

Обзор решений для организации беспроводных сетей многопользовательского доступа, часть 4 - Juniper Networks

Введение

Данной статьей мы продолжаем публикацию серии материалов с обзором беспроводных решений, использующих "тонкие" точки доступа для многопользовательского доступа, представленных на мировом телекоммуникационном рынке. Предыдущие материалы, посвященные оборудованию [Extricom](#) и [Aruba](#), [Extreme Networks](#) были по достоинству оценены читателями. В этой же статье речь пойдет о решении, предлагаемом Juniper Networks.

Сразу оговорюсь, что изложенный ниже материал посвящен оборудованию, которое можно приобрести у [нас в магазине](#).

Линейка беспроводного оборудования от компании Juniper Networks представлена, как и в предыдущих случаях, двумя типами устройств: WLAN-коммутаторами и точками доступа. Точки доступа Juniper Networks являются устройствами полностью зависимыми от контроллера. Возможности подключения к точке через консольный порт для настройки ее в режиме отдельно стоящего решения, отсутствует, ввиду отсутствия самого консольного порта. Дело в том, что компания Juniper Networks считает, что консольный порт на точке - это дырка в безопасности всего решения. Ведь без возможности локальной настройки точка годится только для сдачи в металлолом, а это снижает риски кражи устройства.

Так же отсутствует возможность использовать точку в качестве виртуального контроллера, как это было реализовано в решении [Extreme Networks](#). В случае, если точка доступа во время работы "теряет" связь с контроллером, Wi-Fi-сеть продолжает функционировать в штатном режиме, хоть и без возможности авторизации новых пользователей.

Контроллер точек доступа представляет собой коммутатор с расширенными возможностями. Непосредственно на контроллере имеется встроенная система управления, мониторинга и настройки. Также, имеется внешняя система управления мониторинга и настройки - Ring Master с расширенным функционалом.

Далее будут более детально рассмотрены характеристики устройств.

WLAN-коммутаторы

WLAN-коммутаторы Juniper Networks представляют собой высокопроизводительное оборудование стандартов 802.11a/b/g/n, предназначенное для организации большого количества сервисов беспроводного доступа. С его помощью производится конфигурирование точек доступа, а также значительное наращивание возможностей беспроводной сети.

Линейка WLAN-коммутаторов Juniper Networks представлена следующими моделями:

[WLC2](#) - самая младшая модель в линейке, поддерживает 4 точки доступа в базовой лицензии, без возможности расширения. Имеет два порта 10/100 BASE-T, один из которых с поддержкой PoE. Модель снимается с производства 30 декабря 2013 года.

[WLC8](#) - модель, которая поддерживает подключение до 12 точек доступа, без возможности расширения, имеет 8 портов 100BASE-T, поддержка PoE на 6 портах.

[WLC100](#) - новинка среди модельного ряда, имеет 4 порта 1000BASE-T, поддерживает 4 точки доступа в базовой лицензии, имеет возможность лицензионного расширения до 32 точек доступа, поддержка PoE на двух портах.

[WLC800/880](#) - две практически одинаковые модели, различаются только максимальным числом подключаемых точек доступа 128/256. Поддерживают 16 точек доступа в базовой лицензии. Имеют по 4 порта 1000BASE-FX SFP, а также 4 порта 1000 BASE-T. Модель WLC880 имеет возможность использования защиты трафика по технологии IPsec при подключении точек доступа.

[WLC2800](#) - самый мощный контроллер, представленный в модельном ряде. Имеет "на борту" порты 10G BASE-FX XFP в количестве двух штук. А также 8 портов 1000BASE-FX SFP и 8 портов 1000 BASE-T. Поддерживает 64 точки доступа в базовой лицензии, и имеет возможность лицензионного расширения до 512 точек доступа.

vWLC - софтовое решение, виртуальный контроллер для установки на виртуальную машину vmWare ESX. Поддерживает 4 точки доступа в базовой лицензии, а также имеет возможность лицензионного расширения до 256 точек доступа. Поддерживает функционал полноценного контроллера WLC.

Все контроллеры Juniper Networks поддерживают технологию Local Switching, которая позволяет исключить контроллер из пути прохождения абонентского трафика, что обеспечивает использование широких каналов сети связи для работы сети Wi-Fi.

Точки доступа

Линейка беспроводных точек доступа представлена следующими моделями:

[WLA321](#) - точка доступа с интегрированными/внешними антеннами и одним радиомодулем, работающими в диапазоне 2.4ГГц либо 5 ГГц, поддерживает стандарты 802.11a/b/g/n. Радиомодуль обладает антенной с конфигурацией 2x2 MiMo.

[WLA322](#) точка доступа с интегрированными/внешними антеннами и двумя радиомодулями, работающими в диапазоне 2.4ГГц, 5 ГГц, поддерживает стандарты 802.11a/b/g/n. Радиомодуль обладает антенной с конфигурацией 2x2 MiMo.

[WLA522\(E\)](#) - точка доступа с интегрированными/внешними антеннами и двумя радиомодулями, работающими в диапазоне 2.4ГГц, 5 ГГц, поддерживает стандарты 802.11a/b/g/n. Радиомодули обладают антенной с конфигурацией 2x2 MiMo. Поддерживает работу в режиме 2:2SS

[WLA532\(E\)](#) - точка доступа с интегрированными/внешними антеннами и двумя радиомодулями, работающими в диапазоне 2.4ГГц, 5 ГГц, поддерживает стандарты 802.11a/b/g/n. Радиомодули обладают антенной с конфигурацией 3x3 MiMo. Поддерживает работу в режиме 3:3SS. Точка является решением high end, и обеспечивает максимальную производительность.

Мы видим, что модельный ряд устройств не слишком разнообразен, и не представляет для конечного пользователя широты выбора решения.

Обзор устройств

Для тестирования нам достался комплект оборудования, состоящий из коммутатора WLC2 (с предустановленной лицензией на подключение 4 точек доступа), 2 точек доступа: WLA532, ПО RingMaster с предустановленной демо-лицензией на 90 дней, ПО SmartPast guest Access, а так же vWLC.

В комплектацию коммутатора входит:

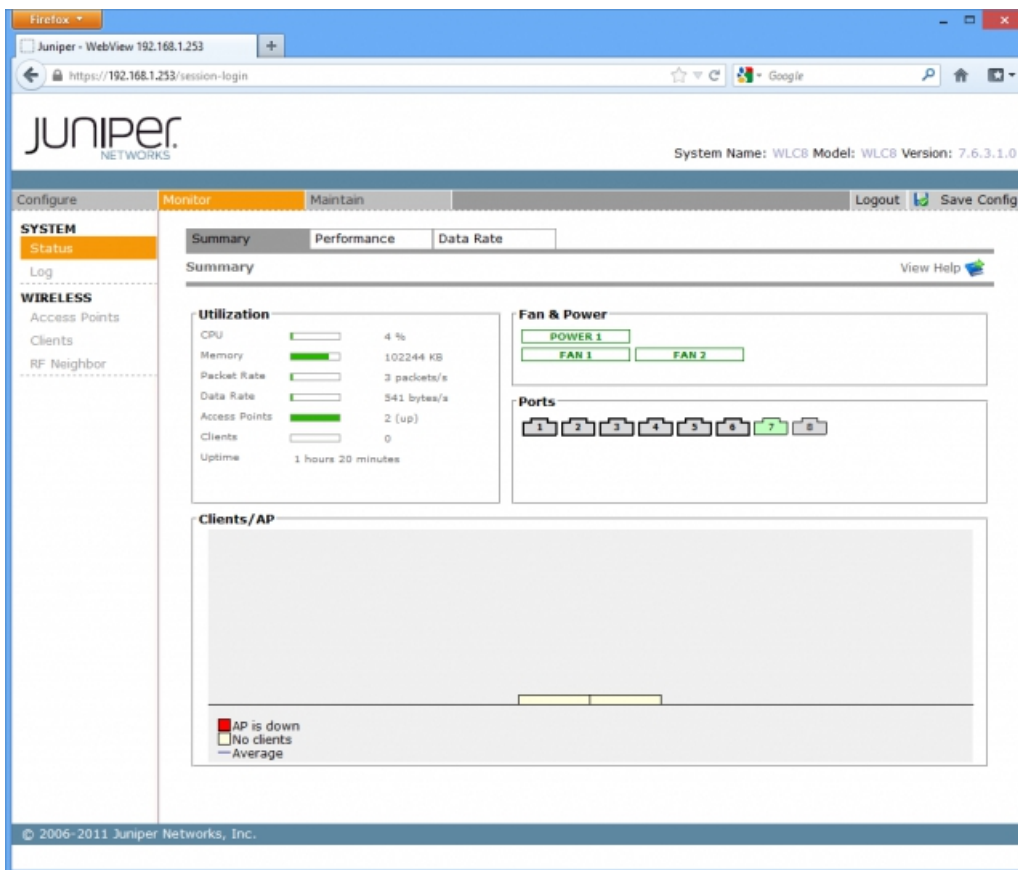
- Собственно, сам коммутатор;
- Шнур питания;
- Консольный кабель;
- Диск с документацией.

Точки доступа поставляются с элементом крепления точки доступа к стене или потолку.

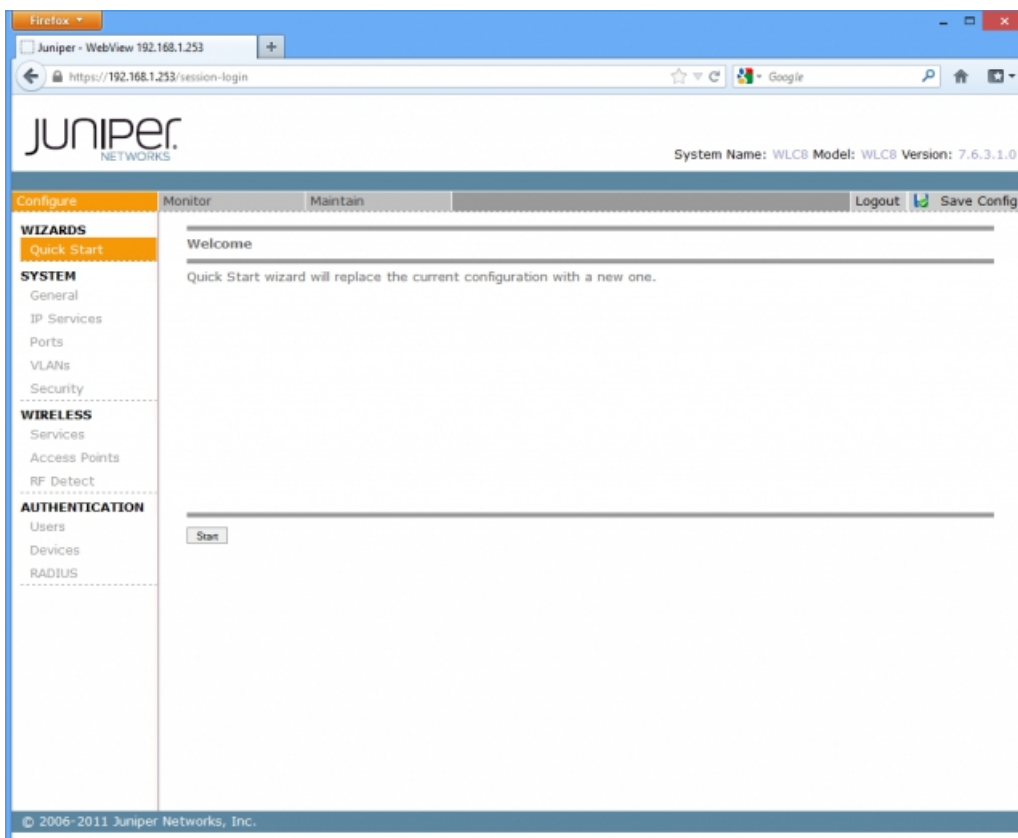
Базовая настройка комплекта

После подключения к сети, контроллер заморгал лампочками и благополучно загрузился. Базовая настройка производится с консоли. Для особенно ленивых существует команда: quickstart, которая запускает мастер базовой настройки, позволяющий настроить такие параметры как: основной адрес управления, радиочастотный план, задать время и имя устройства, а также, если очень необходимо, настроить SSID. После прохождения мастера, можно подключиться к контроллеру и посмотреть на его веб-интерфейс.

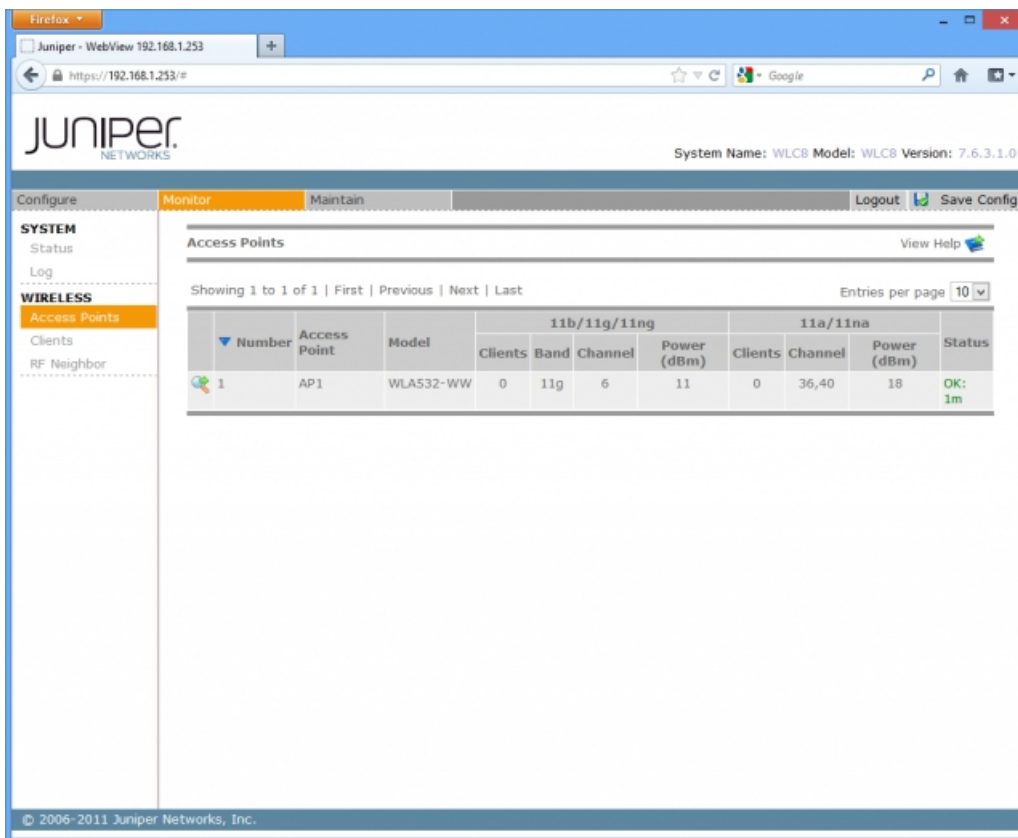
Веб-интерфейс позволяет осуществить базовые настройки, мониторинг, и обслуживание комплекта беспроводных устройств от Juniper Networks.



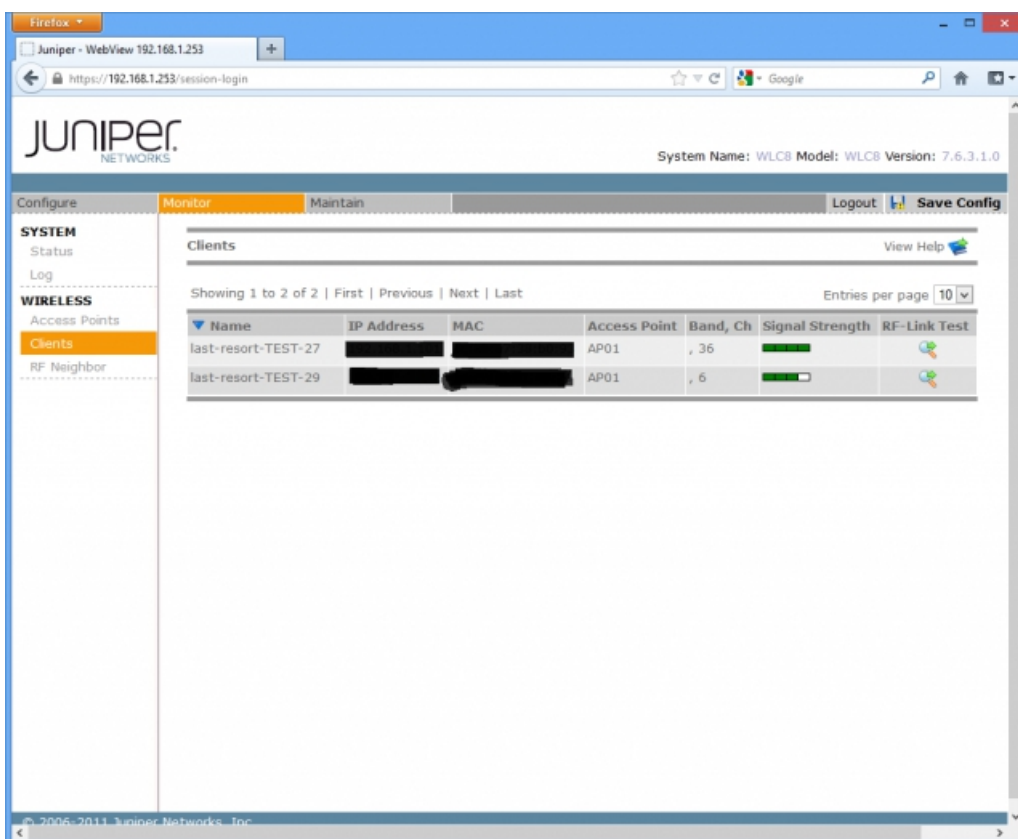
Режим мониторинга позволяет посмотреть базовую информацию о системе.



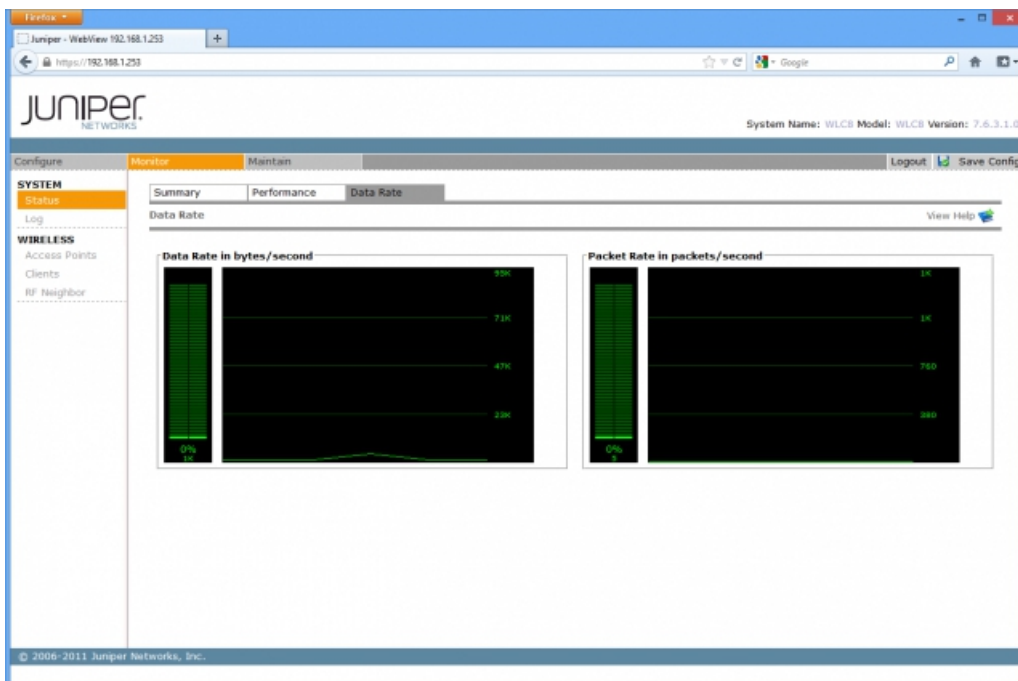
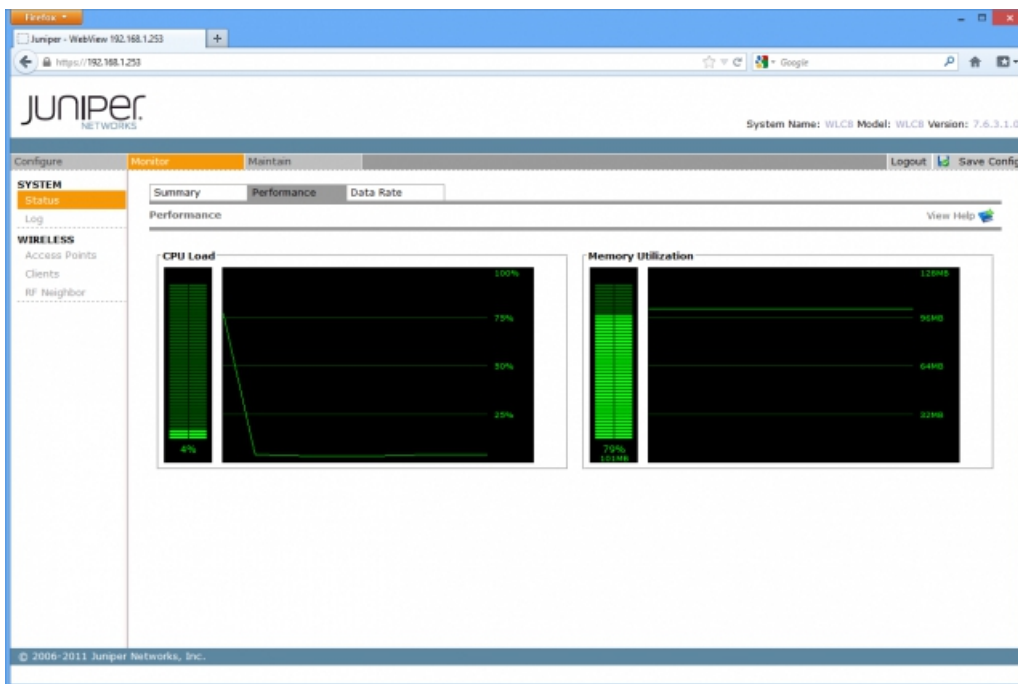
Окно настройки, так же как и консоль, позволяет нам запустить quickstart, и повторить все настройки заново. Можно настроить порты и номера Vlan для выбранного SSID, а также сам SSID, и произвести настройку точек доступа. В принципе, данного функционала хватает на то, чтобы заставить систему работать. А настройка не требует серьезных умственных усилий.



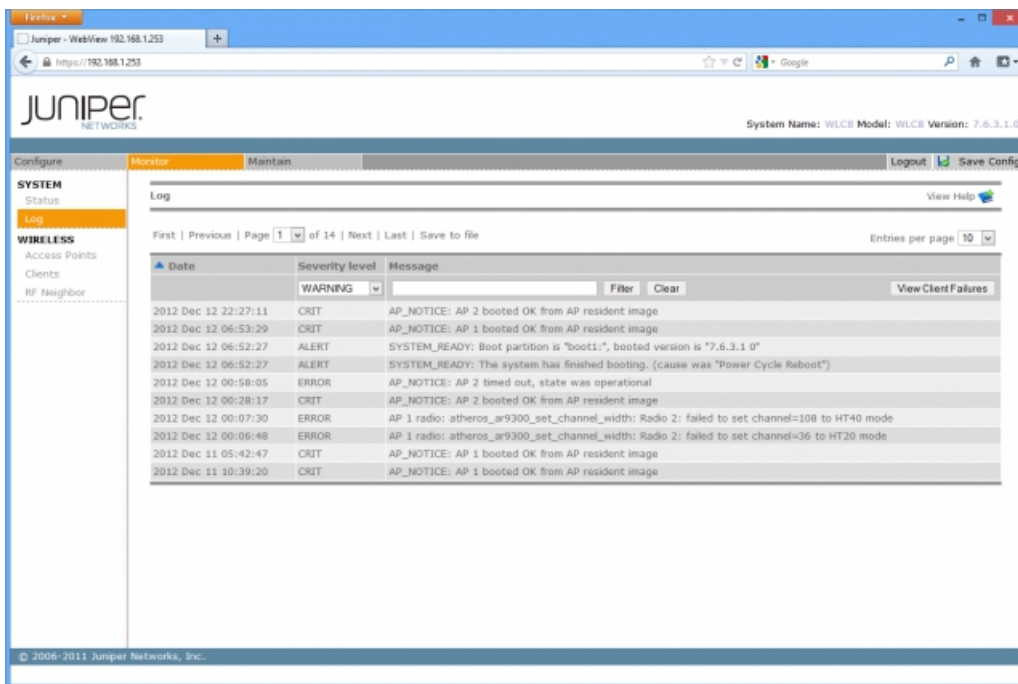
Из меню мониторинга мы можем не только посмотреть основное состояние системы, но и проверить состояние точек доступа, как и подключенных клиентов.



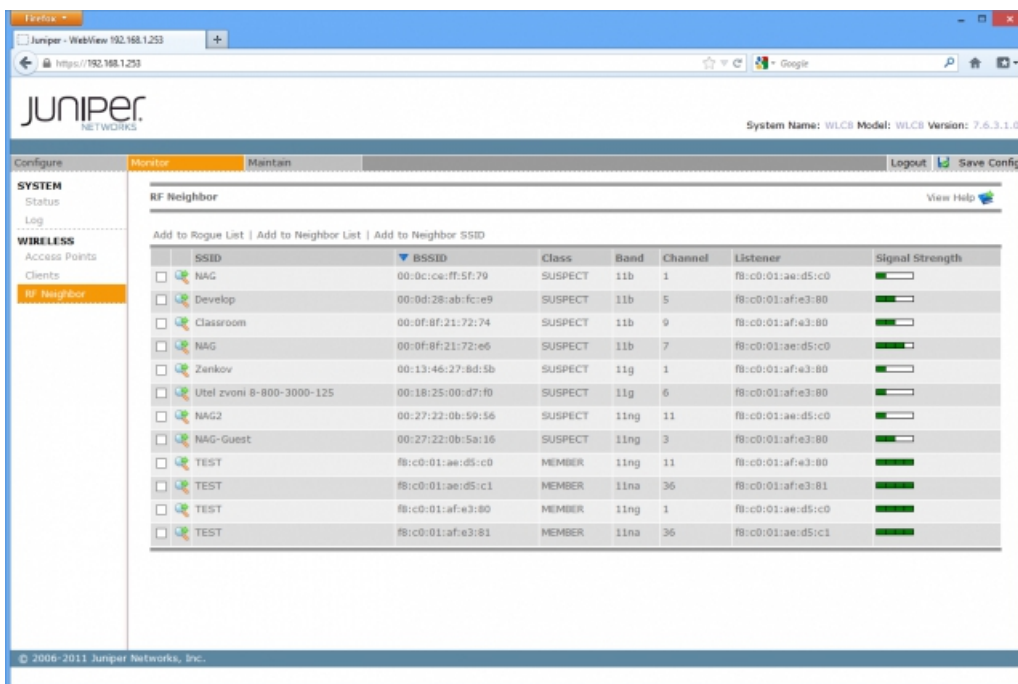
Также, можно посмотреть общую загруженность системы, и пропускную способность.



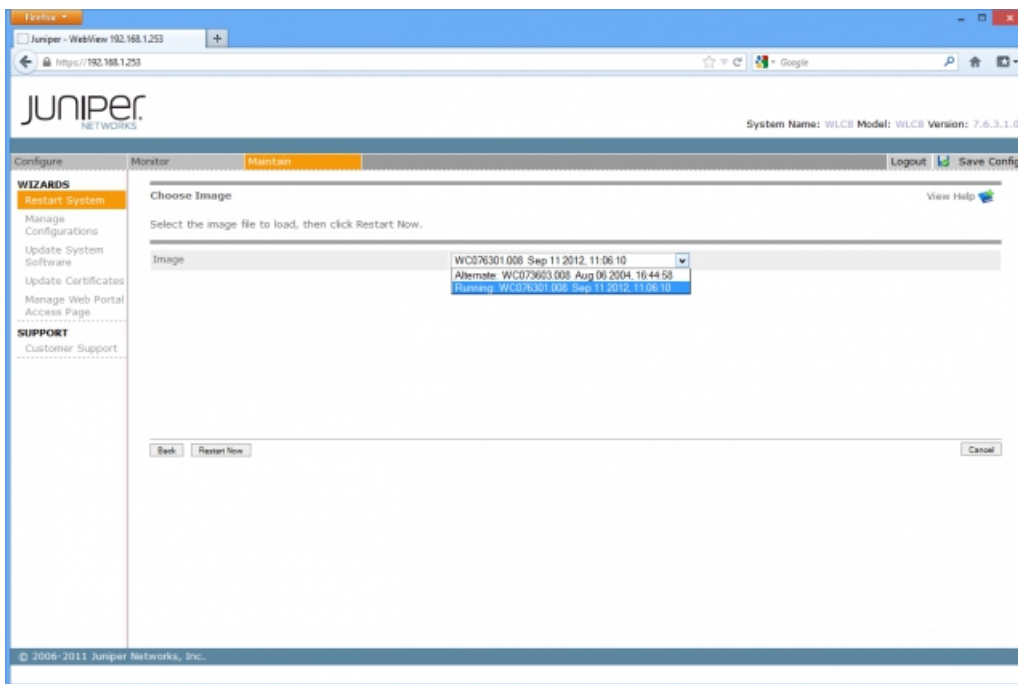
Основные логи работы устройств доступны в меню Log.



Кроме того, можно просмотреть списки других SSID и сетей, отметить их как враждебные, что бы предпринять контр-меры.



Ну и, конечно же, провести апгрейд программного обеспечения, а также посмотреть список установленных релизов.

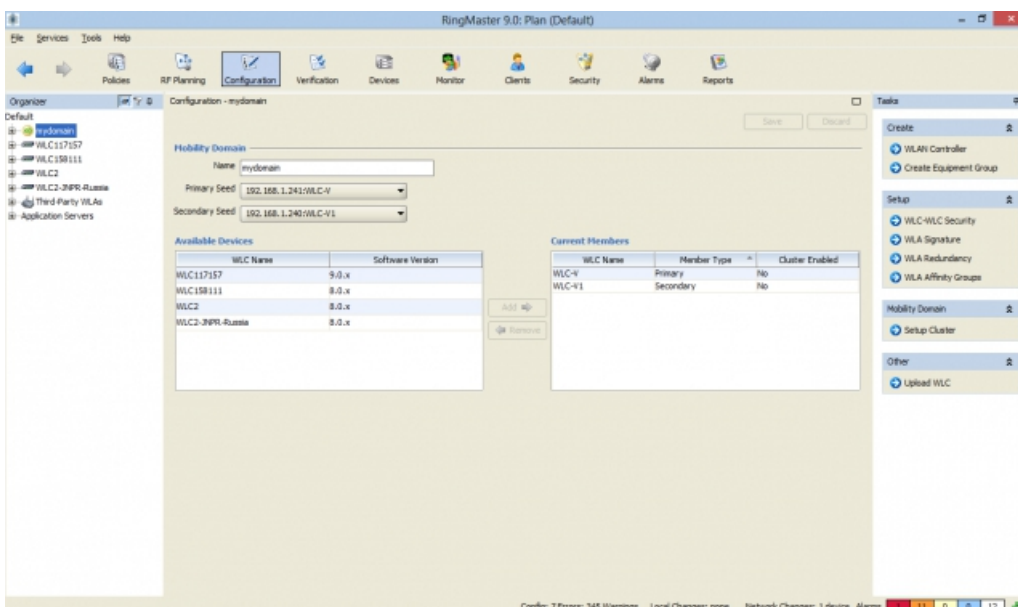


Вот в принципе и все, что позволяет делать решение "из коробки", установленное напрямую на контроллере. Мы же, для осуществления настройки, воспользовались расширенными возможностями системы управления RingMaster.

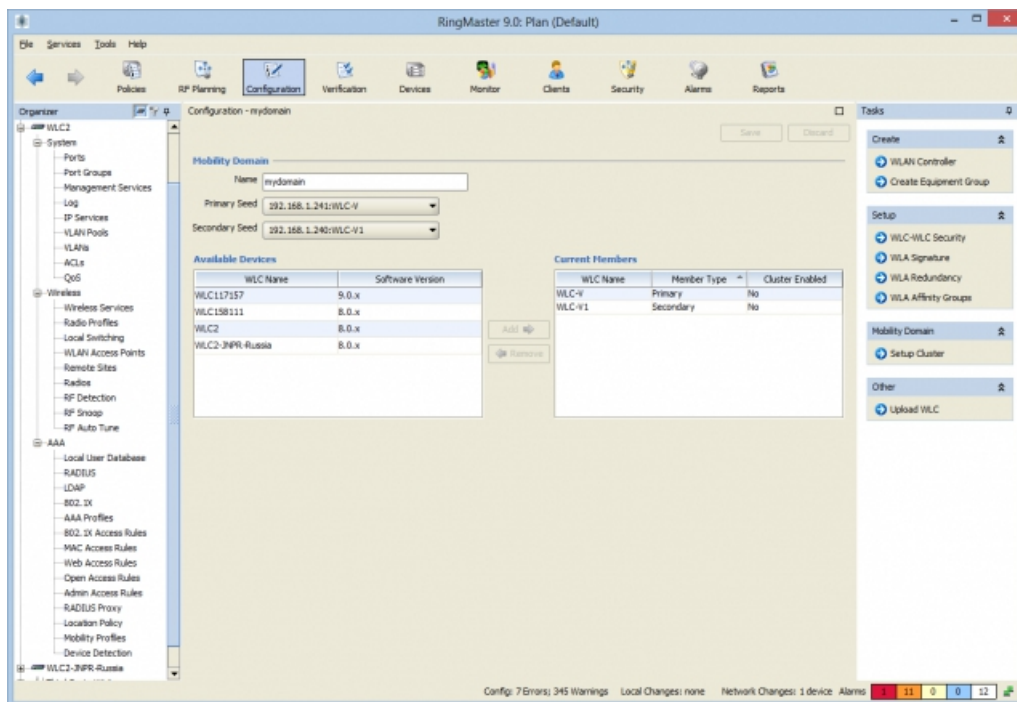
ПО Ringmaster обладает более широким функционалом по сравнению с решением из коробки. Оно устанавливается на отдельно стоящий сервер, и лицензируется дополнительно, в зависимости от необходимых для работы сервисов.

Мы для работы воспользовались локальной установкой на рабочую станцию. После установки серверной/клиентской части, ПО потребовало лицензию, без которой работа с ПО не является возможной.

После установки лицензии, RingMaster запустился и приветствовал нас окном конфигурирования оборудования.



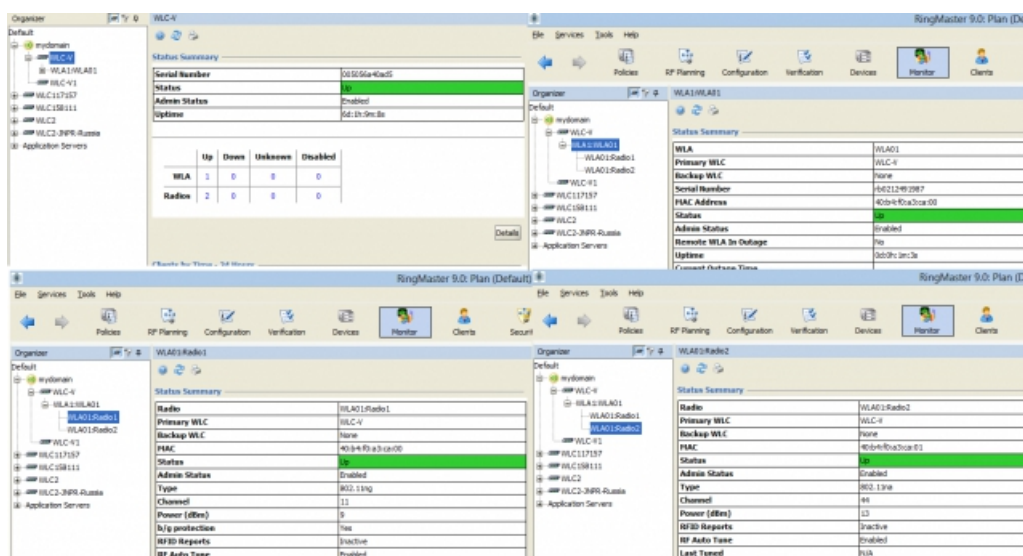
Для того чтобы получить доступ к настройкам нашего контроллера, необходимо сначала подключить его к системе управления. Для этого надо выбрать пункт Upload WLC. После прохождения несложной процедуры, мы увидим, что контроллер появился в левой части программы, откуда можно непосредственно приступить к настройкам.



Можно заметить, что настройка с помощью системы RingMaster обладает более широкими возможностями, чем настройка через веб-интерфейс контроллера.

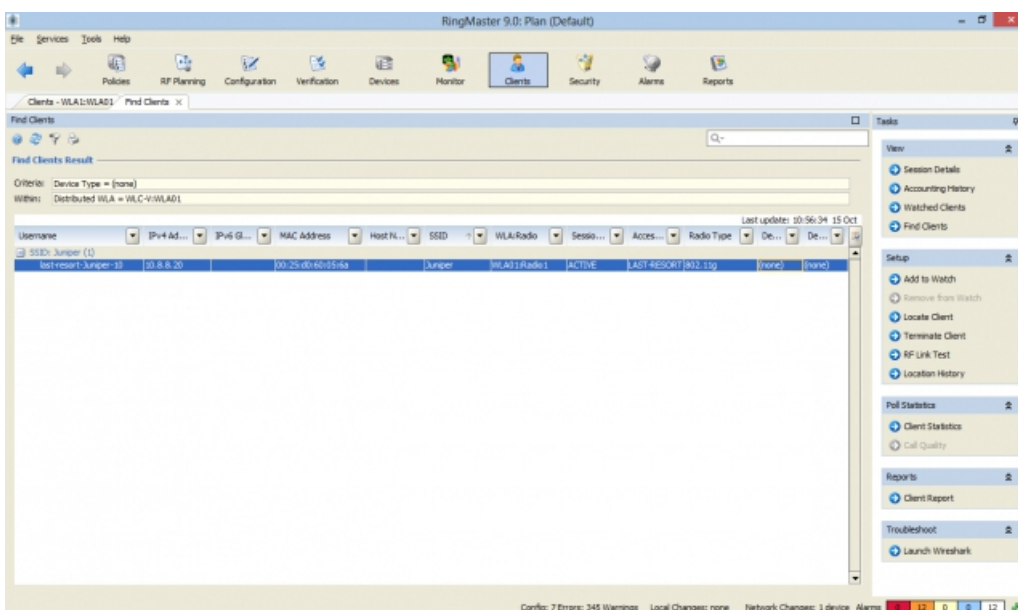
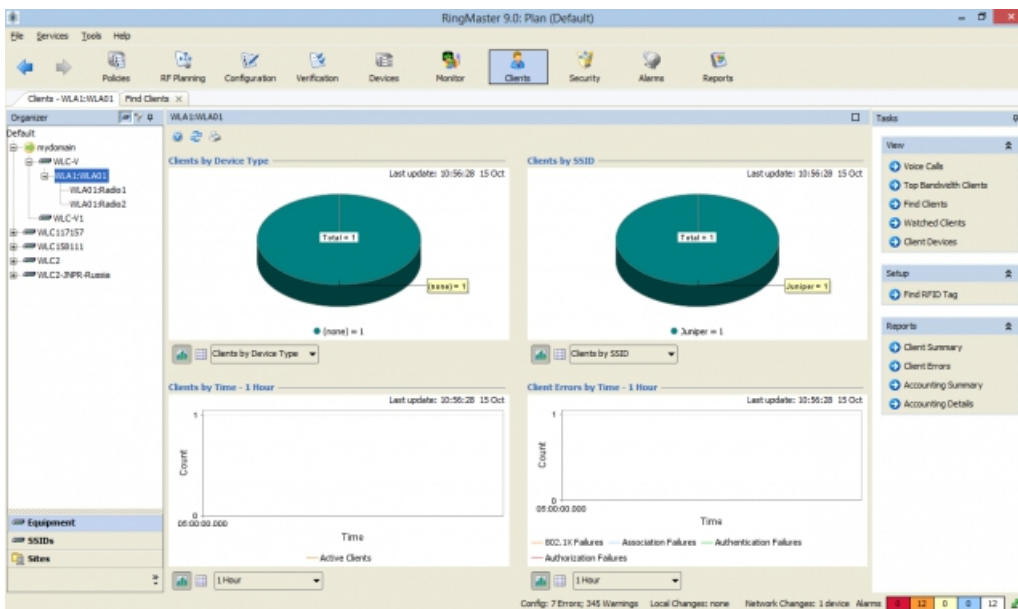
После изменения каких-либо параметров оборудования, необходимо нажимать кнопку Deploy. После этого произойдет проверка заданной конфигурации, и применение ее на оборудовании. Система Ring Master позволяет подключать любое число контроллеров, для осуществления их настройки и управления, а также доступное в рамках данной лицензии количество точек доступа.

После осуществления настроек оборудования и подключения точек доступа, можно перейти в меню мониторинга, где посмотреть состояние работающего комплекта.



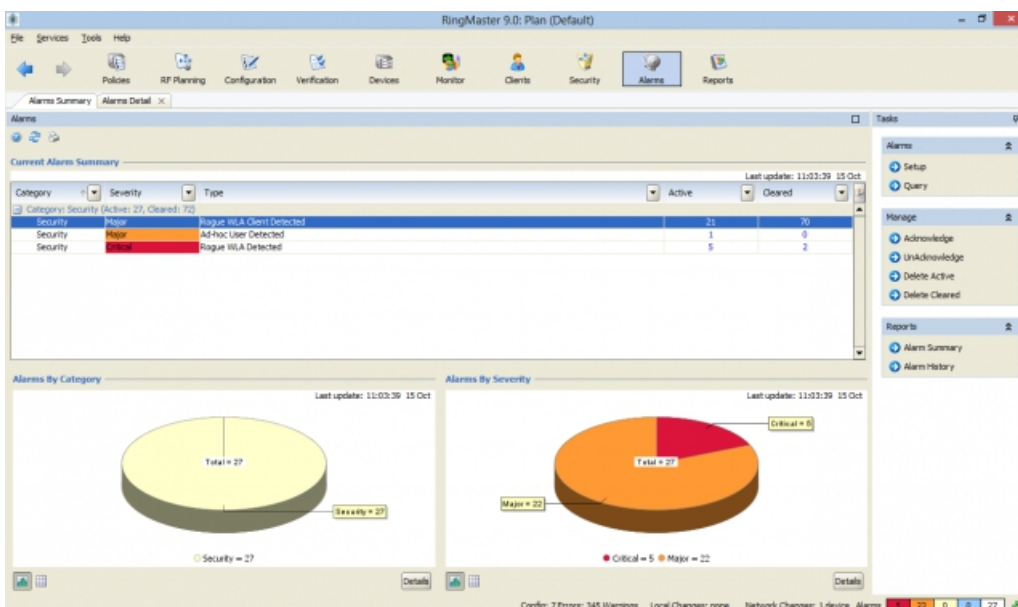
Мы видим, что наш контроллер, точка доступа, и даже оба радио на точке доступа находятся в состоянии UP, т.е. работают.

Окно мониторинга позволяет оценить количество аварий в данный момент, средний трафик, проходящий через оборудование, и количество клиентов, подключенных к нашей сети. С помощью навигации можно переходить в более детальные разделы. Например, в раздел Clients:



Здесь мы можем увидеть как суммарное количество подключенных клиентов, так и детальную информацию по каждому клиенту.

Окно обнаружения проблем на сети позволяет просмотреть суммарное количество проблем, а также детальную информацию по той или иной проблеме.



RingMaster 9.0: Plan (Default)

File Services Tools Help

Polices RF Planning Configuration Verification Devices Monitor Clients Security **Alarms** Reports

Alarms Summary Alarms Detail x

Queries: Category = Security and Severity = Major and State = Active and Source = WLC-V

Updated: [v] Severity: [v] Category: [v] Description: [v] Object: [v] State: [v]

Time Occurred	Severity	Category	Description	Object	State
11:01:53 15 Oct	Major	Security	A Client with MAC: f4b7a2ed-33-c9, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: c4137fe31a-ae04, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: 4b2c7f402-2e68, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: 9c3a70-23-33-79, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: 70f2f55a5-43-96, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: c2d3294-47-fb8b, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: c252a1f50a7-99, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: 0c0e2af53c7a-56, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: 00255bc72-aa64, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: 84a6c89b33-04, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active
11:01:53 15 Oct	Major	Security	A Client with MAC: 74de12be1-c0-30, SSID: (none), is communicating with an unauthorized WLA	WLC-V	Active

Updated: Last Week (11) 09:30:39 11 Oct

Details Events

Time Occurred	Description	Event State	No. of Listeners	SSID
11:23:04 04 Oct	A Client with MAC: f4b7a2ed-33-c9, SSID: (none), is communicating with an unauthorized WLA	Active		(none)
17:17:19 09 Oct	A Client with MAC: f4b7a2ed-33-c9, SSID: (none), is communicating with an unauthorized WLA	Active	1	(none)
11:01:53 15 Oct	A Client with MAC: f4b7a2ed-33-c9, SSID: (none), is communicating with an unauthorized WLA	Active	1	(none)

Config: 7 Errors; 345 Warnings Local Changes: none Network Changes: 1 device Alarms 1 22 0 0 27

Tasks: 0

Alarms

- Event Details
- Setup
- Query

Manage

- Acknowledge
- Unacknowledge
- Delete

Related Tasks

- Add to Black List
- Locate

Раздел Безопасность, позволяет осуществить обзор доступных беспроводных сетей и устройств, классифицировать их в группы. Группы могут быть вражеские и разрешенные. Можно также применить контр-меры или указать местоположение вражеских точек доступа.

RingMaster 9.0: Plan (Default)

File Services Tools Help

Polices RF Planning Configuration Verification Devices Monitor Clients **Security** Alarms Reports

Unauthorized Networks

SSID: [v] Rogue Devices: [v] Suspect Devices: [v] Clients: [v] Last update: 11:12:28 15 Oct

SSID	Rogue Devices	Suspect Devices	Clients
P3LOT_FREE1	0	0	0
(none)	0	0	17
Technical	1	0	0
Guest	1	0	0
Total	2	0	17

Details

IDS Alarms Last update: 11:12:28 15 Oct

DoS Alarms Last update: 11:12:28 15 Oct

Ad-hoc Device(s) = 1

Rogue WLA = 5

Client(s) of Rogue WLA = 17

Total = 23

Rogue WLA(s) = 5 Client(s) of Rogue WLA = 17 Ad-hoc Device(s) = 1

Config: 7 Errors; 345 Warnings Local Changes: none Network Changes: 1 device Alarms 1 22 0 0 23

Tasks: 0

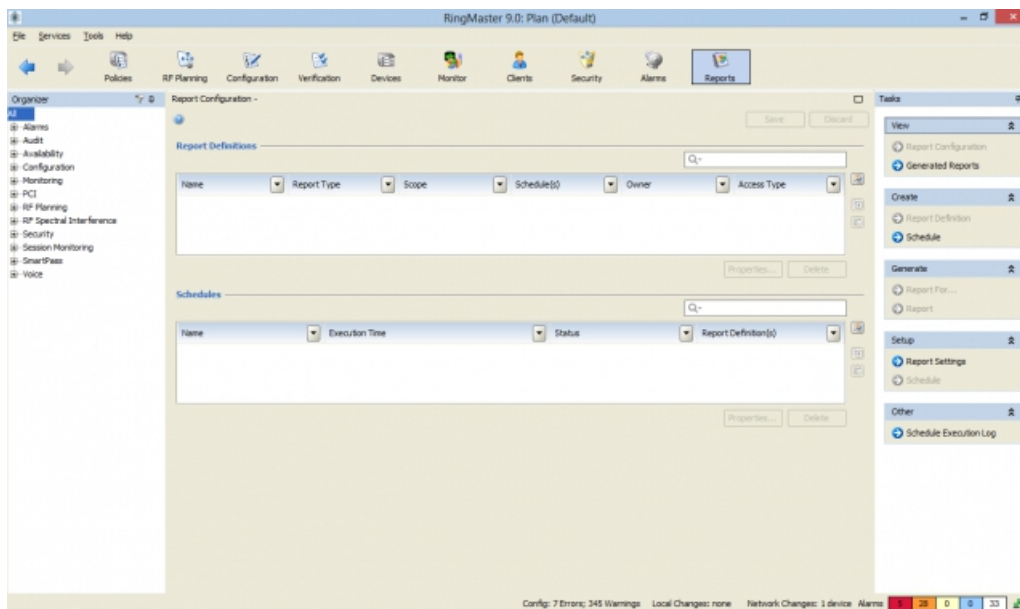
Setup

- RF Classification
- Known SSIDs List

View

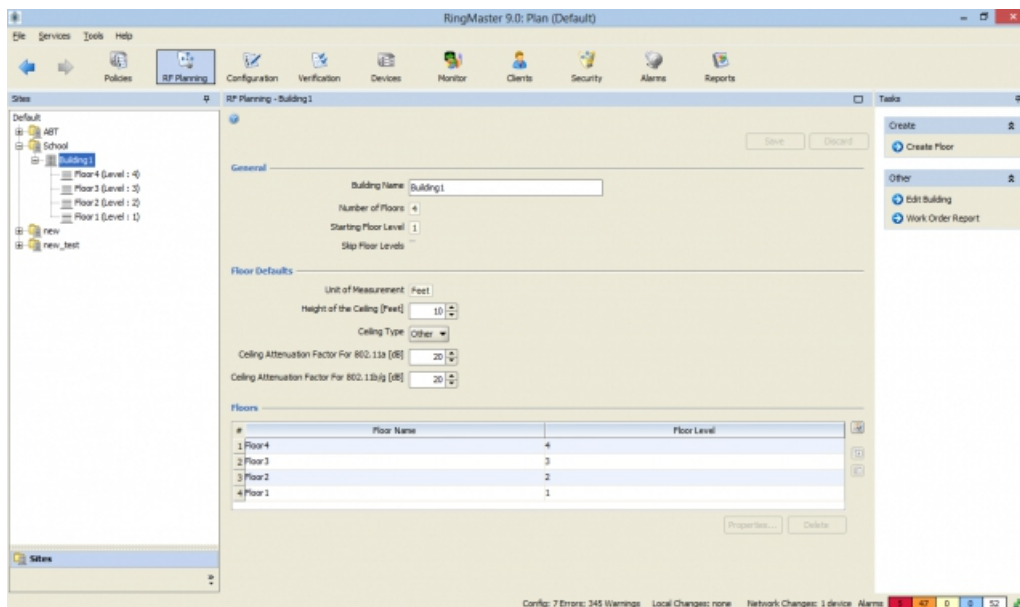
- Rogue Devices
- Suspect Devices
- Clients of Rogue Devices
- Unauthorized Devices
- View Countermeasures

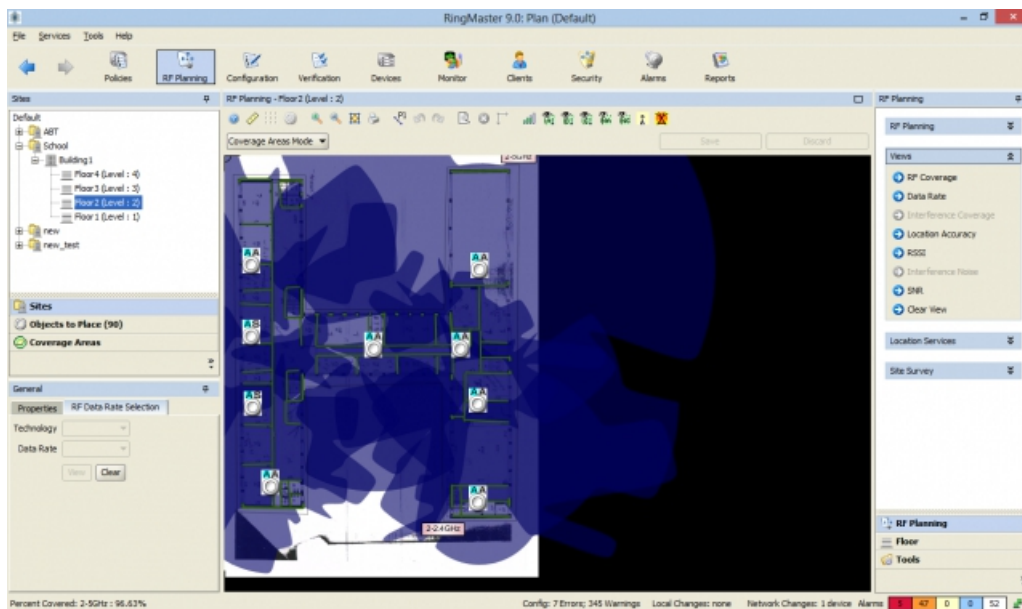
Кроме того, существует раздел ведения отчетности, который позволяет настроить отчеты по любой полученной в RingMaster информации. После чего выслать вам на электронную почту или выгрузить на FTP-сервер.



Одна из основных отличительных особенностей RingMaster - функционал RF planning.

Данный функционал отдельно лицензируется, но может использоваться без лицензии в режиме просмотра. Позволяет с помощью имеющихся планов помещений произвести расстановку и расчет количества точек доступа для удовлетворения заданных параметров беспроводной сети. Планы могут быть либо нарисованными в AutoCAD, либо перенесенными с помощью встроенных инструментов из обычных графических файлов.





Существует возможность создать максимально точный план помещения, указать расположение ключевых объектов, например серверных шкафов, и мест расположения оборудования, задать точный масштаб и т.д. В результате мы получим схему согласно нашему рисунку. По данной схеме можно посмотреть область покрытия сети, в зависимости от режима работы - 802.11a/b/g на/ng - посмотреть уровни соотношения сигнал/шум, определить нахождение клиентов, или вражеских точек доступа, и многое другое.

Тестирование

Как и в прошлый раз, тестирование было разделено на несколько этапов:

- Проверка уровня сигналов радиомодулей и покрытия частотного диапазона;
- Тест скорости передачи данных в пределах одной точки доступа;
- Тест скорости передачи данных между разными точками доступа;
- Проверка перехода между зонами покрытия точек доступа под нагрузкой.

Уровень сигналов получился примерно следующий:

[\[Обзор решений для организации беспроводных сетей многопользовательского доступа, часть 4 - Juniper Networks\]](#)

Уровень сигнала довольно сильный, с учетом того, что точка доступа находится за железным шкафом и бетонной стеной.

Тест скорости передачи данных в пределах одной точки доступа

[\[Обзор решений для организации беспроводных сетей многопользовательского доступа, часть 4 - Juniper Networks\]](#)

Подключиться к точке доступа нам удалось на скорости 130 Мбит/с. При передаче UDP-трафика на скорости 100 Мбит/с, с принимающей стороны мы увидели скорость порядка 88 Мбит.

Для сравнения мы провели тестирование на других скоростях.

[\[Обзор решений для организации беспроводных сетей многопользовательского доступа, часть 4 - Juniper Networks\]](#)

При передаче на скорости 54 Мбит/с мы получили результат в 50 Мбит/с.

Тест скорости передачи данных между разными точками доступа

Между разными точками доступа тест проводился через стену, согласно методике, описанной выше. Мы подключили тестовый ноутбук к одной AP и ноутбук-клиент - к другой. Тест через стену (с использованием двух точек):

[\[Обзор решений для организации беспроводных сетей многопользовательского доступа, часть 4 - Juniper Networks\]](#)

Тестовый сервер показал скорость порядка 70 Мбит/с.

Проверка перехода между зонами покрытия точек доступа под нагрузкой

Проверка перехода под нагрузкой показала, что при правильной настройке оборудования потерь пакетов практически не происходит, как и в случае с оборудованием предыдущих вендоров.

Тестирование, как и в прошлые разы, происходило в ограниченных условиях, поэтому провести более детальные тесты не получилось.

Немного про vWLC

Нами был протестирован виртуальный вариант контроллера vWLC. Данный контроллер ставится на виртуальную машину, и имеет полный функционал контроллера.

Проверка показала, что данное решение имеет такой же CLI-интерфейс как и "настоящий" контроллер WLC, и точно такие же настройки. RingMaster распознал виртуальный контроллер и позволил осуществить его настройку. После установки двух контроллеров мы настроили домен мобильности,

[\[Обзор решений для организации беспроводных сетей многопользовательского доступа, часть 4 - Juniper Networks\]](#)

```
WLC-V# sh mobility-domain
Mobility Domain name: mydomain
Flags: u = up[2], d/e = down/config error[0], c = cluster enabled[0],
       p = primary seed, s = secondary seed (S = cluster preempt mode enabled),
       a = mobility domain active seed, A = cluster active seed (if different),
       m = member, y = syncing, w = waiting to sync, n = sync completed,
       f = sync failed
Member: * = switch behind NAT
```

Member	Flags	Model	Version	NoAPs	APCap
192.168.1.241	upa--	WLC-V	9.0.1.2	1	4
192.168.1.240	us---	WLC-V	9.0.1.2	0	4

WLC-V#

который позволяет осуществлять балансировку точек доступа между контроллерами, и возможность осуществлять "бесшовный роуминг" при миграции между точками доступа, подключенными к разным контроллерам.

Как и при тестировании проводимом выше, тест показал, что при переходе между точками доступа, теряется незначительное количество пакетов, которое не ведет к потере работоспособности клиента в сети.

После этого мы пошли дальше, и настроили кластер из двух устройств.

[\[Обзор решений для организации беспроводных сетей многопользовательского доступа, часть 4 - Juniper Networks\]](#)

```
WLC-V# sh cluster
Network Resiliency Cluster Enabled
Mode : PRIMARY-SEED
Cluster Active Seed : YES
Network Resiliency Status : Resilient
Keepalive interval : 30ms
Keepalive retry-count : 5
WLC-V# sh mobility-domain
Mobility Domain name: mydomain
Flags: u = up[2], d/e = down/config error[0], c = cluster enabled[2],
       p = primary seed, s = secondary seed (S = cluster preempt mode enabled),
       a = mobility domain active seed, A = cluster active seed (if different),
       m = member, y = syncing, w = waiting to sync, n = sync completed,
       f = sync failed
Member: * = switch behind NAT
```

Member	Flags	Model	Version	NoAPs	APCap
192.168.1.241	upacn	WLC-V	9.0.1.2	0	8
192.168.1.240	us-cn	WLC-V	9.0.1.2	1	8

WLC-V#

Точки доступа подключились к кластеру согласно нашим настройкам и отработали функционал отключения одного из контроллеров из режима кластера. Второй контроллер полностью переключал всю работу на себя, переводя точки доступа и клиентские сессии.

Так же можно заметить, что максимально число точек доступа при работе в кластере увеличилось в два раза. Было четыре штуки, а стало восемь штук на контроллер. Эта особенность поведения устройства в кластере, для того, чтобы в случае выхода одного устройства из строя, второе могло бы работать со всеми оставшимися точками доступа.

Немного о технологии Mesh

Нам удалось протестировать технологию Mesh. В данном случае одна точка доступа работает как портал, к которому можно подключить другие точки доступа, для обеспечения связности сети посредством беспроводных каналов связи. Для этого создается специальный профиль с выбранными нами SSID. Затем, выбранные точки доступа настраиваются так, чтобы при загрузке они подключались к данному SSID.

В итоге, наша точка доступа подключилась, и начала вещать нормальный SSID для доступа к сети.

```
WLC-V# sh sessions mesh-ap
1 of 1 sessions matched
Mesh ID          SessID Type Address          Mesh-AP Number AP/Rdo
-----
LR-Juniper-26    34* open 28.8.8.10        2                1/2
```

WLC-V#

WLC-V# sh ap mesh-links

AP: 1 IP-addr: 10.8.8.19

Operational Mode: Mesh Portal

Bridging: Disabled

AP: 2 IP-addr: 10.8.8.28

Operational Mode: Mesh Portal , Mesh AP

Bridging: Disabled

Uplink Mesh Portal: 2049 (54.0 Mbps)

```
-----
      packets      bytes
TX:      418      96700
RX:      459     259247
Uplink Mesh Portal Candidate AP's (* - Current Uplink Mesh Portal)
Radio Mesh Portal MAC  RSSI SSID
-----
*2  40:b4:f0:a3:ca:01  -72 Juniper
```

Если посмотреть следующий вывод

WLC-V# sh ap status

Flags: o = operational[2], c = configure[0], d = download[0], b = boot[0]
a = auto AP, m = mesh AP, p/P = mesh portal (ena/actv), r = redundant[0]
z = remote AP in outage, i/I = insecure (control/control+data)
u = unencrypted, e/E = encrypted (control/control+data)
Radio: E = enabled - 20MHz channel, S = sentry, s = spectral-data
W/w = enabled - 40MHz wide channel (HTplus/HTminus)
D = admin disabled, U = mesh uplink
IP Address: * = AP behind NAT

AP	Flag	IP Address	Model	MAC Address	Radio 1	Radio 2	Uptime
1	oP-i	10.8.8.19	WLA532E-WW	40:b4:f0:a3:ca:00	S	9/9	W 44/13 02h52m
2	opmi	10.8.8.28	WLA532E-WW	40:b4:f0:a3:f3:00	E	1/9	U 44/13 01h24m

WLC-V#

Мы можем увидеть, что первая точка доступа имеет флаг P - mesh portal, active. Вторая точка доступа имеет флаг m - mesh.

После подключения к полученному SSID мы получили доступ в сеть интернет.

Немного о системе SmartPass

Так же нам перепала радость проверить систему гостевого доступа SmartPass. Данная система будет интересна тем, кто хочет организовать свою Wi-Fi-сеть с возможностью раздачи временных кодов доступа, рассылкой уведомлений через sms или электронную почту, а также учетом активности пользователей. Хорошим примером может служить заведение гостиничного бизнеса или предприятие питания.

Данная система устанавливается на выделенный сервер аналогично системе RingMaster, и настраивается как функционал CaptivePortal в системе RingMaster.

ПО имеет возможность создания базы данных пользователей с разграничением прав доступа к сети, а также генерации специальных "чеков", которые содержат данные для входа в сеть. Данные чеки можно модифицировать внешне, согласно требуемым задачам, и рассылать пользователям на почту или сотовый телефон.

Нами было проведено исследование, в результате которого мы получили систему авторизации гостевого доступа к сети, получили уведомление с логином/паролем на почту и на сотовый телефон, и смогли успешно авторизоваться и работать.

Итоги

В результате тестов выяснилось:

Положительные моменты:

- оборудование соответствует заявленному функционалу;
- уровень сигнала устойчивый и приемлемый даже при работе через металлические конструкции и стены;
- скорость передачи данных стабильная (при работе одного клиента);
- работает роуминг клиента, без обрыва связи;
- неплохой набор документации по эксплуатации;
- удобная система управления и мониторинга, с дружелюбным интерфейсом, и широким набором функций;
- понятная и логичная структура конфигурации в режиме CLI;
- Возможность настроить каждое устройство в отдельности, для уникальности определенных параметров;
- возможность управления всеми устройствами в сети, через систему RingMaster;
- технология local switching;
- имеется возможность обеспечить режим работы высокой надежности (кластер, домен мобильности);
- имеется решение для обеспечения гостевого доступа;
- сравнительно невысокая стоимость лицензий по сравнению с конкурентами;
- имеется контроллер с портами 10G.

Не очень положительные моменты:

- небольшой модельный ряд точек доступа, точки доступа в среднем ценовом сегменте в скором времени будут сняты с производства;
- модельный ряд контроллеров не обеспечивает необходимой гибкости решения по соотношению цена/число подключаемых точек доступа;
- Нет нормальной системы управления "из коробки";
- Внешняя система управления RingMaster стоит дополнительных затрат и лицензируется.

Ссылки, размещенные в тексте:

Предыдущие материалы, посвященные оборудованию [Extricom](#) и [Aruba](#), [Extreme Networks](#) были по достоинству оценены читателями.

В этой же статье речь пойдет о решении, предлагаемом Juniper Networks.

...материал посвящен оборудованию, которое можно приобрести у [нас в магазине](#).

как это было реализовано в решении [Extreme Networks](#).

[WLC2](#) - самая младшая модель в линейке, поддерживает 4 точки доступа...

[WLC8](#) - модель, которая поддерживает подключение до 12 точек доступа...

[WLC100](#) - новинка среди модельного ряда, имеет 4 порта 1000BASE-T...

[WLC800/880](#) - две практически одинаковые модели, различаются только максимальным числом подключаемых точек доступа...

[WLC2800](#) - самый мощный контроллер, представленный в модельном ряде.

[WLA321](#) - точка доступа с интегрированными/внешними антеннами и одним радиомодулем...

[WLA322](#) - точка доступа с интегрированными/внешними антеннами и двумя радиомодулями...

[WLA522\(E\)](#) - точка доступа с интегрированными/внешними антеннами и двумя радиомодулями...

[WLA532\(E\)](#) - точка доступа с интегрированными/внешними антеннами и двумя радиомодулями...