Иван Лопухов

Железный ключ к управлению беспроводными сетями IEEE 802.11a/b/g/n

Большие сети – большие проблемы

Распространение беспроводных сетей Wi-Fi и их интеграция в сети Ethernet привели к смене привычной топологии построения сети: вместо одиночных беспроводных точек доступа в проводных сетях появились целые беспроводные сегменты сети с централизованным управлением. Управление большим количеством оборудования Wi-Fi – нетривиальная задача, решаемая с помощью специального оборудования и методов.

Точки доступа Wi-Fi не относятся к типу Plug-and-Play, развертывание и эксплуатация беспроводной сети связаны со следующими задачами:

- установка, конфигурирование, обслуживание точек доступа,
- настройка гостевого доступа в сеть, регистрация новых точек доступа – индивидуально для каждой точки доступа,
- управление перекрытием частот смежных точек доступа, ручная настройка радиоканалов,
- последовательная перенастройка всех точек доступа, постепенная смена топологии сети,
- комплексное управление безопасным доступом в сеть в местах общего доступа.

Решение этих задач – обязательная и затратная процедура, серьёзно увеличивающая суммарную стоимость владения сетью. Снизить эти затраты помогает централизованное управление беспроводным оборудованием, то есть создание некого сервера сети, регулирующего трафик в сегменте WLAN. Коммутаторы и маршрутизаторы Ethernet не совсем подходят для данной задачи, так как в случае их применения на них приходится двойной объём трафика сети, и они в конце концов станут «бутылочным горлышком», снижающим общую пропускную способность сети.

Для оптимального управления беспроводной сетью нужен специальный контроллер WLAN, способный выполнять следующие задачи:

- гибкое распределение ресурсов сети в зависимости от типа пользователя и приложения, функции роуминга между сегментами WLAN на 3-м уровне OSI,
- централизованная авторизация и конфигурирование всех точек доступа из одного устройства,
- быстрое развертывание сети WLAN, снижение стоимости владения сетью,
- централизованное обновление прошивок точек доступа,
- расширение защищённой сети, включение в неё удалённых точек доступа,
- автоматический контроль точек доступа на предмет интерференции сигналов,
- резервированная концепция WLAN-контроллера на случай его отказа, отсутствие каких-либо списков паролей в памяти контроллера,
- централизованная регистрация и мониторинг клиентов сети.

Выполнение описанных специфических задач невозможно без специального протокола.

Стандарт CAPWAP

Протокол контроля и обеспечения беспроводных точек доступа CAPWAP (Control And Provisioning of Wireless Access Points) был разработан организацией IETF (Internet Engineering Task Force) как базовый стандарт управления беспроводными сетями.

Данный протокол использует разные каналы для передачи данных:

- канал контрольных данных, защищённых с помощью протокола DTLS. По нему передаётся административная информация между точками доступа и контроллером WLAN;
- канал передачи данных, который также при необходимости может быть защищён с помощью протокола DTLS. Данные из WLAN в LAN передаются внутри протокола CAPWAP.

При инкапсуляции передаваемых данных внутрь CAPWAP-тоннелей исключается избыточная нагрузка на WLAN-контроллер и во внешнюю сеть попадают только необходимые данные. Визуально такая структура представлена на рисунке 1.

Структура сети с контроллером WLAN

В традиционной сети Ethernet с единичными беспроводными точками доступа все функции по обеспечению передачи данных, управления трафиком, управления и диагностики интегрированы в каждое устройство. В концепции централизованного управления сетью WLAN эти задачи поделены между двумя устройствами:

- контроллер WLAN выполняет административные функции,
- точки доступа выполняют передачу данных.

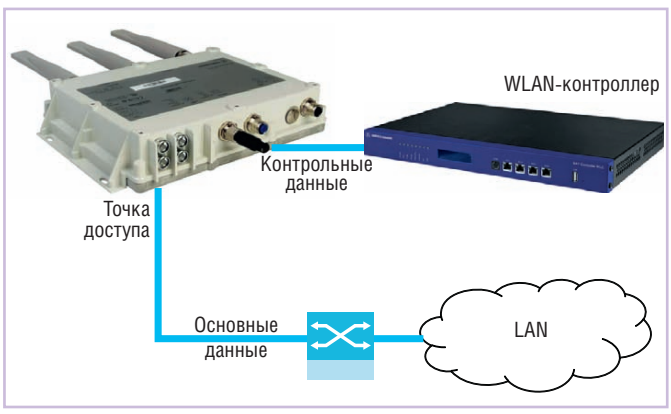

Рис. 1. Структура WLAN-контроллера

Протокол CAPWAP предусматривает три варианта интеграции WLAN-контроллера в сеть:

- перенос MAC-адресов во WLAN-контроллер. Функции канального уровня выполняет контроллер, точки доступа становятся физическими преобразователями проводной среды в беспроводную;
- разделение MAC-адресов. Приложения, критичные ко времени доставки данных по сети, функционируют через точки доступа, остальные приложения обращаются во WLAN-контроллер;
- без переноса MAC-адресов. Трафик передаётся через точки доступа, администрирование параметров которых ведётся через контроллер.

Оптимальным является третий вариант, при котором обеспечивается простое масштабирование сети. Кроме того, WLAN-контроллер не становится «бутылочным горлышком» сети, фактически принимая всю нагрузку на себя. Основной объём данных проходит по сети, минуя процессор контроллера. Это особенно актуально в работе с точками доступа стандарта 802.11n, нагрузка от которых до 10 раз выше нагрузки сетей 802.11b/g.

Повелитель «летучих мышей»

Пример такого WLAN-контроллера – Hirschmann BAT-Controller WLC, устройство, созданное производителем для администрирования своих точек доступа серии BAT. Контроллер представлен на рисунке 2.

Рис. 2. Контроллер беспроводных сетей Hirschmann BAT-Controller WLC

Внешне это шасси формата 1U для установки в 19" стойку. На лицевой части имеются LCD-дисплей, индикаторы состояния, 4 интерфейса 10/100/1000Base-TX, последовательный интерфейс локального управления и USB-порт для автоматических конфигурационных адаптеров Hirschmann. Питание контроллера – от розетки 220 В. Рассмотрим основные функциональные особенности BAT-Controller WLC.

1. Авторизация и конфигурация точек доступа.

Поддержание точек доступа в сконфигурированном рабочем состоянии – основная задача контроллера WLAN. Для этого каждая точка доступа должна быть привязана к контроллеру, чтобы получать от него актуальную конфигурацию. Привязка оборудования осуществляется по так называемым цифровым сертификатам. В определённый момент времени WLAN-контроллер раздаёт сертификаты доступным точкам доступа, делая их доверенными. По этим сертификатам в дальнейшем оборудование идентифицируется контроллером, который по MAC-адресу находит в своих профилях оборудования правильную конфигурацию и высылает её точке доступа. Неавторизованным точкам доступа также может высылаться стандартная конфигурация, позволяющая выполнить дальнейшую настройку.

2. Настройка без единого касания.

Функция автоматической настройки даёт возможность точкам доступа выпускать цифровые сертификаты и передавать их вместе с типовыми конфигурациями заново подключаемым точкам доступа. Данная функция актуальна для развёртывания или наращивания сети без привлечения IT-специалистов, тем самым может сэкономить трудовые ресурсы.

3. Наследование параметров.

WLAN-контроллер может управлять различными типами оборудования. Тем не менее профили оборудования, содержащиеся в его памяти, могут не совпадать со всеми возможными разновидностями точек доступа. Например, во многих странах параметры режимов радиомодулей различны. Чтобы избежать ручной настройки множества однотипных параметров, выбранные параметры могут быть унаследованы из указанных источников. При этом возможно даже перекрёстное наследование разных параметров между двумя профилями оборудования.

4. Раздельное управление распределёнными точками доступа.

Подчинённые точки доступа могут находиться в разных подсетях. Для управления ими WLAN-контроллер использует разные виртуальные сети. Типовые параметры беспроводных сетей устанавливаются, как обычно. Таким образом, контроллер очень удобен на верхнем уровне сети для управления распределённой корпоративной сетью.

5. CAPWAP-туннелирование и роуминг 3-го уровня OSI.

Особенность WLAN-контроллера – разделение трафика сети на контрольные данные, передаваемые внутри протокола CAPWAP, и общие данные, передаваемые по сети в обход контроллера. Такой подход позволяет гибко сбалансировать нагрузку на сеть, не обрушивая всю нагрузку на процессор WLAN-контроллера. Однако некоторые данные, например голосовые (VoWLAN), проходят через сам WLAN-контроллер, который обеспечивает «бесшовный» роуминг на 3-м уровне сети. Таким образом голосовое соединение между SIP-телефонами не прерывается даже при переходе между подсетями WLAN.

6. Обновление прошивок и кодов.

WLAN-контроллер позволяет централизованно обновлять прошивки и специальные коды (script) точек доступа. Для этого они сохраняются на Web-сервере, контроллер проверяет их файлы и при необходимости обновляет устройства. Централизованное обновление может быть выборочным, например, ограниченным конкретными MAC-адресами.

7. Оптимизация радиоканалов.

Каждая точка доступа в пределах одного стандарта (802.11a/b/g/n) имеет несколько (от 13 до 64) радиоканалов, по которым может вестись передача сигнала. Абонент должен находиться в том же стандарте и на одинаковом канале передачи. При одновременной передаче на одном радиоканале возникает интерференция сигнала, поэтому каналы распределяются между точками доступа (рис. 3). Для автоматического распределения радиоканалов между точками доступа сети WLAN-контроллер проводит их последовательное включение. По мере включения радиомодули точек доступа автоматически выбирают свободный канал.

8. Функционирование сети без WLAN-контроллера и его резервирование.

В современных сетях используется резервирование узлов и каналов связи для повышения устойчивости сети к отказам оборудования. Аналогично в случае отключения WLAN-контроллера сеть не должна прерывать обмен данными. Точки доступа, потеряв связь с контроллером, продолжают функционировать согласно последней полученной конфигурации. При этом, если конфигурация временная, то устройство будет функционировать до истечения «срока годности» конфигурации, затем будет ждать соединения с WLAN-контроллером. Также контроллеры в сети могут быть дублированы по схеме 1:1, либо беспроводная сеть может обслуживаться одновременно несколькими WLAN-контроллерами. При одновременной работе нескольких контроллеров они разде-

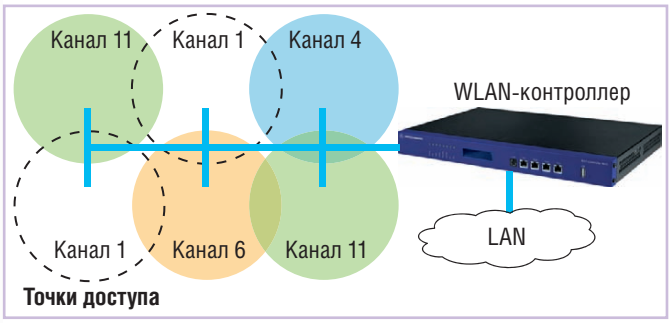

Рис. 3. Распределение радиоканалов между точками доступа WLAN

ляют обслуживание точек доступа, при отказе контроллеров в группе обслуживаемое оборудование перераспределяется между оставшимися WLAN-контроллерами.

9. Управление клиентским доступом.

Для авторизации и учёта пользователей по беспроводной сети часто используется технология RADIUS-сервера. Если специальной конфигурации для клиента сети не требуется, точка доступа передаёт запрос на подключение WLAN-контроллеру. Тот либо сверяется с собственной клиентской базой, либо передаёт запрос специализированному RADIUS-серверу. Данные запросы также могут передаваться на сервер, минуя WLAN-контроллер.

10. Управление сетями VLAN.

Большие распределённые сети требуют разделения на сегменты, в которых организуются виртуальные сети VLAN. Однако мобильность беспроводного доступа подразумевает перемещение клиентов между подсетями. В этом случае используются динамические VLAN-сети и RADIUS-сервер, назначающий идентификатор сети VLAN подключаемому клиенту.

Заключение

WLAN-контроллер типа Hirschmann BAT-Controller WLC оптимален для больших сетей с количеством точек доступа более 15. Для небольших промышленных сетей Ethernet, содержащих как беспроводное оборудование, так и коммутаторы Ethernet, больше подойдёт индивидуальное управление оборудованием либо программное обеспечение Hirschmann HiVision. Но для управления несколькими десятками точек доступа BAT-Controller WLC становится необходимым.

В промышленных сетях Ethernet приложения вроде VoIP играют второстепенную роль. Сеть обычно обслуживает несколько приложений и, следовательно, передаёт одновременно разный по приоритетности и характеру трафик. Настройку и обслуживание мультисервисной сети, использующей беспроводное оборудование, целесообразно проводить с помощью такого специализированного устройства, как Hirschmann BAT-Controller WLC. Контроллер поможет избежать многих ошибок, повысит безопасность беспроводной сети за счёт встроенного межсетевого экрана, снизит суммарную стоимость владения сетью. Кроме того, простая локализация пользователя с помощью WLAN-контроллера поможет отслеживать перемещение клиентов сети, а значит, и персонала, пользующегося беспроводным оборудованием. ●

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Компания Signatec присоединяется к DynamicSignals

В конце августа 2011 года компания **DynamicSignals LLC** объявила о приобретении активов компании **Signatec, Inc**, тем самым продолжив успешную практику предыдущих слияний.

С этого момента Signatec становится одним из брендов, входящих в **DynamicSignals** наряду с уже имеющимися в её составе компаниями, такими как **Gage**, **KineticSystems**, **Preston Scientific** и **Cyber Systems**.

Обе компании, и Signatec, и DynamicSignals, имеют долгую историю и приверженность традициям наиболее полного удовлетворения потребностей своих клиентов.

Signatec, уже более 10 лет эксклюзивно представляемая на российском рынке компанией ПРОСОФТ, хорошо известна своими высокоскоростными устройствами ввода-вывода и системами обработки больших объёмов данных в реальном времени. Оборудование, поставленное клиентам за эти годы, нашло широкое применение в промышленности, науке, безопасности и зарекомендовало себя как высоконадёжное и производительное.

DynamicSignals основана 40 лет назад и изначально была известна под брендом KineticSystems. Сейчас компания располагает офисами в Анахайме (Калифорния) и в Лашине (Монреаль, Канада), штаб-квартира и завод находятся в Локпорте (Чикаго).

DynamicSignals предлагает продукцию известных стандартов CAMAC, VXI, PCI/PCIe, cPCI и PXI/PXIe-платформы, разработанные для общепромышленных применений. Номенклатура включает в себя как сверхвысокоскоростные АЦП с небольшим числом каналов, так и многоканальные низкочастотные платы сбора данных. Дополнительно для удовлетворения запросов рынка и специфических требований конкретных приложений создаются собственные системы. Компания вертикально интегрирована, все продукты разрабатываются и производятся самостоятельно, для монтажа электронных компонентов имеются собственные автоматические сборочные линии.

В результате продукция широко используется в таких областях, как авиация, ракетостроение, испытание реактивных двигателей, аэродинамические трубы, системы контроля надёжности конструкций, баллистические тестовые системы. Список клиентов DynamicSignals внушителен, в него входят прямые заказчики из министерства обороны, ВВС и ВМФ США, NASA, однако чаще всего оборудование для подобных проектов поставлялось через крупных генподрядчиков, таких как Northrop, Boeing, Lockheed, BAE, EADS, Honeywell, Raytheon, General Electric, General Dynamics, Rockwell и др.

Компании DynamicSignals и Signatec поблагодарили своих клиентов за успешное сотрудничество в прошлом и выразили уверенность, что объединение ресурсов позволит в будущем предоставить им ещё больше преимуществ и возможностей.

Для российских заказчиков ПРОСОФТ, уже использующих или только собирающихся применять продукты Signatec, это позволит в самом ближайшем будущем ориентироваться на расширенную номенклатуру, производимую всеми брендами, входящими в состав DynamicSignals. ●