Estudo de caso Implantação de telefonia IP - ACU

Contents

Introduction

A rede acadêmica e de pesquisa australiana (AARNet) é uma rede IP de alta velocidade em todo o país que interconecta 37 universidades australianas e a Commonwealth Scientific and Industrial Research Organization (CSIRO).

O AARNet foi criado inicialmente como uma rede de dados, mas transportou Voz sobre IP (VoIP) desde o início de 2000. A rede VoIP atualmente implantada é uma solução de desvio de tarifa que transporta chamadas VoIP entre as universidades e as PABXs (private automatic branch exchange) da CSIRO. Ele também fornece gateways de rede telefônica pública comutada (PSTN - Public Switched Telephone Network) que permitem que a PSTN salte no ponto mais econômico. Por exemplo, uma chamada de um telefone PABX em Melbourne para um telefone PSTN em Sydney é transportada como VoIP de Melbourne para o gateway de Sydney PSTN. Ele está conectado à PSTN.

A Universidade Católica Australiana (ACU) é uma das universidades que se conectam à AARNet. No final de 2000, a ACU começou uma implantação de telefonia IP que implantou aproximadamente 2.000 telefones IP em seis campi universitários.

Este estudo de caso abrange a implantação de Telefonia IP ACU. O projeto está concluído. No entanto, há questões de arquitetura significativas a serem abordadas no backbone AARNet se a rede precisar ser dimensionada quando outras universidades seguirem os passos da ACU. Este documento descreve esses problemas e propõe e discute várias soluções. A implantação da Telefonia IP ACU provavelmente será ajustada posteriormente para se alinhar com a arquitetura recomendada final.

Observação: a Deakin University foi a primeira universidade australiana a implantar telefonia IP. No entanto, a Deakin University não usa o AARNet para transportar tráfego de telefonia IP.

AARNet

As universidades australianas e o CSIRO construíram o AARNet em 1990 através do Comitê de Vice-Chanceler Australiano (AVCC). 99% do tráfego da Internet na Austrália foi para os membros fundadores durante os primeiros anos. Uma pequena quantidade de tráfego comercial era proveniente de organizações que mantinham estreita associação com o setor terciário e de pesquisa. O uso pela base de usuários não AARNet aumentou para 20% do tráfego total até o final de 1994.

A AVCC vendeu a base de clientes comerciais da AARNet à Telstra em julho de 1995. Esse evento gerou o que viria a ser Telstra BigPond. Isso estimulou um maior crescimento do uso comercial e privado da Internet na Austrália. A transferência de propriedade intelectual e expertise resultou no desenvolvimento da Internet na Austrália. Caso contrário, tal não teria acontecido tão rapidamente.

O AVCC desenvolveu o AARNet2 no início de 1997. Foi mais um refinamento da Internet na Austrália, que emprega links ATM de alta largura de banda e serviços de Internet sob um contrato com a Cable & Wireless Optus (CWO) Limited. A rápida implantação de serviços IP pela CWO para atender aos requisitos do AARNet2 deve-se, em parte, à transferência de conhecimento e experiência da AARNet.

ACU

ACU é uma universidade pública criada em 1991. A universidade tem aproximadamente 10.000 alunos e mil funcionários. Há seis campus na costa leste da Austrália. Esta tabela mostra os campus da ACU e seus locais:

Campus	Cidade	Estado
Monte Saint Mary	Strathfield	Nova Gales do Sul (NSW)
MacKillop	North Sydney	Nova Gales do Sul (NSW)
Patrick	Melbourne	Victoria (VIC)
Aquino	Ballarat	Victoria (VIC)
Sigadou	Canberra	Território da capital da Austrália (ACT)
McAuley	Brisbane	Queensland (QLD)

A ACU contou com uma solução Telstra Spectrum (Centrex) antes da implantação da solução de Telefonia IP que este estudo de caso descreve. A mudança para a telefonia IP foi motivada principalmente pelo desejo de reduzir custos.

CSIRO

O CSIRO tem aproximadamente 6.500 funcionários em vários locais na Austrália. O CSIRO realiza pesquisas em áreas como agricultura, minerais, energia, manufatura, comunicações, construção, saúde e meio ambiente.

O CSIRO foi a primeira organização a usar o AARNet para VoIP. A organização foi pioneira no trabalho inicial feito nessa área.

AARNet

O backbone AARNet é um componente significativo em qualquer implantação de telefonia IP em qualquer universidade. Proporciona a interconexão das universidades com dois serviços principais na área de voz:

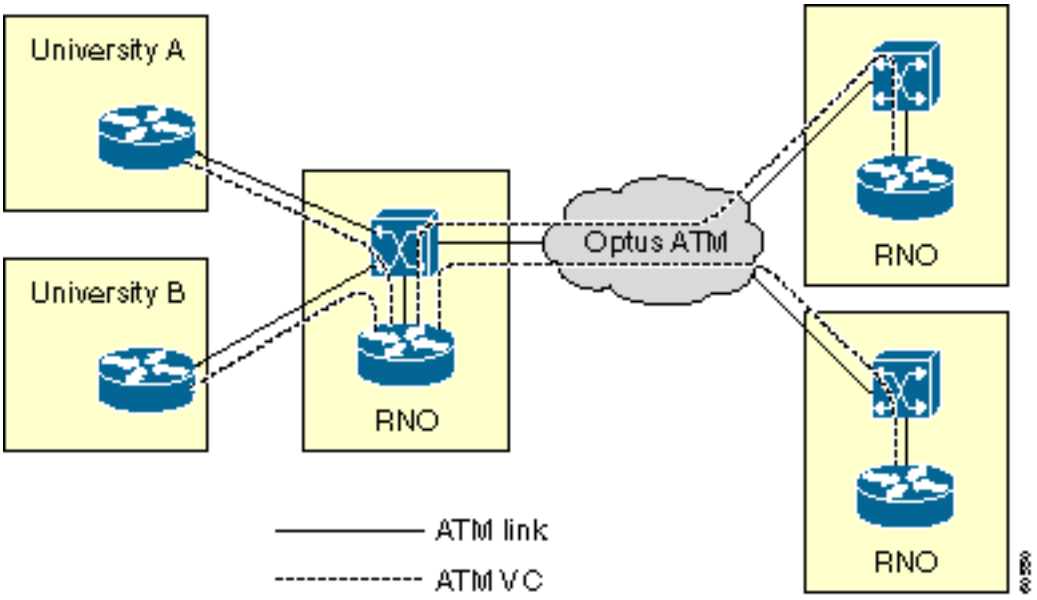
- Transporte de pacotes VoIP Realtime Transport Protocol (RTP) com garantia de Qualidade de Serviço (QoS) apropriada para voz
- Ponto de conexão de baixo custo para as PSTNs em todo o país

Esta seção descreve a arquitetura AARNet atual e como ela fornece esses serviços. Ele também descreve alguns dos problemas de escalabilidade que surgem à medida que mais universidades implantam a solução de Telefonia IP. Por fim, ele discute as possíveis soluções para esses problemas de escalabilidade.

Topologia AARNet

O AARNet consiste em um único POP (ponto de presença) em cada estado. Os POPs são chamados de RNOs (Regional Network Operations, operações regionais de rede). As universidades se conectam ao RNO em seu respectivo estado. Os RNOs, por sua vez, são interconectados por uma malha completa de PVCs Optus ATM. Juntos, eles constituem o AARNet.

O RNO típico consiste em um switch ATM Cisco LS1010 e um roteador conectado ATM. O roteador RNO se conecta a cada roteador universitário por um único PVC ATM através de um link de micro-ondas E3. Cada roteador RNO também tem uma malha completa de PVCs ATM que a rede Optus ATM fornece a todos os outros RNOs. Este diagrama representa a topologia geral do AARNet da rede:



Há inúmeras exceções à topologia. Alguns deles são significativos de uma perspectiva de voz. Estas são algumas exceções:

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

Esta tabela mostra os estados e territórios que têm atualmente um RNO. A tabela inclui capitais para leitores que não estão familiarizados com a geografia australiana.

Estado	Capital	RNO?	Conexões do campus
Nova Gales do Sul	Sydney	Yes	TBD
Victoria	Melbourne	Yes	TBD
Queensland	Brisbane	Yes	TBD
Austrália do Sul	Adelaide	Yes	TBD
Austrália Ocidental	Perth	Yes	TBD
Território da Capital Australiana	Canberra	Yes	TBD
Território do Norte	Darwin	No	—
Tasmânia	Hobart	No	—

Qualidade de Serviço

Partes do AARNet já estão habilitadas para QoS para voz como resultado do projeto de desvio de tarifa VoIP. A QoS é necessária para o tráfego de voz para fornecer esses recursos, que minimizam o atraso e a instabilidade e eliminam a perda de pacotes:

- Policiamento—Marcar o tráfego de voz de fontes não confiáveis.

- Enfileiramento—A voz deve receber prioridade sobre todo o tráfego restante para minimizar o atraso durante o congestionamento do link.
- Fragmentação e Intercalação de Enlace (LFI - Link Fragmentation and Interleave)—Os pacotes de dados devem ser fragmentados e os pacotes de voz intercalados em enlaces lentos.

O tráfego deve ser classificado para policiar corretamente e enfileirar pacotes de voz. Esta seção descreve como a classificação é feita no AARNet. Os capítulos subsequentes descrevem a implementação de vigilância e enfileiramento.

Classificação

Nem todo o tráfego obtém a mesma QoS. O tráfego é classificado nessas categorias para fornecer seletivamente QoS:

- Dados
- Voz de fontes conhecidas e confiáveis
- Voz de fontes desconhecidas

Somente dispositivos confiáveis recebem QoS de alta qualidade no AARNet. Esses dispositivos são principalmente gateways identificados pelo endereço IP. Uma lista de controle de acesso (ACL) é usada para identificar essas fontes confiáveis de voz.

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

A precedência de IP é usada para distinguir o tráfego de voz do tráfego de dados. A voz tem precedência de IP de 5.

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

Combine os exemplos anteriores para identificar pacotes de uma 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 uma 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 origem não confiável é classificado e marcado como inativo quando o tráfego chega em uma interface. Estes dois exemplos mostram como a vigilância é executada dependendo do tipo de tráfego que deve chegar em uma determinada interface:

O roteador procura pacotes de voz não confiáveis e altera sua precedência de IP para 0 se houver fontes de voz confiáveis downstream.

```
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 altera sua precedência de IP para 0 se não houver fontes de voz conhecidas downstream.

```
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 sem voz

Todo o VoIP no AARNet era de desvio de tarifa até recentemente. Essa condição resulta em relativamente poucos endpoints de VoIP. O projeto de enfileiramento atual distingue entre interfaces que têm dispositivos VoIP downstream e interfaces que não têm. Esta seção discute o enfileiramento em interfaces não VoIP.

Uma interface que não seja de voz é configurada para enfileiramento moderado ponderado (WFQ - Weighted Random Early Detection) ou WRED (Weighted Random Early Detection). Eles podem ser configurados diretamente na interface. No entanto, o mecanismo de enfileiramento é aplicado por meio de um mapa de política para facilitar a alteração do mecanismo de enfileiramento em um determinado tipo de interface. Há um mapa de política por tipo de interface. Isso reflete o fato de que nem todos os mecanismos de enfileiramento são suportados em todas as interfaces.

```
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 de política são anexados às respectivas interfaces e são específicos aos tipos de interface. Por exemplo, isso simplifica o processo de alteração do mecanismo de enfileiramento

em portas Ethernet baseadas em processador de interface versátil (baseadas em VIP) de WRED para WFQ. Requer uma única alteração no mapa de políticas. As alterações são feitas em todas as interfaces Ethernet baseadas 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

Qualquer interface que tenha dispositivos VoIP de downstream confiável é configurada para LLQ (Low Latency Queuing, enfileiramento de baixa latência). Qualquer pacote que o faça através da classificação de interface de entrada e mantenha uma precedência de 5 está sujeito ao LLQ. Qualquer outro pacote está sujeito a WFQ ou WRED. Isso depende do tipo de interface.

Mapas de política separados são criados para cada tipo de interface para tornar a QoS mais fácil de administrar. Isso é semelhante ao design de enfileiramento de não voz. No entanto, existem vários mapas de política para cada tipo de interface. Isso ocorre porque a capacidade dos tipos de interface para transportar tráfego de voz varia dependendo da velocidade do link, das configurações de PVC e assim por diante. O número no nome do mapa de políticas reflete o número de chamadas atendidas para 30 chamadas, 60 chamadas, etc.

```
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 de política são anexados às respectivas interfaces. Neste exemplo, o mapa de política é específico para um tipo de interface. Atualmente, não é dado nenhum tratamento especial à sinalização de voz. Os mapas de política podem ser facilmente alterados em um local se isso se tornar um requisito em um estágio posterior em um determinado tipo de interface. A alteração tem efeito para todas as interfaces 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
```

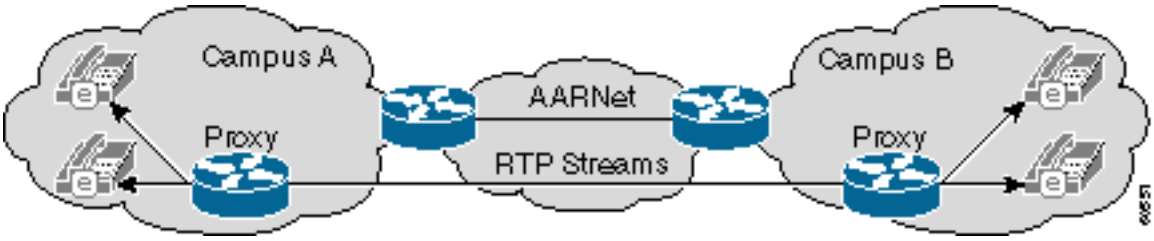
Escalabilidade LLQ

O mecanismo de enfileiramento tem alguns problemas de escalabilidade. A principal questão é que ele depende de saber o endereço IP de cada dispositivo VoIP confiável na rede. Essa era uma limitação razoável no passado quando havia um número limitado de gateways VoIP que lidavam com desvio de tarifa. O número de endpoints de VoIP aumenta drasticamente e torna-se cada vez mais impraticável com a implantação da telefonia IP. As ACLs tornam-se muito longas e difíceis de gerenciar.

As ACLs foram acrescentadas para confiar no tráfego de uma sub-rede IP de voz específica em cada campus da ACU no caso da ACU. Esta é uma solução provisória. Essas soluções a longo prazo estão sendo investigadas:

- proxy H.323
- policiamento de ingresso de QoS

A ideia principal por trás da solução proxy H.323 é fazer com que todo o tráfego de RTP entre no AARNet de um determinado campus por meio de um proxy. O AARNet vê todo o tráfego de RTP de um determinado campus com um único endereço IP, como mostrado neste diagrama:

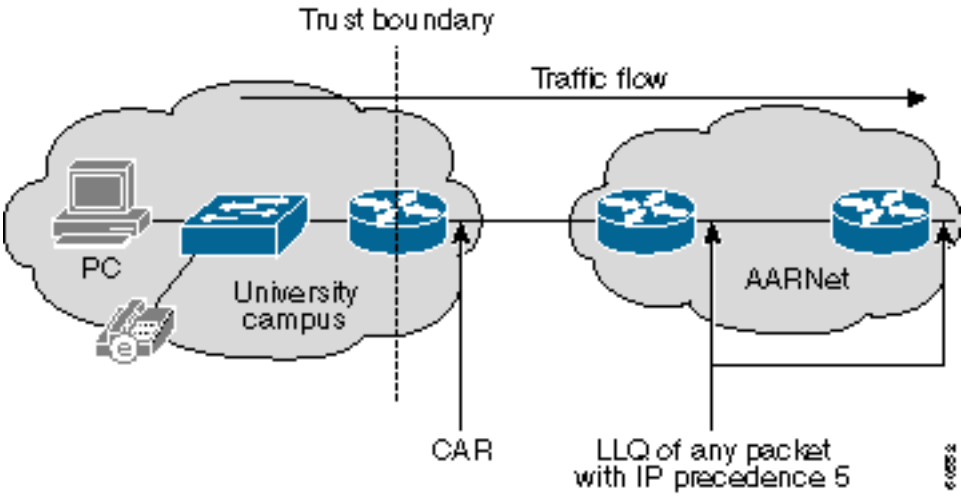


O número de entradas nas ACLs de QoS é limitado a uma linha por campus se esse esquema for implantado de forma consistente. Esse esquema ainda tem potencial para somar 100 ou mais matrículas, já que há 37 universidades com vários campi. Isso também não é escalável. Pode ser necessário migrar para um projeto com um único ou limitado número de super-proxies compartilhados em cada RNO. Isso reduz o número de endereços IP confiáveis para seis. No entanto, isso abre um problema de política de QoS no caminho do campus para o proxy no RNO.

Observação: os troncos entre clusters do Cisco CallManager não funcionam atualmente através de um proxy H.323 porque a sinalização entre clusters não é H.225 nativo.

O policiamento de ingresso de QoS é uma solução alternativa. Um limite de confiança é estabelecido no ponto em que o campus se conecta ao RNO com esse projeto. O tráfego que entra no AARNet é policiado pelo recurso Cisco IOS® Committed Access Rate (CAR) nesse limite. Uma universidade que usa AARNet para VoIP assina uma certa quantidade de largura de banda de QoS do AARNet. Em seguida, o CAR monitora o tráfego que entra no AARNet. O excesso de tráfego tem precedência de IP marcada para 0 se a quantidade de tráfego de RTP com precedência de IP 5 exceder a largura de banda subscrita.

Este diagrama mostra uma configuração de CAR:



Este exemplo mostra como uma configuração de CAR lida com essa vigilância:

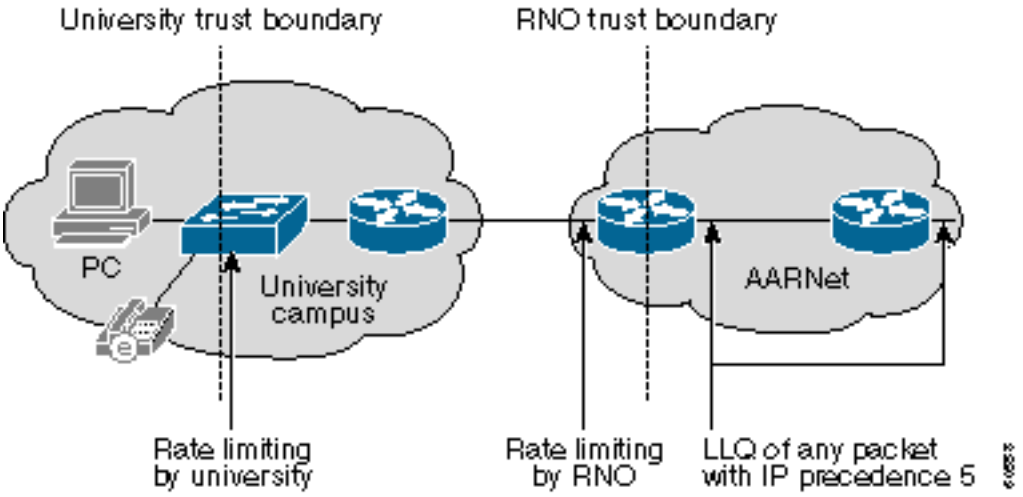
```
Interface a1/0.100
rate-limit input access-group 100 2400000 0 0 conform-action set-prec-transmit 5
exceed-action set-prec-transmit 0

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

Estas são algumas vantagens de uma abordagem de configuração de CAR:

- O núcleo não precisa mais lidar com policiamento. Agora é tratado no limite de confiança. Portanto, o LLQ no núcleo não precisa saber sobre endereços IP confiáveis. Qualquer pacote com precedência de IP de 5 no núcleo pode estar sujeito ao LLQ com segurança porque já passou pela vigilância na entrada.
- Não são feitas suposições sobre a arquitetura, os equipamentos e os protocolos de VoIP escolhidos pelas universidades. Uma universidade pode optar por implantar um Session Initiation Protocol (SIP) ou Media Gateway Control Protocol (MGCP) que não funcione com proxies H.323. Os pacotes VoIP recebem a QoS apropriada no núcleo, desde que tenham uma precedência de IP de 5.
- O CAR é resiliente contra ataques de negação de serviço (DoS) de QoS. Um ataque de QoS do que se origina de uma universidade não pode danificar o núcleo. O CAR limita o ataque, que não pode gerar mais tráfego do que o que está presente quando o número máximo de chamadas VoIP permitidas está ativo.As chamadas VoIP para ou desse campus podem sofrer durante um ataque. Mas cabe a cada universidade se proteger internamente. A universidade pode apertar as ACLs de CAR no roteador de modo que todas as sub-redes VoIP selecionadas, exceto as selecionadas, tenham a precedência de IP marcada como inativa.Cada campus tem um limite de confiança interna no ponto em que os usuários se conectam à LAN do campus no projeto final. O tráfego com uma precedência de IP de 5 que esse limite de confiança recebe é limitado a 160 kbps por porta de switch, ou duas chamadas VoIP G.711. O tráfego que excede essa taxa é marcado como inativo. A implementação deste esquema requer switches Catalyst 6500 ou algo semelhante com funcionalidade de limitação de taxa.
- O provisionamento de largura de banda no núcleo simplifica conforme cada universidade assina uma quantidade fixa de largura de banda de QoS. Isso também simplifica a cobrança de QoS, pois cada universidade pode pagar uma taxa mensal fixa com base em uma assinatura de largura de banda de QoS.

A principal fraqueza deste projeto é que o limite de confiança está localizado no roteador da universidade, de modo que as universidades devem ser capazes de administrar corretamente o CAR. O limite de confiança é puxado de volta para o RNO. O equipamento administrado por RNO lida com a vigilância no projeto final. Este design requer limitação de taxa baseada em hardware, como o switch Catalyst 6000 ou um processador Cisco 7200 Network Services Engine (Cisco 7200 NSE-1). No entanto, ele dá ao AARNet e aos RNOs controle total sobre a vigilância de QoS. Este diagrama mostra este projeto:



Fragmentação e intercalação de links

O VoIP está sendo transportado apenas através de VCs (Virtual Circuits, circuitos virtuais) ATM de velocidade relativamente alta. Portanto, nenhuma LFI é necessária. O VoIP também pode ser transportado através do Frame Relay Forum (FRF) ou linhas alugadas para universidades rurais no futuro. Isso exige mecanismos de LFI, como Multilink PPP (MLP) com Interleave ou FRF.12.

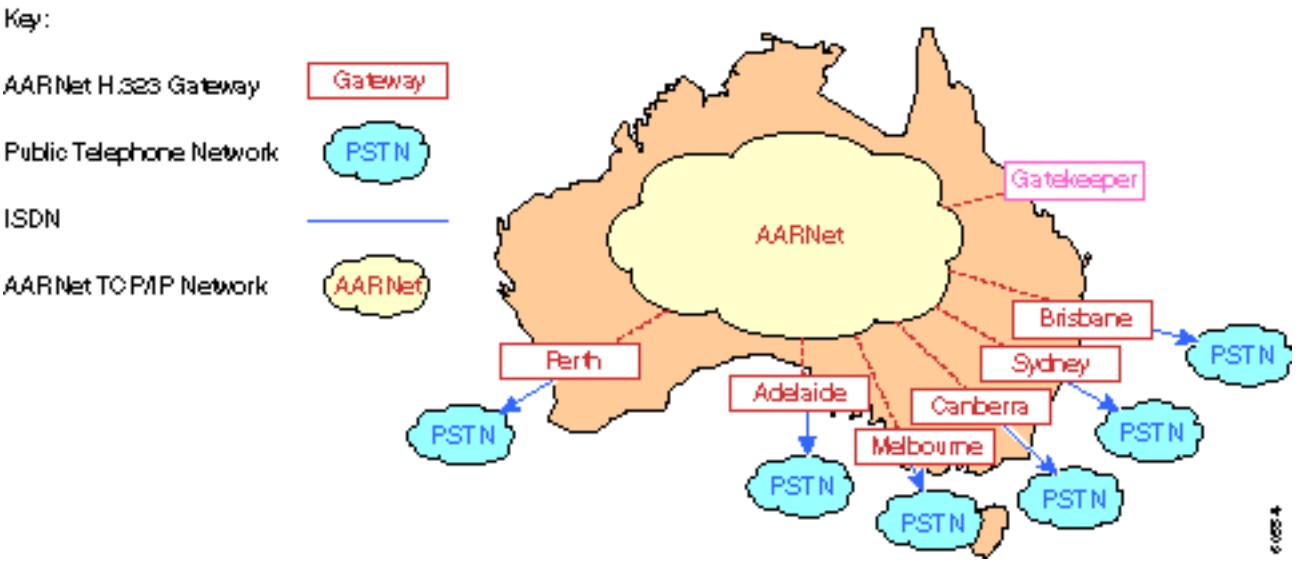
Gateways

Há dois tipos de gateways H.323 no AARNet:

- PSTN—PSTN para gateway VoIP
- PABX—PABX para gateway VoIP

A distinção entre um gateway PSTN e PABX é principalmente funcional. Os gateways PSTN fornecem conectividade com a PSTN. Os gateways PABX conectam um PABX universitário ao backbone VoIP. A mesma caixa física atua como um PSTN e um gateway PABX em muitos casos. Atualmente, há 31 gateways na solução de Telefonia IP ACU. A maioria desses gateways são servidores de acesso universal Cisco AS5300. Os outros gateways são roteadores da série Cisco 3600 ou roteadores da série Cisco 2600. Espera-se que sejam adicionados no mínimo dez gateways adicionais durante o segundo trimestre de 2001. A AARNet transportou aproximadamente 145.000 chamadas VoIP em abril de 2001.

A AARNet implementou gateways H.323 ligados à PSTN na maioria das cidades principais, como mostra este diagrama:



As universidades podem usar esses gateways para fazer chamadas de saída para a PSTN. As universidades precisam manter seus próprios troncos para chamadas de entrada porque não têm suporte no momento. O AARNet pode negociar um preço muito competitivo com a operadora devido ao volume de chamadas que passam por esses gateways. As chamadas também podem ser abandonadas no ponto mais econômico. Por exemplo, alguém em Sydney que liga para um número Perth pode usar o gateway Perth e ser cobrado somente por uma chamada local. Isso também é conhecido como Tail End Hop Off (TEHO).

Um único gatekeeper é implantado para executar a resolução de E.164 para endereço IP. Todas as chamadas para a PSTN são enviadas ao gatekeeper, que retorna o endereço IP do gateway mais apropriado. Consulte as seções Planos de Discagem e Gatekeeper para obter informações mais detalhadas sobre gatekeepers.

Cobrança e tarifação

Os gateways PSTN usam RADIUS e autenticação, autorização e contabilização (AAA) para fins de faturamento. Cada chamada através de um gateway gera um registro de detalhes de chamadas (CDR) para cada perna da chamada. Esses CDRs são publicados no servidor RADIUS. O endereço IP do Cisco CallManager no CDR identifica exclusivamente a universidade e garante que a parte correta seja cobrada.

Segurança do gateway

Proteger os gateways PSTN contra ataques de DoS e fraudes é uma grande preocupação. Os clientes H.323 estão amplamente disponíveis. O Microsoft NetMeeting é fornecido com o Microsoft Windows 2000, portanto, é relativamente fácil para um usuário não técnico fazer chamadas gratuitas através desses gateways. Configure uma ACL de entrada que permita a sinalização H.225 de endereços IP confiáveis para proteger esses gateways. Essa abordagem tem todos os mesmos problemas de escalabilidade que a seção QoS descreve. O número de entradas na ACL cresce à medida que o número de endpoints H.323 confiáveis cresce.

Os proxies H.323 oferecem algum alívio nesta área. As ACLs de gateway precisam permitir um endereço IP por campus universitário se todas as chamadas através do gateway PSTN passarem por um proxy de campus. Dois endereços IP como proxy redundante são desejáveis na maioria dos casos. Mesmo com proxies, a ACL pode conter mais de 100 entradas.

O proxy deve ser protegido por ACLs, pois qualquer H.323 pode configurar uma chamada através do proxy. A ACL de proxy deve permitir dispositivos H.323 locais conforme exigido pela política local, pois isso é feito por campus.

Os endereços IP dos dois Cisco CallManagers devem ser incluídos nas ACLs de gateway se um campus quiser permitir que somente as chamadas de telefones IP usem os gateways AARNet PSTN. Os proxies não adicionam nenhum valor nesta situação. O número de entradas ACL necessárias é de duas maneiras.

Observe que as chamadas IP de telefone para IP entre campus não precisam passar pelo proxy.

Planos de discagem

O plano de discagem VoIP atual é direto. Os usuários podem fazer estes dois tipos de chamadas de uma perspectiva de gateway VoIP:

- Ligue para um telefone em um campus diferente, mas na mesma universidade.
- Chame um telefone PSTN ou um telefone em uma universidade diferente.

Os peers de discagem do gateway refletem o fato de que há apenas dois tipos de chamadas. Basicamente, há dois tipos de peer de discagem VoIP, como mostrado neste exemplo:

```
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 peer de discagem é usado se alguém ligar para o ramal 7... em outro campus neste exemplo. Essa chamada é roteada diretamente para o endereço IP do gateway remoto. Como o gatekeeper é ignorado, o Call Admission Control (CAC) não é executado.

O segundo peer de discagem é usado quando a chamada é para um número PSTN. Esse pode ser um destes itens:

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

A chamada é enviada ao gatekeeper por meio de uma mensagem de solicitação de admissão (ARQ) no primeiro caso. O gatekeeper retorna o endereço IP do melhor gateway PSTN em uma mensagem de confirmação de admissão (ACF).

A chamada também é enviada ao gatekeeper por meio de uma mensagem ARQ no segundo caso. No entanto, o gatekeeper retorna uma mensagem ACF com o endereço IP do gateway VoIP na universidade que recebe a chamada.

Gatekeeper

O AARNet opera atualmente um único gatekeeper. O único objetivo desse gatekeeper é executar o roteamento de chamadas na forma de E.164 para a resolução de endereços IP. O gatekeeper não executa CAC. O número de troncos PABX conectados aos gateways limita o número de chamadas simultâneas. A largura de banda do núcleo atende a todos os troncos em uso de uma só vez. Isso muda com a implantação da telefonia IP na ACU e em outras universidades. Não há limite natural para o número de chamadas VoIP simultâneas que podem ser originadas dentro ou fora de um determinado campus nesse novo ambiente. A largura de banda de QoS disponível pode ter excesso de assinaturas se muitas chamadas forem iniciadas. Todas as chamadas podem sofrer de má qualidade sob esta condição. Use o gatekeeper para fornecer CAC.

A natureza distribuída e o tamanho potencial da rede de voz da universidade se prestam a uma arquitetura de gatekeeper distribuída. Uma solução possível é ter um projeto de gatekeeper hierárquico de dois níveis no qual cada universidade mantém seu próprio gatekeeper. Esse gatekeeper da universidade é conhecido como gatekeeper de camada 2. O AARNet opera um gatekeeper de *diretório* que é conhecido como gatekeeper de camada 1.

As universidades devem usar essa abordagem de duas camadas para usar um gatekeeper para roteamento de chamadas entre clusters do Cisco CallManager. O gatekeeper roteia chamadas com base em um ramal de 4 ou 5 dígitos neste cenário. Cada universidade exige seu próprio porteiro. Isso ocorre porque os intervalos de ramais se sobrepõem entre universidades, pois esse é um espaço de endereço administrado localmente.

Os gatekeepers nível 2 da universidade executam CAC somente para chamadas de e para aquela universidade. Ele também realiza a resolução E.164 para chamadas entre apenas os campi daquela universidade. A chamada é roteada pelo gatekeeper de camada 2 para o gatekeeper de camada 1 por meio de uma mensagem de solicitação de local (LRQ) se alguém ligar para um telefone IP em outra universidade ou chamar a PSTN por meio de um gateway AARNet. O LRQ é encaminhado ao gatekeeper de camada 2 dessa universidade se a chamada for para outra universidade. Em seguida, esse gatekeeper retorna uma mensagem ACF para o gatekeeper de camada 2 na universidade de origem da chamada. Os gatekeepers de camada 2 executam CAC. Eles só prosseguirão com a chamada se houver largura de banda suficiente disponível nas zonas de chamada e chamada.

O AARNet pode optar por tratar os gateways PSTN AARNet como os de qualquer universidade. O próprio porteiro de nível 2 cuida deles. O gatekeeper de camada 1 também pode atuar como o gatekeeper de camada 2 para esses gateways se a carga e o desempenho permitirem.

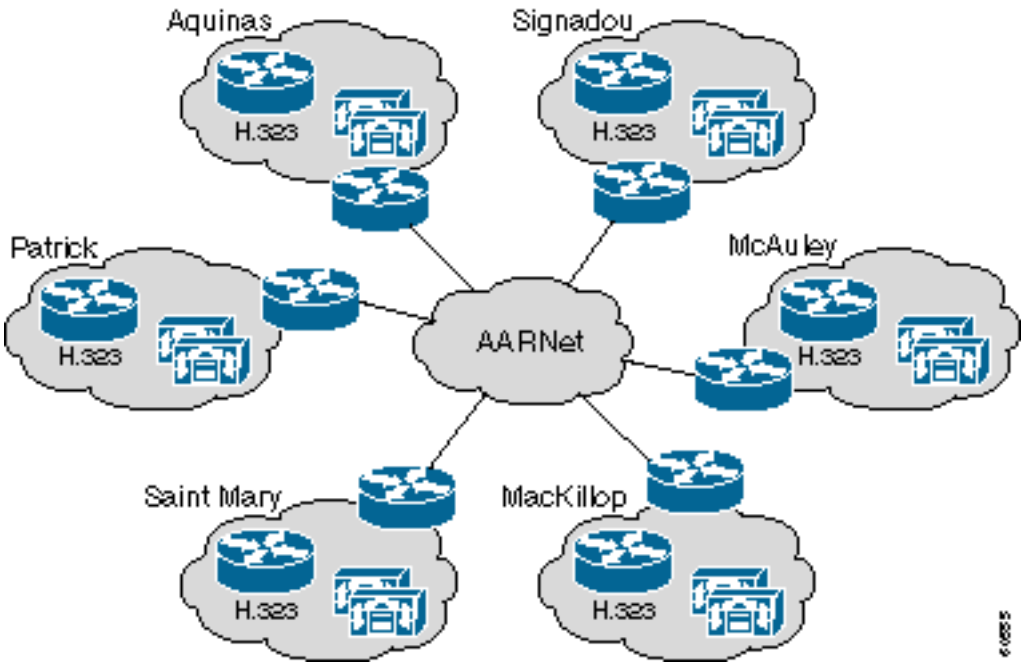
Cada um dos gatekeepers (incluindo o gatekeeper de diretório AARNet) precisa ser replicado porque os gateways são um componente tão crítico. Cada universidade precisa ter dois porteiros. É possível que os gateways Cisco IOS tenham gatekeepers alternativos, como no caso do Cisco IOS Software Release 12.0(7)T. No entanto, isso não é suportado atualmente pelo Cisco CallManager ou por qualquer outro dispositivo H.323 de terceiros. Não use este recurso no momento. Use uma solução simples baseada em Hot Standby Router Protocol (HSRP). Isso exige que os dois gatekeepers se posicionem na mesma sub-rede IP. O HSRP determina qual gatekeeper está ativo.

Rede de telefonia IP ACU

Esta tabela mostra o número aproximado de telefones IP instalados nos campus da ACU:

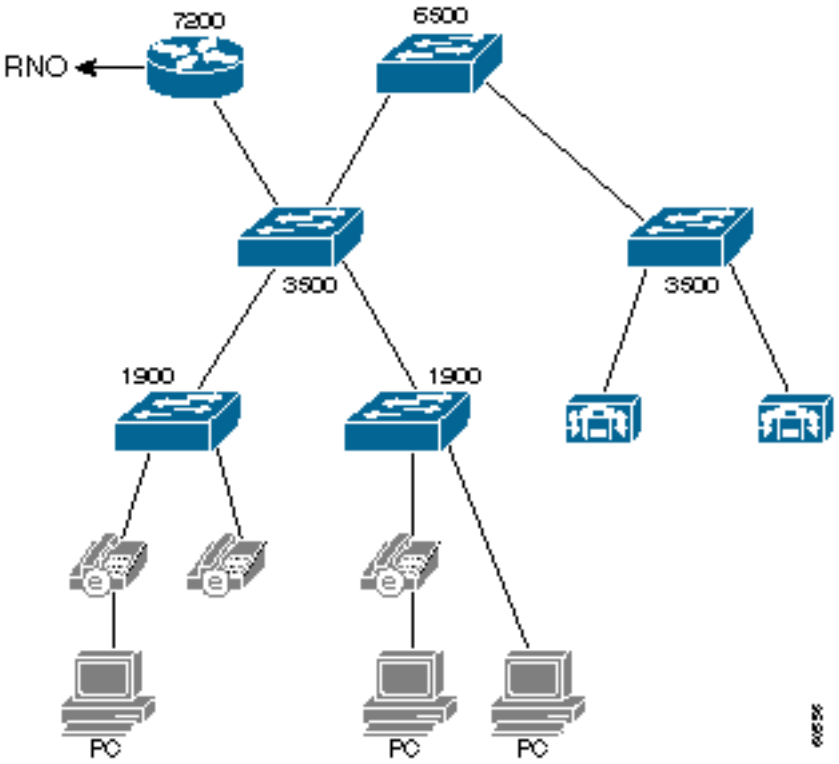
Campus	Cidade	Telefones IP aproximados
Monte Saint Mary	Strathfield	400
MacKillop	North Sydney	300
Patrick	Melbourne	400
Aquino	Ballarat	100
Sigadou	Canberra	100
McAuley	Brisbane	400
	Total:	*1700*

A ACU implantou recentemente uma solução de telefonia IP. A solução consiste em um cluster de dois Cisco CallManagers, um gateway Cisco 3640 em cada campus e telefones IP. O AARNet interconecta os campus. Este diagrama descreve a topologia de alto nível e os vários componentes da rede de Telefonia IP ACU:



Topologia de rede de ACU

Este diagrama mostra um campus ACU típico. Cada campus tem três camadas de switches Catalyst. O wiring closet abriga os switches Catalyst 1900 mais antigos. Os switches Catalyst 1900 conectam-se de volta ao switch Catalyst 3500XL por meio de Framing Estendido. Elas se conectam de volta a um único switch Catalyst 6509 por meio de Gigabit Ethernet (GE). Um único roteador Cisco 7200 VXR conecta o campus ao AARNet por um ATM VC ao RNO local.



O método de conectividade com o RNO difere um pouco de estado para estado, como mostra esta tabela. Victoria baseia-se em Classical IP over ATM (RFC 1577). Os outros RNOs têm uma configuração de PVC direto com encapsulamento RFC 1483. O OSPF (Open Shortest Path First) é o protocolo de roteamento usado entre ACU e RNOs.

Campus	Estado	Conectividade ao RNO	Routing Protocol
Monte Saint Mary	NSW	RFC 1483 PVC	OSPF
MacKillop	NSW	RFC 1483 PVC	OSPF
Patrick	VIC	RFC 1577 IP clássico sobre ATM	OSPF
Aquino	VIC	RFC 1577 IP clássico sobre ATM	OSPF
Sigadou	ACT	RFC 1483 PVC	OSPF
McAuley	QLD	RFC 1483 PVC	OSPF

Os switches da série Catalyst 1900 suportam entroncamento somente nos uplinks. Portanto, os telefones IP e os PCs estão todos em uma VLAN grande. Na verdade, o campus inteiro é uma VLAN grande e um domínio de broadcast. As sub-redes IP secundárias são usadas devido ao grande número de dispositivos. Os telefones IP estão em uma sub-rede IP e os PCs estão em outra. O núcleo do AARNet confia na sub-rede do telefone IP e o tráfego de e para esta sub-rede

IP está sujeito ao LLQ.

O roteador Cisco 7200 roteia entre as sub-redes IP primária e secundária. A MSFC (Multilayer Switch Feature Card) no switch Catalyst 6500 não é usada atualmente.

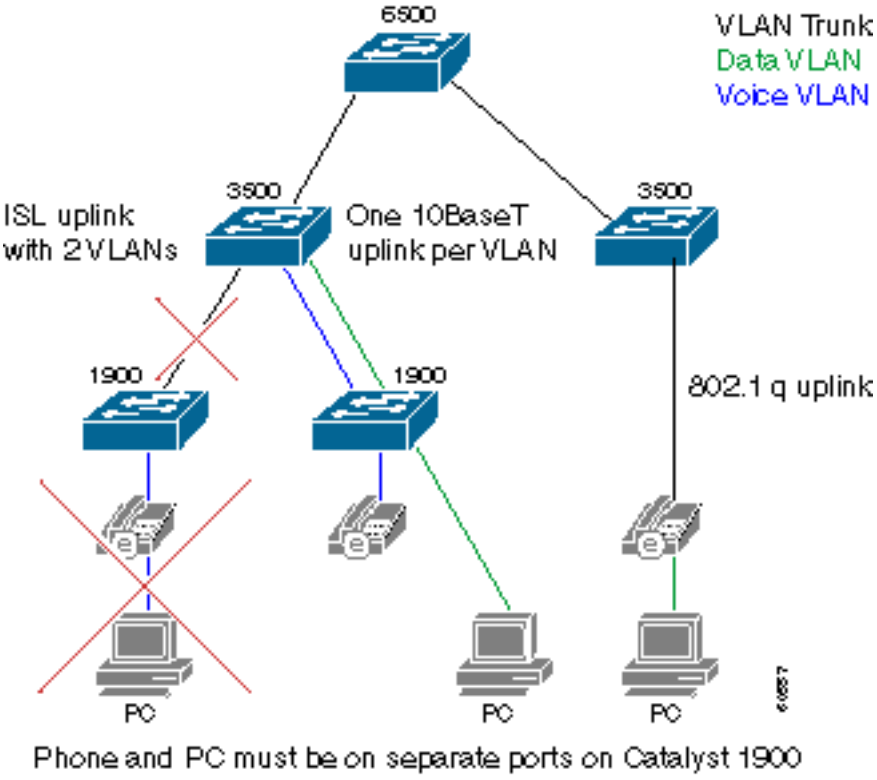
Os switches Catalyst 3500XL e Catalyst 6500 têm recursos de QoS, mas não estão habilitados no momento.

QoS no campus

O projeto atual do campus não está em conformidade com as diretrizes de design recomendadas pela Cisco para telefonia IP. Estas são algumas preocupações sobre QoS:

- O domínio de broadcast é muito grande. O excesso de broadcasts pode afetar o desempenho dos telefones IP, que precisam processá-los.
- Os switches Catalyst 1900 não são compatíveis com QoS. Se um telefone IP e um PC estiverem conectados à mesma porta do switch, os pacotes de voz podem ser descartados se o PC receber dados em uma taxa alta.

Reprojete partes da infraestrutura do campus para obter melhorias significativas. Não é necessária uma atualização de hardware. Este diagrama ilustra os princípios por trás do reprojeto recomendado:



O campus deve ser dividido em uma VLAN de voz e uma VLAN de dados. Os telefones e PCs que se conectam a um switch Catalyst 1900 devem agora se conectar a diferentes portas para conseguir a separação de VLANs. Um uplink adicional de cada switch Catalyst 1900 para o switch Cisco 3500XL é adicionado. Um dos dois uplinks é membro da VLAN de voz. O outro uplink é um membro da VLAN de dados. Não use o entroncamento InterSwitch Link (ISL) como alternativa a dois uplinks. Isso não fornece ao tráfego de voz e dados filas separadas. Os links GE do switch Catalyst 3500XL para o switch Catalyst 6000 também devem ser convertidos em troncos 802.1q para que a VLAN de voz e dados possa ser transportada através desse switch central.

As portas no switch Catalyst 3500XL que estão na VLAN de dados têm uma Classe de Serviço (CoS - Class of Service) padrão zero. As portas que são membros da VLAN de voz têm um CoS padrão de 5. Como resultado, o tráfego de voz é corretamente priorizado quando chega ao núcleo do Catalyst 3500 ou do Catalyst 6500. As configurações de porta do switch QoS Catalyst 3500 variam um pouco dependendo de qual porta do switch VLAN é membro, como mostra este exemplo:

```
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 do switch traseiro no telefone IP caso raramente os telefones IP se conectem diretamente a um switch Catalyst 3500XL. Os telefones IP se conectam ao switch por meio de um tronco 802.1q nesse caso. Isso permite que pacotes de voz e dados trafeguem em VLANs separadas e você pode dar aos pacotes o CoS correto na entrada. Substitua os switches Catalyst 1900 por switches Catalyst 3500XL ou outros switches compatíveis com QoS quando chegarem ao fim da vida útil. Essa topologia se torna o método padrão de conectar telefones IP e PCs à rede. Este cenário mostra a configuração de QoS do switch Catalyst 3500XL:

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

Finalmente, as duas portas que se conectam aos dois Cisco CallManagers devem ter o CoS codificado para 3. O Cisco CallManager define a precedência de IP como 3 em todos os pacotes de sinalização de voz. No entanto, o link do Cisco CallManager para o switch Catalyst 3500XL não usa 801.1p. Portanto, o valor de CoS é forçado no switch como mostrado neste exemplo:

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

O principal obstáculo desse projeto é que duas portas de switch são necessárias na área de trabalho. O campus Patrick pode exigir 400 portas de switch adicionais para 400 telefones IP. Switches Catalyst 3500XL adicionais devem ser implantados se portas suficientes não estiverem disponíveis. Somente uma porta do switch Catalyst 3500XL é necessária para cada duas portas de switch Catalyst 1900 ausentes.

Os switches Catalyst 6500 da ACU atuais têm recursos de QoS, mas não estão habilitados no momento. Esses módulos estão presentes no switch ACU Catalyst 6000 com estes recursos 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	—	—

Conclua estes passos para ativar os recursos de QoS apropriados no switch Catalyst 6000:

1. Diga ao switch para fornecer QoS por VLAN com este comando:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 vlan-based
   ```

2. Diga ao switch para confiar nos valores de CoS recebidos do switch Catalyst 3500XL 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 definido para mapeamento de ponto de código de serviços diferenciados (DSCP). Isso é necessário porque o switch Catalyst 6000 regrava o valor de DSCP no cabeçalho IP com base no valor de CoS recebido. Os pacotes de sinalização VoIP devem ter um CoS de 3, regravado com um DSCP AF31 (26). Os pacotes RTP devem ter um CoS de 5, regravado 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 para 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
```

Configure o MSFC para rotear entre as várias sub-redes IP.

QoS no RNO

O projeto atual de RNO não está em conformidade com as diretrizes de design recomendadas pela Cisco para telefonia IP. Essas preocupações existem em relação à QoS:

- O LLQ não é aplicado no roteador WAN da série Cisco ACU 7200.
- Os campi Patrick e Aquinas conectam-se ao RNO por meio de ATM switched VCs (SVCs). LLQ não é suportado em SVCs.

Um roteador Cisco 7200 conectado à Fast Ethernet conecta o campus a um RNO por meio de um link ATM E4 de 34 Mbps. O tráfego pode enfileirar a saída nos enlaces 34M devido à incompatibilidade de velocidade de 4M versus 100M. Portanto, é necessário priorizar o tráfego de voz. Use LLQ. A configuração do roteador Cisco 7200 é semelhante 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 alocada para LLQ deve ser *N x 24 Kbps*, onde N é o número de chamadas G.729 simultâneas.

Configure um PVC de cada um dos roteadores Patrick e Aquinas Cisco 7200 para o roteador AARNet. Os ATM SVCs no Victoria RNO não suportam LLQ, pois são baseados em Classical IP over ATM (RFC 1577). As outras universidades no Victoria RNO podem continuar a usar o RFC 1577 por enquanto. No entanto, substitua eventualmente a infraestrutura Classical IP over ATM.

Gateways

Cada um dos campus da ACU tem um roteador Cisco 3640 que atua como um gateway H.323. Esses gateways se conectam à PSTN por meio da ISDN. O número de Interfaces de Taxa Primária (PRIs - Primary Rate Interfaces) e canais B depende do tamanho do campus. Esta tabela lista o número de PRIs e canais B para cada campus:

Campus	Quantidade PRI	Quantidade de canais B
Monte Saint Mary	2	30
MacKillop	2	50
Patrick	2	50
Aquino	1	20
Sigadou	1	20
McAuley	1	30

Esses gateways são usados somente como gateways secundários para DOD (Direct Outward Dialing). Os gateways AARNet são os gateways principais. Os gateways ACU são sempre usados para DID (Direct Inward Dialing).

Plano de discagem

O plano de discagem baseia-se em números de ramal de 4 dígitos. O ramal também são os últimos quatro dígitos do número DID. Esta tabela lista os intervalos de ramais e os números DID para cada campus:

Campus	Extensão	DID

Monte Saint Mary	9xxx	02 9764 9xxx
MacKillop	8xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Aquino	5xxx	03 5330 5xxx
Sigadou	2xxx	02 6123 2xxx
McAuley	7xxx	07 3354 7xxx

Uma entrada `num-exp` simples nos gateways trunca o número DID para o ramal de 4 dígitos antes de passá-lo para o Cisco CallManager. Por exemplo, o gateway do campus Patrick tem esta entrada:

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

Os usuários discam zero para selecionar uma linha externa. Esse zero à esquerda é passado para o gateway. Um único peer de discagem POTS roteia a chamada para fora da porta ISDN com base no zero à esquerda.

```
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 em um ramal de 4 dígitos. Em seguida, a chamada corresponde a ambos os peers de discagem VoIP. Com base na preferência mais baixa, ele prefere esta rota ao assinante do 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

Cada um dos campus tem um cluster que consiste em dois servidores Cisco CallManager. Os servidores Cisco CallManager são uma combinação de Media Convergence Server 7835 (MCS-7835) e Media Convergence Server 7820 (MCS-7820). Ambos os servidores executavam a versão 3.0(10) no momento desta publicação. Um Cisco CallManager é o *editor* e o outro Cisco CallManager é o *assinante*. O assinante atua como o Cisco CallManager principal para todos os telefones IP. Esta tabela lista o hardware implantado em cada campus:

Campus	Platform	CallManagers

Monte Saint Mary	MCS-7835	2
MacKillop	MCS-7835	2
Patrick	MCS-7835	2
Aquino	MCS-7820	2
Sigadou	MCS-7820	2
McAuley	MCS-7835	2

Cada cluster é configurado com duas regiões:

- Uma para chamadas intracampus (G.711)
- Uma para chamadas entre campus (G.729)

CAC baseado em local não é apropriado para ACU porque todos os telefones IP atendidos por cada cluster estão em um único campus. Há vantagens em um CAC baseado em gatekeeper para chamadas entre campus, mas isso não está implementado no momento. No entanto, há planos para o fazer num futuro próximo.

Cada Cisco CallManager é configurado com 22 gateways H.323. Ele é composto de troncos intercluster para os cinco outros clusters do Cisco CallManager, seis gateways AARNet PSTN e um gateway ACU em cada campus.

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

As listas de rotas e os grupos de rotas são usados para classificar os gateways PSTN. Por exemplo, esta tabela mostra como as chamadas do Patrick Cisco CallManager em Melbourne para o Sydney PSTN podem usar os quatro gateways para ligar as chamadas a um grupo de roteamento.

Gateway	Prioridade
AARNet Sydney	1
ACU Sydney	2
AARNet Melbourne	3
ACU Melbourne	4

Os Cisco CallManagers são configurados com aproximadamente 30 padrões de rota, como mostrado nesta tabela. Os padrões de rota são projetados para que haja correspondências específicas para todos os números nacionais da Austrália. Dessa forma, os usuários não precisam esperar o tempo limite entre dígitos expirar antes que o Cisco CallManager inicie a chamada. O caractere curinga "!" é usado somente no padrão de rota para números internacionais. Os usuários devem aguardar até que o tempo limite entre dígitos (padrão de 10 segundos) expire antes que a chamada progrida quando discarem para um destino internacional. Os usuários também podem adicionar o padrão de rota "0.0011!#". Os usuários podem inserir um "#" após o último dígito para indicar ao Cisco CallManager que o número discado está completo. Essa ação acelera a discagem internacional.

Padrão de rota	Descrição
0.[2-9]XXXXXXX	Chamada local
0.00	Chamada de emergência - se o usuário se esquecer de discar 0 para a linha externa
0.000	Chamada de emergência
0.013	Assistência de diretório
0.1223	—
0.0011!	Chamadas internacionais
0,02XXXXXXX	Chamadas para Nova Gales do Sul
0,03XXXXXXX	Chamadas para Victoria
0,04XXXXXXX	Chamadas para telefones celulares
0,07XXXXXXX	Chamadas para Queensland
0,086XXXXXX	Chamadas para a Austrália Ocidental
0,08XXXXXXX	Chamadas para o Sul da Austrália e o Norte do Território
0,1[8-9]XXXXXXX	Chamadas para 1800 xxx xxx e 1900 xxx xxx
0,1144X	Emergência
0,119[4-6]	Tempo e clima
0,1245X	Diretório
0,13[1-9]XXX	Chamadas para números 13xxxx
0,130XXXXXX	Chamadas para 1300 xxx xxx números
2[0-1]XX	Chamadas entre clusters para o Signadou
3[0-4]XX	Chamadas entre clusters para Patrick
5[3-4]XX	Chamadas intercluster para Aquinas
7[2-5]XX	Chamadas entre clusters para McAuley
8[0-3]XX	Chamadas entre clusters para MacKillop
9[3-4]XX	Chamadas entre clusters para o Monte Santa Maria
9[6-7]XX	Chamadas entre clusters para o Monte Santa Maria

O número de gateways, grupos de rotas, listas de rotas e padrões de rota configurados no Cisco CallManagers da ACU tem o potencial de crescer para um grande número. Se um novo gateway RNO for implantado, todos os cinco clusters do Cisco CallManager devem ser reconfigurados com um gateway adicional. Pior ainda, centenas de gateways precisam ser adicionados se os Cisco CallManagers da ACU rotearem chamadas VoIP diretamente para todas as outras universidades e ignorarem totalmente a PSTN. Claramente, isso não se expande muito bem.

A solução é tornar o gatekeeper Cisco CallManagers controlado. Você só deve atualizar o gatekeeper quando um novo gateway ou Cisco CallManager for adicionado em algum lugar no

AARNet. Cada Cisco CallManager deve ter apenas o gateway do campus local e o dispositivo anônimo configurados quando isso acontece. Você pode pensar neste dispositivo como um tronco ponto a multiponto. Ele remove a necessidade dos troncos PPP em malha no modelo de plano de discagem do Cisco CallManager. Um único grupo de rotas aponta para o dispositivo anônimo como o gateway preferencial e para o gateway local como o gateway de backup. O gateway PSTN local é usado para determinadas chamadas locais e também para chamadas fora da rede gerais se o gatekeeper ficar indisponível. Atualmente, o dispositivo anônimo pode ser intercluster ou H.225, mas não ambos ao mesmo tempo.

O Cisco CallManager precisa de menos padrões de rota com um gatekeeper do que tem agora. Em princípio, o Cisco CallManager precisa apenas de um padrão de rota única de "!" apontando para o porteiro. Na realidade, a maneira como as chamadas são roteadas precisa ser mais específica por estes motivos:

- Algumas chamadas (como chamadas para 1-800 ou números de emergência) precisam ser roteadas por meio de um gateway local geográfico. Alguém em Melbourne que disca para a polícia ou uma cadeia de restaurantes como a Pizza Hut não quer estar ligado à polícia ou à Pizza Hut em Perth. Os padrões de rota específicos são necessários que apontam diretamente para o gateway PSTN do campus local para esses números.As universidades que planejam executar futuras implantações de Telefonia IP podem optar por depender apenas dos gateways AARNet e não administrar seus próprios gateways locais. Esses números devem ter um código de área virtual anexado pelo Cisco CallManager antes de enviá-lo ao gatekeeper para que este design funcione para chamadas que precisam ser removidas localmente. Por exemplo, o Cisco CallManager pode antecipar 003 para chamadas de um telefone baseado em Melbourne para o número da Pizza Hut 1-800. Isso permite que o gatekeeper roteie a chamada para um gateway AARNet baseado em Melbourne. O gateway retira o principal 003 antes de colocar a chamada no PSTN.
- Use padrões de rota com correspondências específicas para todos os números domésticos a fim de evitar que o usuário aguarde o intervalo entre dígitos antes que a chamada seja iniciada.

Esta tabela mostra os padrões de rota para um Cisco CallManager controlado por gatekeeper:

Padrão de rota	Descrição	Rota	Gatekeeper
0.[2-9]XXXXXXX	Chamada local	Lista de rotas	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 de rotas	AARNet
0,0011!#	Chamadas internacionais	Lista de rotas	AARNet
0,0[2-4]XXXXXXXX	Chamadas para Nova Gales do Sul, Victoria e telefones celulares	Lista de rotas	AARNet
0,0[7-8]XXXXXXXX	Chamadas para o Sul da Austrália, Oeste da Austrália e Território Norte	Lista de rotas	AARNet
0,1[8-9]XXXXXXXX	Chamadas para 1800 xxx xxx e 1900 xxx xxx	Gateway local	Nenhum
0,1144X	Emergência	Gateway local	Nenhum
0,119[4-6]	Tempo e tempo	Gateway local	Nenhum
0,13[1-9]XXX	Chamadas para números 13xxxx	Gateway local	Nenhum
0,130XXXXXXX	Chamadas para 1300 xxx xxx números	Gateway local	Nenhum
[2-3]XXX	Chamadas para Sinadou	Lista de rotas	ACU
5XXX	Chamadas de Aquino	Lista de rotas	ACU
[7-9]XXX	Chamadas para McAuley, MacKillop e Saint Mary	Lista de rotas	ACU

O gatekeeper roteia chamadas internacionais, que não são enviadas através do gateway local. Isso é significativo porque o AARNet pode implantar gateways internacionais no futuro. Se um gateway é implantado nos Estados Unidos, uma simples alteração na configuração do gatekeeper permite que as universidades façam chamadas para os EUA a taxas domésticas dos EUA.

O gatekeeper executa o roteamento de chamadas intercluster com base na extensão de ACU de 4 dígitos. Esse espaço de endereços provavelmente se sobrepõe a outras universidades. Isso dita que a ACU administre seu próprio gatekeeper e use o gatekeeper AARNet como um *gatekeeper de diretório*. A coluna gatekeeper nesta tabela indica se o roteamento de chamada é executado pelo gatekeeper ACU ou pelo gatekeeper AARNet.

Observação: o único problema com a solução de gatekeeper proposta é que o dispositivo anônimo pode ser atualmente intercluster ou H.225, mas não ambos ao mesmo tempo. O Cisco CallManager conta com o gatekeeper para rotear chamadas para ambos os gateways (H.225) e para outros Cisco CallManagers (intercluster) com o projeto proposto. A solução para esse problema é não usar o gatekeeper para roteamento entre clusters ou tratar todas as chamadas via gatekeeper como H.225. A última solução alternativa significa que alguns recursos suplementares podem não estar disponíveis em chamadas intercluster.

Correio de voz

A ACU tinha três servidores de correio de voz com base no Ative Voice Repartee OS/2 com placas telefônicas Dialogic antes antes da migração para a Telefonia IP. O plano é reutilizar esses servidores no ambiente de telefonia IP. Quando implementado, cada servidor Repartee se conecta a um Cisco CallManager por meio de uma interface de mesa de mensagens simplificada (SMDI) e uma placa Catalyst 6000 Foreign Exchange Station (FXS) de 24 portas. Isso fornece correio de voz para três dos seis campus, que deixam três campus sem correio de voz. Não é possível compartilhar corretamente um servidor de Reparação entre os usuários em dois clusters do Cisco CallManager porque não há como propagar o indicador de mensagem em espera (MWI) pelo tronco H.323 intercluster.

A ACU pode comprar três servidores Cisco Unity para os campus que permanecem. Esses servidores são baseados em Skinny, portanto, não são necessários gateways. Esta tabela lista as soluções de correio de voz caso a ACU adquira os servidores de correio de voz adicionais:

Campus	Sistema de correio de voz	Gateway
Monte Saint Mary	Reparo de voz ativo	Catalyst 6000 FXS de 24 portas
MacKillop	Reparo de voz ativo	Catalyst 6000 FXS de 24 portas
Patrick	Reparo de voz ativo	Catalyst 6000 FXS de 24 portas
Aquino	Cisco Unity	—
Sigadou	Cisco Unity	—
McAuley	Cisco Unity	—

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

Recursos de mídia

Os Processadores de Sinal Digital de Hardware (DSPs - Hardware Digital Signal Processor) não estão atualmente implantados na ACU. A conferência usa o recurso de conferência baseado em software no Cisco CallManager. A conferência entre clusters não é suportada no momento.

A transcodificação não é necessária no momento. Somente os codificadores-decodificadores G.711 e G.729 são usados e são suportados por todos os dispositivos finais implantados.

Suporte a fax e modem

O tráfego de fax e modem não é suportado atualmente pela rede de Telefonia IP ACU. A universidade planeja utilizar a placa FXS de 24 portas Catalyst 6000 para essa finalidade.

Versões de software

Esta tabela lista as versões de software ACU usadas no momento desta publicação:

Platform	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	Switch do armário de fiação	—
Processador Cisco 7200	roteador de WAN	12.1(4)
Cisco 3640 Router	gateway H.323	12.1(3a)XI6

Informações Relacionadas

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