

1. Введение

Перед организациями, которые решили полностью перейти на протокол IP, встает еще один выбор: использовать сетевую инфраструктуру одного производителя и решения IP телефонии другого или применять решения IP телефонии производителя, построившего инфраструктуру.

Компания Cisco начала развивать IP телефонию в 1997 году и предлагает решения в этой области дольше, чем любой другой производитель. С самого начала Cisco сфокусировалась на создании единой отказоустойчивой, защищенной, интеллектуальной инфраструктуры, а также интегрированных приложений которые позволяют передавать данные, голос и видео. Cisco выбрала системный подход, который основан на интеграции и инфраструктуры, и приложений. Этот подход позволяет снизить эксплуатационные расходы, повысить производительность труда обслуживающего персонала, обеспечить высокий уровень защиты, и при этом сохранить инвестиции, сделанные в инфраструктуру и приложения. Ощутить эти преимущества можно при использовании инфраструктуры и решений для IP телефонии компании Cisco.

Этот документ призван подчеркнуть преимущества построения IP телефонии на интеллектуальной инфраструктуре Cisco. А также продемонстрировать уникальную ценность системного подхода.

2. Преимущества построения IP телефонии на интеллектуальной инфраструктуре Cisco.

Реализовывая решение IP телефонии Cisco на инфраструктуре Cisco, организация получает интеллектуальную сеть, которая понимает, какие приложения в ней используются. Это значит, что сеть активно участвует в жизни приложений, автоматически предоставляя терминальным устройствам права и привилегии, основанные на нуждах устройства в соответствии с политикой организации. Приложения IP телефонии Cisco также понимают процессы, происходящие в сети, что обеспечивает эффективное взаимодействие с ней. Они автоматически обнаруживают в сети ресурсы, необходимые им для работы. Например, IP телефон Cisco автоматически получает от коммутатора Cisco, к которому он подключается, настройки для электропитания или механизмов обеспечения качества обслуживания. Видеотелефон Cisco автоматически проверяет наличие новой версии программного обеспечения и по сети производит обновление до последней версии.

Когда сеть и приложения работают подобным образом, организация может быстрее внедрять IP телефонию. Если в процессе эксплуатации случается инцидент, он не может нанести большой ущерб для бизнеса, так как сеть автоматически распознает неисправность и самостоятельно принимает меры для ее ликвидации. Это в значительной степени упрощает управление, что в свою очередь снижает затраты на управление сетью.

Компания Sage Research провела исследование, в котором участвовало 226 организаций. Оно показало что в организациях, в которых используется оборудование разных производителей, по сравнению с теми, которые в качестве корпоративного стандарта выбрали оборудование одного производителя, время решения проблем в сети оказалось на 25% дольше. Кроме того организации, выбравшие одного производителя, использующего системный подход для решений IP телефонии и инфраструктуры, смогли уменьшить свои затраты на эксплуатацию на 43%.

2.1. Автоматизация процессов установки и изменения настроек IP телефона

Яркий пример интеграции Cisco IP телефонии и интеллектуальной сети это взаимодействие IP телефона и коммутатора, которое выражается в простоте, с которой можно установить, изменить параметры или

перенести на новое место IP телефон. После того как IP телефон будет подключен к порту коммутатора, автоматически инициализируется обмен сообщениями по протоколу Cisco Discovery Protocol (CDP) с коммутатором доступа. С помощью протокола CDP коммутатор опознает IP телефон и передает ему информацию о настройках. Так как в IP телефон Cisco встроен трехпортовый мини-коммутатор, который позволяет подключать персональный компьютер пользователя через IP телефон, трафик от пользовательского компьютера и трафик IP телефона разделяется с помощью технологии виртуальных локальных сетей (VLAN). Для этого коммутатор сообщает IP телефону номер «телефонной» виртуальной сети (Voice VLAN), чтобы трафик IP телефона передавался с правильной меткой VLAN. Кроме того коммутатор передает настройки механизмов управления качеством обслуживания (QoS) для встроенного в IP телефон мини-коммутатора. Это обеспечивает управление границей доверия маркировки QoS. Встроенный мини-коммутатор может либо доверять, то есть сохранять значение маркировки QoS для трафика, полученного от персонального компьютера пользователя, либо не доверять, то есть заново маркировать трафик согласно настройкам, полученным от коммутатора (например, в значение 0).

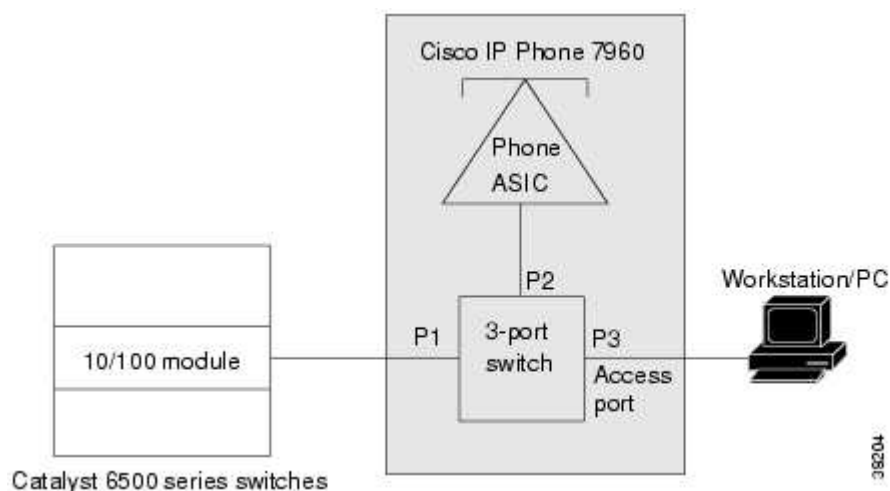


Рис. 1

IP телефоны Cisco поддерживают электропитание по Ethernet (PoE). Протокол CDP позволяет IP телефонам Cisco сообщать коммутатору точную информацию о потребляемой ими мощности, что позволяет коммутатору более эффективно управлять распределением электропитания на абонентские устройства.

Во взаимодействии IP телефона и коммутатора уникально тем, что протокол CDP автоматически распознает и настраивает IP телефон после подключения его к сети – это возможно благодаря тому, что протокол CDP является частью интеллектуальной инфраструктуры Cisco.

Другие производители IP телефонных систем, в которых нет интеграции с CDP, каждый раз, когда пользователь устанавливает или переносит IP телефон, вынуждают ИТ персонал вручную выполнять настройки на IP телефоне и порту коммутатора. По мере того, как сеть IP телефонии растет, административные расходы на поддержку IP телефонов растут экспоненциально.

Автоматизация с помощью протокола CDP выражается в значительном сокращении расходов для больших организаций связанных с установкой, перемещением или изменением настроек IP телефонов. Yankee Group оценивает эту сумму в 150\$, которые можно сэкономить при использовании IP телефонии Cisco.

2.2. Автоматизация настройки QoS в сетевой инфраструктуре.

Компания Cisco разработала функцию AutoQoS в ответ на потребность потребителей быстро внедрять настройки QoS. Эта функция Cisco IOS позволяет автоматически настроить нужные установки QoS на сотнях коммутаторах и маршрутизаторах с помощью всего нескольких команд. Cisco AutoQoS автоматизирует ряд задач, которые раньше выполнялись вручную, например, классификация трафика, создание политик, настройка параметров QoS, мониторинг и создание отчетов.

Результаты от внедрения функции AutoQoS оказались настолько успешными, что компания Cisco решила дополнить эту концепция макросами Cisco Smartport. Используя стандартных или усовершенствованных макросов IT персоналу не нужно заходить на каждый коммутатор, чтобы настроить на порту port security, DHCP Snooping и Spanning Tree PortFast. Вместо этого IT персонал может автоматически загрузить один шаблон на коммутатор, который включает в себя все нужные настройки.

Преимущество для организаций, которые используют IP телефонию и инфраструктуру Cisco заключается в том, что CDP определяет какое устройство подключено к данному порту. Это может быть IP телефон, PC, беспроводная точка доступа, видеотерминал. После этого CDP применяет макрос соответствующий данному устройству полностью автоматизируя процесс подключения, отключения и перемещения любого конечного устройства Cisco.

Cisco Smartport макросы не работают в сетях, построенных на оборудовании других производителей, что выражается в потере дорогостоящего времени и увеличении административных затрат.

2.3. Обеспечение безопасности IP телефонии

Компания Cisco Systems, в отличие от других поставщиков, предлагает своим заказчикам не точечные продукты для защиты отдельных участков информационной системы, а комплексное решение, интегрируемое в инфраструктуру организации для обеспечения безопасности IP телефонии на всех уровнях.

Self-Defending Network (SDN) – стратегия компании Cisco Systems, нацеленная комплексную, эшелонированную защиту в условиях растущей угрозы со стороны вредоносных программ и злоумышленников, воздействующих на бизнес-процессы организации изнутри и извне.

Учитывая скорость распространения современных угроз, например червей и вирусов, средства защиты компании Cisco Systems строятся на основе проактивного подхода, заключающегося в предвосхищении угроз, а не в борьбе с их последствиями. В основе SDN лежит интеграция механизмов безопасности в сетевую инфраструктуру, в которой все ее элементы – от IP телефона до сетевого оборудования, участвуют в процессе обеспечения защищенности, устойчивости и непрерывности бизнеса.

Стратегия Self-Defending Network заключается в автоматизации процесса обеспечения информационной безопасности за счет обнаружения угроз, реагирования соответственно уровню критичности, изолирования зараженных или взломанных узлов, и реконфигурации сетевых устройств с целью предотвращения повторных атак.

Внутри стратегии SDN, Cisco выделяет три направления для защиты IP телефонии:

Защита от вторжений (Threat Defense). При подключении IP телефона сеть необходимо проверить его IP и MAC адрес. Злоумышленники часто применяют технику, известную как IP spoofing, которая заключается в использовании чужого, легального IP адреса. ПО коммутатора доступа - Cisco IOS, включает в себя функции DHCP snooping и IP Source Guard и ряд других функций, которые обнаруживают признаки IP spoofing и предотвращают подобные атаки.

На уровне доступа к сети VLAN помогают организациям логически разделить сеть по принципу разграничения прав доступа пользователей к необходимым им ресурсам. Списки доступа (ACLs) гарантируют, что только пользователи с авторизованным IP адресом, протоколом, портом имеют доступ в определенный VLAN. Cisco первой предложила создавать голосовые VLAN для передачи голоса и отдельные VLAN для передачи данных. Такое разделение помогает повысить производительность сети и устойчивость к атакам. Например, если сетевой червь или вирус заразит компьютер в одном VLAN, то угроза заражения будет ограничена только этим VLAN. ACL и VLAN поддерживаются Cisco IOS на всех маршрутизаторах, межсетевых экранах и на большинстве коммутаторах.

Cisco Firewall provides rich stateful inspection firewalling services for wide range of VoIP standards and other multimedia standards, including Streaming video and streaming audio. For example, the firewalls support the stateful processing of the most important signaling protocols, H.323 and SIP. By carefully controlling the passage of these protocols through the control points in the network, monitoring the specific connection request and required resources and only permitting what is specifically necessary for the operation of the system, Cisco

firewalls help protect against session hijacking and spoofing. Intelligent control of session information is an important component of protecting the voice systems. As with data networks, network-based IDSs and host-based IPSs are crucial to a defense-in-depth strategy. IDSs protect against known forms of attack, where signatures—bit sequences—exist to identify the attack. IPSs, on the other hand, look for unusual traffic on the network, such as an attempt to execute an unusual command, or a malformed packet indicating some form of protocol manipulation. IPSs do not require predefined signatures, and thus provide effective protection against day-zero attacks—often without administrator intervention, providing the crucial automation element.

Cisco Security Agent обеспечивает высокий уровень защиты для конечных устройств, благодаря своей уникальной архитектуре. Установленный на сервер CallManager или персональный компьютер с Cisco IP Communicator, агент отслеживает системные вызовы к ядру системы, которые не соответствуют политике безопасности для конкретной машины, например приложение пытается переполнить буфер. Принцип работы агента основан на поведенческом анализе, что в отличие от анализа на основе сигнатур, позволяет эффективно противостоять неизвестным атакам.

Идентификация и управление доверием (Identity & Trust Management System). Прежде чем пользователь, приложение или устройство получит доступ к необходимым ресурсам, он должен быть идентифицирован, после этого ему будут присвоены соответствующие права и привилегии. Эту задачу решает интеллектуальная инфраструктура Cisco с помощью следующих технологий и продуктов: шифрование паролей, одноразовые пароли, цифровые сертификаты, и аутентификацию, авторизацию и учет, средства безопасности Cisco IOS.

Cisco первый и на сегодняшний день единственный производитель IP телефонии, который заслужил высочайшего рейтинга независимой тестовой лабораторией Miercom «Secure» за доказанную способность защищать IP телефонию от атак злоумышленников. Полный отчет Miercom можно найти по следующему адресу <http://www.nwfusion.com/reviews/2004/0524voipsecurity.html?page=1>

2.4. Встроенная отказоустойчивость.

С самого начала, Cisco проектировала IP телефонию для работы в пакетных сетях. В результате чего Cisco CallManager Cisco IP телефоны, голосовая почта Cisco Unity, Cisco Call Center и другие решения, не привязаны к какому-то конкретному физическому месту и могут быть расположены с любой точки сети. Например, при проектировании своей сети организации могут расположить Cisco CallManager и другие сервера обработки вызовов в любом месте сети и объединить их в кластер. Интеллектуальная инфраструктура будет обеспечивать отказоустойчивость соединений с помощью функции маршрутизации, свойственной пакетным сетям.

Однако, Cisco не ограничивается возможностями сетевой инфраструктуры. Отказоустойчивое решение для удаленного офиса (Survivable Remote Site Telephony) впервые в индустрии было предложено Cisco. Его уникальность состоит в том, что оно реализовано на ПО Cisco IOS, работающем на маршрутизаторах с интегрированными сервисами. В модели с централизованной обработкой звонков, маршрутизатор с функцией SRST берет на себя обработку местных звонков в случае если WAN соединения становятся недоступны и связь с доменом Cisco CallManager теряется. Локальные IP телефоны регистрируются на маршрутизаторе с функцией SRST, который предоставляет им широкий набор телефонных сервисов. После восстановления связи с центральным офисом, локальные IP телефоны заново регистрируются на центральном CallManager. Переключение в режим SRST и обратно происходит автоматически без вмешательства IP персонала.

2.5. Интегрированная платформа для обработки голосовых вызовов на базе маршрутизаторов Cisco ISR

Для удаленных офисов, где организация имеет ограниченное количество IT персонала, преимущества использования единой инфраструктуры для передачи данных и голоса, становятся особенно очевидны. Cisco первый и единственный производитель, который предоставляет полностью интегрированное решение включающее: телефонную станцию, голосовую почту, передачу данных, коммутацию, беспроводную точку доступа и функции обеспечения безопасности на базе одной платформы.

Работая как единая система, маршрутизаторы Cisco с интегрированными сервисами предназначены для обеспечения передовых функций безопасности, предоставления IP телефонии, функций голосового шлюза с поддержкой до 240 пользователей с Cisco CallManager Express и до 720 пользователей с Cisco SRST.

Интеграция в одном устройстве протоколов маршрутизации, функций обеспечения безопасности и голосовых приложений гарантирует целостность системы безопасности как удаленного так и центрального офиса.

Без системного подхода для реализации решений IP телефонии, организация будет вынуждена купить несколько устройств, организовать взаимодействие между ними, потратить больше времени при конфигурации и поиске неисправностей, а в результате получит решение с более слабой защитой и проблемами с обеспечением качества обслуживания (QoS).

Функциональность маршрутизаторов Cisco с интегрированными сервисами

- Встроенная в ПО Cisco IOS полно функциональная телефонная станция Cisco CallManager Express с отказоустойчивым решением (Cisco SRST)
- Интегрированный сервисный модуль или (AIM) модуль голосовой почты Cisco Unity Express с функцией автосекретаря.
- Встроенные слоты для установки DSP для организации голосового шлюза VoIP, транскодирования, и создания многопользовательских конференций.
- Интегрированные голосовые WAN интерфейсные карты (VWICs) для передачи голоса и данных
- Интегрированные сетевые модули поддерживающие до 24 аналоговых, 12 FXO и 8 BRI портов;
- Интегрированные коммутационные модули низкой плотности с поддержкой PoE для обеспечения питанием IP телефонов и беспроводных точек доступа
- Поддержка широкого спектра протоколов маршрутизации средств обеспечения QoS в ПО Cisco IOS

2.6. Быстрое решение проблем в системе IP телефонии с помощью CiscoWorks IP Telephony Environment Monitor (ITEM)

Проблема возникающая в любом компоненте IP телефонии или инфраструктуры обеспечивающей передачу голосового трафика может отразиться на качестве голоса. Компания Cisco создала средства управления, которые позволяют быстро решать проблемы возникающие в IP телефонии Cisco и интеллектуальной инфраструктуре Cisco.

В большинстве крупных организаций, традиционно существуют две сервисные команды, одна из которых отвечает за систему передачи голоса, другая за инфраструктуру передачи данных. Так как проблемы возникают в обеих сферах и часто взаимосвязаны, очень важно иметь возможность обмениваться данными о проблеме друг с другом.

CiscoWorks ITEM это комплект приложений, которые в реальном времени оценивают и создают отчеты о состоянии системы IP телефонии Cisco. Эта информация отражает существующие и потенциальные проблемы в системе IP телефонии и сетевой инфраструктуре.

Но что если в сетевой инфраструктуре были сделаны изменения которые влияют на качество голосового трафика? Что если было установлено новое приложение, которому дан высокий приоритет качества обслуживания (QoS), которое в результате заняло часть пропускной способности отведенной голосовому трафику?

CiscoWorks ITEM имеет средства автоматизированного тестирования для измерения задержки передачи пакетов, переменной задержки и многих других параметров IP SLA при изменении которых ITEM оповещает оператора. Если проблемы находятся в сети передачи данных, команда по поддержке IP телефонии должна скоординировать свою работу с командой передачи данных.

Сегодня, операторы команды передачи данных, следят за состоянием сетевой инфраструктуры с помощью CiscoWorks LAN Management Solution (LMS). Так как обе системы управления являются частью CiscoWorks, они имеют общую архитектуру и терминологию. Поэтому команда поддержки IP телефонии имеет возможность разрешать проблемы связанные с голосом, даже если суть проблемы находится в сетевой инфраструктуре. Обе команды имеют общий набор инструментов и одинаково видят состояние сети. Это

позволяет эффективно и целенаправленно взаимодействовать друг с другом при возникновении проблемы, что ведет к быстрому ее разрешению.

2.7. Сервис и поддержка Cisco Systems

По мере того как организации переходят на IPT решения, они находят значительные преимущества от получения сервисов и поддержки от одного производителя. Сервисы и поддержка которые покрывают Cisco IPT решения и интеллектуальную инфраструктуру Cisco предоставляют выгоды в виде бизнес, технических и экономических преимуществ. Примером может послужить единый сервисный контракт на маршрутизатор с интеграцией сервисов, который включает в себя функциональность нескольких устройств – маршрутизатор, IP телефонная станция, система обнаружения вторжений, беспроводная точка доступа.

По запросу Cisco компания Sage Research провело исследование, которое включало в себе опрос организаций 266. Результаты показали что, возможность значительно снизить стоимость владения сетью есть у организаций которые построили свою сеть на оборудовании одного производителя. Они платят на 26% меньше за стоимость владения такими конечными устройствами как, IP телефоны и приложения для работы с ними. На 43% меньше стоимость владения сетью у организаций внедривших IP телефонию на инфраструктуре от одного производителя, по сравнению с теми организациями, которые используют решения от разных производителей.

Cisco Systems предлагает продукты, сервисы и технологическую экспертизу, подкрепленные лидирующим положением на рынке. Это позволяет Cisco Systems позиционировать себя как единого производителя способного поставлять комплексные IPT решения интегрированные в сетевую инфраструктуру.

Примеры сервисов и поддержки, которые отличают Cisco от других производителей:

- Планирование, проектирование, внедрение и оптимизация процесса перехода на IP телефонию;
- Комплексные, интегрированные решения и системы которые легко заказать, установить, использовать и обновлять;
- Возможности Cisco Capital для предоставления кредита на льготных условиях;
- Обучение, сертификация и экспертиза предоставляемый нашими партнерами;
- Техническая поддержка 24 x 7

В дополнение, полностью интегрированная коммуникационная система от Cisco (где IP телефоны, коммутаторы доступа, маршрутизаторы, беспроводные точки доступа и другие компоненты) позволяет организации иметь единую точку для быстрого решения проблем. Организации не нужно определять где произошла проблема, на оборудовании какого производителя. По мере разработки дополнительной функциональности, Ваша организация будет в числе тех, кто первый сможет воспользоваться новыми возможностями. И конечно Вы всегда можете быть уверены в том, что IP телефонное оборудование и элементы инфраструктуры полностью совместимы.

В конечном итоге, многолетний опыт в разработке решений для IP телефонии и IP сетей позволяют нашим потребителям быть уверенными в том, что они обрели сильного союзника для построения масштабируемого, безопасного и оптимальное IPT решения.