций Fast Handover и Fast Roaming’ом.
- Отсутствие у Engenius guest portal. Было бы весьма неплохо иметь в одной "железке" штатный веб для гостей, систему генерации билетиков с разовыми паролями для гостиничных или кафе сервисов. По информации от вендора, в перспективе такой функционал будет реализован.

Самое интересное, что все то, что есть интересного в UniFi, и нет в Engenius, разработчики обещают доработать и добавить в первом-втором квартале 2015 года

> >And for your question regarding the features:
>
> - Guest portal (web, authorization, a voucher system for the guest network) ➔ Basic captive portal with internal user database will be available in Q3 2015. No plans for voucher system yet.
>
> - The ability to view user information (hostname, ip addr, uptime, tx / rx rate) ➔ March/E 2015 fw will support
>
> - Ability to force disable or disconnect the connected users. ➔ March/E 2015 fw will support

А значит, от Engenius стоит подождать нового ПО.

О финансах

Безусловно, одним из важных критериев при принятии решения является цена. Мы постарались сравнить стоимость предложения от EnGenius с оборудованием других вендоров для решения аналогичных задач. Большой популярностью в сегменте экономичных решений для построения корпоративных беспроводных решений является система UniFi от Ubiquiti. Данное оборудование продается по открытым фиксированным ценам.

Контроллер является условно бесплатным – в виде ПО скачивается с сайта Ubnt.com и разворачивается на сервере и на стороне клиента (надо учитывать тот факт, что сервер также имеет стоимость, как приобретения, так и владения/обслуживания).

Также, не стоит забывать о серии Cisco Aironet, которые можно приобрести в НАГе со статусом б/у в состоянии "like new". В этом случае точка доступа обойдется в ценник $115-270, а контроллер на 50 AP - $380.

Ценообразование других вендоров не является столь прозрачным, поскольку основано на проектной политике и наличия в фиксированном виде разве что уровня GPL. Не стал исключением и EnGenius. Сравнивая уровни цен, можно сказать, что точка доступа EnGenius в зависимости от характеристик будет стоить $200 - $500, что заметно дороже аналогичного решения от Ubiquiti. Однако компенсируется эта стоимость тем, что для аналогичной емкости требуется меньшее количество AP, в силу большего реального количества поддерживаемых активных клиентов. Сравнивая с решениями таких вендоров, как Extreme Networks, Juniper Networks, следует отметить, что цена на базовую dual band-модель с одним радиомодулем незначительно разнится. Если же говорить про более продвинутые модели, такие как 3t3r-радио на каждой частоте, уличное исполнение и т.д., разница в цене составляет 100% и более. Стоимость аппаратного контроллера по GPL от Extreme Networks, Juniper Networks также в 2-3 раза дороже варианта аналогичной емкости от EnGenius.