

БЕСПРОВОДНОЕ РЕШЕНИЕ CISCO ДЛЯ МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЙ

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 своих рабочих мест, но и из конференц-залов, из кафе, из других зданий. Удобства и преимущества, связанные с локальной мобильностью, помогают людям стать более продуктивными.

В результате организации по всему миру начали активно внедрять беспроводные сети с целью увеличения продуктивности и оперативности своих сотрудников, сокращения затрат и снятия ограничений, присущих традиционным проводным подключениям.

В последние годы, даже несмотря на сокращение IT-бюджетов многих компаний, рынок беспроводных ЛВС продолжает расти. По данным исследовательской компании Dell'Oro Group, в 2003 году он вырос на 21 % по сравнению с предыдущим годом и в 2007 г. составит \$3,1 млрд. Компания Synergy Research прогнозирует еще более значительный рост рынка — до \$4,98 млрд. в 2007 г.

С чем же связан такой рост? Причина проста — инвестиции в беспроводные ЛВС выгодны потребителю. Исследование, проведенное в ноябре 2003 г. компанией NOP World, одной из крупнейших в мире исследовательских компаний, показало, в чем заключаются такие выгоды.

- Беспроводные ЛВС позволяют сотрудникам оставаться подключенным к сети дополнительные 3,5 часа в день, что приводит к увеличению их продуктивности на 27 %. Рост продуктивности оказался особенно ощутимым при работе с электронной почтой и другими Интернет-приложениями.
- Использование беспроводных ЛВС в интересах бизнеса там, где это необходимо, и когда необходимо — на работе, дома и в пути — позволяет каждому сотруднику экономить почти 90 минут времени каждый рабочий день.
- 51 % респондентов отметили, что беспроводные ЛВС позволили улучшить точность выполнения повседневных задач.

Более подробную информацию о результатах этого исследования можно найти на веб-сайте Cisco по адресу http://newsroom.cisco.com/dlls/2003_NOP_WLAN_Benefits_Study.pdf.

Использование беспроводных ЛВС не обязательно означает отказ от традиционных проводных подключений. Скорее, их можно во многих случаях рассматривать как технологии, дополняющие возможности друг друга.

В ряде случаев по техническим или экономическим причинам прокладка кабельной инфраструктуры оказывается невозможной или неэффективной. Этими причинами могут быть конструктивные особенности здания, временная аренда помещений, делающая нерациональными вложения в проводку, и другие обстоятельства. В таких случаях развертывание беспроводной ЛВС становится единственно возможным решением для организации высокоскоростного доступа в сеть.

СТРУКТУРА ДОКУМЕНТА

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

Приложение 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 беспроводного решения Cisco для малых и средних предприятий. Сетевому инженеру или администратору

может быть полезно прочитать документ полностью, чтобы получить более подробную информацию о решении и составляющих его продуктах, а также ознакомиться с возможными вариантами внедрения беспроводных ЛВС.

РЕШЕНИЕ CISCO ДЛЯ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ ЛВС

Решение Cisco для построения беспроводных ЛВС прозрачно интегрируется в существующую проводную инфраструктуру организации или создает отдельные полностью беспроводные сети, обеспечивая мобильность пользователей и увеличивая их продуктивность быстро и экономически эффективно.

Решение основано на беспроводных продуктах стандартов IEEE 802.11a/b/g, предназначенных для организации связи как в пределах здания, так и между зданиями. Эти продукты включают в себя точки радиодоступа, радиомосты, антенны и аксессуары, клиентские беспроводные адаптеры, а также средства управления сетью.

ОБЗОР БЕСПРОВОДНЫХ ПРОДУКТОВ CISCO

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).

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 серией радиомостов Aironet 1300, рассмотренной в разделе “Радиомосты Cisco Aironet”.

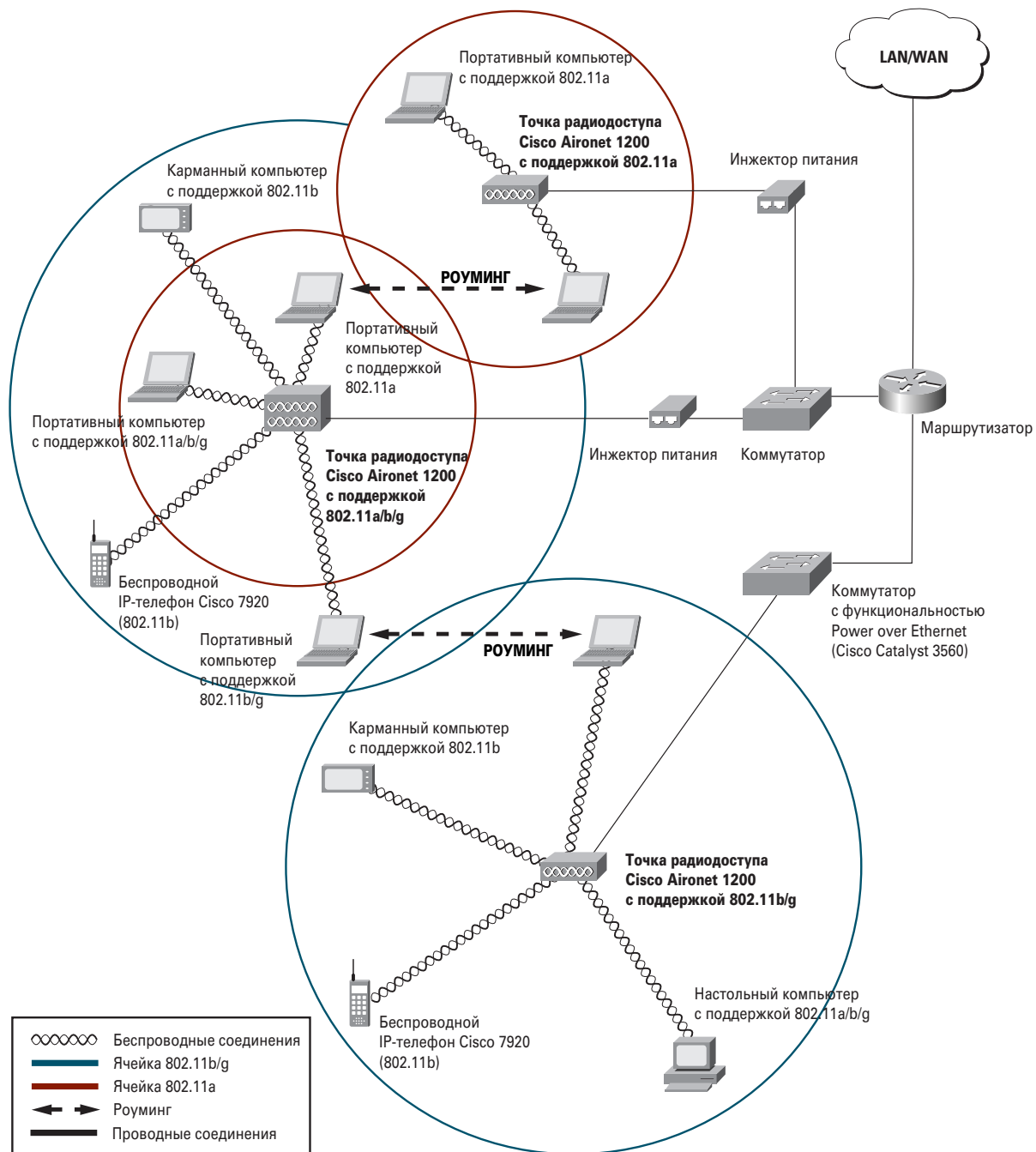


Рис. 1 Роуминг в беспроводной ЛВС

Cisco Aironet 1200



Точки радиодоступа серии Aironet 1200 обеспечивают безопасность, управляемость, возможность модернизации и надежность, необходимые для создания совре-

менных 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, одно- временно 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	Доступные модули: <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 Возможна работа в двух диапазонах одновременно для увеличения числа каналов и суммарной полосы пропускания, доступной на одном устройстве.	Доступные модули: <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
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)

Табл. 1 Характеристики точек радиодоступа Cisco Aironet 1200 и 1100

	Cisco Aironet 1200	Cisco Aironet 1100
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”).

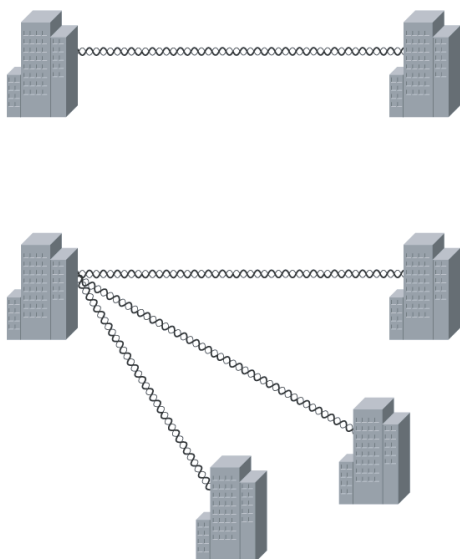


Рис. 2 Решение на базе радиомостов обеспечивает эффективную беспроводную связь между зданиями

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.

Существует отдельный класс радиомостов — мосты для рабочих групп. Эти устройства предназначены для подключения нескольких клиентских устройств с портами Ethernet к беспроводной сети.

Радиомосты Cisco для рабочих групп представлены серией Aironet 350 Series Workgroup Bridge. Серия Aironet 1300 также имеет такую функциональность.

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 инфра-

структуры 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 установке 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-Туре (антенны заказываются отдельно) или интегрированная щелевая антенна (20 дБ или 22,5 дБ)
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)

Табл. 2 Характеристики радиомостов Cisco Aironet 1300 и 1400

	Cisco Aironet 1300	Cisco Aironet 1400
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 °C до 55 °C	От -30 °C до 55 °C

Cisco Aironet 350 Workgroup Bridge



Радиомосты Aironet 350 Workgroup Bridge, разработанные для удаленных рабочих групп, небольших офисов и мобильных пользователей, предоставляют гибкость и свободу беспроводной связи любым устройствам с портами Ethernet. Мост позволяет быстро подключить к беспроводной сети до 8 компьютеров или других устройств, обеспечивая связь этих проводных устройств с точками радиодоступа или беспроводными мостами Cisco.

Основные преимущества радиомостов Cisco Aironet 350 Workgroup Bridge:

- Прозрачное подключение до 8 Ethernet-устройств к беспроводной сети;
- Высокие производительность и дальность действия;
- Стандартизованные средства обеспечения безопасности;
- Две версии устройств — с интегрированной и внешней антеннами.

Характеристики радиомоста для рабочих групп Cisco Aironet 350 Workgroup Bridge

В табл. 3 приведены основные характеристики радиомоста. Полную техническую информацию об устройстве можно найти в документации (<http://www.cisco.com/univercd>).

Табл. 3 Характеристики радиомоста Cisco Aironet 350 Workgroup Bridge

Cisco Aironet 350 Workgroup Bridge	
Поддерживаемый стандарт IEEE 802.11	802.11b (2,4 ГГц, 11 Мбит/с)
Антенны	Два разъема RP-TNC (антенны заказываются отдельно, доступен широкий ассортимент антенн различных видов) или интегрированная дипольная антенна (2 дБ)
Интерфейсы	Ethernet 10Base-T (RJ-45)
Электропитание	От локального источника
Типичная дальность действия	<ul style="list-style-type: none"> • 610 м на открытом пространстве, 107 м в помещении (1 Мбит/с) • 244 м на открытом пространстве, 40 м в помещении (11 Мбит/с)
Рабочий диапазон температур	От 0 °C до 50 °C

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.

Cisco поставляет не просто лучшие в отрасли точки радиодоступа, клиентские адаптеры и радиомосты, она предлагает полное решение для любой инсталляции

особенностям распространения сигналов. В случае организации беспроводной связи между зданиями требуется учитывать расстояния, наличие и тип препятствий, наличие промежуточных узлов и т.д.

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 связью 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-сертифици-

рованные 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 двустороннего 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).

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.

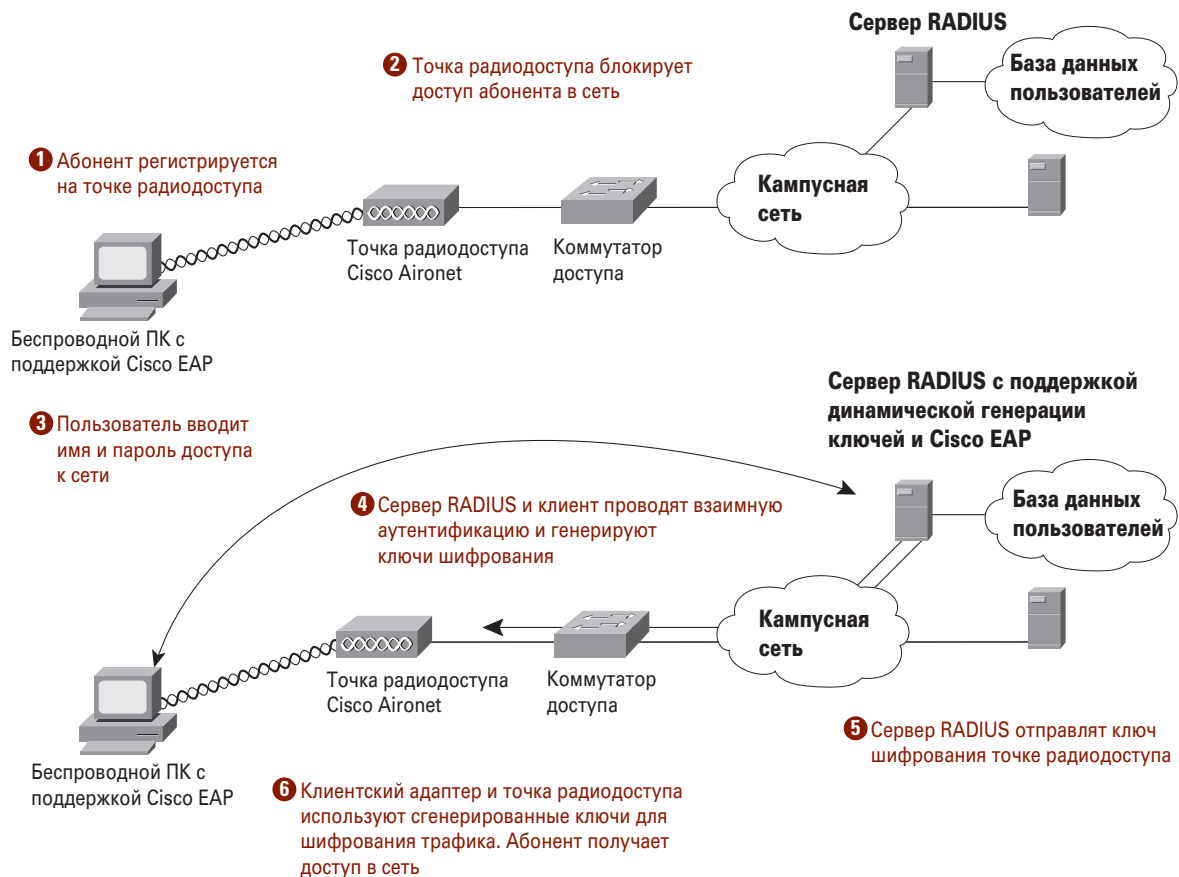


Рис. 3 Cisco Wireless Security Suite обеспечивает безопасность корпоративного класса

Аутентификация точки радиодоступа по отношению к абоненту также является очень актуальной в бизнес-среде, 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 осложняло 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 беспровод-

ной 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;

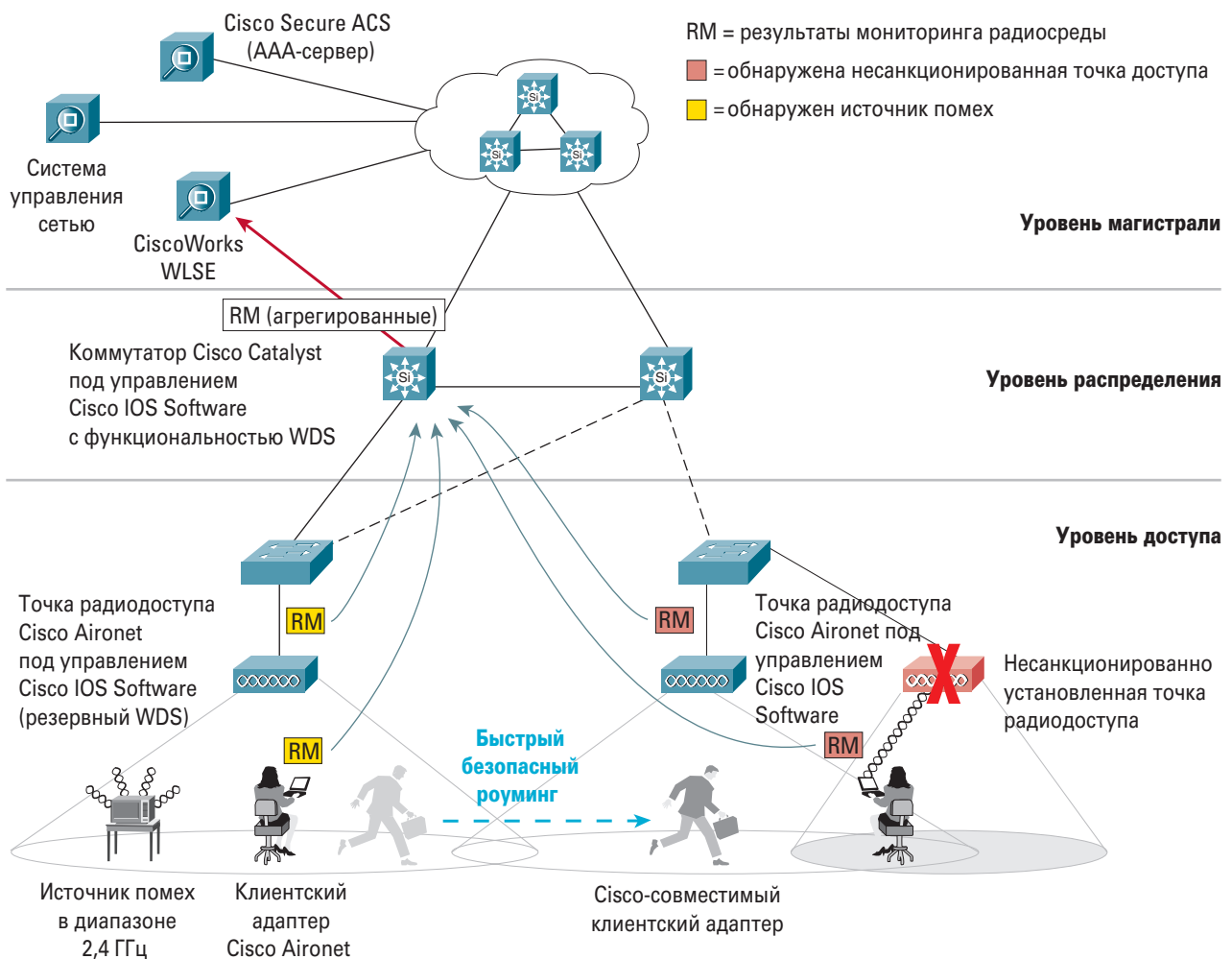


Рис. 4 Архитектура Cisco Structured Wireless-Aware Network (SWAN)

- 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.

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>.

Быстрый безопасный роуминг: Fast Secure Roaming

Быстрый безопасный роуминг, обеспечиваемый архитектурой Cisco SWAN, позволяет аутентифицированным клиентским устройствам перемещаться между зонами радиопокрытия разных точек доступа Cisco Aironet без заметных задержек (менее 150 мс). В традиционных беспроводных ЛВС типичное общее время, необходимое для роуминга, составляет свыше 500 мс. Это время уходит на ассоциацию и аутентификацию на новой точке радиодоступа. В результате в процессе роуминга возможны сбои чувствительных к задержкам приложений.

Функциональность быстрого безопасного роуминга обеспечивается за счет усовершенствования процесса сканирования радиоканалов и ускорения повторной аутентификации абонентов с помощью механизмов Cisco Centralized Key Management. Это делает возможной нормальную работу в процессе роуминга чувствительных к задержкам приложений, например IP-телефонии, ERP-приложений, основанных на Citrix решений и других приложений без потерь сессий.

Мобильность на сетевом уровне: Proxy Mobile IP

Пользуясь функциональностью Proxy Mobile IP, мобильные пользователи могут перемещаться между разными подсетями, сохраняя прозрачное соединение с сетью. Proxy Mobile IP создает туннель между маршрутизаторами “домашней” сети абонента и “удаленными” сетями, позволяя абоненту сохранить первоначальный IP-адрес даже при роуминге за пределы своей подсети. При этом мобильным пользователям не требуется какое-либо дополнительное ПО.

В результате администраторы, внедряя беспроводную сеть, могут сохранить уже существующую в своей сети схему адресации, одновременно обеспечивая прозрачную мобильность пользователей в пределах всей беспроводной сети.

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).

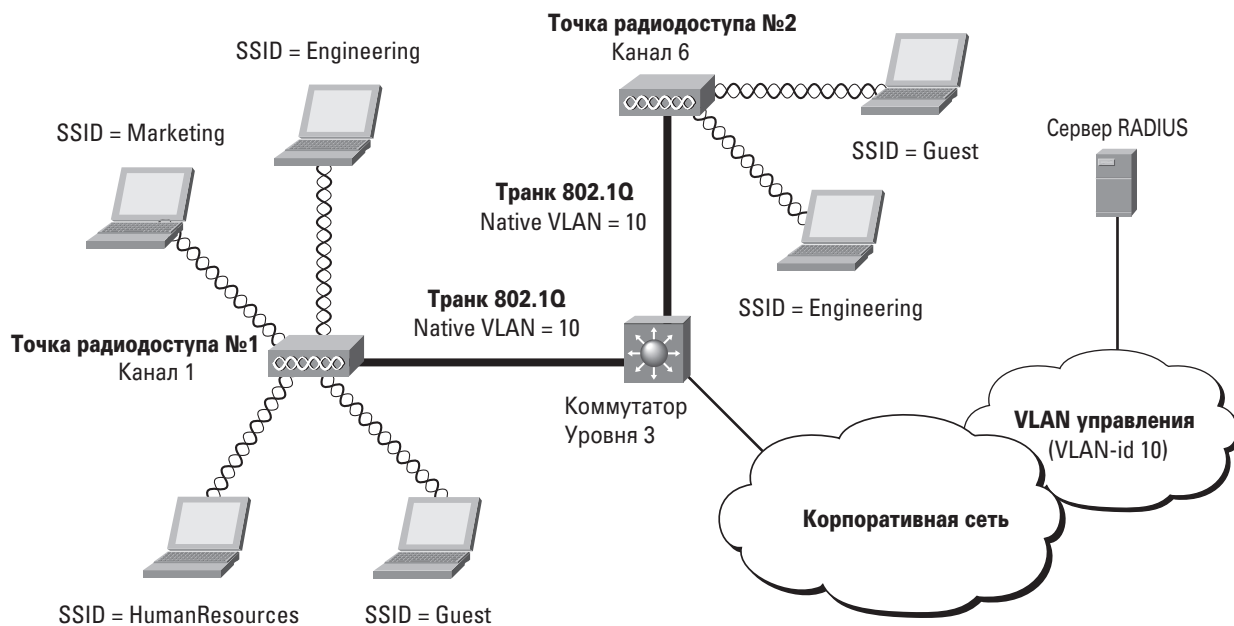


Рис. 5 Виртуальные ЛВС позволяют разделить различные типы пользователей и трафика на одной и той же инфраструктуре

Организация 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 аутентификации 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 разработок 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 самостоятельной 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>.

ВАРИАНТЫ СЕТЕВОГО ДИЗАЙНА ДЛЯ МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЙ

ОБЗОР АРХИТЕКТУРЫ

В этом разделе приводятся обобщенные варианты дизайна сетей, предназначенные для малых и средних предприятий. 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.

Предлагаемые варианты дизайна сетей не претендуют на полный охват всех возможных потребностей малых и средних предприятий; скорее, они сфокусированы на воз-

можных областях применения беспроводных ЛВС, попутно иллюстрируя соответствующую проводную инфраструктуру. По этой причине не рассматриваются или рассматриваются недостаточно подробно аспекты дизайна проводных сетей, которые должны быть раскрыты в условиях реального проектирования. Среди них — вопросы обеспечения высокой доступности сетей, вопросы масштабируемости, функциональности (например, интеграции голоса, видео и данных в одной сети) и т.д.

Разделение сетей на “малые” и “средние” учитывает возможную разницу в технических требованиях, предъявляемых к сетям разных масштабов. В то же время это разделение носит качественный характер и его не стоит воспринимать буквально. Так, например, при проектировании конкретной сети решения, рассмотренные в дизайне средней сети, могут быть применены к малой сети и наоборот.

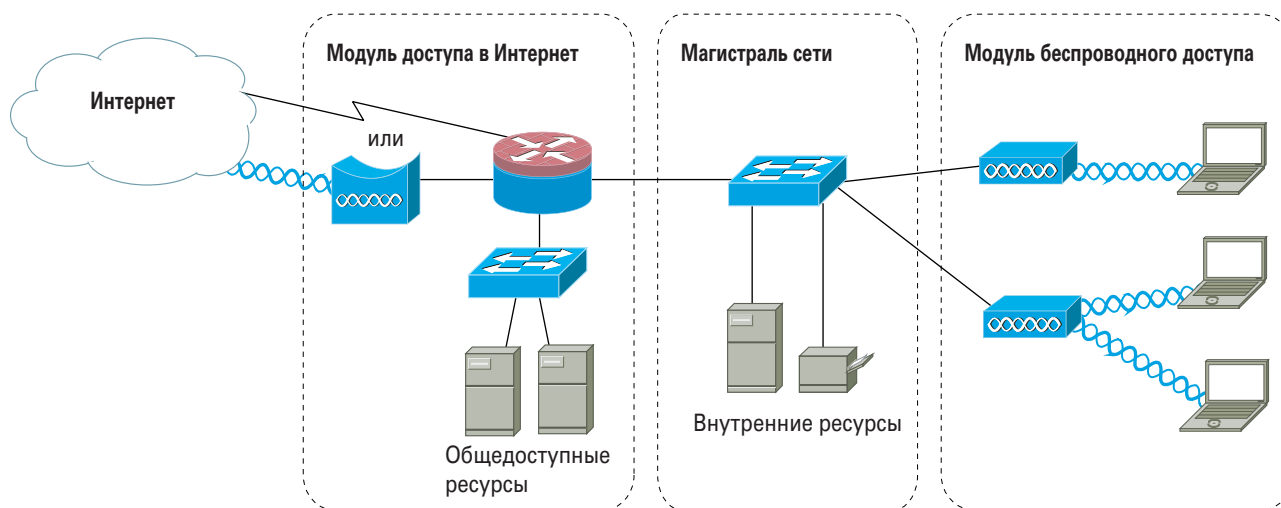


Рис. 6 Вариант дизайна сети малого размера

Обсуждение этого дизайна большей частью ведется на основе малой сети как главной сети организации; также говорится о специфических изменениях дизайна при конфигурации для филиала.

Модуль беспроводного доступа

Модуль обеспечивает связь мобильных пользователей с проводной сетью. В случае малой сети его могут составлять одна или несколько точек радиодоступа, количество и характеристики которых выбираются в зависимости от требований к радиопокрытию, производительности и т.д.

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

ДИЗАЙН СЕТИ МАЛОГО РАЗМЕРА

Типовой дизайн сети малого размера (рис. 6) включает в себя беспроводную и проводную инфраструктуру. Беспроводная инфраструктура обеспечивает доступ мобильных пользователей к ресурсам сети и, возможно, доступ в Интернет. Проводная инфраструктура образует магистраль и периферию ЛВС организации.

В дизайне сети малого размера можно выделить 3 модуля:

- Модуль беспроводного доступа;
- Магистраль локальной проводной сети;
- Модуль доступа в Интернет.

Точки радиодоступа могут поддерживать виртуальные ЛВС, например для сотрудников, гостей, беспроводных IP-телефонов. В этом случае маршрутизация между виртуальными ЛВС может быть реализована в зависимости от требований к производительности на коммутаторе Уровня 3 или маршрутизаторе, устанавливаемым в магистральной сети. Эти же устройства могут производить пакетную фильтрацию между виртуальными сетями для обеспечения контроля доступа, например, предоставляя гостям только доступ в Интернет и к принтеру, в то же время блокируя доступ к серверу с конфиденциальной информацией. Альтернативным вариантом в случае малой сети может быть пакетная

фильтрация на Уровнях 2/3/4 на точке радиодоступа, но это создает дополнительную нагрузку на нее и снижает масштабируемость.

Безопасность беспроводной ЛВС является очень важным вопросом независимо от масштаба сети. Для обеспечения целостности и конфиденциальности данных организации, а также для защиты от несанкционированного доступа в беспроводную сеть необходимо применять современные средства безопасности. На данный момент к ним относятся архитектура аутентификации IEEE 802.1x, протоколы аутентификации EAP (например, LEAP и EAP-FAST) и усовершенствования технологии шифрования WEP под названием TKIP (Temporal Key Integrity Protocol), см. раздел “Высокая безопасность: Cisco Wireless Security Suite”.

Аутентификация беспроводных пользователей по протоколу 802.1x может производиться не централизованным RADIUS-сервером, а самими точками радиодоступа. Это ограничивает масштабируемость, но может быть приемлемым в случае малой сети. Точки радиодоступа Cisco Aironet могут локально аутентифицировать до 50 беспроводных абонентов.

Альтернативный вариант относится к реализации малой сети как сети филиала организации. В таком случае аутентификация может производиться на централизованном сервере контроля доступа, установленном в главном офисе, а локальная аутентификация на точках радиодоступа может применяться в случае нарушения связи с этим сервером. Это позволяет повысить отказоустойчивость, сохраняя масштабируемость.

Поддержка точками радиодоступа приоритезации трафика позволяет применять беспроводную инфраструктуру и для качественной поддержки чувствительных к задержкам приложений, например IP-телефонии.

Магистраль сети

Магистраль сети обеспечивает обмен трафиком между модулем беспроводного доступа и периферией сети организации. Магистраль сети малого предприятия может быть реализована на одном коммутаторе Уровня 2 или Уровня 3, к которому подключаются как устройства соседних модулей, так и другое оборудование, например внутренние серверы, принтеры и ПК. Возможная

альтернатива — оснащение такого оборудования беспроводными интерфейсами и подключение его к сети в модуле беспроводного доступа. В случае невозможности установки беспроводных интерфейсов (например, у принтера), можно подключить такие устройства к радиомосту для рабочих групп.

Для удобства и гибкости инсталляции коммутатор может обладать функциональностью Power over Ethernet (PoE). В этом случае отпадает необходимость использования адаптеров питания для точек радиодоступа и, возможно, других устройств, например IP-телефонов, видеокамер и т.д.

Модуль доступа в Интернет

Основная задача модуля заключается в подключении сети организации к Интернет. В случае малой сети модуль может быть образован маршрутизатором с функциональностью межсетевого экрана или специализированным межсетевым экраном в зависимости от требований к интерфейсам, а также программной и аппаратной функциональности. Эти устройства обеспечивают защиту периметра сети. Кроме того, они также могут реализовывать и другую функциональность, например фильтрацию передаваемого контента на прикладном уровне и систему обнаружения вторжений для активного реагирования на сетевые атаки.

Подключение к Интернет может быть как проводным, так и беспроводным. Беспроводной доступ в Интернет можно обеспечить с помощью радиомоста, взаимодействующего с радиомостом поставщика услуг Интернет.

Межсетевой экран может также терминировать VPN-соединения с удаленными пользователями. В случае дизайна для сети филиала он же может поддерживать VPN-соединение с главным офисом.

Модуль также может обеспечивать подключение к Интернет демилитаризованной зоны при ее наличии в сети организации. Демилитаризованная зона содержит серверы с общедоступной информацией об организации. Например, в ней могут размещаться общедоступные серверы HTTP и FTP, а также серверы DNS и SMTP. Демилитаризованная зона создается из соображений безопасности как обособленный от внутренней сети сегмент, подключаемый к отдельному интерфейсу межсетевого экрана.

ДИЗАЙН СЕТИ СРЕДНЕГО РАЗМЕРА

Дизайн сети среднего размера может охватывать как одно здание, так и удаленные подразделения, находящиеся в других зданиях. В таком случае беспроводная инфраструктура может применяться не только для обеспечения доступа в сеть мобильных пользователей, мобильных рабочих групп и подключения сети к Интернет, но и для организации связи между главным офисом и удаленными подразделениями.

Рассматриваемый вариант дизайна сети среднего размера (рис. 7) охватывает сеть удаленного подразделения (здание А) и сеть главного офиса (здание Б), включающую в себя:

- Модуль беспроводного доступа;
- Модуль беспроводной связи между зданиями;
- Магистраль локальной проводной сети;
- Серверный модуль;
- Модуль доступа в Интернет.

Модуль беспроводного доступа

Модуль беспроводного доступа обеспечивает связь мобильных пользователей с проводной сетью. Важнейшими устройствами модуля являются точки радиодоступа, количество, расположение и характеристики которых определяются в зависимости от требований к радиопокрытию, производительности и т.д. путем проведения обследования объекта (site survey). Процедура обследования объекта может быть облегчена с помощью современных средств управления беспроводной сетью. Так, например, сервер управления CiscoWorks Wireless LAN Solution Engine, входящий в архитектуру Cisco Structured Wireless-Aware Network, позволяет автоматически установить оптимальные значения излучаемой точками радиодоступа мощности и выбрать оптимальные частотные каналы.

После развертывания беспроводной сети возникает задача ее эффективной эксплуатации. Эта непростая сама по себе задача осложняется при отсутствии в штате организации специалиста в области беспроводных сетей. В таких случаях применение средств управления беспроводной сетью становится особенно эффективным.

С ростом количества точек радиодоступа обеспечение роуминга между ними, прозрачного для пользователей, становится все более актуальным. Этот вопрос решается с помощью функциональности быстрого безопасного роу-

минга архитектуры Cisco Structured Wireless-Aware Network, рассмотренной более подробно в разделе “Быстрый безопасный роуминг: Fast Secure Roaming”. Поскольку сеть средней организации включает в себя различные IP-подсети, актуальной также является и задача обеспечения мобильности беспроводных абонентов между разными подсетями с сохранением одного и того же IP-адреса. Решение этой задачи обеспечивается функциональностью Proху Mobile IP точек радиодоступа Cisco или функциональностью модуля Wireless LAN Services Module (WLSM) для коммутаторов серии Catalyst 6500.

В сети среднего предприятия могут находиться абоненты и устройства, которым необходимы различные уровни доступа к сети и настройки безопасности, например, беспроводные ПК постоянных, временных сотрудников и гостей, а также устройства других типов, такие как беспроводные IP-телефоны. Их сегментация может быть успешно проведена с помощью виртуальных локальных сетей, поддержка которых реализована на точках радиодоступа и в соответствующей проводной инфраструктуре.

Безопасность беспроводной ЛВС является очень важным вопросом независимо от масштаба сети. Для обеспечения целостности и конфиденциальности данных организации, а также для защиты от несанкционированного доступа в беспроводную сеть необходимо применять современные средства безопасности.

На данный момент к ним относятся архитектура аутентификации IEEE 802.1x, протоколы аутентификации EAP (например, LEAP и EAP-FAST) и усовершенствования технологии шифрования WEP под названием TKIP (Temporal Key Integrity Protocol), см. раздел “Высокая безопасность: Cisco Wireless Security Suite”.

Сеть удаленного подразделения по структуре напоминает сеть малого предприятия, рассмотренную в предыдущем разделе, хотя в нее внесены изменения, учитывающие специфику случая. Так, в данном случае в дизайне сети отсутствует демилитаризованная зона, а модуль доступа в Интернет заменен на модуль беспроводной связи между зданиями. Соображения, изложенные в предыдущем разделе применительно к магистральной сети, подходят и для магистральной сети удаленного подразделения настоящего раздела. Модуль беспроводного доступа рассмотрен в настоящем разделе.

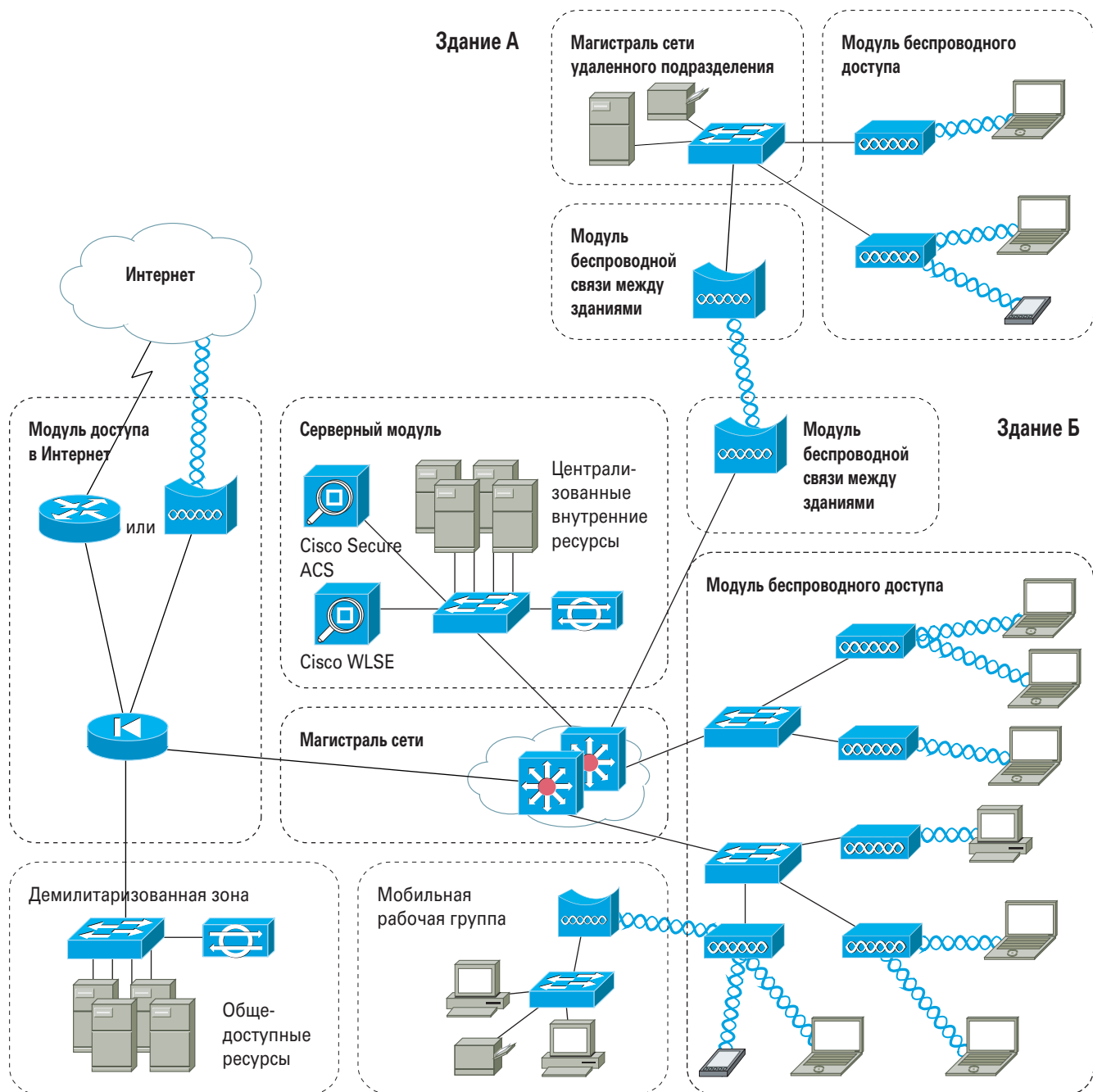


Рис. 7 Вариант дизайна сети среднего размера

Из соображений масштабируемости и управляемости аутентификация беспроводных пользователей по протоколу 802.1x в случае средней сети производится централизованным сервером контроля доступа, например сервером Cisco Secure Access Control Server, установленным в сервер-

ном модуле. Для обеспечения отказоустойчивости такие серверы могут резервироваться, а между ними может быть настроена репликация базы данных пользователей.

Централизованная аутентификация относится и к беспроводным абонентам удаленного подразделения. Для обеспечения доступа этих абонентов в сеть даже в случае

нарушения связи с сервером контроля доступа может применяться локальная аутентификация на точках радиодоступа удаленного подразделения. Точки радиодоступа Cisco Aironet могут локально аутентифицировать до 50 беспроводных абонентов.

Очень часто в корпоративной среде пользователям требуется связь с централизованными сетевыми ресурсами, но не требуется связь между собой. В таких случаях с целью нейтрализации атак типа “злоупотребление доверием” взаимодействие пользователей между собой блокируется путем применения техники частных виртуальных сетей на коммутаторе доступа. Точки радиодоступа Cisco Aironet позволяют достичь этой цели и в случае беспроводной сети с помощью функциональности Public Secure Packet Forwarding (PSPF).

Поддержка точками радиодоступа приоритезации трафика позволяет применять беспроводную инфраструктуру и для качественной поддержки чувствительных к задержкам приложений, например IP-телефонии, ERP-приложений и т.д.

В сети организации могут присутствовать устройства, нуждающиеся в беспроводной связи, но не имеющие беспроводных интерфейсов, например сетевые принтеры или любые другие устройства с портами Ethernet. Такие устройства, обозначенные на рис. 7 мобильной рабочей группой, можно подключить к беспроводной сети с помощью радиомоста для рабочих групп.

В модуль беспроводного доступа средней сети также могут входить коммутаторы доступа (Уровня 2 или Уровня 3), обеспечивающие подключение точек радиодоступа к проводной сети. Для удобства и гибкости инсталляции коммутаторы доступа могут обладать функциональностью Power over Ethernet (PoE). В этом случае отпадает необходимость использования адаптеров питания для точек радиодоступа и, возможно, других устройств, например IP-телефонов, видеокамер и других устройств.

Модуль беспроводной связи между зданиями

Модуль обеспечивает связь между сетями главного офиса и удаленного подразделения и включает в себя радиомост. Радиомост устанавливается в каждом из объединяемых зданий.

Перед установкой радиомостов производится обследование объекта (site survey), учитывающее особенности данной конкретной инсталляции. С учетом требований к производительности, дальности действия и покрываемой территории определяется оборудование, необходимое для инсталляции.

Для обеспечения отказоустойчивости или балансировки нагрузки возможна установка двух пар радиомостов Cisco Aironet, работающих на неперекрывающихся частотных каналах.

При наличии нескольких удаленных подразделений можно подключить их сети с помощью радиомостов к главному (root) мосту, установленному в центральном офисе. В этом случае реализуется топология “точка-многоточка”.

Радиомосты Cisco Aironet поддерживают функциональность виртуальных ЛВС. Это позволяет, например, передать из удаленного подразделения транк 802.1q и терминировать на его устройстве Уровня 3, установленном в главном офисе.

Поддержка приоритезации трафика позволяет обмениваться с удаленными подразделениями чувствительным к задержкам трафиком, например трафиком системы IP-телефонии. В результате отпадает необходимость обеспечения удаленных подразделений отдельным подключением к телефонной сети общего пользования (ТФОП) и появляется возможность использования подключения к ТФОП главного офиса.

Для обеспечения целостности и конфиденциальности передаваемых данных можно использовать средства усиления шифрования TKIP (Temporal Key Integrity Protocol), а радиомосты удаленных подразделений и центрального офиса подвергать взаимной аутентификации по протоколу EAP.

Магистраль сети

Магистраль сети обеспечивает обмен трафиком между подключаемыми к ней модулями (рис. 7). В случае средней сети магистраль может быть объединена с уровнем распределения и состоять из пары коммутаторов Уровня 3 для обеспечения отказоустойчивости и балансировки нагрузки, хотя возможен и более развитый дизайн. Более того, в процессе развития бизнеса организации и, соответственно, ее сети переход к классическому многоуровневому дизайну, при котором в сети выделяются отдельные уровни доступа/

распределения/магистрала, неизбежен. Это связано с тем, что только при таком подходе возможно рациональное использование функциональных возможностей оборудования в соответствующих точках сети и, следовательно, минимизация общей стоимости владения сетью.

Подробное рассмотрение сетевого дизайна выходит за рамки данного документа. Эту информацию можно найти на веб-сайте Cisco по адресу <http://www.cisco.com/go/design>.

Серверный модуль

Модуль содержит централизованные внутренние серверы организации, с которыми работают пользователи как главного офиса, так и удаленных подразделений. В этом же модуле могут находиться и служебные серверы, такие как CiscoWorks Wireless LAN Solution Engine и Cisco Secure Access Control Server.

Для обеспечения повышенной безопасности ресурсов серверного модуля помимо хостовых средств защиты могут применяться и сетевые средства, например сетевая система обнаружения вторжений.

Модуль доступа в Интернет

Основная задача модуля заключается в подключении сети организации к Интернет. В случае средней сети модуль может быть образован маршрутизатором для связи с поставщиком услуг Интернет и межсетевым экраном для защиты периметра сети организации. Из соображений отказоустойчивости маршрутизатор и межсетевой экран могут резервироваться.

Применение маршрутизаторов и межсетевых экранов как отдельных устройств обеспечивают более высокую масштабируемость, поскольку в общем случае система доступа в Интернет может включать в себя дополнительные подсистемы (например, демилитаризованную зону, модули удаленного доступа и электронной коммерции). Кроме того, такой подход обеспечивает более эффективное использование возможностей этих устройств и эшелонированный подход к защите периметра сети.

Подключение к Интернет может быть как проводным, так и беспроводным. Беспроводной доступ в Интернет можно обеспечить с помощью радиомоста, взаимодействующего с радиомостом поставщика услуг Интернет.

Модуль также может обеспечивать подключение к Интернет демилитаризованной зоны при ее наличии в сети организации. Демилитаризованная зона содержит серверы с общедоступной информацией об организации. Например, в ней могут размещаться общедоступные серверы HTTP и FTP, а также серверы DNS и SMTP. Демилитаризованная зона создается из соображений безопасности как обособленный от внутренней сети сегмент, подключаемый к отдельному интерфейсу межсетевого экрана. Для обеспечения повышенной безопасности ресурсов демилитаризованной зоны помимо хостовых средств защиты могут применяться и сетевые средства, например сетевая система обнаружения вторжений.

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. Реном 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 ширококестельного ключа.

VLAN — сокр. от Virtual Local Area Network, виртуальная локальная вычислительная сеть. Служит для логического разделения клиентских устройств ЛВС на различные ширококестельные 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 прочитать ее не мог никто, кроме адресата, который должен ее расшифровать.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ



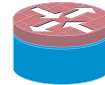
Коммутатор
Уровня 2



Коммутатор
Уровня 3



Маршрутизатор



Маршрутизатор с
функциональностью
межсетевого экрана



Межсетевого 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