Distribuição de Casos Práticos de telefonia IP: Australian Catholic University

Índice

Introdução

O acadêmico e a rede de pesquisa australianas (AARNet) são uma rede IP de alta velocidade de âmbito nacional que interconecte 37 universidades australianas assim como a organização do Commonwealth Scientific e de pesquisa industrial (CSIRO).

O AARNet foi construído inicialmente como uma rede de dados, mas levou a Voz sobre IP (VoIP) desde 2000 adiantado. A rede voip distribuída atualmente é uma solução do contorno de tarifa que leve chamadas VoIP entre as universidades e as private automatic branch exchanges (posto privado de comutação automática) CSIRO (PABX). Igualmente fornece os gateways da rede telefônica pública comutada (PSTN) que permitem o PSTN ao ponto de custo efetivo do desconectar no máximo. Por exemplo, um atendimento de um telefone PABX em Melbourne a um telefone PSTN em Sydney é levado como VoIP de Melbourne ao gateway PSTN de Sidney. É conectado lá ao PSTN.

O Australian Catholic University (ACU) é uma das universidades que conecta ao AARNet. Em finais de 2000, o ACU começou um desenvolvimento da Telefonia IP que distribuísse aproximadamente 2,000 Telefones IP através de seis campus de universidade.

Estes Casos Práticos cobrem o desenvolvimento da Telefonia IP ACU. O projeto é terminado. Contudo, há umas edições arquitetónicas significativas a endereçar no backbone de AARNet se a rede é escalar quando outras universidades seguem nos passos do ACU. Este documento descreve estas edições e propõe e discute várias soluções. O desenvolvimento da Telefonia IP ACU é provável ser ajustado mais tarde a fim cair na linha da arquitetura recomendada final.

Nota: A universidade Deakin era a primeira universidade australiana para distribuir a Telefonia IP. Contudo, a universidade Deakin não usa o AARNet para levar o tráfego da Telefonia IP.

AARNet

As universidades australianas e o CSIRO construíram o AARNet em 1990 com o Australian Vice-Chancellors' Committee (AVCC). O por cento da noventa-nove do tráfego do Internet australiano era aos membros fundadores durante os primeiros anos. Uma quantidade pequena de tráfego comercial era das organizações que tiveram uma associação próxima com o setor terciário e da pesquisa. Use pelo userbase NON-AARNet aumentado a 20 por cento do tráfego total em finais de 1994.

O AVCC vendeu a base de cliente comercial do AARNet a Telstra em julho de 1995. Este evento desovou o que era eventualmente se transformar Telstra BigPond. Isto estimulou um crescimento mais adicional do uso comercial e privado do Internet em Austrália. Transferência da propriedade intelectual e da experiência conduziu ao desenvolvimento do Internet em Austrália. Se não, isto não ocorreria em tal taxa rápida.

O AVCC desenvolveu AARNet2 em 1997 adiantado. Era um refinamento mais adicional do Internet em Austrália, que emprega enlaces ATM e serviços de Internet da largura de banda elevada sob um contrato com o Cable & Wireless Optus (CWO) limitado. A distribuição rápida dos Serviços IP pelo CWO para cumprir as exigências AARNet2 era devida na parte a transferência do conhecimento e da experiência do AARNet.

ACU

O ACU é uma universidade pública que seja estabelecida em 1991. A universidade tem aproximadamente 10,000 estudantes e pessoal 1,000. Há seis terrenos na costa leste de Austrália. Esta tabela mostra os campus de ACU e seus lugar:

Terreno	Cidade	Estado
Montagem Saint Mary	Strathfield	Novo Gales do Sul (NSW)
MacKillop	Norte de Sidney	Novo Gales do Sul (NSW)
Patrick	Melbourne	Victoria (VIC)
Aquinas	Ballarat	Victoria (VIC)
Signadou	Canberra	Australia Capital Territory (ATO)
McAuley	Brisbane	Queensland (QLD)

O ACU confiou em uma solução do Telstra Spectrum (Centrex) antes do lançamento da solução de telefonia do IP que estes Casos Práticos descrevem. O movimento à Telefonia IP foi conduzido principalmente pelo desejo reduzir o custo.

CSIRO

O CSIRO tem o pessoal aproximadamente 6,500 em locais numerosos em Austrália. O CSIRO conduz a pesquisa nas áreas tais como a agricultura, os minerais, a energia, a fabricação, as comunicações, a construção, a saúde, e o ambiente.

O CSIRO era a primeira organização para usar o AARNet para VoIP. A organização abriu caminho o funcionamento inicial feito nesta área.

AARNet

O backbone de AARNet é um componente significativo em todo o desenvolvimento da Telefonia IP da universidade. Fornece a interconexão de universidades os dois serviços principais na área da Voz:

- Transporte de pacotes Realtime do protocolo de transporte de VoIP (RTP) com a garantia do Qualidade de Serviço (QoS) apropriada para exprimir
- Ponto barato do hopoff aos PSTN em torno do país

Esta seção descreve a arquitetura atual de AARNet e como entrega estes serviços. Igualmente esboça algumas das questões de escalabilidade que elevaram enquanto mais universidades distribuem a solução de telefonia do IP. Finalmente, discute as soluções possíveis para estas questões de escalabilidade.

Topologia AARNet

O AARNet consiste em um único POP (Point of Presence) em cada estado. Os PNF são referidos como as operações da rede regional (RNO). As universidades conectam ao RNO em seu estado respectivo. Os RNO são interconectados por sua vez por uma malha cheia do ATM PVCs de Optus. Junto constituem o AARNet.

O RNO típico consiste em um switch ATM de Cisco LS1010 e em um roteador anexo ao ATM. O roteador de RNO conecta a cada roteador de universidade por um único ATM PVC através de um enlace de micro-ondas E3. Cada roteador de RNO igualmente tem uma malha cheia do ATM PVCs que a rede ATM de Optus forneça a todos RNO restantes. Este diagrama representa a topologia aarnet geral da rede:

Há umas várias exceções à topologia. Alguns delas são significativos de uma perspectiva da Voz. Estas são algumas exceções:

- O RNO em Victoria usa o IP clássico sobre ATM (RFC 1577) em vez dos PVC para conectar as universidades ao RNO.
- As universidades rurais conectam tipicamente de volta ao RNO pelo Frame Relay ou pelo ISDN.
- Algumas grandes universidades têm mais de um link de volta ao RNO.

Esta tabela mostra os estados e os territórios que têm atualmente um RNO. A tabela inclui cidades capital para os leitores que não são familiares com a geografia da Austrália.

Estado	Cidade capital	RNO?	Conexões de campus
Novo Gales do	Sydney	Sim	TBD

Sul			
Victoria	Melbourne	Sim	TBD
Queensland	Brisbane	Sim	TBD
Sul da Austrália	Adelaide	Sim	TBD
Austrália ocidental	Perth	Sim	TBD
Território da capital australiana	Canberra	Sim	TBD
Território northern	Darwin	Não	--
Tasmânia	Hobart	Não	--

Qualidade de Serviço

As partes do AARNet QoS-são permitidas já para a Voz em consequência do projeto do contorno de tarifa de VoIP. QoS é necessário para o tráfego de voz a fim fornecer estas características, que minimizam o retardo e tremulação e eliminam a perda de pacotes:

- Policiamento — Marque abaixo do tráfego de voz das fontes não-confiável.
- Enfileirar-se — A Voz deve ser dada a prioridade sobre todo tráfego restante para minimizar o atraso durante o congestionamento de enlace.
- Link Fragmentation and Interleaving (LFI) — Os pacotes de dados devem ser fragmentados e pacotes de voz ser intercalados em enlaces lentos.

O tráfego deve ser classificado para policiar e enfileirar corretamente pacotes de voz. Esta seção descreve como a classificação é feita no AARNet. Os Capítulos subsequente descrevem o policiamento e a implementação de fila.

Classificação

Não todo o tráfego obtém o mesmo QoS. O tráfego é classificado nestas categorias para fornecer seletivamente QoS:

- Dados
- Voz do sabido e origens confiável
- Voz dos origens desconhecida

Somente os dispositivos confiável são dados QoS de alta qualidade no AARNet. Estes dispositivos são principalmente gateways identificados pelo endereço IP de Um ou Mais Servidores Cisco ICM NT. Um Access Control List (ACL) é usado para identificar estes origens confiável da Voz.

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

A Precedência IP é usada para distinguir o tráfego de voz do tráfego de dados. A Voz tem uma Precedência IP do 5.

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

Combine os exemplos anteriores para identificar pacotes de um origem confiável.

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

Use os mesmos princípios para identificar pacotes de voz de um origem desconhecida.

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

Vigilância

O tráfego de voz de uma fonte não-confiável está classificado e marcado abaixo de quando o tráfego chega em uma relação. Estes dois exemplos mostram como policiar é executado segundo que tipo de tráfego é esperado chegar em uma dada interface:

O roteador procura pacotes de voz não-confiável e muda sua Precedência IP a 0 se há umas fontes confiadas da Voz rio abaixo.

```
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
```

O roteador procura todos os pacotes de voz e muda sua Precedência IP a 0 se não há nenhuma fonte conhecida da Voz rio abaixo.

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

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

Enfileiramento da NON-Voz

Todo o VoIP no AARNet era contorno de tarifa até recentemente. Esta circunstância conduz a relativamente poucos pontos finais de VoIP. O projeto de enfileiramento atual distingue entre as relações que têm dispositivos voip rio abaixo e as relações que não fazem. Esta seção discute enfileirar-se em relações de NON-VoIP.

Uma relação da NON-Voz é configurada para o Weighted Fair Queuing (WFQ) ou o Weighted Random Early Detection (WRED). Estes podem ser configurados diretamente na relação. Contudo, o mecanismo de filas é aplicado por meio de um mapa de política a fim fazê-lo fácil mudar o mecanismo de filas em um tipo de dada interface. Há um mapa de política pelo tipo de interface. Isto reflete o fato de que não todos os mecanismos de filas estão apoiados em todas as relações.

```
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
```

Os mapas da política são anexados às interfaces respectivas e são específicos aos tipos de interface. Por exemplo, isto simplifica o processo de mudar o mecanismo de filas em portas Ethernet (com base em VIP) Processador-baseadas interface versátil do WRED ao WFQ. Exige uma única mudança no mapa de política. As mudanças são feitas a todas as interfaces Ethernet com base em VIP.

```
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
```

Enfileiramento de latência baixa

Toda a relação que rio abaixo-confiar dispositivos voip é configurada para o Low Latency Queuing (LLQ). Todo o pacote que a fizer com a classificação da interface de entrada e o retiver uma precedência de 5 é sujeito ao LLQ. Todo o outro pacote é sujeito ao WFQ ou ao WRED. Isto depende do tipo de interface.

Os mapas da política separada são criados para cada tipo de interface a fim facilitar QoS administrar. Isto é similar ao projeto de enfileiramento da NON-Voz. Contudo, os mapas da política múltipla existem para cada tipo de interface. Isto é porque a capacidade dos tipos de interface para levar o tráfego de voz varia segundo a velocidade do link, ajustes PVC, e assim por diante. O número no nome do mapa de política reflete o número de atendimentos cobriu 30 atendimentos, 60 atendimentos, e assim por diante.

```
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
```

Os mapas da política são anexados às interfaces respectivas. Neste exemplo, o mapa de política é específico a um tipo de interface. Nenhum tratamento especial é dado atualmente à sinalização de voz. Os mapas da política podem facilmente ser alterados em um lugar se esta se transforma uma exigência ulteriormente em um tipo de dada interface. A mudança toma a influência para todas as relações desse tipo.

```
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
```

Escalabilidade LLQ

O mecanismo de filas tem algumas questões de escalabilidade. A questão principal é que confia em conhecer o endereço IP de Um ou Mais Servidores Cisco ICM NT de cada dispositivo voip

confiado na rede. Esta era uma limitação razoável no passado em que havia um número limitado de Gateway VoIP que seguram o contorno de tarifa. O número de pontos finais de VoIP aumenta dramaticamente, e torna-se cada vez mais pouco prático com o desenvolvimento da Telefonia IP. Os ACL tornam-se demasiado longos e demasiado duros de controlar.

Os ACL foram adicionados para confiar o tráfego de uma sub-rede específica IP da Voz em cada campus de ACU no caso do ACU. Esta é uma solução temporária. Estas soluções mais a longo prazo estão sendo investigadas:

- Proxy de H.323
- Policiamento do ingresso de QoS

A ideia principal atrás da solução de proxy de H.323 é mandar todo o tráfego RTP incorporar o AARNet de um terreno dado por meio de um proxy. O AARNet vê todo o tráfego RTP de um terreno dado com um único endereço IP de Um ou Mais Servidores Cisco ICM NT, porque este diagrama mostra:

O número de entradas no QoS ACL está limitado a uma linha pelo terreno se este esquema é distribuído consistentemente. Este esquema ainda tem o potencial adicionar acima a 100 ou mais entradas desde que há 37 universidades com campus múltiplos. Isto não é demasiado escalável. Pôde ser necessário mover-se para um projeto com um único ou um número limitado de super-proxys compartilhados em cada RNO. Isto reduz o número de endereços IP de Um ou Mais Servidores Cisco ICM NT confiados a seis. Contudo, isto abre uma edição do Regulamentação QoS no trajeto do terreno ao proxy no RNO.

Nota: Os troncos intercluster do CallManager da Cisco não funcionam atualmente com um proxy de H.323 porque o sinal intercluster não é H.225 nativo.

O policiamento do ingresso de QoS é uma solução alternativa. Um limite confiável é estabelecido no ponto onde o terreno conecta ao RNO com este projeto. Trafique que incorpora o AARNet é policiado pela característica do Committed Access Rate (CAR) de Cisco IOS® neste limite. Uma universidade que use o AARNet para VoIP subscreve a uma certa quantidade de largura de banda de AARNet QoS. O CAR monitora então o tráfego que incorpora o AARNet. O tráfego excedente tem a Precedência IP marcada para baixo a 0 se a quantidade de tráfego RTP com Precedência IP 5 excede a largura de banda subscrita.

Este diagrama mostra uma configuração CAR:

Este exemplo mostra como uma configuração CAR segura este policiamento:

```
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
```

Estas são algumas vantagens de uma aproximação da configuração CAR:

- O núcleo já não precisa de segurar o policiamento. É segurado agora no limite confiável. Consequentemente, o LLQ no núcleo não precisa de saber sobre endereços IP de Um ou Mais Servidores Cisco ICM NT confiados. Todo o pacote com uma Precedência IP de 5 no núcleo pode com segurança ser sujeito ao LLQ porque tem passado já o policiamento no ingresso.
- Nenhuma suposição é feita sobre a arquitetura de VoIP, o equipamento, e os protocolos que

as universidades individuais escolhem. Uma universidade pode escolher distribuir um Session Initiation Protocol (SIP) ou o Media Gateway Control Protocol (MGCP) que não trabalhe com proxys de H.323. Os pacotes voip recebem o QoS apropriado no núcleo enquanto têm uma Precedência IP do 5.

- O CAR é resiliente contra o ataque de recusa de serviço (DOS) de QoS. Um ataque DoS de QoS que origine de uma universidade não pode danificar o núcleo. O CAR limita o ataque, que não pode gerar mais tráfego do que o que esta presente quando o número máximo de chamadas VoIP permitidas é ativo.As chamadas VoIP a ou desse terreno podem sofrer durante um ataque. Contudo, é até a universidade individual para proteger-se internamente. A universidade pode apertar o CAR ACL no roteador de modo que todos com exceção das sub-redes selecionadas de VoIP tenham a Precedência IP marcada para baixo.Cada terreno tem um limite confiável interno no ponto onde os usuários conectam ao campus LAN no design final. Trafique com uma Precedência IP de 5 que este limite confiável receba seja limitado a 160 kbps pela porta de switch, ou a duas chamadas VoIP de G.711. O tráfego além desta taxa é marcado para baixo. A aplicação deste esquema exige os Catalyst 6500 Switch ou o algo similares com a taxa que limita a funcionalidade.
- O abastecimento da largura de banda no núcleo simplifica enquanto cada universidade subscreve a uma quantidade fixa de largura de banda de QoS. Isto igualmente faz a fatura de QoS simples porque cada universidade pode pagar uma taxa mensal lisa baseada em uma assinatura de largura de banda de QoS.

A fraqueza principal neste projeto é que o limite confiável está ficado situado no roteador de universidade, assim que as universidades devem poder administrar corretamente o CAR. O limite confiável é puxado de novo no RNO. o equipamento RNO-administrado segura o policiamento no design final. Este projeto exige a taxa com base em hardware que limita como o Catalyst 6000 Switch ou um processador do Mecanismo de serviços de rede do Cisco 7200 (Cisco 7200 NSE-1). Contudo, dá o controle completo AARNet e RNO sobre o Regulamentação QoS. Este diagrama mostra este projeto:

Fragmentação do link e intercalação

VoIP está sendo levado somente através relativamente dos circuitos virtuais do ATM de alta velocidade (VC). Consequentemente, nenhum LFI é exigido. VoIP pode igualmente ser transportado através do fórum de Frame Relay (FRF) ou das linhas alugadas às universidades rurais no futuro. Isto exige mecanismos LFI tais como o Multilink PPP (MLP) com intercalação ou FRF.12.

Gateways

Há dois tipos de Gateways H.323 no AARNet:

- PSTN — PSTN ao Gateway VoIP
- PABX — PABX ao Gateway VoIP

A distinção entre um PSTN e um gateway de PABX é principalmente funcional. Os gateways PSTN fornecem a Conectividade ao PSTN. Os gateways de PABX conectam uma universidade PABX ao backbone de VoIP. A mesma caixa física atua como um PSTN e um gateway de PABX em muitos casos. Há atualmente 31 gateways na solução de telefonia do IP ACU. A maioria destes gateways são servidores de acesso universal do Cisco AS5300. Os outros gateways são Cisco 3600 Series Router ou Cisco 2600 Series Router. Um mínimo de dez dos gateways adicionais é esperado ser adicionado durante o Q2CY01. O AARNet levou aproximadamente

145,000 chamadas VoIP em abril de 2001.

O AARNet distribuiu Gateways H.323 PSTN-anexado na maioria de cidades principais, porque este diagrama mostra:

As universidades podem usar estes gateways para fazer chamadas externas ao PSTN. As universidades têm que manter seus próprios troncos para chamadas recebidas porque não são apoiadas atualmente. O AARNet pode negociar muito um preço competitivo com o portador devido ao volume de atendimentos que atravessam estes gateways. Os atendimentos podem igualmente ser deixados cair fora no máximo do ponto de custo efetivo. Por exemplo, alguém em Sydney que chama um número perth pode usar o gateway Perth e somente ser carregado para uma chamada local. Isto é sabido igualmente como o desconectar da extremidade traseira (TEHO).

Um gatekeeper único é distribuído para executar o E.164 à definição do endereço IP de Um ou Mais Servidores Cisco ICM NT. Todos os atendimentos ao PSTN são enviados ao porteiro, que retorna então o endereço IP de Um ou Mais Servidores Cisco ICM NT do gateway o mais apropriado. Refira as seções dos Planos de discagem e do porteiro para informações mais detalhadas sobre dos porteiros.

Faturamento e contabilidade

Os gateways PSTN usam o RAIO e o Authentication, Authorization, and Accounting (AAA) para propósitos de faturamento. Cada atendimento através de um gateway gerencie um registro dos destalhes da chamada (CDR) para cada trecho de chamada. Estes CDR são afixados ao servidor Radius. O endereço IP de Um ou Mais Servidores Cisco ICM NT do CallManager da Cisco no CDR identifica excepcionalmente a universidade e assegura-se de que o partido correto esteja faturado.

Segurança de gateway

Proteger os gateways PSTN contra ataques e fraude DoS é uma maior preocupação. Os clientes de H.323 são amplamente disponíveis. O Microsoft NetMeeting é empacotado com Microsoft Windows 2000, assim que é relativamente fácil para um usuário não técnico colocar atendimentos livres através destes gateways. Configurar um ACL de entrada que permita a sinalização H.225 dos endereços IP de Um ou Mais Servidores Cisco ICM NT confiados proteger estes gateways. Esta aproximação tem todas as mesmas questões de escalabilidade que a seção de QoS descreve. O número de entradas no ACL cresce enquanto o número de valores-limite confiados de H.323 cresce.

Os proxys de H.323 oferecem algum relevo nesta área. O ACLS de gateway precisa de permitir um endereço IP de Um ou Mais Servidores Cisco ICM NT pelo campus de universidade se todos os atendimentos através da passagem do gateway PSTN com um proxy de campus. Dois endereços IP de Um ou Mais Servidores Cisco ICM NT como um proxy redundante são desejáveis na maioria dos casos. Mesmo com proxys, o ACL pode conter mais de 100 entradas.

O proxy deve ser protegido através dos ACL desde que todo o H.323 pode estabelecer um atendimento com o proxy. O proxy ACL deve permitir dispositivos locais de H.323 enquanto a política local exige desde que esta está feita em uma base do por-terreno.

Os endereços IP de Um ou Mais Servidores Cisco ICM NT dos dois CallManagers de Cisco devem ser incluídos no ACLS de gateway se um terreno quer permitir que somente os

atendimentos dos Telefones IP usem os gateways AARNet PSTN. Os proxys não adicionam nenhum valor nesta situação. O número de entradas ACL exigidas é dois de qualquer maneira.

Note que os atendimentos telefone-à-IP IP do intercampus não precisam de passar com o proxy.

Planos de discagem

O Plano de discagem atual de VoIP é direto. Os usuários podem colocar estes dois tipos de atendimentos de uma perspectiva do Gateway VoIP:

- Chame um telefone em um terreno diferente mas na mesma universidade.
- Chame um telefone PSTN ou um telefone em uma universidade diferente.

Os gateway dial peer refletem o fato de que há somente dois tipos de atendimentos. Basicamente há dois tipos do dial peer de VOIP, porque este exemplo mostra:

```
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
```

O primeiro dial peer é usado se alguém chama a extensão 7… em um outro terreno neste exemplo. Este atendimento é distribuído diretamente ao endereço IP de Um ou Mais Servidores Cisco ICM NT do gateway remoto. Desde que o porteiro é contorneado, o controle de admissão da chamada (CAC) não é executado.

O segundo dial peer é usado quando o atendimento é para um número PSTN. Este pode ser qualquer um um destes artigos:

- O número de um telefone no PSTN
- O número totalmente qualificado PSTN de um telefone em uma universidade diferente

O atendimento é enviado ao porteiro por meio de um mensagem de requisição de admissão (ARQ) no primeiro caso. O porteiro retorna o endereço IP de Um ou Mais Servidores Cisco ICM NT do melhor gateway PSTN em uma mensagem do Admission Confirm (ACF).

O atendimento é enviado igualmente ao porteiro por meio de um mensagem de ARQ no segundo caso. Contudo, o porteiro retorna um mensagem de ACF com o endereço IP de Um ou Mais Servidores Cisco ICM NT do Gateway VoIP na universidade que recebe o atendimento.

Gatekeeper

O AARNet opera atualmente um gatekeeper único. O propósito único deste porteiro é executar o roteamento de chamada sob a forma do E.164 à definição do endereço IP de Um ou Mais Servidores Cisco ICM NT. O porteiro não executa o CAC. O número de troncos PABX conectou aos gateways limita o número de chamadas simultâneas. A largura de banda do núcleo cobre todos os troncos no uso imediatamente. Isto muda com o lançamento da Telefonia IP no ACU e nas outras universidades. Não há nenhum limite natural no número de chamadas VoIP simultâneas em que pode ser originado ou fora de um terreno dado neste ambiente novo. A largura de banda de QoS disponível pode ser oversubscribed se atendimentos demais são iniciados. Todos os atendimentos podem sofrer da qualidade ruim sob esta circunstância. Use o porteiro para fornecer o CAC.

O tamanho da natureza distribuída e do potencial da rede de voz da universidade empresta-se a uma arquitetura de gatekeeper distribuída. Uma solução possível é ter um projeto de gatekeeper hierárquico de dois níveis em que cada universidade mantém seu próprio porteiro. Este gatekeeper de universidade é referido como um porteiro da série 2. O AARNet opera um *gatekeeper de diretório* que seja referido como um porteiro da série 1.

As universidades devem usar esta aproximação de dois níveis para usar um porteiro para o roteamento de chamada entre Cluster do CallManager daCisco. O porteiro distribui os atendimentos baseados em uns 4 ou em uma extensão 5-digit nesta encenação. Cada universidade exige seu próprio porteiro. Isto é porque as escalas da extensão sobrepõem entre universidades desde que este é um espaço de endereços local-administrado.

Os porteiros do alinhamento de universidade 2 executam o CAC para atendimentos a e dessa universidade somente. Igualmente executa a definição E.164 para atendimentos entre somente os terrenos dessa universidade. O atendimento é distribuído pelo porteiro da série 2 ao porteiro da série 1 por meio de uma mensagem do Location Request (LRQ) se alguém chama um telefone IP em uma outra universidade ou chama o PSTN através de um gateway AARNet. O LRQ está encaminhado ao porteiro da série 2 dessa universidade se o atendimento é para uma outra universidade. Este porteiro retorna então um mensagem de ACF ao porteiro da série 2 na universidade onde o atendimento origina. Ambos os porteiros da série 2 executam o CAC. Continuam somente com o atendimento se há uma largura de banda suficiente disponível em ambos a chamada e as zonas chamadas.

O AARNet pode escolher tratar os gateways AARNet PSTN como aqueles de toda a universidade. Seu próprio porteiro da série 2 ocupa d. O porteiro da série 1 pode igualmente atuar como o porteiro da série 2 para estes gateways se a carga e o desempenho permitem.

Cada um dos porteiros (que incluem o gatekeeper de diretório AARNet) precisa de ser replicated porque os gateways são tal componente crítico. Cada universidade precisa de ter dois porteiros. É possível para Cisco IOS gateway ter gatekeeperes alternativos, como no caso do Cisco IOS Software Release 12.0(7)T. Contudo, isto não é apoiado atualmente pelo CallManager da Cisco ou por nenhum outro dispositivo da terceira de H.323. Não use esta característica neste tempo. Use uma solução (HSRP-baseada) com base nos protocolos do roteador simples do standby recente pelo contrário. Isto exige que ambos os porteiros se sentam na mesma sub-rede IP. O HSRP determina que porteiro é ativo.

Rede de telefonia IP ACU

Esta tabela mostra o número aproximado de Telefones IP instalado nos terrenos do ACU:

Terreno	Cidade	Telefones IP aproximados
Montagem Saint Mary	Strathfield	400
MacKillop	Norte de Sidney	300
Patrick	Melbourne	400
Aquinas	Ballarat	100
Signadou	Canberra	100
McAuley	Brisbane	400
	Total:	***1700***

O ACU distribuiu recentemente uma solução de telefonia do IP. A solução consiste em um conjunto de dois CallManagers de Cisco, em um gateway do Cisco 3640 em cada terreno, e em Telefones IP. O AARNet interconecta os terrenos. Este diagrama descreve a topologia de nível elevado e os vários componentes da rede de telefonia do IP ACU:

Topologia de rede de ACU

Este diagrama mostra um campus típico de ACU. Cada terreno tem três camadas de Catalyst Switches. O armário de fiação abriga os Catalyst 1900 Switch mais velhos. Os Catalyst 1900 Switch conectam de volta ao Catalyst 3500XL Switch por meio do Extended Framing. Estes conectam de volta a um único Catalyst 6509 Switch por meio do gigabit Ethernet. Um único roteador do Cisco 7200VXR conecta o terreno ao AARNet por um ATM VC ao RNO local.

O método de conectividade ao RNO difere levemente do estado para indicar, porque esta tabela mostra. Victoria é baseada no IP clássico sobre ATM (RFC 1577). Os outros RNO têm um PVC reto setup com encapsulamento do RFC 1483. O Open Shortest Path First (OSPF) é o protocolo de roteamento usado entre o ACU e os RNO.

Terreno	Estado	Conectividade ao RNO	Routing Protocol
Montagem Saint Mary	NSW	RFC 1483 PVC	OSPF
MacKillop	NSW	RFC 1483 PVC	OSPF
Patrick	VIC	IP clássico do RFC 1577 sobre o ATM	OSPF
Aquinas	VIC	IP clássico do RFC 1577 sobre o ATM	OSPF
Signadou	ATO	RFC 1483 PVC	OSPF
McAuley	QLD	RFC 1483 PVC	OSPF

O entroncamento do apoio dos Catalyst 1900 Series Switch nos uplinks somente. Consequentemente, todos os Telefones IP e os PC são em um grande VLAN. De fato, o terreno inteiro é uns grandes VLAN e domínio de transmissão. As sub-redes secundárias IP são usadas devido ao número grande de dispositivos. Os Telefones IP estão em uma sub-rede IP, e os PC estão em outra. O núcleo AARNet confia a sub-rede do telefone IP, e o tráfego a e desta sub-rede IP é sujeito ao LLQ.

As rotas do Cisco 7200 Router entre as sub-redes preliminares e secundárias IP. O Mutilayer Switch Feature Card (MSFC) no Catalyst 6500 Switch não é usado atualmente.

O Catalyst 3500XL e os Catalyst 6500 Switch têm características de QoS, mas não é permitido atualmente.

QoS no campus

O projeto de campus atual não segue com as diretrizes do projeto Cisco-recomendadas para a Telefonia IP. Estes são alguns interesses sobre QoS:

- O domínio de transmissão é muito grande. Os broadcasts excessivos podem afetar o desempenho dos Telefones IP, que têm que os processar.

- Os Catalyst 1900 Switch não são QoS-capazes. Se um telefone IP e um PC são conectados à mesma porta de switch, os pacotes de voz podem ser deixados cair se o PC recebe dados em uma taxa alta.

Remodele partes da infraestrutura de campus para conseguir melhorias significativas. Uma upgrade de hardware não é exigida. Este diagrama ilustra os princípios atrás do redesign recomendado:

O terreno deve ser rachado em uma Voz VLAN e em um VLAN de dados. Os telefones e os PC que conectam a um Catalyst 1900 Switch devem agora conectar às portas diferentes a fim conseguir a separação de vlan. Um uplink adicional de cada Catalyst 1900 Switch ao Cisco 3500XL Switch é adicionado. Um dos dois uplinks é um membro da Voz VLAN. O outro uplink é um membro do VLAN de dados. Não use o entroncamento do InterSwitch Link (ISL) como uma alternativa a dois uplinks. Isto não fornece a voz e tráfego de dados as filas separadas. Os links GE do Catalyst 3500XL Switch ao Catalyst 6000 Switch devem igualmente ser convertidos aos troncos 802.1Q de modo que a Voz e o VLAN de dados possam ser levados através deste switch central.

As portas no Catalyst 3500XL Switch que estão no VLAN de dados têm uma classe padrão de serviço (CoS) de zero. As portas que são membros da Voz VLAN têm um padrão CoS de 5. em consequência, o tráfego de voz são dadas a prioridade corretamente uma vez que chega no núcleo do Catalyst 3500 ou do Catalyst 6500. As configurações de porta de switch de QoS do Catalyst 3500 variam levemente segundo que porta de switch VLAN é um membro, porque este exemplo mostra:

```
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
```

Você pode conectar um PC à porta de switch traseira no telefone IP no caso raro que os Telefones IP conectam diretamente a um Catalyst 3500XL Switch. Os Telefones IP conectam ao interruptor por meio de um tronco 802.1Q neste caso. Isto permite que os pacotes de voz e de dados viajem em VLAN separados, e você pode dar a pacotes o CoS correto no ingresso. Substitua Catalyst 1900 Switch com os Catalyst 3500XL Switch ou o outro Switches QoS-capaz como alcançam o fim da vida. Esta topologia transforma-se então o método padrão de conectar Telefones IP e PC à rede. Esta encenação mostra a configuração de QoS do Catalyst 3500XL Switch:

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

Finalmente, as duas portas que conectam dois a Cisco os CallManagers devem ter o CoS com hardcode a 3. CallManager da Cisco ajustam a Precedência IP a 3 em todos os pacotes da sinalização de voz. Contudo, o link do CallManager da Cisco ao Catalyst 3500XL Switch não usa 801.1p. Consequentemente, o valor de CoS é forçado no interruptor enquanto este exemplo mostra:

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

```
switchport access vlan 1
```

O obstáculo principal com este projeto é que duas portas de switch estão exigidas no Desktop. O campus Patrick pôde exigir portas extra de um 400 Switch para 400 Telefones IP. Os Catalyst 3500XL Switch adicionais devem ser distribuídos se as suficientes portas não estão disponíveis. Somente uma porta do Catalyst 3500XL Switch é exigida para cada duas portas faltantes do Catalyst 1900 Switch.

Os Catalyst 6500 Switch atuais ACU têm potencialidades de QoS, mas não são permitidos atualmente. Estes módulos estam presente no Catalyst 6000 Switch ACU com estas potencialidades de enfileiramento:

Slot	Módulo	Portas	Filas RX	Filas TX
1	WS-X6K-SUP1A-2GE	2	1p1q4t	1p2q2t
3	WS-X6408-GBIC	8	1q4t	2q2t
4	WS-X6408-GBIC	8	1q4t	2q2t
5	WS-X6248-RJ-45	48	1q4t	2q2t
15	WS-F6K-MSFC	0		

Termine estas etapas para ativar as características de QoS apropriadas no Catalyst 6000 Switch:

1. Diga o interruptor para fornecer QoS em uma base do VLAN per. este comando:`Cat6K>(enable)`**`set port qos 1/1-2,3/1-8,4/1-8 vlan-based`**
2. Diga o interruptor para confiar os valores de CoS recebidos do Catalyst 3500XL Switch com este comando:`Cat6K>(enable)`**`set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos`**

O CoS deve agora ser ajustado ao traço do Differentiated Services Code Point (DSCP). Isto é exigido porque o Catalyst 6000 Switch reescreve o valor DSCP no cabeçalho IP baseado no valor recebido de CoS. Os pacotes de sinalização voip devem ter um CoS de 3, reescrito com um DSCP de AF31 (26). Os pacotes RTP devem ter um CoS de 5, reescrito com um DSCP de EF (46). Emita este comando:

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

Use este exemplo para verificar o mapeamento de CoS-to-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
```

Configurar o MSFC para distribuir entre as várias sub-redes IP.

QoS no RNO

O projeto atual RNO não segue com as diretrizes do projeto Cisco-recomendadas para a Telefonia IP. Estes interesses existem com respeito a QoS:

- O LLQ não é aplicado no WAN Router do Cisco ACU 7200 Series.
- Os terrenos de Patrick e de Aquinas conectam ao RNO por meio de VC comutados ATM (SVC). O LLQ não é apoiado em SVC.

Um Cisco 7200 Router Ethernet-anexado rápido conecta o terreno a um RNO por meio de um enlace ATM do 34 Mbps E4. O tráfego pode potencialmente enfileirar acima de partida nos links de 34M devido aos 4M contra a má combinação da velocidade de 100M. Consequentemente, é necessário dar a prioridade ao tráfego de voz. Use o LLQ. A configuração do Cisco 7200 Router é

similar a este exemplo:

```
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
```

A largura de banda atribuída ao LLQ deve ser *N x 24Kbps*, onde N é o número de atendimentos simultâneos de G.729.

Estabelecer um PVC de cada um de Patrick e dos Cisco 7200 Router de Aquinas ao roteador AARNet. O ATM SVC em Victoria RNO não apoia o LLQ, porque é baseado no IP clássico sobre ATM (RFC 1577). As outras universidades em Victoria RNO podem continuar a usar por agora o RFC 1577. Contudo, substitua eventualmente o IP clássico sobre a infraestrutura de ATM.

Gateways

Cada um dos campus de ACU tem um Cisco 3640 Router que atue como um gateway de H.323. Estes gateways conectam ao PSTN por meio do ISDN. O número das relações da taxa principal (PRI) e dos canais B depende do tamanho do terreno. Esta tabela alista o número de PRI e de canais B para cada terreno:

Terreno	Quantidade de PRI	Quantidade do canal B
Montagem Saint Mary	2	30
MacKillop	2	50
Patrick	2	50
Aquinas	1	20
Signadou	1	20
McAuley	1	30

Estes gateways são usados somente como gateways secundários para DOD (discagem direta para o exterior). Os gateway AARNet são os gateways principais. Os gateways de ACU são usados sempre para FIZERAM (Direct Inward Dialing).

Plano de discagem

O Plano de discagem é baseado em números de extensão do 4-dígito. A extensão é igualmente os últimos quatro dígitos do numerou. Esta tabela alista as escalas da extensão e FEZ números para cada terreno:

Terreno	Extensão	FEZ
Montagem Saint Mary	9xxx	02 9764 9xxx
MacKillop	8xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Aquinas	5xxx	03 5330 5xxx
Signadou	2xxx	02 6123 2xxx
McAuley	7xxx	07 3354 7xxx

`Uma entrada num-exp` simples nos gateways trunca numerou à extensão do 4-dígito antes que a passe sobre ao CallManager da Cisco. Por exemplo, o gateway do campus Patrick tem esta entrada:

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

Os usuários discam zero para selecionar uma linha exterior. Este zero principal é passado sobre ao gateway. Um único POTS dial peer distribui chamar que a porta de ISDN baseou no zero principal.

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

As chamadas recebidas usam esta entrada num-exp para transformar o número da parte chamada a uma extensão do 4-dígito. O atendimento combina então ambos os dial peer de VOIP. Baseado na preferência inferior, prefere esta rota ao subscritor do CallManager da Cisco:

```
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

Cada um dos terrenos tem um conjunto que consista em dois servidores do CallManager da Cisco. Os servidores do CallManager da Cisco são uma mistura do Media Convergence Server 7835 (MCS-7835) e o Media Convergence Server 7820 (MCS-7820). Ambos os server executaram a versão 3.0(10) na altura desta publicação. Um CallManager da Cisco é o *editor* e o outro CallManager da Cisco é o *subscritor*. O subscritor atua como o CallManager da Cisco principal para todos os Telefones IP. Esta tabela alista o hardware distribuído em cada terreno:

Terreno	Plataforma	CallManagers
Montagem Saint Mary	MCS-7835	2

MacKillop	MCS-7835	2
Patrick	MCS-7835	2
Aquinas	MCS-7820	2
Signadou	MCS-7820	2
McAuley	MCS-7835	2

Cada conjunto é configurado com duas regiões:

- Se para o intracampus chama (G.711)
- Um para chamadas entre campus (G.729)

O CAC baseado em localização não é apropriado para o ACU porque todos os Telefones IP servidos por cada conjunto estão em um único terreno. Há uns méritos a um CAC porteiro-baseado para chamadas entre campus, mas este não é executado atualmente. Contudo, há uns planos a fazer tão em um futuro próximo.

Cada CallManager da Cisco é configurado com 22 Gateways H.323. Isto é composto dos troncos intercluster aos cinco outros Cluster do CallManager daCisco, a seis gateways AARNet PSTN, e a um gateway de ACU em cada terreno.

Tipo de dispositivo de H.323	Quantidade
CallManager de Intercampus	2 x 5 = 10
Gateway AARNet PSTN	6
Gateway ACU PSTN	6
Total:	*22*

As lista e os grupos de rotas da rota são usados para classificar os gateways PSTN. Por exemplo, esta tabela mostra como os atendimentos do CallManager da Cisco de Patrick em Melbourne ao Sydney PSTN podem usar os quatro gateways para amarrar os atendimentos junto com um grupo de rotas.

Gateway	Prioridade
AARNet Sydney	1
Australian Catholic University de Sidney	2
AARNet Melbourne	3
Australian Catholic University em Melbourne	4

Os CallManagers de Cisco são configurados com aproximadamente 30 rotas padrão, porque esta tabela mostra. As rotas padrão são projetadas tão lá são fósforos específicos para todos os números australianos domésticos. Esta maneira, os usuários não tem que esperar o interdigit timeout para expirar antes que o CallManager da Cisco inicie o atendimento. O caractere wildcard “!” é usado somente na rota padrão para números internacionais. Os usuários devem esperar até que o interdigit timeout (segundos do padrão 10) expire antes dos andamentos da chamada quando discam um destino internacional. Os usuários podem igualmente adicionar a rota padrão "0.0011!#". Os usuários podem então entrar no “#” depois que o dígito último para indicar ao CallManager da Cisco que o número discado está completo. Esta ação expede o discagem internacional.

Rota padrão	Descrição
	Chamada local
0.00	Chamada de emergência - se o usuário esquece disca 0 para a linha exterior
0.000	Chamada de emergência
0.013	Assistência de diretório
0.1223	
0.0011!	Chamadas internacionais
	Chama a Novo Gales do Sul
	Chama a Victoria
	Chama aos celulares
	Chama a Queensland
	Chama à austrália ocidental
	Atendimentos ao Sul da Austrália e ao território northern
	Atendimentos a 1800 xxx xxx de xxx xxx e 1900
0.1144X	Emergência
0.119[4-6]	Tempo e tempo
0.1245X	Diretório
0.13[1-9]XXX	Chama aos números 13xxxx
	Chama a 1300 números xxx xxx
2[0-1]XX	Chamadas inter-grânulo a Signadou
3[0-4]XX	Chamadas inter-grânulo a Patrick
5[3-4]XX	Chamadas inter-grânulo a Aquinas
7[2-5]XX	Chamadas inter-grânulo a McAuley
8[0-3]XX	Chamadas inter-grânulo a MacKillop
9[3-4]XX	Chamadas inter-grânulo para montar Saint Mary
9[6-7]XX	Chamadas inter-grânulo para montar Saint Mary

O número de gateways, grupos de rotas, rota alista, e as rotas padrão configuradas nos CallManagers ACU Cisco têm o potencial vir um número grande. Se um gateway RNO novo é distribuído, todos os cinco Cluster do CallManager daCisco devem ser reconfigurados com um gateway adicional. Mesmo mais ruim, as centenas de gateways precisam de ser adicionadas se os CallManagers ACU Cisco distribuem chamadas VoIP diretamente a todas universidades restantes e contorneiam o PSTN completamente. Claramente isto não escala muito bem.

A solução é fazer os CallManagers de Cisco controlados por gatekeeper. Você deve somente atualizar o porteiro quando um gateway novo ou o CallManager da Cisco são adicionados em algum lugar no AARNet. Cada CallManager da Cisco deve ter somente o gateway do campus local e o dispositivo anônimo configurados quando este acontece. Você pode pensar deste dispositivo como um tronco point-to-multipoint. Remove a necessidade para os troncos engrenados PPP no modelo do Plano de discagem do CallManager da Cisco. Um grupo da rota única aponta ao dispositivo anônimo como o gateway preferido e ao gateway local como o

gateway de backup. O gateway PSTN local é com certeza chamadas local usadas e igualmente para chamadas fora da rede gerais se o porteiro se torna não disponível. Atualmente, o dispositivo anônimo pode ser intercluster ou H.225, mas não ambos ao mesmo tempo.

O CallManager da Cisco precisa menos rotas padrão com um porteiro do que tem agora. Em princípio, o CallManager da Cisco precisa somente um teste padrão da rota única de “!” apontar ao porteiro. Na realidade, a maneira em que os atendimentos são distribuídos precisa de ser mais específica por estas razões:

- Alguns atendimentos (tais como atendimentos a 1-800 ou números de emergência) precisam de ser distribuídos geograficamente através de um gateway local. Alguém em Melbourne que disca a polícia ou uma cadeira de restaurante tal como o Pizza Hut não quer ser conectado à polícia ou ao Pizza Hut em Perth. As rotas padrão específicas são precisadas que apontam diretamente ao gateway PSTN do campus local para estes números.As universidades que planeiam executar as disposições futuras da Telefonia IP podem escolher confiar unicamente nos gateway AARNet e não administrar seus próprios gateways locais. Estes números devem ter um código de área virtual prepended pelo CallManager da Cisco antes de enviá-lo ao porteiro a fim fazer este trabalho do projeto para os atendimentos que precisam de ser deixados cair fora localmente. Por exemplo, o CallManager da Cisco pode prepend 003 aos atendimentos de um telefone Melbourne-baseado ao número do Pizza Hut 1-800. Isto permite que o porteiro distribua o atendimento a um gateway AARNet Melbourne-baseado. O gateway descasca os 003 de condução antes que coloque o atendimento no PSTN.
- Use rotas padrão com fósforos específicos para todos os números domésticos a fim evitar ter a espera do usuário para o interdigit timeout antes que o atendimento esteja iniciado.

Esta tabela mostra as rotas padrão para um CallManager da Cisco controlado por gatekeeper:

Rota padrão	Descrição	Rota	Gatekeeper
	Chamada local	Lista da rota	AARNet
0.00	Chamada de emergência	Gateway local	Nenhum
0.000	Chamada de emergência	Gateway local	Nenhum
0.013	Assistência de diretório	Gateway local	Nenhum
0.1223		Gateway local	Nenhum
0.0011!	Chamadas internacionais	Lista da rota	AARNet
0.0011!#	Chamadas internacionais	Lista da rota	AARNet
	Chama a Novo Gales do Sul, a Victoria, e aos celulares	Lista da rota	AARNet
	Chama ao Sul da Austrália, à austrália ocidental, e ao território northern	Lista da rota	AARNet

	Atendimentos a 1800 xxx xxx de xxx xxx e 1900	Gatew ay local	Nenhum
0.1144X	Emergência	Gatew ay local	Nenhum
0.119[4-6]	Tempo e tempo	Gatew ay local	Nenhum
0.13[1-9]XXX	Chama aos números 13xxxx	Gatew ay local	Nenhum
	Chama a 1300 números xxx xxx	Gatew ay local	Nenhum
[2-3]XXX	Chama a Signadou	Lista da rota	ACU
5XXX	Chama a Aquinas	Lista da rota	ACU
[7-9]XXX	Chama a McAuley, a MacKillop, e a montagem Saint Mary	Lista da rota	ACU

O porteiro distribui as chamadas internacionais, que não são enviadas através do gateway local. Isto é significativo porque o AARNet pode distribuir gateways internacionais no futuro. Se um gateway é distribuído no Estados Unidos, uma mudança de configuração de gatekeeper simples permite que as universidades coloquem atendimentos aos E.U. em taxas domésticas E.U.

O porteiro executa o roteamento da chamada inter-grânulo baseado na extensão ACU do 4-dígito. Este espaço de endereços sobrepõe muito provavelmente com outras universidades. Isto dita que o ACU administra seu próprio porteiro e usa o gatekeeper AARNet como um *gatekeeper de diretório*. A coluna de gatekeeper nesta tabela indica se o roteamento de chamada está executado pelo gatekeeper ACU ou pelo gatekeeper AARNet.

Nota: A única advertência com a solução proposta do porteiro é que o dispositivo anônimo pode atualmente ser intercluster ou H.225, mas não ambos ao mesmo tempo. O CallManager da Cisco confia no porteiro para distribuir atendimentos a ambos os gateways (H.225) e a outros CallManagers de Cisco (intercluster) com o projeto proposto. A ação alternativa para esta edição é não ao uso o porteiro para o roteamento intercluster ou para tratar todos os atendimentos através do porteiro como o H.225. A última ação alternativa significa que algumas características suplementares puderam ser não disponíveis em chamadas inter-grânulo.

Correio de voz

O ACU teve três servidores de correio de voz da voz ativa com resposta OS/2-based com placas Dialogic do telefone antes da migração à Telefonia IP. O plano é reutilizar estes server no ambiente de telefonia IP. Quando executado, cada servidor repartee conecta a um CallManager da Cisco por meio de um Simplified Message Desk Interface (SMDI) e de um cartão da estação de câmbio internacional (FXO) 24-Port do catalizador 6000. Isto fornece o correio de voz para três dos seis terrenos, que sae de três terrenos sem o correio de voz. Não é possível compartilhar corretamente de um servidor repartee entre usuários em dois Cluster do CallManager daCisco porque não há nenhuma maneira de propagar o indicador de espera de mensagem (MWI) através do tronco de H.323 do intercluster.

O ACU pôde comprar três server do Cisco Unity para os terrenos que permanecem. Estes server

são com base em Skinny, assim que nenhum gateway é exigido. Esta tabela alista as soluções do correio de voz caso o ACU comprar os servidores de correio de voz adicionais:

Terreno	Sistema de correio de voz	Gateway
Montagem Saint Mary	Voz ativa com resposta	Catalizador 6000 24-port FXS
MacKillop	Voz ativa com resposta	Catalizador 6000 24-port FXS
Patrick	Voz ativa com resposta	Catalizador 6000 24-port FXS
Aquinas	Cisco Unity	
Signadou	Cisco Unity	
McAuley	Cisco Unity	

Os seis servidores de correio de voz operam-se como ilhas isoladas do correio de voz neste plano. Não há nenhuma rede de correio de voz.

Recursos de mídia

Os processadores do sinal digital do hardware (DSP) não são distribuídos atualmente no ACU. As Conferências usam o bridge de conferência com base no software no CallManager da Cisco. A conferência inter-grânulo não é apoiada atualmente.

Transcoding não é exigido atualmente. Os codificador-decodificador somente de G.711 e de G.729 são usados, e são apoiados por todos os dispositivos finais distribuídos.

Suporte a fax e modem

O fax e o tráfego de modem não são apoiados atualmente pela rede de telefonia do IP ACU. A universidade planeia utilizar por esse motivo o cartão do catalizador 6000 24-Port FXS.

Versões de software

Esta tabela alista as versões de software ACU usadas na altura desta publicação:

Plataforma	Função	Versão de software
CallManager	IP-PBX	3.0(10)
Catalyst 3500XL	Switch de distribuição	12.0(5.1)XP
Catalyst 6500	Switch central	5.5(5)
Catalyst 1900	Wiring Closet Switch	
Processador do Cisco 7200	WAN Router	12.1(4)
Cisco 3640 Router	Gateway de H.323	12.1(3a)XI6

Informações Relacionadas

- Suporte à Tecnologia de Voz
- Suporte de Produtos de Comunicação de Voz e de IP
- Troubleshooting da Telefonia IP Cisco
- Suporte Técnico e Documentação - Cisco Systems