NETSHe OS RU chapter 12

Original file

NETSHe Lab

Универсальное программное обеспечение NETSHe для сетевых устройств. Часть 12. Сервер управления и мониторинга (NMMS)	
NETSHeLab длительное время занимается разработками программного обеспечения для сетевых устройств, провайдеров услуг и операторов связи. Среди программного обеспечения центральное место занимает операционная система NETSHe, которая может быть использована в широком спектре сетевых устройств и сервисов.	
Версия 1 Июль, 2020	Станислав Корсаков, ООО «Нетше лаб» (c) 2009-2020 Ярославль

Оглавление

Операционная система NETSHe имеет унифицированную архитектуру для разного типа устройств: маршрутизаторов, точек доступа, абонентских устройств. С ростом числа таких устройств в одной сети возникла закономерная задача: сделать управление этими устройствами максимально простым и автоматическим. Помимо задачи управления в любой сети возникают задачи контроля за работой сетевых устройств, сбора статистики их совместной работы и пр. Решение всех этих задач и сформировало многофункциональный программный продукт NetworkMonitoringandManagementServer (NMMS).

Настоящий документ не является подробным руководством по работе с NMMS, но дает обзорное представление об основном функционале этой системы. С другой стороны, NMMS представляет из себя одно из применений операционной системы NETSHe, поэтому в руководстве о NETSHe это нельзя не сказать: NMMS самостоятельное серверное приложение, работающее под управлением ОС NETSHe.

Краткое описание NMMS

NMMS может поставляться в виде виртуальной машины, самостоятельного устройства, а так же предоставляться в виде веб-сервиса с размещением данных вне площадки заказчика.

Один экземпляр NMMS может обслуживать тысячи устройств. При этом максимальные возможности управления предоставляются для устройств под управлением NETSHe, но это не означает, что другие устройства не могут контролироваться сервером NMMS. NMMS посредством стандартных протоколов мониторинга и управления сетями может управлять устройствами под управлением любого встроенного ПО, от которого требуется поддержка этих стандартных протоколов.

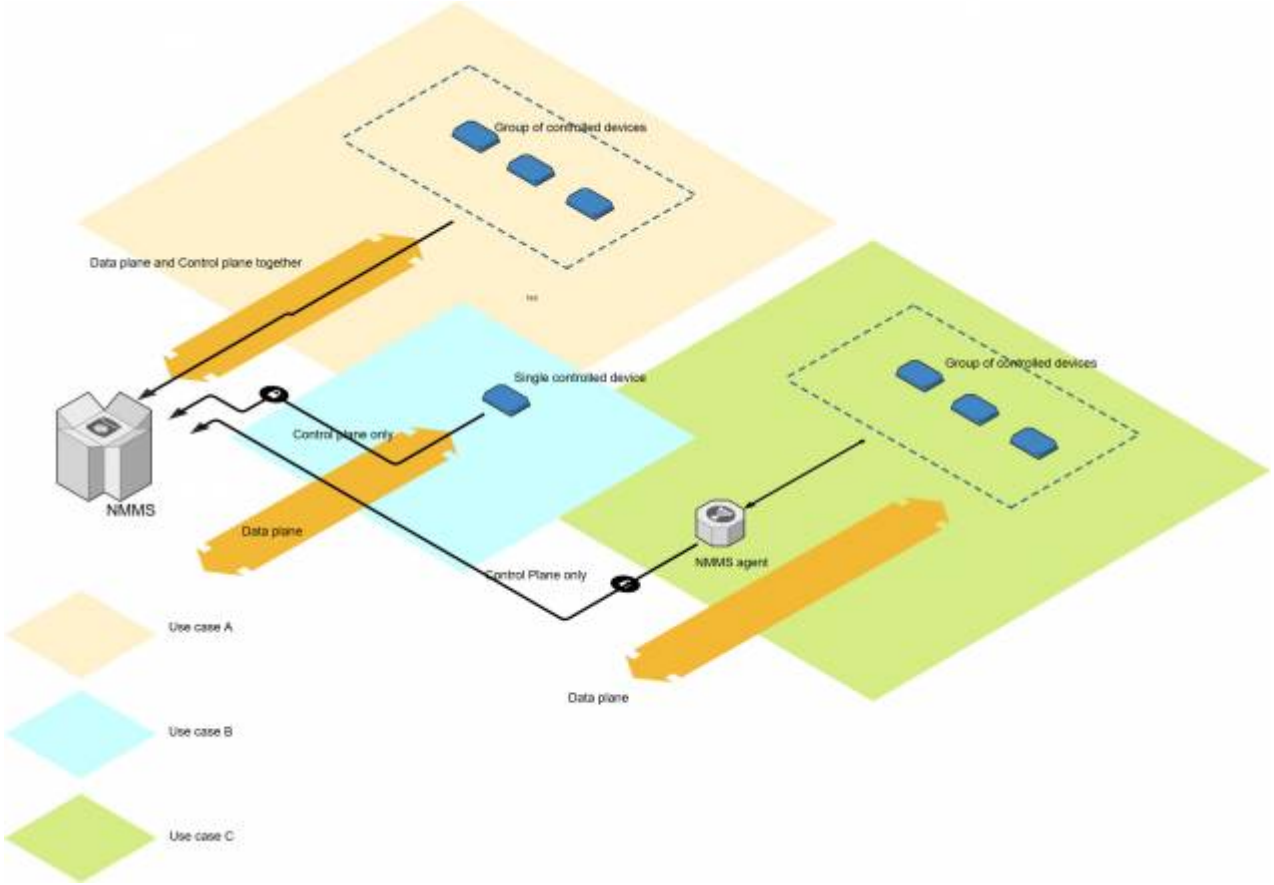
Основной функционал NMMS

В стандартной реализации NMMS реализован следующий функционал:

1. NMMS предлагает единую точку доступа к управлению всеми устройствами, их консолям и веб-интерфейсам.
2. NMMS содержит удобный инструмент для отображения и редактирования параметров устройств и сетевого окружения. Настройки, статистика, адреса, маршруты визуализированы и показываются в едином форматированном виде.
3. Для удобства настройки сходных конфигураций устройства могут быть объединены в группы.
4. Для ускорения ввода в эксплуатацию множества устройств NMMS предлагает механизм развертывания, который помимо первоначальной настройки автоматически предполагает резервное копирование, архивирование настроек, удаленный сброс устройств.
5. Учитывая предыдущий пункт, устройства могут присоединяться к NMMS уже на стадии нулевой конфигурации.
6. Для быстрого развертывания новых версий операционных систем на устройствах NMMS включает механизм централизованного автоматического обновления.
7. Для разделения ролей администраторов, а также для интеграции с существующими системами NMMS поддерживает несколько стандартных сервисов аутентификации и биллинга, а также AAA-, WAC/WLC, hotspot контроллеры.
8. NMMS предоставляет единую точку входа к управлению системой безопасности устройств: конфигурации сетевых экранов, правил управления трафиком и QoS.
9. Имея под управлением беспроводные устройства, NMMS предоставляет дополнительные возможности для беспроводных устройств, в свою очередь объединяя их в группы по типам радиодоступа и общим политикам. С помощью этого свойства можно добиваться лучшего потребления радиоэфира, повышать качество радиосвязи, агрегировать и резервировать радио-линки.
10. NMMS отслеживает весь жизненный цикл устройств: время онлайн, падение интерфейсов, перезагрузки, потребление основных ресурсов на устройстве.
11. NMMS имеет интеграцию с сервером Zabbix, который собирает, хранит и визуализирует сетевые события.
12. Для лучшего представления NMMS размечает устройства на картах OpenStreet.
13. Для обмена с устройствами NMMS использует защищенные соединения.

Топология размещения NMMS в сети

Существуют три основных варианта размещения NMMS в сети, все они показаны на следующей картинке:



Случай A (caseA) предусматривает размещение NMMS непосредственно в одной сети с устройствами, подразумевается, что все устройства располагаются внутри периметра сети и контролируются администраторами. Такой режим называется ‘passthrough’.

Случай B (caseB) предусматривает, что устройства расположены напрямую в Интернете или в подсетях, подключенных к Интернет. Такой режим называется ‘non-passthrough’.

Случай C (caseC) предусматривает, что в устройства располагаются в одной локальной сети со специальным устройством, которое выполняет функции агента NMMS. При этом полезный трафик устройств не проходит через этого агента, агент оперирует только трафиком управления. Такой режим также можно отнести к ‘non-passthrough’.

Обеспечение безопасных соединений NMMS

В зависимости от применяемой топологии передача данных до сервера NMMS и обратно защищается следующим образом:

1. Для передачи трафика управления по Интернет и небезопасным сетям используется OpenVPN, автоматически поднимающийся на сервере и устройствах. Это относится ко всем соединениям режима ‘non-passthrough’, в схеме с агентом применяется между сервером NMMS и его агентом.
2. Для передачи трафика управления по безопасным сетям используется автоматически настраивающийся PPPoE.

Удаленный доступ к консолям и веб-консолям устройств осуществляется по защищенному протоколу HTTPS.

По желанию заказчика или требованиям политик, трафик управления NMMS может быть помещен в VPN туннели, изолирован VLAN или защищен комбинацией протоколов.

Описание процедуры настройки NMMS

Процедура настройки детально описывается в руководстве по NMMS. В данном документе только перечисляются основные шаги в целях продемонстрировать, что настройка NMMS представляет собой простой и быстрый процесс, не обремененный сложной теорией и множеством альтернативных вариантов:

1. На первом этапе администратор открывает веб-интерфейс NETSHe. Напомним, что NMMS работает на компьютере под управлением NETSHe. С помощью WebUI администратор:

a) задает имя сервера,

b) определяет интерфейс для работы NMMS, IP-адрес и параметры удаленного доступа,

c) определяет параметры подключения к RADIUS серверу, его внешнее имя,

d) задает диапазон адресов для серверного интерфейса OpenVPN,

e) задает диапазон адресов для серверного интерфейса PPPoE (для режима passthrough),

f) задает параметры ntp синхронизации времени,

g) указывает сервер DNS для разрешения локальных имен.

1. На следующем этапе администратор подключается к веб-интерфейсу NMMS, параметры которого он уже настроил на первом этапе. При первом подключении администратор увидит мастер настройки, который подскажет, что нужно настроить валюту и параметры предприятия. Далее в мастере же администратор определит свои базовые права и сменит свой пароль.

На этом базовая настройка NMMS завершена, сервер готов регистрировать устройства.

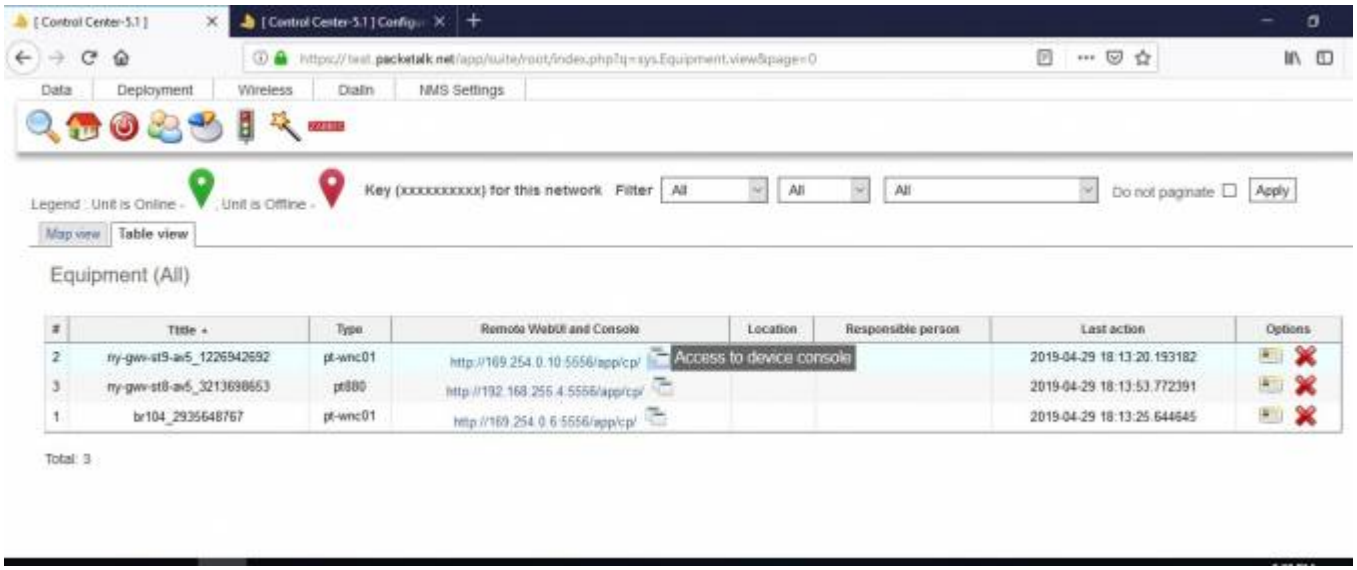
Применение NMMS

Функционал NMMS может быть использован частично или полностью по желанию администраторов сети. В данном разделе будут перечислены основные задачи, решаемые с помощью NMMS. Устройства, зарегистрировавшиеся на сервере NMMS, мы будем называть контролируемыми устройствами.

Удаленный доступ к контролируемым устройствам

Поскольку все устройства показываются в режиме карты и в таблице, легко выбрать нужное устройство и нажать на ссылку для открытия его веб-интерфейса. Где бы ни располагалось

устройство, администратор увидит его, как будто подключившись к его LAN порту. Аналогично рядом есть значок для доступа к консоли устройства.



Группы контролируемых устройств

В целях разграничения административного доступа между несколькими администраторами или для облегчения администрирования устройств одной модели, а также по другим причинам устройства можно объединять в группы.

Каждое контролируемое устройство может принадлежать только к одной группе. При этом на устройство будут действовать политики распространения настроек, обновления ПО, сбора статистики и резервного копирования, определенные для данной группы устройств. Параметры политик, определенные для группы, имеют приоритет перед параметрами общими для всех устройств.

У каждой группы должен быть один администратор, права которого имеют меньший приоритет перед правами главного администратора системы (superuser).

Спектр задач для устройств, задаваемых группе, очень широк. На устройствах можно:

1. создавать новые интерфейсы,
2. управлять маршрутизацией,
3. задавать любые параметры устройствам,
4. управлять сервисами, которые устройства предоставляют пользователям,
5. перегружать, обновлять устройства и т.д.

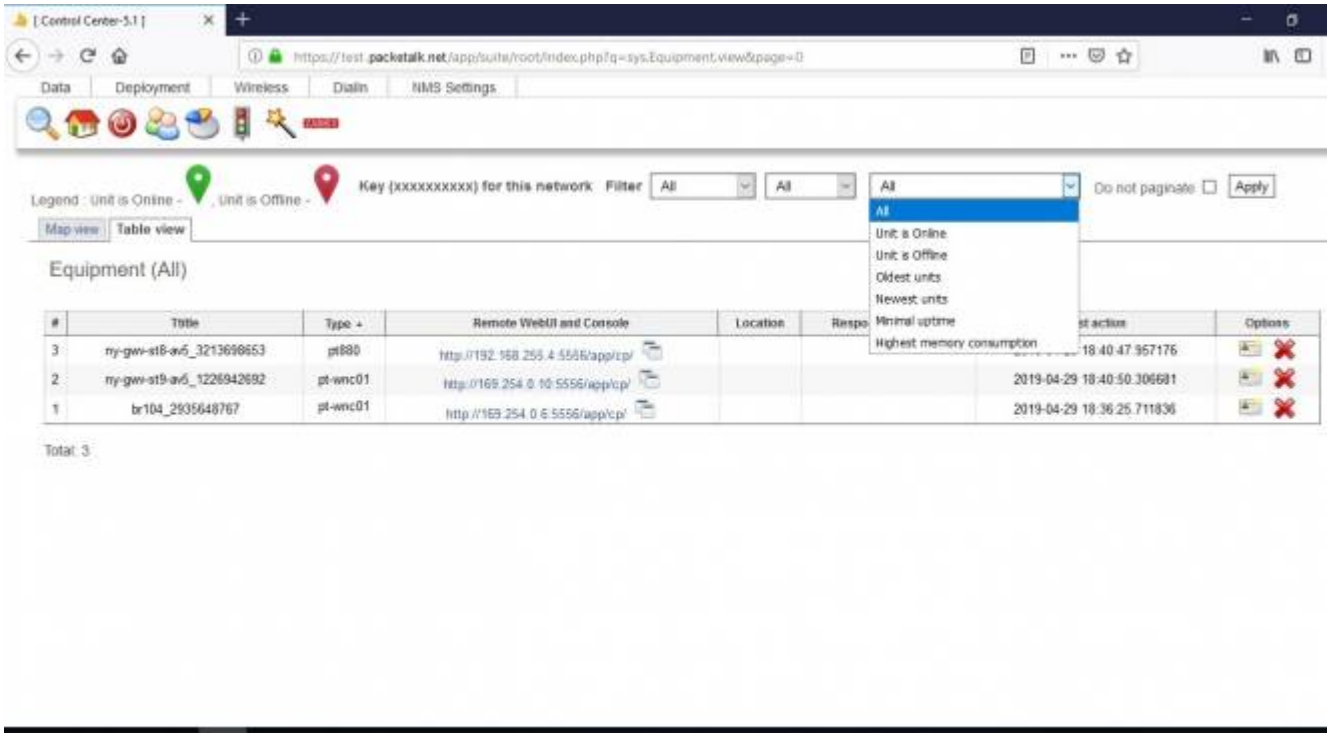
Задачи можно запускать по расписанию.

Среди групповых задач имеются служебные, предназначенные для собственных нужд NMMS, это задачи мониторинга, резервного копирования конфигураций, автоматических отчетов о состоянии и пр.

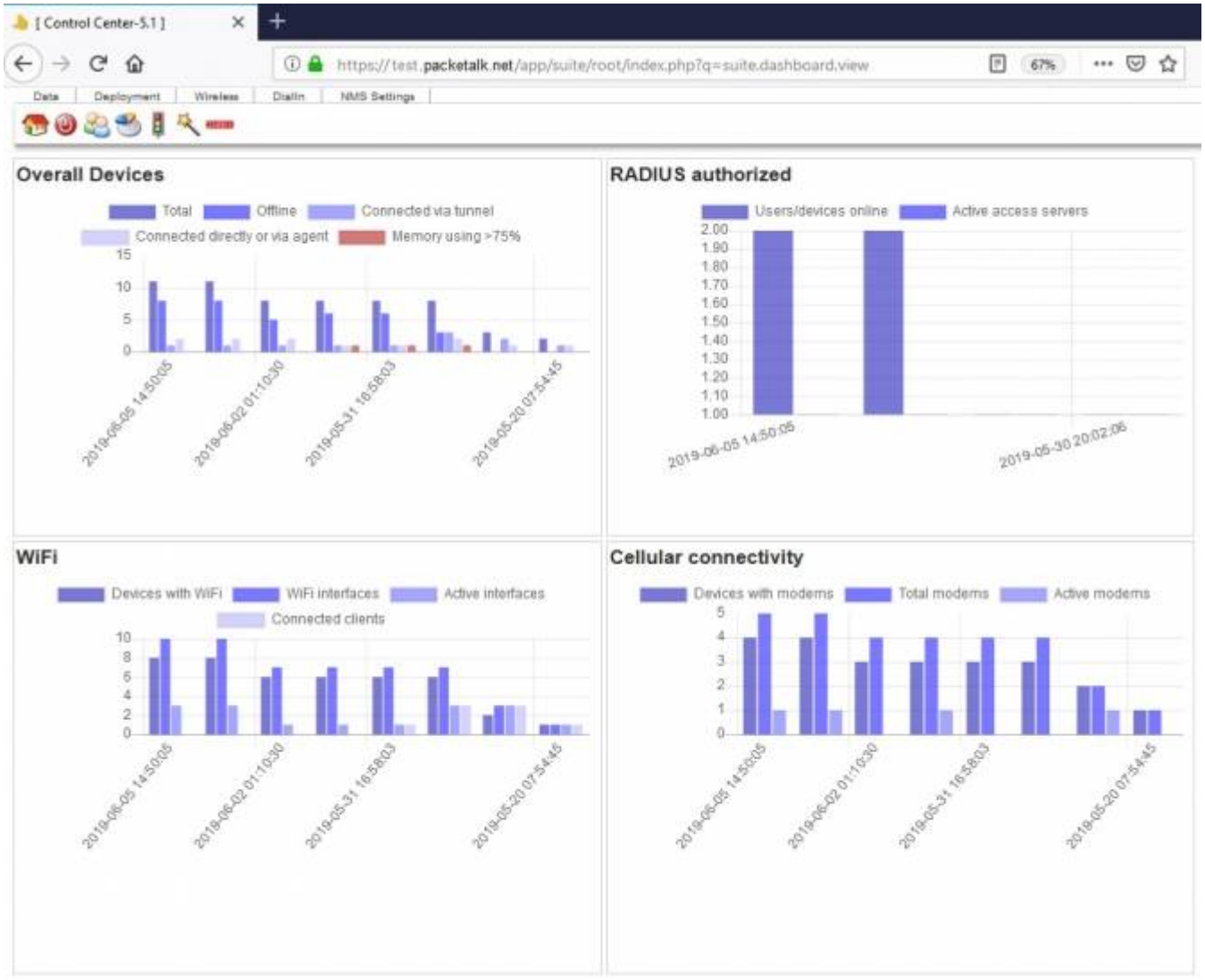
Устройства, не включенные в какую-либо группу, неявно образуют основную группу, к которой применяются задачи и настройки уровня сервера.

Мониторинг контролируемых устройств

В таблице устройств есть средства фильтрации, дающие быстрый обзор последних изменений в сети.



Обзорную статистику и тенденции можно посмотреть на dashboard.



Помимо этого, можно посмотреть подробные журналы любого контролируемого устройства (даже недоступного в момент просмотра) и события на NMMS, связанные с этим устройством, отследить изменения параметров каждого контролируемого устройства с течением времени.

Не следует забывать про широкие возможности Zabbix, который в привычной форме предоставит администраторам свой функционал для анализа, формирования отчетов, диагностических целей в отношении контролируемых устройств.

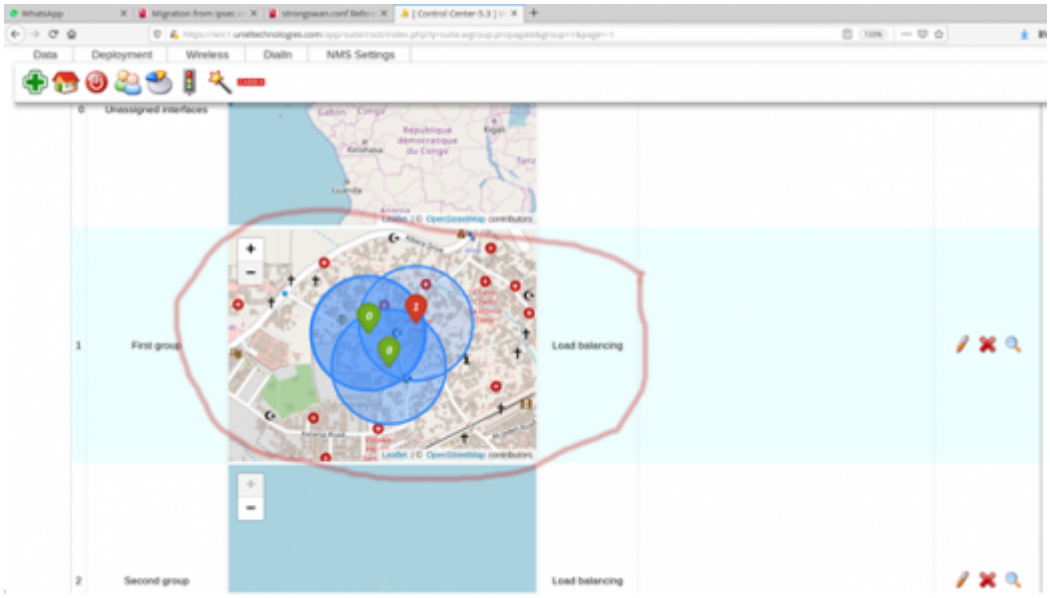
Групповое управление Wi-Fi

Если несколько беспроводных устройств работают в соседстве друг с другом, с помощью анализа информации, получаемой с устройств, можно:

1. эффективно выбирать каналы и уровень сигнала, как следствие, эффективнее выстраивать среду беспроводной передачи,
2. точнее определять и избегать интерференций сигнала и их источники,
3. в режиме реального времени определять деградацию сигнала и передачи трафика, оперативно предотвращать обрывы и повторную авторизацию.

Отображение устройств на карте и размещение на этой же карте источников помех помогает

персоналу определить лучшее расположение точек доступа внутри и вне помещений.



Заключение

Цель данного документа - дать общее представление о NetworkMonitoringandManagementServer (NMMS), созданного в ООО «Нетше лаб». Поскольку ОС NETSHe позволяет надстраивать сервисы по желанию клиентов или потребности проекта, то вариантов применения NMMS тоже значительно больше, чем перечислено выше. В частности, в данном документе не описаны возможности учета трафика (биллинг), регистрация пользователей через популярные Интернет-сервисы, авторизация ваучерами и сертификатами. Эти сервисы могут быть реализованы под заказ, заказчик принимает на себя регистрацию этих сервисов в контролирующих органах, оформление сертификатов и пр. При наличии у заказчика разрешения на использование криптографических средств, они так же могут быть применены в проекте. Аналогично могут быть применены сетевые протоколы, описанные в RFC и реализованные Интернет-сообществом в репозиториях.