

# Корпоративные сети Wi-Fi

**А.Г. Камайкин**, ведущий инженер ЗАО "НПЦ Дэйтлайн"

**И.Е. Осипов**, руководитель проектов ЗАО "НПЦ Дэйтлайн"

**О.Е. Шумарин**, начальник отдела сетевых технологий ЗАО "НПЦ Дэйтлайн"

За последние несколько лет произошло стремительное внедрение технологии Wi-Fi (семейство стандартов IEEE 802.11) в корпоративные сети во всем мире. Основным "двигателем" технологий Wi-Fi на рынке явилось снижение стоимости беспроводных адаптеров и как результат – быстрое развитие абонентской базы (ноутбуки, PDA, Wi-Fi-телефоны). Возможность организации и развития WLAN-сегментов сетей для территориально распределенных подразделений и обеспечение мобильного доступа сотрудников к услугам внутренних сетей и Интернета на базе технологии Wi-Fi оказались эффективным решением корпоративных задач. Поэтому неудивительно, что внедрение технологий Wi-Fi началось именно с корпоративных сетей и распространилось в дальнейшем на сети беспроводного доступа общего пользования и домашние сети. В данной статье приведены основные требования к оборудованию Wi-Fi для построения корпоративных сетей и обзор наиболее интересных решений.

## Требования к современным корпоративным сетям Wi-Fi

Из всех существующих в настоящее время технологий для построения беспроводных корпоративных сетей наиболее востребованной является Wi-Fi, так как остальные технологии либо не получили широкого применения, например CDMA/UMTS, либо не удовлетворяют требованиям по сервисам или скорости передачи данных, например GPRS. Технология WiMAX, включающая полный спектр услуг QoS, на сегодняшний день может рассматриваться как перспективная для городских сетей. Активное внедрение WiMAX сдерживается отсутствием абонентской базы (появление порта-

тивных компьютеров со встроенным чипсетом Rosedale, поддерживающим WiMAX, только планируется), высокой стоимостью оборудования и проблемами с частотным ресурсом.

Основными недостатками технологии Wi-Fi в настоящее время являются ограничение пропускной способности 54 Мбит/с (108 Мбит/с Turbo) и снижение пропускной способности вследствие коллизии при увеличении числа пользователей. Бороться с этим помогают различные механизмы: применение VLAN для сегментирования сети, использование QoS или применение в точках доступа нескольких радиомодулей (например, Proxim Orinoco AP-4000 имеет 2 радиомодуля, один из которых работает в диапазоне 2,4 ГГц (802.11b/g), а другой – в диапазоне 5,8 ГГц (802.11a)).

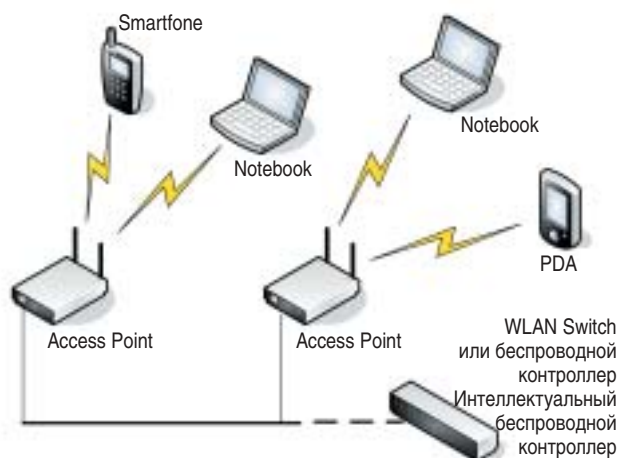
Успех сетей на основе технологии Wi-Fi объясняется простотой развертывания, дешевизной оборудования и относительно высокими скоростями передачи данных в радиоканале (до 54 Мбит/с). Для решения стоящих перед корпоративными пользователями задач сети Wi-Fi должны удовлетворять следующим требованиям:

- мобильность абонента, с организацией "бесшовного" перемещения абонента между точками доступа внутри сети (хэндовер) и меж-сетевого роуминга;
- "мультисервисность" (полный спектр IP-услуг, включая доступ в Интернет, VoIP, видеоконференц-связь и т.д.);
- безопасность (защита от нелегальных подключений).

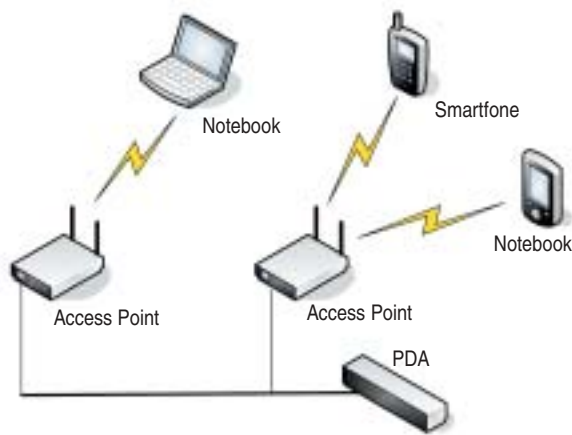
## Мобильность

В настоящее время в корпоративной среде передачи данных и голоса все более востребованной становится мобильность абонента. В России, с ее недостаточно развитой по сравнению с западными странами инфраструктурой связи (особенно на периферии), возможность организации мобильного офиса зачастую является решающим фактором в успешном ведении бизнеса. В области телефонии перспективными представляются решения, обеспечивающие интеграцию традиционных мобильных стандартов и Wi-Fi-доступа.

Технология UMA (Unlicensed Mobile Access), разработанная американской компанией Kineto Wireless, позволяет мобильному телефону переключаться с сотовой сети на сеть Wi-Fi, не прерывая разговор. Некоторые крупнейшие производители мобильных телефонов, например Samsung и LG, уже заявили о намерении использовать UMA в своих устройствах. Это, несомненно, обеспечит технологии Wi-Fi будущее не только в корпоративных сетях, но и в сетях масштаба



**РИС. 1.** Централизованная схема организации сети, в которой каждой точкой доступа управляет WLAN Switch или беспроводной контроллер



**РИС. 2.** Децентрализованная схема организации сети

города (Wireless MAN), а также послужит реальным шагом к "глобальной" мобильности абонентов на основе конвергенции сетей сотовой связи и фиксированных сетей передачи данных.

В стандарте 802.11 нет строгих спецификаций по реализации хэндовера в многосотовых сетях. Однако для обеспечения бесшовного перемещения мобильных абонентов из зоны действия одной точки доступа к другой предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения (association). Реализация хэндовера в сетях Wi-Fi может осуществляться различным образом, например на базе протокола Radius или под управлением интеллектуального беспроводного контроллера, организующего "туннель" при переходе клиента в зону обслуживания соседней точки доступа.

Объединение сетей Wi-Fi (проблема роуминга) для осуществления корпоративных задач, а в дальнейшем и объединение сетей фиксированной и мобильной связи служит решению основной задачи: возможности предоставлять корпоративным пользователям как можно более широкий ассортимент услуг по как можно более низкой цене. Отсюда встает необходимость решать задачу по организации межсетевого роуминга согласно известному принципу "один человек – один номер". При осуществлении интеграции услуг решающим фактором для выбора оборудования послужит выбор оптимальной стратегии конвергенции.

### "Мультисервисность"

В развитии сетей Wi-Fi, которые поддерживают технологии беспроводной IP-телефонии, произошел новый тол-

чок. Появились IP-телефоны со встроенными адаптерами Wi-Fi, их выбор пока невелик и цена высока, так как в них реализованы частные фирменные решения. Но после принятия, в сентябре 2005 г., стандарта IEEE 802.11e ситуация может резко измениться. Стандарт IEEE 802.11e позволяет при сохранении полной совместимости с действующими стандартами 802.11a/b/g расширить функциональность за счет обслуживания потоковых мультимедиа-данных и гарантированного качества услуг QoS.

Необходимо отметить значительную активность в использовании сетей Wi-Fi для видеоприложений и в первую очередь для систем безопасности.

### Безопасность

Для успешного применения в корпоративных сетях оборудование Wi-Fi должно обеспечивать защиту от атак и нелегальных подключений. В сети Wi-Fi абонент может быть подвергнут атакам как на беспроводном сегменте сети (IP и MAC spoofing и т.д.), так и на проводном (DHCP и ARP-spoofing и т.д.).

Для надежной защиты на беспроводном сегменте сети в настоящее время уже недостаточно использования протокола WPA (802.1x/EAP) – аутентификации и кодирования трафика. Стандарт IEEE 802.11i предусматривает использование в продуктах Wi-Fi таких средств, как поддержка алгоритмов шифрова-

ния трафика: TKIP (Temporal Key Integrity Protocol), WRAP (Wireless Robust Authenticated Protocol) и CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol). Этих алгоритмов достаточно для защиты на уровне абонентского трафика, но на уровне корпоративного пользователя используются дополнительные механизмы, включающие более совершенные способы аутентификации при подключении к сети: более криптостойкие методы шифрования, динамическую замену ключей шифрования, использование персональных межсетевых экранов, мониторинг защищенности беспроводной сети, технологию виртуальных частных сетей VPN и т.д.

### Особенности организации сетей беспроводного доступа по технологии Wi-Fi

Корпоративные сети беспроводного доступа по технологии Wi-Fi условно можно разделить на внешние (Outdoor) (табл. 1) и внутриофисные (Indoor) (табл. 2). При построении внешних сетей необходимо получение Решений ГКРЧ и частотных разрешений. При построении внутренних сетей процедура упрощена: если оборудование

ТАБЛИЦА 1. Основные технические характеристики внешнего оборудования Wi-Fi

Производитель	Torus		Strux		BelAir		Aruba	
	Оборудование	Торос 4210	OWS 2410	OWS 3600	BelAir50	BelAir100	BelAir200	AP -80
Характеристики	Стандарт	802.11b/g	802.11a/g	802.11a/g	802.11b/g	802.11a/b/g	802.11a/b/g	802.11a/b/g
Выходная мощность передатчика, дБм	26-36	26-36	До 30	До 30	27	27 (2,4 ГГц); 17 (5,8 ГГц)	27 (2,4 ГГц); 14 (5,8 ГГц)	До 20
Чувствительность приемника, дБм (RX Sensitivity)	-100 (1 Мбит/с); -76 (54 Мбит/с)	-100 (1 Мбит/с); -77 (54 Мбит/с)	Н/д	Н/д	-96 (1 Мбит/с); -71 (54 Мбит/с)	2,4 ГГц: -90 (1 Мбит/с); -71 (54 Мбит/с); 5,8 ГГц: -90 (6 Мбит/с); -71 (54 Мбит/с)	2,4 ГГц: -90 (1 Мбит/с); -71 (54 Мбит/с); 5,8 ГГц: -90 (6 Мбит/с); -71 (54 Мбит/с)	Н/д
Средства безопасности	WPA (64-152 WEP), ESSIDs, AES-шифрование	WPA (64-152 WEP), ESSIDs, AES-шифрование	WPA (WEP) AES	WPA (WEP) AES	WPA (64-128 WEP), AES-шифрование	WPA (64-128 WEP), AES-шифрование	WPA (64-128 WEP), AES-шифрование	WEP (40/64/128/ 152 бит), TKIP, AES
Управление	HTTPS, SNMP V2c	HTTPS, SNMP V2c	HTTPS, SNMP	HTTPS, SNMP	HTTPS, SNMP V2	HTTPS, SNMP V2	HTTPS, SNMP V2	CLI, WEB GUI, SNMP
Сетевые интерфейсы	10/100Base-TX (2); Type-A USB (2)	10/100Base-TX (1)	10/100Base-TX (1)	10/100Base-TX (1)	10/100Base-TX (1)	10/100Base-TX (1); 10/ 100Base-FX (1) (Optical)	10/100Base-TX (1); 10/ 100Base-FX (1) (Optical)	10/100Base-T Ethernet RJ-45 с поддержкой PoE
Поддерживаемые протоколы	TCP+VPN, VLAN, NAT, Layer 2, 3, DHCP QoS	TCP+VPN, VLAN, NAT, Layer 2, 3, DHCP QoS	Н/д	Н/д	TCP+VPN, Layer 2, SNTP	TCP+VPN, Layer 2, SNTP	TCP+VPN, Layer 2, 3, DHCP, QoS	TCP/IP, DHCP, VLAN
Антенны	2 антенны. Только внешние. Разнесенный прием	2 антенны. Только внешние. Разнесенный прием	2 (4) антенны. Только внешние. Разнесенный прием	2 (6) антенны. Только внешние. Разнесенный прием	Внешние антенны (2)	Интегрированные антенны (2). Разнесенный прием	Интегрированные антенны (8). Разнесенный прием	Интегрированные антенны
Подключение доп. внешних антенн	Да	Да	Да	Да	Да	Да	Да	Да
Диапазон рабочих температур, °C	От -40 до +70	От -40 до +55	От -40 до +55	От -40 до +55	От -40 до +50	От -40 до +50	От -40 до +50	От -30 до +50
Сертификат Мининформсвязи России	В стадии сертификации	В стадии сертификации	Подлежит сертификации	Подлежит сертификации	Подлежит сертификации	Подлежит сертификации	Подлежит сертификации	В стадии сертификации
Особенности	Мобильная (монтаж в автомобиле)	Стационарная	До 4 радиомодулей. Полный дуплекс	До 6 радиомодулей. Полный дуплекс	1 радиомодуль	2 радиомодуля	4 радиомодуля. Полный дуплекс	2 радиомодуля

указано в Приложении № 2 Решения ГКРЧ № 04-03-04-003 от 06.12.2004 или внесено в перечень оборудования последующими решениями ГКРЧ, то достаточно регистрации сети в местном радиочастотном центре.

Качество сети во многом определяется качеством проектирования. При развертывании внутриофисных сетей Wi-Fi необходимо провести радиоразведку для обеспечения уверенного приема сигнала во всей требуемой зоне обслуживания и для минимизации количества устанавливаемых точек доступа. При проведении радиоразведки используется одна из точек доступа оборудования, предполагаемого к установке, и программно-аппаратный измерительный комплекс. Этот комплекс состоит из портативного компьютера, оснащенного Wi-Fi-адаптером, и специализированного программного обеспечения, например, хорошо зарекомендовавшей себя Ekahau. Проведение подобных работ особенно актуально на объектах большой протяженности со сложной геометрией помещений, толстыми стенами, зеркалами и т.д.

Варианты схем организации внутриофисных сетей Wi-Fi в зависимости от оборудования показаны на рис. 1 и 2.

Задача организации корпоративных распределенных сетей с большой зоной обслуживания (в пределах города или региона) решается в рамках стандарта 802.11 путем реализации MESH-топологии (рис. 3), основанной на децентрализованной схеме построения, где каждая точка доступа выполняет функции на уровне Layer 2, 3.

Подобная сеть во многом повторяет сотовую архитектуру. В одной соте могут располагаться от 10 до 30 точек доступа. Одна из таких точек – "узловая" подключается к магистрали по оптическому либо проводному кабелю. Узловая точка доступа, так же как и остальные точки доступа в соте, соединяются между собой по транспортному радиоканалу. В зависимости от конкретного решения точки доступа могут выполнять только транспортные функции, либо только функции абонентского доступа, либо обе функции одновременно. Особенностью MESH является использование специальных протоколов, позволяющих контролировать состояние транспортного канала и поддерживать динамическую маршрутизацию по оптимальному маршруту между точками доступа. При отказе какой-либо точки происходит автоматическое перенаправление трафика по другому маршруту, что гарантирует не только доставку тра-

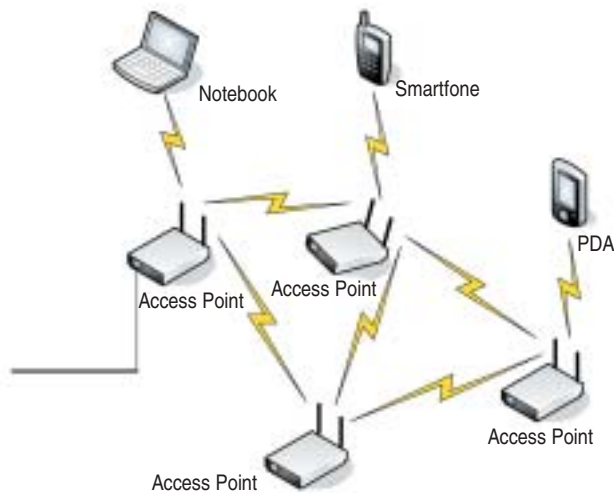


РИС. 3. Организации сети по MESH-топологии

фика адресату, но и доставку с максимальной скоростью. Принятие стандарта 802.11s (де-факто описывающего решение MESH) ожидается в 2007 г.

Особенности организации и использования сетей с топологией MESH определяются социальной и коммерческой целесообразностью. На основе сетей MESH созданы и эффективно работают муниципальные, полицейские, emergency-службы. При этом реализован весь спектр IP-приложений – Ethernet, VoIP, real time video. Использование мобильных точек доступа (установленных на автомобилях) позволяет в считанные минуты организовать исчерпывающее информационное обеспечение "горячей точки".

Абонентское использование подобных сетей становится выгодным при достаточно большом числе пользователей и на сегодняшний день определяется не техническими, а экономическими аспектами.

При создании внешних сетей Wi-Fi приходится сталкиваться с проблемами, ставшими уже традиционными:

- наличие частотных ресурсов (частотные диапазоны 802.11 в крупнейших городах России практически исчерпаны);
- радиочастотное планирование сети в условиях работы при крайне загруженных диапазонах (особенно в диапазоне 2,4 ГГц);
- организация доступа и размещение точек доступа в максимальной близости от абонентов.

### Краткий обзор оборудования

#### Внешние сети

Первоначально оборудование Outdoor не поддерживало MESH-тополо-

гию. Но сейчас большинство производителей Wi-Fi-оборудования представляют решения с поддержкой этой топологии, которая позволяет значительно увеличить зоны обслуживания беспроводных сетей без существенного увеличения затрат (см. табл. 1).

**Aruba Networks** представляет точку доступа AP 80, предназначенную

для наружного монтажа, которая работает исключительно под управлением контроллера Aruba (Aruba Mobility Controller). AP 80 построена на основе двух радиомодулей 802.11a и b/g, что позволяет при одновременном использовании частотных диапазонов 2,4 и 5,8 ГГц применять AP 80 в качестве моста в схеме "точка – точка" и точки доступа в многоточечной схеме. В модификации AP-80S устройство содержит направленную панельную антенну для диапазона 5 ГГц и два разъема для подключения антенн диапазона 2,4 ГГц. Модель AP-80M имеет по одному разъему для подключения антенн диапазонов 2,4 и 5 ГГц. Подключение внешних антенн позволяет формировать необходимую зону обслуживания сети.

**Tropos Networks** (США) – крупнейший производитель оборудования топологии MESH, выпускает линейку оборудования, в состав которой входят точки доступа 5210 (стационарный), 4210 (мобильный), 3210 (внутри-офисный). Характеристики чувствительности –

одни из лучших среди оборудования с топологией MESH. На практике сеть состоит из беспроводных точек доступа Tropos MetroMesh, число которых в сети может достигать нескольких тысяч. MetroMesh-маршрутизаторы помимо функциональных возможностей точек доступа Wi-Fi передают данные по радиоканалу к центральному шлюзу (gateway), соединенному с проводной сетью масштаба WAN или Интернетом. При добавлении в сеть дополнительных маршрутизаторов Tropos MetroMesh они устанавливают связи с соседними устройствами и центральным шлюзом. Система самотестируется и создает динамические таблицы оптимального маршрута. При этом в отличие от обычных точек доступа стандарта 802.11 обратный маршрут выбирается по критерию максимальной полосы пропускания.

**BelAir Networks** (Канада) предлагает линейку оборудования, основу которой составляют три типа outdoor точек доступа BelAir50c, BelAir100, BelAir200. Они имеют широкий спектр характеристик, позволяющих оптимизировать состав оборудования в соответствии с задачей. В зависимости от модели в устройствах установлено от 1 до 4 радиомодулей, обеспе-

ТАБЛИЦА 2. Основные технические характеристики внутриофисного оборудования Wi-Fi

Производитель	Proxim	Aruba	Cisco	Symbol	Colubris
Оборудование	Orinoco AP-4000M	Aruba AP-70	Airospace серии 1000	Symbol AP 300	InReach™ MultiService AP MAP-320
Характеристики					
Стандарт	802.11a/b/g	802.11a/b/g	802.11a/b/g	802.11a/b/g	802.11a/b/g
Выходная мощность передатчика, дБм	До 20	До 20	До 20	До 20	До 20
Чувствительность приемника, дБм	Н/д	Н/д	-73 (54 Мбит/с при BER=10 <sup>-5</sup> )	Н/д	Н/д
Средства безопасности (шифрование)	IEEE 802.11 WEP, MAC Access Control, RADIUS, IEEE 802.1x Authentication, WPA, RAPD, PUPS Encryption	WEP (40/64/128/152 бит), TKIP, AES	WPA, WPA2	VPN, WPA2, 802.1x Authentication, TKIP, AES	WEP, WPA, WPA2, MAC Access Control, 802.1x Authentication
Управление	SNMP, TFTP, Telnet/CLI, WEB	CLI, WEB GUI, SNMP	SNMP, Telnet/CLI, WEB	SNMP, Telnet/CLI, WEB	CLI, WEB GUI, SNMP
Сетевые интерфейсы	10/100Base-TX, RJ-45 с поддержкой PoE, RS-232C	10/100Base-T Ethernet, RJ-45 с поддержкой PoE	10/100Base-T Ethernet, RJ-45 с поддержкой PoE	10/100Base-T Ethernet, RJ-45 с поддержкой PoE	10/100Base-T Ethernet, RJ-45 с поддержкой PoE
Поддерживаемые протоколы	TCP/IP, DHCP, IAPP, Syslog, RADIUS, Virtual LAN	TCP/IP, DHCP, VLAN	TCP/IP, DHCP, VLAN	TCP/IP, DHCP, VLAN	TCP/IP, DHCP, VLAN
Антенны	Интегрированные антенны	Интегрированные антенны	Интегрированные антенны	Интегрированные антенны	2 внешние антенны, разнесенный прием
Подключение доп. внешних антенн	Да	Да	AIR-AP1010-х-K9: нет. AIR-AP1020-х-K9 и AIR-AP1030-х-K9: да	Нет	Нет
Диапазон рабочих температур, °C	От 0 до +45	От 0 до +50	От 0 до +50	От 0 до +40	От 0 до +50
Сертификат Мин-информсвязи России	В стадии сертификации	В стадии сертификации	Н/д	Н/д	Н/д

чивающих работу в стандарте 802.11a/b/g/. Старшая модель (BelAir200) обеспечивает полнодуплексный транспорт и абонентский доступ. Функции организации сети на уровне Layer 2 и Layer 3 (только BelAir200).

**Stryx Systems Inc.** (США) наряду с традиционными решениями для сетей с топологией MESH активно работает в сегменте задач, требующих информационного обеспечения быстро движущихся объектов (до 300 км/ч), например железнодорожного транспорта. Оборудование обеспечивает беспроводную передачу транспортного и абонентского трафика стандарта 802.11a/b/g в режимах полудуплекса (модель OWS 2400-10) и полного дуплекса (старшие модели серии OWS 2400 и OWS 3600).

Особенностью OWS является динамический выбор каналов передачи, что позволяет снизить влияние интерференционных помех на работу сети с топологией MESH. Для всех моделей предусмотрено централизованное конфигурирование по Manager/One или SNMP.

Все модели выполняют сетевые функции на уровне Layer 3 с поддержкой большинства существующих switching и routing сетевых протоколов, таких, как VPN, VLAN, OSPF, RIP Multicast и другие. На сервисном

уровне реализован механизм приоритизации трафика, что обеспечивает уверенную передачу голосовых и видеоприложений.

Система безопасности в стандартном варианте предполагает идентификацию пользователя, шифрование служебного и абонентского трафика, контроль сетевой активности.

### Внутриофисные сети

**Cisco** предлагает оборудование семейства Airespace, представляющее собой решение для построения беспроводной сети, с централизованным управлением распределенными точками доступа при помощи контроллера беспроводной сети, благодаря этому повышается безопасность работы всей сети в целом. По сравнению с классической организацией беспроводной сети данное решение имеет следующие преимущества:

- единая система организации WLAN;
- высокая производительность;
- встроенная система отслеживания перемещений;
- улучшенная система сетевой безопасности;
- простота управления беспроводной сетью большого масштаба.

В основе работы беспроводной сети на оборудовании Cisco Airespace лежит организация радиодомена (RF Do-

main), который условно можно разделить на 3 уровня: уровень данных, контрольный уровень, уровень управления. На уровне данных работают непосредственно устройства Cisco Airespace, на контрольном уровне – Radio Resource Manager (RRM), осуществляющий поддержку перемещения абонентов, управление загрузкой пользователей, обнаружение и противодействие несанкционированным вторжениям в сеть, автоматическое управление каналами и выходной мощностью и т.д., на уровне управления находятся Cisco Wireless Control System (WCS) и Cisco Wireless Location Appliance.

В качестве контроллеров беспроводной сети (Cisco WLAN Controller) могут использоваться WLC 2000, WLC 4100, WLC 4400, а в качестве распределенных точек доступа – устройства Cisco Airespace серии 1000: Cisco 1010 Lightweight Access Point, Cisco 1020 Lightweight Access Point, Cisco 1030 Remote Edge Access Point.

**Aruba Networks** представляет линейку контроллеров мобильных подключений сети и точку доступа AP 70. Для управления сетью Aruba Networks выпускаются четыре типа контроллеров мобильных подключений, рассчитанных на обслуживание от 16 до 512 точек доступа и имеющих пропускную способность процессора шифрования

от 200 Мбит/с до 7,2 Гбит/с. Контроллеры выполняют функции управления и обеспечения безопасности сети, а также обеспечивают внутрисетевой роуминг мобильных пользователей и содержат firewall, VPN-сервер и систему позиционирования.

Контроллер Aruba 6000 включает встроенный firewall стандарта сертификации ICSA и собственный процессор шифрования с пропускной способностью в 7,2 Гбит/с. Общая пропускная способность контроллера составляет 8 Гбит/с. Контроллер поддерживает до 512 точек доступа и до 8000 подключений одновременно.

Контроллер Aruba 5000 представляет собой масштабируемую архитектуру на основе мощного процессора шифрования пропускной способности в 7,2 Гбит/с для обслуживания до 256 точек доступа и до 8000 пользователей и включает ICSA-сертифицированный firewall.

24-портовый контроллер Aruba 2400 позволяет обслуживать до 48 точек беспроводного доступа и до 512 пользователей одновременно. Контроллер имеет два внешних порта Gigabit Ethernet (GBIC). При пропускной способности внутреннего контроллера шифрования в 400 Мбит/с и общей информационной емкости коммутатора в 2 Гбит/с Aruba 2400 подходит для информационного обеспечения локальной беспроводной сети крупного офиса или штаб-квартиры предприятия.

Контроллер мобильных подключений Aruba 800 предназначен для небольших сегментов беспроводной сети. Устройство поддерживает подключение 16 точек доступа и имеет один внешний порт Gigabit Ethernet (GBIC). Встроенная в Aruba 800 система шифрования обеспечивает пропускную способность в 200 Мбит/с.

Точка доступа AP 70 работает в двух частотных диапазонах 2,4 и 5 ГГц, обеспечивает поддержку стандартов 802.11a и 802.11b/g, а также предоста-

вляет безопасный проводной доступ через дополнительный Ethernet-порт.

**Symbol Technologies** представила новый беспроводной коммутатор WS 2000 и точку беспроводного доступа AP 300 с поддержкой протоколов 802.11a/b/g. Оборудование предназначено для предприятий малого и среднего бизнеса.

Новая версия коммутатора WS 2000 дополнена возможностями балансирования нагрузки, а также поддержкой виртуальных частных сетей VPN и стандартов 802.11i (WPA2), 802.11a/b/g и 802.11h. Точка доступа AP 300 совместима с протоколами 802.11a/b/g и позволяет передавать данные на скорости до 54 Мбит/с с возможностью удвоения скорости до 108 Мбит/с для таких приложений, как передача потоковых видеоданных. Устройство не требует прокладки силовых кабелей, поскольку может получать питание по кабелям уже существующих сетей Ethernet. Кроме того, модель AP 300 дополнена поддержкой виртуальных точек доступа, позволяющей каждому из портов выступать в качестве независимой точки доступа, что повышает производительность, пропускную способность сети и время действия батареи, а также снижает общий сетевой трафик.

**Colubris Networks** предлагает линейку оборудования InReach™ Multi-Service Access Points (MAP). Управление точками доступа MAP-320 и MAP-330 осуществляется при помощи многофункционального WLAN-коммутатора, который поддерживает распределенную архитектуру сети, удерживая данные в точке доступа. Такая архитектура увеличивает масштабируемость сети, позволяя одному контроллеру в сети обслуживать 200 точек доступа и тысячи пользователей, не создавая "узкие места" при передаче данных.

**Proxim** в линейке оборудования OriginO предлагает точки доступа AP-4000M, которые являются разви-

тием известного решения для внутриофисных сетей на основе точек доступа AP-4000. С использованием AP-4000M, каждая из которых, как и AP-4000, содержит два радиомодуля (802.11 a/b/g), теперь возможно построение беспроводных сетей по MESH-топологии. Дальнейшим развитием решения AP-4000M являются анонсированные фирмой Proxim точки доступа AP-4000R для внешних сетей Wi-Fi.

## Заключение

В связи с бурным развитием рынка беспроводного оборудования Wi-Fi, удешевлением беспроводных адаптеров и применением их в самых разнообразных абонентских устройствах использование технологии Wi-Fi в корпоративных системах связи многими специалистами оценивается как наиболее перспективное. Наряду с традиционными решениями беспроводного офиса, Wi-Fi активно внедряется в решения специализированных корпоративных задач (склад, телеметрия, система безопасности). В ближайшие годы не стоит ожидать конкуренции между технологиями WiMAX и Wi-Fi в силу ряда причин, наиболее существенными из которых в условиях России являются отсутствие единого частотного диапазона под системы WiMAX на всей территории России и высокая цена вследствие пока еще недостаточной технической проработки и относительно малого количества выпускаемого оборудования. К тому же, судя по наметившейся тенденции по конвергенции фиксированных и мобильных сетей, системы WiMAX и в дальнейшем не будут заменять или вытеснять сети Wi-Fi в корпоративном секторе, скорее всего, будет происходить интеграция сетей на новом уровне. ■

Ваше мнение и вопросы по статье присылайте по адресу [tss@Groteck.ru](mailto:tss@Groteck.ru)