Bluesocket vWLAN: оборудование, решения, конкурентные преимущества

А. Горнак
ООО «НСТ»

ag@nstel.ru

Ключевые проблемы WLAN

- Безопасность
  - Границы WLAN не совпадают с границами предприятия: доступ неавторизованных пользователей, перехват данных, подлог ТД, …
  - Ср-ва обеспечения: аутентификация, авторизация, аккаунтинг, шифрование, IDS/IPS, сканирование клиентов

- Мобильность
  - Хэндовер, L3 роуминг, сохранение параметров безопасности при перемещении
  - Ср-ва обеспечения: проактивное хэширование ключей, управление параметрами подключения пользователей и туннелированием данных
- Управление
  - Управление радиопокрытием, QoS, ТД, пользователями, безопасностью, …
  - Ср-ва обеспечения: встроенные в ТД или выделенные ср-ва управления

Автономные ТД (WLAN 1-го поколения)

Все в одной Точке Доступа

Т.н. «Толстая» ТД
или
Автономная ТД

Преимущества

- Идеальны для SOHO
- До сих пор широко используются
- Независимы и надежны
- Недорогие для малых сетей

Недостатки

- Нецелесообразны для средних и больших сетей (от 10 ТД)
- Трудно применять согласованные правила безопасности
- Децентрализованное управление
- Невозможность работы в тандеме с другими ТД
- Украденные ТД могут продолжать работать

Централизованная WLAN (2-е поколение)

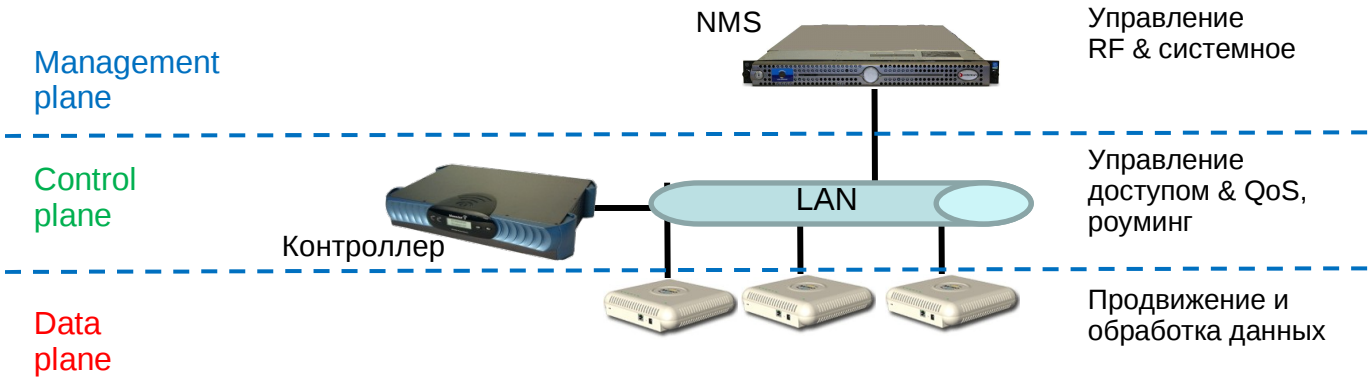
Преимущества

- Удобное централизованное управление
- Высокая безопасность
- Тонкие ТД работают только с контроллером
- Остается наиболее распространенной WLAN архитектурой

Недостатки

- Контроллер ограничивает масштабируемость сети
- Дополнительные задержки, т.к. данные проходят через контроллер
- Для 802.11n и большего кол-ва пользователей требуется более мощный контроллер
- Нежелательные данные проходят через LAN к контроллеру для применения правил безопасности
- Много контроллеров – много мобильных доменов

Концепция децентрализации



- Интеллектуальная обработка данных д.б. максимально приближена к пользователю
- Централизация управления и контроля облегчает эксплуатацию и увеличивает масштабируемость
- Сетевая архитектура не должна содержать «узких» мест

3-е поколение WLAN

(централизованное управление, распределенная передача данных)

TRAPEZE NETWORKS JUNIPER NETWORKS

Colubris NETWORKS hp

«Тонкий» контроллер

Распределенная плоскость данных

«Умные» ТД

Преимущества

- Низкие задержки
- Безопасность на ТД
- Данные передаются даже если связь с контроллером прервана
- Плоскость данных масштабируется независимо от плоскости управления и контроля

Недостатки

- Физический контроллер
- Физический контроллер вводит ограничения на масштабируемость ТД и бесшовную мобильность

Как убрать физический контроллер и его ограничения без отказа от централизованного управления?

4-е поколение WLAN

Bluesocket представляет новую технологию на рынке WLAN: vWLAN

- Привносится мощность виртуализации к WLAN
- Устраняется физический контроллер и управление помещается в VMware hypervisor
- Масштабируемость и надежность WLAN привязана к ЦОД, а не к узко-специализированному серверу
- Освобождает LAN от WLAN управления, делая возможным контроль из Облака

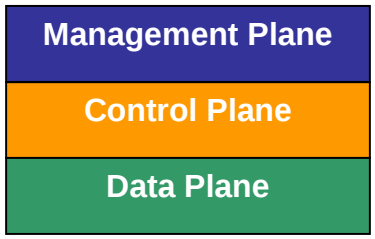
Bluesocket is первая и единственная компания которая объединила виртуализацию с управлением WLAN.
Эта инновация представляет 4-е поколение в эволюции WLAN

vWLAN

Традиционная основанная на контроллере архитектура

WLAN Controller

Точки доступа



· Три плоскости в ценральном контроллере
· Не масштабируемое решение для 11n

Архитектура vWLAN

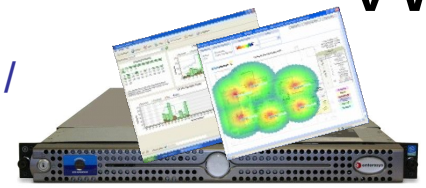
Hypervisor

Точки доступа

· Устраняется оборудование контроллера
· Перемещаются контроль и управление к гипервизору
· Перемещается плоскость данных к ТД

vWLAN

vWLAN™ Appliance / VMware



Blue: Control channel

Orange: Mobility tunnel

- **Простота**: не требуется реорганизации сети (L2 архитектура), сервер с ПО (Vmware) м.б. расположен где угодно
- **Масштабируемость**: до 48000 пользователей на одну 1U платформу vWLAN
- **Безопасность**: поддержка всех передовых индустриальных стандартов и технологий в области безопасности WLAN + гостевой доступ + L3 роуминг
- **Производительность**: максимально эффективная поддержка возможностей 802.11n

vWLAN

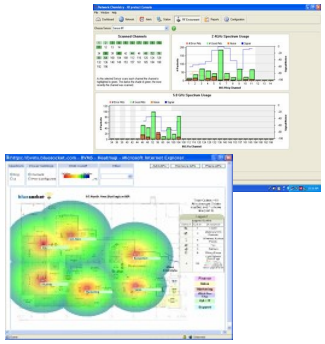
- vWLAN создает виртуальную (логическую) WLAN инфраструктуру внутри существующей проводной сети
- Весь трафик данных передается внутри проводной сети увеличивая скорость и производительность
  - Беспроводной трафик коммутируется напрямую в проводную сеть (минуя контроллер)
  - Управление ролями пользователей осуществляет центральная платформа, но пользовательские правила (безопасность, QoS, …) выполняются на границе сети (на ТД); управление сессиями осуществляет центральная платформа vWLAN
  - Трафик L3 роуминга туннелируется между ТД и подсетями проводной сети
- Платформа vWLAN обрабатывает только события «плоскости управления»
  - Координация пользовательских сессий и роуминг между ТД
  - Аутентификация пользователей
  - Управление RF и RF-IDS
  - Управление ТД и сетью

WLAN архитектуры конкурентов

- Централизованные управление и продвижение данных: Aruba, Meru, Cisco, Extricom
- Распределенные управление и продвижение данных: Aerohive, Xirrus
  - Сложность управления сигнальной информацией между ТД влияет на масштабируемость
  - Потенциально более высокая стоимость ТД
- Централизованное управление и частично распределенное продвижение данных: Juniper, HP, Siemens, Motorola
  - HP – гостевой доступ обеспечивается контроллером
  - Juniper – мобильность на L3 обеспечивается контроллером
  - Siemens – Ограниченные и не основанные на роли пользователей правила/политики на границе сети
- Централизованное управление и полностью распределенное продвижение данных: Bluesocket vWLAN

Портфолио продуктов vWLAN

Management
Software



Беспроводные службы

- Гостевой доступ
- Сканирование клиентов
- Wireless IDS
- Удаленное решение проблем (troubleshooting)
- Расширенная отчетность
- Ослеживание местоположения
- «Горячие» карты

vWLAN
Appliance
- and -
VMWare

vmware

APs	Users
1-1500	1-48,000

AP License Bundle

BlueSecure

802.11n Access Points

BSAP1800
802.11a/b/g/n
Internal Antenna

BSAP1840
802.11a/b/g/n
External Antenna

Платформа vWLAN

Bluesocket's OEM сервер

или

IBM сервер

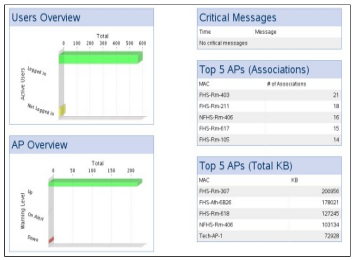
или

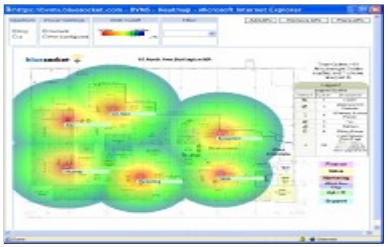
Виртуальный сервер

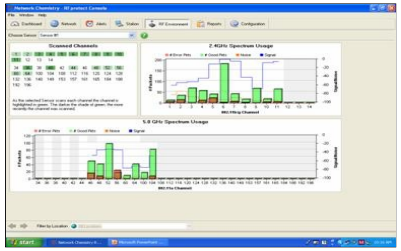
- 3 варианта поставки
- Подключение ТД через L2 или L3
- Поддержка режима резервирования (HA)

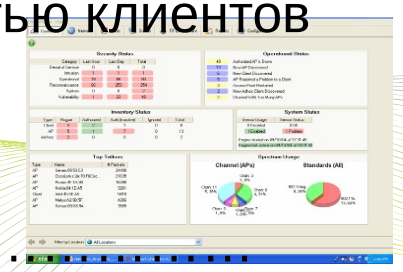
Платформа vWLAN

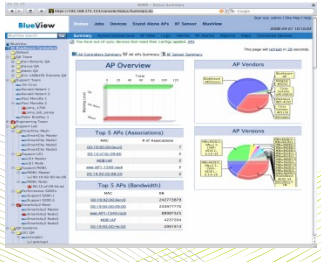
- Встроенная система управления WLAN
  - Управление BSAP (диагностика, мониторинг, …)
  - W-IDS
  - Генерация отчетов
  - Тепловые карты WLAN
- Управление аутентификацией
  - RADIUS, LDAP, AD, WEB
- Управление ролями пользователей
  - VLAN/Subnet
  - QoS/CoS
  - расписания/фильтры
- BlueProtect (Сканирование клиентов)
- Управление трафиком и скоростью клиентов
- Управление мобильностью
- Гостевой доступ
- И многое другое ……











Точки доступа BSAP 1800/1840

- Радиоинтерфейсы 802.11 a/n и 802.11 b/g/n
- До 8-ми виртуальных ТД на радиоинтерфейс
- Балансировка нагрузки беспроводных клиентов
- Безопасный, бесшовный и быстрый хэндовер/роуминг L2/L3
- До 2-х RADIUS серверов на ТД (при 802.1x)
- Режим высокой доступности (резервирования)
- WMM QoS (802.11e), DiffServ
- Конфигурирование VoIP в один клик
- Контроль приема вызова (admission control)
- Безопасность: WEP 64/128, WPA/WPA2, 802.1x, EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-TLS, EAP-SIM, EAP-AKA, 802.11i
- Конфигурируемый режим сенсора (сканирование радиоканалов)
- Интегрированная RF-IDS (обнаружение RF атак и неавторизованных ТД)

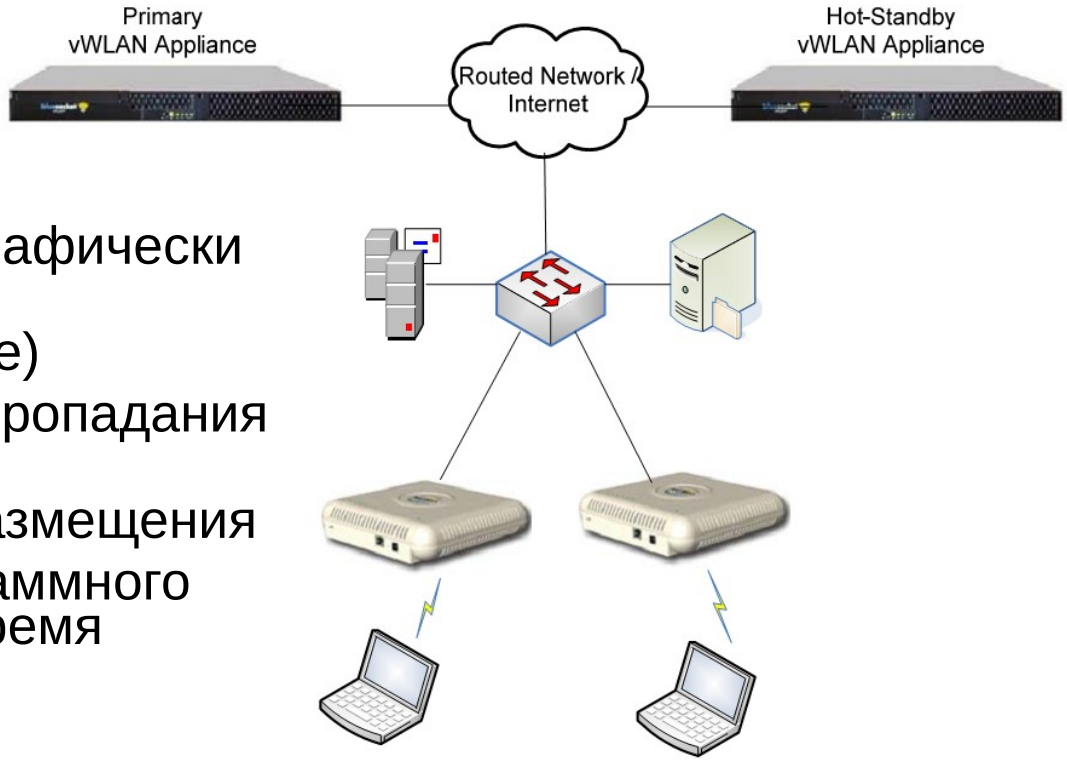
Точки доступа BSAP 1800/1840

- Антенны
  - Встроенные MIMO 3x3 в BSAP 1800
  - 6 внешних R-SMA разъемов в BSAP 1840
- Интерфейсы
  - 1 x 10/100/1000 Base T, поддержка 802.3af (PoE)
- Питание
  - Внешний адаптер переменного тока
  - 802.3af (*достаточно для полной производительности!!!*)
- Монтаж
  - К потолку или на стену (комплект включен в поставку)
- Заказные позиции
  - BSAP-1800-000-00-0 ТД 802.11 a/b/g/n, встроенные антенны
  - BSAP-1840-000-00-0 ТД 802.11 a + b/g
  - BSAP-1840-11N-00-0 ТД 802.11 a/n + b/g/n
  - BSAP-1840-LIC-11N-0 Лицензия на модернизацию 1840 a/b/g до 802.11n

Инновации и технологии

- Высокая доступность (High Availability –HA)
- Безопасность
- Управление мобильностью
- Управление RF
- Управление сетью

Платформа vWLAN: резервирование



- 1+1 Горячий резерв (географически разнесённый)
- М.б. виртуальным (vmware)
- Бесшовный переход без пропадания пакетов
- Без ограничений места размещения
- Бесшовная замена программного обеспечения в рабочее время

Многоуровневая архитектура безопасности

Identity-based

Role-based

Integrated W-IDS

Bluesocket Security Architecture

Stateful Firewall

Endpoint Complianc

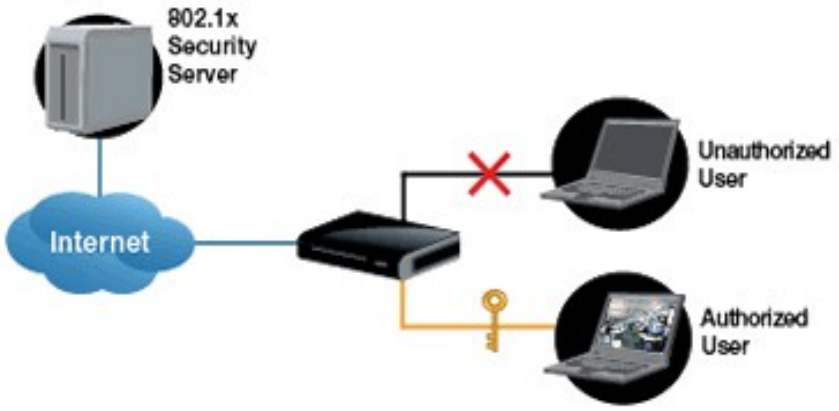
Guest Access

Встроенные функции безопасности упрощают сетевое проектирование и обслуживание

Аутентификация

- **802.1x для RADIUS/LDAP/Local пользователей**

- **Перехватывающий Web портал (Captive Portal)**
  - Полностью настраиваемый интерфейс
  - Привязка к SSID или ТД
  - Поддержка русского языка
- **Двух уровневая аутентификация**
  - Аутентификация пользователя и устройства
  - Конфигурируемое назначение роли на основе представленных атрибутов (только устройство, только пользователь и устройство/пользователь).
- **MAC- Аутентификация**
  - Включает шаблон MAC для группы устройств, таких как сканнеры.

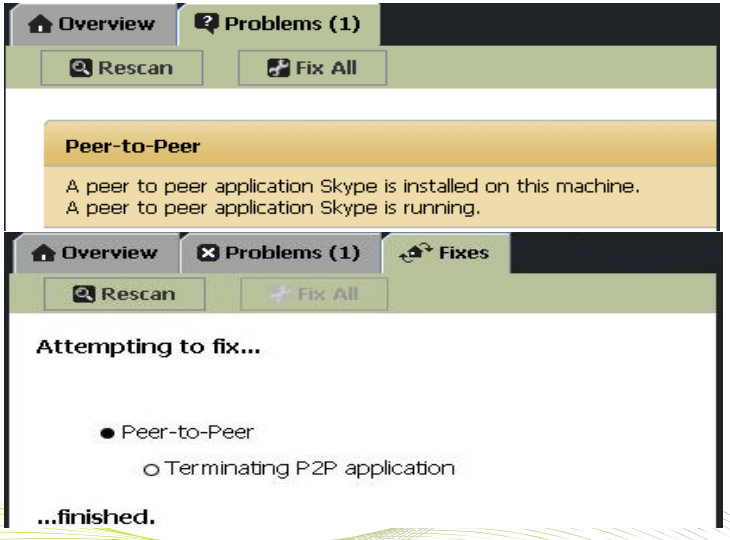


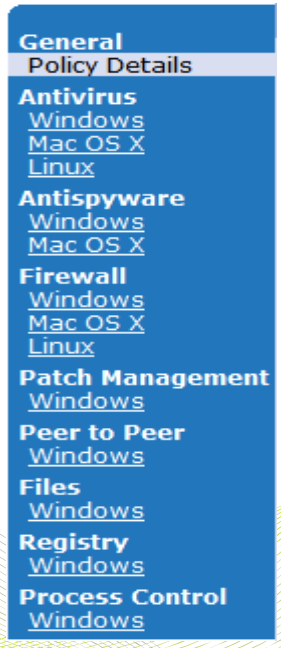
Расширенная служба гостевого доступа

- **Безопасный, простой и удобный доступ**
  - Гибкое применение правил на основе роли
  - Допуск только авторизованным гостям
- **Настраиваемый гостевой портал**
  - Интеграция с ведущими платежными системами и роуминговыми hotspot компаниями (Authorize.net, iPass/PicoPoint)
  - Функция Walled Garden обеспечивает свободный доступ к сайтам спонсоров/рекламодателей
- **«Бесконтактный» Гостевой доступ**
  - Использование аккаунтов из активных LDAP/RADIUS пользователей.
  - Получение параметров доступа по e-mail на смартфон
- **Easy deployment**
  - XML/RPC-SDK обеспечивает интеграцию с интранет, саморегистрацию и др.

Сканирование клиентов (BlueProtect)

- Скан определяет наличие и статус определенных администратором приложений безопасности
- Успешное сканирование необходимо до допуска устройства в сеть
- Авто-восстановление поддерживается для приведения блокированного клиента в соответствие.





Wireless Intrusion Detection / Prevention

- Анализ на основе поведения
- Защита от взлома и направленных атак. Примеры:
  - Rogue APs
  - De-authentication Flood
  - AP Spoof
  - Adhoc networks
  - Sniffing, network mapping, ping flooding, port scanning, tcp-session oriented attacks.

Alert Name	Enabled	Severity	Required Sensor Level
	All	All	All
AP Broadcasting Multiple SSID	Enabled	Warning	Sensor Mode Only
AP Channel Change	Enabled	Informational	Dual Mode or Sensor Mode
AP Denied Association	Enabled	Informational	Dual Mode or Sensor Mode
AP Denied Authentication	Enabled	Informational	Dual Mode or Sensor Mode
AP Down	Enabled	Informational	Sensor Mode Only
AP Low Signal Strength	Enabled	Informational	Sensor Mode Only
AP Overloaded	Enabled	Informational	Dual Mode or Sensor Mode
AP Restarted	Enabled	Informational	Sensor Mode Only
AP SSID Changed	Enabled	Informational	Dual Mode or Sensor Mode
ROGUE AP SSID Changed	Enabled	Informational	Dual Mode or Sensor Mode
AP in WDS Mode	Enabled	Informational	Dual Mode or Sensor Mode
ASLEAP Attack	Enabled	Severe	Sensor Mode Only
AirJack Attack	Enabled	Warning	Sensor Mode Only
Authorized AP Down	Enabled	Informational	Dual Mode or Sensor Mode
Broadcast Attack	Enabled	Informational	Sensor Mode Only
Client Association Change	Enabled	Warning	Dual Mode or Sensor Mode
Client BSSID Changed	Enabled	Warning	Dual Mode or Sensor Mode
Client Limit	Enabled	Informational	Dual Mode or Sensor Mode
Client Rate Support Mismatch	Enabled	Informational	Dual Mode or Sensor Mode
Client To Rogue AP	Enabled	Severe	Dual Mode or Sensor Mode
Deauthentication Flood	Enabled	Severe	Sensor Mode Only
Disassociation Traffic	Enabled	Warning	Sensor Mode Only

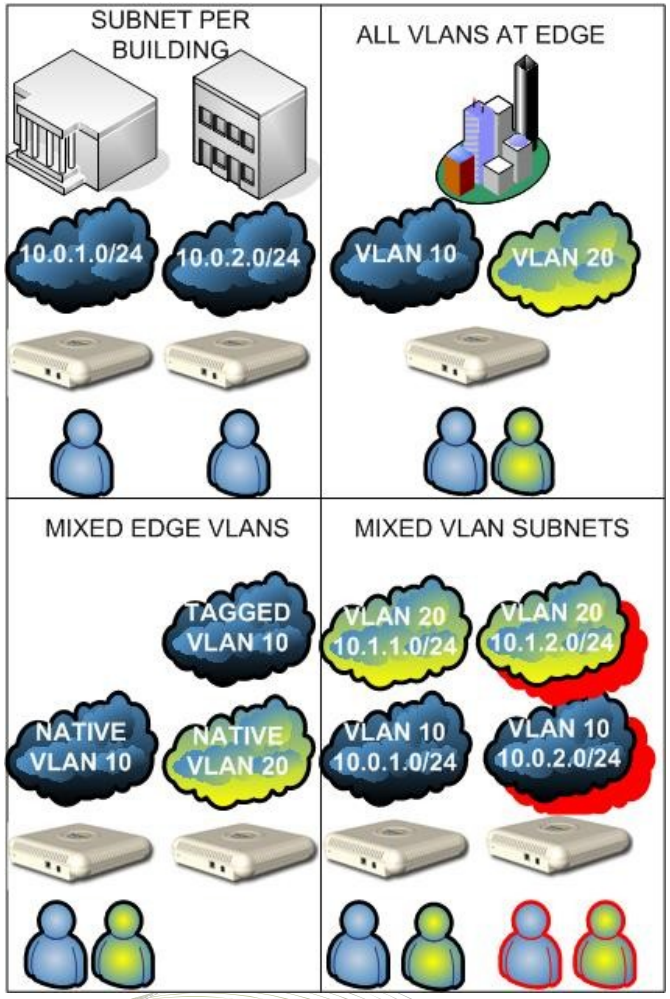
Бесшовная мобильность

L3 Mobility

- L3 мобильность через подсети достигается установкой L3 туннеля между ТД
- Централизованная служба контроля мобильности (Centralized Mobility Control Service) использует RF информацию для определения где должны быть установлены туннели, т.о. роуминг становится бесшовным.

VLAN Extension

- Если VLAN не доступен на ТД для данного пользователя, система направляет трафик к ТД, которая поддерживает этот VLAN
  - Это позволяет клиенту продолжать пользоваться службами, которые были доступны в его исходной подсети
- Гости могут быть туннелированы к ТД, которая имеет доступ к Гостевому VLAN с ближайшим интернет uplink.

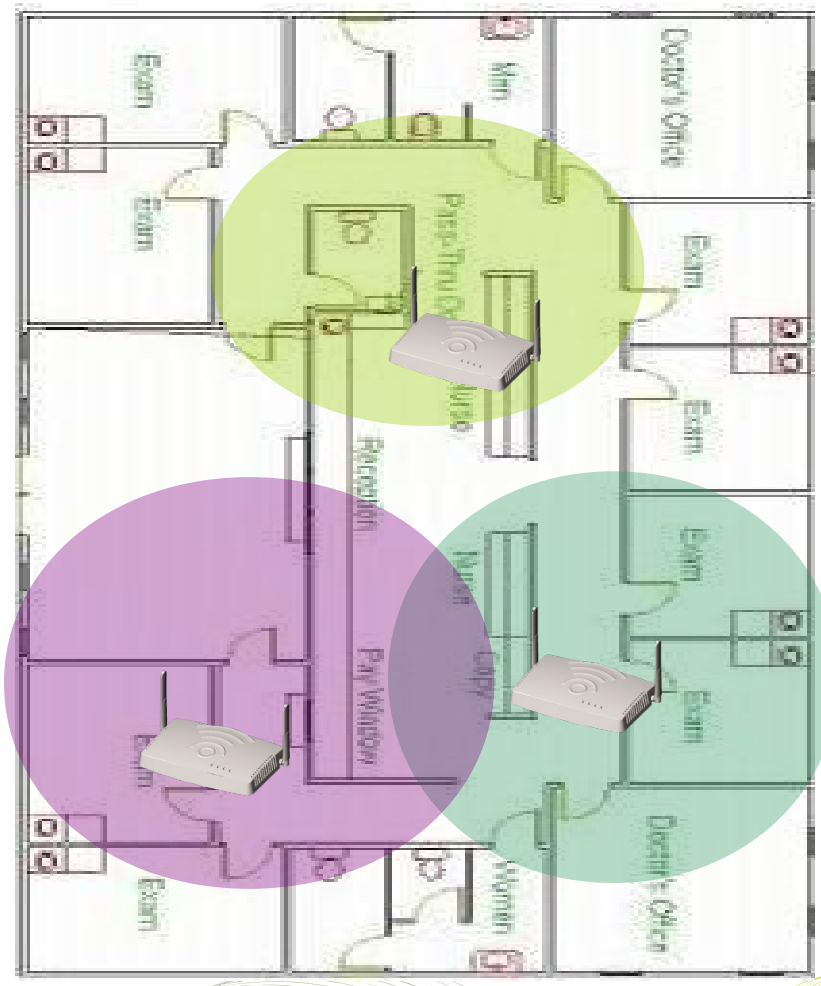


«Следуй за мной»

- **vNeighbor Control Module**
  - Интеллектуально идентифицируются соседние ТД, являющиеся вероятными кандидатами для роуминга
    - Гарантируется сохранность пользовательской сессии и ключей безопасности после роуминга (Производительность)
    - Минимизируется количество ТД сохраняющее информацию сессии пользователя (Масштабируемость)
    - Run-time optimizations based on roaming behavior
  - Используется проверенный централизованный алгоритм Dynamic RF

Управление радиопокрытием (Dynamic RF)

- Адаптивное назначение мощности и канала
  - Глобально назначаются канал и параметры мощности для всех ТД.
  - Включена поддержка для 802.11n HT20 и HT40 каналов.
- Балансировка нагрузки клиентов
- Самовосстановление при отказе ТД.

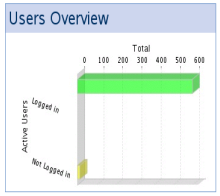


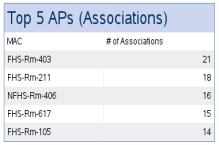
802.11n Fairness Algorithm

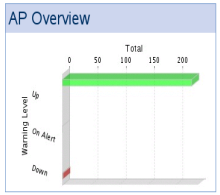
- Смешанное окружение (b, g/a, n) требует алгоритмов справедливого доступа для гарантирования оптимальной сетевой производительности.

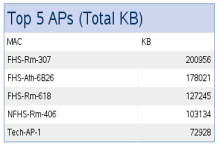
- Алгоритм Bluesocket гарантирует справедливость за счет выделения блоков передачи на ТД каждому клиенту
  - Блок передачи (Transmission unit --TU) конфигурируется как 802.11 пакеты в зависимости от клиентской емкости (11n vs 11b vs 11g/a).
  - Алгоритм работает на TU и может быть применен к любому типу клиентов (11n или наследованным).
  - Выделение TU может быть применено для QoS для трафика/клиента (i.e voice, best effort, etc)

Сетевое управление vWLAN





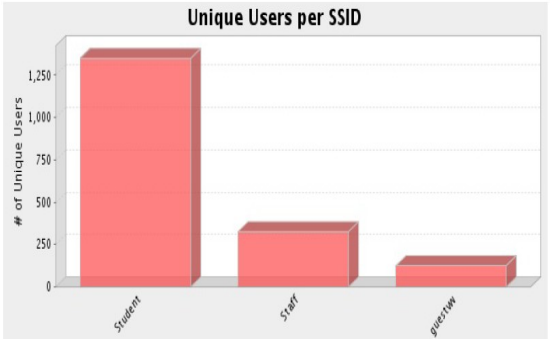




Users per SSID

2010-01-12 07:30:01

SSID	Total	Reg	Unreg	BG	A	VLAN	Bcast	Authentication	Cipher
Student	1352	1334	18	YES	YES	0	YES	WPA2	AES-CCM
Staff	325	310	15	YES	YES	0	YES	WPA2	AES-CCM
guestvw	123	26	97	YES	YES	0	YES	Open System	Disabled



Discovery
Provisioning
Maintenance
Operations
Snapshot/Rollback

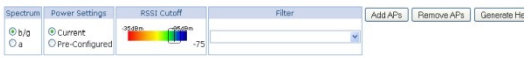
Deployment/

Policy Definition
Key Management
Authentication

Security

Location

Location Maps
RF Views



vWLAN Management Framework

Trouble-Shooting

Status/Monitoring
Logging
Remote Packet Capture
Reporting/Notifications
Alerts/Alarms

RF Manageme

Planning
Heat Maps
Monitoring
RF Optimization

3rd Party Integration

XML-RPC
SNMP
Remote Syslog

Лицензирование

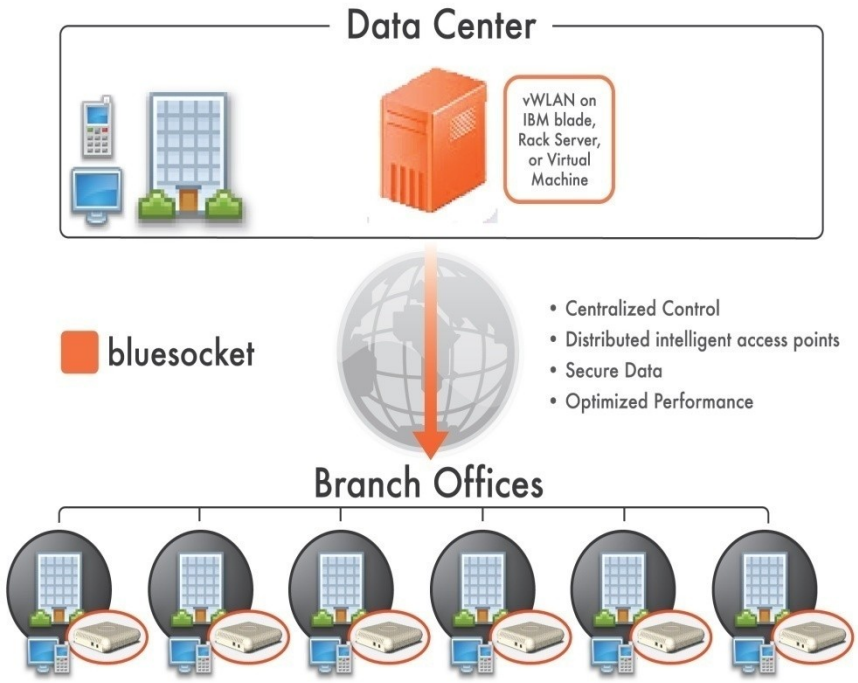
- Стоимость сети WLAN состоит из:
  - Стоимость сервера vWLAN
  - Стоимость точек доступа
  - Лицензий (по кол-ву ТД)
- Виды лицензий:
  - Базовая
  - High Availability
  - BlueProtect

Рынок Wi-Fi решений Bluesocket

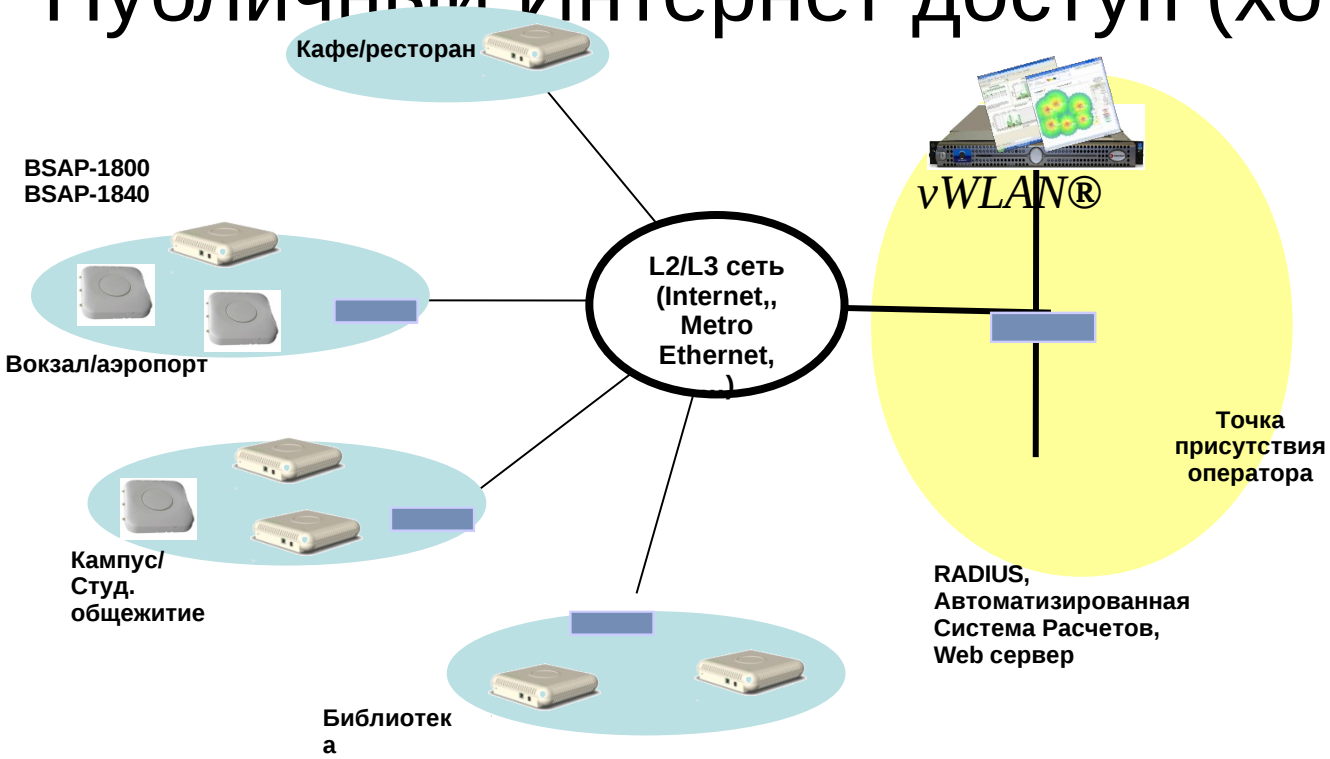
- Корпоративные WLAN
- Торговые сети, логистические компании
- Вокзалы, аэропорты
- Гостиницы
- Кафе, рестораны, зоны отдыха
- Учебные заведения, студенческие общежития
- Спортивные сооружения
- Мед. учреждения
- Места проведения деловых встреч (конференц-залы, выставки, …)
- …

Подключение филиалов предприятия

- Тенденции
  - Растет количество удаленных работников и филиалов
  - Снижение стоимости ИТ в филиалах и перемещение серверов в ЦОД
- Преимущества vWLAN для филиалов
  - Быстрое и простое развертывание сети и включение ее в ИТ инфраструктуру предприятия
  - Высокие скорости 802.11n достаточные для всех офисных приложений
  - Применение правил и управление полосой на границе оптимизируют трафик до его попадания в WAN.
  - Решение о продвижении данных делается ТД для передачи трафика к локальным ресурсам, Интернет или к головному офису



Публичный Интернет доступ (хот споты)



- Контроллер беспроводной сети устанавливается у оператора
- Точки доступа подключаются к контроллеру через L2/L3 сеть
- Контроллер обеспечивает:
  - Управление ТД
  - Web аутентификацию и авторизацию пользователей на RADIUS сервере
  - Управляет политиками безопасности и правилами доступа
  - Взаимодействует с RADIUS и ACP
- Управление учетными записями пользователей и беспроводной сетью обеспечивается через web интерфейс

Преимущества vWLAN

- Масштабируемость
  - Лучшие в отрасли показатели по количеству поддерживаемых ТД и пользователей на один контроллер
  - Плоскость данных ограничена только пропуской способностью ТД (т.е. 200Mbps*1500 APs = 300Gbps)

- Простота
  - Централизованное управляющее ПО реального времени выполняется на vWLAN платформе и масштабируется добавлением лицензий, но не оборудования
    - меньше WLAN устройств для управления и поддержки
    - Наименьшая стоимость владения
  - vWLAN использует возможности BSAP для упрощения функций отслеживания действий пользователей, высокой доступности и мобильности L3

- Безопасность
  - Bluesocket имеет передовые в отрасли наработки по обеспечению расширенной безопасности, универсальной аутентификации, гостевого доступа, W-IDS и проверки соответствия конечных устройств.
    - Правила на границе, а не на контроллере
  - Безопасность реализована как Out-of-Band NAC (внеполосной контроль доступа), что обеспечивает и безопасность и масштабируемость

- Производительность
  - Глубокая интеграция в проводную сеть позволяет обеспечивать работу приложений, чувствительных к задержкам.

vWLAN: больше пользователей, меньше «железа»

Что будет использовать предприятие как основу для масштабируемой WLAN?

Дата центр оптимизированный с VMware vWLAN

или

Стек из узко-специализированных серверов обычный основанный на контроллерах подход

Спасибо за внимание!

Наш адрес:

115114, Россия, Москва
ул. Летниковская, 11/10, стр.6

Телефон **+7 495 641 40 45**
Факс **+7 495 641 40 48**

nst@nstel.ru **www.nstel.ru**