

Руководство по конфигурированию и примеры конфигурирования сервера мониторинга VoIP версии 4.2

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Обзор Сервера Мониторинга VoIP \(VoIP Monitor Server\)](#)

[Структура документа](#)

[Примеры развертывания](#)

[Развертывание с одним коммутатором](#)

[Свернутое ядро \(Один логический центр обслуживания\)](#)

[Свернутое ядро \(Несколько логических центров обслуживания\)](#)

[Трехуровневая сеть, сконфигурированная для резервирования / балансировки нагрузки](#)

[Планирование развертывания](#)

[Условия работы сервера мониторинга VOIP](#)

[Доступ к трафику VoIP](#)

[Домены коммутации на уровне 2](#)

[Единственная копия пакетов VoIP](#)

[Совместимость IP-телефонов](#)

[Протоколы кодирования голоса](#)

[Серверы с одним процессором](#)

[Стратегии развертывания](#)

[VLAN](#)

[Порты IP-телефона](#)

[Порты голосового шлюза \(Voice Gateway\) и администратора вызовов \(CallManager\)](#)

[Обзор SPAN](#)

[Возможности коммутатора](#)

[Поддержка SPAN](#)

[Поддержка RSPAN](#)

[Ограничения сетевого трафика](#)

[Мониторинг по входу и по выходу](#)

[Поддержка VSPAN](#)

[Количество сеансов SPAN](#)

[Использование в сервере мониторинга VoIP нескольких плат NIC](#)

[Проблема](#)

[Решение](#)

[Ограничения](#)

[Проблемы](#)

[Установка в сервере мониторинга VoIP второго сетевого адаптера](#)

[Cisco Agent Desktop для установки ICD](#)

[Установка Cisco Agent Desktop для IPCC](#)

[Пример развертывания простой сети](#)

[Пример развертывания сети со свернутым ядром](#)

[Дополнительные сведения](#)

Введение

В этом документе представлена информация по возможностям сервера мониторинга VOIP версии 4.2 и требованиям к нему, достаточная для эффективного развертывания этого изделия. Также приводятся сведения о том, как сервер мониторинга VOIP следит за IP-пакетами в сети, о рекомендуемых конфигурациях сети, а также примеры использования некоторых стандартных сетевых конфигураций.

Предварительные условия

Требования

Читатели этого документа должны знать о следующих требованиях:

- Контактный IP-центр (IP Contact Center; IPCC) Cisco
- Компьютер с Агентом интеграции компьютерных технологий (Computer Telephony Integration; CTI)
- Коммутаторы Cisco и коммутацию LAN

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Cisco Agent Desktop версии 4.2 и более поздних

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Обзор Сервера Мониторинга VoIP (VoIP Monitor Server)

Сервер мониторинга VoIP поддерживает для Cisco Agent Desktop функции мониторинга и записи, без вмешательства. Это выполняется путем наблюдения за сетевым трафиком к и от определенных IP-телефонов, голосовых шлюзов и (или) Cisco CallManager. Если сервер находит для определенного устройства входящий или исходящий пакет, пакет посылается на приемник. Если администратор наблюдает за вызовом, то приемник - это компьютер администратора, в котором приложение клиента VoIP декодирует голосовой поток и посылает результат на звуковую плату компьютера администратора. Для записи, в качестве приемника выступает Сервер записи и статистики (RASCAL), который декодирует голосовой поток и сохраняет результат в виде файла .wav.

Сервер мониторинга VoIP выполняет это при участии функции мониторинга коммутаторов Cisco Catalyst. В большинстве коммутаторов Catalyst эта функция называется Анализатор коммутируемого порта (Switched Port Analyzer; SPAN). У некоторых коммутаторов Catalyst есть улучшенная функция, называемая Удаленный SPAN (RSPAN). Функция мониторинга позволяет коммутатору копировать сетевой трафик одного или нескольких источников и посылать его на определенный порт назначения. В качестве источников могут выступать порты и/или виртуальные LAN (VLAN). При RSPAN, порты-источники могут располагаться на других коммутаторах. Сервер мониторинга VoIP подключается к коммутатору через порт-адресат. Таким образом сервер мониторинга VoIP Monitor Server может видеть входящий и исходящий трафик IP-телефонов.

Сервер мониторинга VoIP рассматривает только пакеты Real Time Transport Protocol (RTP). Пакеты RTP содержатся внутри протокола User Datagram Protocol (UDP), который в свою очередь находится внутри протокола Ethernet. Сервер мониторинга VoIP знает MAC-адрес IP-телефона, для которого ведется наблюдение или запись разговоров. Он сравнивает эти MAC-адреса с MAC-адресами источника или адресата, которые содержатся в пакете UDP, и на этой основе принимает решение о направлении пакета RTP в приемник.

[Структура документа](#)

В этом документе сначала рассматриваются рекомендуемые варианты развертывания, основанные на нескольких типичных сетевых конфигурациях (от простых до сложных). Для каждого варианта развертывания описываются функции, проблемы и ограничения. Описания в этих разделах достаточно детальны и описывают работу сервера мониторинга VoIP и проблемы, разрешение которых необходимо для успешного развертывания. [Наконец, в приложении содержатся ссылки и некоторые примеры развертывания с использованием существующих коммутаторов. Все это помогает при принятии решений по развертыванию серверов мониторинга VOIP.](#)

[Примеры развертывания](#)

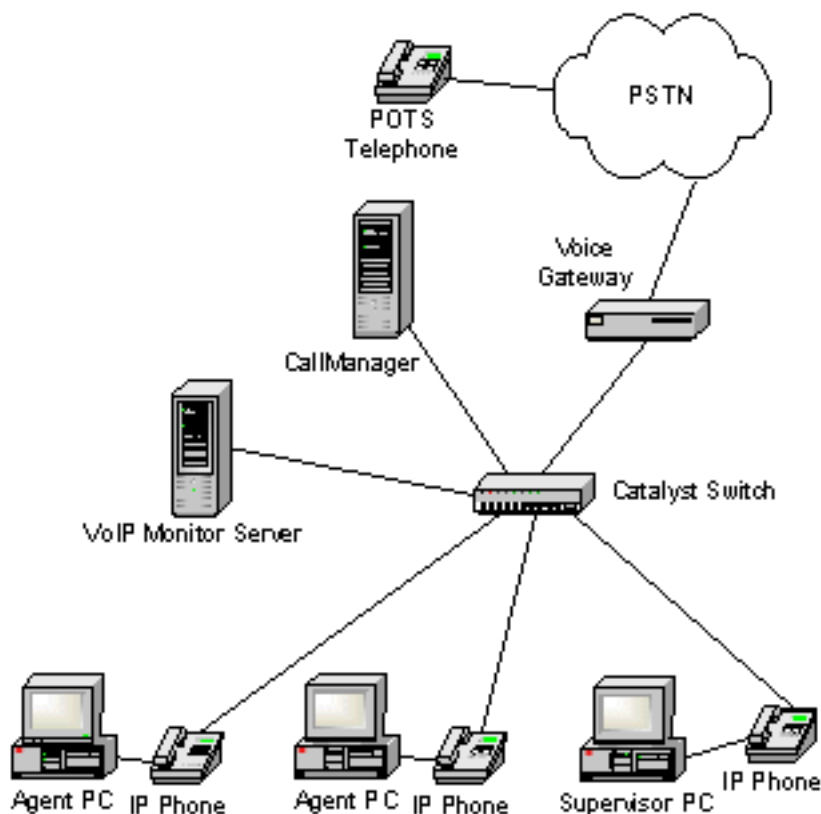
В следующих разделах представлены лучшие примеры вариантов развертывания серверов мониторинга VOIP, основанные на различных типичных сетевых конфигурациях. Выберите сетевую конфигурацию, наиболее близкую к вашей, и обратитесь к замечаниям по развертыванию.

[Развертывание с одним коммутатором](#)

[При развертывании с одним коммутатором, показанным на Рисунке 1, CallManager, голосовой шлюз, сервер мониторинга VoIP и все IP-телефоны подключены к одному и тому](#)

[же коммутатору](#). Количество агентов невелико. Данные и голос разделены с помощью VLAN.

Рисунок 1: Развертывание с одним коммутатором



Мониторинг "агент-агент": Вариант 1

- Для мониторинга голосовых VLAN, на коммутаторе сконфигурирован SPAN. SPAN сконфигурирован только на копирование входящих пакетов.
- [Если коммутатор не поддерживает мониторинг VLAN \(Таблица 6\), используйте Вариант 2.](#)

Мониторинг "агент-агент": Вариант 2

- Установите SPAN для наблюдения за каждым портом коммутатора для IP-телефонов, при этом SPAN должен наблюдать только за входящими портами.

Мониторинг "только вызывающая сторона - агент": Вариант 3

- SPAN конфигурируется для мониторинга портов голосового шлюза и CallManager с возможностью копирования входящих и исходящих пакетов.
- [Если используемый коммутатор не поддерживает наблюдение за портами других VLAN \(Таблица 7\), то голосовой шлюз, CallManager и все IP-телефоны должны быть на одной и той же VLAN.](#)

[За примером конфигурации такой сети с использованием коммутатора Catalyst 3524, обратитесь к Примеру развертывания простой сети.](#)

Свернутое ядро (Один логический центр обслуживания)

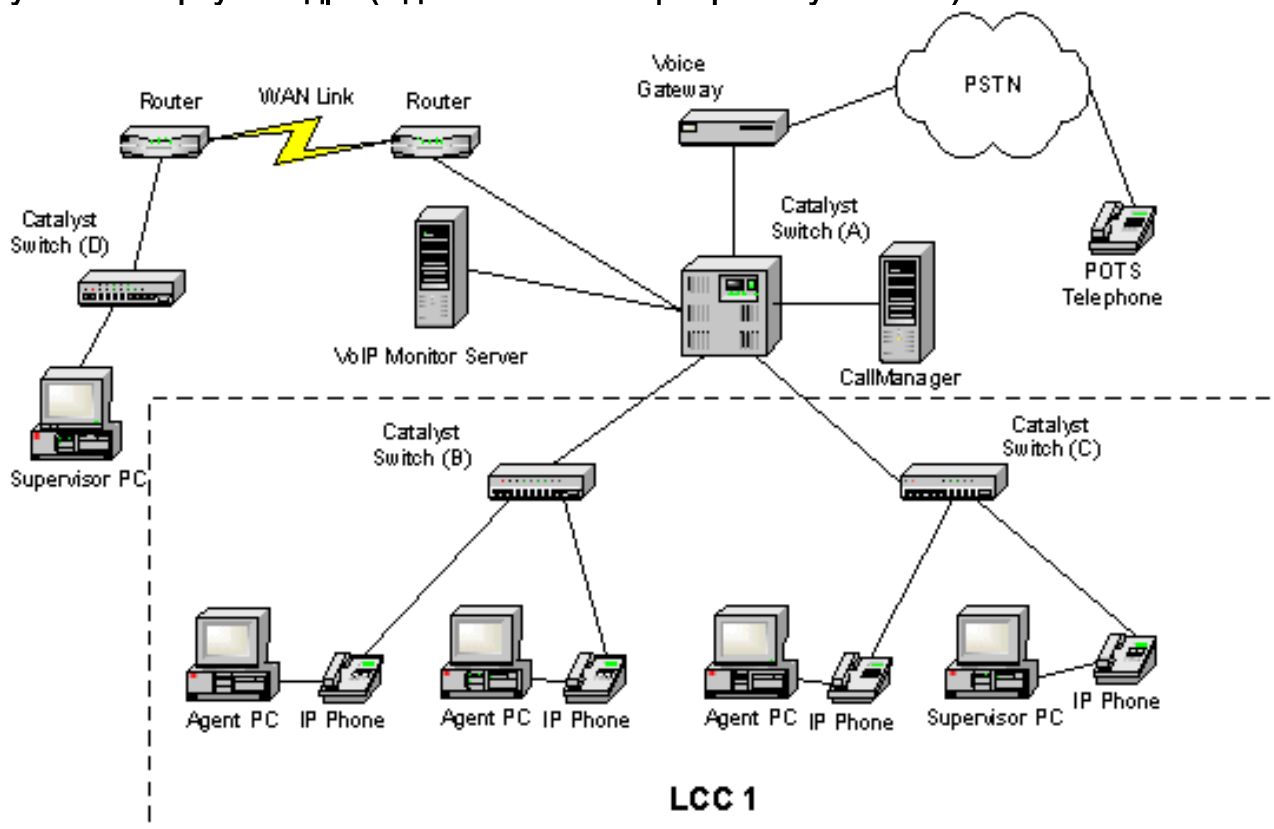
В этой конфигурации, коммутатор А обслуживает как уровень ядра, так и уровень распределения. Коммутаторы В, С и D - это коммутаторы уровня доступа. Все агентские IP-телефоны подключены к коммутаторам В и С. К коммутатору D подключен только администратор. Сервер мониторинга VoIP наблюдает только за IP-телефонами на коммутаторах В и С. Маршрутизаторы между коммутаторами А и D не дают наблюдать за чем-либо на коммутаторе D, тогда как администратор на коммутаторе D может наблюдать за агентами на коммутаторах В и С.

Имеется всего один логический центр обслуживания (LCC; Logical Call Center), а потому и одна установка серверов Cisco Agent Desktop. Трафик данных отделен от трафика голоса с помощью соответствующих VLAN. Все агентские IP-телефоны принадлежат голосовой VLAN.

Сервер мониторинга VoIP может быть подключен к коммутаторам А, В или С. Место его подключения и количество используемых серверов зависит от требуемых функций, количества наблюдаемых агентов и функций, доступных на коммутаторах. В данном случае, когда количество агентов не превышает 128, для обслуживания всей голосовой нагрузки требуется один сервер мониторинга VoIP.

Если количество агентов превышает 128, потребуется создать два или более LCC, в каждом из которых установлены серверы Cisco Agent Desktop, что показано в следующем примере.

Рисунок 2: Свернутое ядро (Один логический центр обслуживания)



Мониторинг "агент-агент": Вариант 1

- Установите на коммутаторе А RSPAN, чтобы можно было наблюдать за каждым портом IP-телефона на коммутаторах В и С. При этом RSPAN конфигурируется на копирование

только входящих пакетов.

- [Если используемый коммутатор не поддерживает мониторинг RSPAN \(Таблица 3\), эта конфигурация не может быть применена.](#) Необходимо создать несколько LCC и использовать несколько серверов мониторинга VoIP. [Это описано в разделе Свернутое ядро \(Несколько логических центров обслуживания\).](#)

Мониторинг "только вызывающая сторона - агент": Вариант 2

- SPAN конфигурируется на коммутаторе А для наблюдения за голосовой VLAN, при этом SPAN конфигурируется для копирования как входящих, так и исходящих пакетов.
- Если в такой конфигурации делаются попытки мониторинга "агент-агент", проблемы с копированием пакетов могут привести к сильному ухудшению качества речи. [Это описано в Единственной копии пакетов VoIP.](#)

Мониторинг "только вызывающая сторона - агент": Вариант 3

- SPAN конфигурируется на коммутаторе ядра/распределения для мониторинга портов голосового шлюза и CallManager ports, с копированием как входящих, так и исходящих пакетов.
- [Если используемый коммутатор не поддерживает наблюдение за портами других VLAN \(Таблица 7\), то голосовой шлюз, CallManager и все IP-телефоны должны быть на одной и той же VLAN.](#)

[За примером конфигурации такой сети с использованием в качестве коммутатора ядра/распределения Catalyst 6000, а в качестве коммутаторов уровня доступа - Catalyst 3524 и Catalyst 4000, обратитесь к Примеру развертывания сети со свернутым ядром.](#)

Свернутое ядро (Несколько логических центров обслуживания)

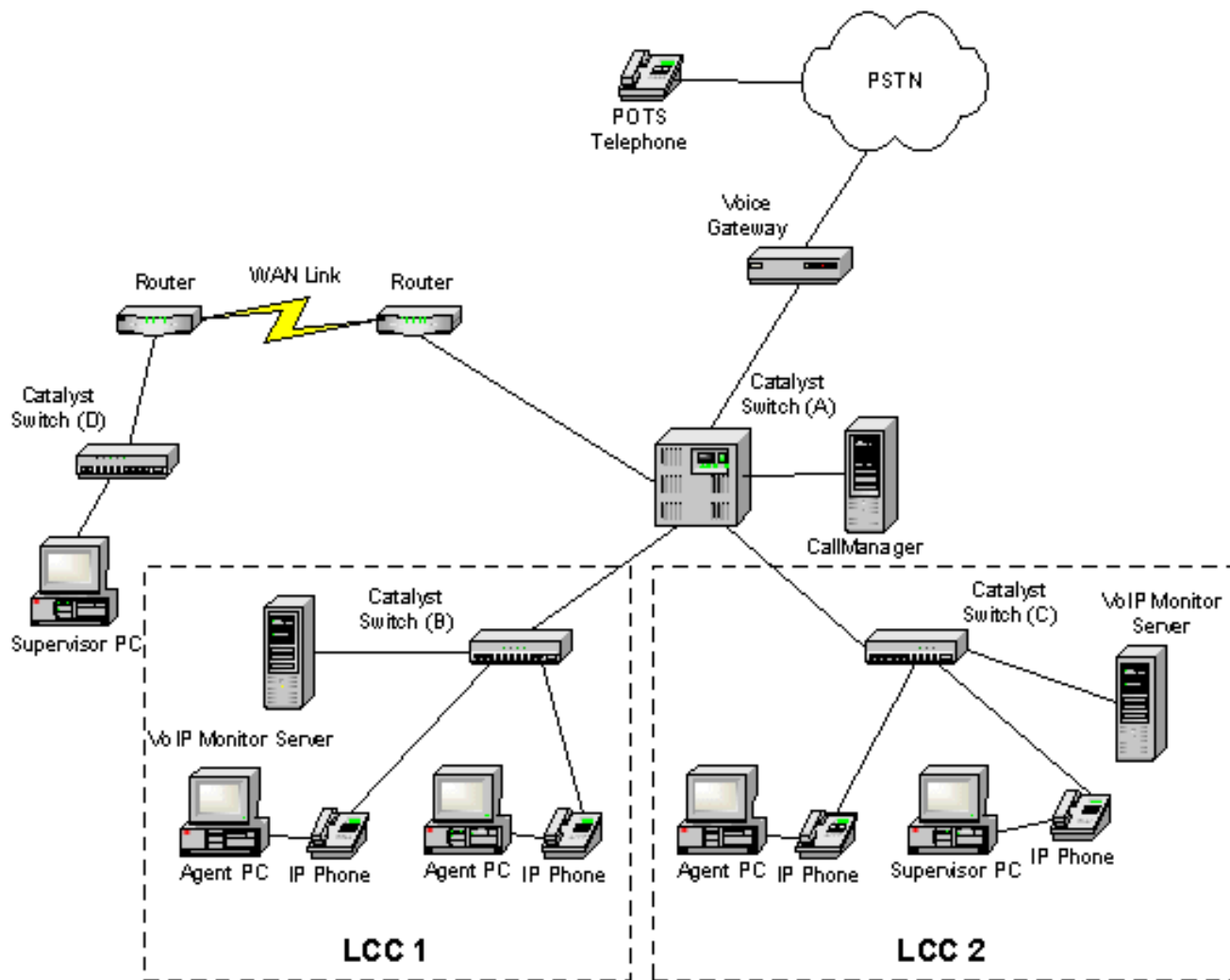
В этой конфигурации, коммутатор А обслуживает как уровень ядра, так и уровень распределения. Коммутаторы В, С и D - это коммутаторы уровня доступа. Все агентские IP-телефоны подключены к коммутаторам В и С. К коммутатору D подключен только администратор. Сервер мониторинга VoIP наблюдает только за IP-телефонами на коммутаторах В и С. Маршрутизаторы между коммутаторами А и D не дают наблюдать за чем-либо на коммутаторе D, тогда как администратор на коммутаторе D может наблюдать за агентами на коммутаторах В и С.

К коммутаторам В и С подключено по 100 агентов. Так как один сервер мониторинга VoIP не может поддерживать голосовой трафик 200 агентов (см. ссылку), создано два LCC. На каждом LCC установлены серверы Cisco Agent Desktop, и поэтому у каждого LCC есть его собственный сервер мониторинга VoIP.

Примечание: Даже если оба объединенные коммутатора имеют меньше чем 128 агентов, это - также конфигурация для разрешения контроля агент-агент.

На коммутаторах В и С, трафик данных и голосовой трафик разделены за счет отдельных VLAN для голоса и данных. Все агентские IP-телефоны принадлежат голосовой VLAN коммутатора.

Рисунок 3: Свернутое ядро (Несколько логических центров обслуживания)



Мониторинг "агент-агент": Вариант 1

- SPAN сконфигурирован на коммутаторах B и C для наблюдения за голосовыми VLAN коммутаторов. SPAN копирует только входящие пакеты.
- [Если коммутатор не поддерживает мониторинг VLAN \(Таблица 6\), используйте Вариант 2.](#)

Мониторинг "агент-агент": Вариант 2

- Установите SPAN так, чтобы можно было наблюдать за каждым IP-портом IP-телефона на коммутаторе уровня доступа.
- В этой конфигурации, сервер мониторинга VoIP может наблюдать и за вызовами "агент-агент".
- Администраторы могут наблюдать за агентами того же LCC.
- Администратор одного из этих LCC может наблюдать за вызовами между агентом в LCC1 и агентом в LCC2, только если наблюдается агент в LCC администратора.

Трёхуровневая сеть, сконфигурированная для резервирования / балансировки нагрузки

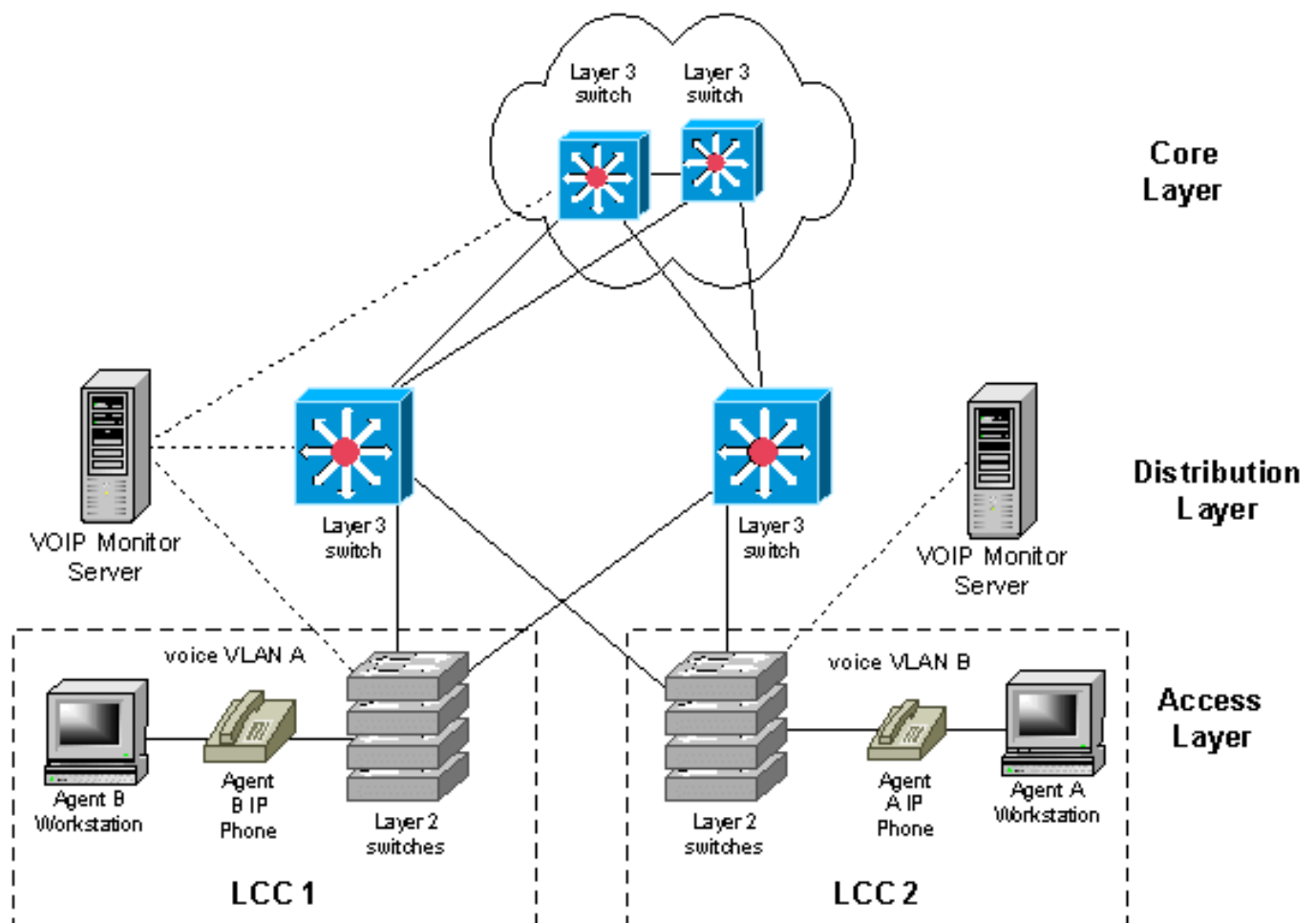
[Как показано на Рисунке 4, два коммутатора ядра с резервированием подключены к двум](#)

[коммутаторам распределения с резервированием](#). Последние, в свою очередь, подключены к двум наборам коммутаторов уровня 2 на уровне доступа. Коммутаторы в наборах соединены друг с другом через магистральные порты. Объединение в наборы позволяет коммутаторам работать как единому целому (с точки зрения сервера мониторинга VoIP). Предполагается, что к каждому набору коммутаторов уровня доступа подключено более 128 агентов. [Поэтому имеется два LCC, что показано на Рисунке 4](#).

Это обычная конфигурация сетей Cisco. Такая конфигурация поддерживает резервирование, балансировку нагрузки или обе функции.

При такой конфигурации, может быть несколько вариантов развертывания серверов мониторинга VoIP, выбор которых зависит от возможностей различных коммутаторов и от желания заказчика наблюдать только за вызовами вызывающая сторона - агент или также за вызовами агент - агент.

Рисунок 4: Трехуровневая сеть, сконфигурированная для резервирования / балансировки нагрузки



[Мониторинг "агент-агент": Вариант 1](#)

- SPAN сконфигурирован на коммутаторах B и C для наблюдения за голосовыми VLAN коммутаторов. SPAN копирует только входящие пакеты.
- [Если коммутатор не поддерживает мониторинг VLAN \(Таблица 6\), используйте Вариант 2](#).

[Мониторинг "агент-агент": Вариант 2](#)

- Установите SPAN так, чтобы можно было наблюдать за каждым IP-портом IP-телефона на коммутаторе уровня доступа.

При такого рода установках, единственная возможность для сервера мониторинга VoIP версии 4.2 - это конфигурирование каждого набора коммутаторов доступа в качестве LCC, при этом все устройства каждого LCC являются частью голосовой VLAN, и для каждого LCC используется отдельный сервер мониторинга VoIP, что и показано на Рисунке 4. В каждом наборе, SPAN конфигурируется для мониторинга голосовой VLAN этого набора.

Планирование развертывания

При планировании развертывания сервера мониторинга VoIP необходимо учесть множество факторов. Принимаемые решения позволяют определить необходимое количество устанавливаемых серверов мониторинга VoIP, их расположение, а также конфигурацию. В Таблице 1 представлены основные факторы, которые необходимо учесть при планировании развертывания серверов мониторинга VoIP. Указана также степень влияния этих факторов на развертывание. Далее в данном документе эти вопросы рассмотрены более подробно.

Таблица 1: Основные факторы

Решение / функция	Важность
Количество агентов	Сервер мониторинга VoIP может поддерживать голосовой трафик 128 вызовов одновременно. Более высокие нагрузки вызывают ухудшение работы. В качестве общего правила можно использовать $APT * N = X$, где APT - это среднее максимальное время разговора, N = количество агентов, а X не должен превышать 128. Это, разумеется, упрощенная формула. При реальном, гораздо более сложном планировании, для вычисления необходимого количества серверов мониторинга VOIP, способных поддерживать данный Contact Center, применяются таблицы Эрланга.
VLAN	Необходимо разделить голос и данные путем использования VLAN для голоса и данных. Это увеличивает производительность сервера мониторинга VoIP, потому что ему не требуется следить за сетевым трафиком, не относящимся к вызовам. Если коммутатор не поддерживает VSPAN или может наблюдать только за одной VLAN, на расположение сервера мониторинга VoIP накладываются ограничения.
LCC	В одном LCC может быть только один сервер мониторинга VoIP. Несколько LCC предполагают наличие нескольких подсетей и нескольких VLAN, что может

	повлиять на способ развертывания серверов мониторинга VoIP.
Расположение маршрутизатора	Между портом сервера мониторинга VoIP и портом(ами), наблюдаемыми через SPAN, не может быть маршрутизаторов. Если они есть, то MAC-адрес голосовых пакетов будет изменяться, что сделает их невидимыми для сервера мониторинга VoIP.
Возможности коммутатора	Относительно SPAN и RSPAN, возможности коммутаторов catalyst различаются. Эти возможности или их отсутствие влияют на место установки серверов мониторинга VoIP.
Требования по мониторингу	Мониторинг только вызовов типа "вызывающая сторона-агент" менее сложен, чем совмещение его с мониторингом типа "агент-агент". На место развертывания серверов мониторинга VoIP влияют требования заказчика.
Количество администраторов	Одновременно администраторы могут устанавливать не более одного сеанса наблюдения на 10 агентских вызовов. Если соотношение должно быть больше, для поддержки нагрузки по мониторингу необходимо установить отдельные LCC и серверы мониторинга VoIP.

Условия работы сервера мониторинга VOIP

Доступ к трафику VoIP

Для правильной работы функций наблюдения и записи, сервер мониторинга VOIP должен иметь доступ к IP-трафику, содержащему требующие наблюдения пакеты RTP. Это означает, что голосовой трафик должен присутствовать на сетевом интерфейсе службы сервера мониторинга VOIP. Это достигается путем установки на коммутаторах, к которым подключаются агентские телефоны, SPAN или RSPAN. При конфигурировании SPAN или RSPAN, на коммутаторе в качестве портов-источников определяется один или более портов или VLAN, а также один порт в качестве порта-адресата. Порт-адресат - это порт, используемый компьютером, на котором работает сервер мониторинга VoIP, для подключения к коммутатору. IP-трафик, проходящий через порты-источники, копируется и направляется на порт-адресат. Сервер мониторинга VoIP изучает каждый пакет и определяет, нужно ли его копировать и посылать администратору для наблюдения или на сервер RASCAL для записи. В идеальном случае, сервер мониторинга VoIP должен следить только за пакетами, которые его интересуют (голосовыми пакетами). [Если голосовые VLAN не используются или коммутатор поддерживает только наблюдение за портами \(Таблица 6\), то есть прямое наблюдение за портом IP-телефона, серверу мониторинга VoIP приходится обрабатывать гораздо больший объем трафика, в котором присутствует и дополнительный.](#) Из-за этого производительность сервера снижается.

Домены коммутации на уровне 2

Поскольку трафик VoIP наблюдается и копируется на основании MAC-адреса IP-телефона, пакеты VoIP не могут подвергаться маршрутизации на уровне 3, так как при этом изменяется MAC-адрес кадров Ethernet. Между портами сервера мониторинга VoIP и портами под наблюдением (доступ к которым осуществляется посредством SPAN и RSPAN) не могут устанавливаться маршрутизаторы.

Единственная копия пакетов VoIP

При конфигурировании на коммутаторах SPAN и RSPAN, важно обеспечить посылку на сервер мониторинга VoIP только одной копии пакета VoIP. Если SPAN установлен на мониторинг двух агентских портов, и между этими агентами установлен вызов, голосовые пакеты, которыми обмениваются два IP-телефона, могут посылаться на сервер мониторинга VoIP дважды: первый раз при выходе с телефона агента А и второй раз - при приеме на телефоне агента В. На большинстве коммутаторов Catalyst, SPAN можно сконфигурировать на копирование только входящих или только исходящих пакетов. Если нужно наблюдать за вызовами "агент-агент", SPAN/RSPAN необходимо установить на копирование только входящих или только исходящих пакетов, но не обоих одновременно. [При использовании коммутаторов, не поддерживающих такую возможность \(Таблица 5\), наблюдение за вызовами "агент-агент" невозможно.](#)

Совместимость IP-телефонов

Сервер мониторинга VoIP работает с телефонами Cisco серии 79xx и программным телефоном Cisco Agent Desktop.

Протоколы кодирования голоса

Сервер мониторинга VoIP поддерживает только протоколы кодирования голоса G.711 и G.729 (при или без подавления пауз). Другие схемы кодирования ПО наблюдения не распознает.

Серверы с одним процессором

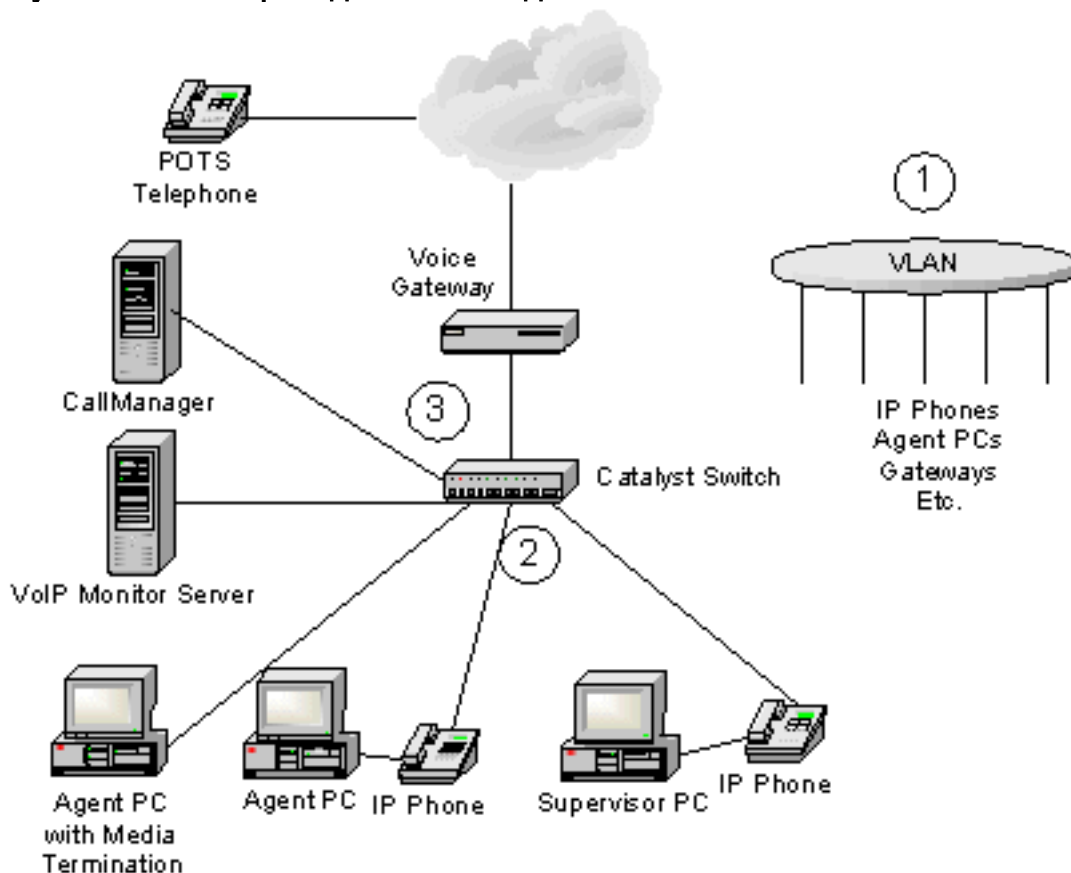
Сервер мониторинга VoIP должен работать на однопроцессорном компьютере. Низкоуровневая библиотека, используемая для наблюдения за сетевым трафиком, не поддерживает симметричную мультипроцессорную среду.

Стратегии развертывания

В этом документе представляются проверенные конфигурации, которые позволяют серверу мониторинга VoIP работать наиболее эффективно при минимальном воздействии на другие конфигурации. В этом разделе в общем виде описываются различные конфигурации для наблюдения, которые можно успешно использовать при развертывании. Эти сценарии в основном направлены на ограничение объема сетевого трафика, который сервер мониторинга VoIP должен обработать при решении требуемых задач. Наблюдение за дополнительным трафиком приводит к увеличению нагрузки на процессор сервера мониторинга VoIP, коммутатор(ы) и сеть. Использование при решении необходимых задач правильных стратегий наблюдения позволяет системе работать наиболее эффективно.

Неверные сценарии наблюдения отрицательно сказываются на сервере мониторинга VoIP и самой системе. Наблюдение за VoIP можно проводить из разных мест в системе. В данном контексте, под наблюдением понимается установка SPAN или RSPAN для наблюдения за одним или более портом или VLAN. Каждый используемый для SPAN источник оказывает влияние на мониторинг VoIP, и формы этого влияния следует понимать.

Рисунок 5: Места проведения наблюдения



[Как показано на Рисунке 5, за голосовым трафиком можно следить в трех местах.](#) К этим местам относятся:

1. Голосовая VLAN
2. Порты коммутаторов IP-телефона/Agent Desktop
3. Порты голосового шлюза (Voice Gateway) и администратора вызовов (CallManager)

VLAN

Предпочтительным является метод наблюдения за голосовыми VLAN. На это есть две основные причины:

- Разделение в сети голосового трафика и трафика данных
- Более простое конфигурирование и техобслуживание SPAN

Настоятельно рекомендуется разделить в сети голосовой трафик и трафик данных с помощью VLAN, так чтобы сервер мониторинга VoIP следил только за голосовой VLAN. Чем меньше сетевого трафика должен обрабатывать сервер мониторинга VoIP, тем выше его производительность.

Порты IP-телефона

Если коммутатор не поддерживает VLAN или VSPAN, для SPAN требуется использование в качестве исходных портов отдельных портов, а не VLAN. Это нежелательно, так как в отличие от наблюдения за VLAN, при этом сервер мониторинга VoIP находится под воздействием как голосового трафика, так и трафика данных. Этот дополнительный трафик снижает производительность сервера.

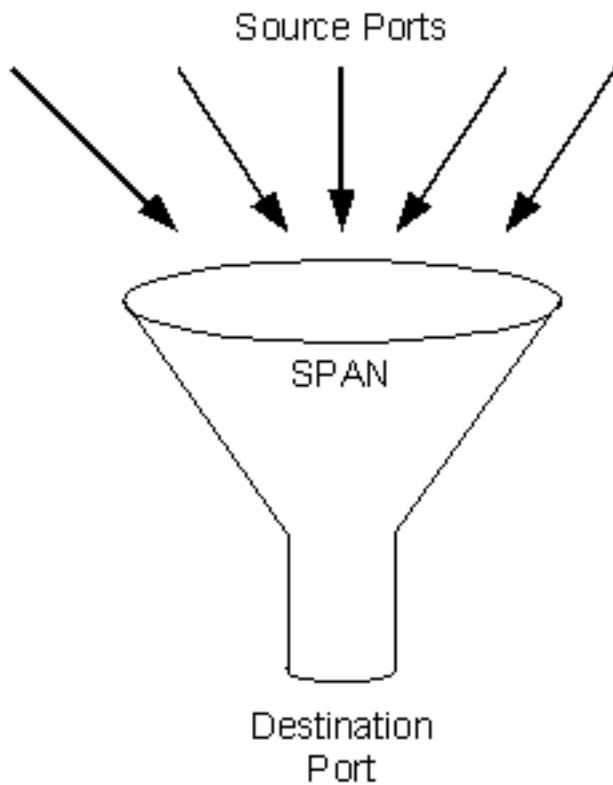
[Порты голосового шлюза \(Voice Gateway\) и администратора вызовов \(CallManager\)](#)

Если наблюдение или запись вызовов "агент-агент" не требуется, можно установить SPAN на наблюдение за портами голосового шлюза и CallManager. Это позволяет серверу мониторинга VoIP видеть все голосовые пакеты, проходящие при вызове между внешней вызывающей стороной и агентом. За вызовами "агент-агент" наблюдать невозможно, так как голосовые пакеты через порт голосового шлюза не проходят. Исключением может быть сценарий, в котором агент разговаривает с внешней вызывающей стороной, а затем устанавливает конференцсвязь с другим агентом. В этом случае, объединение голосовых потоков выполняется с помощью CallManager. Так как сервер мониторинга VoIP наблюдает за портом CallManager, за таким трех (или более)- сторонним вызовом можно успешно наблюдать.

[Обзор SPAN](#)

Работа сервера мониторинга VoIP основана на сеансе SPAN (Switched Port Analyzer; анализатор коммутируемого порта), сконфигурированном в коммутаторе Catalyst. Сеанс SPAN - это функция коммутаторов Cisco Catalyst, которая позволяет копировать IP-трафик одного или более портов и посылать его на другой одиночный порт-адресат в коммутаторе. Порты, которые используются SPAN как входные, называются исходными портами. Порт, на который посылается скопированный трафик, называется портом-адресатом. На некоторых коммутаторах, порт-адресат SPAN называется портом наблюдения. В данном документе, этот порт всегда называется портом-адресатом.

Рисунок 6: Концепция SPAN



[SPAN можно представить в виде воронки, собирающей трафик с различных портов и отправляющей его на один исходящий порт, Рисунок 6.](#) Порт-адресат SPAN используется сервером мониторинга VoIP для наблюдения за голосовым трафиком на агентские телефоны и из них.

В зависимости от модели коммутатора, в качестве портов-источников SPAN может использовать порты или VLAN. Кроме того, в качестве портов-источников могут использоваться только порты определенных типов. Использование портов в качестве портов-источников называется PSPAN (Port SPAN). Использование VLAN в качестве портов-источников называется VSPAN (VLAN SPAN). Некоторые коммутаторы поддерживают только PSPAN. Остальные поддерживают оба: PSPAN и VSPAN. Кроме того, некоторые коммутаторы поддерживают использование в единой конфигурации SPAN как портов, так и VLAN.

Локальные SPAN (LSPAN) - это такие SPAN, порты-источники и порты-адресаты которых расположены на одном и том же коммутаторе. Удаленные SPAN (RSPAN) могут содержать порты-источники, физически расположенные на других подключенных коммутаторах.

Количество SPAN, которые можно сконфигурировать, зависит от коммутатора. Конфигурации и функции SPAN различаются в зависимости от коммутатора Cisco Catalyst. В некоторых коммутаторах, порт-адресат SPAN можно сконфигурировать на представление либо только пакетов, входящих в порты-источники (входящий трафик), либо только пакетов, выходящих из портов-источников (исходящий трафик). Для многих коммутаторов вариантом по умолчанию является представление как входящего, так и исходящего трафика порта-источника.

На некоторых коммутаторах Catalyst switches, порт-адресат SPAN не воспринимает входящие пакеты. В этих случаях, в компьютерах с сервером мониторинга VoIP должно быть две платы NIC: одна для передачи и приема нормального сетевого трафика, а вторая - для приема голосового трафика с коммутатора.

За дополнительной информацией о SPAN и RSPAN обратитесь, пожалуйста, к документации по вашему коммутатору.

Возможности коммутатора

Сервер мониторинга VoIP специально предназначен для работы с линейкой коммутаторов Catalyst компании Cisco. Он может работать с другими коммутаторами, обрабатывающими трафик VoIP, но это не было протестировано.

При установке и конфигурировании ПО сервера мониторинга VoIP необходимо знать и учитывать различия в коммутаторах Cisco Catalyst. Известные на настоящее время особенности коммутаторов приведены в следующих таблицах.

Поддержка SPAN

Некоторые коммутаторы не обладают возможностью поддержки SPAN или чего-либо подобного. В этих случаях сервер мониторинга VoIP не работает, поскольку ПО мониторинга не может получить доступ к голосовому трафику. К этой категории относятся следующие коммутаторы Catalyst.

Таблица 2: Коммутаторы Catalyst, не поддерживающие SPAN

Коммутатор Catalyst
1700
2100
2800
2948G-L3
4840G

Поддержка RSPAN

В некоторых случаях, при развертывании сервера мониторинга VoIP желательно использовать RSPAN. RSPAN поддерживается не всеми коммутаторами. В некоторых случаях, коммутатор может не поддерживать RSPAN, но может существовать промежуточный коммутатор со сконфигурированным RSPAN. [Коммутаторы, не поддерживающие RSPAN, приведены в Таблице 3.](#)

Таблица 3: Коммутаторы Catalyst, не поддерживающие RSPAN

Коммутатор Catalyst
1200
1900
2820
2900
2900XL
2926GS
2926 Гл
2926Т
2926F

2948G
2950
2980G
3000
3100
3200
3500XL
3524-PWR XL
3508GL XL
2550
5000
5002
5500
5505
5509

Ограничения сетевого трафика

В некоторых коммутаторах Catalyst порт-адресат конфигурации SPAN не может работать как нормальное сетевое соединение. Через этот порт может проходить только трафик, скопированный из портов-источников SPAN. Это значит, что для нормальной работы у компьютера с сервером мониторинга VoIP должно быть два сетевых соединения. Ему требуется одна NIC для приема, наблюдения, записи запросов и взаимодействия с другими компонентами ПО Cisco Agent Desktop, которые располагаются в сети на других компьютерах. Вторая NIC предназначена для получения трафика VoIP с целью наблюдения за ним и его записи. [Относящиеся к этой категории коммутаторы приведены в Таблице 4.](#)

Таблица 4: Коммутаторы Catalyst, не поддерживающие исходящий трафик на порте-адресате SPAN

Коммутатор Catalyst
2950
3000
3100
3200
3550

[Шаги по конфигурированию системы для нормальной работы сервера мониторинга VoIP приведены в разделе Использовании в сервере мониторинга VoIP нескольких плат NIC.](#)

Мониторинг по входу и по выходу

В некоторых конфигурациях, сервер мониторинга VoIP может принимать дублированные голосовые пакеты. Эта проблема может возникнуть во многих коммутаторах Cisco Catalyst. Проблема возникает при вызовах "агент-агент", когда SPAN/RSPAN настроен на наблюдение за входящими и исходящими пакетами с обеих сторон вызова. Когда голосовой пакет покидает порт агента А, SPAN копирует его на порт сервера мониторинга VoIP. Когда голосовой пакет приходит на порт агента В, он снова копируется и посылается на сервер

VoIP. То же самое происходит с голосовыми пакетами агента В. Сервер мониторинга VoIP видит все пакеты дважды. Это приводит к ухудшению качества речи. Чтобы этого избежать, на сервер мониторинга VoIP посылаются только входящие пакеты. Определяется это установками SPAN. Некоторые коммутаторы такие установки не поддерживают.

[Коммутаторы, не поддерживающие наблюдение только за входящими пакетами, приведены в Таблице 5.](#)

Таблица 5: Коммутаторы Catalyst, не поддерживающие наблюдение только за входящими пакетами

Коммутатор Catalyst
1900
2900
2820
2900XL
3000
3100
3200
3500XL

[Поддержка VSPAN](#)

В некоторых коммутаторах, SPAN не может использовать VLAN в качестве источников. В этом случае, для мониторинга SPAN назначаются отдельные порты. [Коммутаторы, не поддерживающие VSPAN, приведены в Таблице 6.](#)

Таблица 6: Коммутаторы Catalyst, не поддерживающие VSPAN

Коммутатор Catalyst
1200
1900
2820
2900XL
2950
3000
3100
3200
3500XL
3524-PWR XL

[Количество сеансов SPAN](#)

Имеются ограничения на количество существующих в коммутаторе сеансов SPAN/RSPAN. [Эти ограничения представлены в Таблице 7.](#)

Таблица 7: Ограничения на SPAN для коммутаторов Catalyst

Модель коммутатора	Максимально допустимое количество SPAN
--------------------	--

1200	1
1900	1
2820	1
2900	1
2900XL	1
2926GS	5
2926 Гл	5
2926T	5
2926F	5
2948G	5
2950	1
2980G	5
3000	1
3100	1
3200	1
3500XL	1
3524-PWR XL	1
3508GL XL	1
3550	2
4003	5
4006	5
4912G	5
5000	5
5002	5
5500	5
5505	5
5509	5
6006	30
6009	30
6506	30
6509	30
6513	30

[Использование в сервере мониторинга VoIP нескольких плат NIC](#)

[Проблема](#)

Сервер мониторинга VoIP наблюдает за трафиком RTP из сети и посылает его интересующимся зарегистрированным клиентам. Для этого требуется поддержка со стороны коммутатора, к которому подключен сервер. А именно, сервер мониторинга VoIP должен быть подключен к порту-адресату сконфигурированного SPAN/RSPAN. Любой трафик, проходящий через порты-источники SPAN/RSPAN, копируется на порт-адресат

SPAN/RSPAN, после чего трафик становится доступным серверу мониторинга VoIP.

Изначально предполагалось, что сервер мониторинга VoIP сможет использовать порт SPAN не только для приема, но и для отправки трафика наружу. Это, однако, выполняется не для всех коммутаторов. Есть коммутаторы, которые не разрешают исходящий трафик на порте-адресате SPAN.

Решение

Решение заключается в использовании в компьютере с сервером мониторинга VoIP двух сетевых адаптеров:

1. Одного для наблюдения за потоками RTP; этот адаптер подключен к порту SPAN.
2. Второго для отправки/приема нормального трафика, такого как запросы от клиентов, наблюдаемые потоки RTP. Этот адаптер подключается к нормальному порту коммутатора, который не входит в состав наблюдаемых вышеупомянутым портом SPAN.

Ограничения

1. Так как Cisco CallManager не поддерживает два сетевых адаптера, это решение работает только в конфигурациях, в которых CallManager не работает вместе с сервером мониторинга VoIP.
2. Библиотека наблюдения WinPCap 2.2 работает только с сетевыми адаптерами, привязанными к TCP/IP. Плата для наблюдения должна быть привязана к TCP/IP.

Проблемы

- Сервер мониторинга VoIP не определяет интерфейс, который должен использоваться при отправке пакетов наружу. При использовании общего сетевого адаптера для наблюдения и нормального трафика, проблемы не возникают. При двух сетевых адаптерах, необходимо ограничить нормальный трафик таким образом, чтобы он не проходил через адаптер для наблюдения. Если этого не сделать, потоки RTP от наблюдаемого в настоящее время вызова могут не дойти до администратора, так как порт-адресат SPAN не пропускает исходящий трафик. **Разрешение: Используйте команду route для настройки локальной таблицы маршрутизации таким образом, чтобы нормальный трафик через плату для мониторинга не проходил.** За подробностями обратитесь к вашему сетевому администратору. **Другое решение: Задайте плате для мониторинга "необычный" IP-адрес, который в сети нигде больше не используется, и маску "255.255.255.0".** Кроме этого, при привязке этой платы к TCP/IP, не заполняйте поле шлюза по умолчанию.
- При установке, ICD должен зарегистрироваться в Cisco CallManager с помощью отправки ему IP-адреса. Этот IP-адрес используется CallManager для обращения к ICD. Передаваемый CallManager IP-адрес определяется при определении имени локального хоста с помощью сервера имен (типа сервера DNS или WINS). Если сервер возвращает узлу два IP-адреса, желательно, чтобы служба имен не возвращала IP-адрес платы мониторинга, так как она не может использоваться для исходящего трафика. **Решение: Используйте команды администратора, чтобы снять плату мониторинга с регистрации**

в службе имен (DNS и WINS). Чтобы эти команды работали, для обоих сетевых адаптеров должен быть деактивирован DHCP. **С помощью команды ping <имя локального хоста> проверьте возврат правильного IP-адреса.** За подробностями обратитесь к вашему сетевому администратору.

[Установка в сервере мониторинга VoIP второго сетевого адаптера](#)

(Только для Microsoft Windows 2000)

1. Вставьте в компьютер второй сетевой адаптер.
2. Загрузите компьютер.
3. Проверьте, что ни один адаптер не использует DHCP для получения IP-адреса.
4. Задайте адаптерам нужные IP-адреса.
5. Определите, какой из адаптеров будет использоваться для мониторинга. Соедините его с портом SPAN коммутатора.
6. Подключите второй адаптер к нормальному порту коммутатора, который НЕ наблюдается портом SPAN.
7. **Используйте команду route для настройки локальной таблицы маршрутизации таким образом, чтобы нормальный трафик через плату для мониторинга не проходил.** Чтобы это сделать, обратитесь к сетевому администратору.
8. Убедитесь, что плата для мониторинга не зарегистрирована в DNS и WINS. **Это можно сделать с помощью команды ping <имя локального хоста>.** Это гарантирует, что локальное имя всегда преобразуется в IP-адрес платы для нормального трафика. За дополнительной информацией обратитесь к сетевому администратору.

[Cisco Agent Desktop для установки ICD](#)

[Проблема с установкой ICD](#)

При установке IPCC, Cisco Agent Desktop предлагает пользователю выбрать IP-адрес, используемый сервером мониторинга VOIP для нормального трафика, и IP-адрес сетевого адаптера, который сервер использует для наблюдения. Однако, установка ICD включает установку Cisco Agent Desktop таким образом, что пользователь может определить только IP-адрес платы для наблюдения. По умолчанию, IP-адрес, по которому сервер мониторинга VoIP принимает запросы, появляется в предоставляемой системой нумерации первым. Это работает в сценарии с одной NIC, но может не работать в сценарии с двумя NIC. Если в нумерации первым появляется IP-адрес платы для мониторинга, то эта же самая плата будет использоваться для мониторинга и всего остального трафика. Но именно этого необходимо избежать. Для решения этой проблемы можно использовать введение DDTs для установки ICD.

Решение: Убедитесь, что в установках реестра серверов Cisco Agent записан правильный IP-адрес (инструкции приведены ниже):

[Для компьютера, в котором второй сетевой адаптер уже был до установки ICD](#)

1. Во время установки ICD, когда поступит запрос о "VoIP Monitor Server", введите IP-адрес платы для наблюдений.
2. После установки, проверьте, записан ли в IP-адрес для нормального трафика в

следующих ключах реестра: HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall VoIP
MonitorServer\
Setup\IOR HOSTNAME
HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall RASCAL Server\Setup\IOR HOSTNAME
HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall Chat Server\Setup\IOR HOSTNAME
HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall Enterprise Server\Setup\
IOR HOSTNAME

Примечание: Указанное выше значение отображается в двух строках из-за ограничения по длине.

[Для компьютера, в котором второй сетевой адаптер установлен после установки ICD](#)

1. В реестре перейдите к: HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\NetworkCards
2. Найдите запись для вновь установленной платы.
3. Скопируйте значение в "ServiceName".
4. Вставьте это значение в ключ HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall VoIP Monitor Server\Setup\MonitorDevice.
5. Перед ним добавьте \Device\Packet_ .

[Установка Cisco Agent Desktop для IPCC](#)

[Для компьютера, в котором второй сетевой адаптер уже был до установки ICD](#)

1. Во время установки IPCC, когда поступит запрос о "machine IP address", введите IP-адрес платы для нормального трафика.
2. Во время установки IPCC, когда поступит запрос о "VoIP Monitor Server", введите IP-адрес платы для наблюдений.

[Для компьютера, в котором второй сетевой адаптер установлен после установки ICD](#)

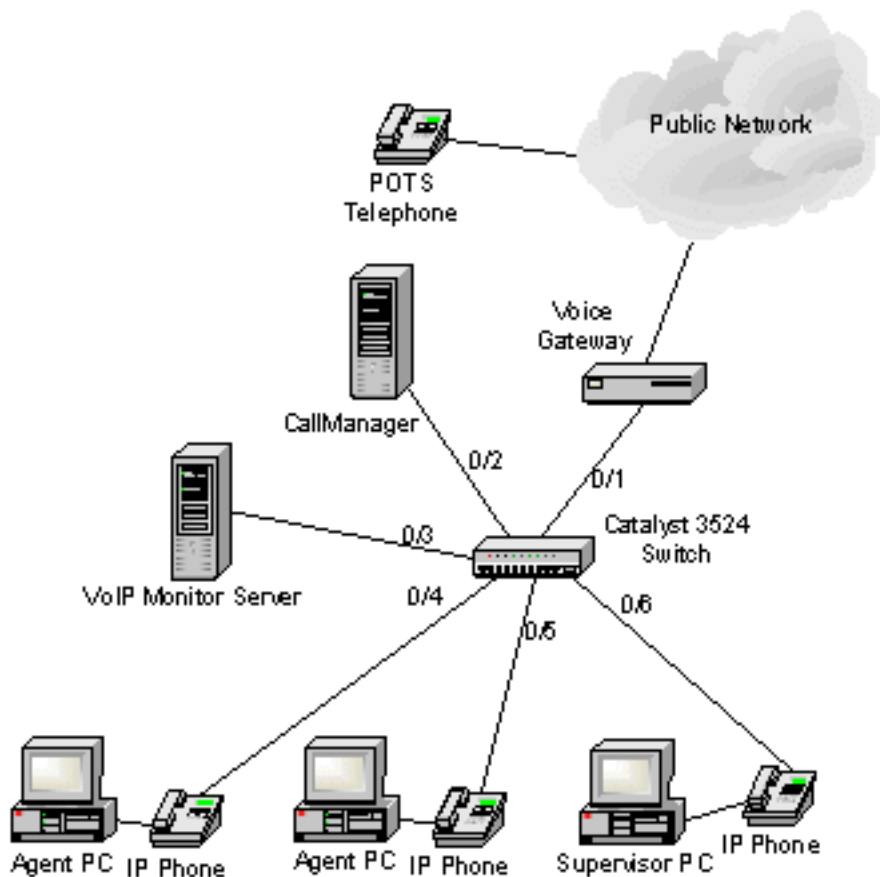
1. В реестре перейдите к NetworkCards.
2. Найдите запись для вновь установленной платы.
3. Скопируйте значение в "ServiceName".
4. Вставьте это значение в ключ HKEY_LOCAL_MACHINE\Software\Spanlink\FastCall VoIP Monitor Server\Setup\MonitorDevice.
5. Перед ним добавьте \Device\Packet_ .

[Пример развертывания простой сети](#)

[Предположения:](#)

- [Порты коммутатора сконфигурированы так, как показано на Рисунке 7.](#)
- Для IP-телефонов используется VLAN1.

Рисунок 7: Пример развертывания простой сети



Создайте на коммутаторе сеанс SPAN:

Шаг	Команда	Описание
1	config t	Переход в режим конфигурирования
2	interface 0/3	Переход в режим конфигурирования для порта Ethernet 0/3
3	port monitor vlan 1	Установка SPAN для наблюдения за голосовой VLAN1

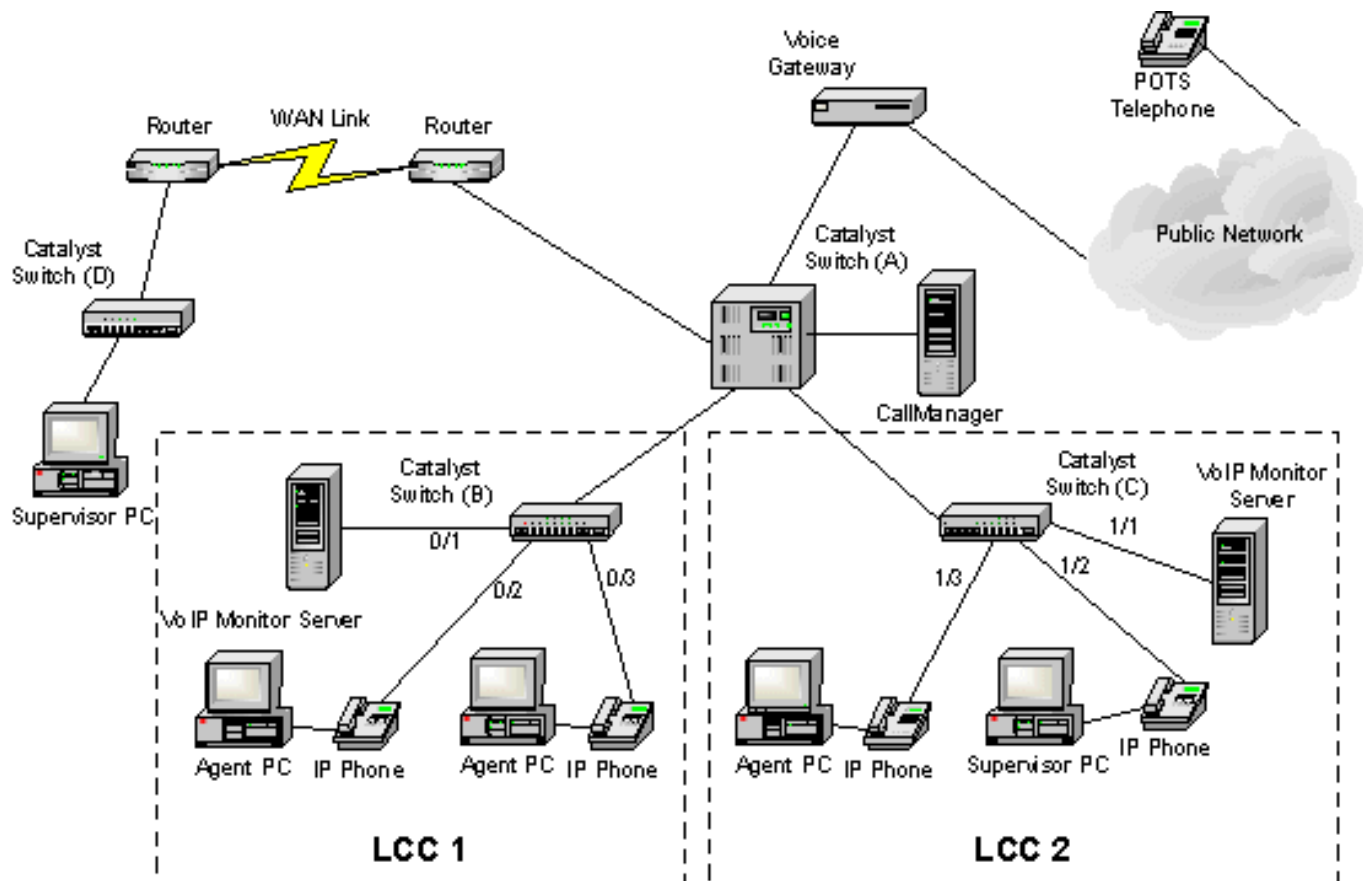
Теперь сервер мониторинга VoIP может видеть весь голосовой трафик подключенных к коммутатору IP-телефонов. Можно прослушивать или записывать как вызовы "вызывающая сторона - агент", так и "агент - агент".

Пример развертывания сети со свернутым ядром

Предположения:

- [Порты коммутатора сконфигурированы так, как показано на Рисунке 8.](#)
- На обоих коммутаторах для IP-телефонов используется VLAN1.

Рисунок 8: Пример развертывания сети со свернутым ядром



[Создайте на коммутаторе B сеанс SPAN:](#)

Шаг	Команда	Описание
1	<code>config t</code>	Переход в режим конфигурирования
2	<code>interface 0/1</code>	Переход в режим конфигурирования для порта Ethernet 0/1
3	<code>port monitor vlan 1</code>	Установка SPAN для наблюдения за голосовой VLAN1

Теперь сервер мониторинга VoIP может видеть весь голосовой трафик подключенных к коммутатору IP-телефонов. Можно прослушивать или записывать как вызовы "вызывающая сторона - агент", так и "агент - агент".

Повторите эти же шаги для коммутатора С.

[Дополнительные сведения](#)

- [Техническая поддержка - Cisco Systems](#)