Пример внедрения IP-телефонии: Australian Catholic University

Содержание

Введение

Австралийский Академик и Сеть научно-исследовательских учреждений (AARNet) являются общенациональным высокоскоростным IP - сетью, который соединяет 37 Австралийских университетов, а также научные организации Австралийского союза и Организацию Технических исследований (CSIRO).

AARNet был первоначально создан как сеть передачи данных, но он нес Передачу голоса по IP (VoIP) с начала 2000 года. Сеть VoIP, в настоящее время развертываемая, является решением обхода междугородней АТС, которое несет вызовы VoIP между университетами и учрежденческими АТС CSIRO (PABX). Это также предоставляет шлюзы открытой коммутируемой телефонной сети (PSTN), которые позволяют PSTN переходу в большей части экономически эффективного этапа. Например, вызов с телефона PABX в Мельбурне к телефону PSTN в Сиднее несут как VoIP от Мельбурна до шлюза PSTN в Сиднее. Это там связано с PSTN.

Australian Catholic University (ACU) является одним из университетов, который соединяется с AARNet. В конце 2000 ACU начал развертывания IP-телефонии, которые развернули

приблизительно 2,000 IP-телефонов через шесть университетских общежитий.

Этот пример практического применения покрывает развертывания IP-телефонии ACU. Проект завершен. Однако существуют значительные архитектурные проблемы для адресации в магистрали AARNet, если сеть должна масштабироваться, когда другие университеты идут по стопам ACU. Этот документ описывает эти проблемы и предлагает и обсуждает различные решения. Развертывания IP-телефонии ACU, вероятно, будут отрегулированы позже для падения в соответствии с заключительной рекомендуемой архитектурой.

Примечание: Университетом Дикин был первый Австралийский университет, который развернет IP-телефонию. Однако университет Дикин не использует AARNet для переноса трафика IP-телефонии.

AARNet

Австралийские университеты и CSIRO создали AARNet в 1990 через Australian Vice-Chancellors ' Committee (AVCC). Девяносто девять процентов австралийского интернет-трафика были привлечению участников в течение первых несколько лет. Малая величина коммерческого трафика была от организаций, которые имели тесную связь с третичным сектором и сектором исследования. Использование базой пользователей не-AARNet увеличилось до 20 процентов общего трафика к концу 1994 года.

AVCC продал ядро коммерческого заказчика AARNet к Telstra в июле 1995. Это событие породило то, что должно было в конечном счете стать Telstra BigPond. Этот стимулированный дальнейший рост коммерческого и личного пользования Интернета в Австралии. Передача интеллектуальной собственности и экспертных знаний привела к разработке Интернета в Австралии. В противном случае это не произошло бы в такой высокой скорости.

AVCC разработал AARNet2 в начале 1997 года. Это было дальнейшее улучшение Интернета в Австралии, которая использует соединения ATM высокой пропускной способности и интернет-сервисы в соответствии с договором с Ограниченной Cable & Wireless Optus (CWO). Быстрое развертывание IP-сервисов CWO для соответствия требованиям AARNet2 было должно частично к передаче знаний и опыта от AARNet.

ACU

ACU является общественным университетом, который был установлен в 1991. Университет имеет приблизительно 10,000 студентов и 1,000 сотрудников. Существует шесть кампусов на восточном побережье Австралии. Эта таблица показывает кампусы ACU и их местоположения:

Кампус	Город	Состояние
Saint Mary установки	Стратфилд	Новый Южный Уэльс (NSW)
Маккиллоп	Северный Сидней	Новый Южный Уэльс (NSW)
Patrick	Мельбурн	Виктория (VIC)
Aquinas	Балларат	Виктория (VIC)
Signadou	Канберра	Australia Capital

		Territory (ACT)
Маколи	Брисбен	Квинсленд (QLD)

ACU полагался на Telstra Spectrum (Centrex) решение перед развертыванием Решения IP-телефонии, которое описывает этот пример практического применения. Перемещение к IP-телефонии вело в основном желание уменьшить стоимость.

CSIRO

CSIRO имеет приблизительно 6,500 сотрудников на многочисленных узлах в Австралии. CSIRO проводит исследование в областях, таких как сельское хозяйство, полезные ископаемые, энергия, производство, связь, конструкция, состояние и среда.

CSIRO был первой организацией, которая будет использовать AARNet для VoIP. Организация вела раннюю работу, сделанную в этой области.

AARNet

Магистраль AARNet является значимым компонентом в любом университете развертывания IP-телефонии. Это предоставляет взаимодействию университетов два основных сервиса в области voice:

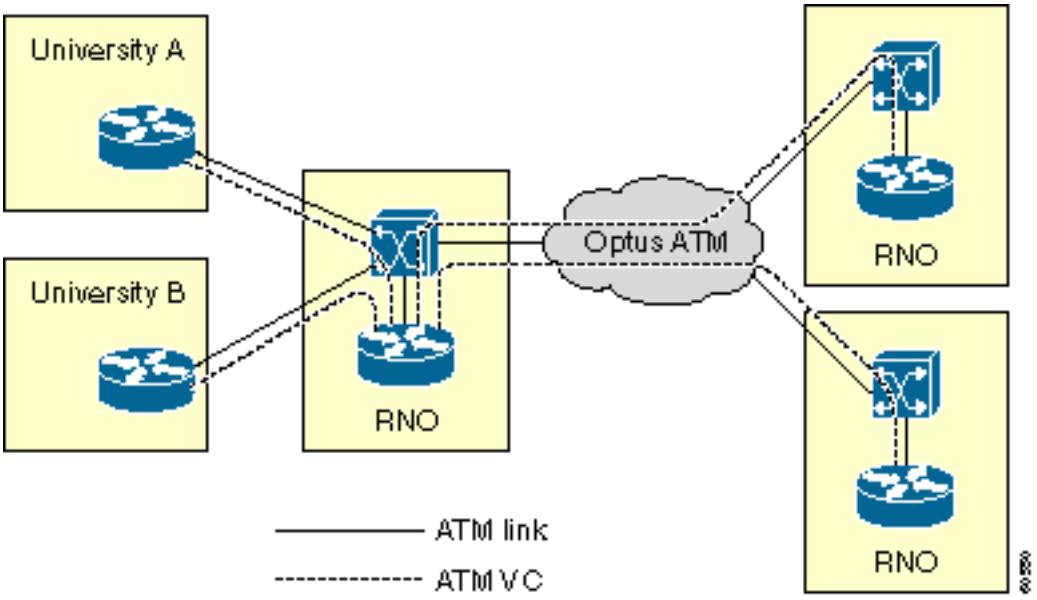
- Транспорт пакетов Протокола RTP VoIP с гарантией Качества обслуживания (QoS), соответствующего голосу
- Недорогие hopoff указывают к PSTNs по всей стране

В этом разделе описываются текущую архитектуру AARNet и как это предоставляет эти услуги. Это также выделяет некоторые проблемы масштабирования, которые возникают, поскольку больше университетов развертывает Решение IP-телефонии. Наконец, это обсуждает возможные решения для этих проблем масштабирования.

Топология AARNet

AARNet состоит из одиночного POP (Point of Presence) в каждом состоянии. POP упоминаются как Операции Региональной сети (RNO). Университеты соединяются с RNO в их соответствующем состоянии. RNO в свою очередь соединены полной сеткой постоянных виртуальных каналов ATM Optus. Вместе они составляют AARNet.

Типичный RNO состоит из одного коммутатора ATM Cisco LS1010 и одного Подключенного к ATM маршрутизатор. Маршрутизатор RNO соединяется с каждым маршрутизатором университета одиночным постоянным виртуальным каналом ATM через микроволновое соединение E3. Каждый маршрутизатор RNO также имеет полную сетку постоянных виртуальных каналов ATM, которые сеть ATM Optus предоставляет всем другим RNO. Эта схема представляет общую Топологию AARNet сети:



Существуют многочисленные исключения к топологии. Некоторые из них являются значительными с речевой точки зрения. Это некоторые исключения:

- RNO в Виктории использует классический IP по ATM (RFC 1577) вместо PVCs для подключения университетов с RNO.
- Подразделения университета, как правило, соединяются назад с RNO Frame Relay или ISDN.
- Некоторые крупные университеты имеют несколько ссылок назад на RNO.

Эта таблица показывает состояния и территории, которые в настоящее время имеют RNO. Таблица включает столицы для читателей, которые не знакомы с географией Австралии.

Состояние	Столица	RNO?	Соединения уровня кампуса
Новый Южный Уэльс	Сидней	Да	TBD
Виктория	Мельбурн	Да	TBD
Квинсленд	Брисбен	Да	TBD
Южная Австралия	Аделаида	Да	TBD
Западная Австралия	Перт	Да	TBD
Территория капитала Австралии	Канберра	Да	TBD
Северные Территории	Дарвин	Нет	--
Тасмания	Хобарт	Нет	--

Качество обслуживания

Части AARNet являются уже поддерживающими QoS для голоса в результате проекта обхода междугородней АТС VoIP. QoS необходимо для голосового трафика для

обеспечения этих функций, которые минимизируют задержку и дрожание и устраняют потерю пакета:

- Применение политик — отмечает голосовой трафик из источников недоверенного.
- Организация очереди — Голосу нужно уделить первостепенное значение по всему другому трафику для уменьшения задержки во время перегрузки соединения.
- Фрагментация и чередование данных в канале (LFI) — Пакеты данных должны быть фрагментированы, и голосовые пакеты чередованы на медленных соединениях.

Трафик должен быть классифицирован, чтобы должным образом определить политику и поместить голосовые пакеты в очередь. В этом разделе описывается классификация сделана на AARNet. Последующие главы описывают применение политик и реализацию организации очереди.

Классификация

Не весь трафик получает то же QoS. Трафик классифицирован в эти категории для выборочного обеспечения QoS:

- Данные
- Голос от известного и надежных источников
- Голос от неизвестных источников

Только надежным устройствам дают высококачественное QoS на AARNet. Эти устройства являются в основном шлюзами, определенными IP-адресом. Список контроля доступа (ACL) используется для определения этих надежных источников голоса.

```
access-list 20 permit 192.168.134.10
access-list 20 permit 192.168.255.255
```

Приоритет IP-трафика используется для различения голосового трафика от трафика данных. Голос имеет приоритет IP-трафика 5.

```
class-map match-all VOICE
match ip precedence 5
```

Объедините предыдущие примеры для определения пакетов от надежного источника.

```
class-map match-all VOICE-GATEWAY
match class-map VOICE
match access-group 20
```

Используйте те же принципы для определения голосовых пакетов от неизвестного источника.

```
class-map match-all VOICE-NOT-GATEWAY
match class-map VOICE
match not access-group 20
```

Применение политик

Когда трафик поступает в интерфейс, голосовой трафик из источника недоверенного классифицирован и отмечен. Эти два примера показывают, как применение политик выполнено в зависимости от того, какой трафик, как ожидают, поступит в данный интерфейс:

Если существуют речевые источники, которым доверяют, нисходящий, маршрутизатор ищет голосовые пакеты недоверенного и изменяет их приоритет IP-трафика на 0.

```
policy-map INPUT-VOICE
class VOICE-NOT-GATEWAY
set ip precedence 0

interface FastEthernet2/0/0
description Downstream voice gateways
service-policy input INPUT-VOICE
```

Если нет никаких известных речевых источников нисходящий, маршрутизатор ищет все голосовые пакеты и изменяет их приоритет IP-трафика на 0.

```
policy-map INPUT-DATA
class VOICE
set ip precedence 0

interface FastEthernet2/0/1
description No downstream voice gateways
service-policy input INPUT-DATA
```

Неголосовая организация очереди

Весь VoIP в AARNet был обходом междугородней АТС до недавнего времени. Это условие приводит к относительно немногим оконечным точкам VoIP. Текущая организация очереди различает интерфейсы, которые имеют VoIP - устройства нисходящий и интерфейсы, которые не делают. В этом разделе рассматриваются организацию очереди на неинтерфейсах VoIP.

Неголосовой интерфейс настроен или для обслуживания очередей на основе равнодоступности (WFQ) или для Взвешенного произвольного раннего обнаружения (WRED). Они могут быть настроены непосредственно на интерфейсе. Однако механизм организации очередей применен посредством карты политик, чтобы облегчить изменять механизм организации очередей на типе данного интерфейса. Существует одна карта политик на тип интерфейса. Это отражает факт, что не все механизмы организации очередей поддерживаются на всех интерфейсах.

```
policy-map OUTPUT-DATA-ATM
class class-default
fair-queue

policy-map OUTPUT-DATA-VIP-ATM
class class-default
random-detect

policy-map OUTPUT-DATA-ETHERNET
class class-default
fair-queue

policy-map OUTPUT-DATA-VIP-ETHERNET
class class-default
random-detect

policy-map OUTPUT-DATA-SERIAL
class class-default
fair-queue

policy-map OUTPUT-DATA-VIP-SERIAL
class class-default
random-detect
```

Карты политик являются присоединенными к соответствующим интерфейсам и являются определенными для типов интерфейса. Например, это упрощает процесс изменения

механизма организации очередей на основанном на многоцелевом интерфейсном процессоре (на основе VIP) Порты Ethernet от WRED до WFQ. Это требует одиночного изменения в карте политик. Изменения внесены во все на основе VIP Интерфейсы Ethernet.

```
interface ATM0/0
service-policy output OUTPUT-DATA-ATM

interface ATM1/0/0
service-policy output OUTPUT-DATA-VIP-ATM

interface Ethernet2/0
service-policy output OUTPUT-DATA-ETHERNET

interface Ethernet3/0/0
service-policy output OUTPUT-DATA-VIP-ETHERNET

interface Serial4/0
service-policy output OUTPUT-DATA-SERIAL

interface Serial5/0/0
service-policy output OUTPUT-DATA-VIP-SERIAL
```

Формирование очереди с низким временем задержки

Любой интерфейс, который доверял нисходящему VoIP - устройства, настроен для Организации очереди с малой задержкой (LLQ). Любой пакет, который делает его через классификацию входящих интерфейсов и сохраняет приоритеты 5, подвергается LLQ. Любой другой пакет подвергается или WFQ или WRED. Это зависит от типа интерфейса.

Карты отдельной политики созданы для каждого типа интерфейса для создания QoS легче администрировать. Это подобно неголосовой организации очереди. Однако карты несколька правил существуют для каждого типа интерфейса. Это вызвано тем, что емкость типов интерфейса для переноса голосового трафика варьируется в зависимости от скорости связи, параметров настройки PVC, и так далее. Номер на название карты политик отражает количество вызовов, обслуженных 30 вызовов, 60 вызовов, и так далее.

```
policy-map OUTPUT-VOICE-VIP-ATM-30
class VOICE
priority 816
class class-default
random-detect

policy-map OUTPUT-VOICE-VIP-ATM-60
class VOICE
priority 1632
class class-default
random-detect

policy-map OUTPUT-VOICE-ATM-30
class VOICE
priority 816
class class-default
random-detect

policy-map OUTPUT-VOICE-ATM-60
class VOICE
priority 1632
class class-default
random-detect
```

```
policy-map OUTPUT-VOICE-ETHERNET-30
class VOICE
priority 912
class class-default
fair-queue

policy-map OUTPUT-VOICE-VIP-ETHERNET-30
class VOICE
priority
class class-default
random-detect

policy-map OUTPUT-VOICE-HDLC-30
class VOICE
priority 768
class class-default
fair-queue
```

Карты политик присоединены к соответствующим интерфейсам. В данном примере карта политик является определенной для типа интерфейса. В настоящее время никакая специальная обработка не дана голосовой сигнализации. Карты политик могут легко быть исправлены в одном месте, если это становится требованием в последующем этапе на типе данного интерфейса. Изменение берет влияние для всех интерфейсов того типа.

```
Interface ATM0/0
service-policy output OUTPUT-VOICE-ATM-30

interface ATM1/0/0
service-policy output OUTPUT-VOICE-VIP-ATM-30

interface Ethernet2/0
service-policy output OUTPUT-VOICE-ETHERNET-60

interface Ethernet3/0/0
service-policy output OUTPUT-VOICE-VIP-ETHERNET-60

interface Serial4/0
service-policy output OUTPUT-VOICE-SERIAL-30

interface Serial5/0/0
service-policy output OUTPUT-VOICE-VIP-SERIAL-60
```

Масштабируемость LLQ

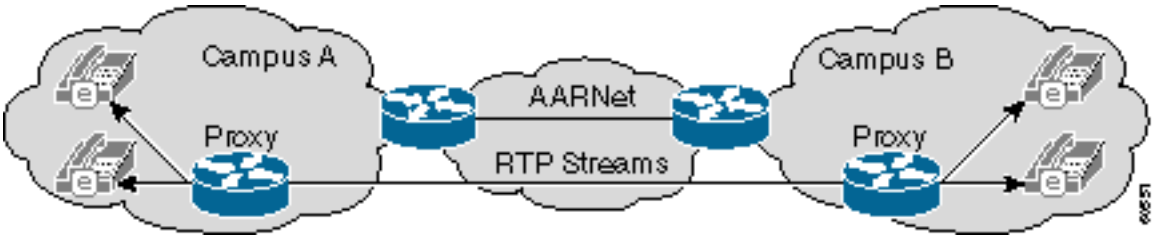
Механизм организации очередей имеет некоторые проблемы масштабирования. Основная проблема - то, что это полагается на знание IP-адреса каждого доверяемого VoIP - устройства в сети. Когда было ограниченное число Шлюзов VoIP, обрабатывающих обход междугородней АТС, это было разумным ограничением в прошлом. Количество оконечных точек VoIP существенно увеличивается, и это становится более непрактичным с развертываниями IP-телефонии. ACL становятся слишком длинными и слишком твердыми для управления.

ACL были добавлены для доверия трафику от определенного голоса подсеть IP в каждом кампусе ACU в случае ACU. Это - временное решение. Эти долгосрочные решения исследуются:

- Прокси H.323
- Применение политик входящих средств QoS

Основная идея позади решения прокси H.323 должна иметь весь трафик RTP, вводят

AARNet от данного кампуса посредством прокси. AARNet видит весь трафик RTP от данного кампуса с одним IP-адресом, поскольку эта схема показывает:

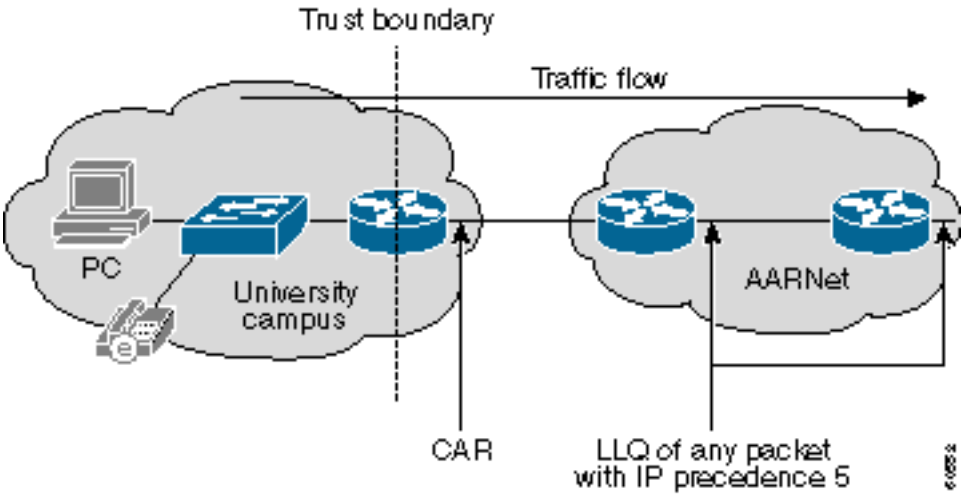


Если эта схема последовательно, развертывается количество записей в QoS на базе списков ACL ограничено одной линией на кампус. Эта схема все еще имеет потенциал для составления в целом 100 или больше записей, так как существует 37 университетов со сложными кампусами. Это также не является масштабируемым. Могло бы быть необходимо переместиться в дизайн с синглом или ограниченным числом совместно используемых суперпрокси в каждом RNO. Это сокращает количество доверенных IP-адресов к шесть. Однако это открывает проблему политик QoS на пути от кампуса до прокси в RNO.

Примечание: Внутрикластерные магистрали Cisco CallManager в настоящее время не работают через прокси H.323, потому что межкластерная сигнализация не является собственным H.225.

Применение политик входящих средств QoS является альтернативным решением. Граница надежности установлена в точке, где кампус соединяется с RNO с этим дизайном. Трафик, который вводит AARNet, охраняется Cisco функция IOS® Committed Access Rate (CAR) на этой границе. Университет, который использует AARNet для VoIP, подписывается на определенную величину пропускной способности AARNet QoS. CAR тогда контролирует трафик, который вводит AARNet. Если сумма трафика RTP с приоритетом IP-трафика 5 превышает подписанную пропускную способность, дополнительному трафику отметили приоритет IP-трафика к 0.

Эта схема показывает Конфигурацию CAR:



Данный пример показывает, как Конфигурация CAR обрабатывает это применение политик:

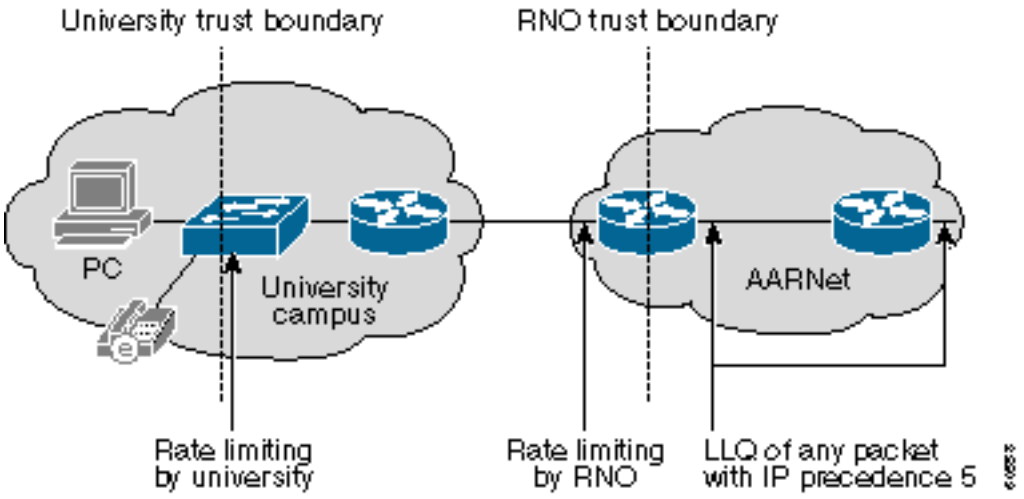
```
Interface a1/0.100
rate-limit input access-group 100 2400000 0 0 conform-action set-prec-transmit 5
exceed-action set-prec-transmit 0

access-list 100 permit udp any range 16384 32767 any range
 16384 32767 precedence critical
```

Это некоторые преимущества подхода Конфигурации CAR:

- Ядро больше не должно обрабатывать применение политик. Это теперь обрабатывается в границе надежности. Поэтому LLQ в ядре не должен знать о доверяемых IP-адресах. Любой пакет с приоритетом IP-трафика 5 в ядре может безопасно подвергнуться LLQ, потому что это уже передало применение политик во входе.
- Никакие предположения не сделаны об архитектуре VoIP, оборудовании и протоколах, которые выбирают отдельные университеты. Университет может принять решение развернуть Протокол SIP или Протокол MGCP, который не работает с прокси H.323. Пакеты VoIP получают соответствующее QoS в ядре, пока у них есть приоритет IP-трафика 5.
- CAR эластичен против атак Отказа в обслуживании (DoS) QoS. Атака DoS QoS, которая происходит из университета, не может повредить ядро. CAR ограничивает атаку, которая не может генерировать больше трафика, чем, что присутствует, когда максимальное число позволенных вызовов VoIP активно.Вызовы VoIP к или от того кампуса могут пострадать во время атаки. Однако это до отдельного университета для защиты себя внутренне. Университет может сжать ACL CAR на маршрутизаторе так, чтобы почти выбрал подсети VoIP, отметили приоритет IP-трафика.Каждый кампус имеет внутреннюю границу надежности в точке, где пользователи соединяются с локальной сетью уровня кампуса в конечной схеме. Трафик с приоритетом IP-трафика 5, который получает эта граница надежности, ограничен 160 кбит/с за порт коммутатора, или два вызова VoIP G.711. Трафик сверх этой скорости отмечен. Реализация этой схемы требует Коммутаторов Catalyst 6500 или чего-то похожего с функциональностью ограничения скорости.
- Инициализация пропускной способности в ядре упрощает, поскольку каждый университет подписывается на фиксированный размер полосы пропускания QoS. Это также делает QoS, тарифицирующее простой, потому что каждый университет может заплатить фиксированную помесячную абонементную плату на основе подписки полосы пропускания QoS.

Главный недостаток в этом дизайне - то, что граница надежности расположена в маршрутизаторе университета, таким образом, университеты должны быть в состоянии правильно администрировать CAR. Граница надежности задержана в RNO. Администрируемое RNO оборудование обрабатывает применение политик в конечной схеме. Этот дизайн требует аппаратного ограничения скорости, такого как Коммутатор Catalyst 6000 или Network Services Engine Cisco 7200 (NSE-1 Cisco 7200) процессор. Однако это дает AARNet и полный контроль RNO над политиками QoS. Эта схема показывает этот дизайн:



Фрагментация и чередование данных в канале

VoIP только несут через относительно виртуальные каналы высокоскоростного режима асинхронной передачи (VC). Поэтому никакой LFI не требуется. VoIP может также быть транспортирован через Frame Relay Forum (FRF) или выделенные линии в подразделения университета в будущем. Это требует механизмов LFI, таких как Протокол PPP (MLP) с Чередованием или FRF.12.

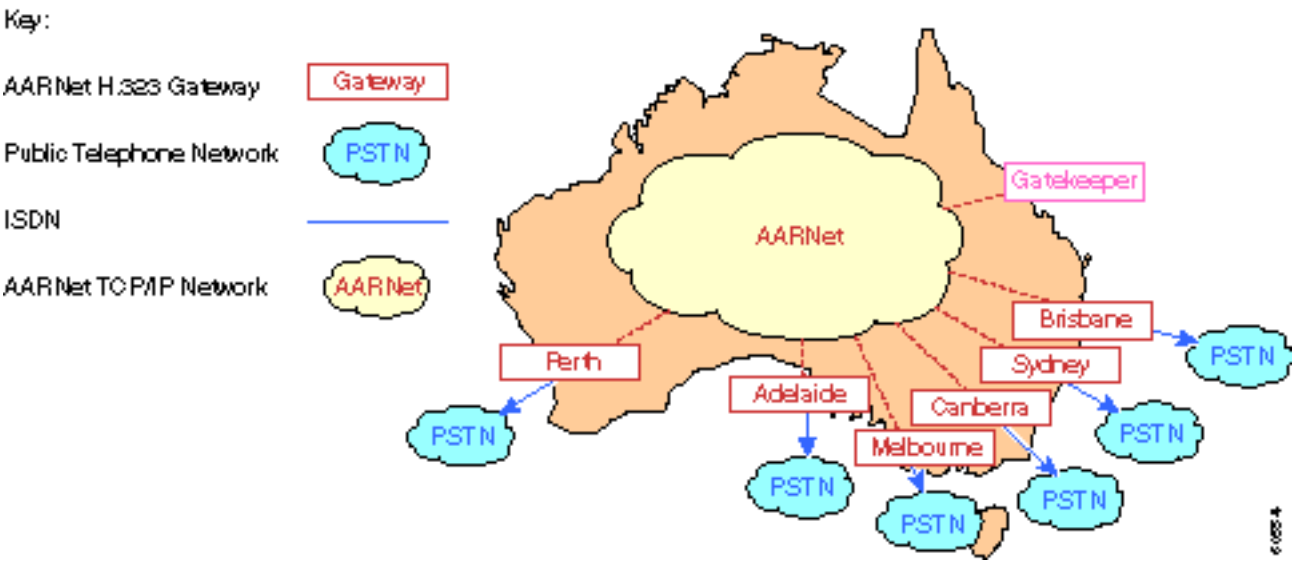
Шлюзы

Существует два вида шлюзов H.323 в AARNet:

- PSTN — PSTN к Шлюзу VoIP
- PABX — PABX к Шлюзу VoIP

Различие между PSTN и шлюзом PABX в основном функционально. Шлюзы PSTN предоставляют подключение PSTN. Шлюзы PABX подключают университетский PABX с магистралью VoIP. Та же физическая коробка действует и как PSTN и как шлюз PABX во многих случаях. В Решении IP-телефонии ACU в настоящее время существует 31 шлюз. Большинством этих шлюзов являются Универсальные серверы доступа Cisco AS5300. Другими шлюзами являются Маршрутизаторы серии Cisco 3600 или Маршрутизаторы серии Cisco 2600. Минимум десять дополнительные шлюзы, как ожидают, будет добавлен во время Q2CY01. AARNet нес приблизительно 145,000 вызовов VoIP в апреле 2001.

AARNet развернул подключенные PSTN шлюзы H.323 в большинстве крупнейших городов, поскольку эта схема показывает:



Университеты могут использовать эти шлюзы для создания исходящих вызовов к PSTN. Университеты должны поддержать свои собственные транки для входящих вызовов, потому что они в настоящее время не поддерживаются. AARNet может выполнить согласование об очень конкурентоспособной цене с носителем из-за громкости вызовов, которые проходят эти шлюзы. Вызовы могут также быть понижены в большей части экономически эффективного этапа. Например, кто-то в Сиднее, кто вызывает Номер Perth, может использовать шлюз Perth и только быть обвинен за локальный вызов. Это также известно как Переход конечного участка (TEHO).

Одно сторожевое устройство развернуто для выполнения E.164 к разрешению IP-адреса. Все вызовы к PSTN передаются сторожевому устройству, которое тогда возвращает IP-адрес самого соответствующего шлюза. См. Схемы набора номеров и Сторожевое устройство разделяет для более подробной информации о сторожевых устройствах.

Тарификация и учет

Шлюзы PSTN используют RADIUS и аутентификацию, авторизацию и учет (AAA) для выставлений счетов. Каждый вызов через шлюз генерирует Подробную запись о вызове (CDR) для каждой ветви вызовов. Этот CDRs зарегистрирован к серверу RADIUS. IP-адрес Cisco CallManager в CDR однозначно определяет университет и гарантирует, что тарифицирована корректная сторона.

Безопасность шлюза

Защита шлюзов PSTN против атак DoS и мошенничества является важным вопросом. Клиенты H.323 широко доступны. Microsoft NetMeeting связан с Microsoft Windows 2000, таким образом, для нетехнического пользователя относительно легко разместить бесплатные вызовы через эти шлюзы. Настройте входящий ACL, который разрешает H.225, сигнализирующему от доверяемых IP-адресов защищать эти шлюзы. Этот подход имеет весь одинаковый проблемы масштабирования, которые описывает раздел QoS. Количество записей в ACL растет, как растет количество доверяемых оконечных точек H.323.

Прокси H.323 предлагают некоторое облегчение в этой области. Если все вызовы через шлюз PSTN проходят через прокси уровня кампуса, списки управления доступом (ACL) шлюза должны разрешить один IP-адрес на университетское общежитие. Два IP-адреса как резервный прокси выбираемы в большинстве случаев. Даже с прокси, ACL может содержать больше чем 100 записей.

Прокси должен быть защищен через ACL, так как любой H.323 может установить вызов через прокси. ACL прокси должен разрешить локальные устройства H.323, поскольку локальная политика требует, так как это сделано на на выполняетсю для каждого кампуса.

Если кампус хочет позволить только вызовам от IP-телефонов использовать PSTN - шлюзы AARNet, IP-адреса этих двух Cisco CallManager должны быть включены в списки управления доступом (ACL) шлюза. Прокси не добавляют значения в этой ситуации. Количество требуемых записей ACL равняется двум так или иначе.

Обратите внимание на то, что IP-ТЕЛЕФОН К ВЫЗОВАМ IP межкампуса не должен проходить через прокси.

Планы дозвона

Текущая схема набора номеров VoIP является прямой. Пользователи могут разместить эти два типа вызовов с точки зрения Шлюза VoIP:

- Вызовите телефон в другом кампусе, но в том же университете.
- Вызовите телефон PSTN или телефон в другом университете.

Адресуемые точки вызова шлюза отражают факт, что существует только два типа вызовов. В основном существует два типа VoIP однорангового соединение, как показано в примере:

```
dial-peer voice 1 voip
destination-pattern 7…
session-target ipv4:x.x.x.x

dial-peer voice 1 voip
destination-pattern 0……
session-target ras
```

Первая точка вызова используется, если кто-то вызывает расширение 7... в другом кампусе в данном примере. Этот вызов направлен непосредственно к IP-адресу удаленного шлюза. Так как сторожевое устройство обойдено, Управление контролем доступа (CAC) не выполнено.

Когда вызов для номера PSTN, вторая точка вызова используется. Это может быть любой одним из этих элементов:

- Количество телефона в PSTN
- Полностью определенное количество PSTN телефона в другом университете

Вызов передается сторожевому устройству посредством запроса на доступ (ARQ) сообщение в первом случае. Сторожевое устройство возвращает IP-адрес лучшего шлюза PSTN в подтверждении допуска (ACF) сообщение.

Вызов также передается сторожевому устройству посредством сообщения ARQ во втором случае. Однако сторожевое устройство возвращает сообщение ACF с IP-адресом Шлюза VoIP в университете, который принимает вызов.

Сторожевое устройство

AARNet в настоящее время управляет одним сторожевым устройством. Единственная цель этого сторожевого устройства должна выполнить маршрутизацию вызова в форме E.164 к разрешению IP-адреса. Сторожевое устройство не выполняет CAC. Количество транков

PABX, связанных со шлюзами, ограничивает количество одновременных вызовов. Базовая пропускная способность обслуживает все транки в использовании сразу. Это изменяется с развертыванием IP-телефонии в ACU и других университетах. Нет никакого естественного предела на количестве одновременных вызовов VoIP, которые могут быть получены в или из данного кампуса в этой новой среде. Если слишком много вызовов инициируются, доступная полоса пропускания QoS может быть превышена. Все вызовы могут пострадать от низкого качества при этом условии. Используйте сторожевое устройство для обеспечения CAC.

Распределенный характер и потенциальный размер университетской голосовой сети предоставляют себя распределенной архитектуре гэйткипера. Одно возможное решение должно иметь двухуровневую иерархическую структуру гэйткипера, в которой каждый университет поддерживает свое собственное сторожевое устройство. Этот привратник университета упоминается как уровень 2 сторожевых устройства. AARNet управляет *сторожевым устройством каталога*, которое упоминается как уровень 1 сторожевое устройство.

Университеты должны использовать этот двухуровневый подход для использования сторожевого устройства для маршрутизации вызова между Кластерами Cisco CallManager. Сторожевое устройство направляет вызовы на основе 4-или 5-разрядного расширения в этом сценарии. Каждый университет требует своего собственного сторожевого устройства. Это вызвано тем, что наложение диапазонов расширения между университетами, так как это - локально администрируемое адресное пространство.

Университетский ярус 2 сторожевых устройства выполняет CAC для вызовов к и из того университета только. Это также выполняет разрешение E.164 для вызовов между только кампусами того университета. Вызов направлен уровнем 2 сторожевых устройства к уровню 1 сторожевое устройство посредством запроса местонахождения (LRQ) сообщение, если кто-то вызывает IP-телефон в другом университете или вызывает PSTN через Шлюз AARNet. Если вызов для другого университета, LRQ передан уровню 2 сторожевых устройства того университета. Это сторожевое устройство тогда возвращает сообщение ACF к уровню 2 сторожевых устройства в университете, где происходит вызов. Оба уровня 2 сторожевых устройства выполняют CAC. Они только продолжают вызов, если существует достаточная пропускная способность, доступная в обоих вызов и вызванные зоны.

AARNet может принять решение рассматривать PSTN - шлюзы AARNet как те из любого университета. Их собственный уровень 2 сторожевых устройства заботится о них. Уровень 1 сторожевое устройство может также действовать как уровень 2 сторожевых устройства для этих шлюзов, если загрузка и производительность разрешают.

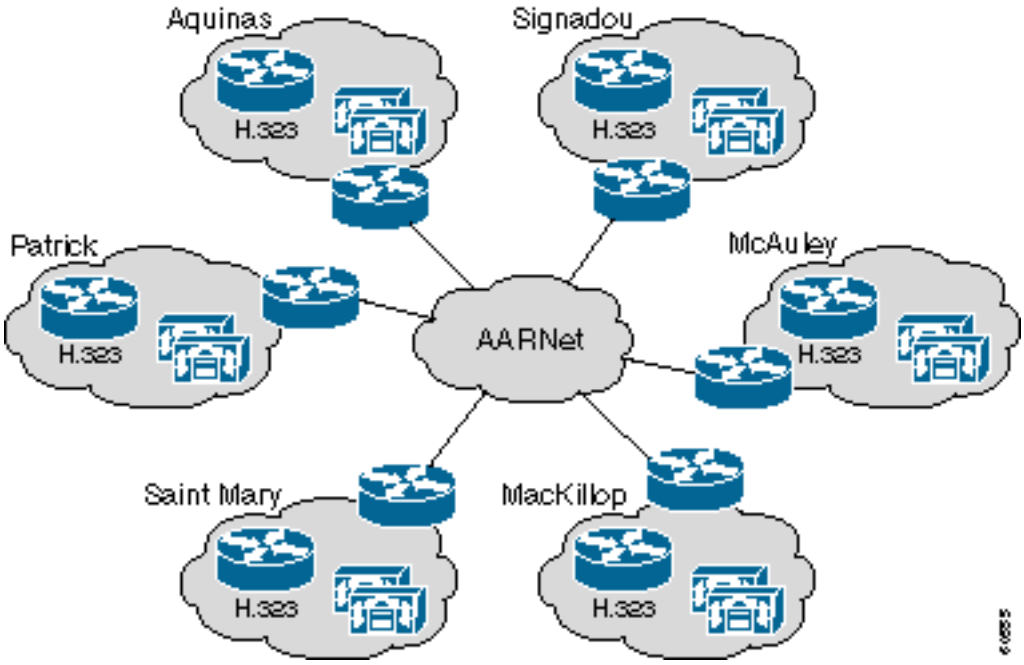
Каждое из сторожевых устройств (включая сторожевое устройство каталога AARNet) должно быть реплицировано, потому что шлюзы являются таким критически важным компонентом. Каждый университет должен иметь два сторожевых устройства. Для шлюзов Cisco IOS возможно иметь альтернативные сторожевые устройства, как в случае программного обеспечения Cisco IOS версии 12.0(7)T. Однако это в настоящее время не поддерживается Cisco CallManager или любым другим сторонним устройством H.323. Не используйте эту функцию в это время. Используйте простое Горячее резервирование основанное на протоколе маршрутизатора (основанное на HSRP) решение вместо этого. Это требует, чтобы оба сторожевых устройства находились в той же подсети IP. HSRP определяет, какое сторожевое устройство активно.

Сеть IP-телефонии в католических университетах Австралии

Эта таблица показывает приблизительное количество IP-телефонов, установленных в кампусах ACU:

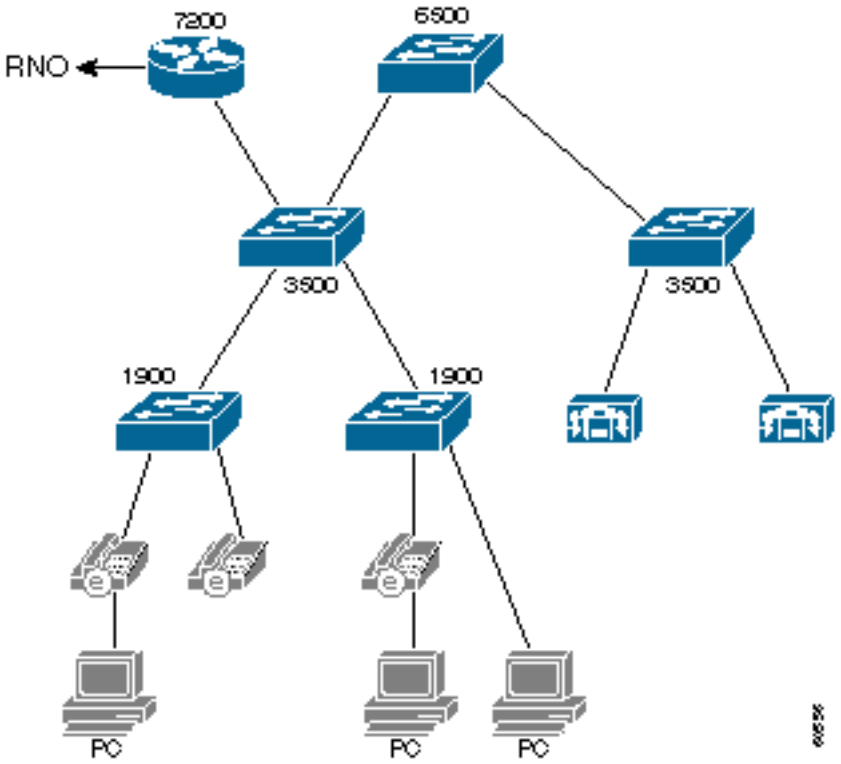
Кампус	Город	Приблизительные IP-телефоны
Saint Mary установки	Стратфилд	400
Маккиллоп	Северный Сидней	300
Patrick	Мельбурн	400
Aquinas	Балларат	100
Signadou	Канберра	100
Маколи	Брисбен	400
	Общее количество:	*1700*

ACU недавно развернул Решение IP-телефонии. Решение состоит из кластера двух Cisco CallManager, шлюза Cisco 3640 в каждом кампусе и IP-телефонов. AARNet соединяет кампусы. Эта схема изображает высокоуровневую топологию и различные компоненты Сети для IP-телефонии ACU:



Сетевая топология ACU

Эта схема показывает типичный кампус ACU. Каждый кампус имеет три уровня Коммутаторов Catalyst. Коммутационный шкаф помещает более старые Коммутаторы Catalyst 1900. Коммутаторы Catalyst 1900 соединяются назад с Коммутатором Catalyst 3500XL посредством Extended Framing. Они соединяются назад с одиночным Коммутатором Catalyst 6509 посредством Гигабитного Ethernet (GE). Одиночный маршрутизатор VXR Cisco 7200 подключает кампус с AARNet VC ATM к локальному RNO.



Способ подключения к RNO отличается немного в зависимости от государства, поскольку эта таблица показывает. Виктория основывается на Классическом IP по ATM (RFC 1577). Другие RNO имеют прямую настройку PVC с инкапсуляцией RFC 1483 года. Протокол OSPF является протоколом маршрутизации, используемым между ACU и RNO.

Кампус	Состояние	Подключение к RNO	Маршрутный протокол
Saint Mary установки	NSW	PVC RFC 1483	OSPF
Маккиллоп	NSW	PVC RFC 1483	OSPF
Patrick	VIC	Классический IP RFC 1577 года по ATM	OSPF
Aquinas	VIC	Классический IP RFC 1577 года по ATM	OSPF
Signadou	ACT	PVC RFC 1483	OSPF
Маколи	QLD	PVC RFC 1483	OSPF

Транкинг поддержки Коммутаторов серии Catalyst 1900 на каналах связи только. Поэтому IP-телефоны и PC - все в одной большой VLAN. Фактически, весь кампус является одной большой VLAN и широковещательным доменом. Вторичные подсети IP используются из-за большого числа устройств. IP-телефоны находятся в одной подсети IP, и PC находятся на другом. Ядро AARNet доверяет подсети IP-телефона, и трафик к и от этой подсети IP подвергается LLQ.

Маршрутизатор Cisco 7200 направляет между основными и вторичными подсетями IP. Mutilayer Switch Feature Card (MSFC) в Коммутаторе Catalyst 6500 в настоящее время не используется.

Catalyst 3500XL и Коммутаторы Catalyst 6500 имеют Характеристики QoS, но им в

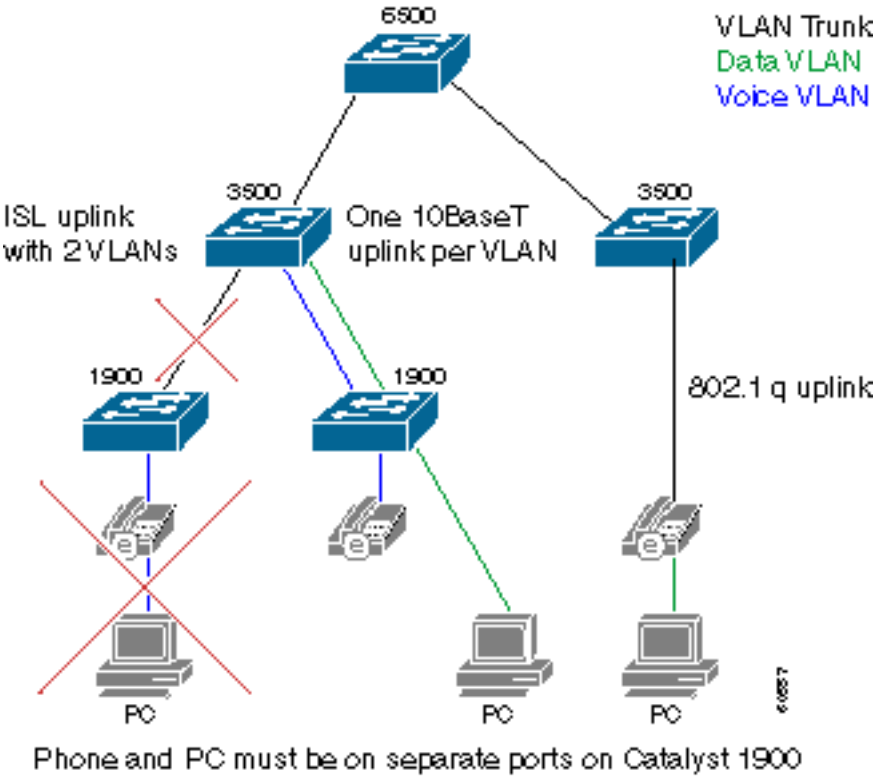
настоящее время не включают.

QoS в кампусе

Текущий проект уровня кампуса не соответствует рекомендациям по проектированию Cisco для IP-телефонии. Это некоторые опасения по поводу QoS:

- Широковещательный домен является очень большим. Избыточное широковещание может влиять на производительность IP-телефонов, которые должны обработать их.
- Коммутаторы Catalyst 1900 не способны к QoS. Если IP-телефон и ПК связаны с тем же портом коммутатора, голосовые пакеты могут быть отброшены, если ПК получает данные в высокой скорости.

Части модернизации инфраструктуры кампуса для достижения важных улучшений. Модернизация оборудования не требуется. Эта схема иллюстрирует принципы позади рекомендуемой модернизации:



Кампус должен быть разделен на голосовой VLAN и VLAN для передачи данных. Телефоны и PC, которые соединяются с коммутатором Catalyst 1900, должны теперь соединиться с другими портами для достижения Разделения VLAN. Добавлен дополнительный канал связи от каждого коммутатора Catalyst 1900 до коммутатора Cisco 3500XL. Один из этих двух каналов связи является участником голосового VLAN. Другой канал связи является участником VLAN для передачи данных. Не используйте Протокол ISL, соединяющий магистралью в качестве альтернативы двум каналам связи. Это не предоставляет трафику речевых пакетов и пакетов данных отдельные очереди. Ссылки GE от Коммутатора Catalyst 3500XL до Коммутатора Catalyst 6000 должны также быть преобразованы в магистрали "802.1q" так, чтобы обе VLAN речи и данных можно было нести через этот основной коммутатор.

Порты на Коммутаторе Catalyst 3500XL, которые находятся в VLAN для передачи данных, имеют класс по умолчанию Сервиса (CoS) нуля. Порты, которые являются участниками голосового VLAN, имеют CoS по умолчанию 5. В результате голосовой трафик правильно

расположен по приоритетам, как только он поступает в ядро Catalyst 3500 или Catalyst 6500. Конфигурации портов коммутатора QoS Catalyst 3500 варьируются немного, в зависимости от которого порт коммутатора VLAN является участником, как показано в примере:

```
Interface fastethernet 0/1
description Port member of voice VLAN
switchport priority 5
switchport access vlan 1

Interface fastethernet 0/2
description Port member of data VLAN
switchport priority 0
switchport access vlan 2
```

Можно подключить ПК с задним портом коммутатора на IP-телефоне в редком случае, который IP-телефоны подключают непосредственно с Коммутатором Catalyst 3500XL. IP-телефоны соединяются с коммутатором посредством магистрали "802.1q" в этом случае. Это позволяет пакетам речи и данных перемещаться на отдельных VLAN, и можно дать пакетам корректный CoS во входе. Коммутаторы Catalyst 1900 замены с Коммутаторами Catalyst 3500XL или другими способными к QoS коммутаторами, поскольку они достигают окончания срока службы. Эта топология тогда становится стандартным методом соединяющихся IP-телефонов и PC к сети. Этот сценарий показывает конфигурацию QoS Коммутатора Catalyst 3500XL:

```
Interface fastethernet 0/3
description Port connects to a 79xx IPhone
switchport trunk encapsulation dot1q
switchport priority extend 0
```

Наконец, два порта, которые соединяются с этими двумя Cisco CallManager, должны иметь жестко закодированный CoS к 3. Cisco CallManager устанавливает приоритет IP-трафика в 3 во всех пакетах голосовой сигнализации. Однако ссылка от Cisco CallManager до Коммутатора Catalyst 3500XL не использует 801.1p. Поэтому значение CoS вызвано в коммутаторе как показано в примере:

```
Interface fastethernet 0/1
description Port member of voice VLAN
switchport priority 3
switchport access vlan 1
```

Основное препятствие с этим дизайном - то, что два порта коммутатора требуются в Рабочем столе. Кампус Patrick мог бы потребовать дополнительных 400 порты коммутатора для 400 IP-телефонов. Если достаточные порты не доступны, должны быть развернуты дополнительные Коммутаторы Catalyst 3500XL. Только один порт Коммутатора Catalyst 3500XL требуется для каждых двух недостающих портов коммутатора Catalyst 1900.

Текущие Коммутаторы Catalyst 6500 ACU имеют возможности QoS, но им в настоящее время не включают. Эти модули присутствуют в Коммутаторе Catalyst 6000 ACU с этими возможностями организации очереди:

Слот	Модуль	Порты	Входные очереди (Rx)	Выходные очереди (Tx)
1	WS-X6K-SUP1A-2GE	2	1p1q4 т	1p2q2 т
3	WS-X6408-GBIC	8	1q4 т	2q2 т
4	WS-X6408-GBIC	8	1q4 т	2q2 т

5	WS-X6248-RJ-45	48	1q4 т	2q2 т
15	WS-F6K-MSFC	0	—	—

Выполните эти шаги для активации соответствующих Характеристик QoS на Коммутаторе Catalyst 6000:

1. Скажите коммутатору предоставлять QoS на для каждой VLAN основание с этой командой:`Cat6K>(enable)` **`set port qos 1/1-2,3/1-8,4/1-8 vlan-based`**
2. Скажите коммутатору доверять значениям CoS, полученным от Коммутатора Catalyst 3500XL с этой командой:`Cat6K>(enable)` **`set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos`**

CoS должен теперь быть установлен в сопоставление кодовой точки дифференцированных сервисов (DSCP). Это требуется, потому что Коммутатор Catalyst 6000 переписывает DSCP-значение в IP - заголовке на основе полученного значения CoS. Пакеты сигнализации VoIP должны иметь CoS 3, переписанный с DSCP AF31 (26). Пакеты RTP должны иметь CoS 5, переписанный с DSCP EF (46). Введите следующую команду:

`Cat6K>(enable)` **`set qos cos-dscp-map 0 8 16 26 32 46 48 56`**

Используйте данный пример для проверки Сопоставления CoS с DSCP.

`Cat6K> (enable)` **`show qos map run COs-DSCP-map`** `CoS - DSCP map: CoS DSCP --- ---- 0 0 1 8 2 16 3 26 4 32 5 46 6 48 7 56`

Настройте MSFC для маршрутизации между различными подсетями IP.

QoS в RNO

Текущий дизайн RNO не соответствует рекомендациям по проектированию Cisco для IP-телефонии. Эти проблемы существуют в отношении QoS:

- LLQ не применен на Маршрутизатор глобальной сети Cisco ACU серии 7200.
- Кампусы Patrick и Aquinas соединяются с RNO посредством коммутированных VC ATM (SVC). LLQ не поддерживается на SVC.

Подключенный Fast Ethernet Маршрутизатор Cisco 7200 подключает кампус с RNO посредством соединения ATM E4 на 34 Мбит/с. Трафик может потенциально стоять в очереди исходящий на 34M ссылки из-за 4M по сравнению с 100M несоответствие скорости. Поэтому необходимо расположить по приоритетам голосовой трафик. Используйте LLQ. Конфигурация Маршрутизатора Cisco 7200 подобна данному примеру:

```
class-map VoiceRTP
match access-group name IP-RTP

policy-map RTPvoice
class VoiceRTP
priority 10000

interface ATM1/0.1 point-to-point
description ATM PVC to RNO
pvc 0/100
tx-ring-limit 3
service-policy output RTPvoice

ip access-list extended IP-RTP
deny ip any any fragments
permit udp any range any range 16384 32768 precedence critical
```

Пропускная способность, выделенная LLQ, должна быть *N x 24 Кбит/с*, где N является

количеством одновременных вызовов G.729.

Установите один PVC от каждого Patrick и Маршрутизаторов Cisco 7200 Aquinas к маршрутизатору AARNet. SVC ATM в RNO Виктории не поддерживают LLQ, поскольку это основывается на Классическом IP по ATM (RFC 1577). Другие университеты в RNO Виктории могут продолжить использовать RFC 1577 на данный момент. Однако в конечном счете замените Классический IP по инфраструктуре ATM.

Шлюзы

Каждый из кампусов ACU имеет Маршрутизатор Cisco 3640, который действует как шлюз H.323. Эти шлюзы соединяются с PSTN посредством ISDN. Количество Интерфейсов первого уровня (PRI) и B-каналы зависит от размера кампуса. Эта таблица приводит количество PRI и B-каналов для каждого кампуса:

Кампус	Количество PRI	Количество B-канала
Saint Mary установки	2	30
Маккиллоп	2	50
Patrick	2	50
Aquinas	1	20
Signadou	1	20
Маколи	1	30

Эти шлюзы используются только в качестве вспомогательных шлюзов для DOD (Прямой номер внешнего набора). Шлюзы AARNet являются основными шлюзами. Шлюзы ACU всегда используются для DID (Direct Inward Dialing).

План дозвона

Схема набора номеров основывается на 4-разрядных добавочных номерах. Расширение является также последними четырьмя цифрами номера DID. Эта таблица приводит диапазоны расширения и номера DID для каждого кампуса:

Кампус	Расширение	DID
Saint Mary установки	9xxx	02 9764 9xxx
Маккиллоп	8xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Aquinas	5xxx	03 5330 5xxx
Signadou	2xxx	02 6123 2xxx
Маколи	7xxx	07 3354 7xxx

Простая запись `num-exp` на шлюзах усекает номер DID к 4-разрядному расширению, прежде чем это передаст его на Cisco CallManager. Например, шлюз кампуса Патрика имеет эту запись:

```
num-exp 84133... 3...
```

Пользователи набирают нуль для выбора внешней линии. Этот начальный нуль передан шлюзу. Одиночный узел обычной телефонной сети направляет вызов порт ISDN на основе начального нуля.

```
Dial-peer voice 100 pots
destination-pattern 0
direct-inward-dial
port 2/0:15
```

Входящие вызовы используют эту экспоненциальную запись для преобразования номера вызываемого абонента к 4-разрядному расширению. Вызов тогда совпадает с обоими VoIP одноранговыми соединение. На основе меньшего приоритета это предпочитает этот маршрут абоненту Cisco CallManager:

```
dial-peer voice 200 voip
preference 1
destination-pattern 3...
session target ipv4:172.168.0.4

dial-peer voice 201 voip
preference 2
destination-pattern 3...
session target ipv4:172.168.0.5
```

Cisco CallManager

Каждый из кампусов имеет кластер, который состоит из двух Cisco CallManager server. Cisco CallManager server являются соединением Сервера медиа-конвергенции 7835 (MCS-7835) и Сервер медиа-конвергенции 7820 (MCS-7820). Оба сервера выполнили версию 3.0 (10) во время этой публикации. Один Cisco CallManager является *издателем*, и другой Cisco CallManager является *абонентом*. Абонент действует как первичное Cisco CallManager для всех IP-телефонов. Эта таблица приводит аппаратные средства, развернутые в каждом кампусе:

Кампус	Платформа	CallManagers
Saint Mary установки	MCS-7835	2
Маккиллоп	MCS-7835	2
Patrick	MCS-7835	2
Aquinas	MCS-7820	2
Signadou	MCS-7820	2
Маколи	MCS-7835	2

Каждый кластер настроен с двумя областями:

- Один для вызовов внутрикампуса (G.711)
- Один для межкампусных вызовов (G.729)

Основанный на местоположении CAC не является соответствующим ACU, потому что все IP-телефоны, подаваемые каждым кластером, находятся в одиночном кампусе. Существуют

достоинства к основанному на сторожевом устройстве CAC для межкампусных вызовов, но это в настоящее время не внедряется. Однако существуют планы сделать так в ближайшем будущем.

Каждый Cisco CallManager настроен с 22 шлюзами H.323. Это составлено из внутрикластерных магистралей к пяти другим Кластерам Cisco CallManager, шести PSTN - шлюзам AARNet и одному шлюзу ACU в каждом кампусе.

Тип устройства H.323	Количество
CallManager межкампуса	2 x 5 = 10
PSTN - шлюз AARNet	6
PSTN - шлюз ACU	6
Общее количество:	*22*

Списки маршрутов и группы маршрутов используются для ранжирования шлюзов PSTN. Например, эта таблица показывает, как вызовы от Patrick Cisco CallManager в Мельбурне к Сиднейскому PSTN могут использовать эти четыре шлюза для связывания вызовов с группой маршрутов.

Шлюз	Приоритет
AARNet Sydney	1
ACU Sydney	2
AARNet Мельбурн	3
ACU Мельбурн	4

Cisco CallManager настроены приблизительно с 30 шаблонами маршрута, поскольку эта таблица показывает. Шаблоны маршрута разработаны, таким образом, существуют определенные соответствия для всех внутренних австралийских номеров. Таким образом, пользователи не должны ждать таймаута при передаче цифр для истечения, прежде чем Cisco CallManager будет инициировать вызов. Подстановочный знак"!" используется только в шаблоне маршрута для международных номеров. Пользователи должны ждать, пока таймаут при передаче цифр (по умолчанию 10 секунд) не истекает перед ходами вызова, когда они набирают зарубеж. Пользователи могут также добавить шаблон маршрута "0.0011! # ". Пользователи могут тогда войти" #" после последней цифры, чтобы указать к Cisco CallManager, что набранный номер завершен. Это действие ускоряет международный набор.

Route Pattern	Описание
0. [2-9] XXXXXXX	Локальный вызов
0.00	Вызов при аварийной ситуации - если пользователь забывает набирать 0 для внешней линии
0.000	Вызов при аварийной ситуации
0.013	Помощь по каталогу
0.1223	—
0.0011!	Международные вызовы

0.02XXXXXXXX	Вызовы в Новый Южный Уэльс
0.03XXXXXXXX	Вызовы Виктории
0.04XXXXXXXX	Вызовы к сотовым телефонам
0.07XXXXXXXX	Вызовы в Квинсленд
0.086XXXXXXX	Вызовы в Западную Австралию
0.08XXXXXXXX	Вызовы в Южную Австралию и Северные Территории
0.1 [8-9] XXXXXXXX	Вызовы к 1800 xxx xxx и 1900 xxx xxx
0.1144X	Аварийная ситуация
0.119 [4-6]	Время и погода
0.1245X	Каталог
0.13 [1-9] XXX	Вызовы к 13xxxx номера
0.130XXXXXX	Вызовы к 1300 xxx xxx номера
2 [0-1] XX	Межкластерные вызовы к Signadou
3 [0-4] XX	Межкластерные вызовы к Patrick
5 [3-4] XX	Межкластерные вызовы к Aquinas
7 [2-5] XX	Межкластерные вызовы Маколи
8 [0-3] XX	Межкластерные вызовы Маккиллопу
9 [3-4] XX	Межкластерные вызовы для Установки Saint Mary
9 [6-7] XX	Межкластерные вызовы для Установки Saint Mary

Количество шлюзов, групп маршрутов, списков маршрутов и шаблонов маршрута, настроенных на ACU Cisco CallManager, имеет потенциал для роста до большого числа. Если новый шлюз RNO развернут, все пять Кластеров Cisco CallManager должны быть реконфигурированы с дополнительным шлюзом. Если ACU Cisco CallManager направляет вызовы VoIP непосредственно во все другие университеты и обходит PSTN в целом, еще хуже, сотни шлюзов должны быть добавлены. Ясно это не масштабируется очень хорошо.

Решение состоит в том, чтобы сделать Cisco CallManager управляемыми гэйткипером. Когда новый шлюз или Cisco CallManager добавлены где-нибудь в AARNet, необходимо только обновить сторожевое устройство. Каждый Cisco CallManager должен иметь только шлюз локального кампуса и анонимное устройство, настроенное, когда это происходит. Можно думать об этом устройстве как о транке точка - много точек. Это удаляет необходимость решетчатых транков PPP в модели схемы набора номеров Cisco CallManager. Группа одного маршрута указывает к анонимному устройству как предпочтительный шлюз и к локальному шлюзу как резервный шлюз. Если сторожевое устройство становится недоступным, локальный шлюз PSTN используется для определенных локальных вызовов и также для общих внешних вызовов. В настоящее время анонимное устройство может быть

или промежуточным кластером или H.225, но не обоими в то же время.

Cisco CallManager нужно меньше шаблонов маршрута со сторожевым устройством, чем он имеет теперь. В принципе Cisco CallManager нужен только образец одного маршрута"!" указывая на сторожевое устройство. В действительности, способ, которым вызовы направлены потребности быть более определенными по этим причинам:

- Некоторые вызовы (такие как вызовы к 1-800 или номера службы экстренной помощи) должны быть направлены через географически локальный шлюз. Кто-то в Мельбурне, кто набирает политику или сеть ресторанов, такую как Pizza Hut, не хочет быть связанным с политикой или Pizza Hut в Перте. Определенные шаблоны маршрута необходимы что точка непосредственно к шлюзу PSTN локального кампуса для этих номеров.Университеты, которые планируют выполнить будущие развертывания IP-телефонии, могут принять решение положиться исключительно на Шлюзы AARNet и не администрировать их собственные локальные шлюзы. Этим номерам должен был предварительно ожидать действительный код зоны Cisco CallManager прежде, чем передать его к сторожевому устройству для создания этой дизайнерской работы для вызовов, которые должны быть понижены локально. Например, Cisco CallManager может предварительно ожидать 003 к вызовам от мельбурнского телефона до Pizza Hut номер 1-800. Это позволяет сторожевому устройству направлять вызов к мельбурнскому Шлюзу AARNet. Шлюз снимает изоляцию с продвижения 003, прежде чем это разместит вызов в PSTN.
- Шаблоны маршрута использования с определенными соответствиями для всех внутренних номеров во избежание наличия пользователя ждут таймаута при передаче цифр, прежде чем будет инициироваться вызов.

Эта таблица показывает шаблоны маршрута для управляемого гэйткипером Cisco CallManager:

Route Pattern	Описание	Маршрут	Сторожевое устройство
0. [2-9] XXXXXXX	Локальный вызов	Список маршрутов	AARNet
0.00	Вызов при аварийной ситуации	Локальный шлюз	Нет
0.000	Вызов при аварийной ситуации	Локальный шлюз	Нет
0.013	Помощь по каталогу	Локальный шлюз	Нет
0.1223	—	Локальный шлюз	Нет
0.0011!	Международные вызовы	Список маршр	AARNet

		утов	
0.0011! #	Международные вызовы	Список маршрутов	AARNet
0.0 [2-4] XXXXXXX	Вызовы в Новый Южный Уэльс, Виктория и сотовые телефоны	Список маршрутов	AARNet
0.0 [7-8] XXXXXXX	Вызовы в Южную Австралию, Западную Австралию и Северные Территории	Список маршрутов	AARNet
0.1 [8-9] XXXXXXX	Вызовы к 1800 xxx xxx и 1900 xxx xxx	Локальный шлюз	Нет
0.1144X	Аварийная ситуация	Локальный шлюз	Нет
0.119 [4-6]	Время и погода	Локальный шлюз	Нет
0.13 [1-9] XXX	Вызовы к 13xxxx номера	Локальный шлюз	Нет
0.130XXX XXXX	Вызовы к 1300 xxx xxx номера	Локальный шлюз	Нет
[2-3] XXX	Вызовы к Signadou	Список маршрутов	ACU
5XXX	Вызовы к Aquinas	Список маршрутов	ACU
[7-9] XXX	Вызовы Маколи, Маккиллопу и Saint Mary установки	Список маршрутов	ACU

Сторожевое устройство направляет международные вызовы, которые не передаются через локальный шлюз. Это значительно, потому что AARNet может развернуть международные шлюзы в будущем. Если шлюз развернут в Соединенных Штатах, простое изменение конфигурации сторожевого устройства позволяет университетам размещать вызовы в US в национальных тарифах US.

Сторожевое устройство выполняет межкластерный вызов, направляющий на основе 4-разрядного расширения ACU. Это адресное пространство, скорее всего, накладывается на другие университеты. Это диктует тот ACU, администрируют его собственное сторожевое устройство и используют сторожевое устройство AARNet в качестве *сторожевого устройства каталога*. Столбец гэйткипера в этой таблице указывает, выполнена ли маршрутизация вызова привратником ACU или сторожевым устройством AARNet.

Примечание: Единственное Предупреждение с предложенным решением для сторожевого устройства - то, что анонимное устройство может в настоящее время быть или промежуточным кластером или H.225, но не обоими в то же время. Cisco CallManager полагается на сторожевое устройство для маршрутизации вызовов к обоим шлюзам (H.225) и другие Cisco CallManager (промежуточный кластер) с предложенным проектом. Обходной путь для этой проблемы не должен или использовать сторожевое устройство для межкластерной маршрутизации или рассматривать все вызовы через сторожевое устройство как H.225. Последний обходной путь означает, что некоторые дополнительные функции могли бы быть недоступными на межкластерных вызовах.

Voice Mail (Голосовая почта)

ACU имел три Приложения Active Voice Repartee OS/2-based серверы голосовой почты с Диалогическими телефонными платами до миграции к IP-телефонии. План состоит в том, чтобы снова использовать эти серверы в Среде IP - телефонии. Когда внедрено, каждый Сервер мгновенного ответа подключает с Cisco CallManager посредством протокола SMDI и Catalyst 6000 карту Станции внешнего обмена (FXS) с 24 портами. Это предоставляет голосовую почту для трех из этих шести кампусов, которая покидает три кампуса без голосовой почты. Не возможно должным образом совместно использовать один Сервер мгновенного ответа между пользователями на двух Кластерах Cisco CallManager, потому что нет никакого способа распространиться индикатор ожидания сообщения (MWI) через транк H.323 промежуточного кластера.

ACU мог бы купить три сервера Cisco Unity для кампусов, которые остаются. Эти серверы на основе Skinny, таким образом, не требуются никакие шлюзы. Эта таблица приводит решения для голосовой почты, если ACU покупает дополнительные серверы голосовой почты:

Кампус	Система голосовой почты	Шлюз
Saint Mary установки	Приложение Active Voice Repartee	Catalyst 6000 FXS с 24 портами
Маккиллоп	Приложение Active Voice Repartee	Catalyst 6000 FXS с 24 портами
Patrick	Приложение Active Voice Repartee	Catalyst 6000 FXS с 24 портами
Aquinas	Cisco Unity	—
Signadou	Cisco Unity	—
Маколи	Cisco Unity	—

Эти шесть серверов голосовой почты действуют в качестве отдельных островов голосовой почты в этом плане. Нет никакой сетевой работы с голосовой почтой.

Медиаресурсы

Аппаратные цифровые процессоры сигналов (DSP) в настоящее время не развертываются в ACU. Конференц-связь использует программный Мост конференц-связи на Cisco CallManager. Конференция между кластерами в настоящее время не поддерживается.

Перекодировка в настоящее время не требуется. Только G.711 и кодеры - декодеры G.729

используются, и они поддерживаются всеми развернутыми конечными устройствами.

Поддержка факса и модема

Факс и модемный трафик в настоящее время не поддерживаются Сетью для IP-телефонии ACU. Университет планирует использовать Catalyst 6000 карта FXS с 24 портами для этой цели.

Версии ПО

Эта таблица приводит ACU версий программного обеспечения, используемый во время этой публикации:

Платформа	Функция	Версия программного обеспечения
(диспетчер вызовов Call Manager)	IP-PBX	3.0 (10)
Catalyst 3500XL	Коммутатор распределения	12.0 (5.1) XP
Catalyst 6500	Основной коммутатор	5.5 (5)
Catalyst 1900	Коммутатор коммутационного шкафа	—
Процессор Cisco 7200	Маршрутизатор глобальной сети	12.1 (4)
Маршрутизатор Cisco 3640	Шлюз H.323	12.1 (3a) XI6

Дополнительные сведения

- Поддержка голосовых технологий
- Поддержка продуктов голосовой и IP-связи
- Устранение неполадок в системах IP-телефонии Cisco
- Cisco Systems – техническая поддержка и документация