Архитектура Smart Business Architecture

Сети без границ для организаций среднего размера

Руководство по развертыванию платформы

Версия: H1CY10

Содержание

Изменения в версиях

Обновления по сравнению с предыдущей версией

- Незначительные грамматические и технические исправления
- Обновления кода IOS (см. Приложение)
- Обновления в модуле "Глобальная сеть (WAN)"
  - Протестированы маршрутизаторы Cisco серии 2911 и 3925 ISR
- Добавлен модуль "QoS"
- Обновления в модуле "Беспроводная связь"
  - Протестирован контроллер WLAN 5500
  - Добавлена настройка высокой доступности
- Обновления в модуле "Режим ускорения работы приложений"
  - Выполнено тестирование WAVE-574 и WAVE-274
- Модуль "Унифицированные коммуникации"
  - Обновления по поддержке 7.1.3

План, позволяющий упростить развертывание

Для партнеров Cisco, обслуживающих заказчиков, база подключенных пользователей которых составляет от 100 до 1000 пользователей, разработано готовое к развертыванию решение, отличающееся простотой, быстротой применения, невысокой стоимостью, масштабируемостью и гибкостью. Решение отличается простотой — его легко настроить, развернуть и управлять им.

Однако за простотой этого развертывания скрывается глубина и охват архитектуры. С учетом отзывов от многих заказчиков и партнеров компанией Cisco разработана надежная основа сети с гибкой платформой, которая обеспечивает поддержку дополнительных сетевых или пользовательских сервисов без дополнительных технических работ.

Данное руководство по развертыванию помогает решить проблемы, возникающие у пользователя в повседневной работе. Эта архитектура

- **обеспечивает надежную основу;**
- **делает развертывание быстрой и простой в выполнении задачей;**
- **ускоряет развертывание дополнительных сервисов;**
- **устраняет необходимость в перепроектировании сети уровня ядра.**

Использование настоящего руководства по развертыванию

В соответствии с принципом простоты использования настоящее руководство разделено на модули. Можно ознакомиться с руководством с самого начала или перейти к любому модулю. Все разделы настоящего руководства могут использоваться по отдельности, благодаря чему обеспечивается возможность развертывания технологии Cisco по определенному модулю без необходимости в изучении предыдущего модуля.

Настоящее руководство по развертыванию начинается с **обзора архитектуры.** В этом разделе приведены основные положения руководства по развертыванию, ценность предлагаемого решения для вас и ваших заказчиков, а также общее представление преимуществ предлагаемой выдающейся архитектуры.

В следующем модуле описывается **глобальная настройка**. Эти элементы являются общими для многих, а иногда и для всех устройств, используемых в решении. Примерами таких элементов может служить настройка SSH для безопасного удаленного управления протоколом Simple Network Management Protocol (SNMP) для наблюдения и устранения неполадок. Также описываются средства управления сетью, используемые для настройки, наблюдения и устранения неполадок в этой архитектуре.

В модуле **"Комплекс зданий"** описывается развертывание сетей для комплекса зданий, сетей доступа и серверных комнат. В этом же модуле описывается качество обслуживания (QoS). Этот важный сервис должен быть включен в базовой архитектуре для обеспечения возможности совместного использования в одной сети различных приложений, таких как передача голоса в режиме реального времени, передача видео высокого качества и передача данных, чувствительных к задержкам.

В модуле **"Глобальная сеть (WAN)"** описывается уровень границы глобальной сети для комплекса зданий, подключение к удаленным филиалам и сетевую инфраструктуру в этих филиалах.

В модуле **"Беспроводная связь"** приведено описание инфраструктуры беспроводной связи для комплекса зданий и ее использование сотрудниками для получения доступа к внутренней сети и Интернету, а также для гостевого доступа к Интернету.

В модуле **"Безопасность"** особое внимание уделяется развертыванию дополнительных сервисов обеспечения безопасности, таких как межсетевые экраны, системы определения вторжений, используемые для защиты информационных ресурсов, а также настройка безопасного удаленного доступа для удаленных работников и удаленных мобильных пользователей. Поскольку безопасность имеет первостепенно значения для архитектуры, она будет описываться в нескольких разделах.

В модуле **"Унифицированные коммуникации (UC)"** описывается развертывание телефонии Cisco® по UC/IP поверх основы сети без перепроектирования сети уровня ядра. Многим заказчикам, развертывающим сети данных, необходима также поддержка в используемой сети передачи голоса по IP или с помощью IP-телефонии — и это простое в использовании руководство обеспечивает возможность быстрого развертывания этого сервиса.

В модуле **"Оптимизация WAN"** описывается оптимизация использования пропускной способности между филиалом и головным офисом, результатом которой является экономия ИТ-ресурсов.

И, наконец, в **Приложении** представлен полный список продуктов, использованных в лабораторных условиях для тестирования этой архитектуры. Сопроводительное руководство к настоящему документу "Руководство по файлам настройки архитектуры Smart Business Architecture для 100-1000 пользователей" доступно на сайте Cisco.com. В нем предоставлены отдельные файлы настройки для продуктов, использованные при тестировании в лабораторных условиях.

Назначение настоящего документа

Настоящее руководство по развертыванию предназначено для партнеров Cisco и инженеров корпорации Cisco Systems®, база подключенных пользователей которых составляет 100-1000 человек. Также оно предназначено для системных инженеров, которые будут развертывать решения Cisco на предприятиях заказчиков. В руководстве представлены поэтапные указания по развертыванию этих решений. Поскольку предлагаемое решение Cisco имеет модульную архитектуру, технические специалисты получают возможность быстро и эффективно выполнить развертывание в точном соответствии с требованиями заказчиков.

Этот документ предназначен для работы в следующих условиях:

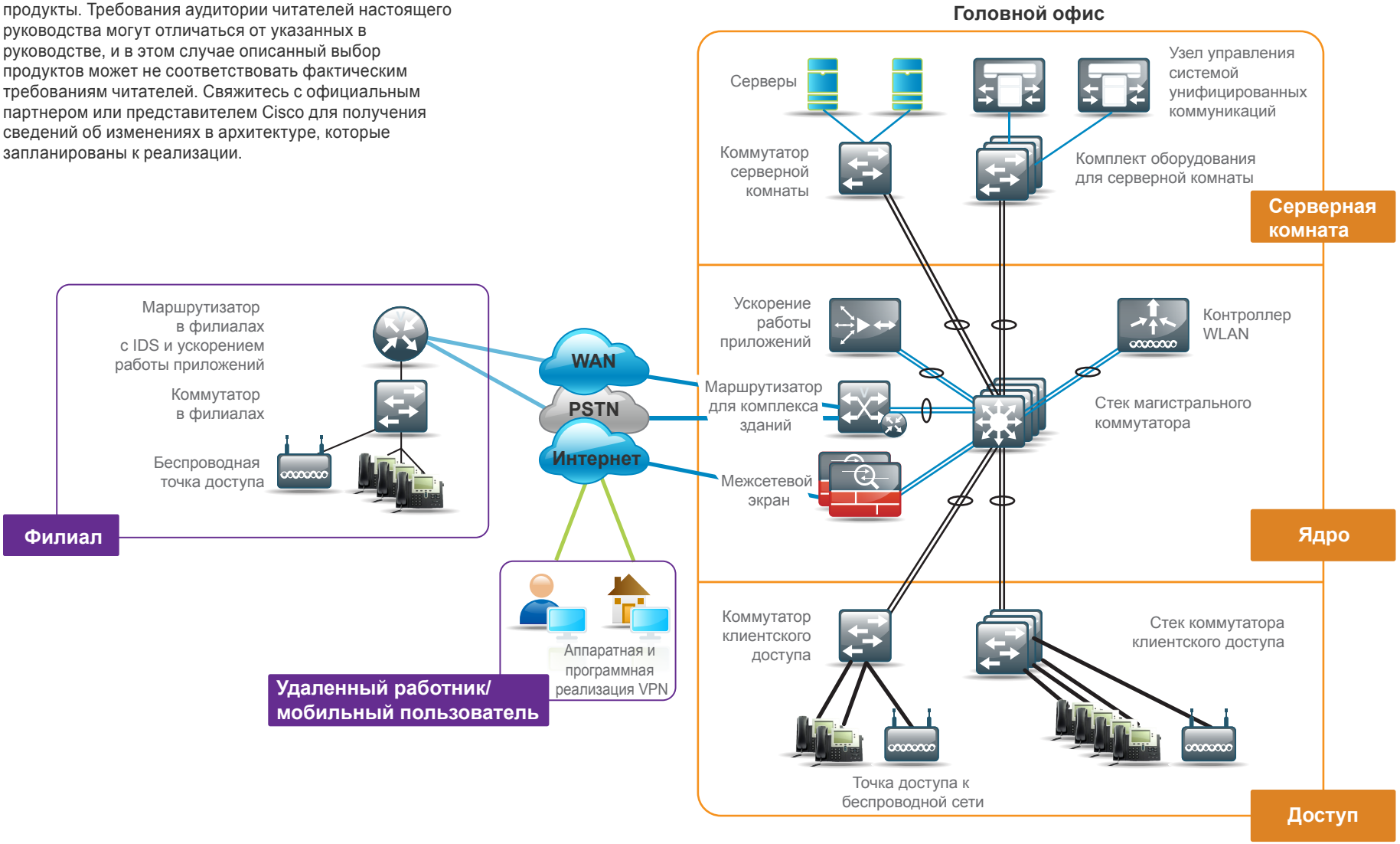
- имеется 100-1000 подключенных сотрудников;
- имеется до 20 филиалов, в каждом из которых работает приблизительно 25 сотрудников;
- необходимо решение для удаленных и мобильных работников;
- необходимо обеспечить безопасность корпоративных ресурсов;
- необходимо обеспечить для сотрудников проводной и беспроводной доступ;
- необходим беспроводной гостевой доступ;
- необходимы решения для проводного и беспроводного голосового доступа;
- имеются приложения для внешнего использования, размещенные вне офисов;
- имеется серверная комната, в которой размещены приложения, используемые в компании;
- необходимо снизить затраты путем оптимизации пропускной способности WAN;
- имеются ИТ-сотрудники с сертификатами CCNA® или аналогичным уровнем знаний;
- требуется гарантия использования проверенного решения;
- необходим переход на новое решение для обеспечения возможности развития предприятия.

План, позволяющий упростить развертывание

Обзор архитектуры

Продукты и задачи этой архитектуры основаны на требованиях заказчиков, партнеров и специалистов по эксплуатации Cisco. В разделе "Обзор архитектуры" ниже описываются критерии выбора и выбранные продукты. Требования аудитории читателей настоящего руководства могут отличаться от указанных в руководстве, и в этом случае описанный выбор продуктов может не соответствовать фактическим требованиям читателей. Свяжитесь с официальным партнером или представителем Cisco для получения сведений об изменениях в архитектуре, которые запланированы к реализации.

Основные характеристики архитектуры сети



План, позволяющий упростить развертывание

Обзор архитектуры

С самого начала одной из главных концепций, использованных при разработке этой архитектуры, была концепция модульности. Процесс развертывания был разделен на модули в соответствии со следующими принципами.

- **Простота использования.** Важнейшее требование заключалось в разработке архитектуры, которая могла быть развернута с минимальной настройкой и управлением в двухдневный срок.
- **Рентабельность.** Другим важным требованием при выборе продукта была необходимость соответствия требованиям бюджета для компании данного размера.
- **Гибкость и масштабируемость.** Рост компании должен соответствовать росту архитектуры. Выбранные продукты должны поддерживать возможность масштабирования или изменения назначения внутри архитектуры.
- **Возможность повторного использования.** Задача заключалась в возможности повторного использования (при наличии соответствующих возможностей) одних продуктов для различных модулей, чтобы сократить количество продуктов, необходимых для обеспечения резервных ресурсов.

В разделе ниже приведен список продуктов и конкретные причины их выбора с учетом рекомендаций, приведенных выше.

Модуль "Комплекс зданий"

Ядро сети, которое используется как сетевой концентратор, обеспечивающий возможность взаимодействия для всех модулей в сети, является одним из наиболее важных модулей в архитектуре. Хотя существует несколько продуктов, которые могут обеспечить функции, необходимые для ядра сети, — в первую очередь отказоустойчивость и высокоскоростную коммутацию, — архитектура обеспечивает уровень гибкости, обеспечивающий возможность роста инфраструктуры внутри компании.

В данной архитектуре обеспечены два варианта: первый для 100-600 пользователей, поддерживаемых архитектурой с уровнем ядра на базе отказоустойчивого стека при использовании коммутатора Cisco Catalyst® серии 3750. Второй вариант предназначен для 500-1000 пользователей, поддерживаемых с помощью отказоустойчивых шасси Cisco Catalyst 4507R, оборудованных двумя модулями супервизорами.

Использование любого из этих двух вариантов обеспечивает необходимый уровень отказоустойчивости и емкости по подключениям. Еще одним важным фактором является плотность портов, т.е. количество физических портов, необходимое для подключения других устройств от других моделей. Выбор продукта должен быть обусловлен требованиями компании.

100-600 пользователей

Линейка продуктов Cisco Catalyst 3750 — это расширяемые коммутаторы гигабитного Ethernet с фиксированным числом портов, которые обеспечивают избыточность с помощью технологии StackWise. Дополнительные сведения приведены в модуле, посвященном ядру сети.

Коммутатор Cisco Catalyst 3750 обеспечивает функции коммутации уровня 3 и уровня 2, и он настроен для маршрутизации трафика между другими модулями в сети комплекса зданий. В будущем, если компании потребуются дополнительные порты в сети уровня ядра, к стеку уровня ядра можно легко добавить дополнительные устройства 3750, или при необходимости в переходе на разделенное ядро/распределение центральных ресурсов можно изменить задачи для используемой в настоящий момент стека уровня ядра Cisco Catalyst 3750. Два варианта функционирования означают, что он может быть повторно использован в серверной комнате или комплексе зданий в качестве коммутатора доступа. При проверке архитектуры компанией Cisco использовалась пара расширяемых коммутаторов Cisco Catalyst 3750G-12S-E с малогабаритными съемными приемопередатчиками, что обеспечило возможность последовательного подключения к портам по витой паре или волоконно-оптическим кабелям. Кроме того, устройство Cisco Catalyst 3750 обеспечивает выполняемое при техническом обслуживании добавление элементов расширения для увеличения емкости по портам. Благодаря этому обеспечивается наивысший уровень доступности и минимальное время простоя.

500-1000 пользователей

Для структуры, обеспечивающей поддержку дополнительных пользователей, необходимы расширенные возможности коммутации и большее количество портов для подключения к дополнительным коммутаторам доступа в комплексе зданий. Для этой архитектуры был выбран отказоустойчивый коммутатор Cisco Catalyst 4507R, оборудованный двумя модулями супервизорами, обеспечивающими отказоустойчивость, необходимую в ядре сети. Гибкая конструкция корпуса позволяет установить различные линейные карты в соответствии с количеством требуемых портов восходящих соединений.

Серверная комната и доступ для комплекса зданий

Как серверная комната, так и доступ в комплексе зданий главным образом предназначены для подключения устройств к сети. Главное различие — необходимость обеспечения передачи питания по кабелю Ethernet (PoE) при доступе для комплекса зданий. Предлагаются две линейки продуктов на выбор: коммутаторы Cisco Catalyst 3560 и Cisco Catalyst 3750.

Cisco Catalyst 3560 — это экономичное, нерасширяемое семейство коммутаторов для быстрого или гигабитного Ethernet с фиксированным числом портов. Оно обеспечивает гибкость и набор функциональных возможностей для коммутируемых сред с многоуровневым разделением доступа. Продукты этого семейства поставляются в вариантах с передачей питания по Ethernet и без таковой. Cisco Catalyst 3750G — это стекируемое семейство коммутаторов с фиксированным числом портов гигабитного Ethernet с большей общей емкостью, достигаемой благодаря задней панели со скоростью соединения 32 Гбит/с и технологии StackWise.

Как Cisco Catalyst 3560, так и Cisco Catalyst 3750 имеют порты 10/100/1000 с поддержкой передачи питания по Ethernet. Хотя для серверной комнаты необходимости в устройствах с PoE нет, минимальное различие в стоимости делает возможным использование единой линейки продуктов в нескольких модулях и изменение назначения устройств по мере роста инфраструктуры.

План, позволяющий упростить развертывание

PoE поддерживает средства IP-телефонии, беспроводные точки доступа, видеокамеры безопасности и другие устройства с низким энергопотреблением. PoE позволяет обеспечить питание устройств в различных местоположениях при помощи витой пары без дополнительных расходов по установке или изменению электрической проводки (например, в подвесных потолках при установке видеокамер и беспроводных точек доступа). Включение возможностей PoE в перспективную архитектуру сетей делает сеть надежной, устраняя дополнительные расходы по перепланировке сети в будущем по мере развертывания новых устройств с поддержкой PoE. В то время как конфигурации различны, управление и возможность использования одной линейки продуктов в среде с множеством различных модулей позволяет снизить производственные расходы.

Модуль "Глобальная сеть (WAN)"

Глобальная сеть (WAN) в головном офисе — это точка подключения между удаленными офисами и головным офисом. В этой архитектуре WAN предполагается, что частные и безопасные подключения предоставляются оператором связи. В то время как структура подразумевает доступ к Интернету, наличие подключения к Интернету не требуется для обеспечения связи между различными площадками. WAN обеспечивает подключение различных площадок и объединяет трафик для перенаправления в Интернет в головном офисе.

При выборе устройства Cisco также принимает во внимание способность поддержки дополнительных функций и сервисов. Кроме главной функции перенаправления трафика между различными площадками, от устройства может потребоваться поддержка голосовых данных и выполнение шлюзовых функций, а также функции оптимизации и обеспечения безопасности, предоставляемые благодаря возможностям расширения, обеспечиваемые подключаемыми модулями.

С учетом всех этих требований наилучшим выбором являются интегрированные сервисные маршрутизаторы Cisco 3845 ISR. Cisco 3845 ISR представляет собой гибкую модульную платформу, которая делает доступной высокоскоростную маршрутизацию, а также другие сервисы, такие как передача голоса, для нужд связи между комплексом зданий или головным офисом и удаленными филиалами.

В таких удаленных филиалах поддерживается до 25 пользователей ПК, IP-телефонов и беспроводных устройств. На всех компьютерах подразумевается использование настольных приложений, а также клиентов электронной почты и других корпоративных приложений, доступных через канал по WAN к серверной комнате головного офиса. Система IP-телефонов также поддерживается WAN. Локальный коммутатор также должен поддерживать PoE для IP-телефонов и беспроводных точек доступа таким образом, чтобы им не требовалось питание от внешнего источника.

Кроме того, оптимизация QoS и WAN позволяют значительно снизить затраты при эффективном использовании LAN и WAN. К тому же имеется возможность применения мер безопасности по предотвращению угроз, возникающих при работе удаленных сотрудников с портативными компьютерами в общедоступных сетях.

Cisco 2811 ISR представляет собой платформу, которая соответствует требованиям подключения филиала по WAN к головному офису. Он обеспечивает интегрированные сервисы в составе системы предотвращения вторжений (IPS), расширенного модуля интеграции (AIM) для обеспечения безопасности и сетевого модуля (NM) глобальных прикладных сервисов для оптимизации передачи данных, голоса и видео по WAN.

Для компьютера, IP-телефона, беспроводных точек доступа и других подключений в офисной среде коммутатор Cisco 3560G (24- или 48-портовый) является наиболее подходящим продуктом для филиалов с такой архитектурой. Он позволяет осуществлять простой доступ к сети, а также предоставляет требуемые возможности PoE. Соответствуя принципам простоты использования, он обладает тем же набором команд, что и коммутаторы Cisco Catalyst 3750 и другие коммутаторы Cisco Catalyst 3560, которые используются в комплексах зданий для сокращения стоимости развертывания и эксплуатационных издержек до минимума.

Последнее устройство в такой топологии — беспроводная точка доступа. Для этой архитектуры было выбрано семейство Cisco AIR-LAP1140, поскольку его продукты поддерживают PoE и могут централизованно управляться из головного офиса при помощи контроллера WLAN.

Модуль "Безопасность"

В рамках этой архитектуры существует множество требований и возможностей реализации функций обеспечения безопасности. Руководство по развертыванию будет предполагать использование IDS в рамках WAN, программное и аппаратное обеспечение виртуальной частной сети для мобильных удаленных пользователей и удаленных работников. Существует дополнительный уровень безопасности на уровне порта коммутатора, к которому подключаются устройства. Подробнее об этом мы расскажем в модулях по комплексам зданий и глобальным сетям.

В головном офисе имеется еще один уровень безопасности, позволяющий защитить информационные активы. Следующие устройства обеспечивают прямую или косвенную защиту против потенциальных угроз.

Первый продукт по обеспечению безопасности периметра головного офиса — Cisco ASA 5510. ASA 5510 это усиленное многофункциональное устройство с возможностями межсетевого экрана, VPN и SSL VPN для удаленных/мобильных пользователей. У него также имеется разъем для дополнительного сервисного модуля. А в этой архитектуре добавляемым дополнительным сервисным модулем является модуль IPS.

Функции IPS SSM

Модуль IPS добавляет возможность проверки данных уровня приложений на атаки и блокировки вредоносного трафика.

Непрямое обеспечение безопасности реализуется за счет обнаружения вторжений Это пассивный способ наблюдения за угрозами. После обнаружения угрозы можно предпринять действия по ее снижению. Продукты семейства Cisco IPS 4200 позволяют компании вести постоянное наблюдение за сетевым трафиком на предмет обнаружения потенциальных угроз. При обнаружении угрозы можно организовать пересылку уведомлений на указанный ресурс и предпринять действия по разрешению этой проблемы.

План, позволяющий упростить развертывание

Удаленный работник и удаленный мобильный пользователь

Основой для работы удаленных работников и удаленных мобильных пользователей являются технологии виртуальных частных сетей или VPN.

Удаленные мобильные пользователи для доступа к Интернету используют точки доступа в кафе, гостиницах, аэропортах и других местах. При подключении мобильного пользователя к Интернету они могут использовать программный клиент VPN для доступа к ресурсам компании. Для этой цели корпорация Cisco предоставляет собственный программный клиент VPN.

Удаленные работники работают в месте, которое не является головным офисом или удаленным филиалом; основным местом работы может быть их домашний офис. Большая часть работы удаленных работников не оправдывает затрат на целенаправленное подключение их к глобальной сети головного офиса, однако остаются в силе многие требования по связи для работников филиала или офиса. Поэтому подключение к главному офису через Интернет более экономично, однако Интернету также присущ более низкий уровень безопасности. Им необходимо подключать компьютер, IP-телефон и, возможно, принтер и беспроводную точку доступа там, где они находятся. Удаленный работник нуждается в безопасном подключении и портах для сетевого офисного оборудования, в том числе PoE для их IP-телефона и точки доступа.

В таком случае оптимальным решением является Cisco ASA 5505. Это экономичный и полнофункциональный межсетевой экран с восемью портами 10/100 (два из которых поддерживают PoE) для IP-телефона или точки доступа. Cisco ASA 5505 также предоставляет аппаратное безопасное подключение из точки нахождения удаленного работника к виртуальной частной сети (VPN). Это устройство можно предварительно настроить перед тем, как отправить его удаленному работнику. Оно очень просто в использовании и развертывании при обеспечении необходимого уровня безопасности.

Модуль "Телефония UC/IP"

Компании ищут возможности получить максимальную рентабельность от инфраструктуры передачи данных. Одна из наиболее распространенных развертываемых технологий — это IP-телефония. IP-телефония — это в основном переход со старого выделенного телефонного коммутатора на программный коммутатор плюс использование сети передачи данных в качестве транспорта для голосовой связи, в отличие от использования раздельных проводок для кабеля и голоса. Рыночная категория, к которой относится IP-телефония и другие формы связи, в том числе видео, известна под названием "унифицированные коммуникации" (UC). Для функционирования этой архитектуры с самого начала необходимо, чтобы все модули поддерживали решения UC от Cisco. Поэтому при добавлении устройства с поддержкой объединенных коммуникаций Cisco UC (и конкретно IP-телефонии) не требуется никаких дополнительных работ или перепланировки сети.

В архитектуре унифицированных коммуникаций Cisco имеется два программных компонента. Первый — это Cisco Unified Communications Manager. Cisco Unified Communications Manager — это концентратор, предназначенный для соединений IP-телефонии и ее управления, а также других приложений связи. Второй — Cisco Unity® Connections. Unity Connections предоставляет такие сервисы, как голосовая почта для 1000 пользователей, интеграция голосовой почты с папкой входящих сообщений электронной почты, а также многие другие функции, повышающие производительность операций.

Поскольку приложения в рамках UC, такие как IP-телефония и голосовая почта, предъявляют разные требования к обработке и хранению данных в зависимости от количества пользователей и дополнительных функций, важно выбрать нужную платформу, основанную на наборе функций, необходимых в будущем. При реализации этой архитектуры рекомендуется использовать следующее оборудование: Cisco Unified Communications MCS 7835 и Cisco Unity Connections MCS 7825.

Модуль "Оптимизация WAN"

Удаленные филиалы должны подключаться к главному офису. Эта возможность подключения отражается на конечных результатах деятельности предприятия, и поэтому ее использование должно осуществляться с расчетом на максимальное снижение затрат. За последние три-четыре года новый класс продуктов, называемый "оптимизацией WAN", позволил голосовым и обычным данным преодолевать эти точки перехода без дополнительных расходов на расширение пропускной способности. Подобно модулю унифицированных коммуникаций, возможность добавления оптимизации WAN при меньшей стоимости и усилиях — одно из основных требований.

В такой ситуации выбирается программное обеспечение Cisco Wide-Area Application Services (WAAS). WAAS может работать на базе определенного круга устройств, которые выбираются исходя из конкретных требований производительности приложений, каналов WAN и количества пользователей.

Решение WAAS состоит из трех компонентов: устройство ускорения работы приложений в каждом из удаленных филиалов, конечная точка ускорения работы приложений в головном офисе, которая является точкой сбора данных из удаленных местоположений, и также приложение Central Manager, которое является точкой контроля для всего решения WAAS. В лаборатории использовался Cisco Wide-Area Engine (WAE) 502 NM, установленный в маршрутизатор удаленного офиса и аппарат Cisco WAVE 574 в качестве конечной точки ускорения работы приложений в головном офисе, при этом Cisco WAVE 274 играл роль центрального диспетчера главного офиса.

См. Руководство по планированию размеров WAAS на портале Cisco.com или свяжитесь со специалистом Cisco WAAS для разработки решения WAAS с оптимальной производительностью.

Технические рекомендации. Любая подчеркнутая команда разбита по формату этого документа. В командной строке ее необходимо вводить как единую полную команду.

Примечания

Модуль "Глобальная настройка"

Обзор технологий

В рамках интеллектуальной архитектуры бизнеса на 100-1000 пользователей существуют параметры, общие для различных систем. Также существуют параметры системы, позволяющие упростить и обезопасить управление этим решением. В этом модуле содержатся рекомендации для таких настроек. Фактические параметры и их значения будут отличаться в зависимости от текущей конфигурации сети. Просмотрите все параметры и изменения настройки перед их установкой.

Типовые файлы настройки для продуктов, используемых в этом руководстве по развертыванию, предоставлены в Приложении.

Каждый раздел или модуль в этом руководстве по развертыванию содержит команды или снимки экрана, предназначенные для того, чтобы пользователь смог настроить конкретный продукт. В большинстве случаев перед командой или снимком экрана описывается его назначение.

Цветной текст, относящийся к конкретному модулю, — это команды, которые следует вводить в командной строке продукта. Также существует несколько "мастеров загрузки". Это поэтапные указания, позволяющие пользователю провести настройку конкретного продукта и требующие консольного подключения.

Прочитайте каждый модуль перед тем, как попытаться выполнить установку, чтобы полностью ознакомиться с командами, архитектурой и их потенциальным воздействием на вашу сеть.

Администрирование системы

Имена пользователей и пароли

Необходимо включить шифрование паролей. При формировании политик, позволяющих придерживаться внешних и внутренних нормативов и требований, следует руководствоваться корпоративными стандартами.

Технические рекомендации. Цветной текст под цвет раздела — это текст для ввода в командной строке.

```
!Set password and encrypt
enable secret [password]
!
service password-encryption
```

Каждое устройство перенаправляется назад к одной и той же системе для синхронизации внутренних часов. Устройства необходимо настроить в соответствии с местным часовым поясом.

```
!Synchronize system clock and local time zone
clock timezone UTC -8
clock summer-time UTC recurring
!
```

Установите прозрачный режим для протокола VTP. Это позволяет перенаправить сведения VTP от других коммутаторов, однако не вводит обновления VTP в локальной базе данных. Коммутаторы в прозрачном режиме не являются активными элементами домена VTP. Они сохраняют собственные настройки VLAN в NVRAM.

```
vtp mode transparent
```

Протокол UDLD (протокол обнаружения однонаправленной связи)

Протокол UDLD — это протокол уровня 2, который позволяет устройствам, подключенным по волоконно-оптической линии связи или витой паре Ethernet, отслеживать физическую конфигурацию кабелей и обнаруживать однонаправленные соединения. Все подключенные устройства должны поддерживать UDLD, чтобы протокол успешно обнаруживал и отключал однонаправленные соединения. При обнаружении однонаправленного соединения средствами UDLD происходит отключение используемого порта и отправка уведомления сетевым устройством. Однонаправленные соединения могут служить причиной таких неполадок, как петли коммутации, "черные дыры" и недетерминированное перенаправление. Кроме того, UDLD позволяет выполнять более быстрое обнаружение сбоя соединения и быстрое восстановление взаимодействия портовых магистралей при оптоволоконных соединениях, более подверженных однонаправленным сбоям.

В нормальном режиме, если состояние подключения порта определяется как однонаправленное, то порт продолжит нормальное перенаправление трафика, однако он будет отмечен как "неопределенный". Порт циклически пройдет по обычным состояниям протокола STP и продолжит перенаправление трафика. В агрессивном режиме порт войдет в состояние “errdisable” и будет отключен. Чтобы восстановить порт после состояния “errdisable”, потребуется его отключить и запустить заново при помощи команд “shut” и “no shut”. В любом из описанных режимов UDLD функционирует одинаково. Ожидается, что отправляемые сообщения и получаемые сообщения должны быть одинаковыми. Режимы отличаются только способом, которым UDLD реагирует на сбой однонаправленного соединения.

```
udld aggressive
```

SSH

Рекомендуется включить SSH для задач удаленного управления. Установите протокол SSH версии 2, поскольку он более безопасен в сравнении с версией 1 и поддерживается большинством клиентов SSH.

При включении SSH потребуется создать ключи RSA. Ниже приводится пример команд, позволяющих включить SSH и обеспечить безопасность запроса доступа при помощи списка доступа.

```
ip domain-name [domain name]
Ip ssh version 2
crypto key generate rsa general-keys modulus
2048
```

Технические рекомендации. Все IP-адреса, номера VLAN и другие специальные значения, используемые в настоящем руководстве по настройке, приведены только в качестве примеров.

Безопасную аутентификацию можно включить либо локально, либо при помощи сервера аутентификации. Опять же, лучше всего придерживаться политик компании.

```
line vty 0 15
 login local
 transport input ssh
 access-class 55 in

access-list 55 permit 192.168.28.0 0.0.0.255
```

Службы доменных имен

Использование полного доменного имени вместо IP-адреса позволяет осуществить доступ к сети, сервисам и специфическим устройствам даже при смене их IP-адреса. Это также требуется для шлюза IP-телефонии. В данной настройке мы добавили сервисы DHCP в ядро сети. Ниже приводятся два примера пулов IP-адресов для клиентов "доступа" и "голоса", в том числе доменное имя и IP-адрес сервера DNS, который будет обслуживать службу доменных имен. Параметр 150 в голосовом пуле — это конкретная команда настройки, определяющая шлюз по умолчанию и IP-адрес сервера TFTP для голосовых сервисов.

```
ip dhcp pool access
ip dhcp pool access
 network 192.168.8.0 255.255.255.0
 default-router 192.168.8.1
 domain-name [cisco.com]
 dns-server 192.168.28.10

ip dhcp pool voice
 network 192.168.12.0 255.255.255.0
 default-router 192.168.12.1
 dns-server 192.168.28.10
 option 150 ip 192.168.28.20 192.168.28.21
 domain-name [cisco.com]
```

Доступ HTTP

Следующие команды позволяют включить использование графического пользовательского web-интерфейса (GUI) как для стандартного протокола HTTP (TCP 80), так и для HTTPS (TCP 443).

```
Ip http server
ip http secure-server
```

Технические рекомендации. Существуют и рекомендованы к использованию методы защищенного доступа через терминалы и Интернет, которые следует использовать при наличии возможности (например, заменить telnet на SSH, а HTTP на HTTPS).

Каждое устройство перенаправляется назад к одной и той же системе для синхронизации сетевого времени. Для этих устройств также необходимо настроить местный часовой пояс.

Технические рекомендации. Если необходимо разрешить безопасный доступ к web-интерфейсу коммутатора, удалите команду "`ip http server`"

Установка связующего дерева

Структура протокола позволяет исключить петли, однако при случайной настройке физических или логических петель команды STP обеспечат отсутствие фактических петель маршрутизации.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-1005 priority 24576
```

Для управления сетью для всех устройств определено сообщество SNMP "только для чтения" (cisco) и "чтение/запись" (cisco123). Использовался SNMP версии (2c).

```
snmp-server enable
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Настройка VLAN

Настройка VLAN упрощена путем приведения номера VLAN в соответствии с маской подсети IP.

Головной офис

Vlan1	Управление	192.168.1.0
Vlan8	Передача данных головного офиса	192.168.8.0/24
Vlan10	Беспроводная передача данных головного офиса	192.168.10.0/24
Vlan12	Передача голосовых данных головного офиса	192.168.12.0/24
Vlan14	Беспроводная передача голосовых данных головного офиса	192.168.14.0/24
Vlan16	Беспроводной гостевой доступ	192.168.16.0/24
Vlan28	Ферма серверов А	192.168.28.0/24
Vlan29	Ферма серверов Б	192.168.29.0/24
Vlan31	Маршрутизация в ядре сети	192.168.31.0/24

Филиал

Vlan64	Проводная передача данных	192.168.64.0/24
Vlan65	Проводная передача голоса	192.168.65.0/24
Vlan69	Беспроводная передача данных	192.168.69.0/24
Vlan70	Беспроводная передача голоса	192.168.70.0/24

Управление сетью

В этой архитектуре существуют различные устройства — от коммутаторов и маршрутизаторов до различных приборов и модулей. Большинство продуктов используют интерфейс командной строки для первоначальной загрузки и настройки режима запуска. Как только продукт включен и работает после первоначальной конфигурации загрузки, многие продукты также обеспечивают графический пользовательский интерфейс. Уровень, до которого каждое устройство может быть настроено после первоначальной конфигурации загрузки пользовательского интерфейса, может различаться в зависимости от конкретного продукта.

Также доступно несколько средств сторонних производителей для управления в двухдневный срок. По завершении развертывания эти средства могут предоставить важнейшую информацию из наблюдения сети и приложений для устранения любых неполадок.

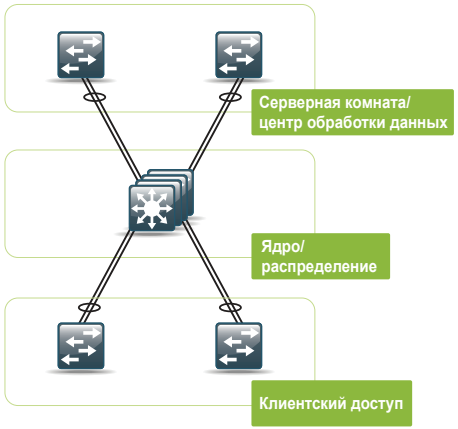
Примечания

Уровень ядра

Обзор технологий

Одним из наиболее замечательных технологических новинок в этом сегменте является архитектура с уровнем ядра на базе отказоустойчивого устройства. Эта архитектура отличается от современных моделей для локальных сетей, организованных по принципу "ядро/распределение/доступ" и, как показано на схеме, главное изменение в уровне ядра сети. Вместо пары двух независимых устройств используется одно отказоустойчивое устройство. Физически уровнем ядра может быть стек коммутаторов Cisco Catalyst 3750 или высокодоступный коммутатор Cisco Catalyst 4507R. Важно заметить, что, хотя уровень ядра выглядит как единичное устройство для настройки и для других устройств в сети, он обладает полностью отказоустойчивой архитектурой. Стек коммутаторов Cisco Catalyst 3750 обладает полностью независимым питанием и процессорами для каждого коммутатора в стеке Cisco StackWise, а коммутатор Cisco Catalyst 4507R обладает возможностью резервирования модуля супервизора, линейными картами и источниками питания. Кроме того, рост сети уровня ядра достигается достаточно просто без простоев за счет добавления линейных карт к коммутатору Cisco Catalyst 4507R или добавлении коммутаторов к стеку Cisco Catalyst 3750.

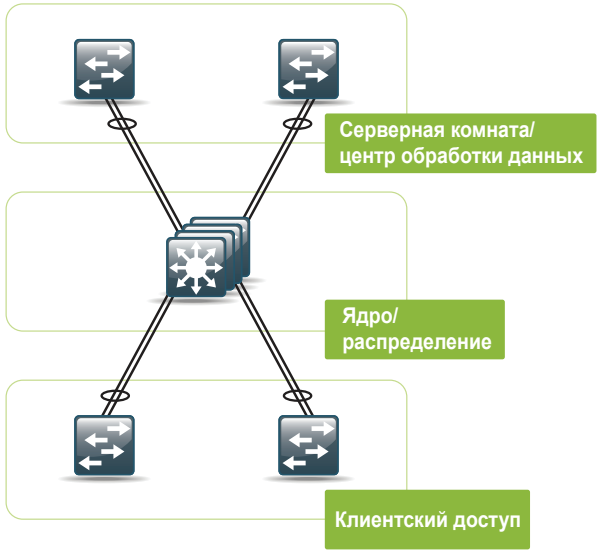
Сеть комплекса зданий



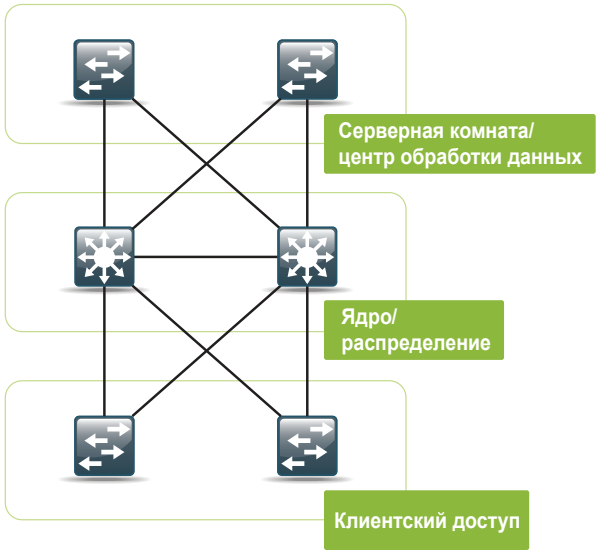
Архитектура с уровнем ядра на базе отказоустойчивого устройства и архитектура с уровнем ядра на базе двух независимых устройств

В архитектуре с уровнем ядра на базе двух независимых устройств имеется восходящий канал от каждого коммутатора доступа к каждому коммутатору уровня ядра.

Архитектура с уровнем ядра на базе отказоустойчивого устройства

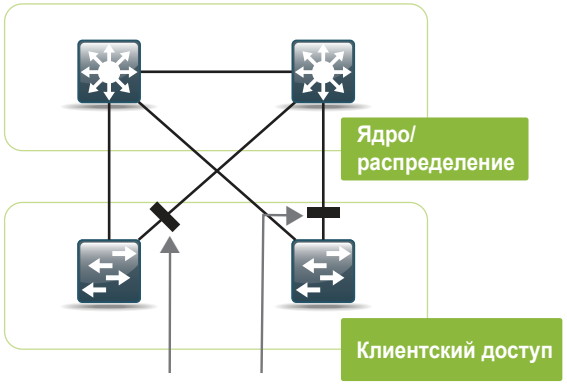


Архитектура с уровнем ядра на базе двух независимых устройств



Если одна и та же VLAN используется со множеством коммутаторов доступа, то необходимо запускать протокол STP, чтобы избежать появления в сети петель уровня 2. Протокол STP обладает двумя главными недостатками: время его восстановления велико в сравнении с другими технологиями, а чтобы предотвратить возникновение петель, ему необходимо блокировать одно из подключений гигабитного Ethernet от уровня доступа, снижая доступную пропускную способность вдвое. Чтобы избежать длительного времени восстановления STP, имеет смысл вынести доступ VLAN из сети доступа на уровень ядра и не создавать соединительную линию для VLAN между двумя коммутаторами уровня ядра, создавая таким образом V-образную архитектуру и топологию без петель. Это позволяет выполнять более быстрое восстановление после сбоев, но означает, что потребуется настроить отдельные VLAN для каждого коммутатора доступа. В прошлом это было приемлемым решением. Однако сегодня в средах с VLAN с передачей голоса и данных для проводного и беспроводного трафика количество VLAN и подсетей, которые необходимо настраивать, может слишком быстро увеличиться. Узлы IPv4 поддерживают только один шлюз по умолчанию.

Традиционная архитектура с HSRP

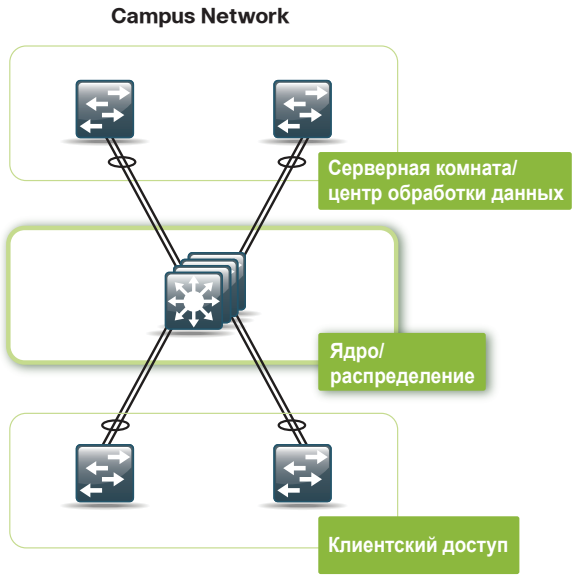


Заблокированные интерфейсы

Чтобы сделать этот отдельный адрес шлюза высокодоступным, используется протокол избыточности первого транзитного участка, чтобы IP-адрес шлюза находился на нормально работающем коммутаторе. HSRP, GLBP и VRRP — это примеры протоколов избыточности первого транзитного участка (FHRP), которые используются для того, чтобы обеспечивать для шлюзов поддержку избыточности. HSRP и VRRP — это наиболее распространенные FHRP, однако они позволяют узлам VLAN взаимодействовать только с одним коммутатором единовременно, поэтому по резервному соединению к уровню ядра трафик не передается вообще. GLBP — это более новый протокол, который позволяет выполнять некоторую балансировку нагрузки, распределяя трафик между двумя маршрутизаторами уровня ядра. Балансировка нагрузки для возвращаемого трафика, который обычно составляет большую часть всего объема трафика, не установлена, поэтому преимущества такой топологии не до конца соответствуют нуждам большинства систем.

Преимущества уровня ядра на базе отказоустойчивого устройства

Благодаря модели уровня ядра на базе отказоустойчивого устройства оба восходящих канала доступа направляются к коммутатору уровня ядра как канал гигабитного EtherChannel, разделенный между несколькими модулями-лезвиями в том случае, если коммутатор уровня ядра — Cisco Catalyst 4507R или если в качестве ядра используется стек коммутаторов Cisco Catalyst 3750. Для коммутатора уровня ядра и коммутатора доступа это представляется как единый канал. Топология без петель более не используется, поскольку на уровне ядра имеется только одно подключение к коммутатору доступа, при этом создается звездообразная топология.



Благодаря **топологии без петель** при сбоях уже не нужен протокол STP для восстановления взаимодействия, и время восстановления нормальной передачи уменьшается. Без петель не существует опасности блокирования восходящих каналов. Оба канала от коммутатора доступа к сети уровня ядра являются сбалансированными по нагрузке при помощи технологии EtherChannel, поэтому входящие и исходящие данные распределяются по каналам для более эффективного использования каналов. Также возможно увеличить пропускную способность к уровню доступа или серверной комнате за счет увеличения числа каналов EtherChannel от 4 до 8.

У сети уровня ядра имеется только один логический интерфейс от уровня доступа для каждой VLAN. Это позволяет исключить необходимость использования протокола избыточности первого транзитного участка, а также упростить настройку. Если ближайший уровень доступа является крупным и требует использования нескольких коммутаторов, их можно объединить в стек, а восходящий канал EtherChannel можно распределить по коммутаторам стека уровня ядра, чтобы свести к минимуму последствия сбоя коммутатора или канала. Более крупный коммутатор Cisco Catalyst 4507R можно использовать вместо коммутаторов Cisco 3750 стека уровня ядра, заменив ее одним коммутатором на основе шасси.

Коммутаторы в серверной комнате можно объединять в стеки или размещать отдельно, они подключаются к коммутатору уровня ядра при помощи восходящих каналов EtherChannel точно так же, как и коммутаторы уровня доступа. Серверы можно подключить к двум коммутаторам автономной работы или к отдельным коммутаторам стека, что позволит добиться высокой доступности и балансировки нагрузки за счет так называемого "объединения сетевых интерфейсов в группы" (создания виртуальных каналов Ethernet на портах 802.3ad).

Подробности настройки

Архитектура с уровнем ядра на базе отказоустойчивого устройства позволяет упростить настройку коммутатора уровня ядра в сравнении с существующими моделями с уровнем ядра на базе двух независимых устройств. Поскольку глобальная настройка уже описана, ниже приводится только описание настройки уровня ядра. Ниже представлена настройка уровня ядра для коммутаторов семейства Cisco Catalyst 3750, которая должна работать с любой моделью этой линейки. Коммутаторы, использующиеся в этой архитектуре, — два коммутатора Catalyst 3750G-12S, объединенные в стек. Также включены все изменения, необходимые для обеспечения работы настройки на коммутаторе уровня ядра Cisco Catalyst 4507R.

Настройка уровня 2

Архитектура с уровнем ядра на базе отказоустойчивого устройства позволяет создавать топологии типа звезда (звездообразные топологии). Хотя в этой архитектуре не используется связующее дерево, которое блокирует подключения, уровень ядра необходимо настроить как основу для всех требований протокола STP.

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1-1005 root primary
```

Технические рекомендации. Протокол STP не следует выключать ни при каких обстоятельствах. Если проводка к коммутатору проведена неправильно или коммутатор настроен неправильно, в результате может появиться петля, что в свою очередь может привести к простою сети.

Подключения EtherChannel выделяются от сети уровня ядра к уровню доступа и коммутаторам фермы серверов, к маршрутизатору WAN и контроллеру WLAN. При физическом подключении устройств к сети уровня ядра при помощи EtherChannel важно, чтобы эти соединения выполнялись на отдельных коммутаторах в центральном стеке. Для упрощения архитектуры был создан виртуальный канал для каждого порта на первом коммутаторе Cisco Catalyst 3750 с таким же портом на втором коммутаторе Cisco Catalyst 3750, поэтому интерфейс 3750-1 Gigabit Ethernet 1/0/1 был помещен на тот же виртуальный канал порта, что и интерфейс 3750-2 Gigabit Ethernet 2/0/1. В интерфейсе командной строки каналы EtherChannel настраиваются на виртуальных каналах по портам интерфейсов. Перед запуском команд EtherChannel рекомендуется соединить устройства кабелями. Портовые каналы для этих подключений настраиваются следующим образом:

```
 interface Port-channel1
switchport trunk encapsulation dot1q
```

Номера сетей VLAN, приводимые в настоящем руководстве, используются в качестве примера и основаны на среде, созданной Cisco в лабораторных условиях. Используемые значения могут различаться. Для каналов необходимо разрешить только обязательные к использованию VLAN (например, для доступа 1,8,12).

```
switchport trunk allowed vlan [VLAN]
switchport mode trunk
```

Ниже описана настройка порта канала для коммутатора Cisco Catalyst 4507R:

```
interface Port-channel1
 switchport
 switchport trunk allowed vlan [VLAN]
 switchport mode trunk
```

Для коммутаторов Cisco Catalyst серии 4500 не требуется использовать команду "`switchport trunk encapsulation dot1q`", а следует использовать команду "`switchport`", поскольку порты являются маршрутизируемыми по умолчанию.

Настройка портов на физических портах, составляющих EtherChannel, идентична. Каналы порта связываются с физическими интерфейсами с использованием команды channel-group. Следующий пример приведен для коммутаторов Cisco Catalyst 3750-12s, использованных в лабораторных условиях; в этой настройке использовались интерфейсы Gigabit Ethernet 1/0/1 и 2/0/1.

В большинстве случаев каналы от сети уровня ядра должны использоваться для нескольких VLAN. Для этого используются теги 802.1Q VLAN. Коммутатор порта настраивается как соединительная линия, что позволяет использовать несколько VLAN в одном физическом канале, и устанавливается тип инкапсуляции dot1q. Ограничение или удаление сетей VLAN, которые могут существовать в одном канале, до одной, которая должна существовать на коммутаторе на другом конце, считается наилучшим возможным приемом. Для этого используется команда "`switchport trunk allowed vlan`".

```
interface GigabitEthernet [port number]
switchport trunk encapsulation dot1q
```

Эти порты подключаются к коммутатору уровня доступа, поэтому к сетям VLAN разрешен только доступ по соединительной линии.

```
switchport trunk allowed vlan 1,8,12
switchport mode trunk
mls qos trust cos
auto qos voip trust
```

Для групп каналов, которые охватывают несколько коммутаторов в стеке, необходимо установить значение "on".

```
channel-group 1 mode on
spanning-tree link-type point-to-point
```

Для коммутатора Cisco Catalyst 4507R не нужно использовать команду "`switchport trunk encapsulation dot1q`". Он не поддерживает автоматическое использование QoS на портах соединительных линий.

Ниже описана настройка портов для подключения к маршрутизатору WAN:

```
interface Port-channel12
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 31
switchport mode trunk

interface GigabitEthernet [port number]
switchport trunk encapsulation dot1q
```

Только сеть VLAN, которая применяется для межсетевого взаимодействия LAN и WAN, может быть использована для этой соединительной линии . Она настроена как соединительная линия, что в дальнейшем обеспечивает возможность простого добавления дополнительных сетей VLAN для предоставления различных сервисов в будущем.

```
switchport trunk allowed vlan 31
switchport mode trunk
mls qos trust dscp
auto qos voip trust
channel-group 12 mode on
spanning-tree link-type point-to-point
```

Для устройств наподобие межсетевых экранов, для которых используется двойное подключение к сети уровня ядра для обеспечения высокого уровня доступности, но не используется подключение по

EtherChannel, выполняется настройка, описанная ниже. На этом этапе не выполняется настройка портов каналов, поскольку у всех межсетевых экранов имеется отдельный внутренний интерфейс.

```
interface GigabitEthernet [номер порта]
 switchport trunk encapsulation dot1q
```

На межсетевом экране разрешены базовая маршрутизация и гостевые VLAN.

```
switchport trunk allowed vlan 16,31
switchport mode trunk
spanning-tree link-type point-to-point
```

Настройка уровня 3

В качестве протокола маршрутизации был выбран EIGRP, поскольку его легко настраивать, для его использования не требуется длительное планирование и он может быть масштабирован для использования в крупных сетях. Настройка маршрутизации EIGRP:

```
ip routing
router eigrp 1
```

При наличии другого адресного пространства, помимо указанного ниже, необходимо использовать другой оператор сети:

```
network 192.168.0.0 0.0.255.255
no auto-summary
passive-interface default
```

Все маршрутизирующие устройства подключаются к сети VLAN 31 в сети уровня ядра:

```
no passive-interface Vlan31
```

Многоадресная передача обеспечивает возможность одновременной передачи одного потока данных на несколько конечных точек с большей эффективностью, чем при использовании одноадресной передачи данных.

Настройка многоадресной маршрутизации:

```
ip multicast-routing distributed
```

В случае с Cisco Catalyst серии 4500 используйте команду:

```
ip multicast-routing
```

Укажите интерфейс, используемый для подключения WAN как точки PIM Rendezvous Point (RP). В данной сети это VLAN 31:

```
ip pim rp-address 192.168.31.1
```

Добавьте эту команду во все интерфейсы:

```
ip pim sparse-mode
```

При отсутствии внешнего сервера для назначения адресов на коммутаторе уровня ядра можно запустить сервер DHCP IOS. Благодаря этому предотвращается назначение сервером DHCP IOS адресов 1-10 для сети 192.168.8.9/24:

Ниже приведен пример одной области:

```
ip dhcp excluded-address 192.168.8.1
192.168.8.10
ip dhcp pool access
network 192.168.8.0 255.255.255.0
default-router 192.168.8.1
domain-name [cisco.com]
dns-server [IP-адрес сервера DNS]
```

Если используется внешний сервер DHCP, то для интерфейсов VLAN используются следующие команды:

```
ip helper-address xxx.xxx.xxx.xxx
```

Эта команда представляет IP-адрес внешнего сервера DHCP.

Технические рекомендации. В конце каждого раздела в модуле рекомендуется выполнить проверку файла используемой настройки по сравнению с файлом настройки в руководстве по файлам настройки, чтобы убедиться в правильности настройки.

Примечания

Клиентский доступ

Обзор технологий

В этой архитектуре настройка уровня доступа очень проста. Архитектура была разработана таким образом, чтобы одна настройка порта могла использоваться для отдельного компьютера, IP-телефона, IP-телефона с подключенным компьютером или беспроводной точки доступа. Для повышения безопасности на уровне доступа было включено несколько функций уровня порта. **Параметры безопасности порта** ограничивают количество MAC-адресов, которые могут быть активны для одного порта. Благодаря этому обеспечивается защита от атак переполнения таблицы MAC-адресов. Средства анализа трафика DHCP позволяют предотвратить работу несанкционированных серверов DHCP в сети и используются для защиты от атак истощения ресурсов DHCP. Проверка ARP связывает IP-адрес с MAC-адресом и обеспечивает защиту от атак, направленных на модификацию ARP-таблицы. Защита источника IP предотвращает атаки, основанные на подмене IP-адреса источника.

Настройка доступа

Коммутатор уровня доступа может быть автономным коммутатором или стеком коммутаторов. Подключение коммутатора доступа к сети уровня ядра выполняется по EtherChannel. При наличии в стеке нескольких коммутаторов канал необходимо разделить между коммутаторами в стеке, что позволит обеспечить высокий уровень доступности. При наличии в стеке трех или более коммутаторов для восходящих каналов следует использовать коммутаторы, не являющиеся диспетчером стека. Для настройки коммутатора как диспетчера стека используйте следующую команду:

```
switch [номер коммутатора] priority 15
```

Для упрощения настройки порта доступа в коммутаторах поддерживается команда "range". Благодаря этому обеспечивается возможность единовременной отправки команды и ее одновременного применения к нескольким портам. Поскольку большая часть портов на уровне доступа будет настроена одинаково, это позволяет сэкономить много времени. Например, команда

```
interface range gigabitethernet 0/1-24
```

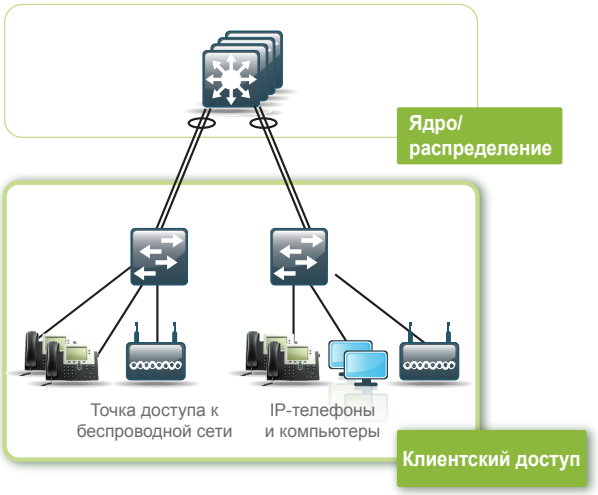
позволяет одновременно вводить команды для всех 24 портов (Gig 0/1 к Gig 0/24).

Существуют варианты этой команды, которые зависят от типа портов и настраиваемого коммутатора.

Для настройки средства анализа трафика DHCP и проверки ARP используется несколько глобальных команд коммутатора:

```
ip dhcp snooping vlan [диапазон VLAN]
ip dhcp snooping

ip arp inspection vlan [диапазон VLAN]
```

Ниже описана настройка для канала порта. В соединительной линии разрешаются только сети VLAN, являющиеся активными в маршрутизаторе доступа. Для ARP проверки и средств анализа трафика DHCP настраивается уровень доверия для портов восходящих каналов, поскольку узлы не подключаются напрямую к ним, проверка не требуется.




```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,8,12
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
```

Физические интерфейсы для EtherChannel настраиваются как соединительные линии, для которых разрешаются только необходимые VLAN. QoS здесь указан как доверенный, поскольку он расположен в сетевом канале и не подключен напрямую к узлу. Для проверки ARP и средства анализа трафика DHCP также указывается как доверенный из-за подключения сетевой инфраструктуры:

```
interface GigabitEthernet [диапазон портов]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,8,12
 switchport mode trunk
 ip arp inspection trust
 mls qos trust dscp
 auto qos voip trust
 channel-group 1 mode on
 spanning-tree link-type point-to-point
 ip dhcp snooping trust
```

Настройка портов узла будет поддерживать ПК, телефоны и беспроводные точки доступа. Для коммутаторов, поддерживающих 802.3AF, для соответствующих устройств доступно интегрированное питание.

```
interface GigabitEthernet [номер порта]
switchport access vlan [сеть VLAN данных]
switchport mode access
switchport voice vlan [VLAN для передачи голоса]
```

Разрешает активность 11 MAC-адресов для порта; дополнительные MAC-адреса рассматриваются как нарушение, и трафик от них будет отклоняться:

```
switchport port-security maximum 11
switchport port-security
```

Установка времени выдержки в 2 минуты:

```
switchport port-security aging time 2
```

При ограничениях будет отклоняться трафик от MAC-адресов, которые считаются нарушениями, но порты при этом выключаться не будут, поскольку это может привести к остановке работы IP-телефона:

```
switchport port-security violation restrict
switchport port-security aging type
inactivity
ip arp inspection limit rate 100
```

Коммутатору сообщается информация о доверии пометкам QoS, исходящим от телефона:

```
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
```

Сокращает время переключения порта в состояние перенаправления:

```
spanning-tree portfast
```

Отключает порт при подключении другого коммутатора к порту:

```
spanning-tree bpduguard enable
ip verify source
ip dhcp snooping limit rate 100
```

Технические рекомендации. Порты, отключаемые вследствие возникающих ошибок, не будут автоматически восстановлены. Их необходимо включить вручную. Чтобы включить функцию автоматического восстановления, используйте глобальную команду

```
errdisable recovery cause all
```

Примечания

Настройка для серверной комнаты

Коммутаторы фермы серверов подключаются к сети уровня ядра при помощи EtherChannel для того, чтобы с помощью объединения двух портов гигабитного Ethernet можно было создать один канал (2 гигабита). При необходимости в увеличении пропускной способности можно увеличить количество каналов от фермы серверов к сети уровня ядра до четырех или восьми.

Ниже описана настройка EtherChannel к сети уровня ядра:

```
interface Port-channel1
 switchport trunk encapsulation dot1q
```

В сетях VLAN выполняется удаление всех каналов, кроме активных в ферме серверов:

```
switchport trunk allowed vlan 1,28-29
 switchport mode trunk

interface GigabitEthernet [номера портов, соответствующие
сетям VLAN]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,28-29
 switchport mode trunk
 mls qos trust dscp
 auto qos voip trust
 channel-group 1 mode on
 spanning-tree link-type point-to-point
```

Ниже приведен пример настройки порта для связи с сервером. Порты сервера доверяют помеченным сервером QoS. Это необходимо для серверов унифицированных коммуникаций в решении, и может потребоваться в зависимости от приложений, работающих на других серверах:

```
interface GigabitEthernet1/0/1
```

Выполняется настройка порта к VLAN, к которой должен принадлежать сервер:

```
 switchport access vlan [vlan]
 switchport mode access
mls qos trust dscp
 auto qos voip trust
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Примечания

Обзор технологий

Маршрутизаторы в этой модели развертывания выбраны из-за способности обеспечивать совместимость при передаче обычных, голосовых и видеоданных между офисами, а также из-за способности маршрутизировать трафик. Такой вариант развертывания включает различные интерфейсы WAN и голоса, а также дополнительные возможности безопасности, сервисы WAAS и модули системы унифицированных коммуникаций Cisco.

Для главного офиса выбран интегрированный сервисный маршрутизатор Cisco 3845 ISR и более новый Cisco 3925 ISR. Это необходимо для поддержки двадцати удаленных офисов, в каждом из которых существуют возможности подключения T1/E1 или ниже. Cisco 3925 ISR был выбран для поддержки дальнейших модификаций и защиты инвестиций. Этот маршрутизатор поддерживает обновляемую системную плату, поскольку в будущем может потребоваться более высокая производительность. Он также поддерживает сетевой модуль T3/E3 для высокоскоростных подключений к WAN. Маршрутизатор в главном офисе может также предоставлять мультимедийные ресурсы системы унифицированных коммуникаций и функции шлюза. Поэтому он был настроен с достаточным DSP и двойным T1/E1 HWIC, который поддерживает различные конфигурации WAN и PSTN PRI при помощи одного разъема HWIC.

Маршрутизаторы для филиалов были выбраны исходя из того, что скорость WAN соответствует T1/E1, имеется поддержка интерфейсов WAAS NM, IPS Security AIM, PSTN и мультимедийных ресурсов системы унифицированных коммуникаций (в т. ч. способность поддержки пользователей унифицированной надежной телефонии удаленной площадки (Unified Survivable Remote Site Telephony). Маршрутизаторы Cisco 2811 ISR и Cisco 2911 ISR выступают в качестве выбранных платформ. В соответствии с ресурсами главной площадки этот маршрутизатор выделяется с DSP и двойным HWIC T1/E1. Если необходимо, порт T1/E1 можно использовать для доступа к PSTN PRI с целью поддержки системы унифицированных коммуникаций. Маршрутизатор Cisco 2911 ISR не поддерживает модули AIM, поэтому следует выбирать Cisco 2811 ISR в том случае, если требуется использовать модуль AIM.

Любые специальные интерфейсы и IP-адреса — это примеры, используемые Cisco для проверки руководства по развертыванию в лабораторных условиях. Используемые интерфейсы и IP-адреса могут различаться.

Сведения о настройке

Из-за разнообразия предложений сервисов WAN и большого числа разнообразного оборудования и программного обеспечения, в данном руководстве рассматривается классический пример арендованного канала T1/E1. Приводится стандартный пример, который можно использовать для интерфейса WAN на главной площадке или в филиале (для получения подробных сведений см. Руководство по настройке.)

В сочетании с HWIC можно использовать канал T1 или E1, поэтому необходимо указать режим. Это выполняется с помощью следующей команды:

```
card type t1 0 0
```

Это глобальная команда настройки, где параметр 0 0 указывает, что HWIC находится в разъеме карты 0 и разъеме WIC — 0.

Для синхронизации маршрутизации используется порт 0 HWIC T1/E1. Сначала плата должна быть настроена для предоставления маршрутизации, после чего для хронометра выставляется значение 1 (самый высокий приоритет) при помощи следующих команд настройки:

```
network-clock-participate wic 0
network-clock-select 1 T1 0/0/0
```

Следующие команды выбирают порт 0 HWIC в качестве исходного для системных часов, которые устанавливается для извлечения значения из линии, синхронизируясь с сетью оператора связи. Следующая команда может различаться в зависимости от скорости обслуживания. В этой модели развертывания команда channel group выделяет все 24 временных интервала для последовательного интерфейса 0/0/0:0, который создается после выполнения следующей команды:

```
controller T1 0/0/0
 clock source line primary
 channel-group 0 timeslots 1-24
```

И этот последовательный интерфейс позволяет настроить адрес, который требуется для WAN. В данном случае использовалась подсеть 10.0.1.0/30:

```
interface Serial0/0/0:0
 ip address 10.0.1.1 255.255.255.252
 ip pim sparse-mode
 load-interval 30
 max-reserved-bandwidth 100
 service-policy output WAN
```

Чтобы включить динамическую маршрутизацию, используется EIGRP с таким же номером автономной системы, что и другой маршрутизатор с коммутаторами. При помощи этой сетевой команды был включен EIGRP на всех интерфейсах в указанном диапазоне сети, все в рамках этого маршрутизатора:

```
router eigrp 1
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 no auto-summary
```

Настройка Ethernet на основной площадке

Маршрутизатор основной площадки подключен к коммутаторам уровня ядра, а оба интерфейса Gigabit Ethernet используют EtherChannel для обеспечения высокой доступности. Каждый интерфейс подключается к другому коммутатору или модулю-лезвию в стеке уровня ядра или модульном коммутаторе.

Настройка интерфейса LAN:

```
interface Port-channel1
 no ip address
 hold-queue 150 in
!
interface Port-channel1.31
 encapsulation dot1Q 31
 ip address 192.168.31.2 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
 channel-group 1
!
```

```
interface GigabitEthernet0/0.31
 channel-group 1
!
interface GigabitEthernet0/1
no ip address
 duplex auto
speed auto
 media-type rj45
 channel-group 1
!
interface GigabitEthernet0/1.31
 channel-group 1
```

В дополнение к настройке EtherChannel определяется интерфейс LAN в качестве интерфейса соединительной линии (802.1q). Теперь, и, возможно, в будущем, потребуется создать другую VLAN для дополнительных целей, например, проводного гостевого доступа. Определяя настройку таким образом с самого начала, можно с легкостью добавить подчиненные интерфейсы при минимальном вмешательстве пользователя.

Настройка Ethernet в филиалах

Настройка маршрутизатора в филиале похожа на настройку маршрутизатора в головном офисе с тем отличием, что EtherChannel не используется и имеется больше подчиненных интерфейсов, поскольку маршрутизатор предоставляет коммутацию уровня 3 в филиале:

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.64
 description Access Subnet
 encapsulation dot1Q 64
 ip address 192.168.64.1 255.255.255.0
!
interface FastEthernet0/0.65
 description Voice Subnet
 encapsulation dot1Q 65
 ip address 192.168.65.1 255.255.255.0
```

```
interface FastEthernet0/0.69
 description Wireless Access
 encapsulation dot1Q 69
 ip address 192.168.69.1 255.255.255.0

interface FastEthernet0/0.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 192.168.70.1 255.255.255.0
```

Эта настройка включает сервисы передачи обычных данных, голосовых данных, беспроводной передачи и гостевого беспроводного доступа на площадке филиала.

Подчиненные интерфейсы и IP-адреса, которые используются в настоящем руководстве, используются только в примерах этого руководства по развертыванию. Убедитесь, что используются правильные интерфейсы маршрутизации и IP-адреса для развертывания.

Примечания

Обзор технологий

Качество обслуживания (QoS) является важной функцией устройств инфраструктуры сети, используемых в данной инфраструктуре. QoS обеспечивает возможность одновременной работы нескольких пользовательских сервисов и приложений, включая передачу голоса в режиме реального времени, передачу видео высокого качества и данных, чувствительных к задержке, в одной сети. Для того чтобы с помощью сети можно было использовать планируемые, измеряемые и иногда гарантированные сервисы, необходимо обеспечить управление параметрами пропускной способности, задержек, нарушения синхронизации и потерь. Даже если для текущих приложений не требуется использование QoS, использование QoS для протоколов управления и сетевых протоколов обеспечивает защиту функций сети и управления при нормальных и нестандартных условиях трафика.

Назначение этой инфраструктуры заключается в предоставлении необходимого класса обслуживания для поддержки добавления к сети трафика передачи голоса, интерактивного видео, важнейших приложений данных и управления трафиком либо при первоначальном развертывании, либо в дальнейшем с минимальным воздействием на работу системы и затратами на инженерно-технические работы.

В настоящей архитектуре применяются следующие классификации QoS. Эта таблица используется только в качестве примера.

Подробности настройки

Настройка инфраструктуры сети QoS для этой архитектуры будет разделена на два раздела: локальная сеть (LAN) и глобальная сеть (WAN). Относящиеся к QoS настройки для других технологий, использующих инфраструктуру сети, будут описываться в соответствующих разделах.

Приложение	Классификация уровня 3			Уровень 2 CoS
	IPP	PHB	DSCP	
Маршрутизация IP	6	CS6	48	6
Голосовая связь	5	EF	46	5
Интерактивная видеосвязь	4	AF41 AF42	34 36	4
TelePresence	4	CS4	32	4
Локально определенные важнейшие данные	3	AF31	26	3
Сигнализация вызовов	3	CS3	24	3
Данные транзакций	2	AF21	18	2
Управление сетью	2	CS2	16	2
Общие данные	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

Локальная сеть (LAN)

В этом примере во всех коммутаторах используются следующие команды базовой настройки:

```
mls qos
```

Эта команда глобально включает QoS в коммутаторе, и ее необходимо включить до применения какой-либо из команд QoS, перечисленных ниже. После включения `mls qos` для наиболее эффективной настройки QoS для определенной платформы используйте одну из команд интерфейса auto qos. Для всех проводных точек доступа используйте версию “cisco-phone”. Благодаря этому обеспечивается возможность для недоверенного персонального компьютера и/или доверенного IP-телефона Cisco® выполнить подключение и автоматически настроить параметры QoS:

```
auto qos voip cisco-phone
```

При первом применении этой команды он автоматически создаст глобальную настройку mls, в которую входят сопоставления QoS и настройка очередей, соответствующие характеристикам коммутатора. К коммутаторам фермы серверов обычно не подключают IP-телефоны. Также по умолчанию "доверенными" при использовании этой команды являются классы обслуживания (CoS), что не является типичным методом обслуживания, который используется серверами, классифицирующими трафик. Следовательно, для коммутаторов фермы серверов необходимо настроить в интерфейсе `"auto qos voip trust",` поскольку при этом будут автоматически созданы команды QoS global [или qos global]. После этого доверенный CoS или CoS по умолчанию может быть изменен на доверенный DSCP (изменения выполняются по отдельности для каждого интерфейса) с помощью команды интерфейса `mls qos trust dscp.`

DSCP является доверенным для всех интерфейсов коммутаторов. Была использована команда "mls qos" для настройки DSCP как доверенного для всех интерфейсов доступа, ферм серверов и сетей уровня ядра, обеспечивающих подключения между коммутаторами.

До перехода к описанию QoS (для WAN) следует отметить определенные специальные требования к другим технологиям, используемым в основе сети. Беспроводные точки доступа в этом примере обеспечивают возможность их размещения на любом порту доступа с автонастройкой IP-адреса и контроллера WLAN (WLC). Однако по умолчанию QoS настраивается как недоверенный для устройств IP-телефонии от других производителей (не Cisco). Следовательно, настройку QoS для порта точки доступа необходимо изменить следующим образом:

Конкретный настраиваемый порт зависит от местоположения подключения точки доступа:

```
interface GigabitEthernet1/0/3
 auto qos voip trust
 mls qos trust dscp
```

Этот интерфейс настраивается точно так же для восходящих каналов связи между коммутаторами, каналов связи между коммутаторами и маршрутизаторами, контроллера беспроводной локальной сети, устройств Cisco Unified Communications Manager и Cisco Unity Connections.

Глобальная сеть (WAN)

Из-за разнообразия интерфейсов WAN и предложений операторов связи рекомендуется проконсультироваться с оператором связи об особенностях настройки при подключении к предлагаемым сервисам WAN. Ниже описывается базовые концепции и способы обеспечения пропускной способности для передачи трафика в будущем. Ниже приведен пример настройки, используемой для передачи голоса и видео в унифицированных коммуникациях, а также для приоритезации интерактивного трафика данных. Настройка QoS для WAN обеспечивает пять дополнительных классов обслуживания помимо класса по умолчанию "Best Effort". Эти дополнительные классы можно настроить, даже если в ближайшем будущем их использование не планируется, поскольку назначенная пропускная способность доступна для другого трафика. Чтобы упростить еще более настройку в этом примере, распределение пропускной способности выполняется на основе процентного соотношения доступного интерфейса или скорости канала.

Настройка разделена на две части: в первой части выполняется сопоставление классификации QoS с классом; вторая часть определяется как политика, которая затем применяется к интерфейсу WAN. Первая часть определена следующим образом:

```
class-map match-all Interactive-Video
 match ip dscp af41 af42
class-map match-any Network-Control
 match ip dscp cs6
 match ip dscp cs2
class-map match-all Critical-Data
 match ip dscp af21 af22
class-map match-all Call-Signalling
 match ip dscp cs3
class-map match-all Voice
 match ip dscp ef
```

В приведенных выше примерах определяются классы для трафика передачи данных, интерактивной передачи видео (видеоконференций), управления сетью (трафика сетевых протоколов и управления) и важнейших данных (с высоким уровнем интерактивности, например для telnet, Citrix и тонких клиентов Oracle).

Во второй части настройки используются имена классов и определяется максимальная гарантированная пропускная способность, выделенная для каждого класса. Также добавляется один дополнительный класс "по умолчанию", определяющий минимальную доступную пропускную способность, предусмотренную для трафика максимальной производительности:

```
policy-map WAN
 class Voice
 priority percent 10
 class Interactive-Video
 priority percent 35
 class Network-Control
 bandwidth percent 10
 class Critical-Data
 bandwidth percent 15
 random-detect dscp-based
 class Call-Signalling
 bandwidth percent 5
 class class-default
 bandwidth percent 25
 random-detect
```

При обычных условиях общая сумма назначений пропускной способности не может превышать 75 процентов, что оставляет доступность в 25 процентов для сетевого трафика. Однако это можно изменить при помощи команды интерфейса:

```
max-reserved-bandwidth
```

Необходимо отметить, что обеспечение необходимой пропускной способности определено в классе Network Control для обеспечения стабильной работы.

В низкоскоростных каналах (скорость ниже T1 и E1) можно добиться дополнительной экономии пропускной способности, включив сжатие заголовков (при достаточной производительности процессора маршрутизатора). Благодаря этому обеспечивается сокращение трафика голосового вызова с узкой полосой с использованием кода G.729 с 24 кбит/с до приблизительно 11 кбит/с. Для стабильной работы сжатия заголовков его необходимо включить на обеих сторонах канала глобальной сети. Согласно политике к классу Voice добавляется дополнительная команда:

```
class Voice
 priority percent 10
 compression header ip rtp
```

Обеспечение пропускной способности является ключевой функцией, определенной в политике QoS на основе стандартных режимов обработки трафика. Пропускная способность для передачи голоса описывается в разделе "Унифицированные коммуникации". Видео определено как местозаполнитель для более поздних этапов, и поскольку отсутствует видеотрафик, полоса пропускания будет доступна для других классов трафика.

При переходе от WAN к LAN, необходимо поддерживать классификации QoS, используемые на уровне 3 (DSCP) в соответствии с уровнем 2 (CoS) в LAN. Поскольку маршрутизатор в комплексе зданий подключается напрямую к сети уровня ядра с использованием уровня 3, при этом специальные требования отсутствуют; однако в филиалах, где маршрутизаторы подключаются к локальной сети с использованием уровня 2, необходимо добавить следующие команды к маршрутизатору для филиалов и применить их к интерфейсу, подключаемому к коммутатору:

```
policy-map Lan-Edge
 class class-default
 set cos dscp
interface FastEthernet0/0.64
 description Access Subnet
 encapsulation dot1Q 64
 ip address 192.168.64.1 255.255.255.0
 service-policy output Lan-Edge
```

Обзор технологий

По мере того, как рабочая среда становится все более мобильной, изменяются и потребности компаний — и технологии, и продукты Cisco изменяются вместе с этими требованиями. Уделяя основное внимание расширению возможностей беспроводной связи, корпорация Cisco предлагает сервисы беспроводной мобильной сети для передачи голоса и данных, что позволяет обеспечить возможности передачи данных для сотрудников, передачи голоса для беспроводных IP-телефонов и беспроводной гостевой доступ для посетителей, подключающихся к Интернету.

Одной из главнейших задач является простота развертывания; архитектура этой беспроводной сети является защищенной и расширяемой, а также обеспечивает работу головного офиса и филиалов, подключенных с использованием WAN. При этом не охватывается структура радиосвязи (RF).

В прошлом самым простым подходом являлось использование автономных точек доступа, но при этом было необходимо обеспечивать управление каждой точкой и отсутствовала возможность расширяемости функциональности.

В основе новой системы лежит устройство контроллера WLAN, поддерживающее масштабирование для выполнения поддержки необходимого количества точек доступа с целью обеспечения необходимой области покрытия. В этом случае Cisco рекомендует использовать устройства Cisco серии 5500, каждое из которых обеспечивают поддержку до 50 точек доступа. Для упрощения работы в системе используется одно устройства, хотя поддерживается возможность группировки нескольких устройств, что обеспечивает дополнительные возможности и более высокую степень доступности. В системе используется контроллер Cisco 5508, в котором имеется восемь малогабаритных сменных портов распределения, обеспечивающих подключение EtherChannel к коммутаторам уровня ядра или модулям-лезвиям Cisco 4500 и для которого можно использовать как медные кабели, так и волокно в зависимости от расстояний и требований.

В головном офисе используются следующие точки доступа: упрощенные точки доступа Cisco серии 1140 с поддержкой 802.11a/b/g/n. Питание обеспечивается с помощью стандартной PoE от коммутаторов, что обеспечивает возможность развертывания точек доступа без установки или изменения имеющихся в здании электрических розеток (что часто требуется, поскольку точки доступа обычно устанавливаются на потолке).

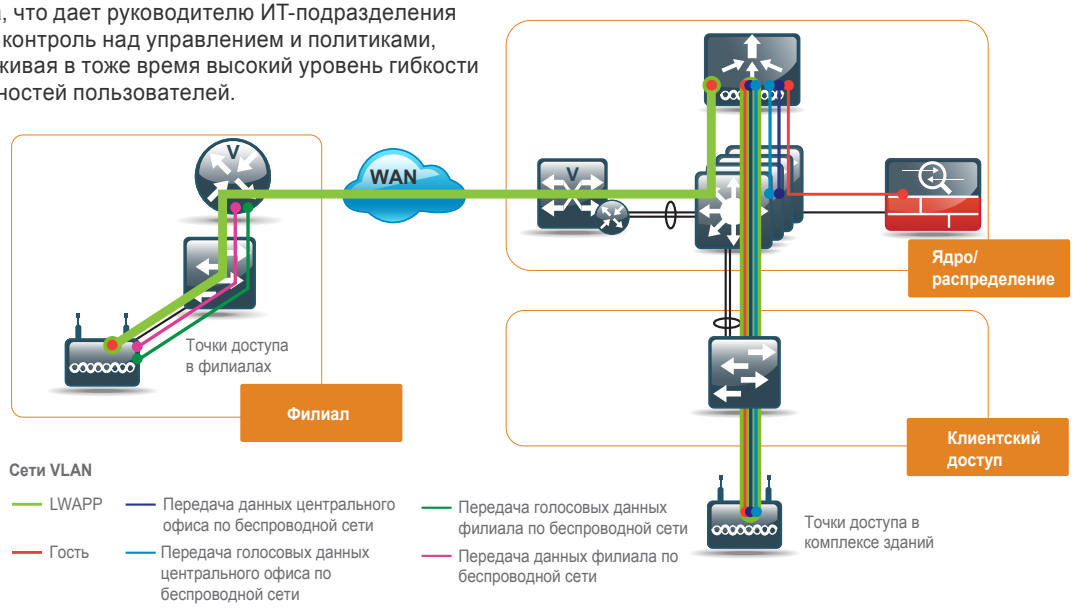
Для филиалов используются следующие точки доступа: Cisco 1140, обеспечивающие 802.11a/b/g/n. В нормальных условиях они используются в режиме "Lightweight"; если подключение между филиалом и головным офисом разорвано, используется режим "Autonomous". Эта возможность достигается за счет использования технологии Hybrid Remote Edge Access Point (H-REAP). H-REAP представляет собой метод развертывания точки доступа, что обеспечивает для точки доступа возможность подключений, что в свою очередь позволяет обеспечить работу без прерываний даже при потере подключения к контроллеру WLAN. При возникновении сбоя в работе контроллера WLAN новые клиенты не имеют возможности подключения, а существующие клиенты не могут обновить ключи шифрования или “повторный ввод”. При нормальных условиях работы центральный контроллер WLAN поддерживает контроль над настройкой, аутентификацией и программным обеспечением точек доступа, что дает руководителю ИТ-подразделения полный контроль над управлением и политиками, поддерживая в тоже время высокий уровень гибкости возможностей пользователей.

Сведения о настройке

Развертывание беспроводной мобильной сети требует наличия сервера RADIUS для выполнения аутентификации и точки входа DNS, которая позволит точкам доступа найти контроллер WLAN.

В головном офисе будет реализована локальная беспроводная сеть для всего комплекса зданий и отдельная WLAN для передачи голоса, использующая контроллер WLAN, с отдельными доменами для вещания.

На всех узлах филиалов будут использовать одни и те же сети WLAN для передачи данных и голоса, для которых будет реализована локальная коммутация в пределах филиала, что позволит избежать прохода данных при передаче через WAN в момент обращения к локальным ресурсам. Для узлов головного офиса и всех узлов филиалов используется одна гостевая WLAN. WLAN туннелируется обратно к контроллеру WLAN и переключается на определенную VLAN, подключенную к Adaptive Security Appliance (ASA), благодаря чему обеспечивается защищенный доступ к сети Интернет. В гостевой WLAN отсутствуют настройки безопасности для беспроводной связи, и используется открытая аутентификация. Управление доступом к Интернету



осуществляется с помощью web-аутентификации с использованием гостевой учетной записи с истекающим сроком действия, созданной локально в контроллере WLAN.

После завершения физической установки и обеспечения питания для контроллера WLAN подключите порты распределения 1 и 2 соответственно к коммутатору уровня ядра (или отдельным модулям-лезвиям) и настройте EtherChannel между ними. Сети VLAN используются в следующей настройке для беспроводной передачи данных HQ (10), беспроводной передачи голоса HQ (14) и беспроводного гостевого доступа (16), а VLAN 31 используется для интерфейсов управления и диспетчера точек доступа:

```
interface Port-channel11
 description WLAN Controller
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,14,16,31
 switchport mode trunk
interface GigabitEthernet1/0/11 and 2/0/11
interface GigabitEthernet1/0/11
 description WLAN Controller
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,14,16,31
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 channel-group 11 mode on
 spanning-tree link-type point-to-point
end

interface Vlan10
 description Data WLAN
 ip address 192.168.10.1 255.255.255.0

interface Vlan14
 description Voice WLAN
 ip address 192.168.14.1 255.255.255.0

interface Vlan16
 description Wireless Guest
 no ip address
```

Используйте следующие команды для развертывания беспроводной мобильной связи:

```
Management and AP-Manager VLAN is 31
Management Interface address 192.168.31.64/24
Default DHCP server address 192.168.1.1
Virtual Interface address 10.10.10.10
Mobility / RF group name = default
Initial SSID = Guest
```

Затем с помощью консоли контроллера WLAN отобразится схема установки. Текст в экранных запросах отформатирован *курсивом,* а вводимые ответы — **полужирным шрифтом**.

После завершения процесса первоначальной загрузки на экране отобразится следующее:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall?
[yes]:no
```

Шаг 1. Введите имя системы.

```
System Name [Cisco_7e:8e:43] (31 characters
max): HQ WLC
```

Шаг 2. Введите имя пользователя и пароль администратора.

Не используйте приведенное ниже имя пользователя. При вводе паролей они отображаются символами "*" (звездочка).

```
Enter Administrative User Name (24 characters
max): Admin
Enter Administrative Password (24 characters
max): *****
Re-enter Administrative Password: *****
```

Шаг 3. Используйте протокол DHCP для настройки IP-адреса портов интерфейса сервиса.

```
Service Interface IP Address Configuration
[none][DHCP]: DHCP
```

Шаг 4. Включите агрегацию каналов.

```
Enable Link Aggregation (LAG) [yes][NO]: yes
```

Шаг 5: Введите IP-адрес и маску подсети для интерфейса управления (т.е. IP-адрес **192.168.31.64**, маска подсети **255.255.255.0**, шлюз по умолчанию **192.168.31.1** и VLAN **31**).

```
Management Interface IP Address:
192.168.31.64
Management Interface Netmask: 255.255.255.0
Management Interface Default Router:
192.168.31.1
Management Interface VLAN Identifier (0 =
untagged): 31
```

Шаг 6. Для клиентов введите сервер DHCP по умолчанию.

(В этом руководстве по развертыванию это **192.168.1.1**, т.е. сервер DHCP, настроенный на коммутаторах уровня ядра. В качестве альтернативы можно использовать адрес сервера DHCP в ферме серверов).

```
Management Interface DHCP Server IP Address:
192.168.1.1
```

Шаг 7. Виртуальный интерфейс, используемый контроллером WLAN для ретрансляции DHCP для мобильной связи и связи между контроллерами (например, 10.10.10.10).

```
Virtual Gateway IP Address: 10.10.10.10
```

Шаг 8. Введите имя, которое будет использоваться как имя по умолчанию для группы мобильной связи и радиосвязи (например, default).

```
Mobility/RF Group Name: default
Enable Symmetric Mobility Tunneling [yes]
[NO]: no
```

Шаг 9. В качестве первоначального имени сети (SSID) введите Guest.

```
Network Name (SSID): Guest
```

Шаг 10. Введите "no", вынуждая использование клиентами IP-адресов DHCP.

```
Allow Static IP Addresses [YES][no]: no
```

Шаг 11. Введите "no", чтобы настроить RADIUS с использованием графического интерфейса пользователя (GUI), как будет выполнено далее в этом руководстве.

```
Configure a RADIUS Server now? [YES][no]: no
```

Для политики безопасности WLAN по умолчанию необходим сервер RADIUS.

Шаг 12. Введите правильный код страны, в которой выполняется развертывание. (Чтобы получить список действующих кодов стран, введите "help").

```
Enter Country Code list (enter 'help' for a
list of countries) [US]: US
```

Шаг 13. Включите функцию автоматического назначения радиочастоты в управлении радиоресурсами (RRM) для контроллера WLAN, введя **yes**.

```
Enable Auto-RF [YES][no]: yes
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 08.07.09
Enter the time in HH:MM:SS format: 10:10:00
Configuration correct? If yes, system will
save it and reset. [yes][NO]: yes
```

Настройка сохранена.

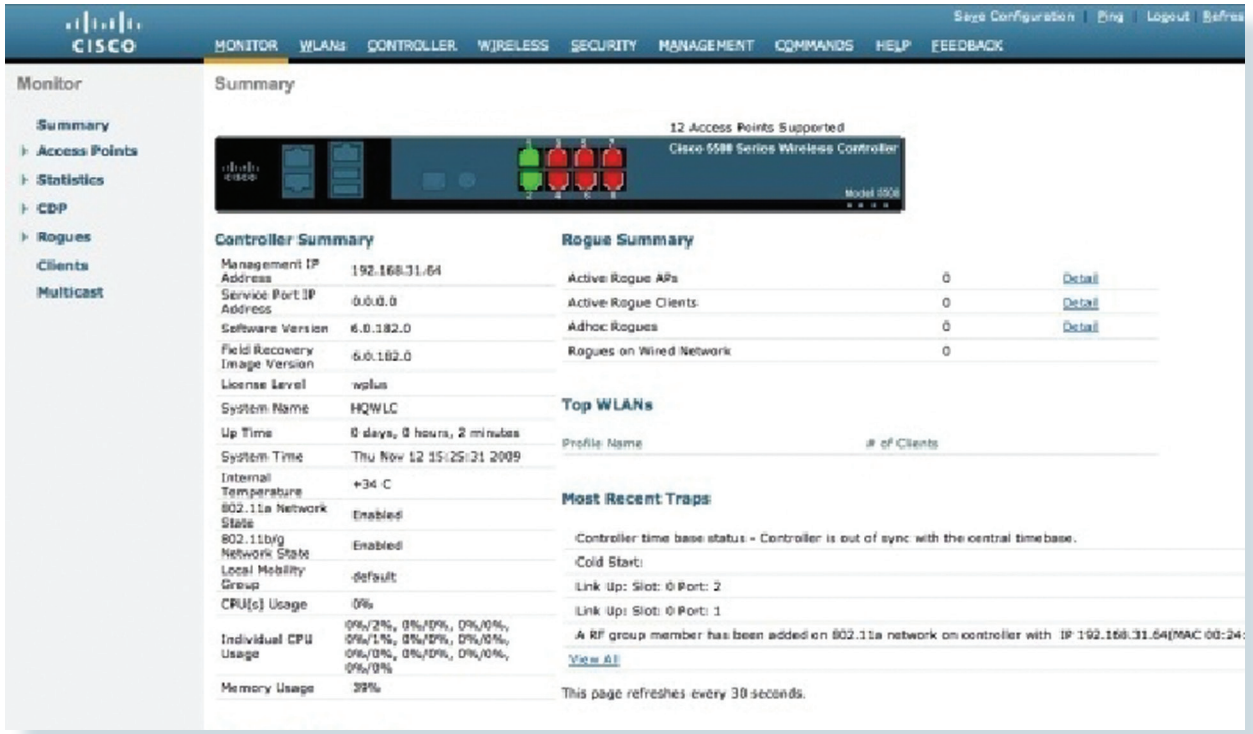
Перезагрузка системы для активации новой настройки...

На этом этапе в контроллере WLAN будет сохранена настройка, после чего выполнена перезагрузка. При отображении запроса на экране введите имя пользователя и пароль, использованный в приведенном выше шаге 2.

Для проверки базовой установки используйте команду show port summary, чтобы убедиться, что оба порта включены и активны. Также с помощью команды show port summary можно проверить правильность IP-адресов и VLAN для интерфейсов диспетчера точек доступа и управления. Следует отметить, что обоими интерфейсами используется порт Link Aggregation Group (LAG), группирующий два порта распределения вместе таким образом, что они обеспечивают балансировку загрузки и высокую доступность для двух коммутаторов уровня ядра, настроенных для EtherChannel.

После проверки можно получить доступ к графическому интерфейсу пользователя контроллера WLAN через web-браузер с помощью клиента, подключенного к проводной сети:

https://192.168.31.64



Также можно использовать доменное имя, если в IP-адрес управления добавлена запись Host.

До перехода к следующим этапам настройки в контроллере WLAN, необходимо убедиться в наличии записи Host для ***cisco-lwapp-controller*** с IP-адресом ***ap-manager*** в сервере DNS, указанном в пулах DHCP или областях адресов DHCP. (В данном случае сервер DNS имеет адрес 192.168.28.10.).

При использовании DHCP для получения данных IP-адреса, маски сети, шлюза и сервера DNS точка доступа использует DNS для разрешения **cisco-lwapp-controller** и создания соединения с контроллером WLAN. В графическом интерфейсе пользователя можно включить радиомодули (по умолчанию они отключены) и выполнить дополнительную настройку. Хотя это не является обязательным, рекомендуется определить запись DNS Host для IP-адреса управления.

В головном офисе для портов доступа, подключенных к точкам доступа, должна использоваться стандартная настройка портов коммутаторов доступа с единственным исключением. Уровень доверия по умолчанию необходимо изменить с CoS на DSCP при помощи команды интерфейса `mls qos trust dscp`.

После входа в web-интерфейс появится возможность проверки базовой работоспособности контроллера WLAN на странице `Monitor>Summary`.

После всех операций настройки обязательно сохраняйте настройку (верхний правый угол графического интерфейса пользователя).

На этой странице показаны включенные порты распределения (выделенные зеленым цветом) и все точки доступа, с которыми установлена связь.

Беспроводной гостевой доступ

Ниже описывается развертывание гостевой беспроводной сети с поддержкой гостевого доступа с именем пользователя и паролем guest для доступа к Интернету как из головного офиса, так и из филиалов.

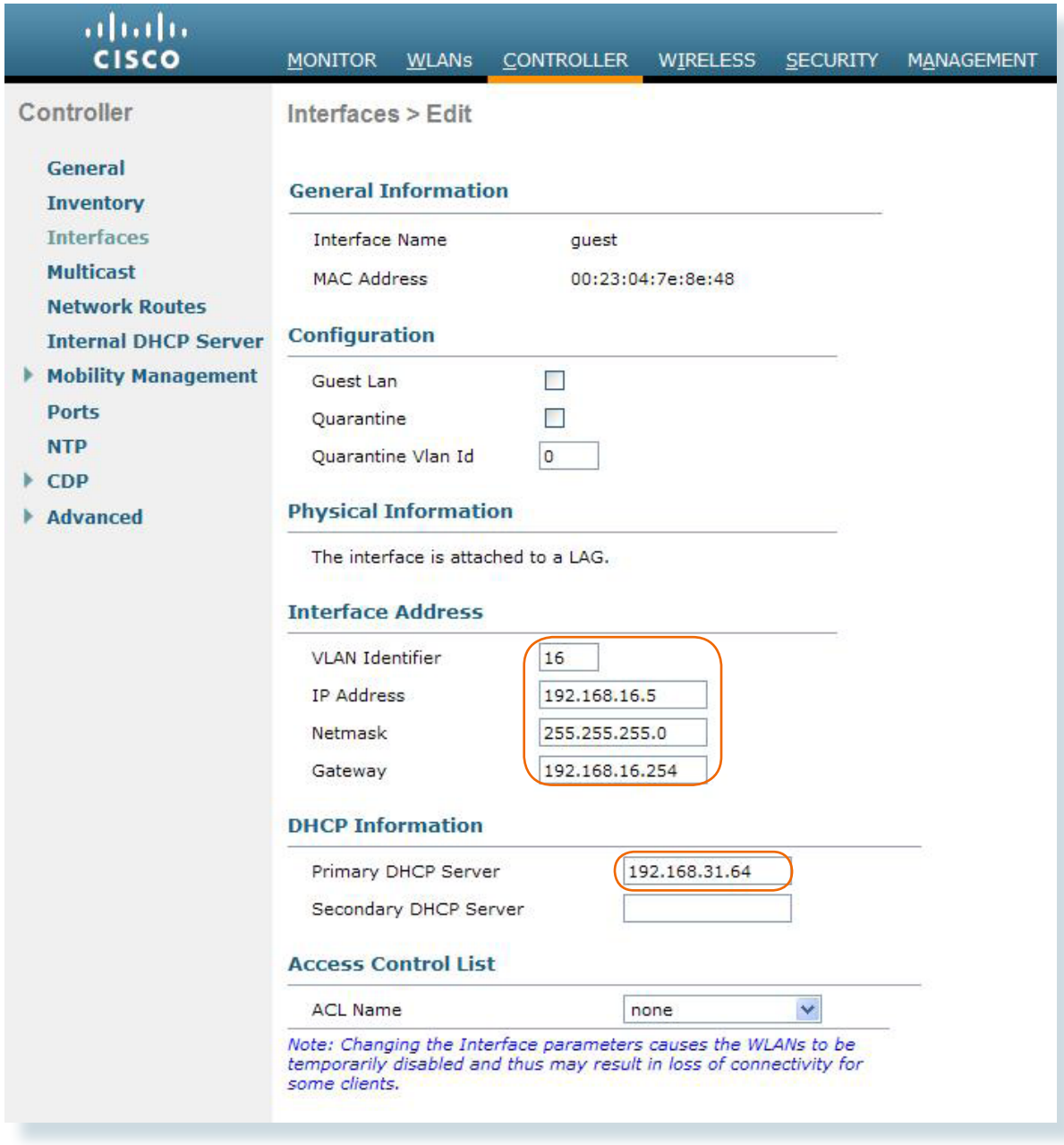
На коммутаторах уровня ядра VLAN 16 ранее использовалась для предоставления направления гостевого трафика специально к устройству ASA. У интерфейса VLAN в коммутаторе уровня ядра отсутствует IP-адрес, т.к. в качества шлюза по умолчанию для этой подсети будет использоваться ASA и не будет обеспечиваться доступ к остальной части сети. Сервисы DHCP и гостевая аутентификация будут обеспечиваться контроллером WLAN. Срок действия "гостевой" учетной записи в контроллере WLAN истекает после заранее определенного периода времени (по умолчанию этот срок равен 24 часам), после чего необходимо выполнить новую аутентификацию с использованием новых созданных имени пользователя и пароля.

В этом развертывании для настройки беспроводного гостевого доступа необходимо использовать следующие данные:

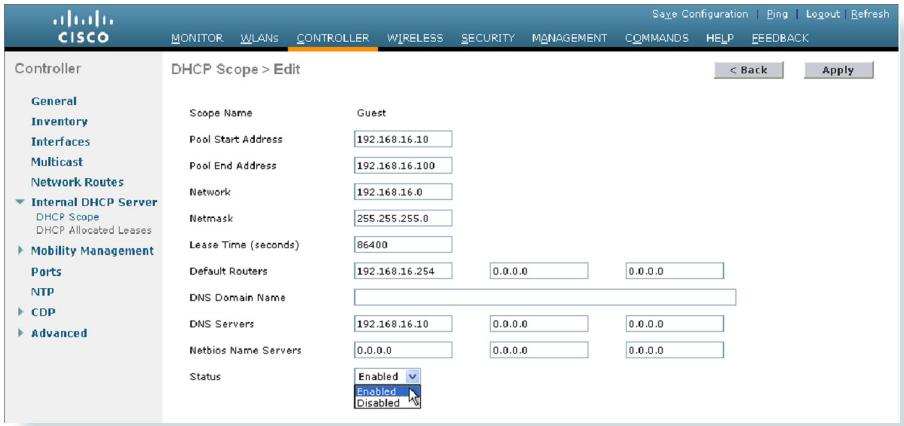
```
VLAN 16
IP address 192.168.16.5
Netmask 255.255.255.0
Gateway 192.168.16.254
Primary DHCP server 192.168.31.64
SSID guest
```

Шаг 1. Убедитесь, что можно использовать VLAN 16 для интерфейсов коммутаторов уровня ядра, подключенных к интерфейсам ASA и контроллера WLAN (VLAN 16).

Шаг 2. Настройте параметры интерфейса на странице управления контроллером WLAN.

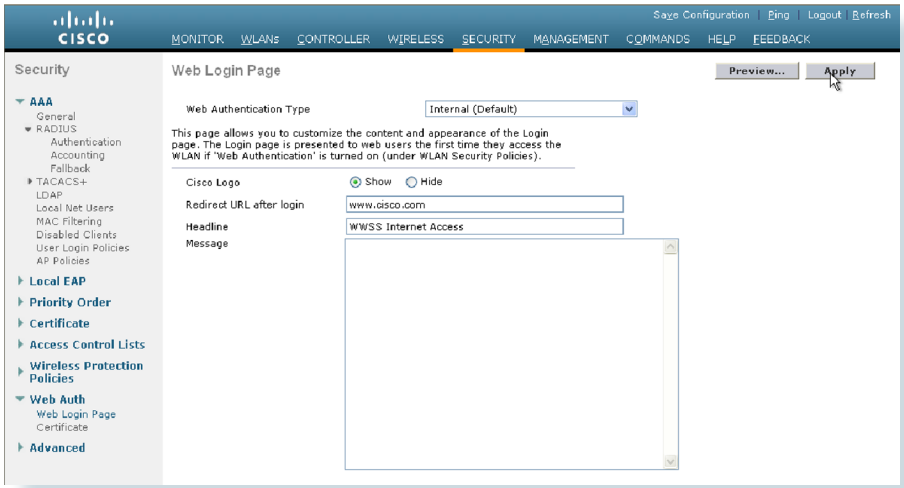


Шаг 3. Настройте область адресов DHCP на внутреннем сервере DHCP контроллера WLAN. Выберите Контроллер > Internal DHCP Server и задайте состояние **"Enabled"**.



Шаг 4. Настройте страницу "Вход в web-аутентификацию" Security>Web Auth>Web Login Page.

Если при первоначальной настройке контроллера WLAN уже была выполнена настройка WLAN для гостевого доступа, на этом этапе нужно внести необходимые изменения в эту WLAN для поддержки web-аутентификации.

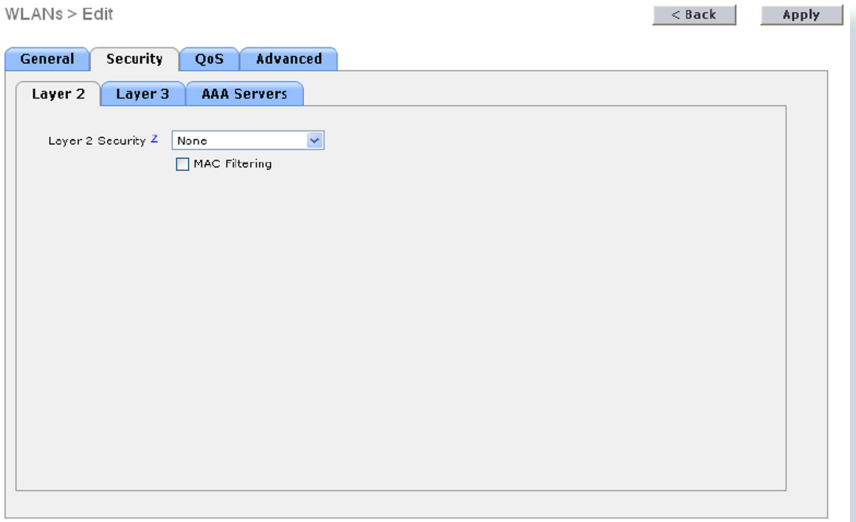


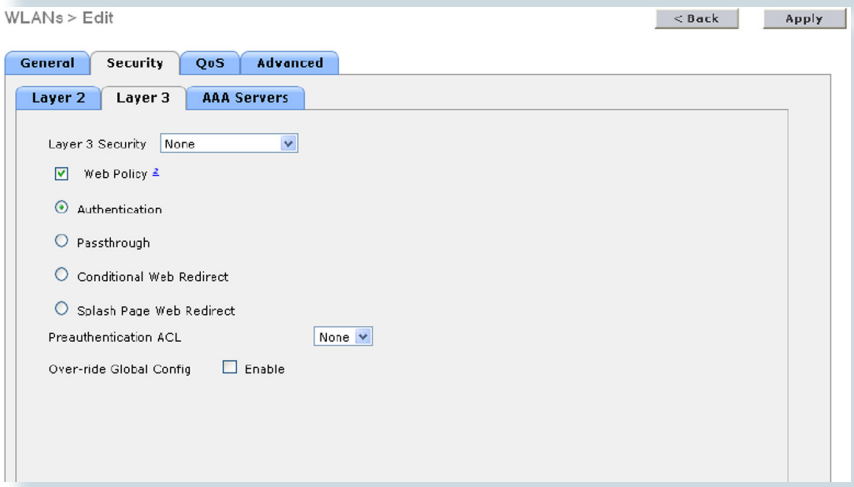
Шаг 5. Задайте для безопасности уровней 2 и 3 значение **None**.

WLAN (выберите идентификаторы WLAN, соответствующие имени сети (SSID) Guest)

На вкладке "Security" выберите вкладку “Layer 2” и установите для безопасности уровня 2 значение "None". Затем перейдите на вкладку "Layer 3" и установите для безопасности уровня 3 значение "None".

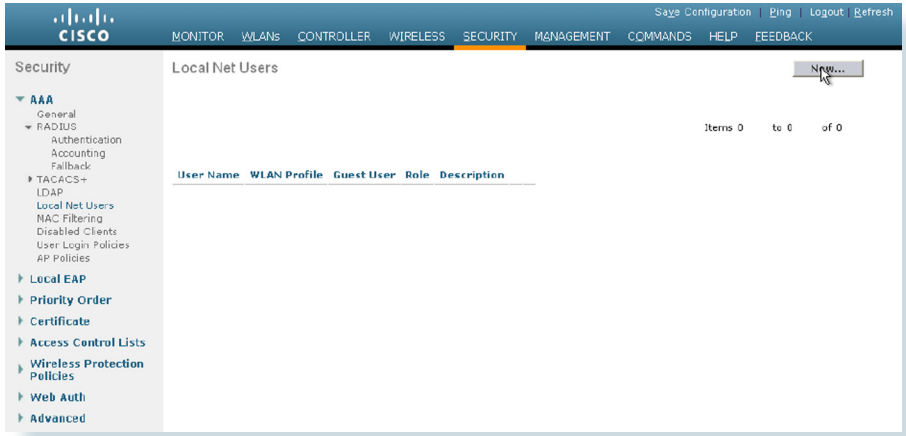
На вкладке "Layer 3 Security" установите флажок "Web-политика" и убедитесь, что установлен флажок "Аутентификация".





Убедитесь, что для аутентификации пользователей-гостей выбран только один метод — LOCAL. Это можно сделать, выбрав RADIUS и/или LDAP и переместив их в поле "Не используется", как показано ниже.

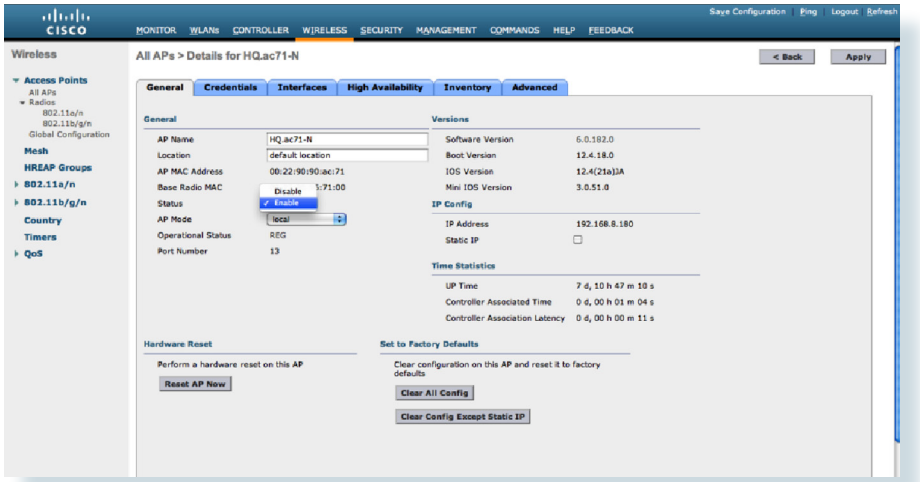
Шаг 6. Добавьте учетную запись пользователя-гостя. Security > Local Net Users



Установите флажок для пользователя-гостя, чтобы разрешить истечение подсчета после 86400 секунд (1 день), и выберите профиль гостевой WLAN.

Теперь можно включить точки доступа: Wireless > All APs

Для всех точек доступа установите состояние "Enabled".



При работе с беспроводным клиентом можно выполнить проверку подключения к гостевой WLAN. Если режим безопасности не включен, должен быть получен IP-адрес, и после открытия web-браузера будет выполнено перенаправление на web-страницу, на которой будет необходимо ввести имя пользователя и пароль для доступа к Интернету, который будет доступен в течение 24 часов.

По умолчанию, для всех точек доступа в этой схеме развертывания будет использоваться гостевая WLAN. Если необходимо ограничить гостевую WLAN и включить только определенные точки доступа, то данные о настройке приведены в разделе "Ограничение сетей WLAN" далее в этом руководстве.

Сети WLAN, которые используются для передачи данных и голоса в головной офис и филиалы, будут использовать учетные записи домена Active Directory (AD) для аутентификации клиентов. Для этого будет использоваться сервер аутентификации Microsoft IAS для обеспечения сервиса RADIUS (Remote Authentication Dial in User Service).

RADIUS

Для этого необходимо выполнить следующие действия.

Шаг 1. Установите IAS на сервер Windows.

Шаг 2. Откройте консоль управления сервисами аутентификации Интернета.

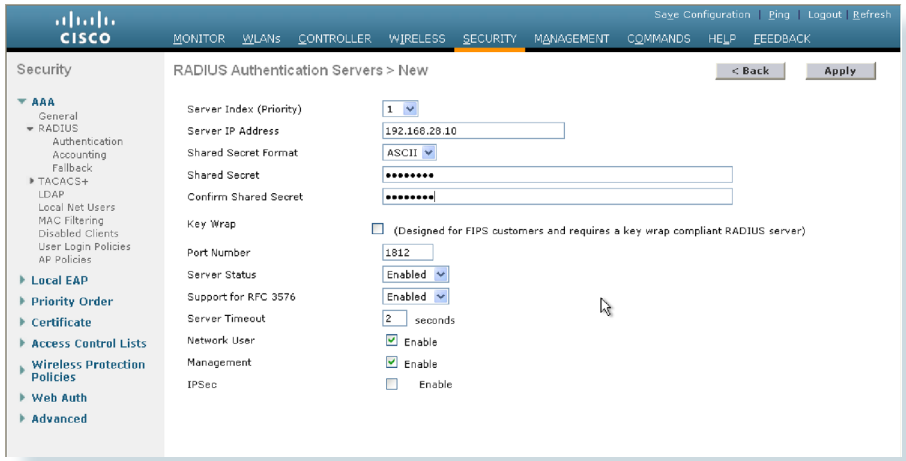
Шаг 3. С помощью мастера настройки политик добавьте политику "Беспроводной доступ" для группы пользователей, в которой разрешено подключение к беспроводной сети (например, для группы "Пользователи домена").

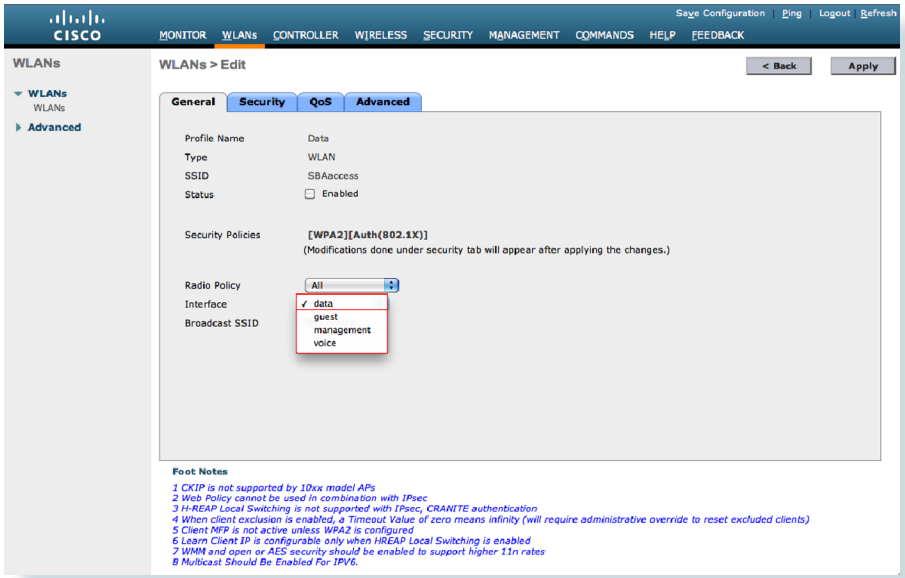
Шаг 4. С помощью мастера настройки клиента RADIUS добавьте нового клиента, который будет использовать IP-адрес (или доменное имя) интерфейса управления контроллером WLAN. В этом действии потребуется открытый ключ, который также будет использоваться при настройке клиента RADIUS контроллера WLAN.

В графическом интерфейсе пользователя контроллера WLAN добавьте сервер RADIUS на странице Безопасность.

```
SECURITY>RADIUS> выберите "Создать"
```

В этом примере IAS устанавливается на сервере 192.168.28.10 (этот сервер также является сервером DNS) и использует тот же открытый ключ, который использовался в шаге 4.



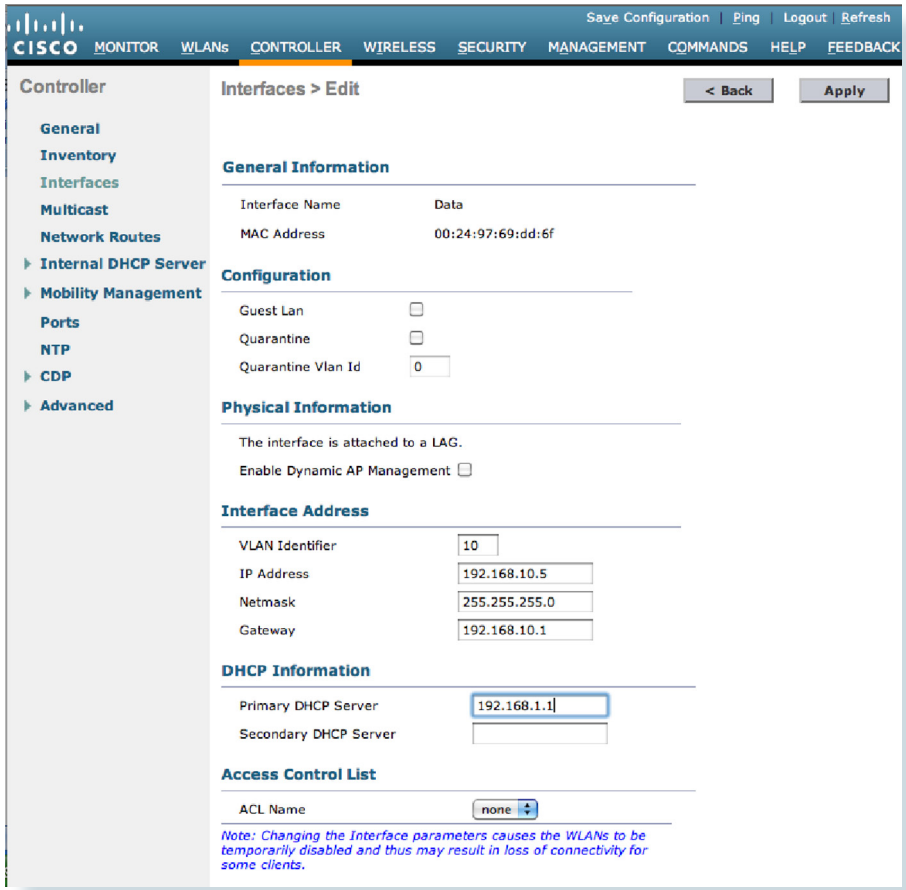


В следующем разделе описывается сеть WLAN для передачи данных и голоса, используемая сотрудниками компании. Во всех сетях WLAN для настройки безопасности, QoS и аутентификации используется ранее настроенный сервер RADIUS.

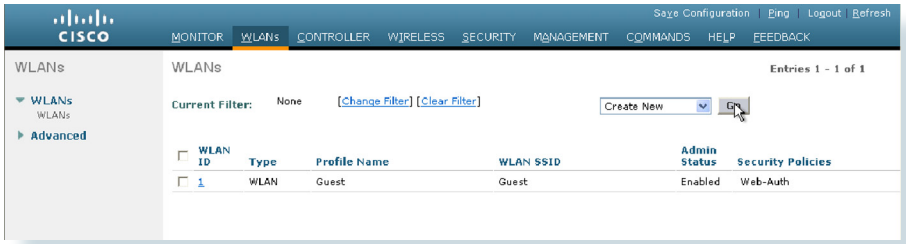
Для настройки доступа к данным в WLAN будут использоваться следующие данные:

```
VLAN 10
IP address 192.168.10.5
Netmask 255.255.255.0
Gateway 192.168.10.1
Primary DHCP Server 192.168.1.1
SSID SBAaccess
```

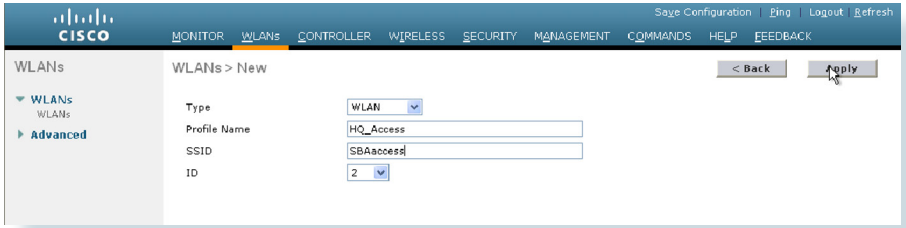
Шаг 1. Настройте интерфейс, который также будет использоваться для управления сетями VLAN/WLAN в головном офисе.



Шаг 2. Настройте WLAN.



Добавьте новую сеть WLAN, выбрав "Создать новую" на странице WLAN и нажав кнопку "Начать".

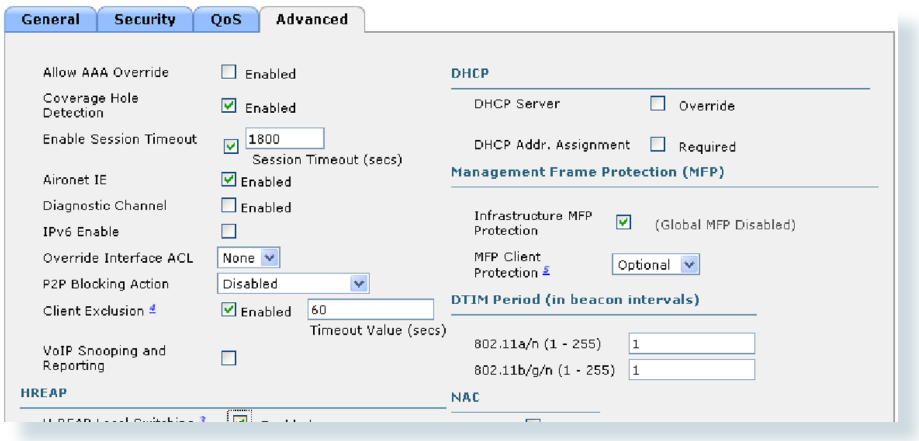


Для типа оставьте без изменения предлагаемую по умолчанию "WLAN" и введите имя профиля и SSID.

Нажмите "Применить". Для состояния выберите "Enable". Для интерфейса выберите имя, созданное в шаге 1 (SBAaccess).

В этой схеме развертывания используются аутентификации WPA2 и 802.1X, а также QoS уровня Silver (оба режима по умолчанию).

Наконец, настройте эти параметры, а также WLAN для передачи голоса для H-REAP. Перейдите на вкладку "Дополнительно" и установите флажок для локальной коммутации H-REAP и оставьте установленным флажок "Распознавать IP-адрес клиента".



Для настройки сети WLAN для передачи голоса в компании будут использоваться следующие данные.

```
VLAN 14
IP address 192.168.14.5
Netmask 255.255.255.0
Gateway 192.168.14.1
Primary DHCP Server 192.168.1.1
SSID SBAvoice
```

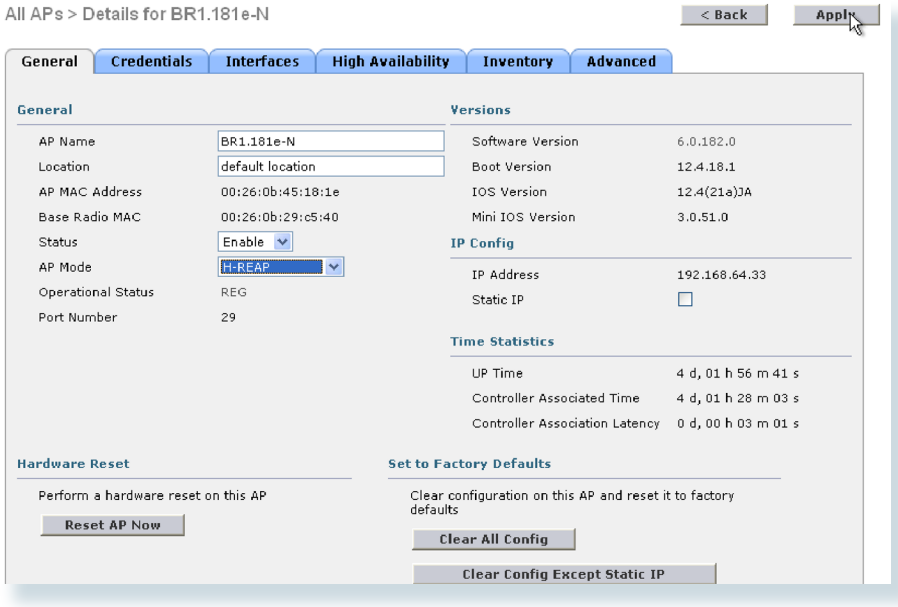
Повторите шаги 1 и 2 с использованием данных настройки голосовой WLAN, но выберите для QoS уровень Platinum, а не Silver.

Настройка беспроводной сети для филиалов

Во всех филиалах будут использоваться сети WLAN для передачи данных и голоса, настроенные для конкретного офиса. Это будут те же сети WLAN, что были настроены ранее для комплекса зданий, с одним значительным отличием.

В головном офисе беспроводной трафик пользователей туннелируется по проводной VLAN для передачи данных с использованием LWAPP на контроллере WLAN, где выполняется переключение на порты LAG, которые являются магистральным каналом 802.1Q в сеть уровня ядра, как показано в начале этого модуля. Если для беспроводного трафика в филиалах также используется такой же режим работы, то трафик, передаваемый между двумя устройствами, будет туннелироваться по WAN к контроллеру WLAN в головном офисе, где он будет туннелироваться в сеть уровня ядра, а потом маршрутизироваться обратно по WAN к филиалам. Это неэффективный способ маршрутизации данных, и он может создать проблемы для унифицированных коммуникаций. Звонок из филиала внешнему абоненту с помощью IP-телефона будет проходить по WAN дважды, хотя для его передачи не требуется выход за пределы филиала. Для разрешения этой проблемы выполняется локальная коммутация сети WLAN для передачи данных и голоса, а для гостевой WLAN используется центральная коммутация. По LWAPP к контроллеру WLAN в головном офисе будет передаваться только трафик управления, контроля и гостевой трафик. Этот режим работы включается при переключении точки доступа из локального режима в режим H-REAP в меню Wireless > AP. Выберите все точки доступа филиалов и измените режим, как указано на предыдущем экране. Нажмите "Применить", после чего будет выполнен сброс точки доступа. После регистрации на контроллере WLAN отобразится дополнительная вкладка H-REAP, используемая для дополнительной настройки, которая будет описана в следующей части этого модуля.

Еще одно преимущество H-REAP заключается в том, что точка доступа может функционировать автономно при потере подключения к контроллеру WLAN, например, из-за простоев WAN. Для этого требуется дополнительная настройка, поскольку беспроводная аутентификация выполняется с использованием сервисов, расположенных в WAN в головном офисе, и не описывается в настоящем руководстве по развертыванию.



После регистрации точки доступа филиала на контроллере необходимо выполнить сопоставление сетей WLAN для передачи данных и голоса. Коммутатор необходимо подключить к точке доступа с использованием соединительной линии к собственной VLAN, сопоставленной с VLAN доступа, что позволит получить адрес от DHCP, который может быть маршрутизирован к контроллеру WLAN в головном офисе.

```
interface GigabitEthernet0/23
 description HREAP Access Point Connection
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 64
 switchport trunk allowed vlan 64-70
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
```

Для настройки всех филиалов будут использоваться следующие данные:

Branch 1:
Data WLAN = VLAN 64
Voice WLAN = VLAN 65

Branch 2:
Data WLAN = VLAN 72
Voice WLAN = VLAN 73

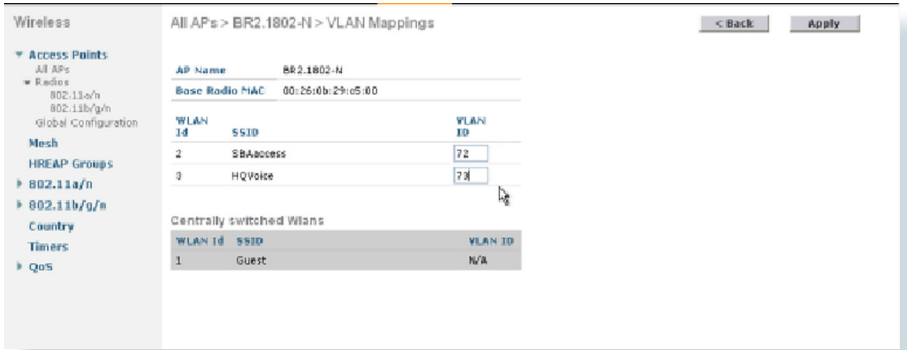
Branch 3:
Data WLAN = VLAN 80
Voice WLAN = VLAN 81

Во всех филиалах выберите все точки доступа и перейдите на вкладку H-REAP. Установите флажок "Поддержка VLAN" и выберите "Применить" (это необходимо сделать до начала сопоставления WLAN и VLAN). Затем повторно выберите эту же точку доступа и опять выберите вкладку H-REAP, нажмите кнопку "Сопоставления VLAN" и назначьте сетям VLAN соответствующие сети WLAN.

Гостевые WLAN назначать нельзя, поскольку исходно они не были настроены как WLAN с локальной коммутацией.

Повторите все эти действия для всех точек доступа в филиалах.

При использовании тех же сетей VLAN для передачи данных и голоса, что и для передачи голоса, в настройку филиалов не нужно вносить никаких изменений. Теперь необходимо выполнить проверку всех WLAN на всех площадках.



Настройка высокого уровня доступности для контроллеров WLAN

Избыточность контроллеров WLAN (WLC) является наиболее важным аспектом при разработке отказоустойчивой беспроводной сети с высоким уровнем доступности. При потере контроллера также для всех локально подключенных точек доступа теряется возможность подключения клиентов к необходимым ресурсам данных. Все точки доступа H-REAP более не могут быть связаны с новыми клиентами и не могут их обслуживать.

Ранее была выполнена настройка всех точек доступа в филиалах как точки доступа H-REAP. Этот процесс представляет собой первый шаг к обеспечению высокого уровня доступности для филиалов. Чтобы обеспечить этот уровень отказоустойчивости для головного офиса и обеспечить для точек доступа филиала возможность дальнейшего использования новых клиентов, а также предоставить необходимый уровень видимости, необходимо добавить новый контроллер.

Первым шагом в этом процессе является настройка нового контроллера в центре данных для обеспечения модели избыточности по схеме N+1. "N" представляет контроллер (или контроллеры), обслуживающие точки доступа в используемой сети. "+1" представляет дополнительный контроллер, на который выполняется переключение при сбое в работе основного контроллера. Для этого контроллера необходимо настроить те же имена сетей (SSID), политики безопасности и активные функции, что и для основного контроллера. В случае сбоя будут изменены сети VLAN, к которым подключены сети WLAN.

Зависимости

1. На всех контроллерах должно быть запущено идентичное ПО.
2. Для всех контроллеров необходимо настроить одни имена сетей (SSID) и сети WLAN.

Сведения о настройке

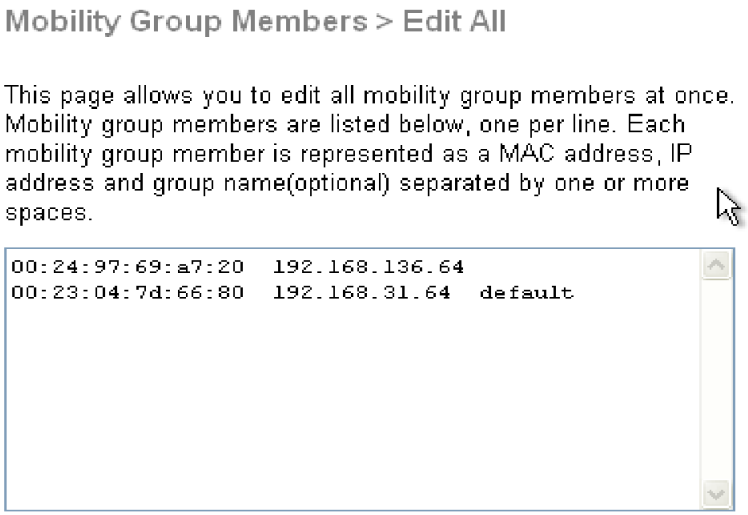
Шаг 1. Настройте коммутатор в центре данных, который будет подключен к дополнительному контроллеру, настроенному ранее, но с использованием VLAN 136, 138, 140, 142 и 144, как показано ниже.

```
interface Port-channel11
 description WLAN Controller
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 136,138,142,144
 switchport mode trunk
```

Используйте в качестве физических подключенных интерфейсов Gigabitethernet 6/0/13 и 7/0/13.

Шаг 2. Настройте дополнительный контроллер, повторив действия по настройке, выполненные ранее, с использованием следующих данных:

```
Management interface: 192.168.136.64
AP Manager Interface: 192.168.136.65
Voice (SBAVoice) WLAN interface: 192.168.142.5/24
DFG 192.168.142.1
DHCP 192.168.152.10

Data (SBAaccess) WLAN interface: 192.168.138.5/24
DFG 192.168.138.1
DHCP 192.168.152.10

Guest (Guest) WLAN interface: 192.168.144.5/24
DFG 192.168.144.254
DHCP 192.168.136.64

Local Pool for your guest net
192.168.144.10 thru 192.168.144.100
DFG 192.168.144.254
DNS (provided by your service provider)
```

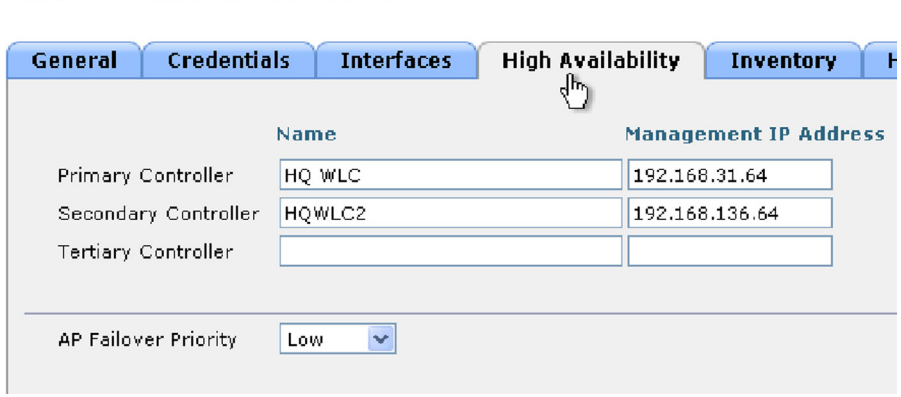


Шаг 3. Настройте на контроллере группу мобильной связи.
`Controller>Mobility Management>Mobility Groups`

Введите MAC-адрес контроллера, IP-адрес и задайте группу мобильной связи "по умолчанию", как настроено ранее для BCEX контроллеров. Нажмите "Применить".

Шаг 4. Для BCEX точек доступа в сети настройте высокий уровень доступности.
`Wireless>AP-Name>High Availability` (вкладка)

Настраивать приоритеты переключения на резервные ресурсы не нужно, поскольку



на всех контроллерах WLAN имеется достаточное количество ресурсов для всех точек доступа в сети. В противном случае необходимо определить точки доступа, являющиеся наиболее приоритетными при переключении на резервные ресурсы.

(ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА)

Шаг 5. Оптимизируйте переключение на резервные ресурсы для сокращения времени переключения для точек доступа.

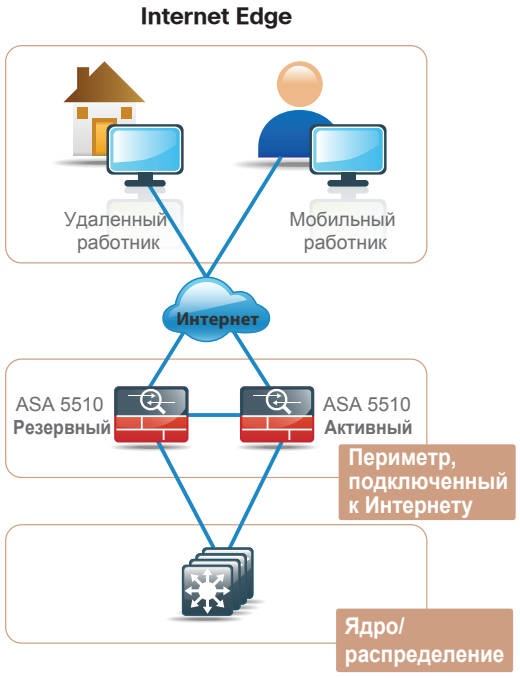
В выходных данных ниже показан тайм-аут для точки доступа в случае недоступности контроллера WLAN, равный 120 секундам. Ниже значение тайм-аута обнаружения изменяется на 60 секунд и выполняется глобальная настройка "резервного" контроллера.

```
(Cisco Controller) >show advanced timers


Authentication Response Timeout (seconds)..... 10
Rogue Entry Timeout (seconds)................. 1200
AP Heart Beat Timeout (seconds)............... 30
AP Discovery Timeout (seconds)................ 10
AP Local mode Fast Heartbeat (seconds)........ disable
AP Hreap mode Fast Heartbeat (seconds)........ disable
AP Primary Discovery Timeout (seconds)........ 120

(Cisco Controller) >config advanced timers ap-primary-discovery-timeout 60

Warning! Setting AP primary discovery timer does not apply to Mesh APs. Apply(y/n)? y



(Cisco Controller) >show advanced timers


Authentication Response Timeout (seconds)..... 10
Rogue Entry Timeout (seconds)................. 1200
AP Heart Beat Timeout (seconds)............... 30
AP Discovery Timeout (seconds)................ 10
AP Local mode Fast Heartbeat (seconds)........ disable
AP Hreap mode Fast Heartbeat (seconds)........ disable
AP Primary Discovery Timeout (seconds)........ 60

 (Cisco Controller) >config advanced backup-controller primary HQWLC2 192.168.136.64

(Cisco Controller) >show advanced backup-controller


AP primary Backup Controller ................. HQWLC2 192.168.136.64
AP secondary Backup Controller ............... 0.0.0.0
```

Примечания

Обзор технологий

Сегодня безопасность является неотъемлемой частью всех развертываний сети. Это обусловлено необходимостью в безопасной, надежной и доступной сети с защитой информационных активов и в соответствии с нормативными требованиями. Поскольку большая часть сетей подключена к Интернету и, следовательно, открыта для постоянного воздействия самораспространяющихся программ, вирусов и целевых атак, компании должны внимательно следить за защитой своих сетевых инфраструктур, пользовательских данных и информации о заказчиках. В этом разделе описываются межсетевые экраны, VPN и системы предотвращения вторжения (IPS). Поскольку нормативные требования могут различаться для разных стран и отраслей, в этом документе не приводится исчерпывающие описания отдельных нормативных требований.



Периметр, подключенный к Интернету, — это участок сети, где сеть компании подключается к Интернету. Этот участок является периметром корпоративной сети. В этой точки в сети обычно используется межсетевой экран, устройство VPN и устройство IPS. В этой архитектуре устройство Cisco Adaptive Security Appliance (ASA) развертывается по периметру, подключенному к Интернету, и выполняет эту функцию в одном недорогом устройстве. В этом разделе описывается базовые настройки межсетевого экрана и VPN. Система IPS будет описываться в отдельном разделе, поскольку специализированные устройства IPS и встроенные в маршрутизатор IPS также развертываются в других точках сети.

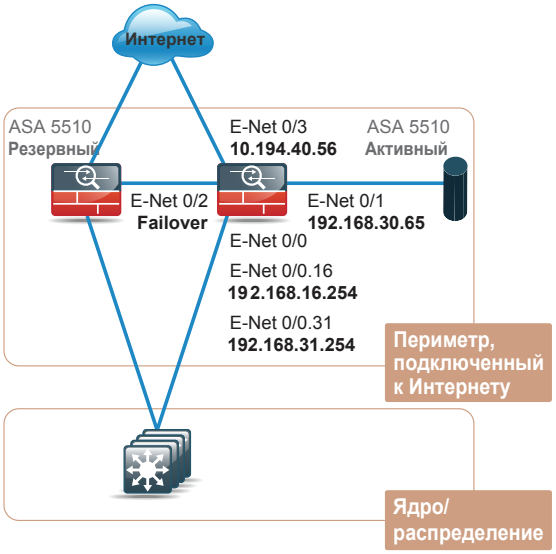
Настройка межсетевого экрана по периметру, подключенному к Интернету

Устройства Cisco ASA настраиваются как пара "активный-резервный" с высоким уровнем доступности. Используется пара "активный-резервный" вместо конфигурации "активный-активный", поскольку она отличается большей простотой. При этом обеспечивается возможность использования этого же устройства для функций межсетевого экрана и VPN (функция VPN отключена в ASA при использовании конфигурации "активный-активный"), а скорость каналов Интернета в этой архитектуре не превышает производительность отдельного устройства ASA. В случае возникновения сбоя в работе активного устройства ASA или при необходимости его отправки для технического обслуживания, функции межсетевого экрана IPS и VPN будут выполняться дополнительным устройством ASA. В самом устройстве ASA запущен EIGRP, что позволяет упростить настройку маршрутизации. При этом при изменениях в сети комплекса зданий и WAN не требуется изменять настройку ASA. Также используется DMZ на случай необходимости в размещении на рабочем участке серверов, доступных для Интернета, но они не описываются в этом примере. Внутренний интерфейс подключен по соединительной линии к коммутатору уровня ядра с интерфейсом VLAN для корпоративного трафика Интернета, а еще одна VLAN настроена для гостевого доступа к Интернету.

Cisco ASA можно настроить с помощью командной строки или из графического интерфейса пользователя Cisco Adaptive Security Device Manager (ASDM). В этом примере для устройств Cisco ASA 5510 и других устройств Cisco серии ASA 5500 используется следующая настройка по умолчанию:

```
interface management 0/0
ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254
management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Чтобы настроить ASA с помощью CLI, подключитесь к порту консоли и используйте терминальный клиент.



Сведения о настройке

Глобальная настройка межсетевого экрана

Чтобы настроить и запустить межсетевой экран, необходимо настроить интерфейсы, настроить маршрутизацию и переключение на резервные ресурсы. **Примечание.** IP-адреса и определенные интерфейсы, используемые в этом примере, отличаются от используемых в реальных сетях. См. рисунок x.x.

Сначала настройте имя хоста и имя домена для ASA:

```
hostname [ASA5510]
domain-name cisco.com
```

Настройте и включите пароль и пароль для консоли/telnet:

```
enable password [password]
passwd [password]
!
```

Затем необходимо настроить интерфейсы межсетевого экрана таким образом, чтобы были включены подключения к внутренней и внешней сети. Необходимо отметить, что у интерфейсов помимо основного адреса имеются резервные IP-адреса. Это часть настройки переключения на резервные ресурсы межсетевого экрана; она будет описана более подробно в разделе, посвященному переключению на резервные ресурсы. У всех интерфейсов в ASA имеется параметр уровня безопасности. Чем выше число, тем выше безопасность на интерфейсе. Внутренним интерфейсам обычно назначается 100, наивысший уровень безопасности, а внешним — 0. По умолчанию трафик может передаваться от интерфейса с более высокой безопасностью к интерфейсу с более низкой безопасностью. Другими словами, трафик может передаваться от внутреннего интерфейса внешнему, но не наоборот.

В этой настройке несколько интерфейсов VLAN подключаются по соединительной линии к внешнему интерфейсу Ethernet 0/0. 31 VLAN используется для передачи внутреннего трафика, а 16 VLAN для беспроводного гостевого доступа.

```
interface Ethernet0/0
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/0.16
 vlan 16
 nameif guest
 security-level 0
 ip address 192.168.16.254 255.255.255.0
standby 192.168.16.253
!
interface Ethernet0/0.31
 vlan 31
 nameif inside
 security-level 100
 ip address 192.168.31.254 255.255.255.0
standby 192.168.31.253
!
```

Ethernet 0/1 представляет собой сеть DMZ для хостов, которые должны быть доступны напрямую из Интернета.

```
interface Ethernet0/1
 nameif DMZ
 security-level 50
 ip address 192.168.30.65 255.255.255.192
standby 192.168.30.66
!
interface Ethernet0/2
description LAN/STATE Failover Interface
!
```

Ethernet 0/3 является внешним интерфейсом и он подключен к ISP.

```
interface Ethernet0/3
 nameif outside
 security-level 0
 ip address 10.194.40.56 255.255.255.0
standby 10.194.40.55
!
```

Настройка высокого уровня доступности межсетевого экрана

Переключение на резервные ресурсы будет выполняться только в том случае, когда оба блока идентичны. Должны быть идентичны следующие характеристики: модель, лицензия и SSM (если SSM установлены). Для второго устройства ASA необходимо обеспечить питание и подключение к той же сети, что и для основного устройства. В этом примере Ethernet 0/2 является интерфейсом переключения на резервные ресурсы, при этом в данном интерфейсе для соединения основного и дополнительного устройства используется кабель с перекрестной разводкой. Интерфейс переключения на резервные ресурсы также является интерфейсом восстановления состояния, что указывает на репликацию всех состояний сеансов из основного в резервный блок в этом интерфейсе. Поскольку там может находиться значительный объем данных, рекомендуется использовать выделенный интерфейс. Чтобы настроить переключение на резервные ресурсы между двумя ASA, используйте приведенные ниже команды:

```
failover
failover lan unit primary
failover lan interface failover Ethernet0/2
failover replication http
failover link failover Ethernet0/2
failover interface ip failover 192.168.30.1
255.255.255.252 standby 192.168.30.2
```

Для каждого общего интерфейса между активными и резервными ASA необходимо настроить резервный адрес. Резервный блок всегда настраивается с резервным адресом. Если резервный ASA становится активным, то он будет использовать основной адрес, а другой ASA в этой паре получит другой адрес, если он еще является активным.

```
ip address 192.168.31.254 255.255.255.0
standby 192.168.31.253
```

Также можно настроить таймеры переключения на резервные ресурсы для ускорения выполнения переключения на резервные ресурсы в случае сбоя в работе устройства или канала. По умолчанию в зависимости от возникшего сбоя для переключения на резервное устройство может занять у ASA от 2 до 25 секунд. При настройке времени опроса при резервном переключении можно уменьшить время переключения до от 0,5 до 5 секунд в зависимости от сбоя. На ASA с низкой или средней нагрузкой время опроса при резервном переключении можно уменьшить без снижения производительности.

```
failover polltime unit 1 holdtime 3
failover polltime interface 1 holdtime 5
```

Настройка маршрутизации в межсетевом экране

Как можно заключить из сказанного выше, все интерфейсы, кроме внутреннего, работают в режиме "passive". Отсутствуют другие маршрутизаторы, с которыми необходимо обмениваться данными на этих интерфейсах, при этом нельзя допустить передачи внутренних данных в менее безопасную сеть. Здесь перераспределяются статические маршруты, поскольку шлюз ASA является единственным связующим звеном между корпоративной сетью и Интернетом. При повторном распределении статических маршрутов ASA передает сведения о настройках по умолчанию остальной сети, и если определенная сеть недоступна, то трафик будет передаваться по маршруту по умолчанию на ASA и трафик будет передаваться в Интернет.

```
router eigrp 1
 network 192.168.0.0 255.255.0.0
 passive-interface guest
 passive-interface DMZ
 passive-interface outside
 redistribute static

route outside 0.0.0.0 0.0.0.0 10.194.40.1 1
```

Настройка NAT/PAT

Завершающим шагом является настройка базовых подключений к Интернету для внутренних хостов. Поскольку при нумерации внутренней сети используется адресация RFC 1918, при которой не поддерживается маршрутизация с использованием Интернета, необходимо преобразовать внутренние частные адреса во внешние открытые адреса. Для этого следует преобразовать все внутренние адреса в открытые адреса внешнего интерфейса.

```
global (outside) 1 interface
nat (inside) 1 192.168.0.0 255.255.0.0
```

Настройка удаленного управления

После первоначальной настройки ASA появляется возможность подключения к устройству удаленно, что упрощает настройку, управление и устранение неполадок.

Приведенная ниже настройка обеспечивает возможность удаленного подключения от любой внутренней сети с использованием HTTPS или SSH. У ASA может быть ограниченный доступ только к одному адресу или доступ к нему может быть предоставлен с помощью сети управления путем изменения операторов сети, приведенных ниже:

```
http server enable
http 192.168.0.0 255.255.0.0 inside
ssh 192.168.0.0 255.255.0.0 inside
ssh version 2
```

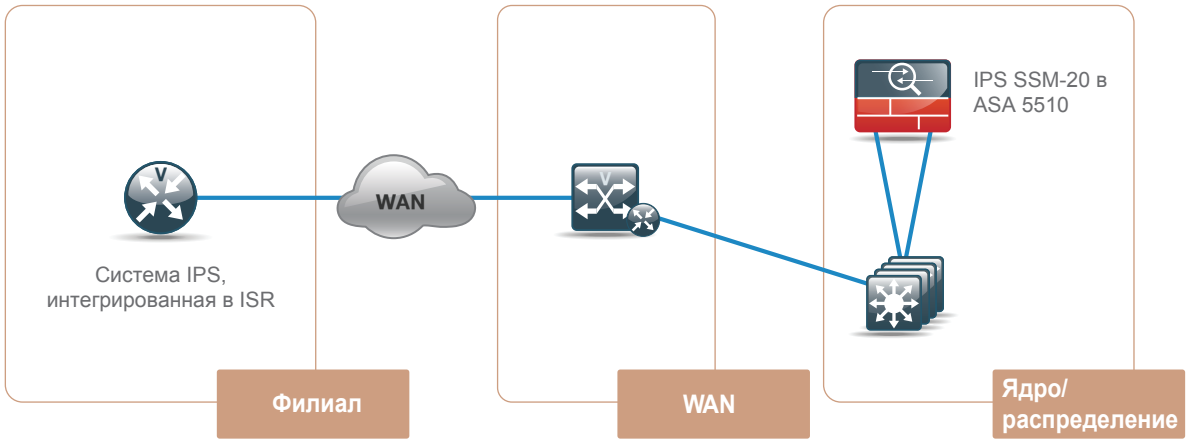
Необходимо настроить имя пользователя и пароль. Это можно сделать локально в ASA или же можно использовать ASA для выбора сервера для AAA. Рекомендуется также локально настроить учетную запись на случай потери связи ASA с сервером AAA.

```
username cisco password [password]
```

Технические рекомендации. Все пароли, приведенные в руководстве, используются в качестве примеров и не должны использоваться при настройке в производственной среде. Соблюдайте политики компаний. Если политики отсутствуют, пароли должны состоять не менее чем из 8 символов с сочетанием верхних и нижних регистров и цифр.

Примечания

Система предотвращения вторжений (IPS)



Настройка IPS

Cisco предлагает IPS с различными форм-факторами и уровнями производительности. IPS можно развернуть как отдельный автономный сервис с устройствами Cisco серии 4200, интегрировать в ASA с модулями SSM или интегрировать в маршрутизаторы Cisco ISR как модули AIM. Cisco 2911 ISR не поддерживает использование модуля AIM-IPS, поэтому Cisco 2811 ISR следует использовать, если в филиале требуется использование интегрированного IPS. Все устройства, развернутые в данной архитектуре, работают в режиме анализа трафика. Благодаря этому обеспечивается возможность проверки всего трафика в сети без прерывания работы сети. После анализа нормального трафика в сети и создания политики, соответствующей требованиям компании, датчики IPS можно переключить из режима анализа трафика в режим транзитной передачи трафика и начать активную блокировку атак или трафика, не соответствующего требованиям политики. Если для компании не требуется использования интегрированных функций и используется IPS для соответствия требованиям, датчики можно использовать в режиме анализа трафика, для которого блокировка не требуется. Возможность наблюдения за операциями, выполняемыми в корпоративной сети, является большим преимуществом, особенно при принятии мер при возможных атаках, политики аудита или общем устранении неполадок. Необходимо принять во внимание значение IPS в режиме анализа трафика.

В этой архитектуре IPS развертываются в трех ключевых местоположениях в сети. Первая система IPS (SSM-20 в Cisco ASA 5510) развертывается по периметру, подключенному к Интернету. Этот датчик обеспечивает для компании возможность анализа входящего и исходящего сетевого трафика Интернета, а также удобную точку проверки трафика VPN после его расшифровки. Вторая **система** — это датчик Cisco IPS серии 4200, подключенный к сети уровня ядра, который используется для анализа трафика, исходящего от выбранных VLAN. Этот датчик может проверять трафик, исходящий от сервера и направляемый на сервер, между беспроводной и проводной сетью, а также трафик, передаваемый между сетями LAN и WAN. Третья **система** в этой сети — это Cisco ISR в филиалах. Ранее существовала возможность централизации IPS в головном узле WAN, поскольку весь трафик должен был проходить через головной офис до перехода в другим точкам в сети. Однако сегодня часто узлы филиалов могут взаимодействовать с другими филиалами или использовать прямой доступ из Интернета к таким технологиям WAN, как MPLS.

Для настройки модуля IPS используется сценарий первоначальной настройки, который необходимо запустить на IPS.

В этом примере выполняется настройка модуля IPS в ASA. Чтобы начать, подключитесь к ASA и откройте сеанс на модуле IPS SSM:

```
ASA5510# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character
sequence is 'CTRL-^X'.
```

Имя пользователя и пароль по умолчанию для IPS — "cisco" и "cisco". После этого этапа все действия по настройке идентичны для всех датчиков Cisco IPS:

```
login: cisco
Password:
Last login: Tue Dec 9 12:28:24 on pts/1
```

```
***NOTICE***
This product contains cryptographic
features and is subject to United States
and local country laws governing import,
export, transfer, and use. Delivery of
Cisco cryptographic products does not imply
third-party authority to import, export,
distribute, or use encryption. Importers,
exporters, distributors, and users are
responsible for compliance with U.S. and
local country laws. By using this product
you agree to comply with applicable laws
and regulations. If you are unable to comply
with U.S. and local laws, return this product
immediately. A summary of U.S. laws governing
Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/
stqrg.html

If you require further assistance,
please contact us by sending email to
export@cisco.com.

 --- Basic Setup ---
 --- System Configuration Dialog ---

At any poin,t you may enter a question mark
'?' for help.

User ctrl-c to abort configuration dialog at
any prompt.

Default settings are in square brackets '[]'.

Current time: Tue Dec 9 11:52:58 2008

Setup Configuration last modified: Tue Dec 09
12:29:33 2008
```

Укажите имя хоста, IP-адрес внешнего интерфейса управления и сети, для которых модуль IPS доступен:

```
Enter host name[sensor]: IPSSSM20B
Enter IP interfa
ce[192.168.1.2/24,192.168.1.1]:
192.168.1.57/24,192.168.1.1

Modify current access list?[no]: yes

Current access list entries:
 No entries
Permit: 192.168.0.0/16
Permit:
Modify system clock settings?[no]:
```

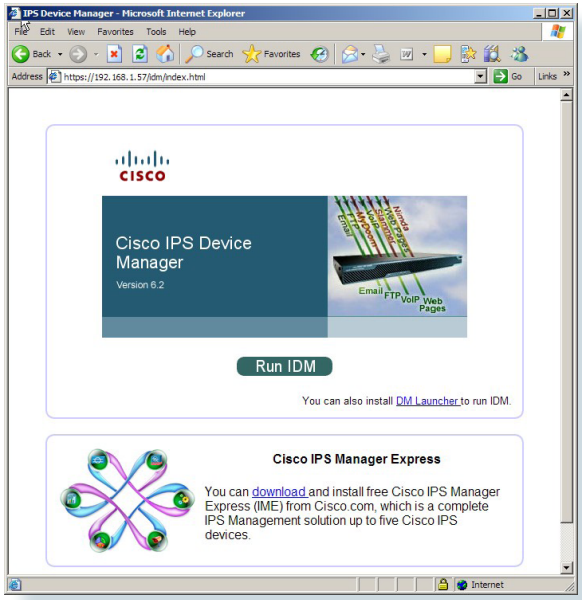
Была указана следующая настройка:

```
service host
network-settings
host-ip 192.168.1.57/24,192.168.1.1
host-name IPSSSM20B
telnet-option disabled
access-list 192.168.0.0/16
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit

[0] Go to the command prompt without saving
this config.
[1] Return to setup without saving this
config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```

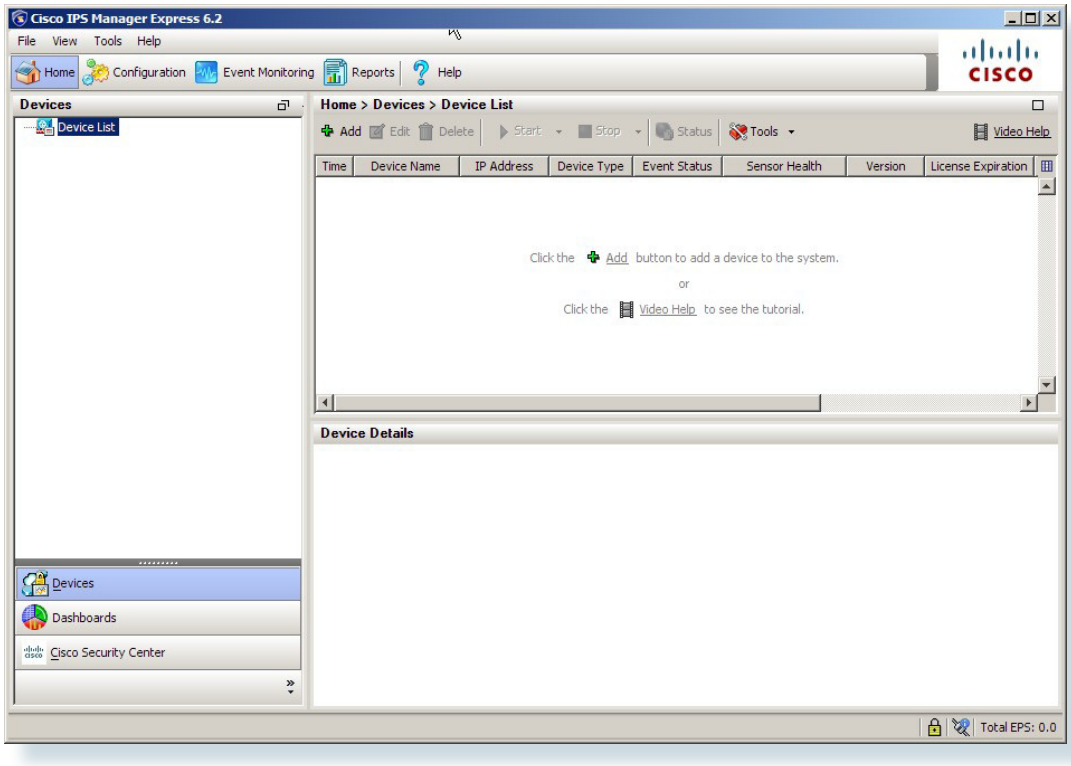
После этого сохраните настройку. На этом этапе не требуется переходить к расширенной настройке.

```
Enter your selection[3]: 2
--- Configuration Saved ---
Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at
https://<sensor-ip-address>. sensor# exit

Remote card closed command session. Press any
key to continue.

Command session with slot 1 terminated.
ASA5510#
```

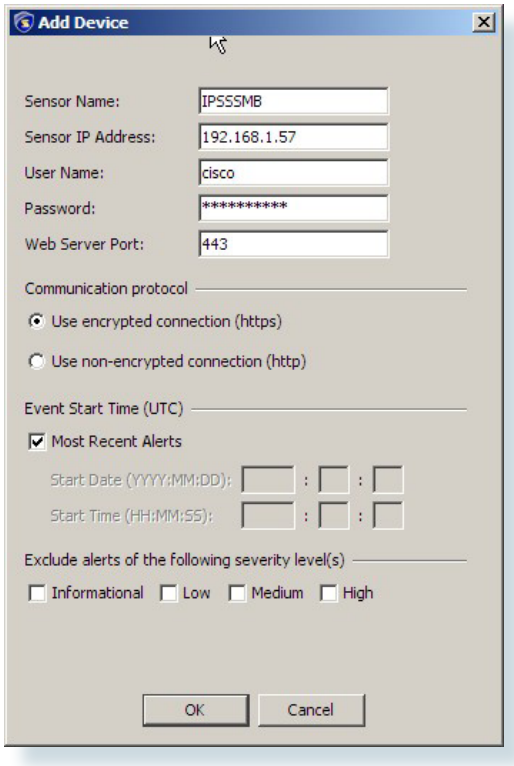
Теперь блок IPS доступен при использовании интерфейса управления, и для настройки остальных параметров можно использовать графический интерфейс.
Чтобы получить доступ к датчику, подключитесь к HTTPS://192.168.1.57. При первоначальном обращении должен отображаться следующий экран:



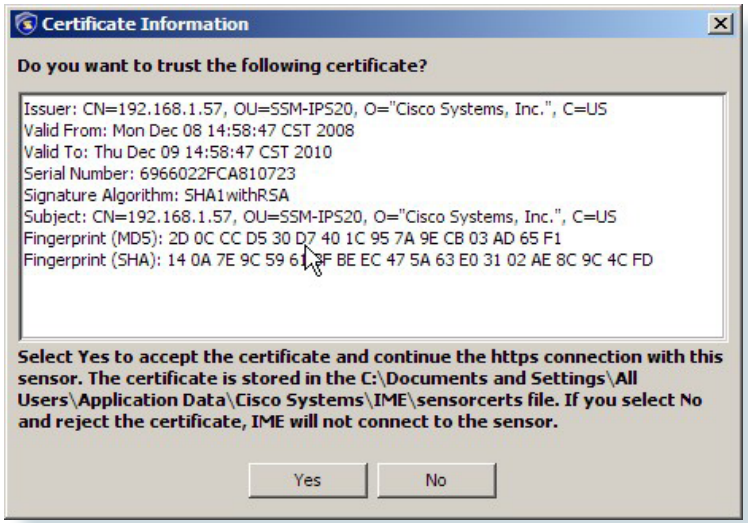
Поскольку в этой сети выполняется настройка нескольких датчиков, следует использовать Cisco IME (IPS Manager Express). При этом обеспечивается возможность управления до 5 датчиками IPS и наблюдения за ними из одного приложения. Чтобы загрузить IME, нажмите на ссылку на начальной web-странице IPS и выполните установку на локальном компьютере. Затем запустите IME, после чего должна отобразиться начальная домашняя страница IME. Чтобы добавить датчик, нажмите кнопку [add] под устройствами.



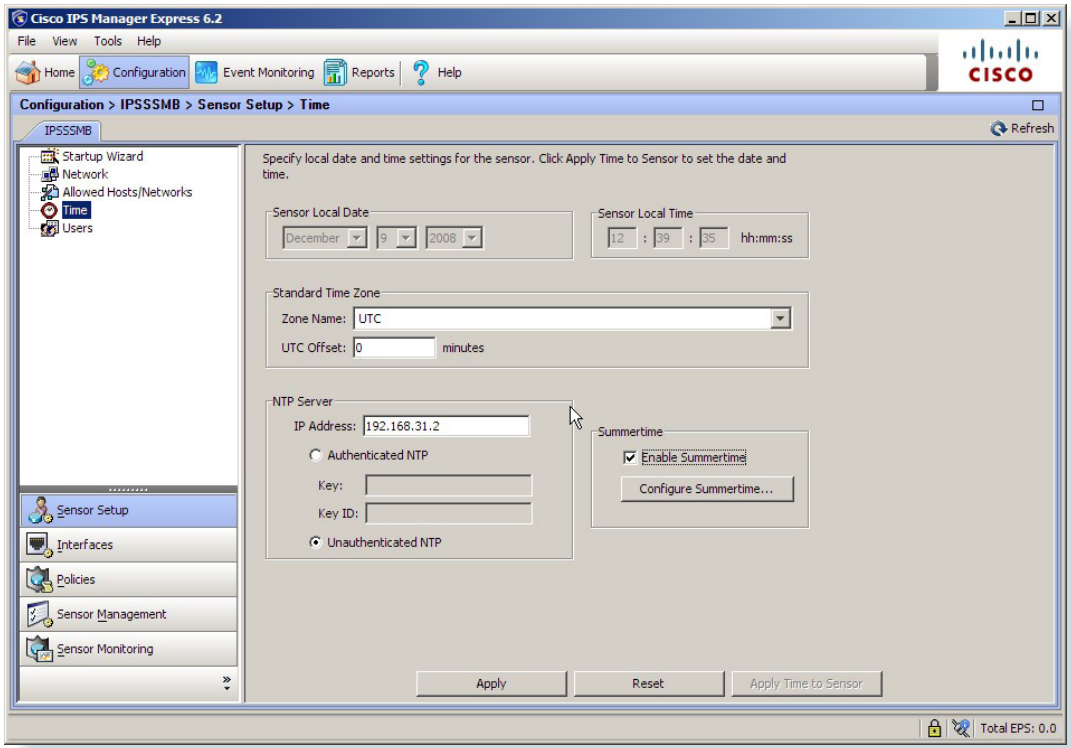
На этом этапе для добавления датчика необходимо ввести имя датчика, IP-адрес, имя пользователя и пароль. Чтобы диспетчер IME мог добавить датчик, он должен быть запущен на компьютере, IP-адрес которого входит в список разрешенных адресов в сети, настроенных для датчика при первоначальной настройке.



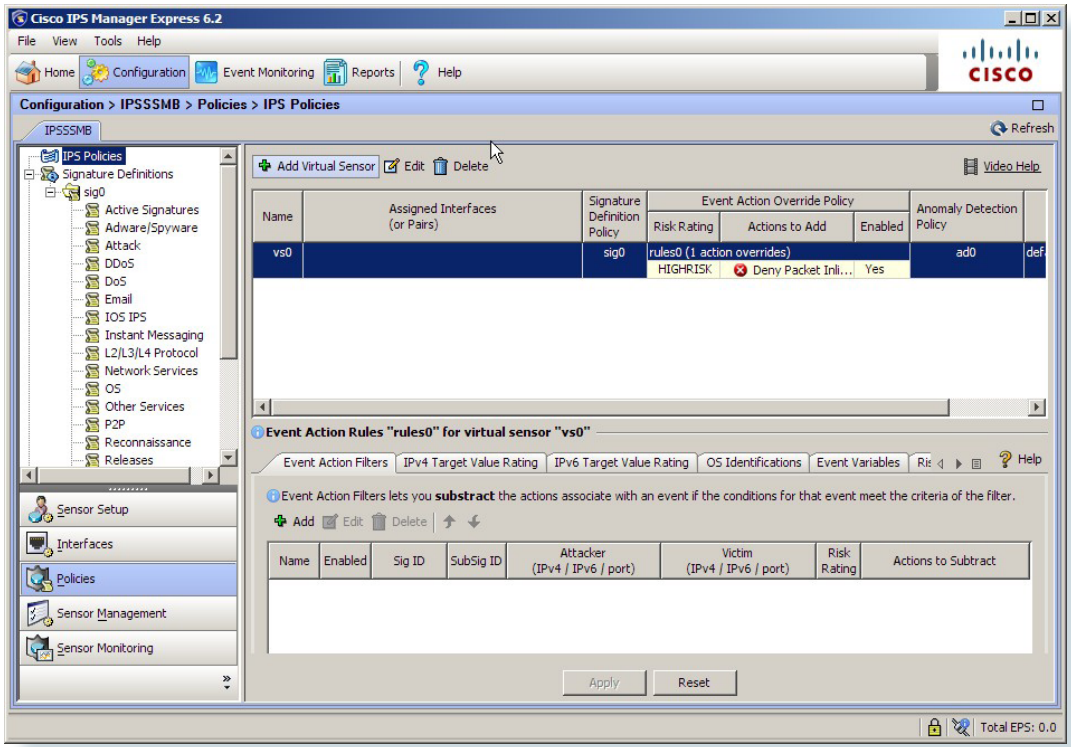
Должно быть получено сообщение с запросом на подтверждение использования клиентского сертификата от датчика. Ознакомьтесь с данными сертификата и убедитесь, что они совпадают с данными, введенными при настройке. Если данные совпадают, нажмите **[yes].**



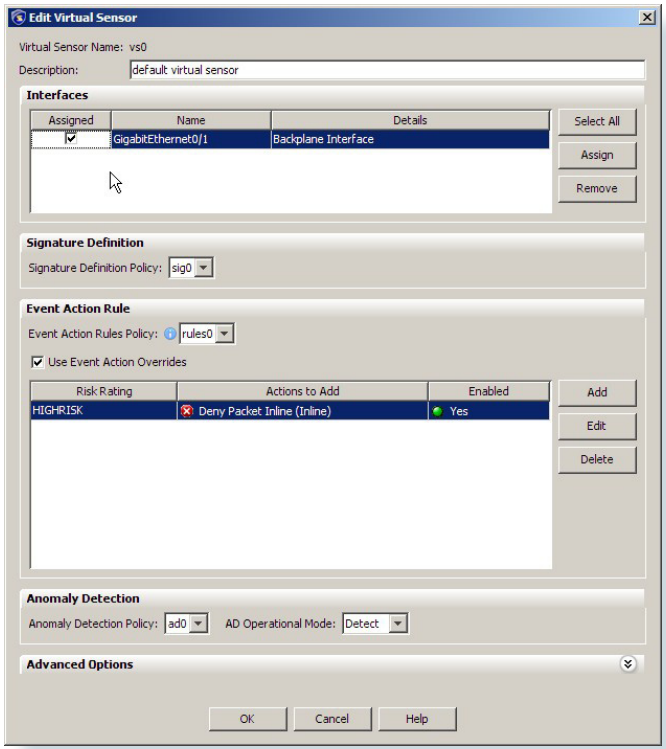
Нажмите **[Настройка]** и **[Время]** и введите IP-адрес сервера NTP. Синхронизация времени имеет первостепенное значение при работе с IPS, поскольку она позволяет точно определить время возникновения события и сравнить его с другими датчиками в сети для наилучшего устранения неполадок и управления системой.



Чтобы получить политику по умолчанию, связанную с интерфейсом, нажмите "Политики", а затем измените настройки существующего виртуального датчика.



В этом случае у модуля IPS в устройстве Cisco ASA имеется только один интерфейс. Выберите его и нажмите **[OK]** и **[Применить]**.



На этом завершается базовая настройка датчика. Следует отметить, что для всех датчиков Cisco IPS используется одно и то же программное обеспечение, следовательно, установка всегда одинакова, за исключением количества и типов интерфейсов, которые связаны с виртуальным датчиком.

Ниже приведены инструкции для определенных моделей по отправке сетевого трафика датчикам для проверки.

Настройка IPS SSM

Это базовая политика, которая используется для проверки соответствия и проверки всех данных, для передачи и приема которых используется ASA в соответствии с правилами доступа. Текущим режимом является режим анализа трафика, что указывает на то, что IPS будет выполнять только проверку без операций сбрасывания.

```
access-list inside_mpc extended permit ip
192.168.0.0 255.255.0.0 any

access-list outside_mpc extended permit ip
any 192.168.0.0 255.255.0.0

class-map inside-class
 match access-list inside_mpc
class-map outside-class
 match access-list outside_mpc

policy-map IDS-Inside
 class inside-class
ips promiscuous fail-open sensor vs0
policy-map IDS-Outside
class outside-class
ips promiscuous fail-open sensor vs0

service-policy IDS-Inside interface inside
service-policy IDS-Outside interface outside
```

Настройка IPS AIM в филиалах

В ISR Cisco 2811 поддерживается AIM-IPS с простой настройкой. Модули AIM не поддерживаются в ISR 2911 или в семействе маршрутизаторов Cisco ISR G2. Модуль следует настраивать следующим образом: настроить интерфейс IDS-датчик как непронумерованный интерфейс, связанный с физическим интерфейсом или интерфейсом замыкания в ISR. Затем следует настроить модуль IPS для использования IP-адреса из той же подсети, что и назначенный для нее интерфейс. В этом примере для модуля устанавливается отказоустойчивый режим, позволяющий отключать модуль без простоев сети.

```
interface IDS-Sensor0/0
 ip unnumbered Loopback0
 service-module fail-open
 hold-queue 60 out
```

Чтобы подключиться к модулю IPS AIM в маршрутизаторе, введите следующую команду:

```
service-module ids-Sensor 0/0 session
```

Для поддержки управления доступом для маршрутизатора необходим маршрут к интерфейсу IDS, что укажет ему точку для отправки трафика. Ниже описан оператор для маршрута:

```
ip route 192.168.1.66 255.255.255.255 IDS-
Sensor0/0
```

Эту команду необходимо применить ко всем интерфейсам, где необходима проверка трафика. В большинстве случаев проверка трафика применяется в точке подключения интерфейса Ethernet и локальной сети. Также в этих случаях выбирается необходимый режим анализа трафика или режим транзитной передачи трафика. Для первоначального развертывания рекомендуется выбрать режим анализа трафика.

```
ids-service-module monitoring promiscuous
access-list 199
```

В приведенном ниже списке доступа отклоняется весь трафик. Трафик, разрешенный списком ACL на IPS, проходит IPS, при этом трафик, отклоняемый IPS ACL, отправляется на модуль IPS для проверки. В представленном ниже примере списка ACL весь трафик направляется для проверки:

```
access-list 199 deny ip any any
```

Если следует отказаться от проверки трафика HTTPS, список ACL должен выглядеть следующим образом:

```
access-list 199 permit tcp any any eq 443
access-list 199 deny ip any any
```

Настройка локальной сети IPS 4200

IPS 4200 подключается к порту гигабитного Ethernet 1/0/9, и сеанс наблюдения отправляет весь трафик от сетей VLAN 1-31 на интерфейс для проверки.

```
monitor session 1 source vlan 1 - 31
monitor session 1 destination interface
Gi1/0/9
```

VPN с возможностью удаленного доступа

Обзор технологий

Устройство Cisco ASA поддерживает IPsec, web-портал и SSL VPN с полным туннелированием для удаленного доступа клиентов и IPsec для аппаратных клиентов и VPN "сеть-сеть". В этом разделе описывается базовая настройка IPsec удаленного доступа, web-портала и VPN по SSL для базового удаленного доступа, а также настройка Cisco EZVPN для доступа аппаратного клиента (ASA 5505).

Для мобильных работников и пользователей, которым иногда требуется удаленное подключение, рекомендуется использовать такие программные клиенты, как Cisco VPN и Cisco AnyConnect. Для использования IPsec VPN у пользователя уже должно быть загружено и настроено программное обеспечение на компьютере для подключения и оптимальной работы с корпоративными компьютерами, такими как ноутбуки. Для доступа VPN по SSL можно использовать web-браузеры для доступа через порталы или Cisco AnyConnect в качестве клиента. Доступ по SSL обладает более высоким уровнем гибкости и используется из большего количества местоположений, чем IPsec, поскольку только некоторые компании блокируют доступ по HTTPS из своих сетей. При использовании SSL может обеспечиваться ограниченный уровень обслуживания при подключении пользователя с неизвестных компьютеров, обеспечивая более высокий уровень безопасности для корпоративной сети.

Аппаратный клиент представляет собой физическое устройство, похожее на небольшой прибор или маршрутизатор, которое обеспечивает "постоянное" обратное подключение к корпоративной сети. Обычно они используются в ситуациях, в которых пользователь подключается регулярно и использует подключение в течение длительного периода времени со статического местоположения, например, домашнего офиса.

Сведения о настройке

Настройка VPN удаленного доступа

Устройство ASA было настроено для удаленного доступа к VPN путем добавления базовой настройки к настройке устройства по умолчанию. Аутентификация пользователей выполняется на локальном контроллере домена Windows.

```
group-policy DfltGrpPolicy attributes
 dns-server value 192.168.28.10
 vpn-tunnel-protocol IPSec svc webvpn
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_
SplitTunnelACL
 address-pools value VPN-Pool
```

Этот список доступа разделенного туннелирования направляет весь трафик с адресом назначения 192.168.0.0/16 во внутреннюю сеть.

```
access-list RA_SplitTunnelACL standard permit
192.168.0.0 255.255.0.0
```

Клиентам с удаленным доступом адрес назначается из пула VPN.

```
ip local pool VPN-Pool 192.168.30.129-
192.168.30.254 mask 255.255.255.128

tunnel-group DefaultRAGroup general-
attributes
address-pool VPN-Pool
```

Web-клиенты и клиенты VPN по IPsec проходят аутентификацию на сервере AAA с именем “AD”. Если сервер недоступен, ASA возвращается к локальной аутентификации.

```
 authentication-server-group AD LOCAL
tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key [password]
tunnel-group DefaultWEBVPNGroup general-
attributes

address-pool VPN-Pool
 authentication-server-group AD LOCAL
```

Ниже описана настройка сервера AAA с именем AD. Устройство ASA поддерживает несколько собственных протоколов аутентификации и не требует промежуточного сервера RADIUS для аутентификации пользователей с использованием таких протоколов, как LDAP, домен NT, Kerberos и т.д.:

```
aaa-server AD protocol nt
aaa-server AD (inside) host 192.168.28.10
 nt-auth-domain-controller 192.168.28.10
```

Последняя часть настройки особенно важна в ситуации, когда внутренние адреса становятся доступны извне с помощью функции NAT. Настройка, описанная ниже, предотвращает преобразование возвращаемого трафика клиентов VPN через NAT и потери этого трафика при отправке обратно из корпоративной сети. В межсетевом экране создается правило исключения NAT 0 или NAT для исходящего трафика, которое запрещает трансляцию исходящего трафика, если адрес назначения принадлежит пулу VPN-Pool Это одна из наиболее распространенных ошибок; если не устранить ее, то в результате клиент VPN будет подключен, но не сможет передавать трафик.

```
access-list inside_nat0_outbound
extended permit ip 192.168.0.0 255.255.0.0
192.168.30.128 255.255.255.128
```

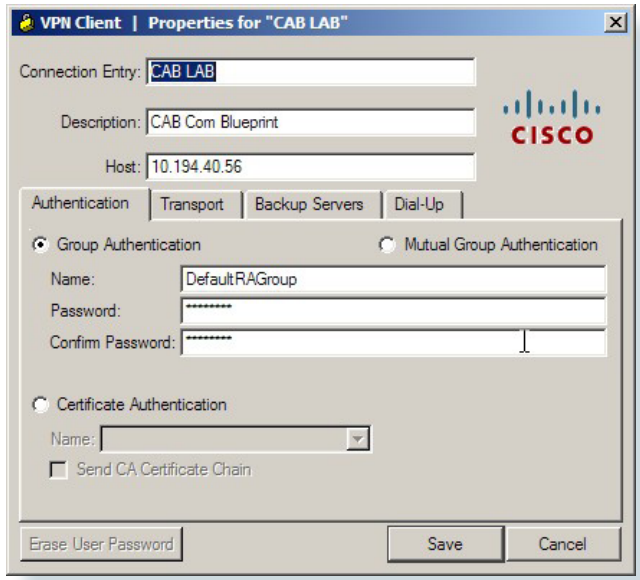
Если используется web-портал, важно включить следующую команду:

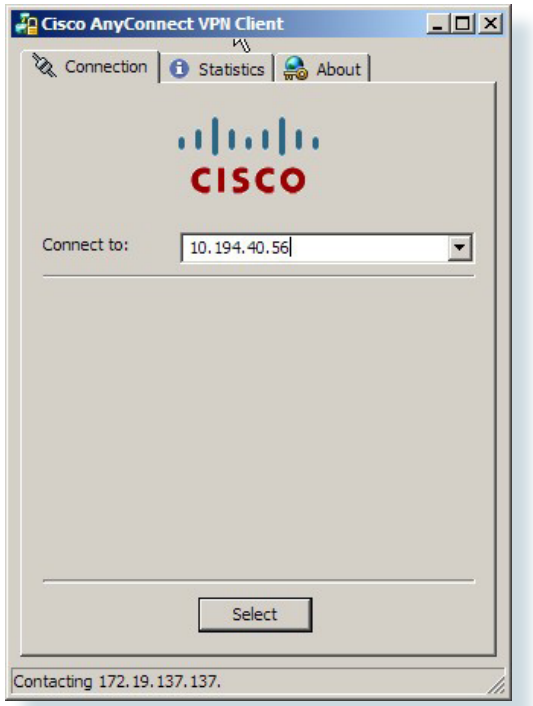
```
http redirect outside 80
```

При этом весь доступ к внешнему интерфейсу для порта 80 (HTTP) будет перенаправлен на порт 443 (HTTPS). Кроме того, для пользователей будет устранена необходимость вводить HTTPS://ssl.company.com для получения доступа к порталу.

Настройка программного клиента VPN

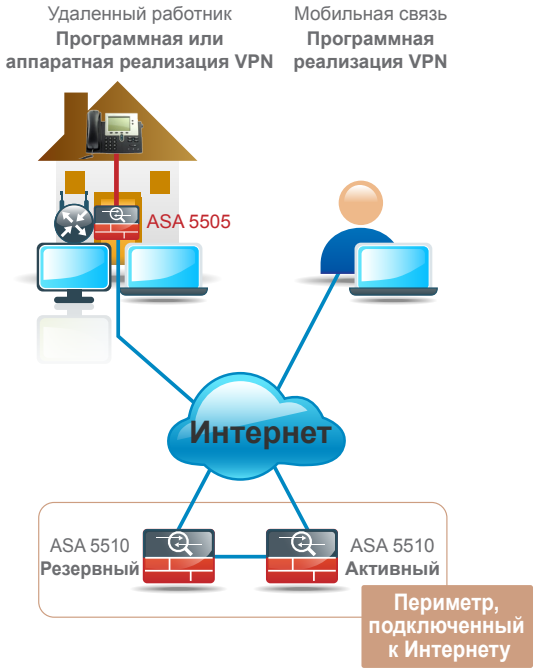
На стороне клиента для IPsec пользователю необходим IP-адрес или доменное имя головного устройства, имя группы и пароль, а также имя пользователя и пароль. Для доступа VPN по SSL пользователю необходим IP-адрес или доменное имя головного устройства, а также имя пользователя и пароль.





Настройка аппаратного клиента VPN

Устройство ASA поддерживает различные типы маршрутизаторов в виде удаленных аппаратных клиентов VPN, а также ASA 5505. В этом примере для удаленного оборудования клиента используется ASA 5505.



Настройка головного устройства VPN

Настройка головного устройства ASA 5510.

Тип шифрования IPsec устанавливается как AES-128 и SHA-1. Устройство ASA поддерживает большое количество наборов преобразований, включая DES, 3DES, AES 128-256 и алгоритмы MD5 и SHA. В примере используется AES-128, поскольку благодаря этому устройству достигается оптимальный баланс безопасности и производительности.

```
crypto ipsec transform-set 5505SET esp-aes esp-sha-hmac
```

Свяжите динамическое криптографическое сопоставление 5505 с алгоритмом шифрования 5505SET:

```
crypto dynamic-map 5505DYN-MAP 5 set transform-set 5505SET
```

Определите срок годности в секундах и байтах, чтобы подключение выполнило повторный ввод для туннелей IPsec после указанного периода.

```
crypto dynamic-map 5505DYN-MAP 5 set security-association lifetime
seconds 28800

crypto dynamic-map 5505DYN-MAP 5 set security-association lifetime
kilobytes 4608000
```

При этом настраивается головное устройство для передачи сведений о маршруте корпоративной сети, благодаря чему обеспечивается доступность удаленной сети.

```
crypto dynamic-map 5505DYN-MAP 5 set reverse-route
```

При этом криптографическое сопоставление связывается с внешним интерфейсом, где выполняется подключение удаленных устройств ASA 5505.

```
crypto map 5505MAP 60 ipsec-isakmp dynamic 5505DYN-MAP
crypto map 5505MAP interface outside

group-policy 5505Group internal

group-policy 5505Group attributes
 vpn-tunnel-protocol IPSec
 ip-comp enable
 split-tunnel-policy tunnelspecified
```

Используется та же политика раздельного туннелирования из настройки удаленного доступа к клиенту.

```
 split-tunnel-network-list value RA_SplitTunnelACL
 user-authentication-idle-timeout 480
 nem enable

username 5505site1 password [password]
username 5505site1 attributes
 vpn-group-policy 5505Group

tunnel-group RA5505 type remote-access
tunnel-group RA5505 general-attributes
 default-group-policy 5505Group
tunnel-group RA5505 ipsec-attributes
 pre-shared-key [password]
```

Это правило NAT 0 или NAT предотвращает преобразование трафика, возвращаемого в удаленную VPN.

```
nat (inside) 0 access-list inside_nat0_outbound
access-list inside_nat0_outbound extended permit ip 192.168.0.0
255.255.0.0 192.168.192.0 255.255.255.0
```

Удаленная настройка VPN

Ниже приведена настройка для удаленного ASA 5505.

Пароль PSK и пароль клиента vpn bp группы vpn должны совпадать.

```
vpnclient server 10.194.40.56
vpnclient mode network-extension-mode
vpnclient nem-st-autoconnect
vpnclient vpngroup RA5505 password [password]
vpnclient username 5505site1 password [password]
vpnclient enable
```

Модуль "Унифицированные коммуникации"

Обзор технологий

Развертывание унифицированных коммуникаций в значительной степени упрощается за счет использования продуктов и настроек в других модулях. Например, коммутаторы доступа обеспечивают передачу питания по Ethernet (PoE) для развертывания телефонов без необходимости в локальной электрической розетке. Во всей сети предварительно настроено обеспечение качества обслуживания (QoS) для поддержки трафика передачи высокого качества голоса и видео. Маршрутизатор в головном офисе в сети WAN поддерживает шлюз в телефонную сеть общего пользования, а также режим моста для конференц-связи путем добавления модулей цифровой обработки сигналов (DSP) для пакетной голосовой связи (PVDM) и интерфейсной платы, соответствующей требованиям к подключению ТфОП. Чаще всего в главном офисе размещается линия (интерфейс) T1/E1 PRI. Помимо других аппаратных модулей, добавленных к маршрутизатору, в код IOS необходимо включить набор функций “Голос”.

Помимо проводной сети, беспроводная сеть также предварительно настроена для использования беспроводных устройств унифицированных коммуникаций, обеспечивая поддержку IP-телефонии для 802.11 Wi-Fi (которая упоминается как "мобильная связь") не только в головном офисе, но и в филиалах. Модуль безопасности и мобильной связи также подготовлен к предоставлению сервисов программных телефонов, а также стандартных телефонов. Эти телефоны можно подключить к Cisco ASA 5505, благодаря чему обеспечивается PoE на двух портах и возможность обратного подключения к Cisco ASA 5510 в головном офисе. HQ Cisco ASA 5510 также поддерживает прокси для телефонной связи, хотя это и не является частью базовой настройки. Благодаря этому обеспечивается возможность развертывания телефонов через Интернет в домашних офисах без реализации VPN через оборудование Cisco ASA 5505. При построении этой платформы были добавлены три устройства для обеспечения диспетчера коммуникаций с высоким уровнем доступности и масштабирования, а также системы голосовой почты, поддерживающей интеграцию клиента электронной почты.

Cisco Unified Communications Manager (Unified CM) был выбран для обеспечения функций АТС для всех пользователей в головном офисе, а также в филиалах. При использовании двух Cisco MCS 7835 для платформы и подключении каждого устройства к различным коммутаторам в ферме серверов предоставляется более высокий уровень доступности, обеспечиваемый специально на случай сбоя в работе коммутатора или платформы MCS. Cisco MCS 7835 представляет собой наилучший выбор, поскольку обеспечивает оптимальный баланс между гибкостью для предоставления сервисов в будущем и затратами. Эта платформа обеспечивает необходимые функции для использования нескольких устройств для каждого пользователя. Например, для большого процента пользователей можно разрешить на настольных телефонах и программных телефонах с достаточным уровнем интеграции компьютерной телефонии (CTI) использование вызова одним нажатием или других приложений, которые можно использовать для удаленного управления телефонами.

Для телефонов, которые не назначены определенным пользователям, т.е. для телефонов в местах общего пользования, конференц-залах, складах и комнатах отдыха, доступны дополнительные функции. Помимо встроенных функций, платформу можно расширить для поддержки других сервисов, включая определение присутствия и мгновенного обмена сообщениями, расширенные функции конференц-связи и совещаний, а также центр контактов и поддержку видеоконференций. К оборудованию платформы относятся массивы RAID и дублированные источники питания, которые позволяют обеспечить более высокий уровень доступности. В филиалах маршрутизатор на основе ISR также поддерживает функцию предоставления сервисов телефонии при неисправности WAN или потери связи с головным офисом. Survivable Remote Site Telephony (SRST) настраивается на маршрутизаторе и автоматически выполняет переключение в случае сбоя в работе.

Голосовая почта считается частью фундамента системы унифицированных коммуникаций и обеспечивается при развертывании Cisco Unity Connection на платформе Cisco MCS 7835, предоставляя всем 1000 пользователям доступность ящика голосовой почты на телефоне или путем интеграции в клиент электронной почты. Unity Connection развертывается как простая система голосовой почты. Однако при дополнительной настройке всего нескольких параметров этого многофункционального приложения обеспечивается интеграция обработки звонков на основе календаря с Microsoft Exchange, Cisco MeetingPlace® Express и других сетевых систем голосовой почты.

Unity Connection развертывается в архитектуре без функций резервирования, хотя при необходимости можно включить поддержку функций резервирования. Настройка Unity Connection описывается в разделе, посвященном методу быстрого развертывания с использованием канала, описанного в конце этого раздела.

Унифицированные IP-телефоны Cisco

Выбор модели телефона зависит от требований пользователя, среды и стоимости. Для поддержки услуг телефонии и передачи видео необходимы телефоны моделей не ниже Cisco 7942G или Cisco 7962G, при этом Cisco 7945G и Cisco 7965G имеют цветные экраны высокого разрешения с подсветкой и поддерживают функции Gigabit Ethernet. Телефоны Cisco 7931G и Cisco 7911G обеспечивают меньший объем функций, и, следовательно, менее дорогостоящи. Радиотелефоны 7921 и 7925 используются в мобильных решениях, а оборудование 7937 для конференц-зала и клиентское ПО IP Communicator являются решением на базе настольного ПК. Здесь представлены не все возможные варианты телефонов для развертывания, однако одни из самых рекомендуемых.

Независимо от выбора модели телефона в качестве протокола сигнализации выбирается протокол SCCP, поскольку он также обеспечивает передачу видео и модули расширения. В проводных телефонах используется протокол CDP для получения голосовой VLAN, настроенной на коммутаторе доступа, а затем протокол DHCP используется для получения следующих данных: IP-адреса, маски подсети, шлюза по умолчанию, имени домена и Option 150. Благодаря этому обеспечивается два IP-адреса Unified CM, и при этом для телефонов обеспечивается поддержка загрузки файлов настройки и микропрограмм. Option 150 добавляется в голосовые области DHCP. Предпочтительным вариантом является Unified CM по схеме "Издатель", а резервным — по схеме "Подписчик".

В следующей настройке обеспечивается DHCP для одной из голосовых подсетей, где 192.168.28.20 является IP-адресом "Издателя", а 192.168.28.21 — IP-адресом “Подписчика” Unified CM:

```
ip dhcp pool voice
 network 192.168.12.0 255.255.255.0
 default-router 192.168.12.1
 dns-server 192.168.28.10
 option 150 ip 192.168.28.20 192.168.28.21
 domain-name cisco.com
```

На уровне доступа будет автоматически выполнено согласование PoE для телефона и уровня доверия для классификаций QoS, использованных в различных сеансах, включая сигнализацию, носители и другие сервисы.

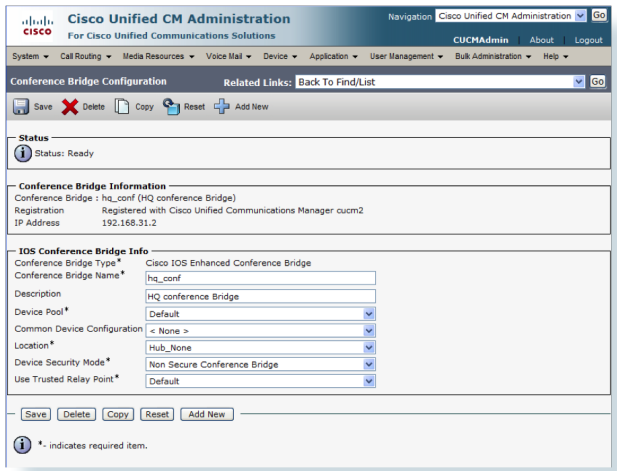
Cisco Unified Communications Manager

Первое установленное устройство унифицированных коммуникаций называется "Издателем", поскольку в нем содержится главная база данных, на которую будут подписываться все другие диспетчеры унифицированных коммуникаций в одном кластере, и эти диспетчеры будут называться подписчиками. После установки диспетчера унифицированных коммуникаций и включения необходимых сервисов, можно будет начинать настройку. Ниже приведены основные рекомендации по упрощению развертывания унифицированных коммуникаций

Мультимедийные ресурсы

Все мультимедийные ресурсы, такие как коммутатор для конференц-связи, "Сигнализатор" (система голосовых сообщений) и музыка при переходе в режим удержания (MoH) необходимо настроить в соответствии с требованиями конкретного офиса. Они должны быть назначены группам мультимедийных ресурсов, а затем спискам мультимедийных ресурсов, назначаемые затем устройствам, таким как телефоны и шлюзы, которые используются при необходимости. При этой схеме развертывания, коммутаторы для конференц-связи развертывались в каждом офисе для минимизации использования полосы пропускания по WAN для вызовов с большим количеством участников (более двух). Сервисы "Сигнализатор" и MoH расположены в центре системы и по умолчанию используют отдельные носители. Также можно использовать Multicast MoH и выполнить централизованное развертывание или использовать маршрутизаторы в филиалах. Однако этот подход не описывается в базовом курсе по построению системы унифицированных коммуникаций.

Ниже приведен пример настройки коммутатора для конференц-связи для унифицированных коммуникаций.



Настройка маршрутизатора головного офиса для унифицированных коммуникаций

Ниже описана настройка для маршрутизатора головного офиса, регистрирующего 10 ресурсов коммутаторов конференц-связи с высоким приоритетом подписчика и низким приоритетом издателя.

```
voice-card 0
 dsp services dspfarm

voice-port 0/0/1:23
ccm-manager sccp local Port-channel1
sccp local Port-channel1.31
sccp ccm 192.168.28.21 identifier 2 priority
1 version 7.0
sccp ccm 192.168.28.20 identifier 1 priority
2 version 7.0
sccp

sccp ccm group 1
 bind interface Port-channel1.31
 associate ccm 2 priority 1
 associate ccm 1 priority 2
 associate profile 1 register hq_conf
 switchback method graceful
 switchback interval 60

dspfarm profile 1 conference
 description HQ Conference Bridges
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 codec g722-64
 codec ilbc
 maximum sessions 10
 associate application SCCP
```

После выполнения определенной первоначальной настройки унифицированные коммуникации могут обеспечить автоматическую настройку многих параметров устройств при перемещении между узлами, а также обеспечивают более быстрый и стабильный механизм развертывания для статических устройств. В основе этого метода развертывания лежит функция, которая называется мобильность устройств. Этот метод работает в унифицированных коммуникациях при использовании IP-адреса устройства для применения профиля; при этом выполняется настройка динамического назначения плана нумерации в зависимости от узла, группы мультимедийных ресурсов, управления кодеками (регионы) и управления принятием вызовов (местоположения). При этом уменьшается количество параметров, требуемых для настройки устройства при его добавлении к системе, а также обеспечивается применение к устройству правильных параметров, зависящих от местоположения, поскольку неверная их настройка недопустима. При отправке устройства в неправильное местоположение оно будет динамически настроено с применением параметров, соответствующих местоположению устройства.

При объединении мобильности устройств с мобильностью добавочных номеров можно использовать подход, при котором телефоны будут поставляться

напрямую в офисы, после чего пользователю останется только начать использовать правильно выбранную модель телефона. Затем пользователь подключается к системе, и после выполнения аутентификации для телефона в унифицированных коммуникациях применяется заранее настроенный профиль пользователя. В качестве альтернативы можно отдельно настроить все устройства пользователей и гарантировать отправку правильно выбранных телефонов не только в соответствующий офис, но и непосредственно на рабочий стол пользователя. Использование одних и тех же функций мобильности устройств и добавочных номеров позволяет упростить процедуру замены телефона. При подключении нового телефона он автоматически получает настройку, соответствующую данному офису и выбираемую на основе IP-адреса. При подключении пользователя применяется настройка, соответствующая этому пользователю. При этом старый телефон просто отключается и возвращается. Мобильность устройств упрощает работу с беспроводными и программными клиентами, часто перемещающимися с одной точки в другую, обеспечивая автоматическое назначение ресурсов, регионов и местоположений.

План нумерации

Назначение плана нумерации заключается в предоставлении для пользователей простого метода набора номеров друг друга в пределах одного местоположения, нескольких местоположений и на PSTN. Также существуют определенные ограничения на местоположения, в которых может требоваться вызов пользователей, и эти ограничения реализованы как класс ограничений (CoR). Чтобы достичь этого, используются различные методы, при сочетании которых обеспечивается структурная основа, которая может быть настроена и расширена другими приложениями.

План нумерации с фиксированной длиной

Телефонные номера, назначаемые линиям, имеют одну длину и состоят из цифры 8, кода местоположения (2 цифры) и добавочного номера (4 цифры). Затем для номера в телефоне применяется маска с помощью “метки текста”, что позволяет указывать только добавочный номер из 4 цифр и имя пользователя (необязательно). Настройка маски внешнего номера телефона обеспечивает возможность прямого набора внутренних номеров (DID) и отображения ТфОП на "черной полосе" в верхней части телефона с полными дисплеями. Таким образом, пользователи в одном местоположении могут звонить друг другу, используя только добавочные номера из 4 цифр. При этом используется механизм преобразования (соответствующий данному местоположению) для преобразования номера из 4 цифр в номер, состоящий из цифры 8 + [код местоположения] + добавочный номер. Для связи между офисами пользователи будут набирать все 7 цифр: 8 + [код местоположения] + добавочный номер. Для вызовов по ТфОП они будут набирать 9 или 0, в зависимости от требований конкретной страны.

Группы локальных маршрутов

Функция группировки локальных маршрутов, реализованная в унифицированных коммуникациях версии 7.0, упрощает настройку плана набора, которая является обязательной для всех филиалов. Функция обеспечивает возможность включения в списки маршрутов групп маршрутов, динамически распределяемых с учетом местоположения устройства. До реализации этой функции необходимо наличие списка маршрутов и групп маршрутов для всех местоположений. Большая часть плана нумерации является глобальной, а для каждого офиса требуется использование только небольшой части.

Шлюзы ТфОП

В шлюзах, используемых для подключения к ТфОП, используются платформы маршрутизации, которые уже применяются для WAN в этой архитектуре. Выбор интерфейса и протокола, используемых для подключения к оператору связи ТфОП, зависят от страны, оператора и стоимости. Независимо от выбора, рекомендуется использовать протокол SIP для подключения шлюза к унифицированным коммуникациям в головном офисе и филиалах, поскольку он обеспечивает схожую настройку для обоих типов местоположений.

Для шлюзов можно использовать MGCP, но этот протокол не следует использовать при отсутствии подключения к серверам Unified CM или при сбое в работе WAN. При таких условиях обычно имеется настроенный протокол перехода на аварийный режим, такой как протокол SIP или H.323 для SRST, используемые для маршрутизации входящих и исходящих звонков по ТфОП. Для дальнейшего упрощения настройки SIP настраивается для использования Unified CM и также доступен для SRST в случае сбоя в работе WAN. Благодаря этому устраняется необходимость настройки шлюза в филиале дважды — один раз для MGCP и один раз для SIP.

Все эти методы, описанные выше, полностью задокументированы в Unified Communications SRND, где также приведены дополнительные рекомендации по развертыванию унифицированных коммуникаций.

Руководство по быстрому развертыванию UC, в котором приводится поэтапное описания развертывания унифицированных коммуникаций Cisco Unified Communications Manager и Unity, доступно на Cisco.com

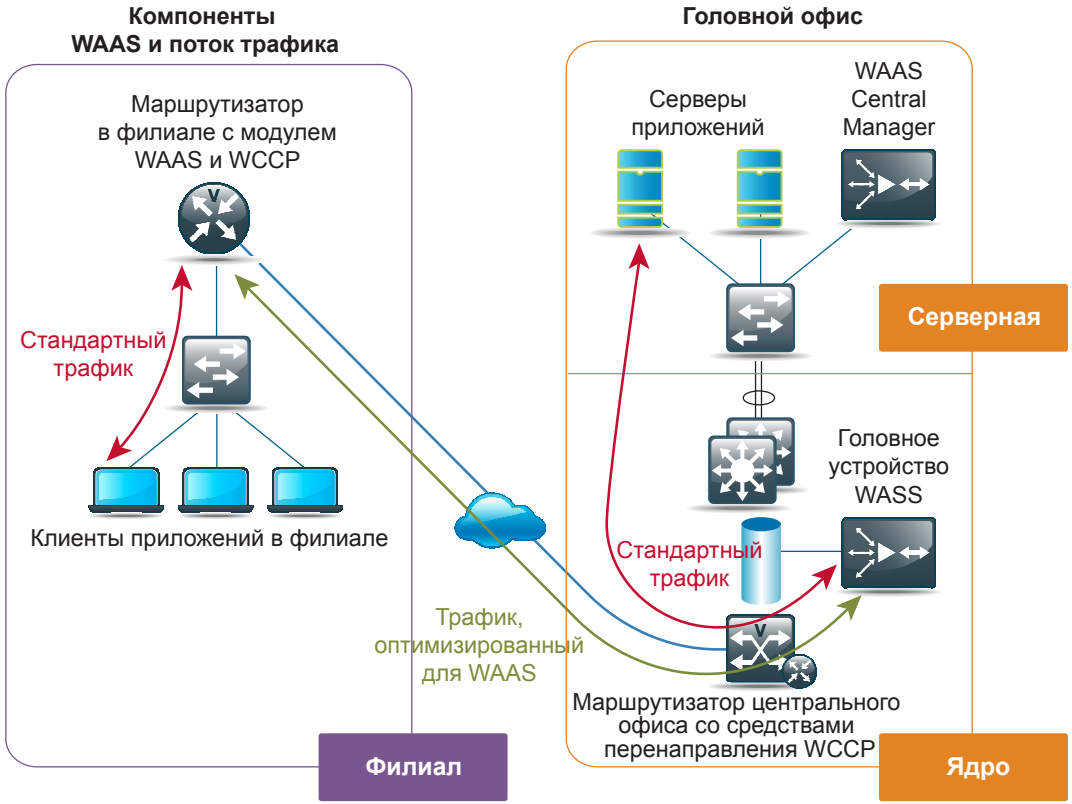
Примечания

Модуль "Режим ускорения работы приложений"

Бизнес-обзор

По мере роста организации для охвата местоположений новых филиалов возникает необходимость в новых инвестициях в развитие сети с целью предоставления пользователям в филиалах возможности доступа к бизнес-приложениям и сервисам, доступным в головном офисе. Подключения к WAN обычно обеспечиваются оператором связи за периодическую оплату предоставленной пропускной способности. Независимо от используемой технологии WAN, стоимость услуг оператора связи увеличивается по мере увеличения предоставляемой пропускной способности, поэтому организации крайне заинтересованы в эффективном использовании этого ресурса.

Для пользователей в филиалах поддержание согласованного времени ответа приложения может представлять собой проблему из-за задержек, вызванных подключениями WAN при размещении приложения в головном офисе. Дублирование ресурсов локально во всех филиалах может быть слишком дорогостоящим, поскольку для этого требуются дополнительные аппаратные и программные ресурсы, а также специалисты для управления. Технологии ускорения работы приложений Cisco обеспечивают организациям возможность повышения производительности работы пользователей без приобретения дополнительной пропускной способности или оборудования для офисов в филиалах.



Cisco Wide Area Application Services (WAAS) представляет собой комплексную систему, разработанную для ускорения и оптимизации передачи данных по сети WAN. Оптимизация использования существующей полосы пропускания часто позволяет организациям увеличивать персонал и добавлять новые приложения в филиалах без затрат на приобретение дополнительной полосы пропускания. Повышение производительности, обеспечиваемое с помощью WAAS, позволяет повысить производительность работы пользователей, позволяя при этом сохранить централизованную структуру важнейшего оборудования и процессов в головном офисе, что еще более снижает эксплуатационные расходы.

Обзор технологий

Cisco WAAS Wide-Area Virtualization Engine (WAVE) Appliances и интегрируемые в маршрутизатор сетевые модули (NME-WAE) обеспечивают необходимые варианты для развертывания в архитектуре Smart Business Architecture. WAAS использует различные технологии для сведения к минимуму передачи трафика между головным офисом и филиалами, что уменьшает потребление пропускной способности WAN.

Cisco WAAS Transport Flow Optimization (TFO) завершает сеанс TCP локально, что позволяет оптимизировать потоки, проходящие через WAN, и обеспечивает изоляцию приложений конечных пользователей от условий WAN. Постоянное использование сжатия Lempel-Ziv (LZ) позволяет сэкономить от 10 до 20 процентов пропускной способности WAN, необходимой для стандартных профилей трафика. Cisco WAAS обеспечивает дополнительную экономию пропускной способности с помощью *алгоритма DRE (исключение избыточности данных),* благодаря которому обеспечивается возможность определения повторяющихся закономерностей данных сети и устраняется необходимость повторной отправки данных по WAN. В зависимости от приложения DRE может уменьшить объем трафика, передаваемого между удаленным местоположением и головным офисом, на 40–80 процентов. Также в WAAS включены дополнительные функции *ускорения работы в зависимости от приложения,* утвержденные поставщиками популярных приложений, таких как Microsoft Outlook и файловые службы и службы печати

Windows. Комбинация технологий, включенных в Cisco WAAS, может обеспечить достаточную экономию для поддержки развертывания таких дополнительных приложений, как передача голоса и видео в существующей сети без затрат на дополнительную пропускную способность.

Cisco WAAS также обеспечивает дополнительную защиту данных путем поддержки централизации ресурсов приложения в головном офисе. После этого появляется возможность применения необходимых процедур защиты данных во всех организациях путем устранения необходимости в создании резервных копий и архивов в филиалах по отдельности. WAAS обеспечивает для конечных пользователей в филиалах возможность добиться такого же уровня производительности, что и у пользователей в головном офисе при централизованном доступе к приложениям. Отличительные характеристики Cisco WAAS:

- оптимизация пропускной способности и предоставления приложений в филиалах с такой же скоростью, как в сетях LAN, позволяя повысить производительность работы пользователей;
- повышение эффективности WAN и снижение необходимости в увеличении пропускной способности;
- централизация важнейших приложений и хранения данных в головном офисе;
- снижение требований к рабочему пространству и питанию, необходимых в каждом филиале.

Для этого развертывания в головном офисе используется устройство WAVE-574, что позволяет оптимизировать WAN как центральную точку подключения для филиалов. Отдельный Central Manager WAVE-274 используется как точка управления, наблюдения и отчетности для решения WAAS. В филиалах используются модули NME-WAE, которые интегрируются напрямую в маршрутизаторы Cisco ISR.

Сведения о настройке

Описанные ниже действия позволяют получить общее представление о задачах, которые необходимо выполнить для настройки базовой среды WAAS.

Шаг 1. Настройте функцию Central Manager на устройстве WAVE в головном офисе. В данном примере архитектуры используется устройство Cisco WAVE-274 для обеспечения функций управления и наблюдения.

Шаг 2. Используйте Setup Utility на головном устройстве WAVE в головном офисе для настройки базовых параметров и регистрации устройства в Central Manager. В данном примере Cisco WAVE-574 используется для обеспечения более совершенных функций обработки для головного узла сети WAAS.

Шаг 3. Аналогично использованию головного устройства WAVE используйте Setup Utility для модулей NME-WAE в офисе филиала для базовой настройки и регистрации в Central Manager. Первоначально доступ к командной строке должен осуществляться с помощью маршрутизатора ISR офиса филиала.

Шаг 4. Настройте протокол WCCP для маршрутизатора WAN в головном офисе и всех маршрутизаторов для сети WAN филиала. WCCP позволяет маршрутизаторам перенаправлять трафик, направляемый WAN, на первое локальное транзитное устройство, где он может быть оптимизирован. Существует альтернативный подход к использованию WCCP — интегрированное развертывание, но WCCP был выбран для примера развертывания, поскольку он обеспечивает простую реализацию без изменения физической топологии основной сети.

Шаг 5. Получите доступ к Central Manager с помощью безопасного подключения из web-браузера для наблюдения, настройки функций и создания отчетов о сети WAAS.

Настройка WAAS Central Manager

Устройство Cisco WAVE-274 используется в Central Manager для обеспечения графического управления, настройки и отчетности для сети WAAS. Это устройство установлено в ферме серверов, поскольку оно не находится непосредственно на пути направления оптимизации WAN, но обеспечивает сервисы управления и наблюдения. Первоначальная настройка Central Manager требует доступа через терминалы к порту консоли для параметров базовой настройки и назначения IP-адреса.

Программу первоначальной настройки можно запустить из командной строки, введя команду “setup”. Для выполнения первых трех действий необходимо отклонить создаваемую по умолчанию настройку, выбрать в качестве режима устройства Central Manager и выбрать интерфейсы для реализации связи в сети. Централизованная система управления (CMS) будет включена после перезагрузки системы.

```
Step 1: The following defaults can be
configured:
Device mode: Application-accelerator
Interception Method: Inline
Management Interface: InlineGroup 1/1
Autosense: yes
Timezone: UTC 0 0

To keep above defaults and continue
configuration, press 'y'
To change above defaults and continue
configuration, press 'n' [y]: n

Step 2:
 Configure WAAS Settings
 -----------------------
 Select device mode :
 1.application-accelerator
 2.central-manager
 Enter your choice [1]: 2

 This configuration will take effect after a
reload.
 Enable CMS automatically after reload(y/n)
[y]: y
```

Все подчеркнутые команды должны вводиться в одной строке.

```
 Step 3:
 Configure network settings
 --------------------------
Select interface to configure as management interface:

 NO INTERFACE NAME STATUS IP ADDRESS NETMASK
 1: InlineGroup 1/1 UP unassigned unassigned
 2:GigabitEthernet 1/0 UP unassigned unassigned
 Enter choice [1]: 2
```

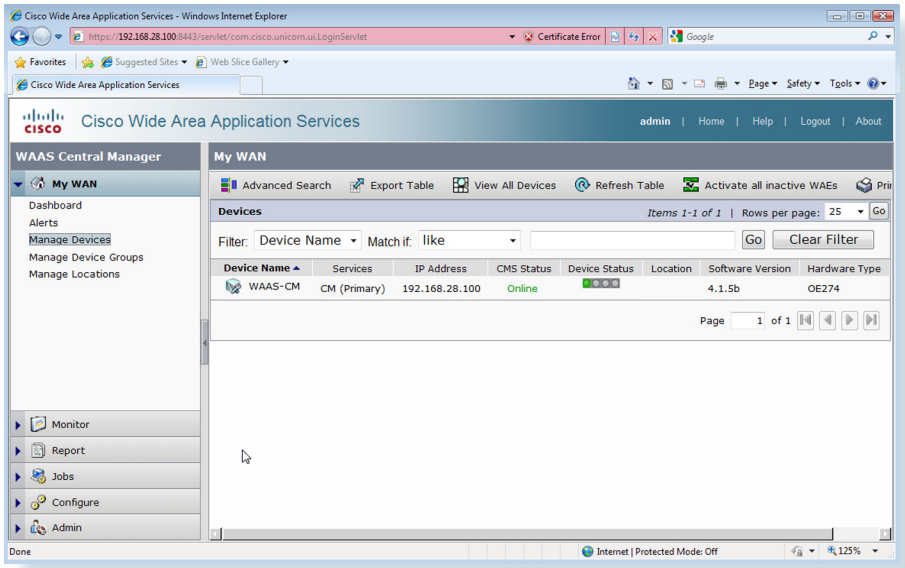
Остальные действия 4–14 по настройке предназначены в основном для настройки сети, протокола NTP и лицензирования продукта. Пример этих пунктов настройки показан ниже:

```
Step 4: Configure autosense for duplex and speed on this interface(y/n)
[y]: y
Step 5: Enable DHCP on this interface (y/n) [n]: n
Step 6: IP address of interface: 192.168.28.100
Step 7: Netmask of this interface: 255.255.255.0
Step 8: Default gateway: 192.168.28.1
Step 9: Domain name server IP: 192.168.28.10
Step 10: Domain name: cisco.local
Step 11: Enter hostname[none]: WAAS-CM
Step 12: Configure NTP [none]: 192.168.31.2
Step 13: Enter timezone [UTC 0 0]: PST -8 0
Step 14:
The product supports the following licenses:
1. Enterprise
Enter the license(s) you purchased [1]: 1

Based on the input, the following configurations will be done:
device mode central-manager
no central-manager address
no wccp version 2
interface GigabitEthernet 1/0
ip address 192.168.28.100 255.255.255.0
autosense
exit
ip default-gateway 192.168.28.1
ip name-server 192.168.28.10
ip domain-name cisco.local
primary-interface GigabitEthernet 1/0
hostname WAAS-CM
ntp server 192.168.31.2
clock timezone PST -8 0

Do you accept these configurations (y/n) [y]: y
Would you like to apply the configurations (y/n) [y]: y
This may take few moments. Please wait.
All CLI configurations were applied
successfully.
```

Для реализации этой настройки необходимо сохранить существующую настройку устройства и перезагрузить систему с помощью следующих команд:

```
WAAS-CM# copy running-config startup-config
WAAS-CM# reload
Proceed with reload?[confirm] y
Shutting down all services, will timeout in 15 minutes.
reload in progress ..Reload requested by CLI@ttyS0.
Reload requested by CLI@ttyS0.
Restarting system.
```

После завершения перезагрузки устройство Central Manager должно быть включено и запущено. Оно будет доступно для web-браузера по IP-адресу, назначенному в шаге 6 программы Setup или для назначенного имени хоста, если оно было настроено в DNS. Укажите безопасный HTTP и номер порта 8443 для доступа Central Manager, например https://192.168.28.100:8443. Выполните вход с использованием имени пользователя “admin” и пароля “default”, назначенными по умолчанию. При выборе "My WAN" -> "Manage Devices" на панели слева должен отображаться экран, на котором показан Central Manager, первоначально настроенный как единственное управляемое устройство.



Настройка WAVE для головного офиса WAAS

Устройство Cisco WAVE-574 развертывается в головном офисе для обеспечения приема трафика WAAS от удаленных узлов филиалов и распределения его по WAN. Это устройство подключается напрямую к коммутатору ядра сети, поскольку он должен использоваться для перенаправления трафика WAN. Эта же программа Setup Utility, использованная при начальной настройке WAAS Central Manager, используется и для настройки устройств WAVE и NME-WAE. Для этих устройств требуется только базовая настройка первоначальных параметров с помощью порта консоли; после завершения этой настройки все функции управления сетью WAAS выполняются с помощью графического интерфейса системы Central Manager.

Шаги настройки Setup Utility головного WAVE схожи с настройкой Central Manager, но нумерация действий начинает различаться после выбора “application-accelerator” в качестве режима работы устройства в шаге 2. После выбора этого режима сценарий настройки изменяется, и появляется возможность регистрации WAVE на существующем Central Manager и выбора WCCP в качестве метода перехвата трафика.

```
Step 1: The following defaults can be configured:
Device mode: Application-accelerator
Interception Method: Inline
Management Interface: InlineGroup 1/1
Autosense: yes
Timezone: UTC 0 0

To keep above defaults and continue configuration, press 'y'
To change above defaults and continue configuration, press 'n' [y]: n

Step 2:
Configure WAAS Settings
Select device mode :
1.application-accelerator
2.central-manager
Enter your choice [1]: 1
Step 3: Enter Central Manager address [none] : 192.168.28.100
Step 4: Select interception method (inline|wccp|other) [inline]: wccp
```

После настройки для WAVE регистрации в Central Manager программа Setup Utility разрешит выполнение настройки базовых параметров сети в шагах 5–15.

```
Step 5:
Configure network settings
--------------------------
Select interface to configure as management interface:

 NO INTERFACE NAME STATUS IP ADDRESS NETMASK
 1: InlineGroup 1/1 U unassigned unassigned
 2:GigabitEthernet 1/ UP unassigned unassigned
 3:GigabitEthernet 2/0 DOWN unassigned unassigned
 Enter choice [1]: 2
Step 6: Configure autosense for duplex and speed on this interface(y/n)
[y]: y
Step 7: Enable DHCP on this interface (y/n) [n]: n
Step 8: IP address of interface: 192.168.31.10
Step 9: Netmask of this interface: 255.255.255.0
Step 10: Default gateway: 192.168.31.1
Step 11: Domain name server IP: 192.168.28.10
Step 12: Domain name: cisco.local
Step 13: Enter hostname[none]: WAAS-HE
Step 14: Configure NTP [none]: 192.168.31.2
Step 15: Enter timezone [UTC 0 0]: PST -8 0
```

При выполнении шага 16 WAVE необходимо специально настроить для установления ассоциации протокола WCCP с локальным маршрутизатором. Поскольку было настроено головное устройство WAAS, веденный IP-адрес должен соответствовать IP-адресу ISR Cisco в головном офисе. В используемом примере сети была настроена соединительная магистраль VLAN между маршрутизатором в головном офисе и стеком коммутатора ядра сети для обеспечения необходимого уровня гибкости. Первичная VLAN, используемая для маршрутизации данных в этом канале, показана как VLAN 31; следует использовать определенную VLAN и настроенный IP-адрес маршрутизации, используемый в сети. WCCPv2 обеспечивает для WAVE возможность выполнения оптимизации нескольких маршрутизаторов. В этом примере настройки требуется только один адрес, который представляет маршрутизатор в головном офисе.

Cisco ISR

В шаге 17 приведены технические характеристики уровня лицензирования.

```
Step 16: Enter the space separated list of routers(maximum 4) for
WCCPv2 [192.168.31.1]: 192.168.31.1
Step 17:
The product supports the following licenses:
1. Enterprise
2. Enterprise & Video
3. Enterprise & Virtual-Blade
4. Enterprise, Video & Virtual-Blade
Enter the license(s) you purchased [1]: 1
```

На этом этапе выполнения сценария в WAVE имеются необходимые данные для обеспечения пробной настройки из командной строки, которую можно использовать для правильной настройки WCCP для маршрутизатора головного офиса. Скопируйте полученные данные в текстовый файл и сохраните его для использования при настройке маршрутизатора в разделе "Настройка WCCP версии 2". Хотя в полученных данных указана необходимость копирования и вставки команд, имена интерфейса, соответствующие маршрутизатору, следует заменить в пробной настройке до их применения на маршрутизаторе.

```
Please copy, paste the following in the router config mode:
ip wccp version 2
ip wccp 61
ip wccp 62
interface <Router LAN sub-interface 1>
ip wccp 61 redirect in
interface <Router WAN interface>
ip wccp 62 redirect in
interface <Router LAN sub-interface 2>
ip wccp redirect exclude in
```

Подтвердите остальные запросы после проверки данных, введенных с помощью Setup Utility. После завершения работы Setup Utility сохраните существующую настройку на устройстве. Можно подтвердить успешное завершение регистрации WAVE в системе WAAS Central Manager, выполнив команду“**show cms info**”.

```
WAAS-HE# copy running-config startup-config
WAAS-HE# show cms info
Device registration information :
Device Id = 326
Device registered as = WAAS Application Engine
Current WAAS Central Manager = 192.168.28.100
Registered with WAAS Central Manager = 192.168.28.100
Status = Online
Time of last config-sync = Thu Oct 29 11:33:59 2009

CMS services information :
Service cms_ce is running
```

Технические рекомендации. В примере настройки пространство частных IP-адресов используется таким образом, чтобы для простоты работы назначалась полная IP-подсеть с маской/24. Для экономии адресного пространства адреса можно назначать из сети /30, поскольку необходимо только два адреса хостов.

Настройка WAAS NME-WAE для филиала

Для оборудования WAAS для офиса филиала в этом примере использовалось следующее: модули NME-WAE, вставленные напрямую в разъем для сетевого модуля маршрутизатора для филиала. Благодаря этому для маршрутизатора Cisco ISR обеспечивается возможность предоставления функций WAAS без необходимости в дополнительном рабочем пространстве, сетевых кабелях или подключениях к сети. Также в филиале с большим количеством пользователей или в филиале, в котором требуется использование функций виртуализации, доступных в устройствах Cisco WAVE, можно использовать отдельное независимое устройство.

Маршрутизатор в филиалах взаимодействует с NME-WAE напрямую с магистральной платой маршрутизатора, но для этого взаимодействия необходимо назначение небольшой подсети IP.

В приведенном ниже примере настройки маршрутизатора филиала описывается назначение необходимой настройки интерфейсу Integrated-Service-Engine, который представляет NME-WAE. При первоначальной настройке интерфейса также необходимо добавить команду “**no shutdown**”.

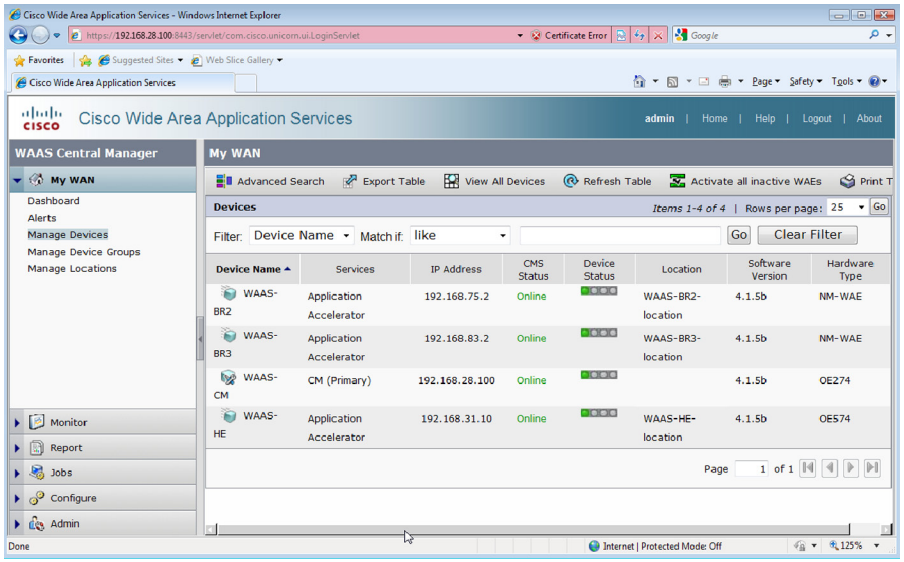
```
interface Integrated-Service-Engine1/0
 ip address 192.168.75.1 255.255.255.0
 service-module ip address 192.168.75.2 255.255.255.0
 service-module ip default-gateway 192.168.75.1
 no keepalive
```

После ввода команд и сохранения настройки откройте сеанс в NME-WAE из командной строки маршрутизатора. Выполните аутентификацию с использованием имени пользователя по умолчанию “admin” и пароля “default”. Введите команду "setup", чтобы запустить программу установки.

```
BR2ISR# service-module integrated-Service-Engine 1/0 session
Trying 192.168.75.1, 2066 ... Open

Cisco Wide Area Application Engine Console
Username: admin
Password:
System Initialization Finished.
NO-HOSTNAME# setup
```

На этом этапе NME-WAE для филиала настраивается аналогичным образом настройке головного устройства WAVE с помощью сценария настройки. IP-адрес самого NME-WAE наследуется от оператора "**service-module ip address**", применяемого к настройке маршрутизатора. При запросе адреса маршрутизатора WCCP используйте адрес, назначенный Integrated-Service-Engine в настройке маршрутизатора (в примере настройки используется 192.168.75.1). После завершения настройки, сохраните настройку в NME-WAE. В сеансе можно выполнить переход обратно к командной строке маршрутизатора, введя управляющую последовательность "**Ctrl-Shift-6 x**". Команду "**show cms info**" также можно использовать для проверки правильности регистрации NME-WAE в Central Manager.

После завершения настройки головного устройства WAVE и модулей NME-WAE для филиалов их необходимо указать в графическом интерфейсе Central Manager, выбрав **My WAN -> Manage Devices**, как показано ниже.



Настройка WCCP для WAAS (версия 2)

WCCP используется в этом примере для направления сетевого трафика, предназначенного для WAN к системе WAAS для выполнения оптимизации. При этом обеспечивается развертывание без ошибок с минимальными требованиями к дополнительной проводке. Также при этом необходимо настроить головной маршрутизатор и маршрутизатор для филиала для WCCP. На маршрутизаторе сначала необходимо включить WCCP (версия 2), несмотря на то, что обычно он включается по умолчанию, а также определить специальные интерфейсы, которые требуют включения перехвата трафика, передаваемого из сети WAN и к ней. Именно в этих случаях следует использовать образцы настроек маршрутизаторов,

Технические рекомендации. Номера 61 и 62, используемые в командах ip wccp, представляют собой идентификаторы сервисов, соответствующие перехвату трафика TCP. Идентификатор 61 указывается для местоположений филиалов, где вероятнее всего расположены клиентские компьютеры, а 62 указывается для местоположения центрального офиса или фермы серверов. Также доступны дополнительные идентификаторы сервисов для более сложных настроек; показанные в примерах настройки обеспечивают сервисы оптимизации для обычных типов трафика TCP.

предоставленные в программе Setup для WAAS. Просто подставьте фактические определения интерфейса в существующей сети в текст, указанный в настройке. В примере настройки сети для головного маршрутизатора требуется следующая настройка:

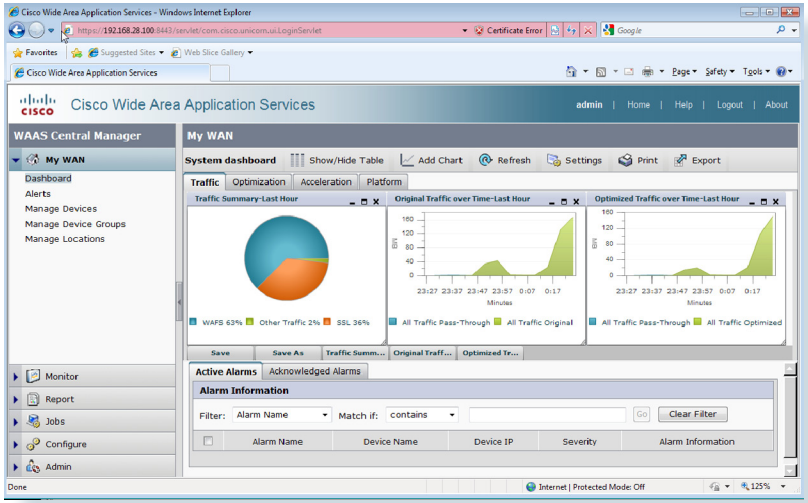
```
(hostname HQ-ISR)

ip wccp version 2
ip wccp 61
ip wccp 62

interface Port-channel1.31
 description Interface to HQ Core Switch
 encapsulation dot1Q 31
 ip address 192.168.31.2 255.255.255.0
 ip wccp 62 redirect in

interface GigabitEthernet0/2
 description Interface to WAN
 ip address 10.0.1.254 255.255.255.252
 ip wccp 61 redirect in
```

Ниже приведен соответствующий пример для маршрутизатора для офиса филиала.

```
(hostname BR2ISR)

ip wccp version 2
ip wccp 61
ip wccp 62

interface FastEthernet0/0.72
 description Wired Data Access
 encapsulation dot1Q 72
 ip address 192.168.72.1 255.255.255.0
 ip wccp 61 redirect in
interface FastEthernet0/1
```

```
 description Interface to WAN
 ip address 10.0.1.246 255.255.255.252
 ip wccp 62 redirect in

interface FastEthernet0/0.76
 description Wireless Data Access
 encapsulation dot1Q 76
ip address 192.168.76.1 255.255.255.0
 ip wccp 61 redirect in
```

Поскольку теперь WCCP настроен для обоих маршрутизаторов (головного и маршрутизатора в филиале для сети WAN), трафик будет перехватываться для оптимизации WAAS. После передачи трафика через систему WAAS статистику можно просмотреть, выбрав "My WAN -> Dashboard" в графическом интерфейсе Central Manager.



Контрольный список настройки WAAS

В таблице 1 указаны различные параметры и данные, необходимые для установки и настройки сети WAAS. Для удобства можно ввести значения в таблицу и воспользоваться ими при настройке сети WAAS. Введенные значения будут отличаться от используемых в данном примере. Эти значения используются только в качестве примера.

Таблица 1. Контрольный список системных параметров сети WAAS

Параметр	Значения WAAS Central Manager	Значения для головного офиса WAE	Значения для филиала WAE — для каждого филиала потребуется отдельный столбец "Филиал"
Скорость интерфейса	По умолчанию	По умолчанию	По умолчанию
Дуплексный режим			
IP-адрес	192.168.28.100	192.168.31.10	192.168.68.2
Маска подсети	255.255.255.0	255.255.255.0	255.255.255.0
Шлюз по умолчанию	192.168.28.1	192.168.31.1	192.168.68.1
Сервер DNS 1	192.168.28.10	192.168.28.10	192.168.28.10
Сервер DNS 2			
Домен DNS	cisco.com	cisco.com	cisco.com
Устройство WAAS (Имя хоста)	WAAS-CM	WAAS-HE	Branch-1
Домен Windows			
IP-адреса маршрутизаторов, перехватывающих трафик в WCCP			
Сервер NTP (необязательно)			
Часовой пояс (необязательно)			

Сводка по режиму ускорения работы приложений

Cisco WAAS предоставляет несколько технологий оптимизаций трафика для ускорения работы приложений при использовании WAN. В этом руководстве по развертыванию описывается базовая настройка, необходимая для использования возможностей WAAS в сети, созданной с использованием архитектуры Smart Business Architecture. В WAAS также имеются специальные шаблоны и настраиваемые параметры для многих приложений, не описываемых в настоящем руководстве. Для получения дополнительной информации свяжитесь с вашим представителем Cisco, обратитесь к уполномоченному торговому партнеру или посетите страницу http://www.cisco.com.

Список продуктов для развертывания в организациях среднего размера

Функциональная область	Продукт	Номера деталей	Версия программного обеспечения
Ядро сети 100-600	Catalyst 3750G Расширяемый, 12 портов, SFP	WS-C3750G-12S-S Catalyst 3750 12 портов, SFP + образ IPB	12.2-50.SE2
Ядро сети 500-1000	Catalyst 4507RE Два супервизора Два источника питания	WS-C4507R-E Catalyst серии 4500-E шасси с 7 разъемами, вентилятор, no ps, с поддержкой Red Sup WS-X4624-SFP-E Catalyst серии 4500-E 24 портов GE (SFP) WS-X45-SUP6-E Catalyst серии 4500-E Sup 6-E, 2x10GE(X2) с двойным гигабитным портом	12.2-50.SG2
Доступ для ПК в головном офисе, телефонов, точек доступа и других устройств	Catalyst 3750G Расширяемый, 24 порта Ethernet 10/100/1000 Мбит/с с PoE и 4 портами SFP Cisco Catalyst 3560G 24 и 48 портов Ethernet 10/100/1000 Мбит/с с PoE и 4 портами SFP	WS-C3750G-24PS-S Catalyst 3750 24 10/100/1000T Мбит/с PoE + 4 SFP + образ IPB WS-C3750G-48PS-S Catalyst 3750 48 10/100/1000T Мбит/с PoE + 4 SFP + образ IPB WS-C3560G-24PS-S Catalyst 3560 24 10/100/1000T Мбит/с PoE + 4 SFP + образ IPB WS-C3560G-48PS-S Catalyst 3560 48 10/100/1000T Мбит/с PoE + 4 SFP + образ IPB	12.2-50.SE2
Коммутатор серверной комнаты	Catalyst 3750G 24 и 48 портов Ethernet 10/100/1000 и 4 порта SFP Catalyst 3560G 24 и 48 портов Ethernet 10/100/1000 и 4 порта SFP	WS-C3750G-24TS-S1U Catalyst 3750 24 10/100/1000T Мбит/с PoE + 4 SFP + образ IPB; 1RU WS-C3750G-48TS-S1 Catalyst 3750 48 10/100/1000 Мбит/с + 4 SFP + образ IPB WS-C3560G-24TS-S Catalyst 3560 24 10/100/1000T Мбит/с + 4 SFP + образ IPB WS-C3560G-48TS-S Catalyst 3560 48 10/100/1000T Мбит/с + 4 SFP + образ IPB	12.2-50.SE2

Список продуктов для развертывания в организациях среднего размера

Функциональная область	Продукт	Номера деталей	Версия программного обеспечения
Маршрутизатор WAN головного офиса	Маршрутизатор Cisco 3925 или 3845 с интегрированными сервисами	C3925-VSEC/K9 C3845-VSEC/K9 HWIC-2CE1T1-PRI	15.0.1M
Маршрутизатор филиала WAN	Маршрутизатор Cisco 2911 или 2811 с интегрированными сервисами	C2911-VSEC/K9 C2811-VSEC-SRST/K9 HWIC-2CE1T1-PRI	15.0.1M
Модули маршрутизаторов филиалов	Модуль ускорения глобальной сети Модуль предотвращения вторжений	NME-WAE-502-K9 AIM-IPS-K9	4.1.5b 7.0(1)E3
Коммутатор для филиала	Catalyst 3750G Стекируемые 24 и 48 портов Ethernet 10/100/1000 Мбит/с с PoE и 4 портами SFP Cisco Catalyst 3560G 24 и 48 портов Ethernet 10/100/1000 Мбит/с с PoE и 4 портами SFP	WS-C3750G-24PS-S Catalyst 3750 24 10/100/1000T Мбит/с PoE + 4 SFP + IPB Image WS-C3750G-48PS-S Catalyst 3750 48 10/100/1000T Мбит/с PoE + 4 SFP + IPB Image WS-C3560G-24PS-S Catalyst 3560 24 10/100/1000T Мбит/с PoE + 4 SFP + IPB Image WS-C3560G-48PS-S Catalyst 3560 48 10/100/1000T Мбит/с PoE + 4 SFP + IPB Image	12.2-50.SE2
Межсетевой экран для подключения к Интернету	Адаптивное устройство обеспечения безопасности (ASA) ASA 5510 с модулем SSM-10 IPS	ASA5510-AIP10-K9	8.0.4.ED 7.0(1)E3
Головной офис — система предотвращения вторжений	Система Cisco IPS (серия 4200)	IPS-4240-K9 (300 Мбит/с) IPS-4255-K9 (600 Мбит/с) IPS-4260-K9 (2 Гбит/с)	7.0(1)E3

Список продуктов для развертывания в организациях среднего размера

Функциональная область	Продукт	Номера деталей	Версия программного обеспечения
Режим ускорения работы приложений CM головного офиса Конечная точка головного офиса	WAVE 574 WAVE 274	WAVE-574-K9 WAVE-274-K9	4.1.5b
Точки беспроводного доступа	1140 фиксированные с внутренними антеннами 1250 повышенной прочности со внешними антеннами	AIR-LAP1142N (в зависимости от страны) AIR-AP1252AG (в зависимости от страны)	
Контроллер WLAN	WLC 5508	AIR-CT5508-12-K9	6.0.182.0
Унифицированные коммуникации	Cisco Unified Communications Manager — MCS 7835 CMC Cisco Unity Connections MCS 7825 UCB	MCS7835I3-K9-CMC2 (требуется 2) MCS7825I4-K9-UCB1	7.1.3 7.1.3
Телефоны	Беспроводной телефон CP-7921G Беспроводной телефон CP-7925G Многокнопочный телефон CP-7931G Телефон с поддержкой конференц-связи CP-7937G Телефон с черно-белым дисплеем CP-7942G Телефон с черно-белым дисплеем CP-7962G Телефон с цветным дисплеем CP-7945G Телефон с цветным дисплеем CP-7965G Телефон руководителя с цветным дисплеем CP-7965G Программный телефон IPCOMM7-SW	Доступно большое количество моделей телефонов, соответствующих специализированным требованиям пользователей и соответствующих стандартам страны, в которой находится пользователь.	
Удаленный работник	Устройство адаптивной защиты 5505	ASA5505-BUN-K9 Устройство ASA 5505 с ПО, 10 пользователей, 8 портов, 3DES/AES	8.0.4

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.**

C07-542268-01 01/10