Контроль приема вызовов VoIP

Содержание

Контроль приема вызовов VoIP

Номер версии	Дата	Примечания
1.1	Июль 2001 г.	Первое опубликование документа
1.2	Август 2001 г.	Незначительные изменения

Идея контроля приема вызовов (Call Admission Control, CAC) применима не к передаче данных, а только к передаче голосовой информации. При превышении запланированного поступающего трафика данных возможностей конкретного соединения сети, проблема перегрузки решается с помощью организации очередей, буферизации и отбрасывания пакетов. Дополнительный трафик попросту откладывается до тех пор, пока интерфейс не будет освобожден или, в случае отбрасывания пакетов, конечный пользователь или протокол запросит повторную передачу информации в связи с истечением времени ожидания.

При наличии трафика в режиме реального времени, чувствительного как к задержке, так и к потере пакетов, проблему перегрузки сети невозможно решить таким образом без риска ухудшения качества обслуживания, ожидаемого пользователями трафика. Для трафика в режиме реального времени, чувствительного к задержке, например, голосового трафика, целесообразнее отложить доступ к сети при ее перегрузке, чем допустить потерю или задержку данных, приводящих к прерывистой, замедленной связи и как следствие — к неудовлетворению потребителей.

Следовательно, контроль приема вызовов (CAC) представляет собой детерминированное решение, основанное на информации, которое принимается перед голосовым вызовом, и базируется на доступности необходимых сетевых ресурсов для обеспечения должного качества обслуживания для нового вызова. Целью данного документа является обзор контроля приема вызовов (CAC), описание различных механизмов контроля приема вызовов и обсуждения наилучшего применения контроля приема вызовов в конткретных сетях.

Целевую аудиторию данного документа составляют пользователи уровней Cisco 3 (компетентный), 4 (специалист) и 5 (эксперт). Документ прежде всего предназначен для сетевых администраторов и эксплуатационных групп поставщиков услуг голосовой связи по протоколу IP (VoIP). Документ содержит следующие разделы:

- Общие сведения о контроле приема вызовов
- Локальные механизмы контроля приема вызовов
- Механизмы контроля приема вызовов на основе измерений
- Механизмы контроля приема вызовов на основе ресурсов
- Как применить контроль приема вызовов к конкретной сети

Общие сведения о контроле приема вызовов

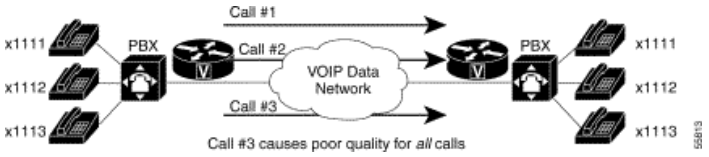
Для программного обеспечения Cisco IOS существует множество механизмов качества обслуживания (QoS) помимо контроля приема вызовов, которые предназначены для проектирования и настройки сети с пакетной коммутацией таким образом, чтобы обеспечить необходимую низкую задержку и гарантированную доставку пакетов, требуемую для голосового трафика. Эти механизмы качества обслуживания содержат такие инструменты, как организация очередей, надзор, формирование трафика, маркировка пакетов, а также фрагментация и чередование. Эти механизмы отличаются от контроля приема вызовов следующим образом:

- Они разработаны для защиты голосового трафика от борьбы с трафиком данных за одни и те же сетевые ресурсы.
- Они разработаны для работы с трафиком, уже присутствующем в сети.

Механизмы контроля приема вызовов расширяют возможности пакета инструментов качества обслуживания (QoS) для защиты одного голосового трафика от негативного влияния другого голосового трафика и защиты сети от избыточного голосового трафика. На рис. 1 показывается необходимость контроля приема вызовов. Если полосы пропускания канала доступа к глобальной сети между двумя офисными АТС достаточно только для двух вызовов методом IP-телефонии, то разрешение третьего вызова ухудшит качество

передачи голоса всех трех вызовов.

Рис. 1. Сеть VoIP без контроля приема вызовов



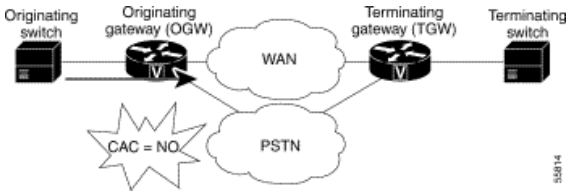
Причина подобного ухудшения заключается в том, что механизм организации очередей обеспечивает надзор, а не контроль приема вызовов, что означает выбрасывание последних пакетов из очереди при получении пакетов, превыщающих настроенный или разрешенный размер. В механизмах организации очередей не предусмотрена возможность определения принадлежности IP-пакета тому или иному голосовому вызову, поэтому любой пакет, превышающий заданную интенсивность входного потока за определенный интервал времени, будет отброшен. Таким образом, для всех трех вызовов будет наблюдаться потеря пакетов, воспринимаемое конечными пользователями как фрагментированная речь.

Такую проблему легче решить для механизмов передачи голоса на уровне 2 (VoFR и VoATM), но она особенно раздражает пользователей приложений VoIP, которые являются более привлекательными и распространенными.

Варианты изменения маршрутизации вызова

На рис. 2 показана точка, в которой решение механизма контроля приема вызовов о недостатке сетевых ресурсов для обработки вызова достигает исходящего шлюза.

Рис. 2. Сеть VoIP с механизмом контроля приема вызовов



После отклонения вызова на шлюзе, который его инициировал, происходит поиск иных возможностей обработки вызова. Таких возможностей существует несколько, большинство из них зависят от конфигурации шлюза. Если отсутствуют какие-либо особые настройки, то исходящий шлюз направит вызывающей стороне сигнал занятости линии. В Северной Америке сигнал занятости линии называется *fast-busy* (сигнал с удвоенной скоростью), а в других частях мира — *overflow tone* (сигнал перегрузки) или *equipment busy* (сигнал занятости оборудования). Такой сигнал часто перехватывается маршрутизаторами ТфОП или офисной АТС и заменяется речевым объявлением: «Все каналы заняты, пожалуйста, перезвоните позже».

Исходящий шлюз можно настроить на использование следующих сценариев маршрутизации:

- Вызов можно перенаправить через альтернативный путь сети с пакетной коммутацией при условии существования такой сети, что требует настройки второй адресуемой точки вызова сети VoIP с более низким приоритетом, чем у выбранного основного узла.
- Вызов может быть переправлен через альтернативный путь сети TDM (time-divison multiplexing), который предварительно должен быть настроен на адресуемой точке вызова аналоговой телефонной сети (POTS) и физическом интерфейсе TDM для ТфОП или офисной АТС.
- Такой вызов может вернуться на исходный маршрутизатор TDM для более выгодного использования одной из следующих функций маршрутизации.
- ◦ Если соединение между исходным маршрутизатором и исходящим шлюзом представляет собой общий канал сигнализации (common channel signaling, CCS), например, QSIG (Q Signalling), PRI (Primary Rate Interface) или BRI (Basic Rate Interface), отклонение вызова может сопровождаться кодом причины, а на исходном маршрутизаторе происходит разрыв канала и возобновляение обработки вызова.
  - ◦ Если соединение между исходным маршрутизатором и исходящим шлюзом представляет собой аналоговый канал или магистраль с сигнализацией по отдельному каналу (channel-associated signaling, CAS), например E&M, T1 CAS, T1 FGD, то вызов должен быть возвращен на маршрутизатор с помощью второго канала на том же интерфейсе.

Маханизмы контроля приема вызовов (CAC)

Поскольку многие интересные аспекты контроля приема вызовов (CAC) в сетях с коммутацией пакетов уже рассматривались, некоторые из найденных решений нашли широкое применение. Ни одно из них не является полным и универсальным, но они могут быть полезны для решения различных аспектов этой задачи. В отличие от сетей с коммутацией пакетов, в которых резервируется свободный временный интервал DS0 для каждого отрезка маршрута вызова, определение свободных ресурсов сети для голосового вызова не является простой задачей. Данный раздел включает в себя следующие подразделы:

- Категории механизмов контроля приема вызовов
- Сравнение видов контроля приема вызовов, основанных на измерениях и ресурсах
- Краткий обзор функций контроля приема вызовов
- Технологические условия применения механизмов контроля приема вызовов
- Определение полосы пропускания голосовой информации
- Критерии оценки механизма контроля приема вызовов

Категории механизмов контроля приема вызовов

В оставшейся части этого документа содержится обсуждение десяти различных механизмов контроля приема вызовов, существующих в текущих версиях программного обеспечения Cisco IOS. Механизмы сгруппированы в следующие три категории:

- Локальные механизмы контроля приема вызовов — применение локальных механизмов контроля приема вызовов на исходящем шлюзе. Решение контроля приема вызовов основывается на информации узла, например, на состоянии исходящего соединения локальной или глобальной сети. Если соединение через локальную сеть с пакетной коммутацией отключено, то не существует точки выполнения общей логики принятия решения на основе состояния оставшейся части сети, т.к. сеть недоступна. В локальных механизмах содержатся элементы настройки для отключения других функций помимо фиксированного числа вызовов. Например, если разработчику сети уже известно, что по исходящему глобальному соединению не проходит более 5 вызовов из-за ограничения полосы пропускания, то видится логичным настроить локальный узел на разрешение не более пяти вызовов.
- Механизмы контроля приема вызовов на основе измерений (CAC) — использование методов контроля приема вызовов на основе измерений предполагает предварительный просмотр сети с пакетной коммутацией для измерения состояния сети и определения, возможен ли новый вызов. Измерение состояния сети подразумевает отправку зондов на IP-адрес назначения (обычно оконечный шлюз или контроллер шлюза), которые возвращаются на исходный шлюз с некоторой информацией о состоянии, собранной во время прохождения сети к месту назначения. Как правило, для передачи голоса интерес представляет информация о потере и задержке.
- Механизмы контроля приема вызовов на основе ресурсов — существует два типа механизмов на основе ресурсов: механизмы, рассчитывающие необходимые ресурсы, и механизмы, резервирующие ресурсы для вызова. К важным ресурсам относятся полоса пропускания соединения, временные интервалы DSP и DS0 на связующих каналах TDM, мощность центрального процессора и память. Некоторые из этих ресурсов можно ограничить на любом узле, через который проходит вызов до назначения.

Существует две дополнительные категории функций контроля приема вызовов, но они не решают вопросы инфраструктуры или проектирования сети и, следовательно, не обсуждаются в этом документе. Вместо этого, эти две категории контроля приема вызовов — безопасность и пользователь — фокусируются на вопросах, связанных с разрешением использовать сеть для вызова или для конечного пользователя, следующим образом:

- Безопасность — является ли данное устройство или шлюз законным в этой сети? Для решения этого вопроса контроля приема вызовов существуют механизмы аутентификации, в том числе протоколы, например H.235.
- Пользователь — авторизован ли конечный пользователь для использования сети? Для подтверждения авторизации существует два метода верификации CLID/ANI и PIN, обычно основанные на интерактивном речевом ответе.

Сравнение видов контроля приема вызовов, основанных на измерениях и ресурсах

Существует небольшое наложение локальных механизмов контроля приема вызовов и механизмов, просматривающих оставщуюся сеть для определения нелокальных условий. Таким образом, легче понять, почему полезны локальные механизмы и механизмы «скопления». Тем не менее, существует значительное наложение методов, основанных на измерениях, и методов, основанных на резервировании ресурсов, этих двух механизмов контроля приема вызовов, «высматривающих скопления». По этому поводу ведутся споры о том, какой метод лучше.

В таблице 1 представлено сравнение сильных и слабых сторон механизмов контроля приема вызовов на основе измерений и ресурсов. С помощью этой информации можно определить наилучший метод для конкретной сети.

Таблица 1. Сравнение возможностей методов контроля приема вызовов на основе измерений и ресурсов

Критерии	Методы на основе измерений	Методы на основе резервирования ресурсов
Топология сети	Независимые от топологии. Зонд перемещается по IP-адресу назначения — без информации об узлах, сетевых сегментах или доступности полосы пропускания на отдельных каналах.	Информация о топологии. Принимается во внимание доступность полосы пропускания на каждом узле и канале.
Прозрачность опорной сети	Прозрачный. Зонды представляют собой IP-пакеты, отправляемые по любой сети, включая SP-опорные сети и Интернет.	Чтобы методы резервирования оставались единственными полными методами, как это и предполагалось, необходимо настроить функцию на каждом интерфейсе пути, что означает наличие у клиента глобальной опорной сети и выполнение кода, реализующего эту функцию, на всех узлах. Наличие опорной сети целиком в некоторых случаях не практично, поэтому может рассматриваться гибридная топология с некоторыми компромиссами с полной природой метода.
Задержка после набора номера	Увеличение задержки после набора номера существует только для первого вызова, после этого информация о назначении кэшируется и периодичный зонд отправляется на IP-адрес назначения. Последующие вызовы либо разрешаются, либо	Увеличение задержки после набора номера существует для каждого вызова, т.к. резервирование протокола RSVP (Resource Reservation Protocol — протокол резервирования ресурсов) должно устанавливаться

	задерживаются на основе последней кэшированной информации.	перед завершением установки вызова.
Технологический уровень отрасли	Некоторые поставщики предлагают средства контроля приема вызовов, подобные эхозапросам. Для покупателей, знакомых с данной операцией, хорошо подходят методы на основе измерений.	—
Точность контроля приема вызовов	Периодичная частота выборки зондов может потенциально разрешить вызов при недостаточной полосе пропускания. Методы на основе измерений хорошо работают в сети с постепенными колебаниями трафика.	Использование протокола RSVP на всех узлах пути гарантирует наличие полосы пропускания для вызова на всем пути и в течение всей продолжительности вызова. Этот метод является единственным методом, достигающим подобного уровня точности.
Защита качества обслуживания голосовой передачи после разрешения вызова	Решение контроля приема вызовов основывается на статистике трафика, собранной зондом, перед разрешением вызова. После разрешения вызова качество вызова определяется эффективностью работы других механизмов качества обслуживания в сети.	Резервирование устанавливается для каждого вызова перед его разрешением. Следовательно, на качество вызова не влияют изменения условий сетевого трафика.
Служебные данные о сетевом трафике	Служебные данные о сети, собранные периодичными зондами, и отправляемые в кэшированное число IP-назначений. Как интервал, так и размер кэша можно	Служебные данные обмена сообщениями протокола RSVP для каждого вызова.

	контролировать настройкой.	
Масштабируемость	В большой сети отправка зондов на тысячи отдельных IP-назначений может оказаться непрактичной. Тем не менее, зонды можно отправлять на граничное оборудование глобальной сети, являющиеся *прокси-серверами* для более многочисленных получателей в широкополосной локальной сети за граничным оборудованием. Это обеспечивает существенную масштабируемость, т.к. глобальная сеть более склонна к перегрузке, чем локальная сеть, соединяющая несколько зданий.	Индивидуальное резервирование потоков важно в граничных каналах с низкой пропускной способностью. Однако индивидуальное резервирование каждого потока вызова может и не иметь смысла в широкополосных соединениях в опорной сети, такой как OC-12. Гибридная топология сети способна удовлетворить эту потребность, а дальнейшая масштабируемость может быть обеспечена новыми инструментами RSVP, разрабатываемыми в этой области.

Краткий обзор функций контроля приема вызовов

В таблице 2 содержится краткий обзор десяти различных механизмов контроля приема вызовов передачи голосовой информации, подробное обсуждение которых приводится в этом документе. В ней также перечисляется первая вверсия ПО Cisco IOS, в которой стала доступна эта функциональность.

Таблица 2. Функции контроля приема вызовов

Тип	Функция контроля приема вызовов	Версия ПО
Локальный		
	Физические ограничения канала DS0	Не зависит от ПО
	Максимальное число подключений на адресуемой точке вызова	11.3

	Полоса пропускания голосовых данных VoFR	12.0(4)T
	Согласование канала	12.1(2)T
	Функция Busyout для локальных вызовов (LVBO)	12.1(2)T
На основе измерений		
	Улучшенная функция Busyout для вызовов (AVBO)	12.1(3)T
	Функция перехода к аварийному режиму сети ТфОП	12.1(3)T
На основе ресурсов		
• Расчет ресурсов		
	Индикация наличия ресурсов	12.0.(5)T (AS5300) 12.1.(3)T (2600/3600)
	Полоса пропускания зоны контроллера шлюза	11.(3) (локальная зона) 12.1.(5)T (промежуточная зона)
• Резервирование ресурсов		
	Протокол резервирования ресурсов	12.1(5)T

Технологические условия применения механизмов контроля приема вызовов

При рассмотрении различных функций, доступных для решения конкретных проектных задач, таких как контроль приема вызовов, целесообразно сразу исключить механизмы, которые не относятся к рассматриваемой сетевой технологии. В таблице 3 приводится краткий обзор голосовых технологий, по отношению к которым применяются различные функции контроля приема вызовов.

Таблица 3. Поддержка технологий передачи голосовых данных механизмами контроля приема вызовов

Функция	VoIP H.323	VoIP SIP	VoIP MGCP	VoFR	VoATM	CM	Видео H.323
Физические ограничения канала DS0	Да	Да	Да	Да	Да	Нет	Нет
Максимальное число подключений	Да	Да	Да	Да	Да	Нет	Нет
Полоса пропускания голосовой информации	Нет	Нет	Нет	Да	Нет	Нет	Нет
Согласование канала	Да	Да	Да	Да	Да	Нет	Нет
Функция Busyout для локальных вызовов	Да	Да	Да	Да	Да	Нет	Нет
Улучшенная функция Busyout для вызовов	Да	Да	Да	Нет	Нет	Нет	Нет
Функция перехода к аварийному режиму сети ТфОП	Да	Да	Да	Нет	Нет	Нет	Нет
Индикация наличия ресурсов	Да	Нет	Нет	Нет	Нет	Нет	Нет[1]
Полоса пропускания зоны контроллера шлюза	Да	Нет	Нет	Нет	Нет	Да	Да
Протокол резервирования ресурсов	Да	Нет	Нет	Нет	Нет	Нет	Нет

1 Следует отметить, что возможности H.323 RAI идейно применяются для видеоприложений H.323. Однако в таблице указывается «Нет», потому что в данном документе рассматриваются голосовые шлюзы Cisco IOS, которые не генерируют индикаторы RAI для видеотрафика.

Определение полосы пропускания голосовой информации

Для успешного внедрения механизмов контроля приема вызовов в конкретной голосовой сети необходимо иметь четкое понимание того, какая полоса пропускания требуется для каждого вызова, чтобы зарезервировать сеть для требуемого числа вызовов и настроить механизмы контроля приема вызовов на отклонение вызовов, превышающих это число. Несмотря на опубликованные требования к полосе пропускания для каждого кодека, не существует единого ответа на вопрос о полосе пропускания для каждого вызова. Помимо используемых кодеков, точные требования к полосе пропускания определяют некоторые другие сетевые параметры.

Хотя целью данного документа не является всестороннее обсуждение расчета полосы пропускания, стоит напомнить некоторые моменты. На уровне физического интерфейса полоса пропускания голосовых данных, используемая для отдельного голосового вызова, зависит от следующих факторов:

- Используемая технология передачи голосовых данных (VoIP, VoATM, VoFR)
- Используемый канал передачи уровня 2 (Ethernet, serial/MLP, FR, ATM)
- Используемый кодек
- Метод сжатия заголовков (применим исключительно к VoIP)
- Обнаружение голосовой активности (VAD, известная также как Silence Suppression)

Для сетей ATM, использующих ячейки с фиксированной длиной, следует рассмотреть размер служебных данных полезной голосовой нагрузки (IP-пакеты для технологии VoIP в сетях ATM или полезная нагрузка кодека для VoATM), которые должны соответствовать ячейкам ATM.

В таблице 4 приводится краткий обзор наиболее общих сочетаний описанных факторов для сетей VoIP и получившихся в результате полос пропускания для вызова.

Таблица 4. Требования к полосе пропускания VoIP

Кодек	Полоса пропускания для кодека (Кбит/с)	Длина замера (мс)	Размер замера (байт)	Замеров на пакет	Размер IP-заголовка (байт)	Технология уровня 2	Размер заголовка уровня 2 (байт)	Требуемая полоса пропускания для голосового вызова (Кбит/с)
G.711	64	10	80	2	40	Ethernet	14	85.6
G.711	64	10	80	2	40	MLP/FR	6	82.4
G.711	64	10	80	2	2 (cRTP)	MLP/FR	6	67.2
G.729	8	10	10	2	40	Ethernet	14	29.6
G.729	8	10	10	2	40	MLP/FR	6	26.4
G.729	8	10	10	2	2 (cRTP)	MLP/FR	6	11,2

Для расчета полосы пропускания для любой комбинации факторов используется следующая формула:

```
Полоса пропускания голосовых данных = (Полезная нагрузка + L3 + L2) * 8 * pps
```

Элементы формулы соответствуют следующим значениям:

- Полезная нагрузка = полезная нагрузка в байтах, сгенерированная кодеком
- L3 = заголовки уровня 3 и более высоких уровней в байтах (0 для VoFR и VoATM)
- L2 = служебная информация заголовка канального уровня в байтах
- 8 = число бит на байт
- pps= число пакетов в секунду, генерируемых кодеком

В методе передачи уровня 2 содержится следующая служебная информация заголовков:

- Ethernet: 14 байт
- PPP и MLP: 6 байт
- FrameRelay: 6 байт
- ATM (AAL5): 5 байт (плюс излишняя информация ячейки)
- MLP через FrameRelay: 14 байт
- MLP по сетям ATM (AAL5): 5 байт на каждую ячейку ATM + 20 байт на инкапсуляцию IP-пакета для MLP и AAL5

Ниже приводятся примеры расчета полосы пропускания.

- G.729 / VoIP / MLPPP / без cRTP / без VAD: (20 + 40 + 6) * 8 * 50 = 26,4 Кбит/с
- G.729 / MLPPP / cRTP / без VAD: (20 + 2 + 6) * 8 * 50 = 11,2 Кбит/с
- G.729 / VoIPovFR / без cRTP / без VAD: (20 + 40 + 6) * 8 * 50 = 26,4 Кбит/с
- G.729 / VoFR / без VAD: (20 + 6) * 8 * 50 = 10,4 Кбит/с

Критерии оценки механизма контроля приема вызовов

Каждый из методов контроля приема вызовов описан в оставшейся части документа, поэтому далее приводится оценка каждого метода по отношению к различным критериям и факторам, что поможет определить наилучший или наиболее подходящий механизм контроля приема вызовов для проекта рассматриваемой сети.

В таблице 5 приводится описание критериев, используемых для оценки различных инструментов контроля приема вызовов.

Таблица 5. Критерии оценки механизмов контроля приема вызовов

Критерии оценки	Описание
Поддерживаемые технологии VoX	Технологии передачи голосовых данных (VoX), к которым применяется метод. Некоторые методы применяются к одной технологии, другие методы применяются к любой.
	Применяется ли метод только

Магистральная телефонная сеть или IP-телефония	между голосовыми шлюзами, соединенными с сетями ТфОП или офисной АТС, или его можно использовать только для оконечных IP-телефонов.
Платформы и версии	Платформы Cisco IOS, для которых доступна эта функция и официальная версия, в котором она была представлена.
Типы поддерживаемых каналов офисных АТС	Некоторые функции контроля приема вызовов зависят от типа канала ТфОП или офисной АТС, используемых в соединении или действующих независимо по каналам CCS, по сравнению с каналами CAS.
Сквозной, локальный или IP-скопления	Пределы видимости механизмов контроля приема вызовов. Некоторые механизмы работают локально только на исходящем шлюзе, другие учитывают скопления между источником и узлом назначения, некоторые рассматривают POTS-интерфейсы назначения, а некоторые работают насквозь.

Работа на уровне вызовов, интерфейсов или конечных пунктов	Различные механизмы включают различные элементы сети. Некоторые методы контроля приема вызовов работают с отдельными вызовами, другие функционируют в масштбае интерфейсов, конечных пунктов или IP-адресатов.
Знание топологии	Учитывает ли механизм контроля приема вызовов топологию сети и обеспечивает ли, как следствие, защиту подключений и узлов в топологии.
Гарантия качества обслуживания на протяжении вызова	Принимается ли механизмом единовременное решение перед разрешением вызова, защищается ли качество обслуживания вызова на протяжении всего вызова при помощи резервирования ресурсов.
Задержка после набора номера	Назначает ли механизм дополнительную задержку после набора номера из-за необходимости в дополнительном обмене сообщениями или обработке во время установления вызова.
	Использует ли метод

Служебная информация сети	дополнительные сообщения, необходимые для сбора информации для принятия решений механизмами контроля приема вызовов.

Локальные механизмы контроля приема вызовов

Локальные механизмы являются самыми простыми механизмами контроля приема вызовов для понимания и внедрения. Они функционируют на исходящем шлюзе и анализируют локальные условия узла. Как правило, служебная информация у таких механизмов небольшая, поэтому если любой из них обеспечивает необходимую функциональность, для внедрения более развитых возможностей есть мало причин. Но нельзя исключать вероятность того, что в сети значительного размера локальных механизмов будет недостаточно для удовлетворительной работы механизмов контроля приема вызовов.

В данном разделе обсуждаются пять локальных механизмов контроля приема вызовов.

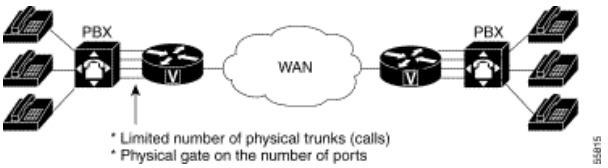
- Физические ограничения канала DS0
- Максимальное число подключений
- Полоса пропускания голосовой информации
- Согласование канала
- Функция Busyout для локальных вызовов

Физические ограничения канала DS0

Физическое ограничение DS0 представляет собой не специальную функцию программного обеспечения, а метод проектирования на основе физических ограничений интерфейса. Хотя эта функция кажется простой при сравнении с некоторыми другими, она, тем не менее, является основой для многих существующий сетей клиентов.

Например, если есть необходимость ограничить число вызовов из исходной офисной АТС на исходящий шлюз до пяти, то необходимо настроить или включить только пять временных интервалов на каналах T1 или E1 между маршрутизатором и исходящим шлюзом. На рис. 3 изображен этот процесс:

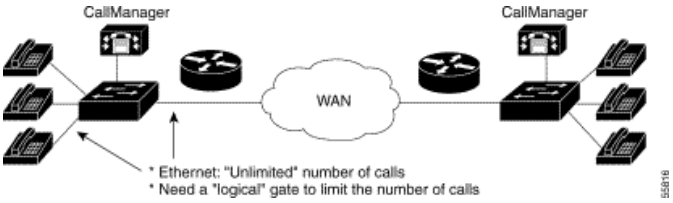
Рис. 3. Физическое ограничение DS0



Будучи локальным, данный метод проектирования контроля приема вызовов обеспечивает достаточную защиту выходного глобального соединения из исходящего шлюза. Данный механизм обладает таким же ограничением, как и другие локальные механизмы: он не обеспечивает защиты против доступности полосы пропускания на любом другом соединении сети. Он хорошо работает в простых радиальных топологиях и приемлемо — в более сложных многоуровневых иерархических сетях. Простое объяснение состоит в том, что максимальное число возможных вызовов (наихудший случай) на любом соединении опорной сети можно точно рассчитать, зная возможное число вызовов с каждого граничного участка и модель максимальной нагрузки между участками.

Хотя данный метод контроля приема вызовов хорошо работает в магистральных приложениях (связь между шлюзами), он не применяется в IP-телефонии из-за отсутсвия физического интерфейса TDM, на котором можно ограничить временные интервалы. Как показано на рис. 4, при возникновении вызова на устройстве в локальной среде возможность полосы пропускания физической среды намного превосходит возможности выходного интерфейса глобальной сети. Без наличия других программных средств в пункте соединения (обычно это граничный маршрутизатор глобальной сети) для «контроля» появления новых вызовов, нет физических возможностей задержки новых вызовов в сети.

Рис. 4. Приложения IP-телефонии



В общем случае ограничение физического проникновения каналов DS0 в сеть часто несет следующие преимущества:

- Не добавляет служебную информацию ЦП или полосы пропускания в сеть
- Хорошо работает со многими приложениями, позволяющими экономить на плате за подключение
- Преобладающий механизм контроля приема вызовов, используемый в сетях без платы за подключение на сегодняшнее время
- Защищает полосу пропускания на выходном соединении с глобальной сетью локального узла
- Может обеспечить *прогнозную* защиту в опорной сети на основе моделей максимальной нагрузки

Метод контроля приема вызовов с помощью физических каналов DS0 обладает следующими ограничениями:

- Не работает с приложениями IP-телефонии
- Ограничен относительно простыми топологиями
- Не реагирует на разрывы соединений или изменение сетевых условий

В таблице 6 представлена оценка механизма ограничений физических каналов DS0 по критериям оценки контроля приема вызовов, описанных в этом документе ранее.

Таблица 6. Краткая информация о механизмах ограничения физических каналов DS0

Критерии оценки	Значение
Поддерживаются технологии VoX	Не зависят от используемой технологии VoX
Магистральные сети и IP-телефония	Только магистральные сети
Платформа (версия)	Все голосовые шлюзы и версии ПО Cisco IOS
Поддерживаемые типы каналов АТС	Все
Сквозной, локальный или IP-скопления	Локальный
Масштаб:	Отдельные

отдельные вызовы, интерфейсы или конечные пункты	каналы DS0 (магистрали) (на каждый вызов)
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет
Служебная информация сети	Нет

Максимальное число подключений

В механизме контроля приема вызовов на основе максимального числа подключений предполагается использовать настройку **max-conn** (максимальное число подключений) адресуемой точки вызова на исходящем шлюзе для ограничения числа одновременных соединений (вызовов), которые могут быть активными на этой адресуемой точке вызова в одно время.

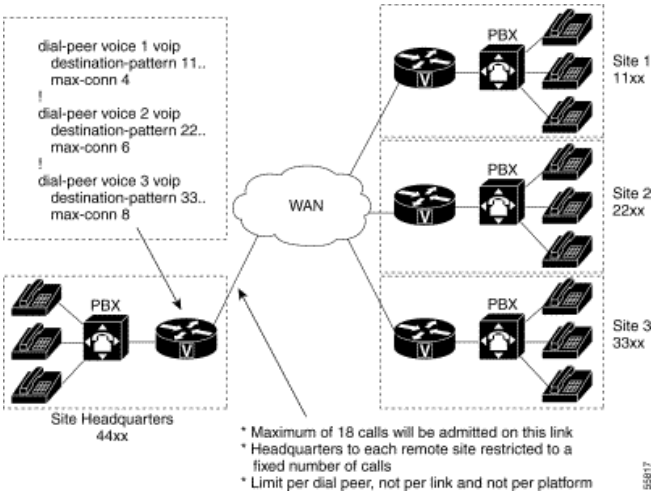
Этот инструмент легко использовать, но число проблем проектирования сети, которые он может решить, ограничено. Инструмент применяется к адресуемой точке вызова, поэтому ограничить общее число вызовов, которые может обрабатывать исходящий шлюз, не представляется возможным, пока не будет ограничено число адресуемых точек вызова, и на каждой из них не будет использована команда **max-conn** (максимальное число подключений).

При наличии такого ограничения команда **max-conn** реализует действенный метод контроля приема вызовов, как минимум, по двум следующим сценариям:

- Для сравнительно небольшого числа адресуемых точек вызова, направляющих вызовы на выходное глобальное соединение, общее число отдельных операторов коммутирующих узлов **max-conn** (максимальное число подключений) обеспечит максимальное количество вызовов, которые могут быть активными в одно время по соединению с глобальной сетью.
- Если целью проекта является ограничение максимального количества вызовов между узлами, а не защита полосы пропускания выходного канала с глобальной сетью, то эта возможность очень удобна в использовании при условии, что адресуемые точки вызова выстроены таким образом, что для каждого удаленного узла имеется только одна адресуемая точка вызова, направляющая на него вызовы.

На рис. 5 отображен пример такого типа сети: три удаленных узла, для каждого в плане набора есть узнаваемые первые цифры. Исходящие адресуемые точки вызова VoIP на узлах головных офисов соотносят удаленные узлы для каждого. Число вызовов на удаленных узлах 1, 2 и 3 будет ограничено до соответственно 4, 6 и 8. Следовательно, на выходном канале глобальной сети может быть не более 18 активных вызовов одновременно. В данной конфигурации подход к обеспечению полосы пропускания соединения для такого числа вызовов отличается предусмотрительностью.

Рис. 5. Число максимальных подключений на адресуемой точке вызова



Параметр максимального числа подключений можно также использовать на адресуемых точках вызова POTS для ограничения числа вызовов, которые могут быть активными на соединениях T1/E1 с АТС/ТфОП, если есть необходимость обеспечить все временные интервалы для этого подключения, но ограничить число вызовов до меньшего числа, чем физическое число временных интервалов.

На примере настройки, приведенном ниже, у вызова VoIP, соответствующего команде **dial-peer voice 800 voip**, все пакеты голосовой нагрузки будут иметь IP-приоритет 5, что означает, что три наиболее значимых бита IP-байта типа обслуживания (ToS) будут установлены на 101. Первая адресуемая точка вызова настроена на получение максимум 24 одновременных вызова. Любой дополнительный вызов будет отправлен второй адресуемой точкой вызова на ТфОП.

```
dial-peer voice 800 voip
!Определяет эту группу поиска как имеющую основной приоритет.
preference 1
!Устанавливает максимальное число подключений (активный контроль принятия).
max-conn 24
 destination-pattern 83123...
 ip precedence 5
 ipv4 target:172.17.251.28
!
dial-peer voice 600 pots
!Определяет эту группу поиска как имеющую второй приоритет.
 preference 2
 destination-pattern 83123...
direct-inward-dial
  port 0:D
!Добавляет префикс 99 перед набираемым номером для оповещения офисной АТС о переполнении сети ТфОП.
prefix 9983123
```

Хотя во многих сценариях эта возможность является полезной, у нее можно отметить следующие недостатки:

- Хотя она и обеспечивает некоторую защиту выходного подключения к глобальной сети голосового шлюза, защиты соединения в опорной сети не существует или она является незначительной.
- Она не работает с приложениями IP-телефонии, которые не используют пользовательские адресуемые точки вызова.
- Ее использование ограничено сетями с простой топологией.
- Она не реагирует на разрывы соединений или изменение сетевых условий.

В таблице 7 приводится оценка механизма максимального числа подключений по критериям оценки контроля приема вызовов, описанных ранее в данном документе.

Таблица 7. Краткая информация о механизме контроля максимального числа подключений

Критерии оценки	Значение
Поддерживаемые технологии VoX	Все оборудование VoX, использующее адресуемые точки вызова

Магистральные сети и IP-телефония	Только магистральные применения
Платформа (версия)	Все голосовые шлюзы и версии ПО Cisco IOS
Поддерживаемые типы каналов АТС	Все
Сквозной, локальный или IP-скопления	Локальный
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	На одну адресуемую точку вызова
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет
Служебная информация сети	Нет

Полоса пропускания голосовой информации

В настройках VoFR при установке отдельной полосы пропускания для вызовов VoFR используется команда настройки интерфейса **frame-relay voice-bandwidth** в классе таблиц FrameRelay. Этот метод обеспечения полосы пропускания работает сходным образом, что и функции резервирования полосы пропускания для общих потоков трафика IP RTP Priority и Low Latency Queueing (LLQ). Однако, с помощью команды **frame-relay voice-bandwidth** также достигается контроль приема вызовов, а с помощью общих команд управления очередью — нет.

Команда **frame-relay voice-bandwidth** может обеспечить контроль приема вызовов, т.к. метод VoFR является технологией уровня 2. С помощью заголовков FRF.11 (голос) или FRF.3.1 (данные) программное обеспечение Frame Relay может определить, к какому типу принадлежит кадр — к голосовому или к типу данных. С помощью программного обеспечения можно также узнать, к какому вызову принадлежит тот или иной кадр, потому что в последующих полях заголовка содержится информация о канале Channel Identification (CID) и полезных данных. С помощью команды **frame-relay voice-bandwidth** устанавливается отдельная полоса пропускания для голоса, а также отклоняется следующий вызов, если этот дополнительный вызов может привести к превышению всей полосы пропускания, выделенной на голосовые данные.

Этот метод контроля приема вызовов используется только в том случае, если технология VoFR является жизнеспособной в данной

сети. Следует также отметить, что по умолчанию размер полосы пропускания голосовых данных устанавливается равным 0, поэтому если не указано резервирование полосы пропускания, то передача голосовых вызовов по соединениям глобальной сети отключена. По полосе пропускания, указанной с помощью этой команды, не передается служебный сигнальный трафик, а только голосовой полезный трафик.

В примере настройки, приведенном ниже, обеспечивается контроль приема вызовов для VoFR при скорости 24 Кбит/с, что достаточно для двух вызовов G.729 со скоростью 10,4 Кбит/с каждый.

```
interface Serial0/0
 encapsulation frame-relay
 no fair-queue
 frame-relay traffic-shaping
!
interface Serial0/0.1 point-to-point
  frame-relay interface-dlci 16
  class vofr
!
map-class frame vofr
  frame cir 60000
  frame bc 600
  frame frag 80
  frame fair-queue
!Скорости в 24 Кбит/с достаточно для двух вызовов G.729 на скорости 10,4 Кбит/с каждый.
  frame-relay voice-bandwidth 24000
```

В таблице 9 приводится оценка механизма полосы пропускания голосовых данных по критериям оценки контроля приема вызовов, описанных ранее в этом документе.

Таблица 8. Краткая информация о механизме оценки полосы пропускания голосовых данных

Критерии оценки	Значение
Поддерживаемые технологии VoX	VoFR
Магистральные сети и IP-телефония	Только магистральные применения
Платформа (версия)	Маршрутизаторы Cisco 2600, 3600, 3810 и 7200, Cisco IOS, выпуск 12.0(4)T
Поддерживаемые типы каналов АТС	Все
Сквозной, локальный или IP-скопления	Локальный
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	На вызов, на PVC
Знание топологии	Нет

Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет
Служебная информация сети	Нет

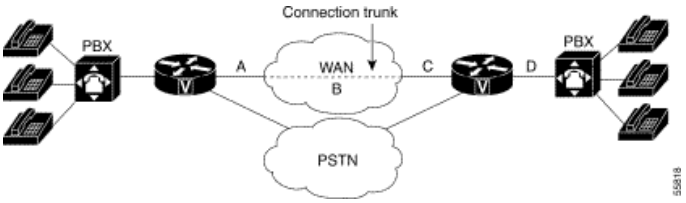
Согласование канала

Согласование канала обеспечивает большую функциональность, чем только контроль доступности вызовов, но здесь обсуждаются только аспекты контроля приема вызовов. Согласование каналов можно использовать в сетях типа *connection trunk* (сети с постоянным голосовым подключением через VoX-часть сети) для мониторинга за состоянием VoX-соединением и возврата сигнала «занято» на исходящую офисную АТС в случае сбоя VoX-соединения.

Эта функция ограничена в своих возможностях, т.к. применяется только в сетях типа «connection trunk». Тем не менее, большинство функций контроля приема вызовов применяется только к коммутируемым сетям.

Внедрение контроля приема вызовов в настройку сети типа «connection trunk» немного отличается от внедрения в коммутируемых сетях, т.к. соединения VoX между двумя шлюзами являются постоянными, как показано на рис. 6. Следовательно, полоса пропускания уже установлена, назначена и должна быть доступна, иначе соединения типа «connection trunk» не будут установлены должным образом.

Рис. 6. Согласование каналов



Уникальным свойством согласования каналов по сравнению с функциями контроля приема вызовов является его видимость не только полного состояния глобальной сети, но и состояния соединений POTS на оконечной стороне сети. На рис. 6 показано, что в случае сбоя на участке A, B, C или D на исходящий шлюз поступает информация об этом, и на исходную офисную АТС вернется сигнал о занятости канала, чтобы запустить механизм маршрутизации на источнике. Эта информация обрабатывается как часть дежурного сообщения, которое генерируется в настройках канала соединения.

Можно настроить точную модель битов для генерирования на исходной АТС. Биты ABCD можно настроить на указание особых сигналов занятости линии или сигнала «не обслуживается», которые будут распознаваться на исходной АТС и вызывать ответные действия.

Согласование каналов, следовательно, не относится к числу рассмотренных ранее функций, работающих в масштабе отдельных вызовов. Это функция обратного информирования АТС о занятости магистрали (или OOS). Если в глобальной сети происходит сбой, канал на офисной АТС больше не обслуживается, поэтому вызовы по каналу становятся невозможными, пока не восстановится подключение с глобальной сетью.

В таблице 9 представлена оценка механизма согласования каналов по критериям оценки контроля приема вызовов, описанных ранее в этом документе.

Таблица 9. Краткая информация о механизме согласования каналов

Критерии оценки	Значение
Поддерживаемые технологии VoX	VoIP/H.323, VoFR, VoATM (только конфигурация канала подключения)
Магистральные сети и IP-телефония	Только магистральные применения
Платформа (версия)	Маршрутизаторы серии Cisco 2600 и 3600, концентраторы с множественным доступом Cisco MC3810, Cisco IOS, выпуск 12.1(3)T
Поддерживаемые типа каналов АТС	Аналоговые каналы и каналы CAS
Сквозной, локальный или IP-скопления	Локальный
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	Отдельные телефонные интерфейсы
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет
Служебная информация сети	Нет, используются существующие ранее дежурные каналы

подключения

Функция Busyout для локальных вызовов

Некоторые механизмы контроля приема вызовов называются механизмами *trunk busy-back* (возврата сигнала занятости канала). Первым механизмом, с которым мы познакомились, было согласование каналов, описанное в предыдущем разделе. Та функциональность работала только в сетях каналов подключения. Подобная возможность требуется и для коммутируемых сетей, и первой из двух функций, которые реализуют эту возможность, является LVBO (Local Voice Busy-Out — функция Busyout для локальных вызовов).

Функция LVBO позволяет полностью отключить обслуживание канального соединения АТС к подключенному шлюзу в тех случаях, когда состояние глобальной сети считается недостаточным для передачи голосового трафика. Данный метод обладает следующими преимуществами:

- Нет необходимости отдельно отклонять каждый вызов, вызывая при этом задержку после набора номера.
- Предупреждает необходимость возврата отклоненного вызова на исходную АТС, используя множественные DS0-интервалы для одного вызова.
- Хорошо работает с перенаправлением отклоненных вызовов с помощью офисной АТС без встроенных логических функций или функций, не настроенных должным образом.
- Решает проблемы возврата АТС, отправляя вызов обратно на третий канал DS0, на ту же линию T1/E1, на шлюз, на котором уже был отклонен и возвращен вызов (состояние, называемое *тромбонированием*). Типы общих каналов сигнализации управляют этим вопросом возврата, т.к. информация о коде причины может вернуться на АТС, на которой запускается процедура перемаршрутизации. Однако на каналах сигнализации по отдельному каналу (CAS) АТС не известно, где возник сбой, и пока цифры не будут обработаны на шлюзе, система управления АТС не сможет принять решение о маршрутизации вызова на другую группу каналов.

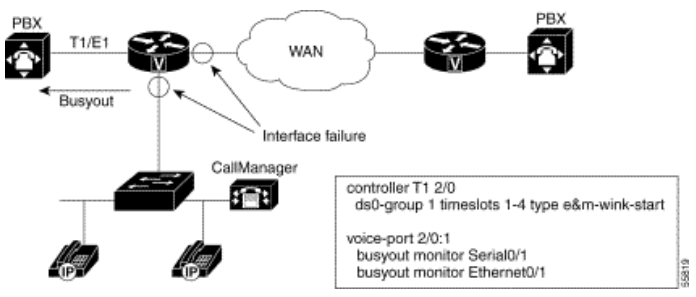
Благодаря функции LVBO обеспечивается возможность мониторинга состояния различных сетевых интерфейсов, локальной и глобальной сети на исходящем шлюзе, и возвращается сигнал о занятости канала на АТС в случае сбоя на одном из контролируемых соединений. Контролироваться может до 32 интерфейсов; если меняется состояние одного или всех интерфейсов, при соответствующей настройке шлюз отправляет сигнал о занятости канала на АТС. Причина, по которой эта функция называется *локальной* функцией busyout для голосовых вызовов, заключается в возможности наблюдать только локальные соединения. Эта функция не позволяет просматривать сеть за соединениями локального шлюза.

В программном обеспечении, существующем в настоящее время, функция LVBO работает только на каналах CAS и аналоговых АТС/ТфОП. На общих каналах сигнализации (CCS) возможность кода причины можно использовать для отправки на маршрутизатор АТС информации о необходимости перенаправить отклоненный вызов. Коммутация LVBO может осуществляться в двух режимах.

- Для назначения отдельным голосовым портам состояния отключения (busyout)
- Для назначения всему каналу T1/E1 статуса отключения (busyout)

На рис. 7 отображена работа функции LVBO с примерной настройкой. В этом примере на исходящем шлюзе происходит наблюдение за двумя интерфейсами, интерфейсом Ethernet e0/1 и WAN s0/1 от имени голосового порта 2/0:1и каналом T1 CAS на АТС. Как показано на рисунке, эта возможность доступна только в случае, если исходное устройство представляет собой интерфейс АТС/ТфОП, хотя устройство назначения может быть любым, в том числе IP-голосовое устройство.

Рис. 7. Работа функции busyout для локальных голосовых вызовов



Для функции LVBO применяются следующие ограничения:

- Локальная видимость реализована только в последнем ПО (Cisco IOS версии 12.2), она наблюдает только интерфейсы локальной сети Ethernet (не Fast Ethernet)
- Применяется только в аналоговых каналах и каналах CAS

В таблице 10 приводится оценка механизма busyout для локальных голосовых вызовов по критериям оценки контроля приема вызовов, описанных ранее в этом документе.

Таблица 10. Краткая информация о механизме согласования каналов

Критерии оценки	Значение
Поддерживаемые технологии VoX	Все
Магистральные сети и IP-телефония	Магистральные сети (вызовы от офисной АТС на IP-телефоны)
Платформа (версия)	Маршрутизаторы серии Cisco 2600 и 3600, концентраторы с множественным доступом MC3810, ПО Cisco IOS, выпуск 12.1(2)T
Поддерживаемые типы каналов АТС	Аналоговые и каналы CAS
Сквозной, локальный или IP-скопления	Локальный
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	Отдельные интерфейсы глобальной, локальной сети или телефонии
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет

Служебная информация сети	Нет

Механизмы контроля приема вызовов на основе измерений

В данном разделе документа внимание концентрируется на следующих методах контроля приема вызовов на основе измерений:

- Улучшенная функция Busyout для вызовов
- Функция перехода к аварийному режиму сети ТфОП

Данные два типа механизмов контроля приема вызовов являются первыми, добавляющими видимость в саму сеть, помимо обеспечения локальной информации на исходящем шлюзе, как описано в предыдущих разделах.

Перед обсуждением действующих возможностей в этой категории, необходимо предоставить базовую информацию о программных зондах агентов гарантированного обслуживания (Service Assurance Agent, SAA), т.к. этот метод является основополагающим, используемым в методах контроля приема вызовов на основе измерений. Программные зонды SAA проходят сеть и достигают заданного IP-назначения, измеряя характеристики потерь и задержки сети по пути прохождения. Такие значения возвращаются в исходящий шлюз и используются для принятия решений о состоянии сети и ее способности передавать голосовой вызов.

Следует отметить приведенные ниже свойства механизмов контроля приема вызовов на основе измерений, которые следуют из использования программных зондов SAA.

- Все программные зонды SAA представляют собой IP-пакеты, следующие к IP-месту назначения, поэтому все методы контроля приема вызовов на основе измерений применяются исключительно для VoIP, включая технологии VoIP over Frame Relay и VoIP over ATM.
- Т.к. программные зонды посылаются по сети, генерируется определенное количество служебного трафика при сборе информации, необходимой для контроля приема вызовов.
- Если для принятия решения о возможности вызова механизмов приема вызовов требуется ожидание отправки и возврата программного зонда, возникает небольшая дополнительная задержка вызова после набора номера. В хорошо спроектированной сети это будет незначительным.

Агент гарантированного обслуживания Cisco

Агент гарантированного обслуживания (SAA) представляет собой возможность сетевого управления, интегрированную в ПО Cisco IOS и обеспечивающую механизм анализа перегрузки сети. Эта функциональность также лежит в основе множества других возможностей ПО Cisco IOS. Она не внедрялась с целью доведения контроля приема вызовов до конца и не входит в пакет механизмов контроля приема вызовов. Но ее возможности измерения задержки сети и потери пакетов полезны как строительные блоки, на которых основаны функции контроля приема вызовов. Функция агента гарантированного обслуживания (SAA) является расширением функции генератора отчетов о времени реагирования (Response Time Reporter, RTR), которая была включена в более ранние версии ПО Cisco IOS.

Программные зонды агента гарантированного обслуживания (SAA) не предоставляют информации ни о конфигурации, ни о доступности полосы пропускания. Тем не менее, если полоса пропускания во время соединения в любом месте прохождения вызова перегружена, то разумно будет допустить, что задержка пакета или потеря значений, которые возвращает зонд, отразит это состояние, даже в косвенном виде.

Сравнение программных зондов агента гарантированного обслуживания (SAA) и эхозапросов

Концепция программных зондов имеет много общего с популярным механизмом эхозапросов *(ping)* в IP-сетях, но программные зонды намного сложнее. Пакеты Агента гарантированного обслуживания можно формировать и настраивать таким образом, чтобы они не отличались от пакетов сети, в которой они измеряют трафик, в данном случае — от голосовых пакетов. Пакет эхозапроса по определению относится к категории трафика, передаваемого только при наличии возможности, и даже в случае установки приоритета IP он не похож на голосовой пакет ни размером, ни протоколом. Пакет эхозапроса не будет также рассматриваться как голосовой пакет и механизмами качества обслуживания, развернутыми в сети. Следовательно, измерение задержки и потерь путем эхозапроса представляет собой весьма грубый и отражающим наихудшие условия способ оценки влияния сети на проходящий по ней голосовой пакет. С развитием сложных механизмов качества обслуживания в опорных сетях эхозапросы становятся абсолютно бесполезны для

оценки способности сети передавать голосовую информацию.

Протокол SAA

Протокол SAA является протоколом типа клиент-сервер на уровне UDP. На клиенте формируется и отправляется программный зонд, а на целевом устройстве, на котором включен генератор отчетов о времени реагирования, зонд возвращается отправителю. Зонды SAA, используемые для контроля приема вызовов, отправляются на случайно выбранные порты из верхней части списка аудиопортов, предусмотренных для UDP (с номерами от 16384 до 32767). Размер пакета зависит от кодека, который используется для вызова. По желанию можно установить приоритет IP. Весь заголовок RTP/UDP/IP используется как заголовок реального голосового пакета. По умолчанию зондом SAA используется порт RTCP (нечетный номер порта RTP), но по желанию зонд также можно настроить на использование порта среды RTP (четный номер порта RTP).

Метод SAA был впервые введен в Cisco IOS версии 12.0(7)T. Он применяется в большинстве старших моделей платформ маршрутизаторов Cisco (например, в сериях Cisco 7200 и 7500), платформы более низкого класса его не поддерживают (например, маршрутизатор Cisco 1750). На момент написания данного документа ни маршрутизаторы кабельного доступа Cisco, ни IP-телефоны не поддерживали зонды SAA и не реагировали на них.

Рассчитанный запланированный показатель ухудшения качества передачи

Международная организация ITU стандартизировала ухудшение качества передачи в сети в документе ITU G.113. В этом стандарте дается определение запланированного показателя ухудшения качества передачи (ICPIF), который вычисляется на основе данных о задержке сети и потере пакетов. Функция ICPIF выдает единое значение, которое можно использовать как критерий оценки ухудшения качества сети.

В стандарте ITU G.113 содержатся следующие интерпретации значений ICPIF:

- 5: Очень хорошо
- 10: Хорошо
- 20: Достаточно
- 30: Предельный случай
- 45: Исключительный предельный случай
- 55: Вероятна сильная реакция клиентов

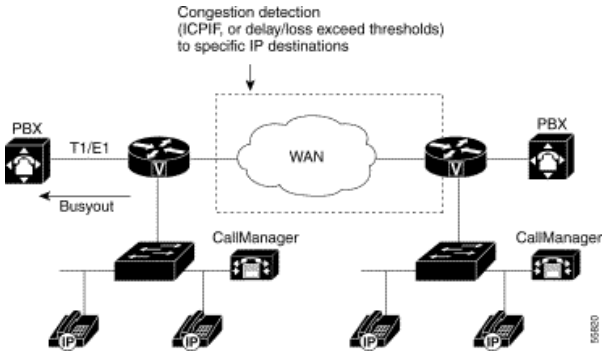
Информация о задержке и потере, собранная зондом SAA, используется для расчета значения ICPIF, которое позже станет отправной точкой для принятия решения механизмом контроля приема вызовов, основанного либо на интерпретации описанных требований ITU, либо на требованиях индивидуальной клиентской сети.

Улучшенная функция Busyout для вызовов (Advanced Voice Busyout)

Функция AVBO является улучшенной функцией LVBO. Хотя функция LVBO обеспечивает отключение на основе локальных условий исходящего шлюза, в функцию добавлена возможность запуска программного зонда SAA по одному или более настроенному IP-назначению. Информация, собранная зондом — либо выраженные значения потерь и задержки, либо пороговое значение перегрузки ICPIF — может использоваться для инициации отключения соединения на офисной АТС.

Следовательно, функция AVBO предоставляет возможность отключить канал офисной АТС или отдельные голосовые порты на основе текущего состояния IP-сети. Эта возможность показана на рис. 8.

Рис. 8. Функция Advanced Voice Busyout



На примере настройки ниже приводится примерная конфигурация функции AVBO на канале T1 CAS офисной АТС.

```
controller T1 2/0
 ds0-group 1 timeslots 1-4 type e&m-immediate-start
!
voice-port 2/0:1
  voice-class busyout 4
!
voice class busyout 4
 busyout monitor Serial0/1
 busyout monitor Ethernet0/1
 busyout monitor probe 1.6.6.48 codec g729r8 icpif 10
```

При использовании улучшенной функции busyout для голосовых вызовов следует помнить о следующих ограничениях:

- Результат функции busyout, основанный на зондах (измерениях), не является абсолютным, существуют условия, при которых случается ложный положительный результат.
- IP-адреса, наблюдаемые зондом, являются статически настроенными, как показано на примере конфигурации. Необходимо вручную убедиться, что эти IP-адреса представляют собой действительные адреса, на которые отправляются вызовы. Не существует автоматической координации между настройкой зонда и действительным IP-назначением, куда адресуемые точки вызова VoIP или программа управления шлюзом может направлять вызовы.
- Узел назначения (устройство с IP-адресом, на который отправляется зонд) *должен поддерживать* функцию ответчика SAA.
- Эта функциональность не может отправлять сигнал о занятости канала на офисную АТС на основе состояния телефонного канала на удаленном узле, функция наблюдает только IP-сеть.
- Функции, основанные на работе зондов SAA, не будут хорошо работать в сетях, где нагрузка трафика значительно меняется за короткий отрезок времени.
- Как и в случае с функцией LVBO, эта возможность применяется только к аналоговым каналам и каналам CAS, каналы CCS пока не поддерживаются.

В таблице 11 приводится оценка механизма AVBO по критериям оценки контроля приема вызовов, описанных в этом документе ранее.

Таблица 11. Краткая информация о механизме AVBO

Критерии оценки	Значение
Поддерживаемые технологии VoX	Только VoIP
Магистральные сети и IP-телефония	Магистральные сети (вызовы от офисной АТС на IP-телефоны)
Платформа (версия)	Серии 2600, 3600, MC3810; версия 12.1(3)T
Поддерживаемые	

типы каналов АТС	Аналоговые и каналы CAS
Сквозной, локальный или IP-скопления	IP-скопления
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	На IP-адрес назначения
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет
Служебная информация сети	Периодичная отправка программных зондов SAA

Функция перехода к аварийному режиму сети ТфОП (PSTN Fallback)

Название функции перехода к аварийному режиму сети ТфОП является в некоторой степени неверным, т.к. вызов можно перенаправить на любой вариант маршрутизации, описанный ранее в этом докумнете, а не только в сеть ТфОП. Но даже если вызов перенаправлен в сеть ТфОП, то перенаправление может быть выполнено исходящим шлюзом или офисной АТС, соединенной с исходящим шлюзом, в зависимости от настройки. По этой причине данная функциональность иногда называется функцией перехода к аварийному режиму работы сети VoIP.

В отличие от AVBO, функция перехода к аварийному режиму работы сети ТфОП представляет собой механизм вызова системы контроля приема вызовов, т.к. эта функция не отключает канал и не отправляет информацию на офисную АТС о том, что IP-скопление не может принять вызов. Решение механизма контроля приема вызовов запускается только при попытке установления вызова.

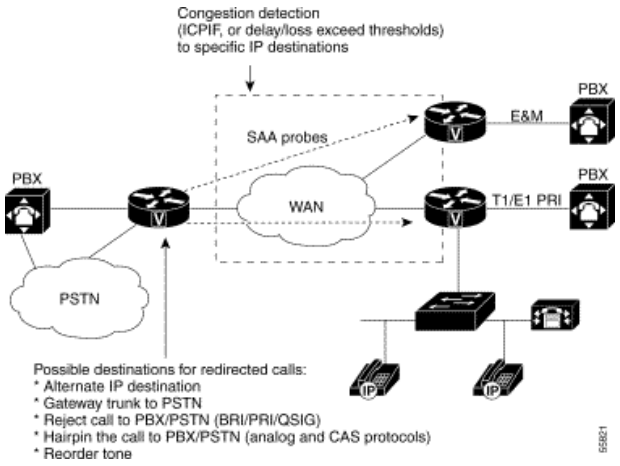
Функция перехода к аварийному режиму работы сети ТфОП основана на зондах SAA, поэтому обладает всеми достоинствами и недостатками методов на основе измерений. Эта функция обеспечивает необыкновенную гибкость, принимая решения контроля приема вызовов на основе любого типа IP-сети, включая Интернет. Все IP-сети передают пакеты зондов SAA как обычный IP-пакет. Следовательно, не имеет значения, состоит ли опорная сеть клиента из одной или нескольких сетей провайдеров услуг, Интернета или любых сочетаний этих типов сетей. Единственное требование заключается в том, что устройство назначения (имеющее IP-адрес, на который отправляется зонд) поддерживает функционирование ответчика SAA.

Конечно устройство должно быть частью сети клиента на конечном узле, а между ними должна находиться опорная сеть поставщика услуг. Функцию перехода к аварийному режиму работы нельзя использовать при вызовах на IP-телефоны и приложения VoIP на основе компьютера, но ее можно использовать косвенно, если место назначения находится за маршрутизатором Cisco IOS, поддерживающим функцию ответчика SAA. Для конечного устройства самого по себе не требуется поддержка возможности перехода к аварийному режиму работы сети ТфОП, это функция относится только к исходящему шлюзу. Все, что необходимо — это ответчик зонда SAA.

Зонды SAA, используемые для функции перехода к аварийному режиму работы сети ТфОП

Как показано на рис. 9, при попытке вызова на исходящем шлюзе используется значение перегрузки сети для IP-назначений для приема или отклонения вызова. Значения перегрузки для задержки, потери или ICPIF получаются при отправке зонда SAA на IP-адрес, на который инициируется вызов. Пороговые значения для отклонения вызова настраиваются на исходящем шлюзе.

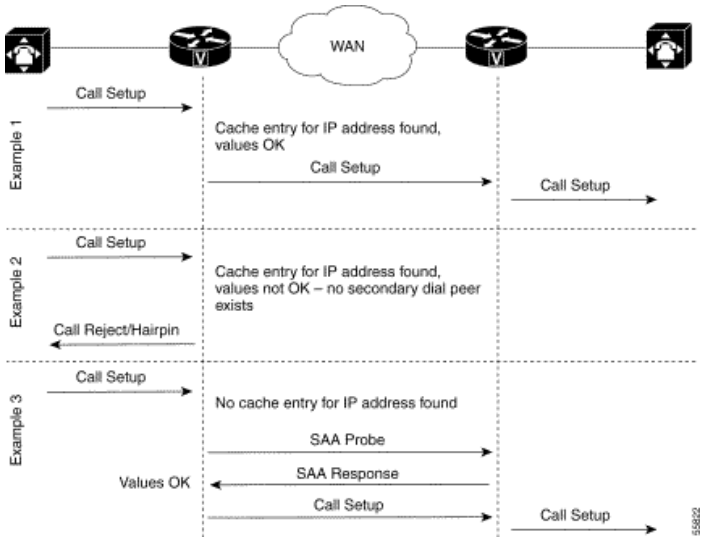
Рис. 9. Функция перехода к аварийному режиму работы сети ТфОП



Кэширование конечных IP-адресов

В отличие от AVBO, функция перехода к аварийному режиму работы сети STN не требует постоянной настройки IP-адресов назначений. Программное обеспечение поддерживает кэш, размер которого можно настраивать, в котором отслеживаются самые последние используемые IP-адреса назначений, на которые отправляются вызовы. Если IP-адрес места назначения нового вызова найден в кэше, решение контроля приема вызовов будет принято немедленно (на примерах 1 и 2 рисунка 10 показаны сценарии «вызов разрешен» и «вызов отклонен» соответственно). Если в кэше записи нет, то запускается новый зонд, и установка вызова откладывается до получения ответа зонда (пример 3 на рис. 10). Следовательно, дополнительная задержка после набора номера происходит *только* при первом вызове на новый IP-адрес назначения.

Рис. 10. Установка вызова функцией перехода к аварийному режиму работы сети ТфОП



После появления в кэше записи IP-адреса назначения на этот адрес будут периодически отправляться программные зонды с настраиваемым временным интервалов для обновления информации в кэше. Если на этот IP-адрес больше не было вызовов, то запись в кэше устаревает, и отправление зондов по этому адресу прекращается. Таким образом, функция перехода к аварийному режиму работы сети ТфОП динамично подстраивается к IP-адресам назначения, на которых просматривается активность вызовов.

Формат программных зондов SAA

Каждый зонд состоит из множества пакетов — это является настраиваемым параметром этой функции Значения задержки, потери и CPIF, поступающие в кэш для всех IP-адресов назначения, усредняются от всех ответчиков.

При использовании для вызова кодеков G.729 и G.711 размер пакетов зонда подстраивается под размер голосового пакета для этого кодека. С другими кодеками используются зонды типа G.711. В версиях ПО Cisco IOS после версии 12.1(3)T поддерживается выбор других кодеков с собственными зондами.

Приоритет IP пакетов зондов можно также настраивать для настройки на приоритет голосового пакета. Данный параметр необходимо установить равным приоритету IP, который используется для других пакетов голосовой среды в сети.

Настройка функции перехода в аварийный режим работы сети ТфОП

Настройка функции перехода к аварийному режиму работы ТфОП применяется только для тех вызовов, которые были отправлены с исходящего шлюза и не имеет отношения к вызовам, полученным на шлюзе. Узел назначения (как правило, но не обязательно оконечный шлюз) должен быть настроен на работу функции SAA Responder. В большинстве сетей шлюзы генерируют вызовы к друг другу, и каждый шлюз является и исходящим, и оконечным. Но в некоторых сетях (например, сетях провайдеров услуг) направление вызовов является односторонним, либо входящим, либо исходящим.

Настройка функции перехода к аварийному режиму работы сети ТфОП происходит на общем уровне и, следовательно, применяется ко всем вызовам шлюза. Невозможно выборочно применить функцию перехода к аварийному режиму работы сети ТфОП к вызовам, инициированным определенными интерфейсами ТфОП/АТС.

Для включения функции перехода к аварийному режиму работы сети ТфОП необходимо ввести следующие команды общей настройки:

- Исходящий шлюз: команда **call fallback**
- Узел назначения: команда **rtr responder**

Для команды **call feedback** существуют следующие ключи и значения по умолчанию:

Ключевое слово команды call fallback	**Значение ключевого слова**	**Значение по умолчанию**
cache-size	Настраивает размер кэша	128
cache-timeout	Настраивает истечение срока кэша	600c
instantaneous-value-weight	Настраивает немедленный вес значения	66
jitter-probe	Настраивает параметры джиттера программного зонда	
• num-packets	Настраивает число пакетов в зонде	15
• precedence	Настраивает приоритет	2

	пакетов в зонде	
• priority-queue	Настройка отправки зондов через голосовую очередь с приоритетом (PQ)	выкл.
key-chain	Настраивает цепочку ключей MD5	нет
map	Настраивает сопоставление IP-адресов	нет
probe-timeout	Настраивает истечение срока зонда	30с
threshold	Настраивает порог задержки/потерь или ICPIF	
• delay n loss m	Настраивает порог задержки	нет
• icpif n	Настраивает порог ICPIF	10

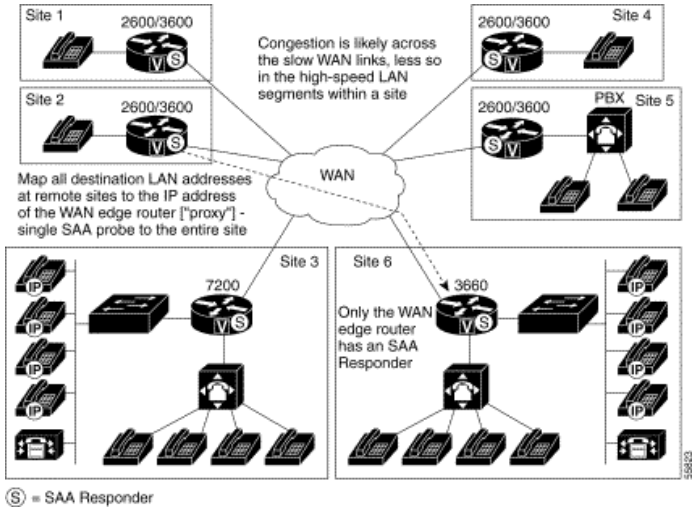
Масштабируемость функции перехода к аварийному режиму работы сети ТфОП

Клиенты с большими сетями часто озабочены проблемой перехода к аварийному режиму работы сети ТфОП, вызывающего большой трафик программных зондов в сети В сетях меньшего размера оконечный шлюз можно использовать в качества узла назначения зондов. Другими словами, IP-адреса, хранящиеся в кэше исходящего шлюза, будут совпадать с IP-адресами оконечных шлюзов, на которые направлен голосовой трафик.

Тем не менее, для больших узлов или локальных узлов с множественными оконечными шлюзами или для узлов с назначениями в виде IP-телефонов или компьютерных приложений, для узлов с граничными маршрутизаторами глобальной сети, отдельных от оконечных шлюзов, IP-адреса мест назначения голосового трафика могут быть преобразованы в меньший набор адресов назначения зондов, хранящихся в кэше следующим образом.

- Рассмотрим пример на основе рисунка 11. На узле 6 расположено большое количество IP-телефонов, каждому присвоен уникальный IP-адрес. Если с узла 1 идет вызов на IP-телефон на узле 6, то нет необходимости хранить записи для каждого IP-адреса назначения узла 6 в кэше узла 1 и отправлять отдельный зонд на каждый IP-адрес. Все IP-адреса узла, на которые были отправлены вызовы, могут быть преобразованы в IP-адреса граничного оборудования глобальной сети на узле 6, и один зонд, направленный из узла 1 в узел 6, может собрать всю информацию о всех вызовах на узел 6 для механизма контроля приема вызовов. Такой же принцип применяется, если на узле 6 установлено множество оконечных шлюзов. Все их IP-адреса могут быть отправлены на граничный маршрутизатор глобальной сети, который может быть (а может и не быть) граничным шлюзом со своими правами.

Рис. 11. Масштабируемость функции перехода к аварийному режиму работы сети ТфОП



Трафик зондов, следовательно, можно существенно снизить за счет отправки зондов на IP-адреса, которые представляют часть сети с высокой вероятностью перегрузки (опорная сеть глобальной сети или граничное оборудование глобальной сети), и не отправляя трафик зондов по высокоскоростной локальной или локальной опорной сети, которая менее подвержена перегрузкам. Похожий механизм масштабируемости также обеспечивает механизм для поддержки IP-адресов назначений, которые не поддерживают работу ответчика SAA.

Краткая информация о функции перехода к аварийному режиму работы сети ТфОП

Функция перехода к аварийному режиму работы сети ТфОП является широко применяемым, независимым от топологии механизмом контроля приема вызовов, который можно использовать в любой опорной сети, независимо от того, имеется ли у клинета собственное оборудования для опорной сети или собственная технология, используемая в опорной сети, или оборудование сети принадлежит поставщику.

При проектировании сети необходимо рассмотреть следующие характеристики функции перехода к режиму аварийной работы сети ТфОП:

- Функция перехода к аварийному режиму работы ТфОП используется только в сетях VoIP, т.к. она основана на IP-зондах.
- Функция перехода к аварийному режиму работы сети ТфОП не перемаршрутизует уже выполненные вызовы при изменении состояния сети.
- Небольшое увеличение задержки после набора номера произойдет только при первом вызове, когда адрес назначения еще не находится в кэше.
- Между таймером зонда SAA и временными настройками H.225 нет взаимодействия, отправка зонда SAA происходит до отправки установки вызова H.323 в место назначения, а срабатывание таймера H.225 происходит после отправки команды установки вызова H.323.
- Функция перехода к аварийному режиму работы сети ТфОП основана на измерениях, и не является, следовательно, абсолютной. Она будет хорошо работать при стабильном трафике, характеризующемся постепенным увеличением и спадом, и плохо — в сетях с колебаниями трафика с пульсирующими увеличениями и спадами.
- Из-за периодичной природы зондов может быть принято ошибочное решение механизма контроля приема вызовов на основе устаревшей информации.
- Отправку зондов на *прокси* можно использовать при сопоставлении IP-адресов назначения на меньшее число IP-адресов узлов, расположенных между исходящим шлюзом и оконечными шлюзами.
- Зонды не выполняют измерение полосы пропускания — только измерение задержки и потерь.
- Аутентификацию цепочки ключей алгоритма MD5 можно настроить на безопасный уровень, что гарантирует запуск зонда только доверенными источниками, которые смогут сорвать атаки типа «отказ от обслуживания» со стороны недоверенных источников, инициирующих большое количество зондов.

В таблице 12 приводится оценка механизма перехода к аварийному режиму работы сети ТфОП по критериям оценки контроля приема вызовов, описанным ранее в этом документе.

Table 12. Краткая информация о механизме перехода к аварийному режиму работы сети ТфОП

Критерии оценки	Значение

Поддерживаемые технологии VoX	Только VoIP
Магистральные сети и IP-телефония	Магистральные сети (вызовы от офисной АТС на IP-телефоны)
Платформа (версия)	Cisco 2600/3600, MC3810: версия 12.1.(3)T AS5300: версия 12.2.(2)T Ответчик SAA с поддержкой 7200/7500
Поддерживаемые типа каналов АТС	• Все типы сигнализации каналов АТС/ТфОП (аналоговый, цифровые CAS и CCS) • Для аналоговых и цифровых каналов CAS — альтернативный IP-адрес назначения, возврат • Для цифровых CCS — отклонение вызова на АТС или сеть ТфОП для перемаршрутизации
Сквозной, локальный или IP-скопления	IP-скопления
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	Отдельные активные/кэшированные IP-адреса назначения
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Только для первого вызова, который инициирует зонд

Служебная информация сети	Периодичная отправка программных зондов SAA

Механизмы контроля приема вызовов на основе ресурсов

В данном разделе обсуждаются следующие три метода контроля приема вызовов на основе ресурсов:

- Индикация наличия ресурсов
- Полоса пропускания зоны контроллера шлюза
- Протокол резервирования ресурсов

Как и методы контроля приема вызовов на основе измерений, эти методы увеличивают возможности видимости самой сети, в дополнение к локальной информации на исходящем шлюзе, что можно использовать для контроля приема вызовов, как обсуждалось в предыдущих разделах.

Сравнение методов расчета и резервирования ресурсов

Существует два типа механизмов контроля приема вызовов на основе ресурсов.

- Те, которые наблюдают за использованием определенных ресурсов и расчитывают значение, влияющее на решение контроля приема вызовов
- Те, которые резервируют ресурсы для вызова

Только механизмы резервирования могут гарантировать качество обслуживания в продолжение вызова. Все другие механизмы контроля приема вызовов (локальные, основанные на измерениях, основанные на расчете ресурсов) просто принимают однократное решение перед установкой вызова на основе информации о состоянии сети в данное время.

Для голосовых вызовов представляют интерес следующие ресурсы:

- Временной интервал DS0 на исходящем и оконечном каналах TDM
- Ресурсы DSP на исходном и оконечном шлюзах
- Использование узлами ЦП — обычно шлюзами
- Использование узлами памяти — обычно шлюзами
- Доступность полосы пропускания на одном или более соединениях по пути следования вызова

В текущих версиях ПО Cisco IOS (версия 12.2) метод контроля приема вызовов на основе расчета ресурсов, обсуждаемый в следующих разделах, рассматривает доступность DS0 и DSP оконечного шлюза (RAI) вместе с полосой пропускания на высоком уровне (управление полосой пропускания зоны управления шлюзом). В настоящее время имеется единственный механизм резервирования ресурсов, который анализирует только доступность полосы пропускания.

Индикация наличия ресурсов

Индикация наличия ресурсов (Resource Availability Indication, RAI) представляет собой функциональность H.323v2, описывающую сообщение RAS, которое отправляется оконечным шлюзом на контроллер шлюза для доставки информации о текущей возможности шлюза обработать больше вызовов. В контроллере шлюза нет информации об отдельных ресурсах или типах ресурсов, которые анализирует шлюз. Это простая индикация типа «да» или «нет», отправляемая оконечным шлюзом для контроля, маршрутизируются ли последующие вызовы на шлюз.

Как механизм контроля приема вызовов, индикация наличия ресурсов (RAI) является уникальной по своей возможности предоставлять информацию об оконечных соединениях POTS. Другие механизмы, обсуждаемые ранее, позволяют принять решение контроля приема вызовов на основе локальной информации на исходящем шлюзе и состоянии скопления IP-адресов между исходящим и оконечным шлюзом. Ни один другой механизм контроля приема вызовов не способен анализировать доступность ресурсов для прекращения вызова POTS на оконечном шлюзе, и в этом заключается ценность механизма индикации наличия ресурсов.

Такая индикация происходит между шлюзом и контроллером шлюза, поэтому механизм RAI применяется только в голосовых сетях H.323, структура которых предполагает использование контроллера шлюза. Еще одна уникальность RAI заключается в том, что

решение механизма контроля приема вызовов определяется оконечным шлюзом. Во всех остальных методах решение механизма контроля приема вызовов определяется исходящим шлюзом или контроллером шлюза.

Расчет ресурсов на шлюзе

На шлюзе выполняются расчеты, которые используются для принятия решения типа «да» или «нет». Разные платформы шлюза могут использовать разные алгоритмы В стандарте H.323 не прописаны ни расчеты, ни ресурсы, которые должны быть включены в расчеты. Он просто указывает формат сообщения RAI и предписывает контроллеру шлюза остановить маршрутизацию вызовов на шлюз, который показывает невозможность принимать дальнейшие вызовы до того момента, пока шлюз не проинформирует контроллер шлюза о возможности снова обрабатывать вызовы.

Для измерения доступности ресурсов для вызовов с использованием маршрутизаторов серий Cisco 2600 и 3600, алгоритмом расчета каждый вызов рассматривается как единица по следующей формуле:

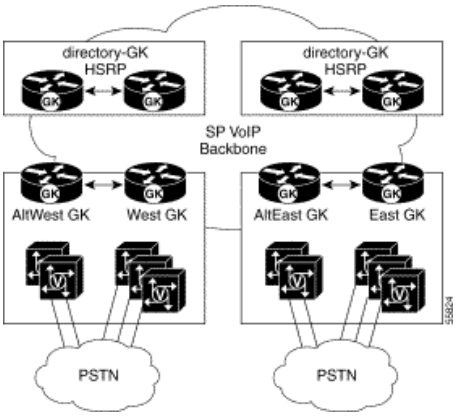
- Каждый свободный сигнал DS0 является единицей
- Каждый процессор DSP высокой степени сложности считается двумя единицами.
- Каждый процессор DSP средней степени сложности считается четырьмя единицами

Индикация RAI рассчитывается по отдельным платформам, а не по интерфейсам T1/E1 или платам (по сетевым модулям или, в частности, по NMM-HDV, в случае использования маршрутизаторов серий Cisco 2600 и 3600). В расчет включены только сигналы DS0, проходящие по сети VoIP до коммутирующего узла.

Где и как используется механизм RAI в сетях провайдеров услуг

Механизм RAI является характерной чертой в сетях провайдеров услуг, которая обеспечивает услуги вызова VoIP, такие как вызовы с помощью дебитовой и кредитовой карты, и телефонные вызовы VoIP на большое расстояние. Общая структура таких сетей показана на рис. 12.

Рис. 12. Топология сети провайдера услуг VoIP



По всему миру существуют точки входа в сеть, в которых на стойках со шлюзами (обычно это серверы доступа Cisco AS5300) происходит подключение к сети ТфОП по каналам T1/E1 — часто каналам PRI Маршрутизация вызова управляется через несколько уровней контроллеров шлюза, как показано на рис. 12. Голосовой вызов имеет большой объем, и эти шлюзы обрабатывают только голосовой трафик, никакой трафик данных, за исключением минимума IP-маршрутизации и трафика управления сетью, не допускается.

Когда клиент на западе страны подключается к сети и набирает номер на востоке страны, контроллер шлюза на востоке должен выбрать шлюз на востоке, у которого имеется доступный ТфОП канал для прекращения вызова. В противном случае вызов не состоится. Если вызов не состоялся, исходящий шлюз должен повторить вызов, или клиент должен заново набрать номер. В любом случае нет гарантии, что снова не будет выбран такой же оконечный шлюз с переполненной мощностью.

Оба сценария являются неэффективными и обеспечивают плохое качество обслуживания. Следовательно, важно, чтобы вызовы не маршрутизировались программой управления шлюзом на оконечный шлюз, который не сможет обработать вызов не из-за ограничений IP, а из-за возможностей канала ТфОП.

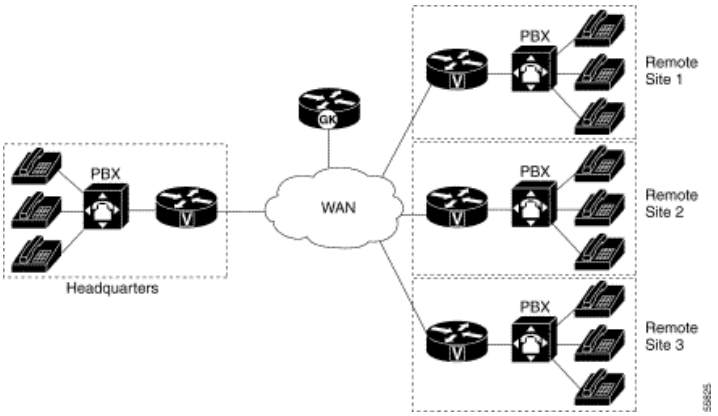
Вообще, вызовы могут быть сбалансированы по нагрузке между оконечными шлюзами в этой зоне контроллера шлюза. Но шлюзы

могут характеризоваться различными уровнями возможностей каналов T1/E1 и, при балансировании нагрузки, на одном шлюзе может оказаться меньше ресурсов, чем на другом. В такой ситуации использование RAI является обязательным, поэтому перегруженный оконечный шлюз может отправить контроллеру шлюза сигнал о том, что он занят и не может больше принимать вызовы.

Где и как используется механизм RAI в корпоративных сетях

Вообще, механизм RAI в корпоративных сетях применяется меньше, чем в сетях провайдеров услуг, где часто встречается всего один шлюз на каждом узле, как показано на рис. 13. Это почти всегда так для большого количества небольших узлов, которые соединяются с намного меньшим числом больших узлов в обычной корпоративной сети. Даже на больших узлах могут быть множество каналов T1/E1 до подключенной офисной АТС, но редко — множество шлюзов.

Рис. 13. Топология корпоративной VoIP сети



Если только один шлюз может завершить вызов *вызванному пользователю* (где *вызванным пользователем* является определенная АТС и определенный шлюз в сети), то механизм RAI не обеспечивает логику сети, которая уже недоступна. При отсутствии альтернативного шлюза для обработки излишних вызовов вызов всегда не удается каждый раз, когда оконечный шлюз занят. Кроме того, в корпоративных сетях вероятность перегрузки обычно выше в IP-скоплениях, чем в множестве оконечных POTS каналах. В сетях провайдеров услуг, которые обсуждались ранее, перегрузки чаще встречаются в оконечных каналах POTS, чем в IP-скоплениях.

Несмотря на эти ограничения, механизм RAI все же можно использовать в корпоративных сетях при условии, что соединения шлюз-АТС на удаленных узлах являются каналами T1/E1. Если оконечный шлюз занят, вместо выбора альтернативного шлюза запустится механизм ТфОП маршрутизации, как в случае с сетями провайдеров услуг.

Операция RAI

Обсуждения того, где и как используется механизм RAI в сетях провайдеров услуг и предприятий четко показывают, что этот механизм наиболее полезен в ситуациях, когда множественные оконечные шлюзы могут связаться с одним телефонным номером (вызванным). Тем не менее, механизм RAI имеет значение в любой ситуации, где есть желание помешать маршрутизации вызова на шлюз, на котором нет возможностей POTS завершить вызов.

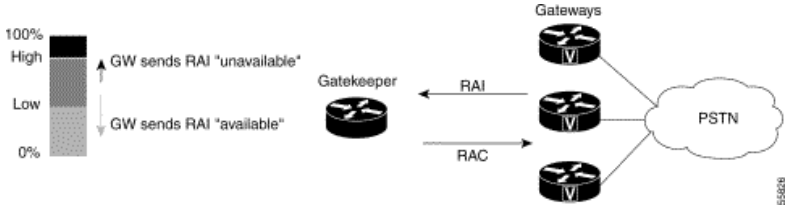
При получении контроллером шлюза сообщения о недоступности RAI от шлюза, контроллер удаляет шлюз из алгоритма выбора шлюза для телефонных номеров, которые этот шлюз могли бы нормально завершить. После сообщения механизма RAI о доступности, полученного позже, этот шлюз будет возвращен алгоритму выбора шлюза в контроллере шлюза.

Механизм RAI является необязательной функцией H.323. Следовательно, при развертывании сети важно убедиться, что и рассматриваемый шлюз, и контроллер шлюза поддерживают эту возможность. Контроллеры шлюза Cisco поддерживают RAI, поддержка RAI шлюзами Cisco подробно описана в последующих разделах данного документа.

Конфигурация RAI

Механизм RAI на шлюзе настроен на высокий и низкий порог, как показано на рис. 14. Если использование ресурса по алгоритму расчета, указанному ранее, превышает высокий порог (значение в процентах), на контроллер шлюза отправляется сообщение о недоступности RAI. Если доступность ресурса падает ниже нижнего порога, на контроллер шлюза отправляется сообщение о доступности RAI. Для предотвращения запаздывания по причине появления или разрыва соединения одного вызова необходимо сдвинуть процентное значение верхнего и нижнего порога в настройках.

Рис. 14. Настройка RAI



Для настройки RAI необходимо использовать команду настройки шлюза **resource threshold** [**all**] [**high** *%-value*] [**low** *%-value*].

Поддержка платформы RAI

Серверы доступа Cisco AS5300 поддерживают RAI, начиная с Cisco IOS версии 12.0(5)T, маршрутизаторы серий Cisco 2600 и 3600, начиная с версии 12.1.3T, поддерживают RAI только на соединениях T1/E1, но не на аналоговых каналах. Другие шлюзы Cisco IOS пока не поддерживают RAI (версии 12.1(5)T и 12.2). В расчет RAI включаются сигналы DSP и DS0, и результаты могут отличаться в зависимости от платформы. В ПО, используемом в настоящее время, в сообщения о доступности RAI не включаются данные для памяти и ЦП.

В таблице 13 приводится оценка механизма RAI по критериям контроля приема вызовов, описанным ранее в этом документе.

Таблица 13. Краткая информация о механизме RAI

Критерии оценки	Значение
Поддерживаемые технологии VoX	Только VoIP
Магистральные сети и IP-телефония	• Магистральные сети • Возможна IP-телефония, но CM не поддерживает механизм RAI.
Платформа (версия)	• Сервер доступа Cisco AS5300: Cisco IOS версии 12.0(5)T • Каналы T1/E1, маршрутизаторы серий Cisco 2600 и 3600: Cisco IOS версии 12.1(3)T
Поддерживаемые типы каналов АТС	Все
Сквозной,	Локальный на оконечном шлюзе

локальный или IP-скопления	(ресурсы DSP и DS0; зависим от платформы алгоритма)
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	На шлюз
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет
Служебная информация сети	Случайное переключение RAI между шлюзом и контроллером шлюза

Полоса пропускания зоны контроллера шлюза

Другим механизмом контроля приема вызовов, специфичным для сетей H.323 с контроллером шлюза, является возможность такого контроллера накладывать ограничение на полосу пропускания в зонах. Разные уровни ПО Cisco IOS обеспечивают различные возможности этой функции. В Cisco IOS версий 12.1(5)T и 12.2 контроллер шлюза способен ограничивать как полосы пропускания вызова в локальной зоне, так и полосу пропускания, используемую между своей собственной зоной и любыми удаленными зонами в сети.

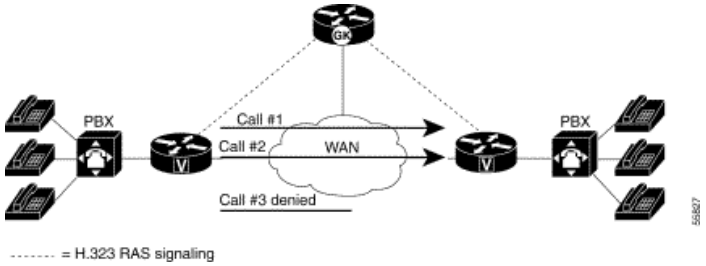
Функционирование полосы пропускания зоны контроллера шлюза

Двумя основными функциями контроллера шлюза H.323 является управление преобразованием адресов и зоной. Возможность управления полосой пропускания зоны позволяет контроллеру шлюзов контролировать число одновременных активных вызовов. Чтобы понять, как работает эта возможность, предположим, что голосовой вызов занимает 64 Кбит/с полосы пропускания. Вопрос о том, как ограничение *числа вызовов* на шлюзе преобразуется в действительную полосу пропускания, используемую для этих вызовов, будет рассматриваться в последующих разделах.

Однозональная топология

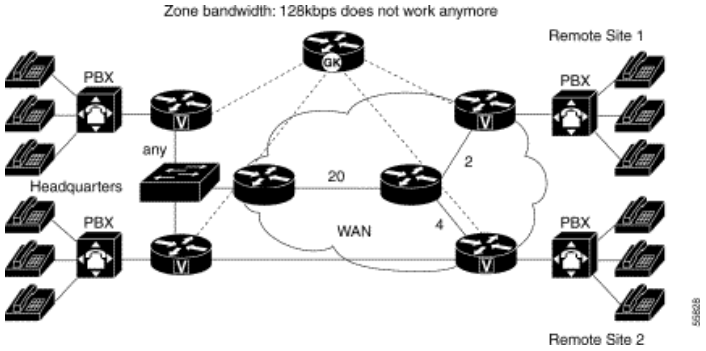
На рис. 15 отображена сеть с однозональным контроллером шлюза, имеющим два шлюза. Эта сеть демонстрирует механизм контроля приема вызовов контроллера шлюза в самом простом виде. Если полоса пропускания глобальной сети подключения между двумя шлюзами не позволяет обрабатывать более двух вызовов, то необходимо настроить контроллер шлюза на отклонение третьего вызова. Предполагая, что для каждого вызова требуется 64 Кбит/с, потребуется настроить контроллер шлюза на ограничение полосы пропускания зоны до 128 Кбит/с для достижения контроля приема вызовов в этой простой топологии.

Рис. 15. Простая однозональная топология



Однако большинство сетей не так просты как те, которые отображены на рис. 15. На рис. 16 отображена более сложная топология, но все же настроенная как однозональная сеть. В этой топологии для отрезков в скоплениях глобальных сетей выделена отдельная полоса пропускания, следовательно, для каждого отрезка характерно свое число вызовов, обрабатываемых на нем. Количество отрезков глобальной сети на рис. 16 показывает максимальное число вызовов, проводимых по этому отрезку.

Рис. 16. Сложная однозональная топология

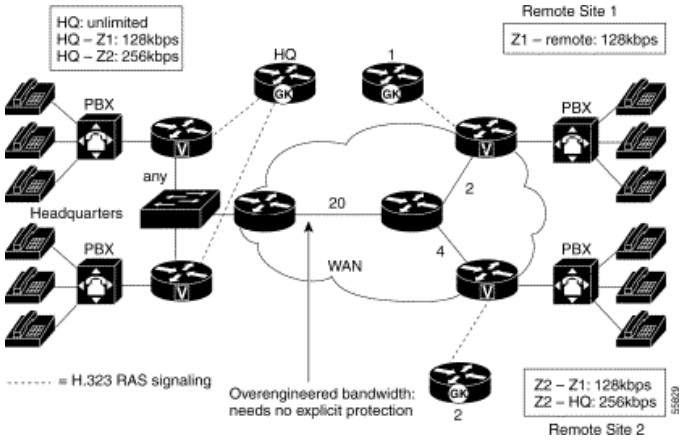


Будем теперь считать, что значение максимальной полосы пропускания контроллера шлюза настроено на 128 Кбит/с, не допуская, таким образом, более двух одновременных вызовов. Желательно, чтобы оба вызова затрагивали узел 1 — контроллер шлюза защитит полосу пропускания подключения по глобальной сети от узла 1 до пункта соединения глобальных сетей, не разрешая более двух вызовов по этому соединению. Но если оба вызова происходят в пределах головных узлов, то нет причин допускать только два вызова, т.к. в опорной локальной сети большая полоса пропускания.

Многозональная топология сети

Для решения проблемы однозональной сети снижения возможностей сети до глобальной сети малой производительности можно спроектировать сеть с множеством зон контроллеров шлюза. Хорошей отправной точкой является создание одной зоны на узел, как показано на рис. 17.

Рис. 17. Простая многозонная топология корпоративной сети



Контроллер шлюза узла 1 ограничивает число активных вызовов на узле 1 (независимо от места инициации и назначения вызова) до двух (128 Кбит/с). На узле 1 расположен только один шлюз, поэтому нет необходимости настраивать ограничение для внутризонального голосового трафика. Весь трафик между зонами ограничен двумя вызовами, чтобы защитить подключение глобальной сети к узлу 1.

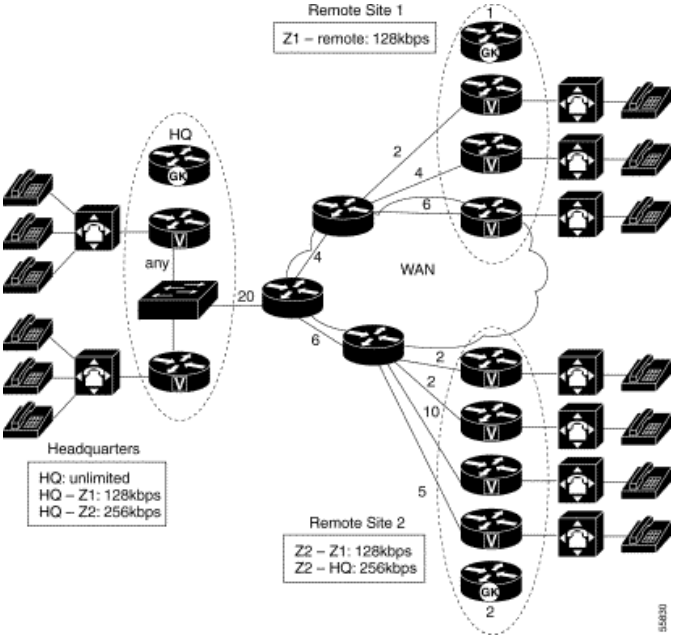
На узле 2 расположен один шлюз, следовательно, нет необходимости ограничивать внутризональный трафик. Для следующих сценариев существуют отдельные ограничения трафика между зонами.

- Вызовы между узлом 2 и головным узлом (ограничивающим фактором здесь служит максимальное число вызовов, равное четырем на соединении между глобальной сетью и узлом 2).
- Вызовы между узлом 1 и узлом 2 (ограничивающим фактором здесь является максимальное число вызовов, равное 2 на соединении между глобальной сетью и узлом 1).

На головном узле используется такая же настройка, за исключением того, что в пределах узла вызовы не ограничены — не из-за того, что имеется единственный шлюз, а из-за достаточно широкой полосы пропускания между шлюзами на этом узле.

На топологии сети рисунка 17 контроллер шлюза контроля приема вызовов обеспечивает достаточную степень детализации для защиты голосового трафика по низкоскоростным соединениям с глобальной сетью. Но рассмотрим другую топологию сети, в которой на одну зону приходится множество шлюзов, и на каждом шлюзе (удаленном узле) имеется отдельное соединение по глобальной сети с точкой соединения. Такая топология сети показана на рис. 18.

Рис. 18. Комплексная многозональная топология корпоративной сети

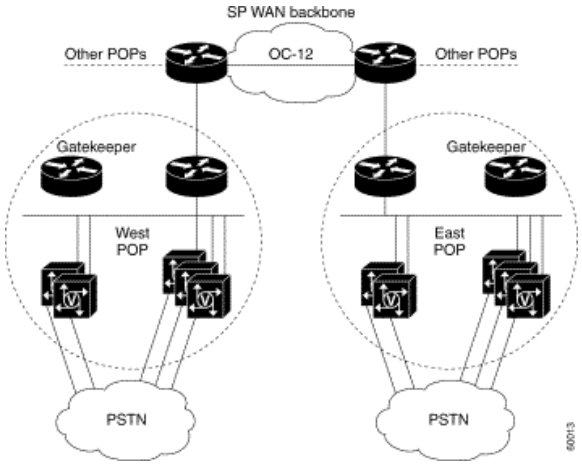


Из трех шлюзов на удаленном узле 1 низкоскоростной канал доступа к глобальной сети может обрабатывать максимум два одновременных вызова. Ограничение полосы пропускания настраивается не для шлюза, а для зоны, поэтому у механизма контроля приема вызовов контроллера шлюза нет возможности ограничить вызовы на определенные шлюзы этой зоны. Поэтому наилучшим решением будет настроить сеть для канала с наименьшим общим знаменателем: для узлов 1 и 2 наименьшим общим знаменателем является полоса пропускания в 128 Кбит/с или два вызова.

Такая настройка гарантирует должное качество голосовой передачи все время, но это является расточительным по отношению к шлюзам, которые могут пропускать более двух вызовов, не перегружая при этом полосу пропускания глобальной сети. При такой настройке сети механизм контроля приема вызовов сработает слишком рано и отразит определенные вызовы на сеть ТфОП, когда фактически они должны были бы передаваться по глобальной сети. Поэтому при такой топологии недостаточно одного лишь механизма контроля приема вызовов контроллера шлюза для обеспечения качества передачи голоса по глобальной сети и оптимизации использования полосы пропускания всех соединений глобальной сети.

Последней рассматриваемой настройкой является сеть провайдера услуг, в которой шлюзы в точках входа в сеть соединены с оконечным маршрутизатором глобальной сети по технологии Fast Ethernet, что показано на рис. 19.

Рис. 19. Топология сети провайдера услуг с множеством шлюзов на зону



В этой сети одного лишь механизма контроля приема вызовов контроллера шлюза вновь недостаточно, даже несмотря на то, что на зону приходится множество шлюзов, потому что соединения на конкретные шлюзы в этой зоне не являются соединениями, которые нуждаются в защите. Полосой пропускания, которую необходимо защищать, является соединение доступа в глобальную сеть с опорной сетью, где собирается голосовой трафик от всех шлюзов. Ограничение полосы пропускания контроллера шлюза будет несомненно ограничивать число вызовов по этому каналу. Предполагается, что опорное соединение OC-12 тщательно спроектировано и не требует защиты.

Итак, многозональная сеть с контроллером шлюза обладает следующими характеристиками механизма контроля приема вызовов:

- Можно защитить полосу пропускания глобальной сети на каждом соединяющем узле при условии, что каждый узел является зоной. (Для небольших удаленных узлов в корпоративных сетях это часто преобразуется в одну зону на шлюз, что не всегда можно считать практичным проектным решением.)
- Полосу пропускания в пределах узла можно при необходимости защитить, но часто это малозначимо, потому что на один узел приходится один шлюз (небольшие удаленные офисы или точки входа клиентского оборудования в службу поставщика услуг, управляемую по сети), или из-за высокоскоростного подключения по локальной сети между шлюзами (крупные узлы или точки входа в сеть поставщиков услуг).
- Механизм контроля приема вызовов контроллера шлюза представляет собой метод, который хорошо подходит для ограничения числа вызовов между узлами.
- Механизм контроля приема вызовов контроллера шлюза не может защитить полосу пропускания на сегментах глобальной сети, не связанных напрямую с зонами. Например, опорное соединение, отмеченное 20 вызовами на простой корпоративной топологии, показанной на рис. 17, нельзя защитить с помощью механизма контроля приема вызовов контроллера шлюза, если не следовать принципу наименьшего общего знаменателя. Поэтому на этом канале была избыточно зарезервирована полоса пропускания для максимального количества возможных вызовов.

Структура одной зоны на один шлюз

Структура одной зоны на один шлюз предлагает подробную детализацию механизма контроля приема вызовов контроллером шлюза, поэтому стоит рассмотреть ее подробнее. В корпоративных сетях такая сеть имеет смысл со следующих точек зрения:

- Географический анализ
- Контроль приема вызовов для защиты канала доступа глобальной сети в узел, содержащий один шлюз.
- Планы набора часто совпадают с узлами, поэтому префикс зоны легко переводится на шлюз, обслуживающий данный узел, если шлюз равен зоне.

Контроллер шлюза является логическим, а не физическим объектом. Следовательно, каждый контроллер шлюза не означает отдельный блок в сети, а попросту соответствует оператору отдельной локальной зоны в настройке.

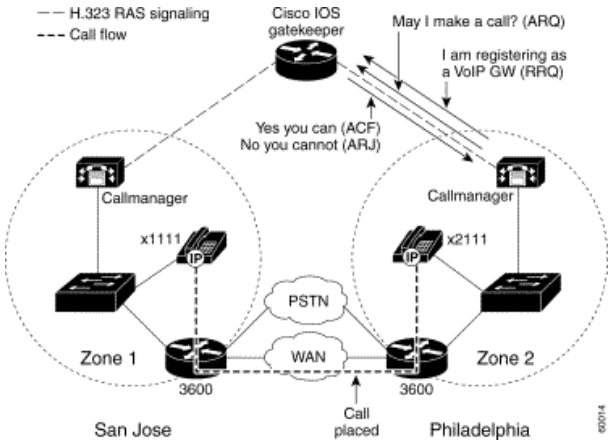
При сочетании шлюза и контроллера шлюза возможно отражение (как в Cisco IOS версии 12.1(5)T и версии 12.2), т.е. каждый шлюз — особенно на небольших удаленных узлах — может быть и контроллером шлюза при условии, что мощности ЦП на этой платформе достаточно для всех этих функций. (Подходит также для функционирования в качестве граничного маршрутизатора глобальной сети).

Тем не менее, структура «одна зона на один шлюз» противоречит масштабируемости, которую вносит идея контроллера шлюза в сети H.323, и отвергает идею «централизованного плана набора» сетей с контроллерами зон до тех пор, пока план набора не применяется на отдельном уровне с использованием руководящих контроллеров шлюза. Следовательно, необходимо тщательно взвесить преимущества и ограничения такой структуры.

Управление шлюзом в сетях администрирования вызовов

Из всех механизмов контроля приема вызовов, описанных в этом документе, учет полосы пропускания зоны контроллера шлюза является единственным методом, применимым к распределенным сетям администрирования вызовов с множественными узлами. В этом сценарии механизм администрирования вызовов выполняет роль VoIP шлюза в контроллере шлюза сети H.323, что показано на рис. 20.

Рис. 20. Контроллер шлюза в топологии администрирования вызовов



Расчет полосы пропускания зоны

Контроллеру шлюза ничего не известно о топологии сети и размере полосы пропускания, назначенной для голосовых вызовов. Ему также ничего не известно об использовании настроенной полосы пропускания другим трафиком в настоящий момент. Контроллер шлюза резервирует фиксированную часть полосы пропускания, статически настроенную, как было показано в предыдущих примерах сети, затем вычитает определенную полосу для каждого установленного вызова. После прекращения вызова полоса пропускания возвращается в пул. Если при запросе на новый вызов оставшаяся часть полосы пропускания становится меньше нуля, вызов отклоняется. Следовательно, контроллер шлюза *не резервирует* полосу пропускания, и просто выполняет статистические вычисления, чтобы принять решение о возможности нового вызова.

Информирование контроллера шлюза о размере полосы пропускания для вызова является задачей шлюза. Следовательно, видео-шлюзы могут запрашивать разную полосу пропускания для каждой установки вызова: один видео-сеанс может потребовать 256 Кбит/с, другой — 384 Кбит/с. Голосовые шлюзы должны учитывать кодек, инкапсуляцию уровня 2 и функции сжатия (например, сжатый RTP [cRTP]) при запросе полосы пропускания от контроллера шлюза Cisco. Иногда эти функции не определяются во время настройки вызова, и в этом случае запрос изменения полосы пропускания можно вывести на контроллер шлюза после настройки величины полосы пропускания, используемой вызовом. В настоящее время в продуктах Cisco эта возможность еще не реализована.

В предыдущем примере был установлен фиксированный размер полосы пропускания 64 Кбит/с на вызов, этот размер используется в настоящее время шлюзами Cisco H.323. Кодек и другие элементы, определяющие полосу пропускания, такие как cRTP, не рассматриваются в настоящее время, если полоса пропускания вызова анализируется при расчете полосы пропускания зоны контроллера шлюза. Эта ситуация изменится в дальнейших версиях ПО, но до того времени использование этого механизма требует ручных математических вычислений числа вызовов, которые могут быть разрешены на основе вычисления: *n* раз 64 Кбит/с на вызов и общей доступной полосы пропускания глобальной сети.

Полоса пропускания контроллера шлюза, тем не менее, остается не точной теорией, потому что у шлюза может не быть полной информации о полосе пропускания, необходимой для вызова. Технологии уровня 2, используемые в глобальных сетях или опорных отрезках сети, и функции, работающие с отдельными точками маршрута, например cRTP, могут использоваться в сети глубже, чем способен проконтролировать шлюз. Ниже приводятся некоторые примеры.

- Шлюз можно присоединить к элементу сети Ethernet локальной сети, где не применяется протокол cRTP и где заголовки уровня 2 превышают заголовки Frame Relay или MLP на отрезках глобальной сети.
- В локальной сети, соединяющей несколько зданий, может использоваться другой кодек, чем в сегменте глобальной сети, используя возможность преобразования кодека на оконечном оборудования глобальной сети.
- В опорной сети в качестве транспортной технологии можно использовать режим асинхронной передачи (ATM), а при расчете полосы пропускания необходимо принимать во внимание заполнение ячейки.
- Протокол cRTP можно использовать на граничном маршрутизаторе глобальной сети.

Ни шлюз, ни контроллер шлюза не обладает информацией об описанной топологии сети, *если шлюз не является* также граничным маршрутизатором глобальной сети. В таком случае у шлюза/граничного маршрутизатора немного больше видимости. Но, вероятно, ему будет не видна опорная сеть ATM, которая, как результат, не принимается во внимание.

Настройка полосы пропускания зоны

Как в Cisco IOS версии 12.1(5)T и версии 12.2, следующие типа ограничений полосы пропускания зоны можно настраивать на контроллере шлюза:

- Максимальная пропускная способность для всего трафика H.323 между локальной зоной и заданной удаленной зоной. (По желанию, для каждой удаленной зоны можно повторить настройки отдельно).
- Максимальная полоса пропускания, разрешенная для одного сеанса в локальной зоне (обычно используется не для голосовых, а для видеоприложений).
- Максимальная пропускная способность коллективного трафика H.323, разрешенного для всех удаленных зон.

Для настройки полосы пропускания зоны контроллера шлюза необходимо использовать следующие команды:

- **bandwidth** {**interzone** | **total** | **session**} {**default** | **zone** zone-name} *max-bandwidth*
- **bandwidth remote** *max-bandwidth*

Краткая информация о полосе пропускания зоны контроллера шлюза

Механизм контроля приема вызовов контроллера шлюза хорошо работает в сетях такой структуры, где есть потребность ограничить число вызовов между узлами. Это может потребоваться из-за ограничений полосы пропускания или политики компании. Если на отрезках глобальной сети установлены ограничения полосы пропускания, перевести максимальное число разрешенных вызовов между узлами в величину полосы пропускания, которая влияет на запрет вызовов шлюзом после превышения этого значения, можно с помощью ручных вычислений.

Контроль полосы пропускания зоны контроллера шлюза является ключевой частью проектов видео-сети H.323. В видео-сетях полоса пропускания является основным вопросом, потому что на сеанс передачи видео-информации требуется полоса пропускания большей величины, чем голосовой. Кроме этого, различным видео-сеансам может потребоваться разная величина полосы пропускания для передачи видео, что делает бесполезным метод ручных вычислений, используемый для передачи голоса.

При проектировании механизма контроля приема вызовов контроллера шлюза необходимо помнить о том, что избыточные контроллеры шлюза в какой-то мере усложняют вопрос. Например, если для избыточности на контроллере шлюза используется протокол HSRP, то между контроллерами шлюзом отсутствуют совместные базы данных. Если происходит сбой на первичном шлюзе, вторичный контроллер шлюза может принять на себя выполнение его функций, но у него не будет информации о величине полосы пропускания, используемой в зоне в настоящее время, и о числе активных вызовов. Пока эта информация, отражающая реальное положение, не соберется, вторичный контроллер шлюза пропустит в сеть слишком большое число вызовов. Если для обеспечения избыточности используются альтернативные контроллеры шлюза, проблема легко обходится.

Главным достоинством механизма контроля приема вызовов контроллера шлюза является то, что он является единственным методом, который может интегрировать IP-телефонию в смешанные сети, содержащие шлюзы IOS и администраторы вызовов.

В таблице 14 приводится оценка механизма полосы пропускания зоны контроллера шлюза по критериям оценки контроля приема вызовов, описанных ранее в этом документе.

Таблица 14. Краткая информация о механизме полосы пропускания зоны контроллера шлюза

Критерии оценки	Значение
Поддерживаемые технологии VoX	Только VoIP/H.323
	• Магистральные

Магистральные сети и IP-телефония	сети и IP-телефония • Некоторые предупреждения об использовании администратора вызовов и шлюзов Cisco IOS в одной зоне
Платформа (версия)	• Шлюзы Cisco IOS, начиная с версии 11.3 • Механизм администратора вызовов (CM) был немного изменен в записи E.164 и полосе пропускания, требуемой для вызова.
Поддерживаемые типы каналов АТС	Все
Сквозной, локальный или IP-скопления	Сквозной между исходящим и оконечным шлюзом, без информации о топологии сети (доступности полосы пропускания) между ними.
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	На вызов
Знание топологии	Нет
Гарантия качества обслуживания на протяжении вызова	Нет
Задержка после набора номера	Нет
Служебная информация сети	Часть RAS-сообщений контроллера шлюза

Протокол резервирования ресурсов

Протокол RSVP является единственным механизмом контроля приема вызовов, который выполняет резервирование полосы пропускания, и не принимает решение о выполнении вызова перед установкой вызова на основе метода «лучшее предположение, предварительный просмотр». Это обеспечивает протоколу RSVP уникальное преимущество, которое заключается в том, что он не только предоставляет контроль приема вызовов для голоса, но и гарантирует качество обслуживания при меняющихся условиях сети в продолжение всего вызова.

Развертывание протокола резервирования ресурсов (RSVP)

В ПО Cisco IOS версии 12.1(5)T протокол RSVP синхронизирован с конечным аппаратом H.323, следовательно, доступен в выпуске 12.2. Различные компоненты этой функциональности появлялись в более ранних версиях ПО, но все элементы механизма контроля приема вызовов были реализованы в версиях, начиная с 12.1(5)T. Ниже приводится краткая информация о поддержке RSVP.

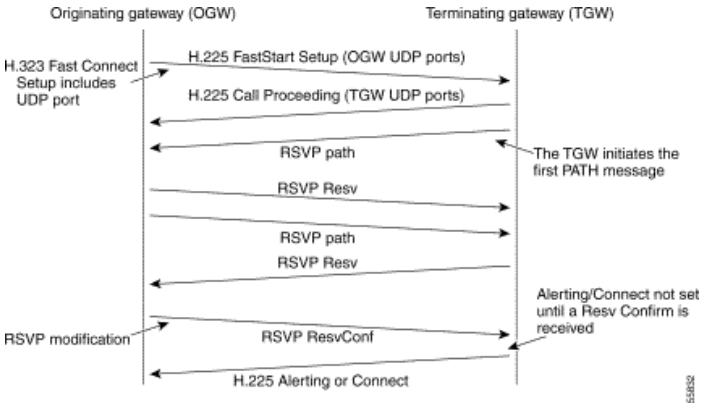
- Протокол RSVP синхронизирован с H.323 Standard Connect: выпуск 12.1(1)T
- Поддержка протоколом RSVP механизма LLQ: выпуск 12.1(3)T
- RSVP синхронизирован с H.323 FastConnect: выпуск 12.1(5)T
- Поддержка протоколом RSVP каналов FR PVC: выпуск 12.1(5)T

Поддержка протоколом RSVP каналов ATM PVC и поддержка RSVP на IP-телефонах планируется реализовать в будущих версиях ПО.

Резервирование протокола RSVP для голосового вызова

На рис. 21 показана диаграмма вызова сообщений установки вызова H.323 и сообщений резервирования RSVP

Рис. 21. Установка вызова RSVP для голосового вызова H.323



Установка H.323 отложена перед тем, как начинает звонить телефон назначения, инициированный оповещающим сообщением H.225. Резервирование протокола RSVP выполняется в двух направлениях, потому что для голосового вызова требуется путь прохождения речевых сигналов в двух направлениях и, следовательно, полоса пропускания в двух направлениях. Оконечный шлюз полностью принимает решение контроля приема вызовов на основе успеха двух резервирований. В этой точке конечный аппарат H.323 продолжает работу либо с команды H.225 Alerting/Connect (вызов разрешается и обрабатывается), либо с команды H.225 Reject/Release (вызов отклонен). Резервирование протокола RSVP происходит к тому моменту, когда телефон с набранным номером начинает звонить, и абонент слышит сигнал обратного вызова.

Протокол RSVP имеет следующие важные отличия от других методов контроля приема вызовов, описанных в этом документе:

- Возможность поддерживать качество обслуживания на протяжении всего вызова.
- Знание топологии Согласно описываемой концепции, резервирование RSVP устанавливается на каждом интерфейсе, через который проходит вызов по сети (в следующих разделах будет представлено описание исключений) и, следовательно, гарантируется полоса пропускания для каждого сегмента, без необходимости знания ни фактической полосы пропускания на интерфейсе, ни пути, по которому протоколом маршрутизации направляются пакеты. (Таким образом, протокол RSVP автоматически подстраивается к изменениям конфигурации сети, и нет потребности в ручных вычислениях, чтобы сохранять синхронизированными различные аспекты настройки.)

Протокол RSVP является сквозным резервированием на вызов и может просматривать только этот вызов. Неизвестно число других активных вызовов, исходящих с узла или проходящих через интерфейс, а также источник и адрес назначения любого другого вызова. Следовательно, нет способа настроить уровень объединения контроля приема вызовов с протоколом RSVP, таких как механизм контроля вызовов типа «узел-на-узел», который можно было настроить с контролем полосы пропускания контроллера шлюза.

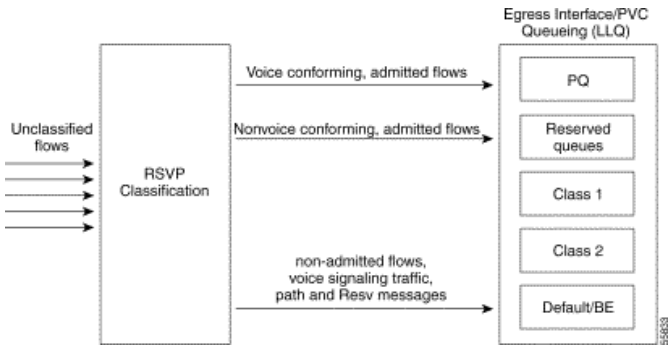
Классификация голосовых пакетов по критерию минимального времени ожидания (LLQ)

LLQ является одним из важных механизмов обеспечения качества Cisco QoS, который гарантирует качество голоса благодаря установке более высокого приоритета голосовым пакетам над пакетами данных на выходном интерфейсе маршрутизатора. Для работы этого механизма необходимо классифицировать голосовые пакеты так, чтобы они помещались в очередь приоритетов LLQ. Традиционно это достигается с помощью классификации списка контроля доступа (Access Control List, ACL), где порты TCP (сигналы) и UDP (среда) сопоставлены так, чтобы направлять голосовые пакеты в соответствующую очередь.

Общими средствами Cisco IOS для трафика с резервированием RSVP протокол RSVP снабжается собственным набором зарезервированных очередей в составе WFQ (взвешенной очереди с обслуживанием по принципу равнодоступности). Эти очереди, несмотря на более низкий вес, отделены от PQ. Пакеты в зарезервированных очередях не получают приоритета над пакетами из других очередей из-за низкого веса. Давно известно, что этого метода (очереди с низким весом в составе очереди WFQ) недостаточно для обеспечения качества голосовой связи по перегруженному интерфейсу с несколькими разными потоками трафика. Следовательно, при настройке RSVP на голосовой вызов необходимо относить голосовые пакеты к очереди PQ. Пакеты потока данных RSVP в этом случае не требуется относить к PQ.

Протокол RSVP классифицирует поток пакетов как голосовой поток на основании *профиля*. В профиле учитывается размер пакета, скорость появления и другие параметры. Поток пакетов, соответствующий определенным параметрам, считается голосовым. В случае несоответствия он считается неголосовым потоком, который может включать как данные, так и видео. Внутренний профиль настроен таким образом, что весь голосовой трафик, исходящий со шлюза Cisco IOS, соответствует этим параметрам и будет, следовательно, считаться голосовым потоком без необходимости в дополнительной настройке. Для обработки специфического трафика от приложений сторонних поставщиков, таких как NetMeeting, может потребоваться настройка профиля. Процесс поясняется на рис. 22.

Рис. 22. Критерии классификации пакетов RSVP



RSVP является первым выходным интерфейсом, который проверяет приходящий пакет. Если протокол RSVP классифицирует пакет как относящийся к голосовому потоку, то пакет попадает в раздел PQ механизма организации очередей LLQ. Если поток не соответствует голосовому профилю, но является, тем не менее, потоком, зарезервированным RSVP, то он будет помещен в обычные зарезервированные очереди RSVP. Если поток не является ни голосовым потоком, ни потоком данных RSVP, другим классификаторам выходного интерфейса (например, ACL и операторам соотнесения в таблице классов) предоставляется возможность классифицировать пакет для постановки в очередь.

Важно отметить, что протокол RSVP классифицирует только полезный голосовой трафик, а не служебный трафик. Если для голосового служебного трафика необходим иной способ обработки, чем Best-effort (передача только при наличии возможности), то для классификации этого необходимо использовать один из прочих механизмов классификации, например, ACL или DSCP. Если принятие решения становится ответственностью одного механизма RSVP, служебный трафик будет считаться трафиком Best-effort (передаваемым только при наличии возможности), как показано на рис. 22.

Присвоение полосы пропускания в протоколе RSVP и механизме LLQ

Голосовой трафик RSVP можно смешивать с трафиком «приоритетного класса» (в пределах таблицы политики) в очереди PQ, но настройка проще при использовании одного механизма классификации. Тем не менее, рекомендуется использовать только один или другой для голоса, но не сразу оба. Необходимо настроить либо протокол RSVP для определения приоритета голосового трафика, либо

настроить карту политики с приоритетом полосы пропускания, и классифицировать голосовой трафик в очередность LLQ с помощью механизма ACL. Оба метода работают вместе, но они не используют совместно назначение полосы пропускания и, как следствие, приводят к неэффективному использованию полосы пропускания на интерфейсе.

Полоса пропускания определена в настройке для входного устройства, поэтому все полосы и классы приоритета будут назначенными полосами пропускания во время настройки. Во время настройки ни одна полоса пропускания не назначается протоколу RSVP, т.к. он запрашивает полосу пропускания во время начала потока трафика, при инициации голосового вызова. Следовательно, протоколу RSVP назначается полоса пропускания из пула, которая остается после того, как полосы пропускания были выделены для других механизмов.

Полоса пропускания для кодека

И LLQ, и RSVP рассматривают IP-пакет уровня 3 Инкапсуляции уровня 2 (FR, MLPPP и т.д.) добавляются после постановки в очередь, поэтому полоса пропускания, назначенная для вызова механизмами LLQ и RSVP, основана на полосе пропускания пакетов уровня 3. Это число может немного отличаться от фактической полосы пропускания, используемой на интерфейсе после включения заголовков и концевика уровня 2. Полоса пропускания, зарезервированная RSVP для вызова, часто не включает в себя протоколы cRTP и VAD. В таблице 15 приводится краткая информация о полосе пропускания, которую протокол RSVP назначает для вызовов, используя различные кодеки шлюзов Cisco IOS.

Таблица 15. Резервирование полосы пропускания RSVP на голосовые кодеки

Кодек	Полоса пропускания, зарезервированная на вызов в очередности LLQ
G.711 (a-law и m-law)	80 Кбит/с
G.723.1 и G.723.1A (5,3 Кбит/с)	22 Кбит/с
G.723.1 и G.723.1A (6,3 Кбит/с)	23 Кбит/с
G.726 (16 Кбит/с)	32 Кбит/с
G.726 (24 Кбит/с)	40 Кбит/с
G.726 (32 Кбит/с)	48 Кбит/с
G.728	32 Кбит/с

G.729 (все выпуски)	24 Кбит/с

Конфигурация RSVP

Выполняют следующие три задачи на шлюзе для инициации или завершения голосового трафика с помощью RSVP:

- Включают возможность синхронизации между RSVP и H.323. Это общая команда, которая включается по умолчанию при загрузке Cisco IOS версии 12.1(5)T или более поздних версий.
- Настраивают RSVP на исходящем и оконечном узлах коммутирующих узлов VoIP. Настраивает команды Requested QoS (req-qos) и Acceptable QoS (acc-qos) **guaranteed-delay** для работы RSVP в качестве механизма контроля приема вызовов. (Другие комбинации параметров могут привести к резервированию, но не к контролю приема вызовов)
- Включение RSVP и определение максимальной величины полосы пропускания на интерфейсе, который проходит вызов.

В следующем примере конфигурации включен RSVP.

```
!Общая команда, включающая RSVP в качестве механизма контроля приема вызовов, включена по умолчанию.
call rsvp-sync
controller T1 1/0
 ds0-group 0 timeslots 1-24
!
!Профиль классификации RSVP. По умолчанию устанавливается «да» для всего голосового трафика шлюза Cisco IOS.
ip rsvp pq-profile voice-like
!
voice-port 1/0:0
!
dial-peer voice 100 pots
 destination-pattern 2......
port 1/0:0
!
dial-peer voice 300 voip
 destination-pattern 3......
session target ipv4:10.10.2.2
!Настраивает механизм контроля приема вызовов протокола RSVP для голосовых вызовов, используя коммутирующий узел.
 req-qos guaranteed-delay
 acc-qos guaranteed-delay
```

В следующем примере настройки включается RSVP на интерфейсе PPP.

```
interface Serial0/1
 bandwidth 1536
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp
!Включает WFQ в качестве основного метода организации очередей. Результат в LLQ с протоколом RSVP.
fair-queue 64 256 36
!Включает RSVP на интерфейсе.
ip rsvp bandwidth 1152 24
```

В следующем примере конфигурации включается RSVP для интерфейса Frame Relay.

```
interface Serial0/0
 bandwidth 1536
 encapsulation frame-relay
 no fair-queue
 frame-relay traffic-shaping
!
interface Serial0/0.2 point-to-point
 ip адрес 10.0.0.2 255.255.255.0
 frame-relay interface-dlci 17
  class VoIPoFR
!Включает RSVP на подинтерфейсе.
ip rsvp bandwidth 64 24
map-class frame-relay VoIPoFR
 no frame-relay adaptive-shaping
 frame-relay cir 128000
 frame-relay bc 1280
 frame-relay mincir 128000
!Включает WFQ в качестве основного метода организации очередей. Результат в LLQ с протоколом RSVP.
frame-relay fair-queue
 frame-relay fragment 160
```

Масштабируемость протокола RSVP

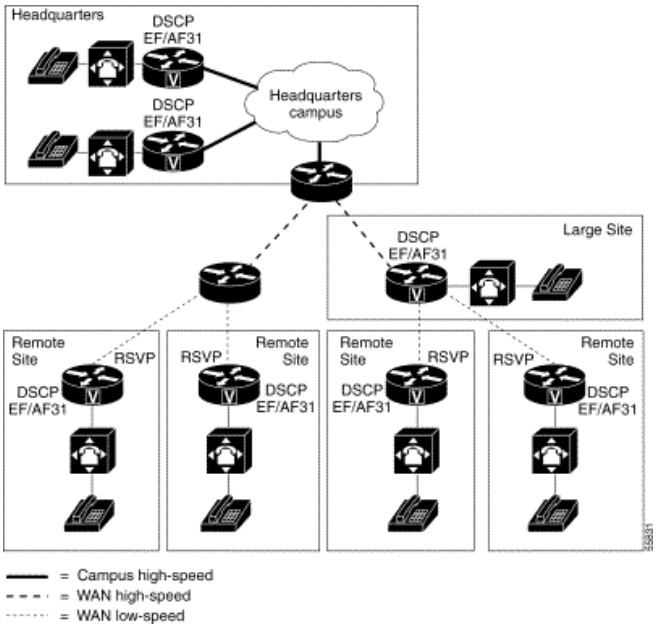
Часто высказывается опасение насчет масштабируемости RSVP на основе большого числа индивидуальных резервирований потоков, которые могут быть необходимыми в соединениях высокоскоростной опорной сети, где объединяется много голосовых вызовов.

Действительно, смысла в индивидуальном управлении потоком, например, по соединениям опорной сети OC-12 может и не быть. По этой причине в коде Cisco IOS версии 12.1(5)T и более поздних выпусков сообщения RSVP прозрачно переправляются, если этот протокол не настроен на любом интерфейсе платформы. Не выполняется и не управляется ни одно резервирование, но путь и пакеты Resv не отбрасываются.

Это делает возможным создание гибридных топологий, где используется RSVP вокруг границ сети для защиты медленных соединений доступа в глобальную сеть или перегрузки, в то время как высокоскоростные локальные сети, соединяющие несколько офисов, и опорные соединения глобальной сети не используют RSVP. Конечно, такая топология является компромиссом между настоящим сквозным резервированием и гарантией качества обслуживания RSVP, но вполне рабочим. На опорных соединениях может достигаться необходимая защита от излишних устройств или от одного из других механизмов контроля приема вызовов, описанных ранее, в то время как для подключения с высокой вероятностью конфликта (обычно граничное оборудование локальной сети) можно пользоваться протоколом RSVP.

На рис. 23 отображена гипотетическая сеть, настроенная на использование DiffServ в опорной и локальной сети, но использующая резервирования RSVP на граничных соединениях с глобальной сетью.

Рис. 23. Гибридная топология DiffServ/RSVP



Краткая информация о механизме контроля приема вызовов RSVP

Необходимо помнить о следующих факторах, относящихся к использованию протокола RSVP в качестве механизма контроля приема вызовов:

- В ПО Cisco IOS, который используется в настоящее время, вызовы H.323 по умолчанию инициируются с помощью технологии FastConnect, если настроен протокол RSVP.
- Пакеты RSVP (PATH и RESV) проходят по сети как трафик, передаваемый только при наличии возможности.
- В качестве основы для LLQ на интерфейсе/PVC должна быть включена поддержка WFQ.

Протокол RSVP является настоящим сквозным механизмом контроля приема вызовов, *только* если он настроен на любой интерфейс, через который проходит вызов.

Из-за уникальной веозможности протокола RSVP функционировать в качестве сквозного механизма контроля приема вызовов и гарантировать качество обслуживания на всей продолжительности вызова, в сети появляются некоторые «издержки» следующего рода:

- Передача сигналов (передача сообщений и обработка)
- Отдельное состояние (память) для каждого потока
- Задержки после набора номера
- В случае сбоя в соединении сети протокол RSVP не обеспечивает перенаправление вызова после его установки
- В Cisco IP-телефонах RSVP пока не поддерживается

В таблице 16 приводится оценка механизма RSVP по критериям оценки механизмов контроля приема вызовов, описанных ранее в этом документе.

Таблица 16. Краткая информация о механизме RSVP

Критерии оценки	Значение
Поддерживаемые технологии VoX	Только VoIP/H.323
Магистральные сети и IP-телефония	В настоящее время — только магистральные сети
Платформа (версия)	Шлюзы Cisco IOS в версиях 12.1(5)T и 12.2
Поддерживаемые типы каналов АТС	Все
Сквозной, локальный или IP-скопления	• Сквозной между исходящим шлюзом и оконечным контроллером шлюза (при условии, что все промежуточные узлы настроены на использование RSVP) • Может быть использована на граничном оборудовании глобальной сети с опорой DiffServ
Масштаб: отдельные вызовы, интерфейсы или конечные пункты	На вызов
Знание топологии	Да
Гарантия качества обслуживания на протяжении	Да

вызова	
Задержка после набора номера	Да
Служебная информация сети	PATH/RESV и периодические дежурные сообщения

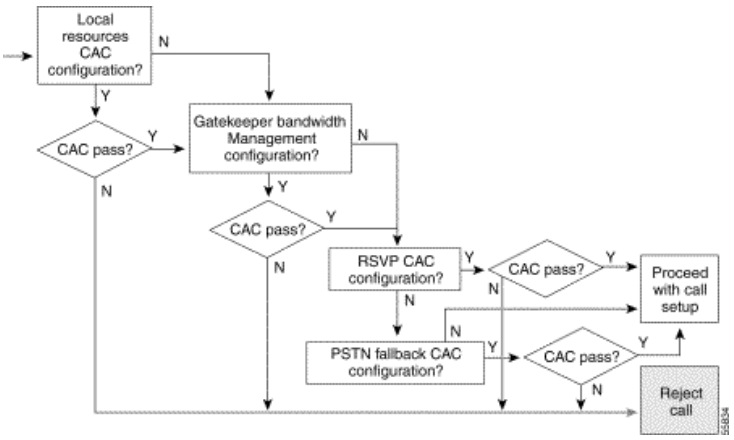
Как применить контроль приема вызовов к конкретной сети

Хотя возможности, предлагаемые различными механизмами контроля приема вызовов, в некоторой степени перекрываются, некоторые из них решают разные аспекты проблемы контроля приема вызовов и, следовательно, имеет смысл использовать их вместе. Часто возникают следующие вопросы:

- Могут ли два метода контроля приема вызовов использоваться вместе на одном шлюзе в одно время для одного вызова?
- (В случае положительного ответа на предыдущий вопрос): в каком порядке принимается решение механизмов контроля приема вызовов?

На рис. 24 подводится итог последовательности элементов контроля приема вызовов, которые могут функционировать на исходящем шлюзе на основе Cisco IOS версий 12.1(5)T и 12.2. Функциональность и ПО меняются, фиксируются различные ошибки ПО, поэтому эта информация может меняться без уведомления. Как показано на диаграмме потока, единственными взаимоисключающими функциями являются RSVP и механизм перехода к аварийному режиму работы сети ТфОП.

Рис. 24. Последовательность использования механизмов контроля приема вызовов на исходящем шлюзе



В следующих разделах описывается развертывание механизмов контроля приема вызовов:

- Когда и какие механизмы контроля приема вызовов применять
- Контроль приема вызовов в магистральных сетях
- Защищаемые области сети
- Анализ различных топологий сети

Когда и какие механизмы контроля приема вызовов применять

При большом многообразии доступных механизмов контроля приема вызовов возникает вопрос: «Когда необходимо использовать тот или иной элемент контроля приема вызовов?» Как было отмечено при описании отдельных функциональностей, а также в результатах сравнений и сводок, приводимых в этом документе, различные механизмы выполняют разные функции и решают разные вопросы проблемы контроля приема вызовов. Некоторые их этих критериев могут быть более важными в конкретных сетях, чем другие. Таким образом, не существует единого рецепта использования того или иного механизма. Как и в случае с другими функциональностями программного обеспечения, необходимо принимать решение, рассматривая цели конкретной сети.

В этом разделе дается попытка дать некоторые рекомендации, касающиеся критериев проектирования сети, которые могут относиться к конкретной сети, и функциям, которые сооответствуют этим критериям. Критериями выбора функциональностей, которые необходимо использовать сначала, являются «критерии оценки», приводимые в конце каждого раздела, посвященного отдельной функциональности. Например, если проектируется сеть VoIP на основе протокола SIP, нет смысла рассматривать механизмы контроля приема вызовов, разработанные для сети H.323. Если такой уровень обзора уже выполнен, можно использовать предположения этого раздела для дальнейшего сужения выбора механизмов.

Контроль приема вызовов в магистральных сетях

В отличие от коммутируемых сетей, где каждый вызов устанавливается отдельно по сети с пакетной коммутацией после набора номера пользователей, магистральные сети состоят из уже готовых соединений внутри сети с пакетной коммутацией. Кажется, что офисная АТС устанавливает отдельно каждый вызов, но в сетях с пакетной коммутацией существует постоянный канал (двухточечное соединение, идея которого близка идее выделенной линии), постоянно включенный, постоянно готовый и постоянно выполняющий вызовы на ограниченные, заранее заданные адреса назначений. Эти готовые настройки коммутируемой сети обычно используются при наличии сигналов между офисными АТС, которые должны проводится через коммутируемую сеть прозрачно и в неизменном виде. Шлюзы не могут интерпретировать сигналы, они их попросту туннелируют по коммутируемой сети.

Для такой сети существует два основных приложения.

- Сети, в которых сигналы, например, быстрый отбой или сигнал ожидания сообщения (MWI) должны проходить в офисную АТС через коммутируемую сеть для активации вызовов на телефоны за пределами офиса, отделены от офисных АТС, в которых установлены механизмы, сетями коммутируемого доступа.
- Сети, в которых между офисными АТС используются собственные сигналы для активации частных сетевых возможностей АТС. (Примеры включают в себя Lucent DCS, Siemens CorNet и NEC CCIS.)

Настройки канала связи шлюза Cisco IOS для установки соединения используют одинаковые базовые инструменты (такие как коммутируемые узлы) с коммутирующими сетями. Разница заключается в том, что эти вызовы устанавливаются один раз при загрузке шлюза или добавлении настройки, и остаются неопределенно долгое время. Если связь в сети обрывается, и вызов прекращается, то маршрутизатор установит связь заново при ближайшей возможности. Для шлюзов понятно, проводится ли по этому соединению реальный вызов (с голосами людей). По этой причине в большинстве случаев не применяются стандартные механизмы контроля приема вызовов. Настройки канала соединения не будут работать полностью, если полосы пропускания для этого соединения не хватает, поэтому после установки соединения необходима достаточная полоса пропускания для этого вызова.

Следующие механизмы контроля приема вызовов в порядке поступления вызовов (call-by-call) применяются *только* в коммутируемых сетях, и их *не следует* использовать с настройками каналов связи.

- Максимальное число подключений
- Функция перехода к аварийному режиму сети ТфОП (PSTN Fallback)
- Индикация наличия ресурсов
- Полоса пропускания зоны контроллера шлюза

Настройки канала соединения, однако, могут использовать возможности отключения механизмов контроля приема вызовов офисных АТС. При отключении какого-либо устройства в сети и при постоянном разрыве соединения, а также при сбое интерфейса, полезно будет отключить один канал от АТС. К этим функциям относятся следующие:

- Согласование канала
- Функция Busyout для локальных вызовов
- Улучшенная функция Busyout для вызовов (Advanced Voice Busyout)

Согласно концепции, протокол RSVP нельзя использовать для гарантии наличия (резервирования) полосы пропускания для уже готовых соединений, чтобы обеспечить качество голосовой передачи при изменениях условий сети. Тем не менее, т.к. сети с каналами связи являются фиксированными, двухточечными соединениями, то число активных вызовов в любом сегменте сети (с точки зрения маршрутизатора) является фиксированным и легко проектируется с помощью назначения полосы пропускания вручную и использования стандартных настроек LLQ для обеспечения полосы пропускания. Следует тщательно рассмотреть, будет ли протокол RSVP полезен в такой ситуации.

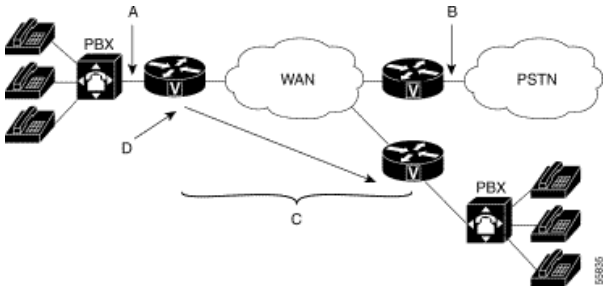
Защищаемые области сети

В большей мере методы контроля приема вызовов полезны и необходимы в коммутируемых сетях, где часто невозможно предсказать

точное число вызовов на определенном участке сети в данное время. Статистические методы проектирования голосовых сетей существуют уже десятилетиями, тем не менее нет механизмов, которые позволяли бы определять, кто и кого будет вызывать по сети в определенное время. До тех пор, пока топология сети не будет простой, полоса пропускания в некоторых точках сети может быть перегружена большим числом вызовов. В офисных АТС такая ситуация приводит к сигналу занятости линии или к прерыванию разговора сообщением «все линии заняты».

При рассмотрении методов контроля приема вызовов для запуска сравнимого условия «все линии заняты», когда сеть с пакетной коммутацией перегружена для обработки вызова, следует рассмотреть цели проектирования сети. Все аспекты контроля приема вызовов, показанные на рис. 25, существуют в каждой сети, но некоторые характеристики в отдельных сетях более важны, чем другие. Аспекты сети, которым может потребоваться защита механизмами контроля приема вызовов, разделены на четыре области (A, B, C и D), как показано на рис. 25.

Рис. 25. Разделение областей сети



Область A представляет собой исходящее соединение POTS. В случае необходимости не допускать вызов с исходящей АТС в сеть с пакетной коммутацией, когда сеть не способна завершить вызов, следует рассматривать функции busyout контроля приема вызовов. Это может быть важным, если возврат является неприемлемым методом восстановления отклонения вызова или если в системе (PBX/Key) отсутствует возможность выбрать другой маршрут для отклоненного или возвращенного вызова.

Область B является завершающей стороной соединения POTS. Если имеется вероятность этого из-за особых моделей трафика, в которых завершающая сторона POTS является частью сети, более восприимчивой к перегрузке, следует использовать шлюз RAI. В корпоративных сетях это редко является значимым, но в сетях провайдеров услуг, эта область является чрезвычайно важной частью сети, нуждающейся в защите.

Область C является IP-опорной частью сети. Эта область является наиболее обычной областью сети, вызовы от которой у корпоративных клиентов (включая сети управляемых услуг провайдеров услуг) есть необходимость защищать, потому что такая инфраструктура не выделена для голоса, а разделяется между многими видами трафика. К механизмам контроля приема вызовов, защищающим сетевые «скопления» относятся следующие:

- Функция перехода к аварийному режиму сети ТфОП (PSTN Fallback)
- Полоса пропускания зоны контроллера шлюза
- Протокол резервирования ресурсов

Эти методы контроля приема вызовов основаны на IP, что предполагает, что имеется больше методов контроля приема вызовов, доступных для сетей VoIP, чем для сетей VoFR и VoATM. Для сетей VoIP контроль приема вызовов также необходим больше, потому что технологии уровня 2, как и протоколы Frame Relay и ATM, не могут в действительности защитить против потери пакетов VoIP, как в случае с трафиком VoFR и VoATM.

Область D является логическим разделом сети между узлами. Независимо от действительной инфраструктуры, соединяющей узлы, может возникнуть необходимость ограничивать трафик не между узлами, а в пределах узла или ограничить его на основе других критериев. Например, если сеть в штаб-квартирах может обрабатывать 24 вызова одновременно, то может будет нужно обеспечить, чтобы все 24 вызова не обрабатывались одним или другим узлом в любое время, но что определенное число мощности имеется на других узлах, так что узлы с низким трафиком не блокируются узлами с большим трафиком.

К механизмам контроля приема вызовов, которые можно использовать с такой ситуации, относятся следующие:

- Максимальное число подключений
- Полоса пропускания зоны контроллера шлюза

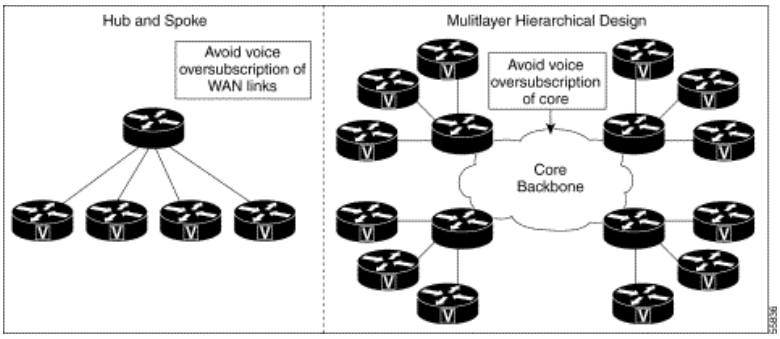
Анализ различных топологий сети

На самом общем уровне существует две следующие топологии сети, которые необходимо рассмотреть:

- Звездообразная сеть
- Многоуровневая иерархическая сеть с распределенными слоями

Эти две топологии концептуально отображены на рис. 26.

Рис. 26. Топологии корпоративных сетей



Звездообразную сеть легче обслуживать. В этом случае полезны большая часть механизмов контроля приема вызовов, потому что только периферийные части сети нуждаются в защите. Не существует невидимой опорной сети, а периферийные соединения могут быть единственными соединениями, подключенными к шлюзам на удаленных узлах. Почти все из следующих механизмов контроля приема вызовов можно использовать для достижения хорошего эффекта в сети такого типа.

- Физические ограничения канала DS0
- Максимальное число подключений
- Улучшенная функция Busyout для вызовов (Advanced Voice Busyout)
- Функция перехода к аварийному режиму сети ТфОП
- Индикация наличия ресурсов
- Полоса пропускания зоны контроллера шлюза
- Протокол резервирования ресурсов

Многоуровневые иерархические сети более представлены в сетях большего размера, где удаленные узлы объединяются на одном или более уровнях промежуточных пунктов перед центральной сетью, которая объединяет агрегации более высокого уровня. Многие механизмы контроля приема вызовов будут защищать соединения глобальной сети на самом низком уровне сети, но немногие смогут просматривать объединения и основные участки сети. К механизмам, способным просматривать сеть, относятся следующие:

- Улучшенная функция Busyout для вызовов
- Функция перехода к аварийному режиму сети ТфОП (PSTN Fallback)
- Протокол резервирования ресурсов

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/97328/tech_tk652_tk701_technologies_white_paper09186a00800da467.shtml