

Сетевой доступ без границ

Представление о рабочем месте изменяется. Теперь оно не ограничивается офисом и даже страной, в которой мы работаем.

"Сети без границ" — это архитектура Cisco® нового поколения, которая способствует созданию эффективного процесса доставки сервисов и приложений, меняя таким образом представление о рабочем месте. Архитектура обеспечивает безопасный, надежный и постоянный доступ к любому ресурсу при помощи любого устройства для любых пользователей в любой точке мира. Архитектура "Сети без границ" Cisco решает основные задачи ИТ и бизнеса, обеспечивая подлинную "работу без границ" благодаря более тесному взаимодействию с сотрудниками и заказчиками.

Работа "без границ" возможна только благодаря интеллектуальным сетевым элементам, предназначенным и спроектированным в соответствии с требованиями глобального рабочего пространства, в котором численность мобильных ресурсов постоянно растет. Решения "доступа без границ" Cisco являются главным компонентом этой архитектуры, который позволяет реализовать различные сервисы, такие как мобильность, безопасность, медиасеть и технология Cisco EnergyWise. Использование этих сервисов позволяет упростить эксплуатацию ИТ-инфраструктуры организации и повысить производительность работы сотрудников. При использовании интеллектуального уровня доступа, обладающего необходимой информацией о контексте работы, средства уровня доступа располагают идентификационной информацией пользователя, а также сведениями о его местонахождении в сети. При использовании такого уровня доступа можно определить тип подключающегося к сети устройства и настроить сеть на предоставление оптимального качества обслуживания (QoS) и доступа к сервисам. Уровень доступа получает возможность учитывать особенности функционирования различных сервисов и создать оптимальные условия для работы пользователя. Только использование сетей с интеллектуальным уровнем доступа может позволить организации выполнить беспрепятственный переход к защищенным сетям "без границ". Ваша организация сможет снизить уровень энергопотребления и упростить процедуры эксплуатации ИТ-инфраструктуры, а также повысить свою рентабельность, приведя совокупную стоимость владения к оптимальным показателям.

Решения Cisco по построению уровня доступа для организаций без границ сосредоточены в следующих ключевых областях (рис. 1):

- **Устойчивость.** Решения коммутации Cisco Catalyst® позволяют организации уделять больше внимания охране окружающей среды путем измерения эффективности энергопотребления, интеграции сервисов и постоянного интегрирования инноваций, таких как технология Cisco EnergyWise. Она представляет собой решение корпоративного класса, позволяющее снизить затраты на электроснабжение и объемы выбросов парниковых газов. Технология EnergyWise отслеживает энергопотребление всех устройств Cisco, подключенных к сети — от устройств PoE до контроллеров зданий, подключенных к IP-сети — и создает комплексные отчеты по энергопотреблению, позволяющие оптимизировать общий объем энергопотребления на основе пользовательских политик.
- **Упрощение эксплуатации.** Технология Catalyst Smart Operations — это комплексный набор средств, упрощающих развертывание, настройку и устранение неполадок локальных сетей. В дополнение к адаптивным технологиям, предусматривающим постоянную работу устройств (например, Cisco StackWise® и FlexStack), технология Smart Operations обеспечивает полностью автоматическую установку и замену коммутаторов, быстрое обновление и упрощение системы устранения неполадок при одновременном снижении эксплуатационных затрат. Коммутаторы Cisco Catalyst автоматически применяют необходимые настройки в зависимости от подключаемого сетевого устройства (беспроводная точка доступа, IP-телефон, видеочасть и т. п.), упрощая таким образом настройку сети и обеспечивая мобильность. При применении шаблонов, основанных на оптимальных методиках Cisco, ошибки настройки сводятся к минимуму, а ввод сети в эксплуатацию выполняется с минимумом усилий.

- Безопасность сетей без границ.** Решение Cisco TrustSec — это основной компонент архитектуры Cisco Borderless Security, который обеспечивает безопасный доступ к корпоративным сервисам приложений на основе системы идентификации пользователей. Среди возможностей решения TrustSec — контроль доступа с учетом политик, обеспечение работы в сети с идентификацией и назначением ролей, а также целостности и конфиденциальности данных. Кроме того, коммутаторы Cisco Catalyst используют встроенные средства обеспечения безопасности — ведущее в отрасли решение, которое предоставляет надежную защиту на уровне 2, противодействуя атакам типа "посредник" (например, подмена MAC-адреса или IP-адреса отправителя или атаки на протокол ARP). Предоставляя мощные и удобные средства для эффективного предотвращения большинства типовых и потенциально разрушительных угроз безопасности уровня 2, встроенные средства безопасности Cisco обеспечивают надежную защиту всей сети. Более того, развертывание комплексной системы предотвращения вторжений (IPS) для проводных и беспроводных сетей также помогает защититься от сетевых атак.
- Работа в "сети без границ".** Чтобы конечные пользователи смогли оценить преимущества работы в сети без границ, важно предоставить им возможности безопасного и надежного подключения из любой точки мира, что, в свою очередь, положительно скажется на производительности. Хотя Ethernet уже является стандартом де-факто для построения локальной предприятия, в последнее время все большее распространения получают беспроводные сети, обеспечивающие работу все более мобильных сотрудников. С ратификацией стандарта 802.11n беспроводные сети теперь дополняют проводные там, где это допустимо по соображениям производительности и надежности. Еще одним требованием для эффективной работы в "сетях без границ" является поддержка все более популярных видеоприложений, которые способствуют эффективной совместной работе и позволяют сократить затраты. Медиасеть Cisco позволяет сформировать надежную платформу для передачи качественного видеоизображения по той же проводной и беспроводной сети, по которой передаются данные и голос. Медиасеть Cisco использует интеллектуальные сетевые решения, позволяющие снизить сложность ИТ-инфраструктуры и ускорить развертывание мультимедийных решений путем динамического выделения ресурсов, необходимых для обеспечения качества обслуживания (QoS) и доставки контента.

Рис. 1. Четыре ключевых области решений Cisco в области сетевого доступа



Устойчивость

Повышение стоимости электроэнергии, необходимость защиты окружающей среды и законодательные требования породили необходимость в надежной и экологичной работе ИТ-инфраструктуры. Сегодня методы измерения энергопотребления и контроля над использованием электроэнергии являются объектом внимания организаций по всему миру. Все заказчики ищут способы снизить энергопотребление и повысить эффективность работы. Кроме того, они хотят сформировать единое решение для управления расходом электроэнергии различными устройствами и средствами коммуникации.

Технология Cisco EnergyWise — новая архитектура управления энергопотреблением, которая позволяет средствам и ресурсам ИТ выполнять измерения и тонкую настройку использования электроэнергии, чтобы значительно сократить расходы. Технология Cisco EnergyWise позволяет снизить энергопотребление на всех устройствах, подключенных к сети Cisco — от устройств PoE (например, IP-телефонов) и точек беспроводного доступа до контроллеров зданий и системы освещения. Эта технология основана на архитектуре интеллектуальной сети и позволяет ИТ-подразделениям и коммунальным службам осознавать, оптимизировать, и эффективно управлять энергопотреблением в масштабе всей корпоративной инфраструктуры, контролируя практически каждое устройство, подключенное к сети. Коммутаторы Cisco Catalyst (в том числе Cisco Catalyst серий 2960-S, 3560-X и 3750-X) поддерживают технологию Cisco EnergyWise. Дополнительное измерительное оборудование в составе коммутаторов Cisco Catalyst серий 3560-X и 3750-X обеспечивает возможность более точного измерения большего числа параметров энергопотребления и управления ими.

Для получения дополнительных сведений о технологии Cisco EnergyWise посетите страницу http://www.cisco.com/en/US/prod/switches/ps5718/ps10195/white_paper_c11-514539.html.

Упрощение развертывания коммутаторов и сокращение расходов с помощью Catalyst Smart Operations

Catalyst Smart Operations — это комплексный набор средств, упрощающих развертывания коммутаторов локальной сети и точек беспроводного доступа, а также позволяющих снизить совокупную стоимость владения. Оптимизация процедур эксплуатации ИТ-инфраструктуры предприятия позволяет сократить расходы и обеспечивает работу сети на уровне, необходимом для приложений нового поколения. Технология Catalyst Smart Operations помогает организациям оптимизировать процедуру эксплуатации и ускоряет выполнение процедур предоставления доступа к сервисам и масштабирования сервисов в сети специалистами ИТ-подразделения.

Как Catalyst Smart Operations помогает на предприятии?

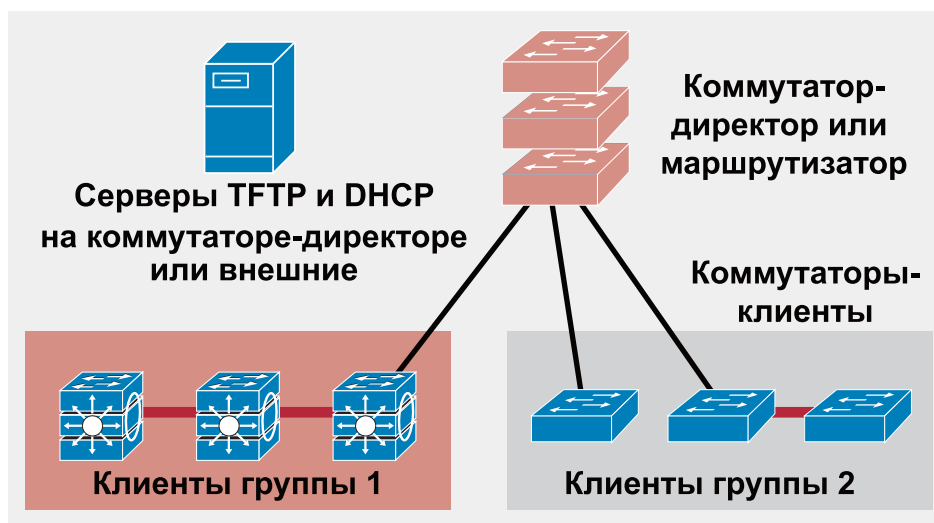
Catalyst Smart Operations позволяет сделать установку, настройку, замену и диагностику LAN проще и дешевле за счет упрощения эксплуатации и развертывания сети. Технология Catalyst Smart Operations включает три основных механизма: Smart Install, Smart Configuration и Smart Troubleshooting. Smart Install обеспечивает полную автоматизацию установки коммутаторов в сети, Smart Configuration — быстрое обновление и автоматическую замену коммутатора, а Smart Troubleshooting облегчает поиск и устранение неполадок. На рисунке 2 показаны эти решения и их преимущества для предприятия.

Рис. 2. Три основных механизма Catalyst Smart Operations

**Smart Install: установка сети доступна каждому**

Catalyst Smart Operations использует Smart Install для запуска технологии plug and play, обеспечивающей простоту установки образа ПО ОС Cisco IOS® и настройки коммутаторов с минимальным участием пользователя. Все, что необходимо сделать пользователю для запуска процесса установки в режиме plug and play — это распаковать коммутатор, включить его и подключить к сети. Принцип работы Smart Install основан на идее использования коммутатора-директора или сетевого коммутатора, который помогает установить другие коммутаторы. Коммутатором-директором могут служить коммутаторы семейства Cisco Catalyst серий 3560 или 3750, а все остальные устанавливаемые коммутаторы-клиенты могут принадлежать семейству Catalyst серий 2960, 3560, или 3750 (см. рис. 3).

Рис. 3. Сеть с поддержкой решения Smart Install



На коммутаторе-директоре настраивается информация о местоположении образов и файлов конфигурации. После того, настройка любого коммутатора, подключаемого к директору, будет выполнена при помощи механизма на основе протокола DHCP. Пользователю потребуется указать DHCP-сервер, который будет выделять IP-адреса, и TFTP-сервер, на котором хранятся файлы образов и файлы конфигурации. Эти серверы могут располагаться как на коммутаторе-директоре, так и на других серверах. Директор будет вести список всех коммутаторов в сети и сможет предоставлять пользователю подробные сведения об этих коммутаторах, в том числе тип коммутатора, имя хоста, IP-адрес и версию Cisco IOS. Механизм Smart Install может назначать имена хостов и создавать постоянные IP-адреса для клиентских коммутаторов, снимая с администратора нагрузку по ведению схемы IP-адресации. В группы коммутаторов, определенные на директоре, обычно включаются похожие коммутаторы одного типа. Все устройства, входящие в группу, могут обновляться одновременно, что упрощает процедуры обновления и управления изменениями на коммутаторах.

Smart Configuration: автоматическая настройка при помощи Auto SmartPorts

Механизм Smart Install используется для установки любого коммутатора в сети при помощи технологии plug and play. Использование Auto SmartPorts в сочетании со Smart Install позволяет ускорить и упростить процесс установки. Smart Install может загрузить окончательную конфигурацию коммутатора на клиентский коммутатор, но только при условии, что к каждому порту будет подключено предварительно заданное устройство. Например, первые 10 портов выделены для подключения IP-телефонов, а порты с 11 до 20 выделены для точек доступа, и эту схему необходимо задать перед установкой коммутатора.

Механизм Auto SmartPorts может автоматически настраивать порты доступа в зависимости от устройства, подключаемого к порту. Не обязательно знать, к какому порту необходимо подключить каждое устройство, поскольку по мере подключения устройств выполняется автоматическое определение их типа, а порт настраивается автоматически. Поэтому базовую конфигурацию можно загрузить при помощи Smart Install, а автоматическая настройка портов Ethernet при помощи Auto SmartPorts будет происходить по мере подключения устройств к сети. Всю процедуру установки можно выполнить без знания конфигурации Cisco IOS. Поддерживается автоматическое обнаружение и настройка портов для любых устройств с уникальным идентификатором производителя в MAC-адресе (OUI), в том числе принтеров, ПК и устройств, которые поддерживают протоколы CDP и LLDP, например, IP-телефонов, точек доступа и IP-камер. Также при отключении устройства от порта коммутатора соответствующую конфигурацию можно удалить с этого порта. Эта особенность позволяет пользователям перемещать устройства с одного порта на другой.

Auto SmartPorts настраивает порт в соответствии с предварительно заданными конфигурациями, которые основываются на многолетнем опыте Cisco в области сетевых технологий, в т. ч. в сфере безопасности, мобильности и IP-телефонии, обеспечения доступности, качества (QoS) и управляемости. При этом от пользователя требуются минимальные усилия и знания. Механизм Auto SmartPorts также поддерживает макрокоманды, которые могут быть заданы пользователем. Пользователь может применить встроенные макрокоманды Cisco или изменить их, чтобы создать конфигурацию, подходящую для нужд предприятия.

Smart Configuration: управление конфигурациями и замена устройств без участия оператора

Директор Smart Install может выполнять не только задачи первоначальной установки коммутаторов, но и решать текущие задачи управления конфигурациями, резервного копирования настроек, а также при необходимости заменить коммутатор без участия оператора. Администратор может использовать коммутатор-директор как единую точку управления группой коммутаторов, что позволяет проводить одновременное обновление или настройку группы коммутаторов. Кроме того, любые изменения конфигурации коммутаторов-клиентов будут автоматически резервироваться и архивироваться на директоре или на сетевом TFTP-сервере. В ходе процесса Smart Configuration для каждого коммутатора архивируются два экземпляра конфигурации с предыдущими и самыми последними настройками. Функция архивирования конфигураций делает возможной замену любого неисправного коммутатора без участия оператора. Директор отслеживает конфигурацию, привязанную к клиенту. Поэтому при замене неисправного коммутатора на новый коммутатор загружается последний файл конфигурации и образ Cisco IOS, что обеспечивает замену коммутаторов без участия оператора. Замена коммутатора настолько проста, что любой пользователь может отключить неисправный коммутатор и заменить его коммутатором аналогичной модели, после чего сеть сама настроит новый коммутатор.

Smart Configuration: снижение операционных затрат

Очевидно, что Catalyst Smart Operations позволяет сократить расходы и упростить эксплуатацию коммутаторов и подключенных устройств. В таблице 1 показаны типичные значения показателей ROI при использовании механизмов Catalyst Smart Operations. Экономия затрат обычно превышает 70 процентов после внедрения Smart Install и Smart Configuration. Еще одно важное преимущество использования Catalyst Smart Operations — отсутствие необходимости в глубоких познаниях пользователя в области сетевых технологий и коммутации при установке или замене коммутаторов.

Таблица 1. Снижение затрат при помощи Catalyst Smart Operations

Без Cisco Integrated Catalyst Smart Operations

	Сумма	Затраты*
Ежегодно развертываемое оборудование	100 коммутаторов	
Время, необходимое для развертывания	1,5 часа на каждый коммутатор	9000 долларов США
Число обновлений в год	4 обновления в год	
Время, необходимое для обновления сети	75 часов в год	

*Средняя зарплата ИТ-специалиста 60 долл. США/час

Снижение затрат при помощи Catalyst Smart Operations

	Сумма	Интеллектуальные сети	Экономия
Время, необходимое для развертывания	15 мин/коммутатор	1500 долларов США	83%
Время, необходимое для обновления сети	20 часов в год	4800 долларов США	73%

Стекирование Cisco StackWise Plus и Cisco FlexStack: объединение коммутаторов

Cisco StackWise и StackWise Plus — это современные инновационные технологии стекирования, разработанные Cisco. Они позволяют настроить группу коммутаторов, чтобы при подключении с помощью кабелей для стекирования они работали как единое устройство. Стек коммутаторов выступает в качестве единого устройства на уровне передачи данных и управления сетью, а также характеризуется повышенной устойчивостью и высоким уровнем доступности. Технология Cisco StackWise обеспечивает метод совместного использования ресурсов стека, в который могут входить до 9 коммутаторов. Отдельные коммутаторы объединяются при помощи интеллектуальных технологий, создавая единый модуль коммутации со скоростью обмена данными между коммутаторами, равной Гбит/с. Коммутаторы можно добавлять и удалять из работающего стека без ущерба для работы сети и производительности. В случае сбоя стек коммутаторов позволяет восстанавливать передачу данных за долю секунды. Кроме того, он характеризуется высокой доступностью при передаче трафика. Также доступны межстековые функции, такие как EtherChannel, позволяющие обеспечить высокую отказоустойчивость за счет использования нескольких соединений и коммутаторов для передачи трафика. Такой подход позволяет снизить риск возникновения неполадок. Технология Cisco StackWise Plus поддерживается коммутаторами Cisco Catalyst серий 3560 и 3750. Для получения дополнительных сведений о Cisco StackWise ознакомьтесь с [официальным документом по технологии StackWise](#).

Семейство продуктов Cisco Catalyst серии 2960-S поддерживает технологию стекирования Cisco FlexStack. Cisco FlexStack обеспечивает отличные функциональные возможности стекирования, при которых все коммутаторы работают как один модуль коммутации с объединенной панелью данных и единым IP-адресом, сходным с Cisco StackWise. Внедрение Cisco FlexStack выполняется путем установки модуля стекирования в базовый коммутатор локальной сети Cisco Catalyst серии 2960-S. Новая технология Cisco FlexStack позволяет объединять в стек четыре коммутатора, производительность стека составляет 20 Гбит/с. Добавление и удаление элементов стека при помощи модуля стекирования с возможностью горячей замены обеспечивается при использовании семейства коммутаторов Cisco Catalyst серии 2960-S. Поскольку сам модуль поддерживает "горячую замену", добавление и удаление коммутаторов из стека выполняется быстро и исключает возможность ошибки благодаря функциям автоматической настройки и загрузки образов. При этом для включения в стек автономных коммутаторов, приобретенных без средств поддержки стекирования, достаточно просто в них модули стекирования. В технологии FlexStack не используется кольцевая схема взаимодействия, характерная для Cisco StackWise. Таким образом, переключение на резервный ресурс выполняется медленнее. FlexStack предназначается для пользователей, которым не требуются возможности масштабирования и высокая устойчивость, доступная в решении StackWise Plus.

Smart Troubleshooting: обнаружение и устранение сетевых неполадок

Smart Troubleshooting — это набор функциональных возможностей, позволяющий быстро устранить сетевые неполадки. ОС Cisco IOS поддерживает широкий спектр команд отладки, которые подаются из командной строки и позволяют обнаруживать и устранять сетевые неполадки. К другим функциям, которые могут помочь при проведении диагностики, относятся Generic Online Diagnostics (GOLD) и Onboard Failure Logging (OBFL). GOLD позволяет пользователям запускать программные тесты, позволяющие определить, насколько хорошо функционирует коммутатор, и получить, помимо прочего, сведения о состоянии оборудования, благодаря чему пользователи могут убедиться в работоспособности устройства. Широкий набор средств тестирования оборудования можно использовать для обнаружения аппаратного сбоя или проведения нагрузочного тестирования коммутатора, что позволит убедиться в его работоспособности. OBFL напоминает "черный ящик": при сбое устройства коммутации OBFL отслеживает главные параметры коммутатора, чтобы изолировать неполадку. Выходные данные OBFL могут помочь повысить качество продуктов. Кроме того, они позволят заказчикам определить причины сбоя и даже предотвратить их возникновение в будущем.

Решение Catalyst Smart Operations позволяет заказчикам снизить эксплуатационные затраты, оценить преимущества полностью автоматизированной установки, простоты настройки и упрощенной процедуры замены коммутатора, наряду с сокращением времени развертывания. Cisco — это разумный выбор коммутационного решения, которое обладает инновационными возможностями по обеспечению простоты в работе, благодаря такой технологии как Catalyst Smart Operations.

Безопасность без границ с интеллектуальной системой защиты от угроз и решением Cisco TrustSec

Коммутаторы семейства Cisco Catalyst серий 2960-S и 2960 обеспечивают надежную защиту от угроз уровня 2, противодействуя атакам типа "посредник" (например, подмена MAC-адреса или IP-адреса отправителя или атаки на протокол ARP). Решение TrustSec, основной элемент архитектуры безопасности без границ, помогает корпоративным заказчикам защитить свои сети, данные и ресурсы с помощью контроля доступа на основе политик, сети с поддержкой идентификации и ролевой модели доступа, а также средств обеспечения целостности и конфиденциальности данных.

Защита от угроз

Встроенные средства обеспечения безопасности Cisco — лучшее в отрасли решение, которое реализовано на коммутаторах Cisco Catalyst и обеспечивает упреждающую защиту критически важной сетевой инфраструктуры вне зависимости от используемой технологии доступа. Предоставляя мощные и простые в использовании инструменты для эффективного предотвращения большинства распространенных и потенциально разрушительных угроз безопасности уровня 2, встроенные средства обеспечения безопасности Cisco обеспечивают надежную защиту сети.

Встроенные средства обеспечения безопасности Cisco включают следующие функции.

- **Механизм Port Security:** предотвращает переполнение таблицы MAC-адресов за счет ограничения числа MAC-адресов, которым разрешено подключение к одному физическому порту. Механизм Port Security ограничивает число известных MAC-адресов, чтобы предотвратить переполнение таблицы MAC-адресов.
- **Средства анализа DHCP-трафика:** предотвращает имитацию трафика от сервера DHCP и атаки типа "посредник", причем коммутатор доступа выступает в качестве небольшого межсетевого экрана между пользователями и легитимным сервером DHCP. Теперь злоумышленник не может назначить свое устройство в качестве шлюза по умолчанию или выполнять перенаправление и анализ потоков трафика между двумя оконечными устройствами.
- **Динамический анализ ARP-трафика:** предотвращает возможность имитации ARP-трафика за счет обеспечения отклика коммутатора только на "действительные" ARP-запросы и ARP-ответы. Эта функция не позволяет злоумышленнику скрытно прослушивать обмен данными между двумя оконечными устройствами, собирая пароли или подслушивая разговоры по IP-телефону.
- **IP Source Guard:** предотвращает возможность использования IP-адреса доверенного хоста злоумышленниками и интернет-червями. IP Source Guard разрешает передачу только тех пакетов, адреса отправителя которых являются подлинными.
- **Обнаружение точек доступа злоумышленника:** точки доступа, которые не контролируются сотрудниками ИТ-подразделения, редко соответствуют стандартам корпоративной безопасности, в результате чего они позволяют злоумышленникам легко получить доступ в корпоративную WLAN. Заказчикам требуются средства интеллектуального обнаружения и своевременного блокирования точек доступа злоумышленника, которые могут выполнять следующие задачи.
 - Немедленно отключать устройство, от которого исходит угроза.
 - Точно обнаруживать местонахождение такого устройства с целью его удаления.

Например, сотрудник включает точку доступа потребительского класса, чтобы предоставить группе сотрудников беспроводной доступ. Но злоумышленники обнаруживают, что точка доступа потребительского класса использует слабое шифрование, поэтому предпринимают попытки проникнуть в корпоративную сеть. В такой ситуации контроллер LAN обнаруживает точку доступа злоумышленника, а система WCS отключает ее от сети путем выключения порта доступа на коммутаторе.

Cisco TrustSec

Решение Cisco TrustSec (рис. 4) защищает доступ к сети, обеспечивает выполнение политик безопасности и предоставляет решения безопасности на основе таких стандартов, как 802.1X, обеспечивая безопасную совместную работу и соблюдение политик.

Рис. 4. Cisco TrustSec



Возможности TrustSec отражают лидерское мышление Cisco, инновации и стремление к успеху заказчиков. Новые возможности TrustSec включают следующие решения.

- IEEE 802.1AE MACsec с поддержкой управления с использованием предварительно утвержденного стандарта 802.1X-REV: лидер в отрасли с первичным управлением по предварительно утвержденному стандарту 802.1X-Rev. Средства MACsec, реализованные в коммутаторах Cisco Catalyst серий 3750-X и 3560-X, предоставляют возможности по обеспечению на уровне порта для подключения хоста конфиденциальности и целостности данных, передаваемых по Ethernet-каналам, на уровне 2 со скоростью среды передачи. За счет этого выполняется защита от атак типа "посредник" (анализ трафика, модификация и повторная передача трафика).
- Гибкая система аутентификации поддерживает множество механизмов проверки подлинности, в том числе стандарт 802.1X, резервный метод аутентификации по MAC-адресу (MAB), а также web-аутентификацию при помощи одной целостной конфигурации.
- Открытый режим, создающий удобную для пользователей среду на основе 802.1X.
- Интеграция технологии профилирования устройств и гостевого доступа на коммутаторах Cisco, что позволяет значительно повысить уровень защищенности при одновременном снижении затрат на развертывание и эксплуатацию.
- Возможности комплексного управления политиками, например, изменение авторизации RADIUS и использование загружаемого списка контроля доступа (ACL).
- Использование 802.1X с NEAT обеспечивает расширенный безопасный доступ, при котором компактные коммутаторы в конференц-залах имеют такой же уровень безопасности, как и коммутаторы в закрытом коммутационном шкафу.
- Комплексный поиск и устранение неисправностей, мониторинг и возможности создания отчетов.

Для получения дополнительных сведений о решении Cisco TrustSec посетите страницу <http://www.cisco.com/go/trustsec>.

Работа в "сетях без границ": объединенная система доступа

Возможность работы в "сетях без границ" определяется возможностью обеспечить доступ определенного пользователя с конкретного устройства в нужное время. Цель состоит в том, чтобы конечные пользователи получали целостный опыт при использовании приложений для совместной работы, таких как Cisco Telepresence™, или программ для проведения видеоконференций, вне зависимости от используемой технологии доступа.

С ратификацией стандарта 802.11n беспроводные сети достигли высокого уровня развития технологий, что позволяет им обеспечивать производительность, безопасность и надежность, ожидаемую от проводных сетей. Хотя в качестве основной технологии доступа WLAN может использоваться при определенных ограничениях, верным решением стало бы нахождение баланса между обоими способами доступа с учетом существующих и будущих требований пользователей к приложениям и обеспечению безопасности, а также к показателям надежности. Портфель коммутационных решений Cisco для сетей Ethernet поддерживает мобильные решения, что позволит заказчикам воспользоваться преимуществами перехода на технологию 802.11n. Благодаря средствам поддержки технологии PoE коммутаторы серии Cisco Catalyst могут обеспечить питание точек беспроводного доступа 802.11n с двумя радиомодулями. Это преимущество способствует повышению уровня надежности сети и более эффективной работе пользователей.

Коммутаторы серии Cisco Catalyst поддерживают технологию Cisco EnergyWise — архитектуру управления электроэнергией, которая позволит ИТ-специалистам и сотрудникам коммунальных служб измерять и регулировать расход электроэнергии, что позволяет значительно снизить затраты на электроэнергию как для проводного, так и для беспроводного доступа. Для точек доступа стандарта 802.11n эта технология позволяет включать и отключать точки доступа во время простоев.

Основная задача, связанная с устранением понятия периметра сети, состоит в обеспечении защиты сети от взлома и атак вне зависимости от того, где находится источник атаки (т. е. проводные и беспроводные клиенты). Коммутаторы семейства Cisco Catalyst поддерживают решение Cisco TrustSec, которое упрощает развертывание служб идентификации и позволяет сформировать единую среду политик для обеих сетей.

Коммутаторы Cisco Catalyst упрощают развертывание беспроводных сетей WLAN при помощи средства Catalyst Smart Operations путем автоматической настройки коммутатора при подключении точки доступа Cisco. Коммутаторы Cisco Catalyst поставляются с оптимизированными шаблонами конфигураций для точек доступа Cisco. При обнаружении точки доступа Cisco коммутаторы Cisco Catalyst автоматически настраивают интерфейс (для подключения точки доступа) надлежащим образом. Использование оптимизированных шаблонов Cisco позволяет свести к минимуму ошибки оператора, сокращая время настройки сети.

Cisco — отраслевой лидер в области предоставления качественной обработки трафика всех типов. По мере того, как все большая доля трафика приходится на беспроводную связь, возникает необходимость в обеспечении такой же качественной работы беспроводной сети, что и при проводной связи. Инновационные технологии Cisco, такие как AutoQoS (предназначенная для автоматического определения и развертывания политик QoS) и Auto SmartPorts (предназначенная для динамического применения политик QoS к порту коммутатора в зависимости от пользовательского устройства) значительно снижают стоимость операций при развертывании QoS.

Унифицированный уровень доступа: мониторинг и устранение неполадок на площадке заказчика

Большинство исследований показывают, что администраторы сети тратят значительное количество времени на поиск и устранение неполадок оборудования и определение их причин. Скорость устранения неполадок напрямую влияет на рентабельность всей компании. Поиск и устранение неполадок оборудования значительно упрощается за счет использования унифицированного решения, позволяющего отслеживать ресурсы, устройства и пользователей вне зависимости от места и типа их подключения. За счет централизованной системы мониторинга и управления, которая поддерживается сервисами определения местоположения, упрощаются бизнес-процессы и повышается производительность пользователей.

- **Мониторинг и управление сетью.** Это централизованное решение позволяет контролировать местоположение проводных и беспроводных устройств в сети. Если такое устройство, как IP-телефон, перемещается из одного здания в другое, решение быстро получает сведения о его местоположении, обеспечивая централизованное отслеживание и поддерживая работу служб экстренного реагирования, таких как E911. Оно позволяет отслеживать местоположение любого IP-устройства, подключенного к коммутаторам Cisco Catalyst, в том числе различных беспроводных устройств (например, беспроводных клиентов, беспроводных меток, телеметрической аппаратуры, источников помех и точек доступа злоумышленника).
- **Поиск и устранение неполадок на устройствах заказчика с поддержкой обнаружения местоположения.** Эта функция позволяет отслеживать проводные и беспроводные клиенты, способствуя таким образом быстрому устранению неполадок. В случае возникновения неполадок при подключении устройства служба поддержки может использовать это решение, чтобы определить, как именно устройство использует сеть (по проводному или беспроводному каналу) и определить его точку входа в сеть, порт доступа коммутатора или точку доступа. После обнаружения конкретной зоны или местоположения круг поиска неполадки значительно сужается. Также поддерживаются отчеты за различные периоды времени, что позволяет более глубоко анализировать использование оборудования.
- **Отслеживание активов и повышенная безопасность.** Эта функция обеспечивает централизованную инвентаризацию проводных и беспроводных устройств, а также управление активами для улучшения бизнес-процессов. Сетевой сервис определения местоположения в также обеспечивает возможность контроля местоположения активов по зонам. Приложения по управлению зонами или инвентарем смогут определить зоны и отслеживать мобильные активы, которые проникают в зону или покидают зону. Решение оповещает сотрудников, занимающихся обеспечением работы сети, если устройство покидает зону или если устройство не регистрировалось в сети в течение определенного времени, что позволяет быстро реагировать на угрозы безопасности. Кроме обнаружения точек доступа злоумышленника, это решение может также отследить порт коммутатора, к которому она подключена, чтобы заблокировать ее и защитить сеть.

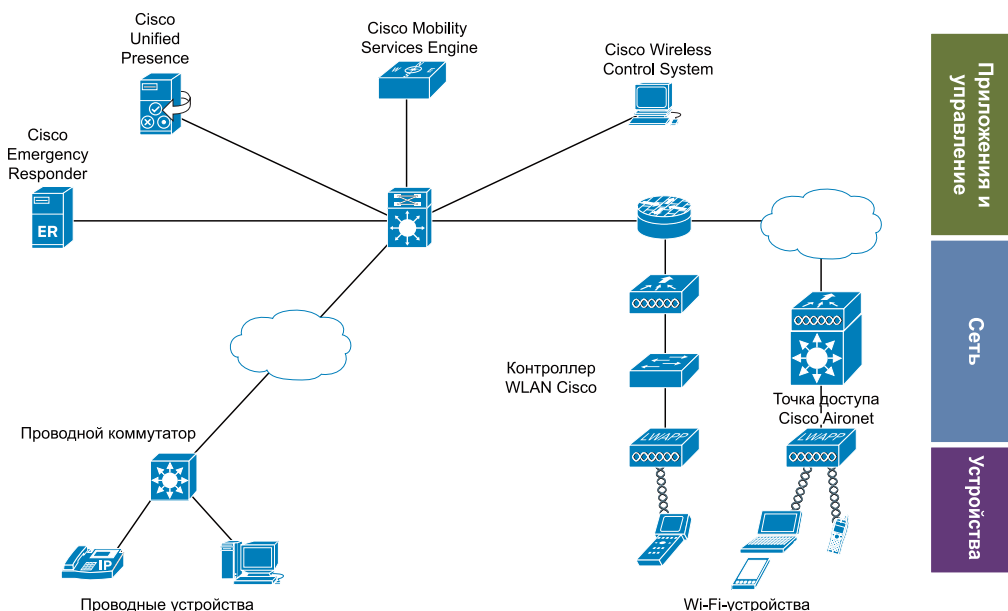
Cisco Mobility Services Engine (MSE) поддерживает открытый API (на основе протоколов SOAP и XML) для любого бизнес-приложения, которому требуются сведения о местоположении устройств. Несколько партнеров уже провели интеграцию с открытым API Cisco MSE, чтобы реализовать различные приложения для обеспечения безопасности и проверки сети. Доступ к этому API предоставляется всем технологическим партнерам Cisco. Такой подход обеспечивает полную интеграцию решений в бизнес-процессы заказчиков.

Политики на основе местоположения позволяют улучшить мониторинг и управление ресурсами. Сведения о местоположении проводного устройства позволяют применить именно тот набор политик, который нужен для контролируемых устройств, причем не только на основе учетных данных пользователя, но и в зависимости от местоположения устройства. Например, использование телефона в вестибюле офисного здания может управляться при помощи политик, отличных от тех, которые применяются для телефона в конференц-зале или в офисе одного из сотрудников. Современные политики нередко определяются статически в зависимости от MAC-адреса оконечного устройства, а не от местоположения самого устройства.

Архитектура сетевых сервисов определения местоположения

Это решение предназначено для предоставления сервисов определения местоположения для конечных устройств, подключенных к коммутаторам Cisco Catalyst. Само решение состоит из трех компонентов: Cisco MSE серии Cisco 3300, системы WCS и коммутаторов доступа Cisco Catalyst (рис. 5).

Рис. 5. Архитектура определения местоположения Cisco



Cisco MSE серии 3300

Решение Cisco MSE серии 3300 постоянно отслеживает местоположение проводных и беспроводных устройств. Это достигается путем отправки данных о местоположении в MSE проводными и беспроводными элементами сетевой инфраструктуры (контроллерами и коммутаторами) по мере возникновения изменений в сети. Как проводная, так и беспроводная инфраструктура сети взаимодействуют с MSE при помощи протокола NMSP.

В случае с коммутаторами, сведения, отправляемые в MSE — это, обычно, MAC-адрес, MAC-адрес порта коммутатора, IP-адрес и имя пользователя стандарта IEEE 802.1x (если доступно). Эта информация отправляется при любом изменении состояния подключения устройства. В случае с контроллерами, WLAN, сведения, которые отправляются средством MSE — это обычно MAC-адрес, IP-адрес, имя пользователя в стандарте IEEE 802.1x (если доступно) и данные измерения в стандарте IEEE 802.11, необходимые для определения физического местоположения.

Система управления Cisco WCS

Cisco WCS — это система управления MSE, которая предоставляет администраторам пользовательский интерфейс, содержащий общие функции управления MSE, такие как конфигурацию и мониторинг. Cisco WCS определяет местоположение конечных устройств на карте-схеме. Кроме информации о текущем местоположении, WCS также предоставляет хронологическую информацию, которая дополняет возможности поиска и устранения неполадок при подключении устройств к сети заказчика.

Коммутаторы Cisco Catalyst

Коммутаторы Cisco Catalyst предоставляют необходимые сведения о местоположении подключенных к ним оконечных устройств. Сведения о местоположении могут содержать физический адрес (также известный как штатный адрес), а также сведения об оконечных устройствах, таких как IP-адрес, MAC-адрес, порт, VLAN и имя пользователя. Штатное местоположение можно настроить глобально на коммутаторе путем задания дополнительных сведений для интерфейсе, например, указать номер комнаты и рабочего места. Коммутаторы получают сведения об оконечном устройстве/пользователе при помощи таких технологий, как IEEE 802.1x, отслеживание DHCP, динамический анализ ARP-трафика (DAI) и IP Source Guard. При подключении оконечного устройства к коммутатору доступа коммутатор может передать сведения о местоположении устройства и общие данные о нем на центральный сервер Cisco MSE. Кроме того, если оконечное устройство использует протоколы Cisco Discovery Protocol или Link Layer Discovery Protocol (LLDP), на MSE можно направить дополнительные сведения, например, номер версии и серийный номер. Поскольку сведения о местоположении оконечного устройства в корпоративной сети определяются в соответствии с точкой подключения, сервисы определения местоположения предоставляют актуальные сведения о местоположении оконечных устройств, обеспечивая таким образом мобильность, оптимизацию ресурсов и эффективность работы.

Работа в "сетях без границ": видео

Поддержка передачи видео в сети служит основой для:

- превосходных ощущений пользователя;
- бесперебойных сеансов обмена видеоданными;
- снижения степени использования полосы пропускания;
- безопасной работы видеосистем;
- снижения совокупной стоимости владения.

Рост видеотрафика превосходит все ожидания. Согласно данным исследования, проведенным в 2008 году Cisco Visual Networking Index (VNI), к 2012 году совокупный объем интернет-трафика вырастет в 4 раза. Но последние данные, полученные Cisco VNI в третьем квартале 2009 года, указывают на то, что объем интернет-трафика к 2013 году увеличится в семь раз. От большинства ИТ-подразделений крупных организаций будет требоваться такое же качество предоставления видеосервисов бизнес-класса, как и от коммерческих операторов связи.

Что изменилось в сфере видеосервисов?

Видеотрафик характеризуется непостоянной скоростью передачи (VBR) и высоким уровнем неравномерности. Поэтому при планировании сетей для предприятия необходимо учитывать требования к видеосредствам, особенно в условиях, когда границы между проводным и беспроводным доступом стираются. Требования к пропускной способности могут значительно отличаться в зависимости от приложения и сеанса (см. табл. 2). Требования к потоковой передаче видео и приложения для видеоконференций непредсказуемы и могут создавать непредвиденные пики трафика.

Таблица 2. Требования к пропускной способности для видеоприложений

Приложение	Пропускная способность	
Настольный компьютер	200 кбит/с — 1,5 Мбит/с	
Видеоконференция	768 кбит/с — 5 Мбит/с	
Решение Cisco TelePresence	1,5 Мбит/с — более 24 Мбит/с	
Цифровая панель	SD 1,5 Мбит/с — 5 Мбит/с	HD 5 Мбит/с — 8 Мбит/с
Корпоративное ТВ	SD 1,5 Мбит/с — 5 Мбит/с	HD 8 Мбит/с — 15 Мбит/с
Видеонаблюдение	256 кбит/с — 8+ Мбит/с	

Необходимо оптимизировать сеть для эффективной передачи потоковых данных с групповой адресации. Высокая эффективность работы возможна только внутри высокодоступной сети при использовании средств QoS. Простота развертывания, как и возможности управления оконечными устройствами, приложениями и портами доступа позволят значительно сократить затраты.

QoS при передаче видео

Видеотрафик представляет собой трафик с высокими требованиями к пропускной способности, кроме того, при передаче видео необходимая пропускная способность может изменяться. Потеря или задержка всего нескольких пакетов может вызвать искажения на всем экране. В сетях комплексов зданий со скоростью передачи данных по технологиям gigabit/10gigabit Ethernet необходимость обеспечения качества обслуживания (QoS) часто недооценивается или не учитывается вообще. Такое отношение вызвано тем, что некоторые администраторы сетей применяют QoS только к политикам определения очереди, в то время как возможности набора средств QoS выходят далеко за рамки средств обработки очереди. Классификация, маркировка и контроль соблюдения политик — важные функции QoS, которые оптимально выполнять на уровне доступа (в месте доступа). Коммутаторы Cisco Catalyst серий 2960, 3560 и 3750 поддерживают целостную конфигурацию для обеспечения QoS при передаче видео для самых разнообразных видеоприложений корпоративного класса. Для получения дополнительных сведений ознакомьтесь с информацией, предоставленной в разделе [Medianet Campus QoS Design](#).

Высокая доступность при передаче видео

Высокая доступность сервисов предоставляет пользователям дополнительные возможности: видеосеанс остается работоспособным даже при отказе компонентов инфраструктуры. Таким образом, прерывания используемых видеопотоков сводятся к минимуму благодаря архитектуре доступа с высоким уровнем доступности.

Последняя инновация в новых коммутаторах Cisco Catalyst серий 3560-X и 3750-X — Cisco StackPower™. Это система перекрестного подключения к электросети, которая позволяет совместно использовать источник питания стека как единый ресурс для всех коммутаторов. При сбоях в подаче электроэнергии питание для критически важных приложений поддерживается, а низкоприоритетные устройства отключаются согласно правилам, которые назначает пользователь.

Технологии Cisco StackWise и Cisco StackWise Plus позволяют создать единую логическую архитектуру коммутации за счет объединения коммутаторов с фиксированной конфигурацией. Любой коммутатор стека может служить главным, что обеспечивает высокую устойчивость при передаче трафика. Для получения дополнительных сведений ознакомьтесь с [официальным документом о технологии Cisco StackWise](#).

Широкий спектр технологий Cisco обеспечивает возможность создания архитектур с высоким уровнем резервирования.

- Технология Flex Links позволяет коммутаторам обеспечивать быструю двунаправленную конвергенцию при сбое главного канала передачи информации. Предотвращается потеря пакетов, а для активных видеосеансов обеспечивается высокое качество. Для получения дополнительных сведений ознакомьтесь со статьей о [Flex Links](#).
- Канал EtherChannel в рамках стека позволяет коммутаторам, объединенным в стек, создавать подключение EtherChannel, чтобы отказ отдельного коммутатора не влиял на подключение остальных коммутаторов стека.
- Протоколы RSTP и MSTP обеспечивают быструю сходимость дерева STP и обеспечивают возможность балансировки нагрузки и распределенной обработки на уровне 2. Элементы стека функционируют как единый узел, объединенный связующим деревом.

- Средства безостановочной передачи трафика на уровне 3 позволяет обеспечить на периферии тот же уровень резервирования, что и в ядре.
- Технология обнаружения каналов, передача по которым выполняется только в одном направлении (UDLD), позволяет обнаруживать и закрывать неработающие порты, что обеспечивает высокий уровень доступности.

Сокращение используемой пропускной способности с использованием групповой адресации

Проведение высококачественных видеомероприятий по глобальной сети в прямом эфире — это одна из наиболее трудных задач, стоящих перед сетью. Руководители компаний часто используют видеосервисы для распространения важнейшей бизнес-информации в реальном времени. В подобных ситуациях необходима качественная доставка трафика с первого раза. Особую сложность представляет использование сетей с индивидуальной адресацией, поскольку перегрузка канала передачи информации при попытке нескольких клиентов просматривать мероприятие в реальном времени может стать причиной неприемлемого качества видеосигнала и нарушить работу других важных приложений.

Механизм групповой адресации протокола IP позволяет нескольким адресатам одновременно получать идентичные копии потока, при этом поток не дублируется ни в одном из сетевых каналов. Просматривать поток может любое число пользователей: от одного до нескольких тысяч. При этом нагрузка на источник потока всегда будет равна одному потоку. Эта возможность является одним из многих преимуществ механизма групповой IP-адресации для серверов и каналов передачи. Cisco занимает лидирующую позицию на рынке в области технологий групповой адресации, обладающих высокой доступностью и гибкостью. Все коммутаторы семейства Catalyst серии 3750 поддерживают механизм интеллектуальной групповой адресации Smart Multicast, при котором не происходит репликации пакетов внутри стека. Сотрудники ИТ-подразделения Cisco внедрили технологию Single Source Multicast (SSM), которая является еще более эффективной технологией передачи данных от одного источника множеству получателей. Cisco является единственным поставщиком, способным предоставить комплексное решение для передачи видео с использованием средств групповой адресации. Для получения более подробной информации о том, как механизм групповой IP-адресации используется в ИТ-подразделении Cisco для обеспечения масштабируемой и экономичной передачи мультимедийных потоков, перейдите к этому [примеру](#). Подробнее об использовании [групповой IP-адресации на уровне доступа](#)

Обеспечение безопасности видеопотоков

IP-видеотрафик, как и любой IP-трафик, уязвим для атак, если не приняты надлежащие меры безопасности. Недавно сотрудники компании Viper Lab продемонстрировали, как можно взломать IP-систему видеонаблюдения, заменив изображение места преступления на другой ролик. Кроме того, они показали, как можно подслушивать видеозвонок по IP-сети. В коммутаторах Cisco Catalyst предусмотрены встроенные функции обеспечения безопасности, которые можно легко использовать для обеспечения безопасности IP-трафика при передаче видео. Ознакомьтесь с дополнительными сведениями о встроенных средствах обеспечения безопасности Cisco Catalyst и Cisco TrustSec, предназначенных для защиты инфраструктуры и использования MACsec для шифрования данных.

Снижение ТСО

В типовом варианте развертывания корпоративной инфраструктуры для передачи видео используется множество устройств различных типов, каждое из которых характеризуется различными требованиями к уровню доступа. Для проведения видеоконференций доступно множество устройств: от решения Cisco TelePresence и других систем, устанавливаемых в выделенных помещениях, до персональных видеокамер высокой четкости, видеотелефонов и т.п. Также существуют цифровые информационные панели, для которых необходимо создать условия, отличающиеся от тех, которые необходимы для IP-системы видеонаблюдения.

Для каждого устройства, которое может быть подключено к каждому порту коммутатора, смонтированного в коммутационном шкафу, обычно формируется более 10 строк в файле конфигурации коммутатора. При этом предприятию требуется в среднем несколько тысяч портов. Добавление, перемещение и внесение изменений вручную может потребовать больших затрат. Поэтому большинство предприятий останавливаются на фиксированном распределении портов, что ведет к превышению допустимого количества клиентских устройств и еще большим денежным инвестициям. Даже с учетом этого, глобальные изменения политик тоже могут повлечь за собой огромные расходы. Коммутаторы Cisco Catalyst обладают возможностями автоматической настройки при обнаружении устройств. Благодаря встроенной функции обнаружения IP-телефонов, цифровых мультимедийных проигрывателей и IP-камер видеонаблюдения, а также других устройств, при развертывании больше не требуется превышать допустимое количество выделенных портов. Теперь ИТ-подразделению необходимо поддерживать только одну конфигурацию для каждого типа устройства для любого числа портов коммутаторов. Добавление, перемещение и изменения происходят автоматически, что позволяет значительно снизить эксплуатационные расходы. Подробную информацию можно получить в разделе [Настройка Auto Smartports](#).

Создание WLAN с поддержкой мультимедийных приложений

Cisco предоставляет высокопроизводительную беспроводную сеть в качестве необходимой основы, в которой реализованы такие новейшие технологии, как 802.11n. С их помощью можно значительно повысить пропускную способность и обеспечить надежность и предсказуемость для мультимедийной WLAN. Благодаря таким технологиям ИТ-инфраструктура предприятия сможет соответствовать уникальным требованиям мультимедийных приложений, а нагрузка на ИТ-ресурсы может снизиться. Внедрение этих возможностей предполагает использование лучшей в своем классе беспроводной сети, интегрированной с проводной сетью, чтобы обеспечить передачу видео корпоративного класса вне зависимости от типа используемой для доступа сети (проводной или беспроводной).

Мультимедийные сети Cisco (медиасети) характеризуются не только высокой производительностью, но и интеллектуальными средствами оптимизации передачи видео за счет адаптивности, приоритезации, QoS, резервирования ресурсов, мониторинга, надежной передачи трафика с групповой адресацией и роуминга. Эти функции обеспечивают непрерывную передачу видеотрафика независимо от технологии доступа.

Возможности беспроводных сетей с поддержкой мультимедийных приложений расширены благодаря стандарту беспроводной связи 802.11n, и могут обслуживать такие инновационные решения, как Cisco VideoStream. Таким образом обеспечивается равномерное предоставление доступа к голосовым и видеоприложениям из беспроводной сети по проводной сети с использованием средств групповой адресации. Для получения дополнительных сведений о технологии Cisco VideoStream посетите страницу http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/ps10325/white_paper_c11-577721.html.

Заключение

"Сети без границ" Cisco — архитектура нового поколения, создающая условия для работы в современном мире. Эта архитектура гарантирует безопасное, надежное и беспрепятственное подключение любых пользователей в любой точке мира с помощью любых устройств и к любым ресурсам. Работа в "сетях без границ" возможна только благодаря интеллектуальному уровню доступа к сети, спроектированному в соответствии с потребностями глобального рабочего пространства. Решения Cisco для создания уровня доступа к сети — это главный элемент этой архитектуры, который обеспечивает мобильность, безопасность, определение местоположения, а также предоставляет пользователям возможности медиасетей и технологии EnergyWise, создавая таким образом оптимальные для пользователя условия работы. Интеллектуальная система организации доступа к сети позволяет воплотить идею мобильного рабочего места, безопасной совместной работы и обеспечить соответствие нормативам при одновременном снижении энергопотребления и повышении эффективности работы. Интеллектуальные решения для доступа к сети позволяют внедрить инновационные бизнес-модели и создать новые условия для работы, благодаря чему повышается качество обслуживания заказчиков и их приверженность вашей компании.

Дополнительная информация

Для получения дополнительных сведений о коммутаторах Cisco Catalyst серий 3560-X и 3750-X посетите web-страницы <http://www.cisco.com/go/3560x> и <http://www.cisco.com/go/3750x>

Для получения дополнительных сведений о коммутаторах Cisco Catalyst серии 2960-S посетите web-страницу <http://www.cisco.com/go/2960>.

Для получения дополнительной информации о "сетях без границ" Cisco посетите web-страницу <http://www.cisco.com/go/borderless>.

Ознакомиться с подробной информацией о решении Cisco TrustSec можно на web-странице <http://www.cisco.com/go/trustsec>.

Для получения дополнительных сведений о медиасети Cisco посетите web-страницу <https://www.cisco.com/web/solutions/medianet>

Дополнительная информация о Cisco EnergyWise находится на web-странице <http://www.cisco.com/go/energywise>.

Для получения дополнительной информации о мобильных решениях Cisco с учетом контекста посетите web-страницу <http://www.cisco.com/go/contextaware>.

Для получения дополнительных сведений о решении Cisco MSE, посетите web-страницу <http://www.cisco.com/go/mse>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDR, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)