

БЕСПРОВОДНОЕ РЕШЕНИЕ CISCO ДЛЯ МАЛЫХ И СРЕДНИХ ОПЕРАТОРОВ

Сергей Полищук,
sepolisc@cisco.com

ВВЕДЕНИЕ

Спустя почти 20 лет после появления первых промышленных образцов технология беспроводных локальных вычислительных сетей (ЛВС) достигла зрелости. Медленные, дорогостоящие и часто несовместимые друг с другом системы уступили место основанному на стандартах оборудованию, предоставляющему пользователям надежное, безопасное и недорогое беспроводное подключение к сети на скоростях Ethernet.

Беспроводные ЛВС позволяют пользователям иметь доступ к сети не только со своего рабочего места, но и из общественных мест — из конференц-залов, кафе, аэропортов. Удобства и преимущества, связанные с мобильностью доступа к сетевым ресурсам, помогают людям стать более продуктивными.

В связи с этим все большее число компаний применяет мобильные технологии, например ноутбуки с беспроводными адаптерами и клиенты виртуальных частных сетей, для обеспечения доступа своих сотрудников к корпоративным данным не только на рабочем месте, но и за пределами офиса.

Согласно исследованию компании In-Stat/MDR, проведенному в конце 2002 г., за пределами офиса проводят значительную часть своего рабочего времени 78 миллионов мобильных профессионалов, и эта цифра возрастет до 106 миллионов к 2006 г.

Обслуживание мобильных профессионалов составляет значительную долю бизнеса отелей, аэропортов и других общественных предприятий¹. И все больше и больше таких клиентов нуждается в надежном высокоскоростном доступе в Интернет из номеров гостиниц, из конференц-залов, из кафе и других общественных мест. В условиях жесткой конкуренции между общественными предприятиями предоставление клиентам востребованных услуг связи стало конкурентным преимуществом, повышающим лояльность существующих клиентов, привлекающим новых и дающим дополнительную прибыль.

Это привело к бурному росту рынка общественного беспроводного доступа и широкому распространению так называемых “хот-спотов” (hot spots). По оценкам In-Stat/MDR, хот-споты уже можно найти более чем в 12 000 отелей, аэропортов и других общественных предприятий по всему миру. В 2004 г. их количество достигнет 56 000, а в 2006 г. — превысит 113 000. Предприятия,

1. Поскольку эти предприятия предоставляют услуги связи, в дальнейших разделах они называются операторами.

предложившие услуги беспроводного доступа раньше конкурентов, захватят большую долю доходного рынка услуг для мобильных профессионалов и получают дополнительные источники прибыли.

СТРУКТУРА ДОКУМЕНТА

Настоящий документ состоит из двух основных разделов. Первый раздел описывает ключевые продукты, составляющие беспроводное решение общественного доступа Cisco для малых и средних операторов, и их преимущества. Второй раздел содержит обобщенные варианты построения сетей, включающих такие продукты, и рекомендации по их применению.

Приложение к документу содержит определения основных технических терминов, используемых в документе, и расшифровку условных обозначений.

КОМУ АДРЕСОВАН ДОКУМЕНТ

Документ адресован разным группам читателей и допускает различные акценты и глубину прочтения. Например, IT-менеджер, ознакомившись с вводными частями каждого раздела, получит общее представление о возможностях беспроводных решений Cisco для построения сетей общественного беспроводного доступа. Сетевому инженеру или администратору может быть полезно прочесть документ полностью, чтобы получить более подробную информацию о решениях и составляющих его продуктах, а также ознакомиться с их возможными вариантами внедрения.

РЕШЕНИЯ CISCO ДЛЯ ПОСТРОЕНИЯ СЕТЕЙ ОБЩЕСТВЕННОГО БЕСПРОВОДНОГО ДОСТУПА

Решения Cisco позволяют общественным предприятиям повысить прибыль путем предоставления своим клиентам услуг высокоскоростного беспроводного доступа, повысить лояльность уже существующих клиентов и привлечь новых.

Предоставление услуг общественного беспроводного доступа, как минимум, требует применения технологий локальных вычислительных сетей (беспроводных и проводных), технологий территориально распределенных сетей,

технологий контроля доступа. Cisco предлагает интегрированные решения, включающие в себя все эти технологии, обеспечивая высокую производительность и безопасность во всей сети (end-to-end).

Как и любая другая сеть, сеть беспроводного доступа должна базироваться на надежной, масштабируемой и высокопроизводительной сетевой инфраструктуре. К ней относятся маршрутизаторы Cisco и коммутаторы Cisco Catalyst, поддерживающие широкий спектр функций для передачи данных, голоса и видео в сочетании с функциональностью обеспечения безопасности.

К ключевым компонентам, специфичным для сетей общественного беспроводного доступа, относятся беспроводная инфраструктура и средства управления доступом.

Дальнейшие разделы рассматривают эти компоненты более подробно.

ОБЗОР БЕСПРОВОДНЫХ ПРОДУКТОВ CISCO

Главной задачей беспроводной инфраструктуры является обеспечение доступа мобильных абонентов к ресурсам проводной сети, в том числе к Интернет. Ключевыми устройствами беспроводной инфраструктуры сетей хот-спотов являются точки радиодоступа. Эти устройства, установленные в конференц-залах, кафе, бизнес-центрах и других общественных местах, взаимодействуют с абонентскими беспроводными сетевыми адаптерами, обеспечивая мобильным пользователям доступ в сеть на скоростях, сопоставимых со скоростью проводной сети офиса.

В зависимости от специфики конкретной инсталляции также могут потребоваться радиомосты, внешние антенны и аксессуары, клиентские беспроводные адаптеры, а также средства управления беспроводной сетью.

Точки радиодоступа Cisco Aironet

Точки радиодоступа служат в качестве моста между беспроводной и проводной сетями, позволяя мобильным абонентам получать доступ к ресурсам, расположенным в проводной сети. При наличии нескольких точек радиодоступа мобильные абоненты могут перемещаться между зонами их радиопокрытия, сохраняя связь с проводной сетью (рис. 1).

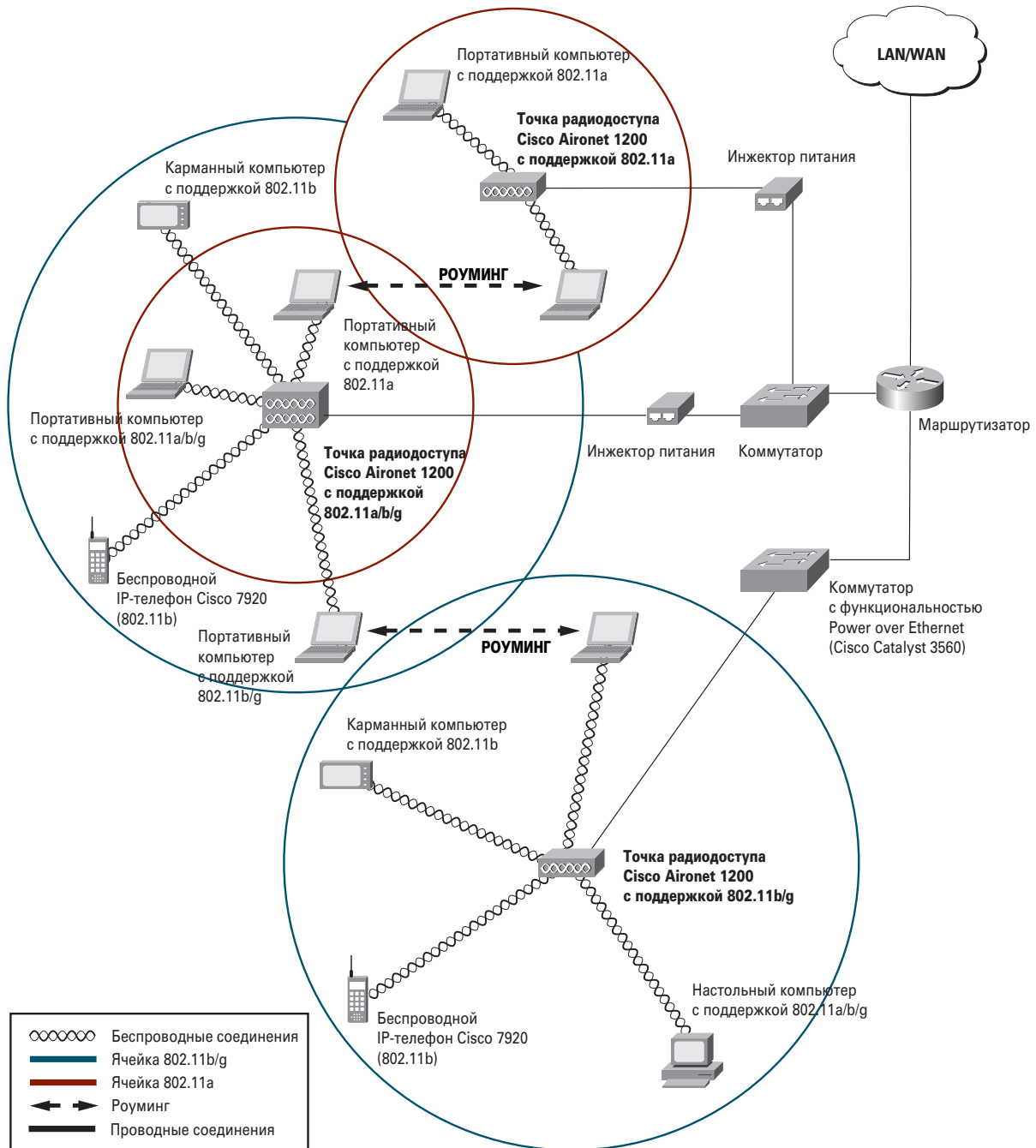


Рис. 1 Роуминг в беспроводной ЛВС

Современные точки радиодоступа Cisco представлены сериями Aironet 1200 и Aironet 1100. Устройства обеих серий обладают функциями и преимуществами, описанными в разделе “Преимущества решения Cisco”. Кроме того,

функциональность точки радиодоступа поддерживается и сериями радиомостов Aironet 1300, рассмотренной в разделе “Радиомосты Cisco Aironet”.

Cisco Aironet 1200



Точки радиодоступа серии Aironet 1200 обеспечивают безопасность, управляемость, возможность модернизации и надежность, необходимые для создания современных высокопроизводительных беспроводных ЛВС. Поддерживая работу в частотных диапазонах 2,4 ГГц и 5 ГГц одновременно, Cisco Aironet 1200 защищает инвестиции, сделанные в уже имеющееся оборудование стандарта IEEE 802.11b, и открывает путь к переходу на технологии IEEE 802.11a и IEEE 802.11g. Модульная конструкция устройств поддерживает одно- и двухдиапазонные конфигурации, а также позволяет потребителю самостоятельно менять эти конфигурации по мере изменений требований к ним и развития технологий. Защита инвестиций обеспечивается и возможностью модернизации программного обеспечения Cisco IOS, что позволяет воспользоваться новой функциональностью, которую Cisco разработает в будущем, без замены аппаратного обеспечения.

Точка радиодоступа поддерживает широкий спектр антенн и фидеров Cisco, что позволяет обеспечить наиболее оптимальные радиопокрытие и размещение антенны для каждой конкретной инсталляции.

Алюминиевый корпус устройства обеспечивает устойчивость к жестким условиям окружающей среды, одновременно удовлетворяя эстетическим требованиям современных офисов.

Aironet 1200 поддерживает подачу электропитания по кабелю Ethernet и локальное питание, имеет в комплекте крепежную систему для крепления к стенам и потолку, работает в широком диапазоне температур.

Эти и другие особенности делают Cisco Aironet 1200 одной из наиболее гибких точек радиодоступа на рынке, идеально приспособленной под самые разные требования.

Более подробную информацию о продукте можно найти по адресу <http://www.cisco.com/go/aironet>.

Cisco Aironet 1100



Точки радиодоступа Cisco Aironet 1100 предоставляют безопасное, доступное и простое в использовании решение для построения беспроводной ЛВС, одновременно обладающее функциональностью корпоративного класса, необходимой сетевым профессионалам.

Устройство работает в частотном диапазоне 2,4 ГГц и поддерживает заменяемые пользователем радиомодули стандартов IEEE 802.11g и IEEE 802.11b.

Компактный размер, интегрированная ненаправленная антенна и инновационный дизайн крепления точки радиодоступа гарантируют быструю и простую инсталляцию.

Более подробную информацию о продукте можно найти по адресу <http://www.cisco.com/go/aironet>.

Характеристики точек радиодоступа Cisco Aironet 1200 и Aironet 1100

В табл. 1 приведены основные характеристики точек радиодоступа. Полная техническая информация об этих устройствах доступна в документации (<http://www.cisco.com/univercd>).

Табл. 1 Характеристики точек радиодоступа Cisco Aironet 1200 и 1100

	Cisco Aironet 1200	Cisco Aironet 1100
Поддерживаемые радиомодули	<p>Доступные модули:</p> <ul style="list-style-type: none">• 802.11a (5 ГГц, 54 Мбит/с): CardBus• 802.11b (2,4 ГГц, 11 Мбит/с): Mini-PCI• 802.11g (2,4 ГГц, 54 Мбит/с): Mini-PCI <p>Возможна работа в двух диапазонах одновременно для увеличения числа каналов и суммарной полосы пропускания, доступной на одном устройстве.</p>	<p>Доступные модули:</p> <ul style="list-style-type: none">• 802.11b (2,4 ГГц, 11 Мбит/с): Mini-PCI• 802.11g (2,4 ГГц, 54 Мбит/с): Mini-PCI

Табл. 1 Характеристики точек радиодоступа Cisco Aironet 1200 и 1100

	Cisco Aironet 1200	Cisco Aironet 1100
Антенны	<ul style="list-style-type: none"> 802.11b и 802.11g: два разъема RP-TNC (антенны заказываются отдельно, доступен широкий ассортимент антенн различных видов) 802.11a: интегрированные щелевая (6 дБ) и дипольная (5 дБ) антенны 	Встроенная дипольная антенна со сферической диаграммой направленности
Программная функциональность	Обеспечивается операционной системой Cisco IOS Software; это делает возможным реализацию соответствующих функций и преимуществ, описанных в разделе "Преимущества решения Cisco".	
Интерфейсы	Fast Ethernet 100Base-TX (RJ-45), консольный порт (RJ-45)	Fast Ethernet 100Base-TX (RJ-45)
Электропитание	От локального источника питания или по кабелю Ethernet (от коммутатора или устройства Power Injector)	
Аппаратная платформа	Процессор PowerPC 200 МГц, 16 Мб ОЗУ, 8 Мб Flash	
Особенности исполнения	Алюминиевый корпус, сертификация UL 2043, средства защиты от кражи	Пластиковый корпус, сертификация UL 2043, средства защиты от кражи
Диапазон рабочих температур	От -20 °С до 55 °С	От 0 °С до 40 °С

Радиомосты Cisco Aironet

Радиомосты обеспечивают беспроводную связь между территориально удаленными друг от друга сетями. При этом возможно соединение (рис. 2) как двух сетей (топология "точка-точка"), так и нескольких (топология "точка-многоточка").

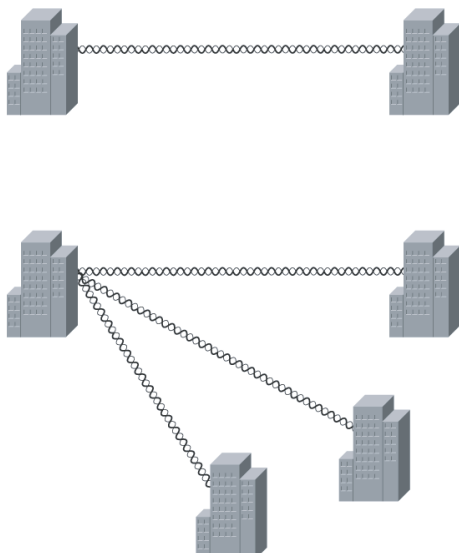


Рис. 2 Решение на базе радиомостов обеспечивает эффективную беспроводную связь между зданиями

Такое решение стоит гораздо дешевле, чем традиционные выделенные линии, при значительно более высоких пропускной способности, гибкости и скорости развертывания.

Современные радиомосты Cisco представлены сериями Aironet 1300 и Aironet 1400.

Cisco Aironet 1300



Устройства серии Cisco Aironet 1300 Series Outdoor Access Point/Bridge — гибкие платформы, обладающие функциональностью радиомоста, радиомоста для рабочих групп и точки радиодоступа. Aironet 1300

обеспечивает высокоскоростную и экономически эффективную беспроводную связь между стационарными и мобильными сетями и абонентами. Построение территориально распределенной беспроводной инфраструктуры с помощью Aironet 1300 предоставляет потребителю гибкое, простое в использовании решение, удовлетворяющее высоким требованиям к безопасности, предъявляемым сетевыми профессионалами.

Типичными областями применения для устройств Cisco Aironet 1300 являются:

- Беспроводная связь между сетями в пределах группы зданий;
- Наружная инфраструктура для мобильных сетей и пользователей;
- Общественный доступ вне помещений;
- Временные сети.

Серия Aironet 1300 поддерживает стандарты IEEE 802.11b и IEEE 802.11g, обеспечивая скорость передачи данных до 54 Мбит/с в диапазоне 2,4 ГГц. Работая под управлением операционной системы Cisco IOS, Aironet 1300 обеспечивает такие возможности, как быстрый безопасный роуминг, средства обеспечения качества обслуживания (QoS) и виртуальные ЛВС (VLAN).

Основные преимущества Cisco Aironet 1300:

- Возможность работы в режимах точки радиодоступа, радиомоста и радиомоста для рабочих групп;
- Поддержка сетевых топологий “точка-точка” и “точка-многоточка”;
- Поддержка архитектуры Cisco Structured Wireless-Aware Network;
- Улучшенные механизмы безопасности на основе стандарта 802.1x;
- Усиленное исполнение устройств, оптимизированное для жестких условий эксплуатации в широком диапазоне температур;
- Интегрированные или внешние антенны для гибкости внедрения.

Cisco Aironet 1400



Устройства Cisco Aironet 1400 Wireless Bridge обеспечивают высокоскоростную и надежную связь в диапазоне 5,8 ГГц между территориально распределенными проводными ЛВС. Построение

территориально распределенной беспроводной инфраструктуры с помощью Aironet 1400 предоставляет потребителю гибкое, простое в использовании решение, удовлетворяющее требованиям к безопасности, предъявляемым сетевыми профессионалами. Радиомосты Aironet 1400 специально разработаны как экономически эффективная альтернатива выделенным линиям. Их основные преимущества:

- Поддержка сетевых топологий “точка-точка” и “точка-многоточка”;
- Лучшие в отрасли дальность действия и пропускная способность (до 54 Мбит/с);
- Улучшенные механизмы безопасности;
- Усиленное исполнение устройств, оптимизированное для жестких условий эксплуатации в широком диапазоне температур;
- Интегрированные или внешние антенны для гибкости внедрения;
- Простота в инсталляции и эксплуатации.

Характеристики радиомостов Cisco Aironet 1300 и Aironet 1400

В табл. 2 приведены основные характеристики радиомостов. Полная техническая информация об этих устройствах доступна в документации (<http://www.cisco.com/univercd>).

Табл. 2 Характеристики радиомостов Cisco Aironet 1300 и 1400

	Cisco Aironet 1300	Cisco Aironet 1400
Поддерживаемые стандарты IEEE 802.11	<ul style="list-style-type: none"> • 802.11g (2,4 ГГц, 54 Мбит/с) • 802.11b (2,4 ГГц, 11 Мбит/с) 	802.11a (5,8 ГГц, UNII-3, 54 Мбит/с)
Антенны	Два разъема RP-TNC (антенны заказываются отдельно, доступен широкий ассортимент антенн различных видов) или интегрированная щелевая антенна (13 дБ)	Один разъем N-Типе (антенны заказываются отдельно) или интегрированная щелевая антенна (20 дБ или 22,5 дБ)

Табл. 2 Характеристики радиомостов Cisco Aironet 1300 и 1400

	Cisco Aironet 1300	Cisco Aironet 1400
Программная функциональность	Обеспечивается операционной системой Cisco IOS Software; это делает возможным реализацию соответствующих функций и преимуществ, описанных в разделе “Преимущества решения Cisco”.	
Интерфейсы	Fast Ethernet (F-Type), консольный порт на устройстве Power Injector	Fast Ethernet (F-Type)
Электропитание	От устройства Power Injector по двойному коаксиальному кабелю Ethernet. Power Injector конвертирует стандартный интерфейс Ethernet RJ-45 в двойной коаксиальный интерфейс F-Type и передает электропитание от локального источника в коаксиальную линию	
Типичная дальность действия	<ul style="list-style-type: none"> • 34,1 км (1 Мбит/с, антенна с усилением 21 дБ) • 3,1 км (54 Мбит/с, антенна с усилением 21 дБ) 	<ul style="list-style-type: none"> • 37 км (9 Мбит/с, антенна с усилением 28 дБ) • 21 км (54 Мбит/с, антенна с усилением 28 дБ)
Особенности исполнения	Алюминиевый корпус, сертификация UL 2043, средства защиты от кражи	Пластиковый корпус, сертификация UL 2043, средства защиты от кражи
Рабочий диапазон температур	От –30 °С до 55 °С	От –30 °С до 55 °С

Антенны и аксессуары Cisco Aironet



Каждая инсталляция беспроводной ЛВС имеет свою специфику. При планировании инсталляции в пределах здания необходимо учесть размеры помещений, строительные материалы, внутренние перегородки и другие факторы, способные привести к многочисленным путям и особенностям распространения сигналов. В случае организации беспроводной связи между зданиями требуется учитывать расстояния, наличие и тип препятствий, наличие промежуточных узлов и т.д.

Каждая инсталляция беспроводной ЛВС имеет свою специфику. При планировании инсталляции в пределах здания необходимо учесть размеры помещений, строительные материалы, внутренние перегородки и другие факторы, способные привести к многочисленным путям и особенностям распространения сигналов. В случае организации беспроводной связи между зданиями требуется учитывать расстояния, наличие и тип препятствий, наличие промежуточных узлов и т.д.

Cisco предоставляет не просто лучшие в отрасли точки радиодоступа, клиентские адаптеры и радиомосты, она предлагает полное решение для любой инсталляции беспроводной ЛВС. По этой причине в ассортимент беспроводных продуктов Cisco входит широкий спектр антенн, фидеров и аксессуаров.

Используя ненаправленные и направленные антенны различных видов для диапазонов 2,4 ГГц и 5 ГГц, фидеры с низкими потерями энергии, крепежные комплекты и другие аксессуары, потребитель может получить беспроводное решение, полностью удовлетворяющее самым строгим требованиям.

Подробный каталог антенн и аксессуаров Cisco доступен на веб-сайте Cisco по адресу <http://www.cisco.com/go/aironet>.

Беспроводные клиентские адаптеры Cisco Aironet

Клиентские адаптеры обеспечивают связь мобильных абонентов с беспроводной сетью в пределах радиопокрытия сети. Беспроводные адаптеры могут работать в режиме Infrastructure для связи с сетевой инфраструктурой, например точками радиодоступа, или в режиме Ad Hoc, взаимодействуя друг с другом.

С помощью беспроводных клиентских адаптеров можно быстро подключить новых сотрудников к сети, обеспечить связь временные рабочие группы, организовать доступ в Интернет из конференц-залов или других общественных мест.

Беспроводные клиентские адаптеры Cisco поддерживают стандарты IEEE 802.11a, 802.11b, 802.11g и доступны в исполнениях CardBus, PCMCIA и PCI. Они обеспечивают потребителя полным набором средств безопасности Cisco Wireless Security Suite, включая поддержку протоколов EAP (LEAP, PEAP-GTC, PEAP-MSCHAP v2 и EAP-TLS), усовершенствования шифрования TKIP, поддержку WPA и готовность к поддержке шифрования AES. Присутствуют развитые средства управления, поддерживается мониторинг радиосреды в рамках архитектуры Cisco SWAN (<http://www.cisco.com/go/swan>) и функциональность быстрого безопасного роуминга, позволяющая мобильному абоненту перемещаться между зонами радиопокрытия разных точек радиодоступа Cisco без заметной задержки.

Современные беспроводные клиентские адаптеры Cisco Aironet представлены тремя сериями продуктов, описанными ниже. Кроме того, существуют Cisco-сертифицированные адаптеры других производителей, дополняющие решение. Подробную информацию о них можно найти по адресу <http://www.cisco.com/go/aironet>.

Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter



Эти двухдиапазонные адаптеры (2,4 ГГц и 5 ГГц) позволяют подключать мобильные и настольные компьютеры к беспроводным ЛВС стандартов IEEE 802.11a, 802.11b и 802.11g. Адаптеры доступны в исполнении CardBus (для мобильных ПК) и PCI (для настольных).

Cisco Aironet 350 Wireless LAN Client Adapter

Адаптеры стандарта IEEE 802.11b работают в диапазоне 2,4 ГГц и доступны в исполнении PCMCIA (для мобильных ПК) и PCI (для настольных).



Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapters



Эти CardBus-адаптеры работают в диапазоне 5 ГГц (UNII-1 и UNII-2), обеспечивая связь мобильных абонентов по стандарту 802.11a на скорости до 54 Мбит/с.

Cisco-совместимые клиентские адаптеры

Широкая номенклатура Cisco-совместимых адаптеров дополняет беспроводное решение Cisco. Такие адаптеры поддерживают лицензированную у Cisco функциональность в рамках программы Cisco Compatible Extensions. Функциональность относится к средствам обеспечения безопасности, качества обслуживания, управления и мониторинга радиосреды. Совместимость гарантируется за счет разностороннего тестирования устройств и отмечается логотипом Cisco Compatible.

Более подробную информацию о программе Cisco Compatible Extensions можно найти по адресу <http://www.cisco.com/go/ciscocompatible/wireless>.

Сервер управления CiscoWorks Wireless LAN Solution Engine



CiscoWorks Wireless LAN Solution Engine (WLSE) представляет собой централизованное решение для управления беспроводной инфраструктурой Cisco Aironet. WLSE обеспечивает быстрое развертывание беспроводной ЛВС и повышает эффективность ее эксплуатации, снижая общую стоимость владения беспроводной сетью.

Развертывание беспроводной ЛВС значительно облегчается и ускоряется за счет функциональности автоматизированного обследования объекта путем определения сервером WLSE оптимальных настроек точек радиодоступа, в том числе излучаемой мощности и частотных каналов. WLSE автоматически конфигурирует беспроводную инфраструктуру и предоставляет администратору средства централизованного конфигурирования всех установленных точек радиодоступа.

WLSE облегчает эксплуатацию беспроводной ЛВС за счет автоматизации повторяющихся во времени задач (например, управления конфигурациями и обновления программного обеспечения). Упреждающий мониторинг производительности, неисправностей и безопасности, проводимый WLSE, делает беспроводную ЛВС более эффективной.

Используя возможности мониторинга радиосреды, встроенные в продукты Cisco Aironet и Cisco-совместимые клиентские адаптеры, WLSE обнаруживает и локализует источники помех, генерирует оптимальные в данный момент времени параметры беспроводной инфраструктуры, обеспечивает автоматическое восстановление радиопокрытия в случае отказа части точек радиодоступа, тем самым обеспечивая высокую производительность и отказоустойчивость беспроводной ЛВС.

WLSE повышает безопасность беспроводной ЛВС, обнаруживая за счет мониторинга радиосреды и блокируя несанкционированно установленные точки радиодоступа, а также обнаруживая неассоциированных беспроводных абонентов. Мониторинг конфигураций беспроводной инфраструктуры обеспечивает повсеместное соблюдение политики безопасности организации.

WLSE является ключевым компонентом архитектуры Cisco Structured Wireless-Aware Network (<http://www.cisco.com/go/swan>), рассмотренной ниже в разделе

“Удобное управление: Cisco Structured Wireless-Aware Network”. Подробную информацию о WLSE можно найти на веб-сайте Cisco по адресу <http://www.cisco.com/go/wlse>.

ПРЕИМУЩЕСТВА РЕШЕНИЯ CISCO

Высокая безопасность: Cisco Wireless Security Suite

Набор дополнений и улучшений механизмов IEEE 802.11 аутентификации и шифрования Cisco Wireless Security Suite, включенный во все продукты Cisco Aironet, обеспечивает безопасность корпоративного класса за счет средств взаимной аутентификации архитектуры 802.1x и сильных динамических средств шифрования Temporal Key Integrity Protocol (TKIP). Решение Cisco также полностью поддерживает стандарт 2003 года Wi-Fi Protected Access (WPA) и будет поддерживать стандарт безопасности IEEE 802.11i после его принятия.

Cisco Wireless Security Suite поддерживает широчайший спектр протоколов аутентификации EAP, клиентских устройств и операционных систем. Он предотвращает изощренные пассивные и активные атаки на беспроводные ЛВС и предоставляет надежные, масштабируемые и централизованные средства управления безопасностью, минимизируя затраты организации на обеспечение безопасности беспроводной ЛВС.

Имея средства Cisco Wireless Security Suite, сетевым администраторам не нужно заниматься поддержкой статических ключей шифрования, а беспроводная ЛВС может запрашивать у абонентских устройств повторную аутентификацию настолько часто, насколько это необходимо.

Решение обеспечивает безопасность, близкую к безопасности проводных ЛВС. Таким образом, потребители могут воспользоваться удобствами и преимуществами, предоставляемыми локальной мобильностью, одновременно сохраняя безопасную сетевую среду (рис. 3).

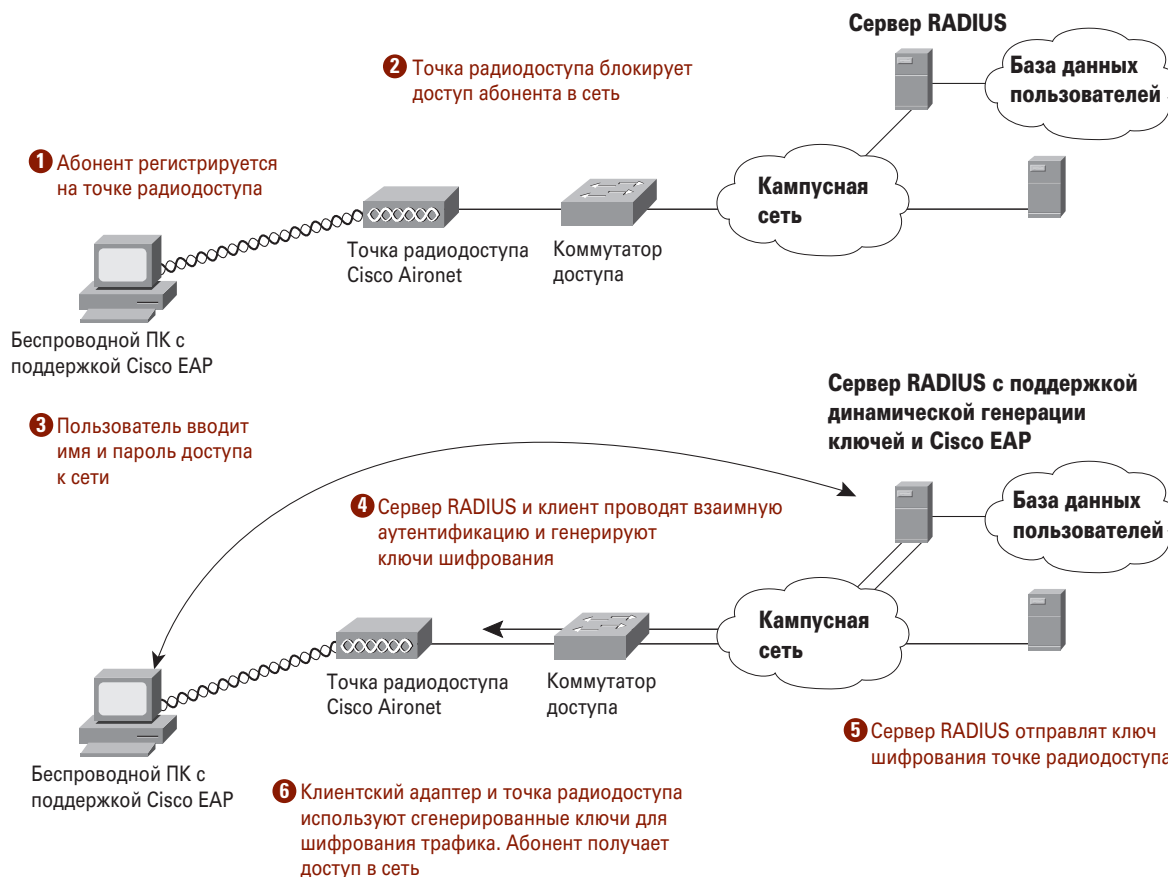


Рис. 3 Cisco Wireless Security Suite обеспечивает безопасность корпоративного класса

Протокол аутентификации канального уровня 802.1x обеспечивает поддержку взаимной аутентификации абонента и сети. При этом реализуется защита от атак “Man-in-the-middle” и перебора паролей (brute force attacks), имеются централизованные средства управления ключами шифрования, включая их замену.

Аутентификация точки радиодоступа по отношению к абоненту также является актуальной, подтверждая легитимность точки радиодоступа, с которой абонент ассоциируется. Такая аутентификация обеспечивается средствами протоколов EAP и защищает пользователей от передачи конфиденциальной информации несанкционированно установленным точкам радиодоступа, выдающим себя за беспроводную инфраструктуру организации. Решение Cisco Structured Wireless-Aware Network (SWAN) защищает организацию от несанкционированно установленных точек радиодоступа путем их автоматического обнаружения, локализации и блокирования. До решения Cisco SWAN эти процедуры должны были быть проделаны вручную, что усложняло эксплуатацию, особенно в случае больших инсталляций или отсутствия на объекте квалифицированного персонала.

Cisco Wireless Security Suite также устраняет уязвимости средств шифрования Wired Equivalent Privacy (WEP) за счет ряда усовершенствований под названием TKIP. Как и WEP, TKIP предусматривает использование шифрования Ron's Code 4 (RC4). Однако для устранения присущих WEP уязвимостей TKIP добавляет контроль целостности данных (MIC) зашифрованных кадров, по пакетную смену ключей шифрования и периодическую смену широковещательного ключа.

Cisco Wireless Security Suite взаимодействует с клиентскими устройствами различных видов и поддерживает многочисленные протоколы аутентификации архитектуры 802.1x, включая EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), Cisco LEAP, EAP-Transport Layer Security (EAP-TLS), Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) и EAP-Subscriber Identity Module (EAP-SIM).

Сервер контроля доступа Cisco Secure Access Control Server (<http://www.cisco.com/go/acs>) поддерживает эти протоколы и обеспечивает масштабируемое, централизованное управление доступом пользователей в сеть и административным доступом по протоколам RADIUS и TACACS+.

Более подробную информацию о безопасности в беспроводных решениях Cisco можно найти по адресу <http://www.cisco.com/go/aironet/security>.

Удобное управление: Cisco Structured Wireless-Aware Network

Архитектура Cisco Structured Wireless-Aware Network (SWAN) обеспечивает высокую безопасность, централизованные средства управления и развертывания беспроводной ЛВС, минимизируя общую стоимость владения сетью. Архитектура SWAN (см. рис. 4) предусматривает интеграцию “радио-осведомленной” (wireless-aware) функциональности в проводную инфраструктуру Cisco и включает в себя четыре основных компонента:

- Точки радиодоступа Cisco Aironet, работающие под управлением Cisco IOS Software. Помимо предоставления услуг связи мобильным абонентам они также производят мониторинг радиосреды;
- Сервер CiscoWorks Wireless LAN Solution Engine (WLSE), обеспечивающий централизованное управление беспроводной инфраструктурой;
- Сервер Cisco Secure Access Control Server (ACS), обеспечивающий контроль доступа в сеть;
- Wi-Fi сертифицированные беспроводные клиентские адаптеры. Применение клиентских адаптеров Cisco Aironet или Cisco-совместимых предоставляет дополнительные преимущества, в том числе мониторинг радиосреды и поддержку другой фирменной функциональности Cisco.

Клиенты и точки радиодоступа производят мониторинг радиосреды (RM) и отправляют его результаты на устройство с функциональностью Wireless Domain Services (WDS). В качестве такого устройства может выступать точка радиодоступа Cisco, работающая под управлением Cisco IOS Software, или модуль Catalyst 6500 Series Wireless LAN Services Module (WLSM); в будущем функциональность WDS будет реализована и на других коммутаторах и маршрутизаторах Cisco.

WDS систематизирует, агрегирует результаты мониторинга радиосреды и отправляет их на сервер управления WLSE в виде набора небольших сообщений. Другой важнейшей функцией WDS является ускорение повторной аутентификации абонента в процессе роуминга между точками радиодоступа. Необходимое количество WDS определяется масштабами беспроводной ЛВС.

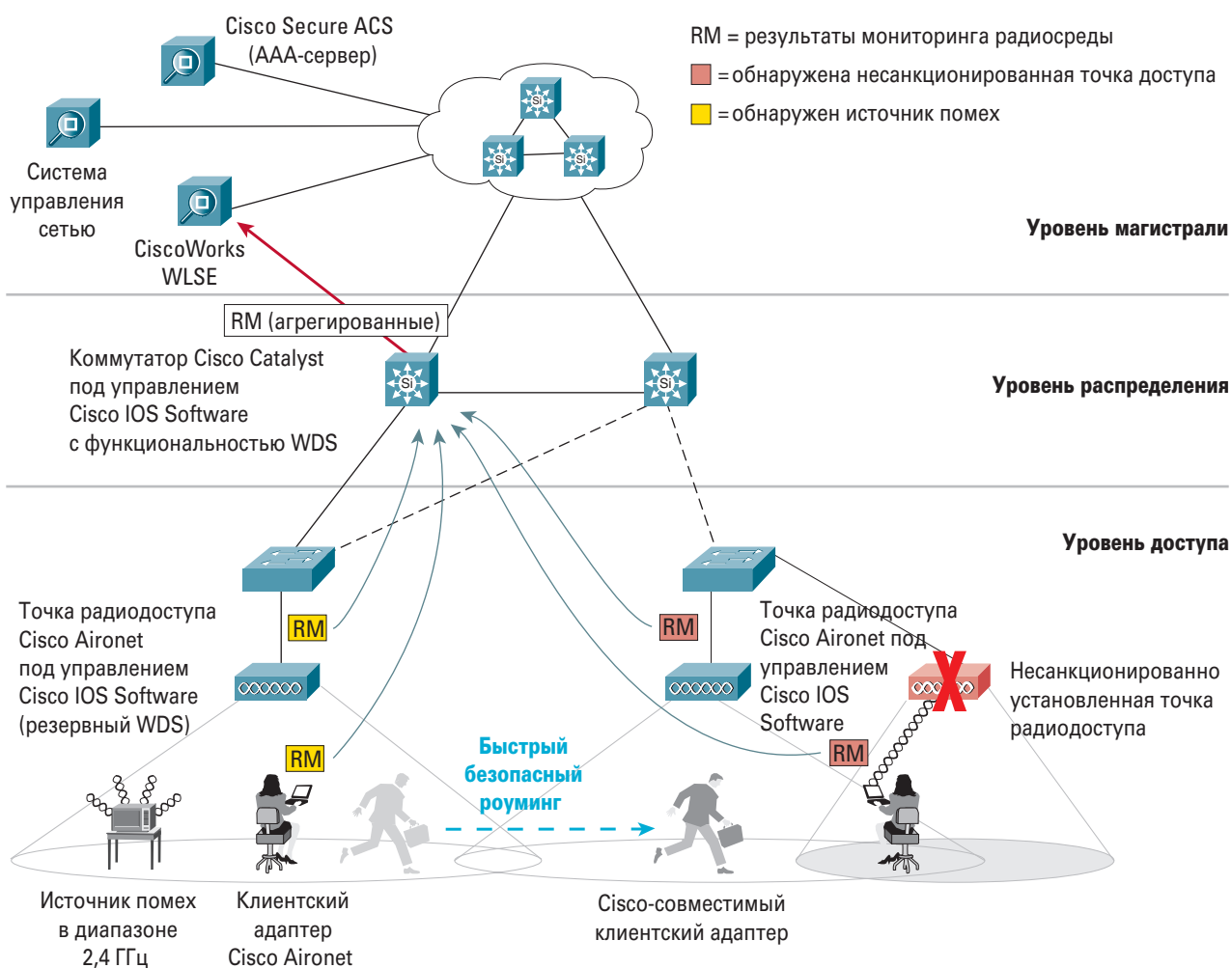


Рис. 4 Архитектура Cisco Structured Wireless-Aware Network (SWAN)

Компоненты архитектуры SWAN образуют иерархию, проходя взаимную аутентификацию и взаимодействуя друг с другом. В результате обеспечиваются:

- Обнаружение и локализация несанкционированно установленных точек радиодоступа;
- Обнаружение и локализация источников помех;
- Автоматизированное обследование объекта (в т.ч. повторное) для облегчения развертывания и сохранения высокой производительности беспроводной ЛВС;
- Передовые средства диагностики и устранения неисправностей в беспроводной ЛВС;

- Быстрый безопасный роуминг на канальном и сетевом уровнях;
- Продолжение 802.1x-аутентификации абонентов даже в случае нарушения связи с сервером контроля доступа (WAN Link Remote Site Survivability);
- Автоматическое восстановление радиопокрытия беспроводной ЛВС при отказе части точек радиодоступа;
- Централизованное конфигурирование и обновление ПО.

Более подробная информация об архитектуре Structured Wireless-Aware Network доступна по адресу <http://www.cisco.com/go/swan>.

Поддержка виртуальных локальных сетей

Беспроводная инфраструктура Cisco Aironet поддерживает до 16 виртуальных ЛВС (VLAN). Это позволяет потребителю внедрять различные политики и услуги, например разные настройки безопасности и качества обслуживания для различных типов пользователей и приложений.

Функциональность VLAN распространяется на беспроводную ЛВС путем поддержки ее инфраструктурой тегов IEEE 802.1Q. Кадры, приходящие на точку радиодоступа

из разных VLAN проводной сети, передаются в рамках разных SSID (Service Set Identifier) с разными ключами WEP. Таким образом, абоненты могут получать только кадры, относящиеся к своим VLAN и, соответственно, SSID. С другой стороны, кадры, получаемые от абонентов разных SSID, точка радиодоступа маркирует разными тегами 802.1Q и отправляет в проводную сеть (рис. 5).

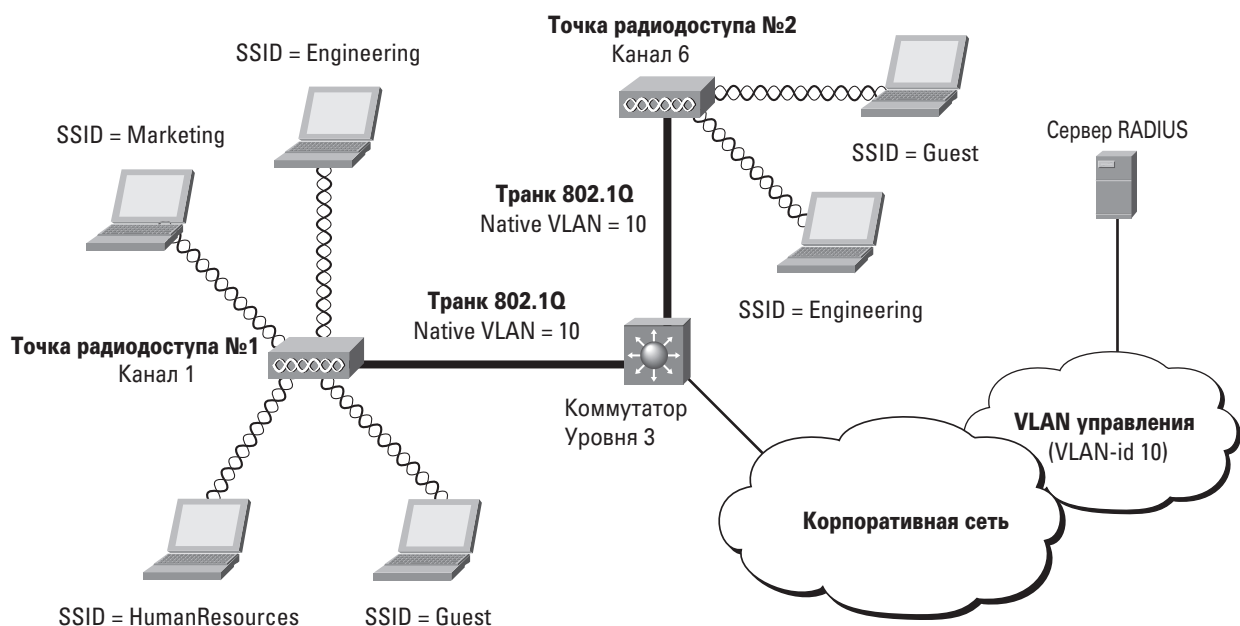


Рис. 5 Виртуальные ЛВС позволяют разделить различные типы пользователей и трафика на одной и той же инфраструктуре

Оператор может использовать различные беспроводные виртуальные ЛВС для отделения трафика сотрудников от трафика гостей. VLAN идеальны для обеспечения беспроводного доступа в общественных местах, например в приемных, кафе, аэропортах без угрозы для безопасности внутренней сети организации. Кроме того, отдельные VLAN можно организовать для трафика каких-либо приложений, например для голосового трафика.

Виртуальные ЛВС могут потребоваться также для внедрения различных видов политик. Например, организация может воспользоваться преимуществами протокола EAP-FAST в виртуальной ЛВС, предназначенной для сотрудников, одновременно используя другой протокол аутентифи-

кации в гостевой VLAN для обеспечения максимальной совместимости с различными клиентскими устройствами гостей.

Поддержка качества обслуживания (QoS)

Продукты Cisco Aironet обеспечивают приоритезацию трафика, поддерживая стандарт IEEE 802.1p. Это позволяет приоритезировать трафик реального времени, такой как голос и видео, по отношению к асинхронному трафику, например электронной почте, для повышения качества работы сетевых приложений и оптимизации использования полосы пропускания.

Для максимальной защиты инвестиций потребителя обновление программного обеспечения продуктов Cisco позволит воспользоваться преимуществами будущих стандартов QoS, таких как IEEE 802.11e.

Максимальная отдача от интеллектуальной проводной сети Cisco

В идеале беспроводное решение Cisco внедряется как дополнение к интеллектуальной проводной инфраструктуре Cisco, позволяя организациям получить максимальную отдачу от присутствующей в обоих решениях функциональности.

Когда продукты Cisco Aironet сочетаются с коммутаторами Cisco Catalyst, ключевые интеллектуальные функции, например виртуальные ЛВС и механизмы качества обслуживания, становятся доступны как в проводной, так и беспроводной сетях. Кроме того, становится возможной интеграция “радио-осведомленной” функциональности в проводную инфраструктуру, описанной в разделе “Удобное управление: Cisco Structured Wireless-Aware Network”.

Поддержка других производителей

Беспроводные решения Cisco полностью совместимы с отраслевыми стандартами и легко интегрируются с проводными сетями и клиентскими устройствами других производителей. Поддерживая как самые последние, так и давно принятые стандарты, продукты Cisco обеспечивают надежную и безопасную связь в любой основанной на стандартах среде. В то же время поддержка такой средой фирменных наработок Cisco позволяет потребителю воспользоваться преимуществами, далеко выходящими за рамки стандартов.

Благодаря программе Cisco Compatible Extensions на рынке доступны беспроводные клиентские устройства от различных производителей с лицензированной у Cisco функциональностью (см. раздел “Cisco-совместимые клиентские адаптеры”). Более подробную информацию о программе можно найти по адресу <http://www.cisco.com/go/ciscocompatible/wireless>.

Защита инвестиций

Потребители могут модернизировать программное обеспечение своего оборудования, чтобы воспользоваться новой функциональностью, которую Cisco разработает в будущем, а также модернизировать аппаратуру путем са-

мостоятельной замены радиомодулей для получения преимуществ новых высокоскоростных стандартов беспроводных ЛВС. Усиленное исполнение устройств и широкий диапазон допустимых температур эксплуатации гарантируют годы безотказной работы даже в жестких условиях.

Гибкость внедрения

Беспроводные продукты Cisco Aironet поддерживают подачу электропитания по кабелю Ethernet и локальное питание, снижая стоимость и сложность внедрения. Широкий выбор 2,4 ГГц антенн, а также инновационный дизайн 5 ГГц антенны гарантируют оптимальное радиопокрытие, удовлетворяющее специфические требования потребителя. Удобные крепежные конструкции обеспечивают быстроту и простоту инсталляции в различных положениях и условиях.

Сервис и поддержка

Доступность и производительность — ключевые требования, предъявляемые к любой сети. Сейчас, когда сети превратились в основу бизнеса, их значение резко возросло. Сервис и поддержка, предоставляемые Cisco, поддерживают постоянную работоспособность сети при разумных и предсказуемых затратах, способствуя повышению производительности труда во всей организации.

Cisco предлагает широкий спектр сервисных программ. Эти инновационные программы помогают потребителю защитить инвестиции в свои сети, оптимизировать работу сетей и подготовить их к внедрению новых приложений.

Подробная информация о сервисе и поддержке Cisco доступна по адресу <http://www.cisco.com/go/smartnet>.

СРЕДСТВА УПРАВЛЕНИЯ ДОСТУПОМ

Средства управления доступом предоставляют абонентам возможность выбора нужных им сетевых сервисов, обеспечивают контроль доступа абонентов в сеть и биллинг. Средства управления доступом не просто предоставляют пользователям доступ к сети, а предлагают им ассортимент сетевых сервисов на основе выбранной предприятием бизнес-модели. Например, могут быть доступны бесплатные, базовые и расширенные сервисы.

Для построения успешной сети общественного беспроводного доступа важно, чтобы процесс выбора сервисов и доступа к ним был простым для пользователей и требовал

минимум усилий с их стороны. Современный подход к решению этой задачи, реализованный в продуктах Cisco, предполагает использование веб-интерфейса (рис. 6).



Рис. 6 Процедура доступа пользователей к сервисам

В рамках этого подхода пользователь подключается к сети, запускает веб-браузер и вводит произвольный URL. Генерируемый при этом HTTP-запрос прозрачно для пользователя перенаправляется на страницу регистрации, на которой он может пройти аутентификацию, выбрать нужные ему сервисы, пополнить баланс и т.д. Для поддержки абонентов со статическими настройками (IP-адрес, DNS, прокси) сеть производит соответствующие трансляции адресов и спуфинг. Возможно предоставление свободного доступа к определенным сервисам, например, к меню (в кафе), к расписанию самолетов (в аэропорту) и т.д. После успешной аутентификации и выбора сервисов пользователю предоставляется доступ к ним. При этом производится учет потребляемых сетевых ресурсов, необходимый для организации биллинга.

В зависимости от масштабов сети общественного беспроводного доступа возможны разные подходы к реализации средств управления доступом.

Так, в случае малой инсталляции (например, в гостинице или кафе) оптимальным решением может быть интеграция функциональности управления доступом в одно устройство. Это решение представлено устройством Cisco Building Broadband Service Manager (BBSM). Часто в таких случаях поддержка и управление сетевой инфраструктурой осуществляется силами владеющей этой инфраструктурой организации.

Если речь идет о более крупной инсталляции (например, в сети гостиниц или кафе) установка отдельного устройства в каждом заведении может оказаться неэффективной, как минимум, с точки зрения управляемости и масштабируемости. В таких случаях более эффективным становится подход, при котором средства управления доступом устанавливаются централизованно, и их функциональность используется всеми хот-спотами. При этом также обычно организуется централизованный доступ к сетевым сервисам, удобный для абонентов тем, что они могут воспользоваться одинаково широким набором услуг в любом заведении сети.

Такой централизованный подход реализован в решении на базе продуктов Cisco Subscriber Access and Management (SAM).

Дальнейшие разделы рассматривают эти два решения более детально.

Cisco Building Broadband Service Manager (BBSM)



Cisco BBSM — это шлюз контроля доступа, обеспечивающий “plug-and-play” доступ пользователей в сеть, дифференцированный по скорости и стоимости, возможность самостоятельного выбора услуг, многочисленные опции аутентификации и биллинга, средства генерации отчетов и управление на основе web-интерфейса.

Шлюз поддерживает различные виды технологий доступа пользователей — беспроводные ЛВС Wi-Fi, Ethernet, Long-Reach Ethernet (LRE), DSL, кабельные сети и обычно устанавливается на границе между сетью общественного доступа организации и сетью оператора связи.

Cisco BBSM обеспечивает доступ в сеть для клиентских устройств с самыми разными настройками. Абоненты могут пользоваться устройствами не только с автоматической (DHCP) конфигурацией сетевых интерфейсов, но и со статически заданными IP-адресами (в том числе дублирующими друг друга), со статическими настройками прокси- и DNS-серверов. Такая “plug-and-play” функциональность позволяет воспользоваться услугой доступа в сеть широкому спектру пользователей без необходимости дорогостоящей технической поддержки.

Для получения доступа в сеть пользователю достаточно открыть веб-браузер и выбрать любой URL. При этом BBSM автоматически перенаправит пользователя на начальную страницу (Connect Screen), на которой он может ознакомиться с перечнем доступных сервисов и пройти аутентификацию. Организация может изменить внешний вид начальной страницы для создания фирменного стиля.

Аутентификация пользователей может производиться:

- По учетной записи на внешнем RADIUS-сервере;
- По коду доступа локально на сервере BBSM;
- По порту устройства (в случае проводного подключения).

При этом возможны различные варианты оплаты услуг:

- Авансовая (prepaid) и кредитная (postpaid) оплата доступа по учетной записи на RADIUS-сервере;
- Оплата путем приобретения купонов с кодом доступа;
- Кредитная карта;
- Бесплатный доступ;
- Счет в систему управления гостиницей (PMS, Property Management System).

Функциональность Walled Garden позволяет определить сайты, доступные пользователям бесплатно, например портал компании со справочной и маркетинговой информацией.

Типичные показатели производительности BBSM при различных размерах пакетов и типах трафика составляют 85 Мбит/с (250 одновременных сессий) и 45 Мбит/с (1000 одновременных сессий).

Продукт доступен в трех вариантах: в виде отдельного устройства высотой 1 RU для установки в 19" стойку, устройства в настольном исполнении и в виде комплекта программного обеспечения. Все варианты имеют идентичную программную функциональность, но имеют разные опции лицензирования, определяющие количество одновременно работающих пользователей и возможность интеграции с системами управления гостиницами.

Более подробную информацию о Cisco BBSM можно найти по адресу <http://www.cisco.com/go/bbsm>.

Преимущества решения Cisco

- Доступ пользователей “plug-and-play”;
- Широкие возможности аутентификации;
- Поддержка широкого спектра биллинговых систем (свыше десятка наименований), наличие RS-232 и TCP/IP интерфейсов к ним;
- Наличие SDK для поддержки дополнительных биллинговых систем;
- Высокая производительность;
- Наличие вариантов исполнения и гибких опций лицензирования.

Cisco Subscriber Access and Management (SAM)

Cisco Subscriber Access and Management — это решение операторского класса для управления доступом абонентов к сетевым сервисам (рис. 7).

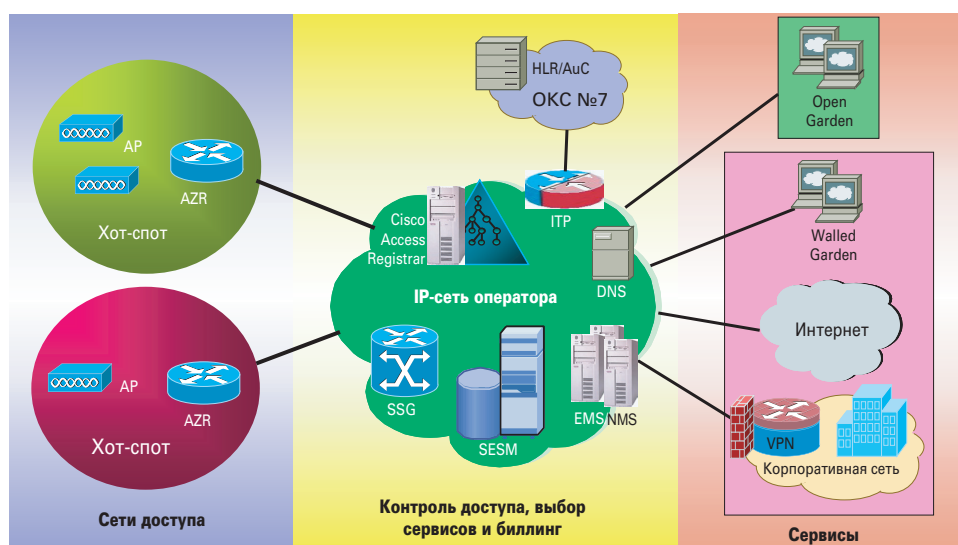


Рис. 7 Архитектура решения Cisco Subscriber Access and Management

Архитектура SAM поддерживает широкий спектр технологий доступа. Это открывает дополнительные возможности расширения абонентской базы по мере развития бизнеса оператора. Абоненты могут подключаться к сети, используя:

- Сеть доступа Wi-Fi или Metro Ethernet по протоколам IP или PPPoE;
- Сеть доступа GPRS или 3G по протоколам IP или L2TP;
- Сеть доступа ATM по протоколам IP, PPPoA и PPPoEoA;
- Сеть доступа CDMA/Mobile IP по протоколу IP.

Контроль доступа, выбор сервисов и биллинг осуществляется централизованно независимо от технологии доступа и места подключения абонента.

SSG является шлюзом выбора сервисов, контролирующим доступ к предлагаемым абонентам сетевым сервисам.

SESM реализует веб-портал для пользователей, с помощью которого они выбирают нужные им сервисы.

Сервер контроля доступа (Cisco Access Registrar) хранит учетные записи пользователей или может выступать как прокси к другим серверам для аутентификации. Вместе с SSG сервер контроля доступа обеспечивает учет потребления сетевых ресурсов, необходимый для биллинга. Возможные опции биллинга включают авансовую (prepaid) и кредитную (postpaid) оплату, доступ на основе подписки, на основе объемов потребления услуг, типов сервисов и контента). Полная функциональность биллинга реализуется с помощью внешнего сервера биллинга.

Решение допускает интеграцию с базами данных пользователей GSM-сетей, что открывает возможности сотрудничества с сотовыми операторами. В этом случае инфраструктура GSM-сетей может применяться для аутентификации и авторизации пользователей хот-спотов по протоколу EAP-SIM.

Для поддержки аутентификации EAP-SIM используется HLR Proxy, терминирующий сообщения EAP и генерирующий сообщения MAP для аутентификации на HLR в сети GSM-оператора. Сервер контроля доступа Cisco Access Registrar поддерживает такую функциональность. Для обеспечения интерфейса между сетями IP и ОКС №7, необходимого для передачи сообщений между HLR Proxy и HLR, используется MAP-шлюз.

Функциональная область сервисов включает в себя серверы с контентом, предназначенным для абонентов сети общественного беспроводного доступа. Хотя наиболее типичным видом сервиса является доступ в Интернет, воз-

можны и другие сервисы, специфичные для данной сети. Серверы Open Garden могут не требовать аутентификацию и авторизацию пользователей (например, в случае аэропорта могут бесплатно предоставлять информацию о времени прилетов и вылетов самолетов). Walled Garden серверы могут предлагать специальный контент, требующий аутентификацию пользователя и/или учет (например, дополнительные сервисы, такие как доступ к мультимедийному контенту). Кроме того, оператор сети общественного беспроводного доступа может обеспечить управляемый доступ пользователей к корпоративной сети с помощью услуги виртуальной частной сети (VPN).

Cisco Service Selection Gateway (SSG)

Cisco SSG — это шлюз выбора услуг для операторов связи, разделяющий сети доступа и сети с предлагаемыми абонентам сервисами. SSG позволяет абоненту максимально гибко подключаться к различным сетям на выбор (Интернет, корпоративные сети, сети других операторов), обеспечивая персонализированную маршрутизацию абонентского трафика.

SSG является центральным компонентом решения Cisco Subscriber Access and Management. Он хранит состояние подключений всех пользователей сетей доступа, обеспечивает свободный доступ к Open Garden серверам и управляет доступом к платным сервисам. Сервисы могут включать доступ к Интернет, к мультимедийному контенту (аудио и видео), к средствам электронной коммерции, к играм и другим услугам.

SSG принудительно перенаправляет запросы неаутентифицированных пользователей на веб-портал SESM, где они могут пройти аутентификацию или завести себе учетную запись, выбрать нужные им сервисы, пополнить баланс. Далее SSG прозрачно предоставляет доступ абонентов к выбранным сетевым сервисам и обеспечивает учет.

Учет ведется по пользователю, сервису, времени и/или трафику. Возможно использование авансовой и кредитной схемы оплаты для одного абонента, одновременно подключенного к разным сервисам.

При подключении SSG может также дополнительно осуществлять:

- авторизацию абонентов для подключения к каждому сервису;

- трансляцию адресов, если адресное пространство подключаемой сети не соответствует адресному пространству, в котором абоненты получают адреса;
 - ограничение скорости подключения;
 - одновременное подключение к нескольким сервисам.
- SSG представляет собой функциональность Cisco IOS и работает на широком спектре маршрутизаторов Cisco (начиная с Cisco 2651XM и заканчивая Cisco 7600).

Cisco Subscriber Edge Services Manager (SESM)

Cisco SESM представляет собой веб-портал, предназначенный для аутентификации абонентов, выбора сервиса и управления своей учетной записью.

SESM реализует следующие функции.

- Веб-портал для управления доступом абонентов к сетевым сервисам и их самообслуживания;
- Контроль доступа абонентов в сеть по протоколам RADIUS и LDAP;
- Средства для авансового (prepaid) и кредитного (postpaid) биллинга;
- Интегрированные средства управления;
- Набор инструментальных средств разработки (SDK).

SESM допускает полное изменение внешнего вида интерфейса пользователя, в том числе его персонализация в зависимости от физического нахождения и типа абонентского устройства, а также предпочтений пользователя (например, языковых). Это повышает качество обслуживания абонентов и способствует повышению их лояльности оператору.

Продукт реализован на языке Java и поддерживается на платформах Linux, Solaris и Windows 2000.

Преимущества решения Cisco

- Высокая масштабируемость;
- Поддержка широкого спектра технологий доступа абонентов;
- Поддержка интеграции с сетями сотовых операторов;
- Развитые средства управления;
- Возможность полного изменения внешнего вида веб-портала, изменение контента в зависимости от настроек и физического расположения абонентского устройства.

ВАРИАНТЫ СЕТЕВОГО ДИЗАЙНА ДЛЯ МАЛЫХ И СРЕДНИХ ОПЕРАТОРОВ

ОБЗОР АРХИТЕКТУРЫ

В этом разделе приводятся обобщенные варианты дизайна сетей, предназначенные для построения сетей общественного беспроводного доступа малых и средних операторов. Сначала указываются функциональные компоненты (модули), из которых могут состоять такие сети. Затем следует более подробное описание модулей: указываются основные устройства, обсуждается их функциональность, рассматриваются возможные альтернативы.

Поскольку брошюра посвящена решениям для общественного беспроводного доступа, предлагаемые варианты дизайна сетей не претендуют на полный охват всех возможных потребностей малых и средних операторов. По этой причине не рассматриваются или рассматриваются недостаточно подробно вопросы дизайна сетей, связанные с реализацией функциональности, отличной от беспроводного доступа.

Сетевые элементы в примерах дизайна, рассматриваемых в следующих разделах, проводятся с помощью условных обозначений. Условные обозначения раскрыты в Приложении.

ДИЗАЙН СЕТИ ДЛЯ МАЛОГО ОПЕРАТОРА

Дизайн малой сети обсуждается на примере гостиницы. Такой дизайн (рис. 8) включает в себя беспроводную и проводную инфраструктуру. Беспроводная инфраструктура обеспечивает доступ мобильных абонентов к ресурсам сети и, как правило, доступ в Интернет. Проводная инфраструктура образует магистраль и периферию ЛВС организации, хотя также может использоваться в дополнение к беспроводной для доступа пользователей в номерах.

В дизайне малой сети можно выделить 3 модуля:

- Модуль беспроводного доступа (WLAN);
- Модуль проводного доступа (Long-Reach Ethernet);
- Магистральный модуль.

Дальнейшие разделы рассматривают эти модули подробнее.

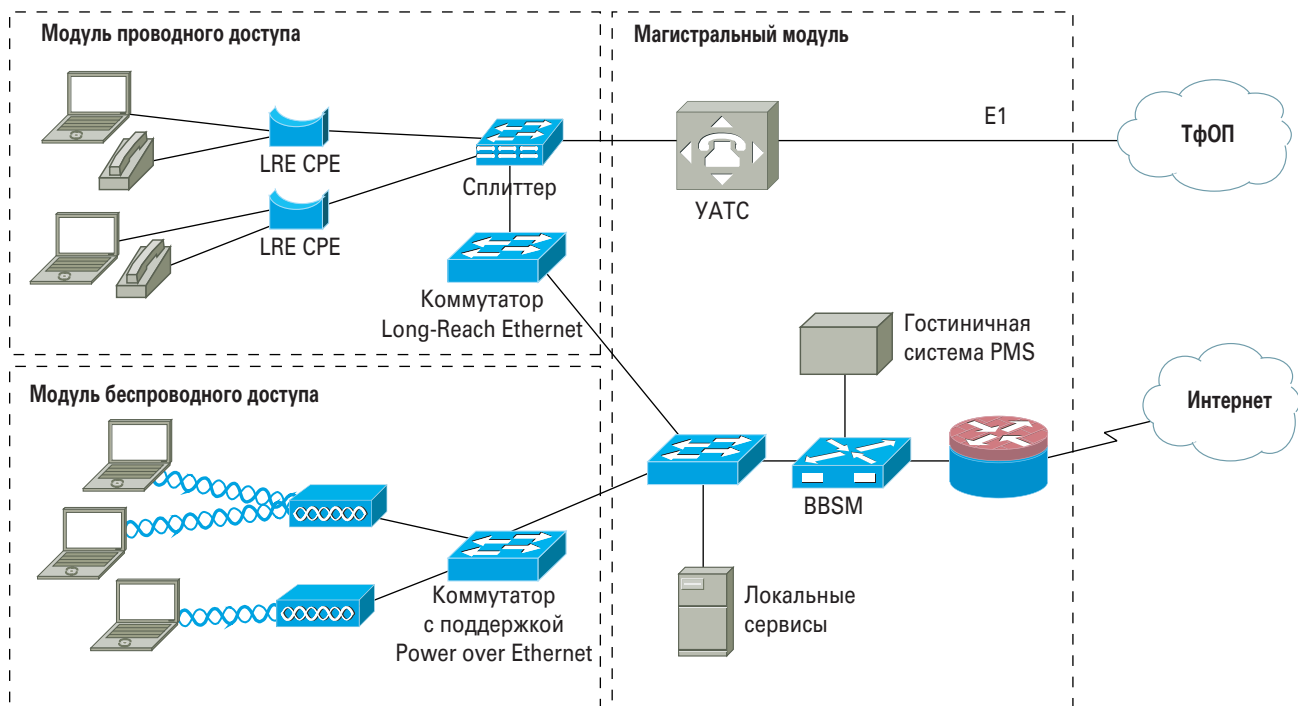


Рис. 8 Вариант дизайна сети для гостиницы

Модуль беспроводного доступа

Главная задача модуля — предоставление доступа в сеть мобильным пользователям. К таким пользователям в первую очередь относятся постояльцы гостиницы, хотя та же самая беспроводная инфраструктура может успешно применяться и для доступа персонала.

Для обеспечения безопасности сети персонал и гости используют разные виртуальные ЛВС, настроенные на точках радиодоступа. При этом для гостей может быть настроена виртуальная ЛВС с открытым доступом, поскольку они проходят аутентификацию на шлюзе контроля доступа (BBSM). Виртуальная ЛВС для персонала, наоборот, в целях обеспечения безопасности служебной части сети гостиницы должна быть защищена сильными средствами аутентификации и шифрования.

Для предотвращения возможных атак одних абонентов на других беспроводную связь между ними можно заблокировать путем применения техники Public Secure Packet Forwarding (PSPF) на точках радиодоступа.

Поддержка приоритезации трафика инфраструктурой Cisco Aironet позволяет успешно применять средства беспроводной IP-телефонии (например, для сотрудников) и другие чувствительные к качеству обслуживания приложения.

Модуль проводного доступа

Хотя полное радиопокрытие гостиницы (в том числе в номерах) является предпочтительным с точки зрения удобства доступа в сеть, его обеспечить удастся не всегда, например, по экономическим причинам. Кроме того, в номерах могут устанавливаться проводные IP-телефоны, устройства Set-Top Box для обеспечения просмотра видео поверх IP на стандартных телевизорах или плазменных панелях.

В таких случаях возможен компромиссный вариант — оснащение гостиничных номеров проводным подключением к сети, а общественных мест гостиницы — беспроводным. Если в гостиничные номера проложена кабельная проводка (например, стандартная витая пара для подключения аналоговых телефонов), то ее можно использовать для высокоскоростной (до 15 Мбит/с) передачи данных с помощью технологии Cisco Long-Reach Ethernet (см. рис. 8).

Детальное рассмотрение технологии LRE выходит за рамки данной брошюры. Более подробную информацию о ней можно найти по адресу <http://www.cisco.com/go/lre>.

Магистральный модуль

Как следует из названия, модуль реализует магистраль ЛВС гостиницы на базе коммутируемой проводной инфраструктуры. К этой магистрали подключаются модули WLAN и LRE, а также сетевая периферия, представленная маршрутизатором и сервером BBSM.

Маршрутизатор обеспечивает подключение сети гостиницы к Интернет. Для защиты периметра сети он может иметь функциональность межсетевого экрана или подключаться к отдельному межсетевому экрану.

BBSM, устанавливаемый между маршрутизатором и коммутируемой магистралью Ethernet (рис. 8), обеспечивает контроль доступа к Интернет. Для интеграции с системой управления гостиницей у BBSM предусмотрены интерфейсы RS-232 или TCP/IP.

В гостинице можно реализовать как платные сервисы (например, доступ в Интернет), так и бесплатные (например, доступ к контенту на серверах, подключенных к локальной сети гостиницы).

В целях обеспечения безопасности в сети гостиницы настраиваются разные виртуальные локальные сети для постояльцев и персонала. Кроме того, рекомендуется внедрение специализированных средств безопасности, например систем обнаружения вторжений.

ДИЗАЙН СЕТИ ДЛЯ СРЕДНЕГО ОПЕРАТОРА

Рассматриваемый в настоящем разделе дизайн средней сети (рис. 9) охватывает несколько хот-спотов, физически расположенных в разных местах.

Примерами организаций, которым подходит подобный сетевой дизайн, могут быть:

- *Операторы связи.* Они могут эксплуатировать всю сетевую инфраструктуру (end-to-end), хотя также возможны варианты сотрудничества с владельцами заведений, в которых устанавливаются хот-споты, и с другими операторами.
- *Владельцы заведений.* К ним относятся организации, имеющие ряд заведений под одной маркой — сети кафе, гостиниц и других общественных предприятий. Они могут установить и эксплуатировать сетевую инфраструктуру в заведениях, в то время как сервисы и контроль доступа к ним обеспечиваются оператором связи. Возможна и другая модель, при которой вся инфраструктура устанавливается и эксплуатируется владельцами заведений.
- *Виртуальные сетевые операторы (BCO).* Они сосредоточены, с одной стороны, на привлечении максимального количества абонентов путем сотрудничества с владельцами заведений, с другой — на взаимодействии с операторами связи, фактически предоставляющими сетевые сервисы. BCO можно рассматривать в качестве посредников.



Рис. 9 Вариант дизайна сети для среднего оператора

Дизайн составляют две ключевые подсистемы, которые можно назвать сетями доступа и сетью центрального офиса.

Под сетями доступа понимаются сети, через которые мобильные пользователи получают доступ к сервисам — к Интернет, серверам с контентом организации и т.д. Дизайн таких сетей рассматривается в разделе “Сети доступа”.

Под сетью центрального офиса понимается централизованная инфраструктура, включающая в себя:

- средства контроля доступа и выбора сервисов на базе решения Cisco SAM;
- локальные сервисы (например, серверы с контентом);
- средства подключения к удаленным сервисам (Интернет, сетям других операторов, корпоративной сети и т.д.).

Инфраструктура может быть установлена в главном офисе сети предприятий, а может устанавливаться у оператора связи. Хотя при этом возможны самые разные варианты дизайна сети, ключевые компоненты, специфичные для сетей общественного беспроводного доступа, остаются те же. Они рассматриваются в разделе “Сеть центрального офиса”.

Сети доступа

Сети доступа в общем случае включают в себя точки радиодоступа (Access Point, AP), коммутаторы (Access Zone Switch, AZS) и маршрутизаторы (Access Zone Router, AZR).

Точки радиодоступа (AP)

Назначение точек радиодоступа — обеспечение связи мобильных абонентов с проводной сетью, через которую они получают доступ к сетевым сервисам. Модуль могут составлять одна или несколько точек радиодоступа, количество и характеристики которых выбираются в зависимости от требований к радиопокрытию, производительности и т.д.

Важной задачей, стоящей перед компанией, является обеспечение безопасности в радиосреде. Необходимо сделать так, чтобы абоненты не имели возможности злоупотреблять своим доступом в сеть, проводя атаки на сеть организации или на других абонентов. Для решения этой задачи используется шифрование трафика на канальном уровне беспроводного сегмента, поддержка функциональ-

ности PSPF (аналог Private VLAN Edge) на точках радиодоступа и коммутаторах доступа, защиты от перехвата и злоупотребления ARP-пакетами при проведении атак на стек маршрутизаторов доступа.

Все эти функции нужны для того, чтобы абоненты не могли перехватывать данные друг друга и проводить атаки типа Fraud.

Тем не менее, поскольку не все абонентские устройства поддерживают современные технологии обеспечения безопасности, например WPA, для охвата и этой части пользователей услуг хот-спотов целесообразно также обеспечить и открытый доступ в беспроводную сеть без шифрования трафика. В таком случае точки радиодоступа не участвуют в процессе аутентификации абонента, а передают эту задачу шлюзу контроля доступа.

Эту же физическую инфраструктуру беспроводной сети можно использовать для повышения эффективности работы обслуживающего персонала организации и, соответственно, повышения качества обслуживания клиентов. В качестве примера можно привести оснащение официантов сети кафе беспроводными POS-терминалами.

В результате точки радиодоступа должны поддерживать, как минимум, три класса мобильных пользователей. Из них два класса относятся к клиентам, поддерживающим современные технологии безопасности или не поддерживающим их, и еще один класс — к сотрудникам предприятия. Для этого на точках радиодоступа настраиваются различные SSID, соответствующие отдельным виртуальным ЛВС с различными настройками безопасности. Инфраструктура Cisco Aironet позволяет обеспечить безопасность сети предприятия с помощью средств, описанных в разделе “Высокая безопасность: Cisco Wireless Security Suite”.

Интерфейсы управления точек радиодоступа можно вынести в отдельную виртуальную сеть, недоступную из беспроводной сети. Это позволяет исключить ситуации, когда абоненты беспроводной сети изменяют настройки точек доступа для проведения дальнейших атак на сеть организации.

Поддержка точками радиодоступа приоритизации трафика позволяет применять беспроводную инфраструктуру для качественной передачи чувствительного к задержкам трафика, например мультимедийного контента, беспроводной IP-телефонии для сотрудников и поддержки других приложений.

Коммутатор доступа (AZS)

Точки радиодоступа подключаются к коммутатору (например, Catalyst 3550), обеспечивающему агрегацию на Уровне 2 для средних и крупных хот-спотов. Также коммутаторы могут использоваться для идентификации расположения пользователей путем добавления соответствующих параметров в поле Опции 82 DHCP-запросов абонентских устройств. Это можно использовать для динамического изменения веб-интерфейса SESM в зависимости от расположения пользователя. Коммутатор подключается к маршрутизатору, обеспечивающему доступ пользователей хот-спота к сетевым ресурсам.

Возможен и альтернативный вариант — подключение точек радиодоступа (одной или нескольких) непосредственно к маршрутизатору. Для этого можно либо использовать дополнительный Ethernet-порт маршрутизатора, либо установить в него модуль, реализующий коммутируемые порты Ethernet. Хотя такой подход имеет относительно невысокую масштабируемость, он может оказаться оптимальным в случае маленьких хот-спотов.

Точки радиодоступа могут получать электропитание по кабелю Ethernet, воспользовавшись функциональностью PoE коммутаторов или коммутирующих модулей маршрутизаторов Cisco. Это увеличивает гибкость инсталляции и снижает ее стоимость.

Маршрутизатор доступа (AZR)

Для подключения хот-спотов к главному офису применяется стандартный маршрутизатор Cisco. Он обеспечивает пограничную маршрутизацию и связь с территориально распределенной сетью, сервисы DHCP, поддерживает виртуальные ЛВС 802.1q для сегментации трафика. Кроме того, маршрутизатор также может обеспечивать функциональность NAT и Proxu ARP для поддержки клиентов со статическими IP-адресами, Опцию 82 DHCP для указания местоположения (нужную для предоставления абоненту специфичной для его местоположения информации) и выполнять другие необходимые функции.

В качестве маршрутизаторов доступа могут выступать устройства серий Cisco 1700, 2600XM, 2691 и 3700.

Сеть центрального офиса

Задача сети центрального офиса применительно к общему беспроводному доступу заключается в агрегировании WAN-подключений хот-спотов удаленных заведений, управлении доступом мобильных абонентов к сервисам и подключении всей системы к сетевым сервисам.

Агрегация

К агрегатору подключаются маршрутизаторы (AZR) хот-спотов, развернутых в удаленных заведениях. В качестве агрегатора обычно используется высокопроизводительный маршрутизатор Cisco. Для обеспечения высокой доступности у агрегатора резервируются ключевые компоненты (системный модуль, блоки питания и т.д.). Кроме того, могут быть зарезервированы устройства целиком.

В случае применения туннелирования трафика от AZR агрегатор также может терминировать эти туннели.

Типичными примерами маршрутизаторов для агрегации являются маршрутизаторы серий Cisco 7x00, хотя модель определяется исходя из требований конкретной сети.

Шлюз контроля доступа и выбор сервисов

В качестве шлюза контроля доступа используется маршрутизатор Cisco с функциональностью SSG. Он хранит состояние подключений всех пользователей сетей доступа, обеспечивает свободный доступ к Open Garden серверам и управляет доступом к платным сервисам.

SSG принудительно перенаправляет запросы неаутентифицированных пользователей на веб-портал SESM, где они могут пройти аутентификацию или завести себе учетную запись, выбрать нужные им сервисы, пополнить баланс. Далее SSG предоставляет абонентам прозрачный доступ к выбранным сетевым сервисам и обеспечивает учет.

Функциональность RADIUS Proxu, обеспечиваемая маршрутизатором SSG, нужна в сценарии, когда сеть осуществляет аутентификацию абонентов на точках радиодоступа (см. подраздел “Точки радиодоступа (AP)”). Чтобы абонент не был вынужден второй раз аутентифицироваться на веб-странице портала, SSG должен тем или иным способом получить информацию об успешности аутентификации на уровне точки доступа. Для этого SSG может работать в режиме RADIUS Proxu, выступая в роли RADIUS-сервера для точек доступа, а на самом деле передавая RADIUS-запросы на настоящий RADIUS-сервер. В

таком случае он имеет всю необходимую информацию, чтобы сразу разрешить доступ успешно аутентифицированному на уровне точки доступа абоненту.

Для обеспечения поддержки абонентов со статическими настройками (DNS, IP-адрес) реализуется функциональность DNS Redirection и Permanent TCP Redirection, также динамическая трансляция адресов (NAT), реализованная на маршрутизаторах доступа (AZR).

Типичными сериями маршрутизаторов, подходящих для реализации функциональности шлюза контроля доступа, являются маршрутизаторы Cisco 7200, 7300 или 7400, хотя в зависимости от специфики конкретной инсталляции возможно также применение серий Cisco 2651XM и 3700.

SESM реализует портал для абонентов. Его работа тесно связана с SSG, с которым он взаимодействует по протоколу RADIUS. Для поддержки статически настроенных абонентов SESM обеспечивает функциональность HTTP Proxy, DNS Proxying/spoofing, Redirection.

SESM реализован на Java и работает на любой платформе с соответствующей версией Java Runtime Environment (JRE). Для операторских решений рекомендуется платформа Sun Solaris.

Служебные серверы (такие как SESM, DNS, сервер AAA) подключаются через коммутатор к отдельному интерфейсу маршрутизатора с SSG. По аналогичной схеме могут подключаться и серверы с локальными сервисами. В качестве локальных сервисов могут выступать предоставление абонентам платного мультимедиа-контента, специфичной для местоположения информации (например, города, в котором расположен хот-спот территориально распределенной сети организации) и т.д.

Подключение к внешним сервисам

Доступ абонентов к внешним сервисам реализуется с помощью дополнительной инфраструктуры. Одним из важнейших внешних сервисов является доступ в Интернет, хотя могут быть и другие сервисы, например доступ к корпоративной сети, к игровым сетям и т.д.

Как правило, для этого используется имеющаяся инфраструктура оператора связи (при инсталляции центральной сети у него) или инфраструктура доступа к внешним сетям общественного предприятия.

ПРИЛОЖЕНИЕ

ГЛОССАРИЙ

802.1x — стандарт IEEE, определяющий архитектуру контроля доступа на уровне логических портов устройств. Стандарт предполагает использование протокола EAP для аутентификации клиента на сервере контроля доступа и допускает различные типы сред передачи данных, такие как 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless).

802.11a — стандарт IEEE, определяющий спецификации канального и физического уровней для беспроводных ЛВС, работающих на скоростях до 54 Мбит/с в диапазоне 5 ГГц.

802.11b — стандарт IEEE, определяющий спецификации канального и физического уровней для беспроводных ЛВС, работающих на скоростях до 11 Мбит/с в диапазоне 2,4 ГГц.

802.11g — стандарт IEEE, определяющий спецификации канального и физического уровней для беспроводных ЛВС, работающих на скоростях до 54 Мбит/с в диапазоне 2,4 ГГц.

802.11i — стандарт IEEE, определяющий улучшенные средства безопасности канального уровня IEEE 802.11.

AES — сокр. от Advanced Encryption Standard. Новый стандарт шифрования, разработанный институтом National Institute of Standards and Technology (NIST) в качестве замены стандарта Data Encryption Standard (DES). AES предусматривает использование ключей шифрования увеличенной длины — 128, 192 или 256 бит.

EAP — сокр. от Extensible Authentication Protocol. “Обобщенный” протокол для обеспечения аутентификации между клиентом и сервером контроля доступа, работающий поверх протоколов 802.1x, RADIUS или TACACS+. Существуют различные виды протоколов EAP, реализующие различные методы аутентификации.

EAP-FAST — сокр. от Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling. Протокол обеспечивает взаимную аутентификацию клиента и сервера контроля доступа с помощью атрибутов Protected Access Credential (PAC) с целью установления между ними защищенного туннеля и дальнейшую аутентификацию клиента по имени пользователя/паролю. EAP-FAST обеспечивает полную поддержку динамических средств шифрования. Протокол разработан компанией Cisco Systems и доступен как предварительный стандарт IETF.

EAP-MD5 — сокр. от Extensible Authentication Protocol Message Digest 5. Протокол обеспечивает аутентификацию по имени пользователя/паролю, используя хэширование MD5 в целях безопасности. Протокол не обеспечивает взаимную аутентификацию и обмен динамическими ключами WEP.

EAP-SIM — сокр. от Extensible Authentication Protocol Subscriber Identity Module. Протокол позволяет устройствам, таким как GSM-телефонам, аутентифицироваться в сетях 802.11. EAP-SIM требует наличия в абонентском устройстве модуля SIM, содержащего информацию о пользователе.

EAP-TLS — сокр. от Extensible Authentication Protocol Transport Level Security. Протокол обеспечивает взаимную аутентификацию клиента и сервера контроля доступа с помощью цифровых сертификатов и требует наличия инфраструктуры PKI. EAP-TLS основан на протоколе SSL v3.0.

EAP-TTLS — сокр. от Extensible Authentication Protocol-Tunneled Transport Level Security. Протокол использует инфраструктуру PKI для аутентификации сервера контроля доступа и имя пользователя/пароль для аутентификации пользователей. EAP-TTLS разработан компанией Funk Software и доступен как предварительный стандарт IETF.

LAN — сокр. от Local Area Network, локальная вычислительная сеть. См. ЛВС.

LEAP — сокр. от Lightweight Extensible Authentication Protocol. Протокол обеспечивает взаимную аутентификацию пользователя и сервера контроля доступа по имени пользователя/паролю, дважды используя хэширование MD4 в целях безопасности, а также обмен динамическими ключами WEP. LEAP разработан компанией Cisco Systems.

IEEE — сокр. от Institute of Electrical and Electronics Engineers.

IOS — сокр. от Internetwork Operating System. Операционная система, под управлением которой работает широкий спектр оборудования Cisco.

PEAP — сокр. от Protected Extensible Authentication Protocol. Протокол обеспечивает гибридную аутентификацию — для аутентификации сервера контроля доступа используется инфраструктура PKI, для аутентификации клиента используется любой другой тип, например, пароли или одноразовые пароли.

PKI — сокр. от Public Key Infrastructure. Инфраструктура криптографии с открытыми ключами обеспечивает аутентификацию личности, контроль целостности и гарантию конфиденциальности передаваемых сообщений, авторизацию доступа, авторизацию транзакций и невозможность отрицания транзакций.

PoE — сокр. от Power over Ethernet. Технология передачи электропитания от сетевой инфраструктуры подключаемым к ней клиентским устройствам по стандартному медному кабелю Ethernet. Первоначально разработана компанией Cisco Systems в 2000 г. как технология Inline Power. В 2003 г. утверждена стандартом IEEE 802.3af.

RC4 — сокр. от Ron's Code 4. Алгоритм симметричного потокового шифрования, разработанный в 1987 г. Роном Райвестом (Ron Rivest).

SSID — сокр. от Service Set Identifier. Уникальный идентификатор, присваиваемый беспроводным ЛВС с целью их логического отделения друг от друга. SSID может включать в себя до 32 алфавитно-цифровых символов.

TKIP — сокр. от Temporal Key Integrity Protocol. Набор усовершенствований технологии WEP, включающие в себя контроль целостности данных (MIC) зашифрованных кадров, по пакетную смену ключей шифрования и периодическую смену широкополосного ключа.

VLAN — сокр. от Virtual Local Area Network, виртуальная локальная вычислительная сеть. Служит для логического разделения клиентских устройств ЛВС на различные широкополосные домены.

UL 2043 — стандарт Underwriters Laboratories, регламентирующий скорость выделения дыма и количество теплоты, образующейся при горении электрооборудования. Особенно важен для оборудования, размещаемого в помещениях с людьми и поблизости с воздуховодами, например, над фальшпотолками.

UNII — сокр. от Unlicensed National Information Infrastructure. Обозначает частотный диапазон в 5 ГГц области спектра, включающий в себя диапазоны UNII-1 (5,15–5,25 ГГц), UNII-2 (5,25–5,35 ГГц) и UNII-3 (5,725–5,825 ГГц).

WEP — сокр. от Wired Equivalent Privacy. Опциональные средства шифрования стандарта IEEE 802.11, основанные на алгоритме RC4.

WLAN — сокр. от Wireless Local Area Network, беспроводная локальная вычислительная сеть. См. ЛВС.

WPA — сокр. от Wi-Fi Protected Access. Совокупность средств безопасности, основанная на предварительной версии стандарта IEEE 802.11i. WPA включает в себя средства шифрования WEP и TKIP, а также протоколы 802.1x и EAP.

Аутентификация — процесс установления “личности” конечного пользователя или устройства.

Авторизация — процесс установления полномочий, доступных конечному пользователю или устройству.

Антенна — радиотехническое устройство, предназначенное для излучения или приема электромагнитных волн.

дБ — сокр. от “децибел”. Относительная логарифмическая величина, применяемая для выражения усиления или ослабления сигналов. Например, отличие двух сигналов по мощности в 10 раз означает отличие на 10 дБ, 100 раз — 20 дБ, 1000 раз — 30 дБ.

Кадр (фрейм) — логическая единица данных канального (второго) уровня семиуровневой модели взаимодействия открытых систем (OSI).

ЛВС — сокр. от “локальная вычислительная сеть”. Высокоскоростная сеть, покрывающая относительно небольшую площадь, например здание или группу зданий. Примерами технологий ЛВС являются технологии IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), IEEE 802.11 (Wireless).

Фидер — линия передачи электромагнитных волн от приемника или передатчика к антенне.

Усиление антенны — способность антенны концентрировать излученное электромагнитное поле в каком-либо определенном направлении. Характеризуется коэффициентом усиления, показывающим, насколько нужно уменьшить мощность, подводимую к направленной антенне, по сравнению с теоретической абсолютно ненаправленной антенне, чтобы среднее значение плотности потока мощности в точке наблюдения осталось таким же.

Шифрование — процесс применения к информации определенного алгоритма с целью ее изменения таким образом, чтобы прочесть ее не мог никто, кроме адресата, который должен ее расшифровать.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ



Коммутатор
Уровня 2



Коммутатор
Уровня 3



Маршрутизатор



Маршрутизатор с
функциональностью
межсетевого экрана



Межсетевой экран



Радиомост



Точка радиодоступа



Настольный ПК



Портативный ПК



Карманный ПК



Сервер управления



Сервер



Сенсор сетевой
системы обнаружения
вторжений



Принтер



Cisco Systems
Россия, 113054, Москва
бизнес-центр "Риверсайд Тауэрз"
Космодамианская наб., 52,
стр. 1, 4-1 этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
<http://www.cisco.ru>
<http://www.cisco.com>

Cisco Systems
Россия, 191186, Санкт-Петербург
бизнес-центр "Регус"
Невский проспект, 25
этаж 2, офис 30
Тел.: +7 (812) 346 77 17
Факс.: +7 (812) 346 78 00
<http://www.cisco.ru>
<http://www.cisco.com>

Cisco Systems
Казахстан, 480099, Алматы
бизнес-центр "Самал 2"
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
<http://www.cisco.ru>
<http://www.cisco.com>

Cisco Systems
Украина, 252004, Киев
бизнес-центр "Горайзон
Тауэрз"
Ул. Шовковича, 42-44, этаж 9
Тел.: +38 (044) 490 36 00
Факс: +38 (044) 490 56 66
<http://www.cisco.com/ua>
<http://www.cisco.com>

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia
• Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru •
Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South
Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States •
Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPIX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0304R)
31/1/2005