Implementación de telefonía IP en caso práctico: ACU

Contenido

Introducción

La Australian Academic and Research Network (AARNet) es una red nacional de IP de alta velocidad que conecta 37 universidades australianas, así como la Commonwealth Scientific and Industrial Research Organization (CSIRO).

AARNet se construyó inicialmente como una red de datos, pero ha transportado voz sobre IP (VoIP) desde principios de 2000. La red VoIP actualmente implementada es una solución de desvío de llamadas que transporta llamadas VoIP entre las universidades y las centralitas automáticas privadas (PABX) de CSIRO. También proporciona gateways de red telefónica pública conmutada (PSTN) que permiten a PSTN saltar al punto más rentable. Por ejemplo, una llamada de un teléfono PABX de Melbourne a un teléfono PSTN de Sidney se transporta como VoIP desde Melbourne a la gateway PSTN de Sidney. Está conectado a la PSTN.

La Universidad Católica Australiana (ACU) es una de las universidades que se conecta con AARNet. A finales de 2000, ACU comenzó una implementación de telefonía IP que implementó aproximadamente 2000 teléfonos IP en seis campus universitarios.

Este caso práctico abarca la implementación de la telefonía IP de ACU. El proyecto se ha completado. Sin embargo, hay importantes problemas arquitectónicos que hay que abordar en la estructura básica de AARNet si la red se va a ampliar cuando otras universidades sigan los pasos de la ACU. Este documento describe estos problemas y propone y discute diversas soluciones. Es probable que la implementación de telefonía IP de ACU se ajuste más adelante para ajustarse a la arquitectura recomendada final.

Nota: La Universidad Deakin fue la primera universidad australiana en implementar telefonía IP. Sin embargo, Deakin University no utiliza AARNet para transportar tráfico de telefonía IP.

AARNet

Las universidades australianas y la CSIRO construyeron AARNet en 1990 a través del Comité de Vicecancilleres de Australia. El 99 por ciento del tráfico de Internet australiano fue dirigido a los miembros fundadores durante los primeros años. Un pequeño volumen de tráfico comercial procedía de organizaciones que tenían una estrecha asociación con el sector terciario y de investigación. El uso por parte de la base de usuarios no AARNet aumentó hasta el 20% del tráfico total a finales de 1994.

La AVCC vendió la base comercial de clientes de AARNet a Telstra en julio de 1995. Este evento generó lo que eventualmente se convirtió en Telstra BigPond. Esto estimuló un mayor crecimiento del uso comercial y privado de Internet en Australia. La transferencia de propiedad intelectual y conocimientos especializados dio lugar al desarrollo de la Internet en Australia. De lo contrario, esto no habría ocurrido a un ritmo tan rápido.

La AVCC desarrolló AARNet2 a principios de 1997. Fue un nuevo perfeccionamiento de Internet en Australia, que emplea enlaces ATM de gran ancho de banda y servicios de Internet en virtud de un contrato con Cable & Wireless Optus (CWO) Limited. El rápido despliegue de los servicios de IP por parte de CWO para cumplir los requisitos de AARNet2 se debió en parte a la transferencia de conocimientos y experiencia de AARNet.

ACU

ACU es una universidad pública que se fundó en 1991. La universidad tiene aproximadamente 10.000 estudiantes y 1.000 empleados. Hay seis campus en la costa este de Australia. Esta tabla muestra los campus ACU y sus ubicaciones:

Campus	Ciudad	Estado
Monte Saint Mary	Strathfield	Nueva Gales del Sur (NSW)
MacKillop	North Sydney	Nueva Gales del Sur (NSW)
Patrick	Melbourne	Victoria (VIC)
Aquinas	Ballarat	Victoria (VIC)
Signadou	Canberra	Territorio de la Capital de Australia (ACT)
McAuley	Brisbane	Queensland (QLD)

ACU se basó en una solución Telstra Spectrum (Centrex) antes de la implementación de la solución de telefonía IP que describe este caso práctico. El cambio a la telefonía IP se debió principalmente al deseo de reducir los costes.

CSIRO

La CSIRO cuenta con aproximadamente 6.500 funcionarios en numerosos emplazamientos de Australia. La CSIRO lleva a cabo investigaciones en ámbitos como la agricultura, los minerales, la energía, la fabricación, las comunicaciones, la construcción, la salud y el medio ambiente.

CSIRO fue la primera organización en utilizar AARNet para VoIP. La organización fue pionera en la labor realizada en esta esfera.

AARNet

La red troncal AARNet es un componente significativo en cualquier implementación de telefonía IP de la universidad. Proporciona la interconexión de las universidades con dos servicios principales en el área de voz:

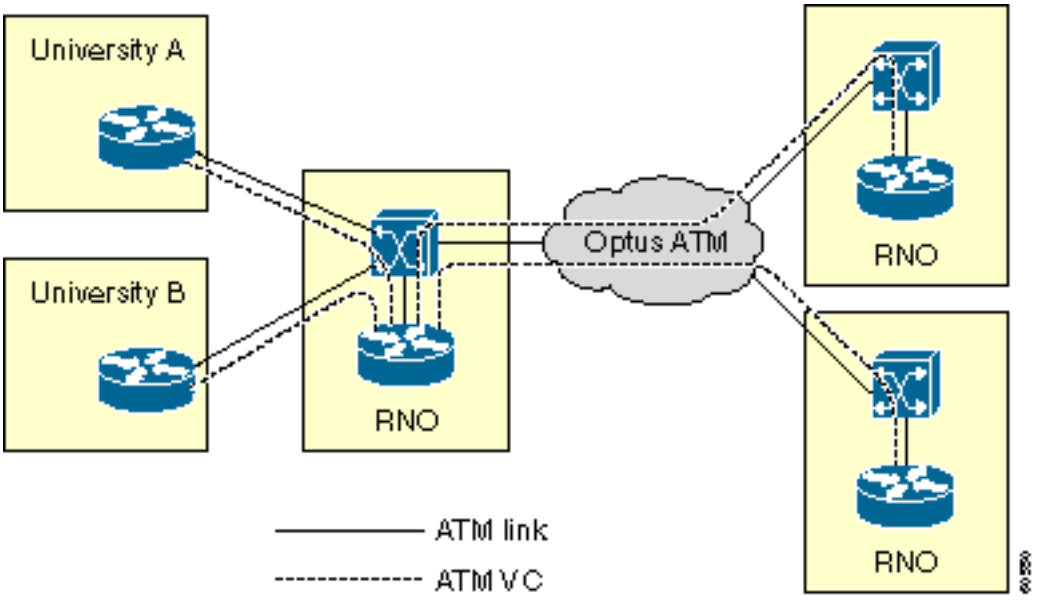
- Transporte de paquetes de protocolo de transporte en tiempo real (RTP) de VoIP con la garantía de calidad de servicio (QoS) adecuada para voz
- Los beneficios de bajo coste apuntan a las PSTN en todo el país

Esta sección describe la arquitectura AARNet actual y cómo ofrece estos servicios. También describe algunos de los problemas de escalabilidad que surgen a medida que más universidades implementan la solución de telefonía IP. Por último, analiza las posibles soluciones para estos problemas de escalabilidad.

Topología AARNet

AARNet consiste en un único POP (punto de presencia) en cada estado. Los POP se denominan Operaciones de Red Regionales (RNO). Las universidades se conectan a la RNO en sus respectivos estados. Los RNO a su vez están interconectados por una malla completa de PVC ATM Optus. Juntos constituyen AARNet.

El RNO típico consta de un switch ATM Cisco LS1010 y un router conectado a ATM. El router RNO se conecta a cada router universitario mediante un único PVC ATM a través de un link de microondas E3. Cada router RNO también tiene una malla completa de PVC ATM que la red Optus ATM proporciona a todos los demás RNO. Este diagrama representa la topología general de AARNet de la red:



Hay numerosas excepciones a la topología. Algunos de ellos son significativos desde el punto de vista de la voz. Estas son algunas excepciones:

- El RNO de Victoria utiliza IP sobre ATM clásico (RFC 1577) en lugar de PVC para conectar las universidades con el RNO.
- Las universidades rurales normalmente se conectan a RNO por Frame Relay o ISDN.
- Algunas universidades grandes tienen más de un enlace con el RNO.

Esta tabla muestra los estados y territorios que actualmente tienen un RNO. La tabla incluye ciudades capitales para lectores que no están familiarizados con la geografía australiana.

Estado	Ciudad Capital	¿RNO?	Conexiones de campus
Nueva Gales del Sur	Sídney	Yes	TBD
Victoria	Melbourne	Yes	TBD
Queensland	Brisbane	Yes	TBD
Australia del Sur	Adelaide	Yes	TBD
Australia Occidental	Perth	Yes	TBD
Territorio de la capital australiana	Canberra	Yes	TBD
Territorio del Norte	Darwin	No	—
Tasmania	Hobart	No	—

Calidad del servicio

Algunas partes de AARNet ya están habilitadas para QoS para voz como resultado del proyecto de desvío de llamadas VoIP. QoS es necesario para el tráfico de voz a fin de proporcionar estas funciones, que minimizan el retraso y la fluctuación y eliminan la pérdida de paquetes:

- Regulación de tráfico: marca el tráfico de voz de fuentes no confiables.
- Colocación en cola: se debe dar prioridad a la voz sobre el resto del tráfico para minimizar el retraso durante la congestión del link.
- Fragmentación y entrelazado de enlaces (LFI): los paquetes de datos deben fragmentarse y los paquetes de voz deben interconectarse en enlaces lentos.

El tráfico se debe clasificar para vigilar correctamente y poner en cola los paquetes de voz. Esta sección describe cómo se hace la clasificación en AARNet. Los capítulos posteriores describen la implementación de la regulación y la colocación en cola.

Clasificación

No todo el tráfico obtiene la misma QoS. El tráfico se clasifica en estas categorías para proporcionar selectivamente QoS:

- Datos
- Voz desde fuentes conocidas y de confianza
- Voz de fuentes desconocidas

Sólo los dispositivos de confianza reciben QoS de alta calidad en AARNet. Estos dispositivos son principalmente gateways identificados por dirección IP. Se utiliza una lista de control de acceso (ACL) para identificar estas fuentes de voz fiables.

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

La precedencia IP se utiliza para distinguir el tráfico de voz del tráfico de datos. La voz tiene una precedencia IP de 5.

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

Combine los ejemplos anteriores para identificar los paquetes de una fuente de confianza.

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

Utilice los mismos principios para identificar los paquetes de voz de una fuente desconocida.

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

Control de tráfico

El tráfico de voz de un origen no confiable se clasifica y se marca cuando el tráfico llega a una interfaz. Estos dos ejemplos muestran cómo se realiza la regulación de tráfico dependiendo del tipo de tráfico que se espera llegue en una interfaz dada:

El router busca paquetes de voz no confiables y cambia su precedencia IP a 0 si hay fuentes de voz confiables en flujo descendente.

```
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
```

El router busca todos los paquetes de voz y cambia su precedencia IP a 0 si no hay fuentes de voz conocidas en sentido descendente.

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

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

Colocación en cola sin voz

Hasta hace poco, todo VoIP en AARNet se saltaba el peaje. Esta condición da lugar a relativamente pocos terminales VoIP. El diseño de cola actual distingue entre las interfaces que tienen dispositivos VoIP en sentido descendente y las que no lo tienen. Esta sección trata sobre la colocación en cola en interfaces que no son de VoIP.

Se configura una interfaz que no es de voz para la cola equilibrada ponderada (WFQ) o la detección temprana aleatoria ponderada (WRED). Estos se pueden configurar directamente en la interfaz. Sin embargo, el mecanismo de colocación en cola se aplica mediante un mapa de política para facilitar el cambio del mecanismo de colocación en cola en un tipo de interfaz determinado. Hay un policy map por tipo de interfaz. Esto refleja el hecho de que no todos los mecanismos de colocación en cola son soportados en todas las 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
```

Los mapas de políticas se adjuntan a las interfaces respectivas y son específicos de los tipos de interfaz. Por ejemplo, esto simplifica el proceso de cambio del mecanismo de colocación en cola

en los puertos Ethernet basados en el procesador de interfaz versátil (basados en VIP) de WRED a WFQ. Requiere un único cambio en el mapa de políticas. Los cambios se realizan en todas las interfaces Ethernet basadas en 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
```

Colocación en cola de latencia baja

Cualquier interfaz que tenga dispositivos VoIP de confianza descendente se configura para colas de baja latencia (LLQ). Cualquier paquete que lo haga a través de la clasificación de la interfaz entrante y conserve una precedencia de 5 está sujeto a LLQ. Cualquier otro paquete está sujeto a WFQ o WRED. Esto depende del tipo de interfaz.

Se crean mapas de política separados para cada tipo de interfaz para facilitar la administración de QoS. Esto es similar al diseño de cola sin voz. Sin embargo, existen varios mapas de políticas para cada tipo de interfaz. Esto se debe a que la capacidad de los tipos de interfaz para transportar tráfico de voz varía según la velocidad del link, la configuración de PVC, etc. El número del nombre del mapa de políticas refleja el número de llamadas atendidas para 30 llamadas, 60 llamadas, 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
```

Los mapas de políticas se adjuntan a las interfaces respectivas. En este ejemplo, el policy map es específico de un tipo de interfaz. Actualmente no se da un tratamiento especial a la señalización de voz. Los mapas de políticas pueden modificarse fácilmente en un lugar si esto se convierte en un requisito en una etapa posterior en un tipo de interfaz determinado. El cambio afecta a todas las interfaces de ese 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
```

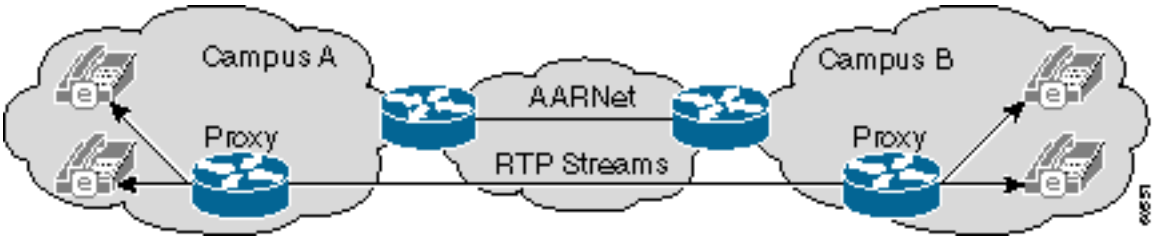
Escalabilidad LLQ

El mecanismo de colocación en cola tiene algunos problemas de escalabilidad. El problema principal es que se basa en conocer la dirección IP de cada dispositivo VoIP de confianza en la red. Esta era una limitación razonable en el pasado, cuando había un número limitado de gateways VoIP que gestionaban el desvío de tarifas. El número de terminales VoIP aumenta drásticamente y cada vez resulta más poco práctico con la implementación de telefonía IP. Las ACL se vuelven demasiado largas y difíciles de administrar.

Las ACL se han agregado para confiar en el tráfico de una subred IP de voz específica en cada campus de ACU en el caso de ACU. Esta es una solución provisional. Estas soluciones a largo plazo se están investigando:

- Proxy H.323
- Regulación de entrada de QoS

La idea principal detrás de la solución proxy H.323 es que todo el tráfico RTP entre AARNet desde un campus determinado mediante un proxy. AARNet ve todo el tráfico RTP desde un campus determinado con una única dirección IP, como muestra este diagrama:

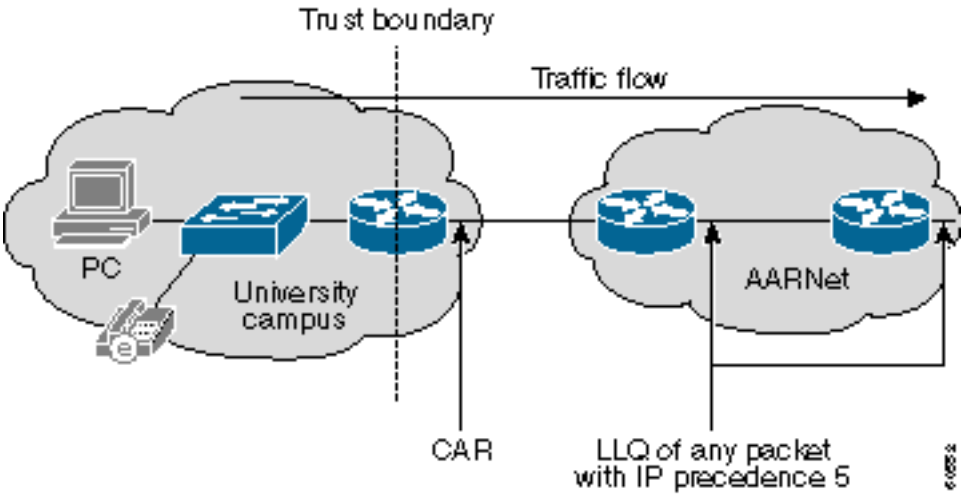


El número de entradas en las ACL de QoS se limita a una línea por campus si este esquema se implementa de forma uniforme. Este plan todavía tiene el potencial de sumar hasta 100 entradas o más, ya que hay 37 universidades con múltiples campus. Esto tampoco es escalable. Podría ser necesario pasar a un diseño con un número único o limitado de superproxies compartidos en cada RNO. Esto reduce el número de direcciones IP de confianza a seis. Sin embargo, esto abre un problema de regulación de QoS en la trayectoria desde el campus al proxy en el RNO.

Nota: Los troncales de interclúster de Cisco CallManager no funcionan actualmente a través de un proxy H.323 porque la señalización entre clústers no es H.225 nativo.

La regulación de entrada de QoS es una solución alternativa. Se establece un límite de confianza en el punto en el que el campus se conecta al RNO con este diseño. El tráfico que entra en AARNet se controla mediante la función Velocidad de acceso comprometido (CAR) de Cisco IOS® en este límite. Una universidad que utiliza AARNet para VoIP se suscribe a una cierta cantidad de ancho de banda AARNet QoS. CAR monitorea el tráfico que entra en AARNet. El exceso de tráfico tiene precedencia IP delimitada a 0 si la cantidad de tráfico RTP con precedencia IP 5 excede el ancho de banda suscrito.

Este diagrama muestra una configuración CAR:



Este ejemplo muestra cómo una configuración CAR maneja esta regulación:

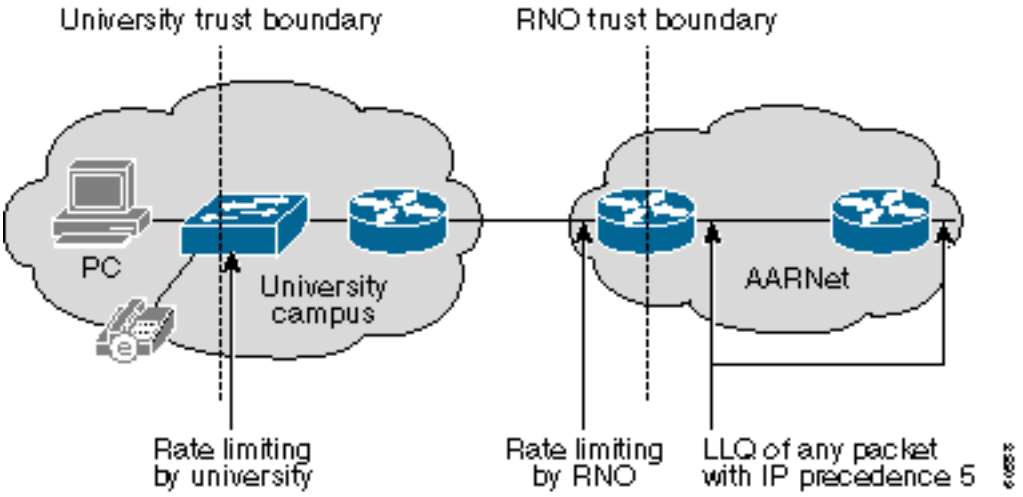
```
Interface a1/0.100
rate-limit input access-group 100 2400000 0 0 conform-action set-prec-transmit 5
exceed-action set-prec-transmit 0

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

Estas son algunas de las ventajas de un enfoque de configuración CAR:

- El núcleo ya no necesita controlar la regulación. Ahora se gestiona en el límite de confianza. Por lo tanto, el LLQ en el núcleo no necesita saber sobre las direcciones IP de confianza. Cualquier paquete con una precedencia IP de 5 en el núcleo puede estar sujeto a LLQ de forma segura porque ya ha pasado la regulación en el ingreso.
- No se hacen suposiciones sobre la arquitectura, el equipo y los protocolos de VoIP que elijan las universidades individuales. Una universidad puede optar por implementar un protocolo de inicio de sesión (SIP) o un protocolo de control de gateway de medios (MGCP) que no funcione con los proxies H.323. Los paquetes VoIP reciben la QoS adecuada en el núcleo siempre y cuando tengan una precedencia IP de 5.
- CAR es resistente a los ataques de denegación de servicio (DoS) de QoS. Un ataque DoS de QoS que se origina en una universidad no puede dañar el núcleo. CAR limita el ataque, que no puede generar más tráfico que el que está presente cuando el número máximo de llamadas VoIP permitidas está activo.Las llamadas VoIP desde o hacia ese campus pueden sufrir durante un ataque. Sin embargo, depende de cada universidad protegerse internamente. La universidad puede ajustar las ACL CAR en el router de modo que todas las subredes VoIP excepto las seleccionadas tengan la precedencia IP marcada hacia abajo.Cada campus tiene un límite de confianza interno en el punto en el que los usuarios se conectan a la LAN del campus en el diseño final. El tráfico con una precedencia IP de 5 que recibe este límite de confianza está limitado a 160 kbps por puerto de switch o a dos llamadas VoIP G.711. El tráfico que excede esta velocidad se marca hacia abajo. La implementación de este esquema requiere switches Catalyst 6500 o algo similar con funcionalidad de limitación de velocidad.
- El aprovisionamiento de ancho de banda en el núcleo se simplifica a medida que cada universidad se suscribe a una cantidad fija de ancho de banda de QoS. Esto también simplifica la facturación de QoS, ya que cada universidad puede pagar una cuota mensual fija basada en una suscripción de ancho de banda de QoS.

La principal debilidad en este diseño es que el límite de confianza está ubicado en el router universitario, por lo que las universidades deben ser capaces de administrar correctamente la CAR. El límite de confianza se devuelve al RNO. El equipo administrado por RNO maneja la regulación en el diseño final. Este diseño requiere limitación de velocidad basada en hardware, como el switch Catalyst 6000 o un procesador Cisco 7200 Network Services Engine (Cisco 7200 NSE-1). Sin embargo, proporciona a AARNet y a los RNO un control total sobre la regulación de QoS. Este diagrama muestra este diseño:



Fragmentación y entrelazado de link

VoIP sólo se transporta a través de circuitos virtuales ATM (VC) de velocidad relativamente alta. Por lo tanto, no se requiere LFI. VoIP también se puede transportar a través de Frame Relay Forum (FRF) o líneas alquiladas a universidades rurales en el futuro. Esto requiere mecanismos LFI como PPP de links múltiples (MLP) con Interleave o FRF.12.

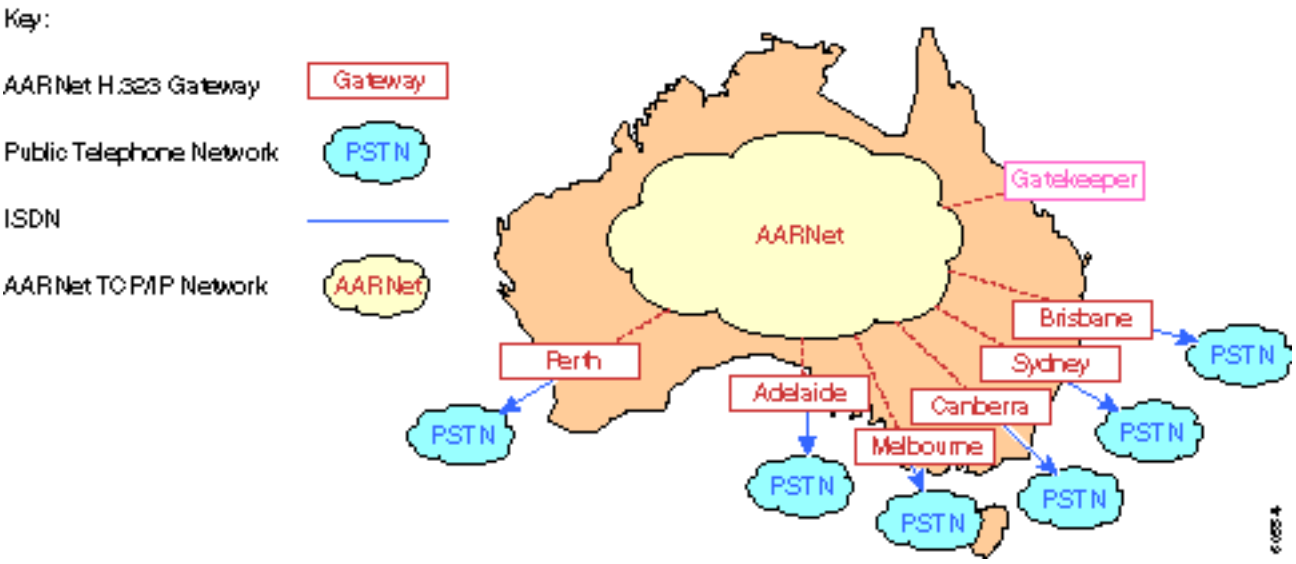
Gateways

Hay dos tipos de gateways H.323 en AARNet:

- PSTN: gateway de PSTN a VoIP
- PABX: gateway PABX a VoIP

La distinción entre un gateway PSTN y PABX es principalmente funcional. Los gateways PSTN proporcionan conectividad a la PSTN. Los gateways PABX conectan una centralita privada de la universidad a la red troncal VoIP. En muchos casos, el mismo cuadro físico actúa como gateway PSTN y PABX. Actualmente hay 31 gateways en la solución de telefonía IP de ACU. La mayoría de estos gateways son servidores de acceso universal Cisco AS5300. Los otros gateways son Cisco 3600 Series Routers o Cisco 2600 Series Routers. Se espera añadir un mínimo de diez gateways adicionales durante el segundo trimestre de 2001. AARNet realizó aproximadamente 145 000 llamadas VoIP en abril de 2001.

AARNet ha implementado gateways H.323 conectados a PSTN en la mayoría de las ciudades principales, como muestra este diagrama:



Las universidades pueden utilizar estos gateways para realizar llamadas salientes a PSTN. Las universidades tienen que mantener sus propios troncales para las llamadas entrantes porque actualmente no son compatibles. AARNet puede negociar un precio muy competitivo con el operador debido al volumen de llamadas que pasan por estas gateways. Las llamadas también se pueden cancelar en el punto más rentable. Por ejemplo, alguien en Sydney que llama a un número Perth puede utilizar la puerta de enlace Perth y sólo se le puede cobrar por una llamada local. Esto también se conoce como Salto de finalización de cola (TEHO).

Se implementa un único gatekeeper para realizar E.164 a la resolución de direcciones IP. Todas las llamadas a PSTN se envían al gatekeeper, que luego devuelve la dirección IP del gateway más apropiado. Consulte las secciones Planes de marcación y Gatekeeper para obtener información más detallada sobre los gatekeepers.

Facturación y contabilidad

Los gateways PSTN utilizan RADIUS y la autenticación, autorización y contabilidad (AAA) para fines de facturación. Cada llamada a través de una puerta de enlace genera un registro de detalles de llamada (CDR) para cada tramo de llamada. Estos CDR se publican en el servidor RADIUS. La dirección IP del CallManager de Cisco en el CDR identifica de forma única a la universidad y garantiza que se facturará a la persona correcta.

Seguridad de gateway

Proteger los gateways PSTN contra los ataques de DoS y el fraude es una preocupación importante. Los clientes H.323 están ampliamente disponibles. Microsoft NetMeeting se incluye con Microsoft Windows 2000, por lo que es relativamente fácil para un usuario no técnico realizar llamadas gratuitas a través de estos gateways. Configure una ACL entrante que permita la señalización H.225 desde direcciones IP de confianza para proteger estos gateways. Este enfoque tiene todos los mismos problemas de escalabilidad que la sección QoS describe. El número de entradas en la ACL crece a medida que crece el número de terminales H.323 de confianza.

Los proxies H.323 ofrecen cierto alivio en esta área. Las ACL de gateway deben permitir una dirección IP por campus universitario si todas las llamadas a través del gateway PSTN pasan a través de un proxy de campus. En la mayoría de los casos, es deseable tener dos direcciones IP como proxy redundante. Incluso con los proxies, la ACL puede contener más de 100 entradas.

El proxy debe estar protegido mediante ACL, ya que cualquier H.323 puede configurar una llamada a través del proxy. La ACL de proxy debe permitir los dispositivos H.323 locales según lo requiera la política local, ya que esto se hace por campus.

Las direcciones IP de los dos Cisco CallManagers se deben incluir en las ACL de gateway si un campus desea permitir que sólo las llamadas de teléfonos IP utilicen las puertas de enlace PSTN AARNet. Los proxies no añaden ningún valor en esta situación. El número de entradas de ACL necesarias es de dos formas.

Tenga en cuenta que las llamadas de teléfono IP a IP entre campus no necesitan pasar a través del proxy.

Planes de marcado

El plan de marcación VoIP actual es sencillo. Los usuarios pueden realizar estos dos tipos de llamadas desde una perspectiva de gateway VoIP:

- Llame a un teléfono de un campus diferente pero de la misma universidad.
- Llame a un teléfono PSTN o a un teléfono de otra universidad.

Los pares de marcado de la gateway reflejan el hecho de que sólo hay dos tipos de llamadas. Básicamente hay dos tipos de par de marcado VoIP, como muestra este ejemplo:

```
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
```
El primer par de marcado se utiliza si alguien llama a la extensión 7... en otro campus de este ejemplo. Esta llamada se enruta directamente a la dirección IP del gateway remoto. Puesto que se omite el control de acceso, no se realiza el control de admisión de llamadas (CAC).

El segundo par de marcado se utiliza cuando la llamada es para un número PSTN. Puede ser uno de estos elementos:

- El número de un teléfono en PSTN
- El número PSTN completo de un teléfono de una universidad diferente

La llamada se envía al gatekeeper mediante un mensaje de solicitud de admisión (ARQ) en el primer caso. El gatekeeper devuelve la dirección IP de la mejor gateway PSTN en un mensaje de confirmación de admisión (ACF).

La llamada también se envía al gatekeeper mediante un mensaje ARQ en el segundo caso. Sin embargo, el gatekeeper devuelve un mensaje ACF con la dirección IP del gateway VoIP en la universidad que recibe la llamada.

Gatekeeper

AARNet actualmente opera un único gatekeeper. El único propósito de este gatekeeper es realizar el ruteo de llamadas en la forma de E.164 a la resolución de direcciones IP. El gatekeeper no realiza CAC. El número de líneas troncales PABX conectadas a las puertas de enlace limita el número de llamadas simultáneas. El ancho de banda del núcleo se ocupa de todos los troncales en uso a la vez. Esto cambia con la implantación de la telefonía IP en ACU y otras universidades. No hay límite natural en el número de llamadas VoIP simultáneas que se pueden originar dentro o fuera de un campus determinado en este nuevo entorno. El ancho de banda QoS disponible puede sobresuscribirse si se inician demasiadas llamadas. Todas las llamadas pueden sufrir de mala calidad en esta condición. Utilice el control de acceso para proporcionar CAC.

La naturaleza distribuida y el tamaño potencial de la red de voz de la universidad se presta a una arquitectura de gatekeeper distribuida. Una solución posible es tener un diseño jerárquico de control de acceso de dos niveles en el que cada universidad mantenga su propio control de acceso. Este gatekeeper universitario se denomina gatekeeper de nivel 2. AARNet opera un gatekeeper de *directorio* que se denomina gatekeeper de nivel 1.

Las universidades deben utilizar este enfoque de dos niveles para utilizar un gatekeeper para el ruteo de llamadas entre los clústeres de Cisco CallManager. El gatekeeper enruta las llamadas basándose en una extensión de 4 o 5 dígitos en este escenario. Cada universidad necesita su propio gatekeeper. Esto se debe a que los rangos de extensión se superponen entre universidades, ya que se trata de un espacio de dirección administrado localmente.

Los gatekeepers de nivel 2 de la universidad realizan CAC solo para llamadas hacia y desde esa universidad. También realiza la resolución E.164 para las llamadas entre los campus de esa universidad. El gatekeeper de nivel 2 dirige la llamada al gatekeeper de nivel 1 mediante un mensaje de solicitud de ubicación (LRQ) si alguien llama a un teléfono IP en otra universidad o llama a la PSTN a través de una gateway AARNet. El LRQ se reenvía al gatekeeper de nivel 2 de esa universidad si la llamada es para otra universidad. Este gatekeeper luego devuelve un mensaje ACF al gatekeeper de nivel 2 en la universidad donde se origina la llamada. Ambos gatekeepers de nivel 2 realizan CAC. Solo proceden con la llamada si hay suficiente ancho de banda disponible en las zonas de llamada y de llamada.

AARNet puede optar por tratar las puertas de enlace AARNet PSTN como las de cualquier universidad. Su propio gatekeeper de nivel 2 se ocupa de ellos. El gatekeeper de nivel 1 también puede actuar como gatekeeper de nivel 2 para estas gateways si la carga y el rendimiento lo permiten.

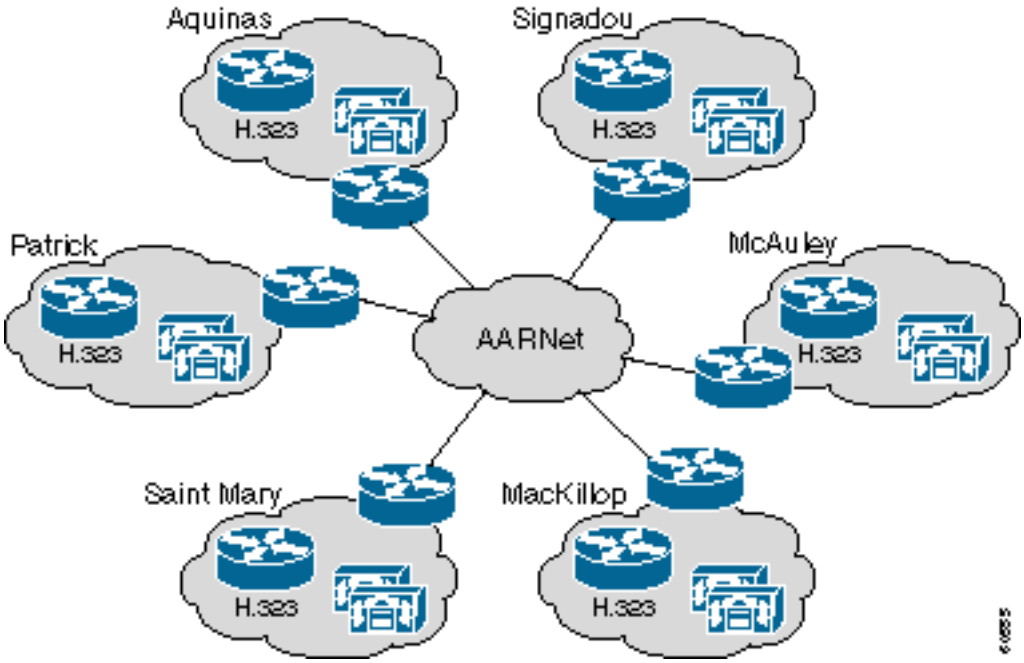
Cada uno de los gatekeepers (incluido el gatekeeper de directorio AARNet) debe replicarse porque las gateways son un componente crítico. Cada universidad necesita tener dos guardianes. Es posible que los gateways del IOS de Cisco tengan gatekeepers alternativos, como en el caso de la versión 12.0(7)T del software del IOS de Cisco. Sin embargo, actualmente Cisco CallManager o cualquier otro dispositivo H.323 de terceros no soportan esto. No utilice esta función en este momento. Utilice en su lugar una solución sencilla basada en el protocolo de router de espera en caliente (basada en HSRP). Esto requiere que ambos gatekeepers estén en la misma subred IP. HSRP determina qué gatekeeper está activo.

Red de ACU IP Telephony

Esta tabla muestra el número aproximado de teléfonos IP instalados en los campus de ACU:

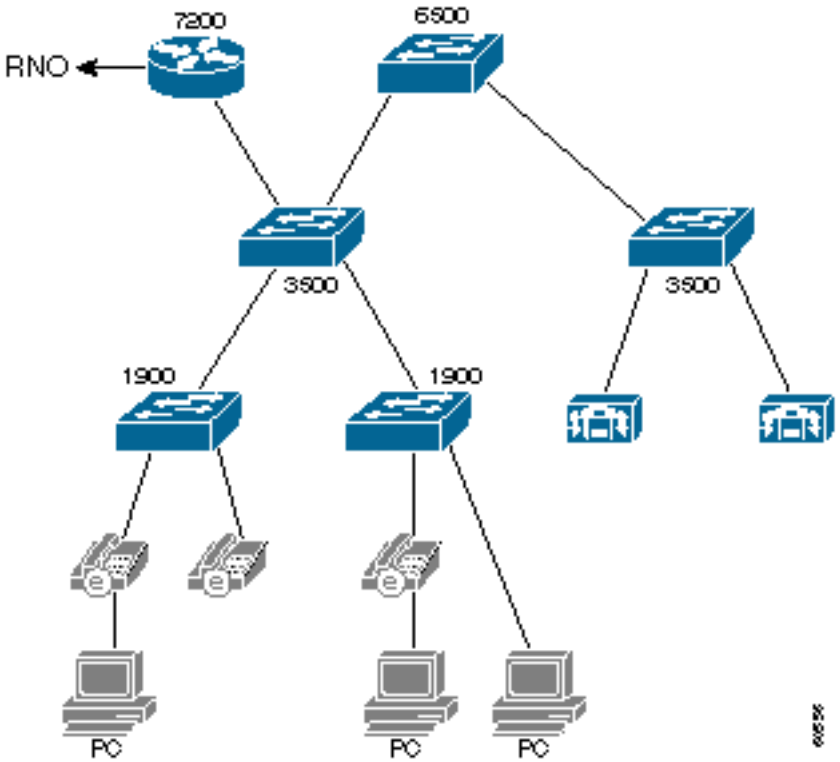
Campus	Ciudad	Teléfonos IP aproximados
Monte Saint Mary	Strathfield	400
MacKillop	North Sydney	300
Patrick	Melbourne	400
Aquinas	Ballarat	100
Signadou	Canberra	100
McAuley	Brisbane	400
	Total:	*1700*

ACU implementó recientemente una solución de telefonía IP. La solución consta de un clúster de dos Cisco CallManagers, un gateway Cisco 3640 en cada campus y teléfonos IP. AARNet interconecta los campus. Este diagrama describe la topología de alto nivel y los diversos componentes de la red de telefonía IP ACU:



Topología de red ACU

Este diagrama muestra un campus ACU típico. Cada campus cuenta con tres capas de switches Catalyst. La sala de cableado alberga los switches Catalyst 1900 más antiguos. Los switches Catalyst 1900 se vuelven a conectar al switch Catalyst 3500XL mediante el entramado extendido. Estos dispositivos se vuelven a conectar a un único switch Catalyst 6509 mediante Gigabit Ethernet (GE). Un único router Cisco 7200 VXR conecta el campus a AARNet mediante un VC ATM al RNO local.



El método de conectividad con el RNO varía ligeramente de un estado a otro, como muestra esta tabla. Victoria se basa en IP clásica sobre ATM (RFC 1577). Los otros RNO tienen una configuración de PVC directa con encapsulación RFC 1483. Open Shortest Path First (OSPF) es el protocolo de routing utilizado entre ACU y los RNO.

Campus	Estado	Conectividad con RNO	Protocolo de ruteo
Monte Saint Mary	NSW	PVC RFC 1483	OSPF
MacKillop	NSW	PVC RFC 1483	OSPF
Patrick	VIC	RFC 1577 IP clásica sobre ATM	OSPF
Aquinas	VIC	RFC 1577 IP clásica sobre ATM	OSPF
Signadou	ACT	PVC RFC 1483	OSPF
McAuley	QLD	PVC RFC 1483	OSPF

Los switches Catalyst de la serie 1900 soportan el trunking sólo en los links ascendentes. Por lo tanto, los teléfonos IP y los PC están todos en una VLAN grande. De hecho, todo el campus es una gran VLAN y un dominio de difusión. Las subredes IP secundarias se utilizan debido al gran número de dispositivos. Los teléfonos IP están en una subred IP y los PC en otra. El núcleo AARNet confía en la subred del teléfono IP y el tráfico hacia y desde esta subred IP está sujeto a LLQ.

El router Cisco 7200 enruta entre las subredes IP primaria y secundaria. La tarjeta de función del switch multicapa (MSFC) del switch Catalyst 6500 no se utiliza actualmente.

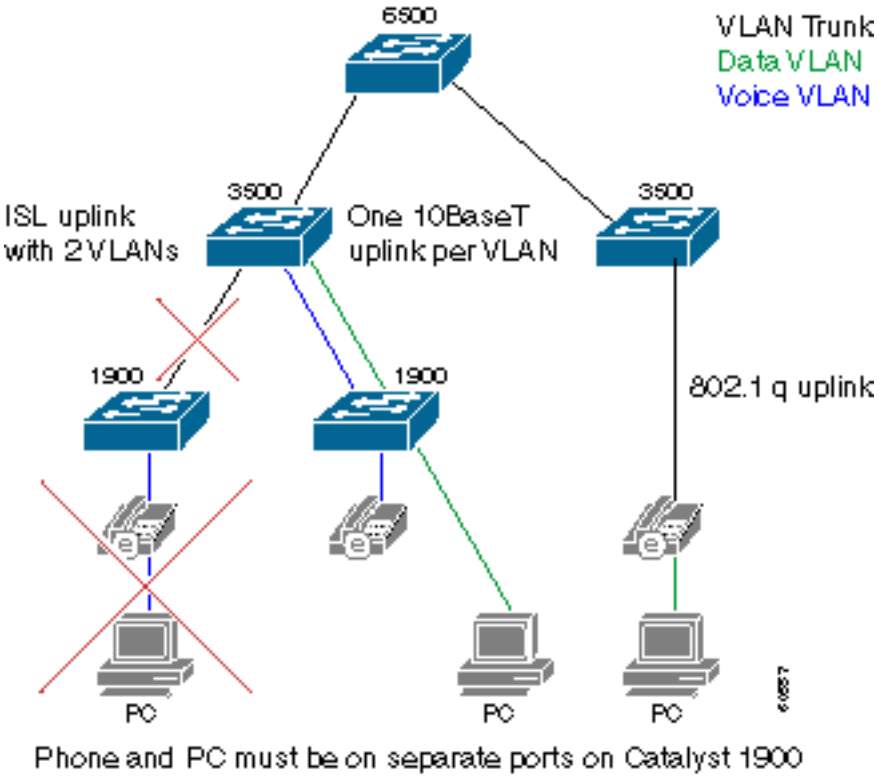
Los switches Catalyst 3500XL y Catalyst 6500 tienen funciones de QoS, pero actualmente no están habilitados.

QoS (Calidad de servicio) en el Campus

El diseño actual del campus no cumple con las directrices de diseño recomendadas por Cisco para la telefonía IP. Estas son algunas preocupaciones sobre QoS:

- El dominio de difusión es muy grande. Las transmisiones excesivas pueden afectar al rendimiento de los teléfonos IP, que tienen que procesarlos.
- Los switches Catalyst 1900 no son compatibles con QoS. Si un teléfono IP y un PC están conectados al mismo puerto de switch, los paquetes de voz se pueden descartar si el PC recibe los datos a una velocidad alta.

Rediseñe las partes de la infraestructura del campus para lograr mejoras significativas. No se requiere una actualización de hardware. Este diagrama ilustra los principios detrás del rediseño recomendado:



El campus debe dividirse en una VLAN de voz y una VLAN de datos. Los teléfonos y los PC que se conectan a un switch Catalyst 1900 ahora deben conectarse a diferentes puertos para lograr la separación de VLAN. Se agrega un link ascendente adicional de cada switch Catalyst 1900 al switch Cisco 3500XL. Uno de los dos links ascendentes es un miembro de la VLAN de voz. El otro link ascendente es un miembro de la VLAN de datos. No utilice enlaces troncales InterSwitch Link (ISL) como alternativa a dos enlaces ascendentes. Esto no proporciona al tráfico de voz y datos colas separadas. Los links GE del switch Catalyst 3500XL al switch Catalyst 6000 también se deben convertir en troncales 802.1q para que tanto la VLAN de voz como de datos se puedan transportar a través de este switch de núcleo.

Los puertos del switch Catalyst 3500XL que se encuentran en la VLAN de datos tienen una clase de servicio (CoS) predeterminada de cero. Los puertos que son miembros de la VLAN de voz tienen un CoS predeterminado de 5. Como resultado, el tráfico de voz se prioriza correctamente una vez que llega al núcleo Catalyst 3500 o Catalyst 6500. Las configuraciones del puerto del switch de QoS de Catalyst 3500 varían ligeramente dependiendo del puerto del switch VLAN que sea miembro, como muestra este ejemplo:

```
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
```

Puede conectar un PC al puerto del switch trasero del teléfono IP en el caso poco común de que los teléfonos IP se conecten directamente a un switch Catalyst 3500XL. En este caso, los teléfonos IP se conectan al switch mediante un tronco 802.1q. Esto permite que los paquetes de voz y datos viajen en VLAN separadas, y puede dar a los paquetes la CoS correcta en el ingreso. Sustituya los switches Catalyst 1900 por switches Catalyst 3500XL u otros switches compatibles con QoS a medida que alcanzan el fin de su vida útil. A continuación, esta topología se convierte

en el método estándar para conectar teléfonos IP y PC a la red. Este escenario muestra la configuración de QoS del switch Catalyst 3500XL:

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

Por último, los dos puertos que se conectan a los dos Cisco CallManagers deben tener el CoS codificado en 3. Cisco CallManager establece la precedencia IP en 3 en todos los paquetes de señalización de voz. Sin embargo, el link de Cisco CallManager al switch Catalyst 3500XL no utiliza 801.1p. Por lo tanto, el valor de CoS se fuerza en el switch como muestra este ejemplo:

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

El obstáculo principal con este diseño es que se necesitan dos puertos de switch en el escritorio. El campus de Patrick podría requerir 400 puertos de switch adicionales para 400 teléfonos IP. Si no hay suficientes puertos disponibles, se deben implementar switches Catalyst 3500XL adicionales. Sólo se necesita un puerto de switch Catalyst 3500XL para cada dos puertos de switch Catalyst 1900 que faltan.

Los switches ACU Catalyst 6500 actuales tienen capacidades de QoS, pero actualmente no están habilitados. Estos módulos están presentes en el switch Catalyst 6000 de ACU con estas capacidades de colocación en cola:

Ranura	Módulo	Puertos	Colas RX	Colas 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	—	—

Complete estos pasos para activar las funciones de QoS apropiadas en el switch Catalyst 6000:

1. Indíquele al switch que proporcione QoS por VLAN con este comando:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 vlan-based
   ```

2. Indíquele al switch que confíe en los valores de CoS recibidos del switch Catalyst 3500XL con este comando:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos
   ```

El CoS ahora se debe establecer en la asignación de punto de código de servicios diferenciados (DSCP). Esto es necesario porque el switch Catalyst 6000 reescribe el valor DSCP en el encabezado IP basándose en el valor CoS recibido. Los paquetes de señalización VoIP deben tener un CoS de 3, reescrito con un DSCP de AF31 (26). Los paquetes RTP deben tener un CoS de 5, reescrito con un DSCP de EF (46). Ejecutar este comando:

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

Utilice este ejemplo para verificar la asignación de CoS a 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 la MSFC para rutear entre las diversas subredes IP.

QoS (Calidad de servicio) en RNO

El diseño RNO actual no cumple con las directrices de diseño recomendadas por Cisco para telefonía IP. Estas preocupaciones existen con respecto a QoS:

- LLQ no se aplica en el Cisco ACU 7200 Series WAN Router.
- Los campus Patrick y Aquinas se conectan al RNO mediante VC conmutados ATM (SVC). LLQ no se soporta en los SVC.

Un router Cisco 7200 conectado a Fast Ethernet conecta el campus a un RNO mediante un enlace E4 ATM de 34 Mbps. El tráfico puede potencialmente poner en cola hacia arriba en los links 34M debido a la discordancia de velocidad de 4M frente a 100M. Por lo tanto, es necesario priorizar el tráfico de voz. Utilice LLQ. La configuración del router Cisco 7200 es similar a este ejemplo:

```
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
```

El ancho de banda asignado a LLQ debe ser *N x 24Kbps*, donde N es el número de llamadas G.729 simultáneas.

Configure un PVC de cada uno de los routers Patrick y Aquinas Cisco 7200 al router AARNet. Los SVC ATM en el RNO Victoria no admiten LLQ, ya que se basa en IP clásica sobre ATM (RFC 1577). Las otras universidades de la RNO Victoria pueden seguir usando RFC 1577 por ahora.

Sin embargo, eventualmente reemplace la infraestructura Classical IP over ATM.

Gateways

Cada una de las instalaciones ACU tiene un router Cisco 3640 que actúa como gateway H.323. Estas puertas de enlace se conectan a la PSTN mediante ISDN. El número de interfaces de velocidad primaria (PRI) y canales B depende del tamaño del campus. Esta tabla enumera el número de PRI y canales B para cada campus:

Campus	Cantidad PRI	Cantidad del canal B
Monte Saint Mary	2	30
MacKillop	2	50
Patrick	2	50
Aquinas	1	20
Signadou	1	20
McAuley	1	30

Estos gateways se utilizan solamente como gateways secundarios para DOD (Marcación directa saliente). Las puertas de enlace AARNet son las principales. Las puertas de enlace ACU siempre se utilizan para DID (Direct Inward Dialing).

Plan de marcado

El plan de marcación se basa en números de extensión de 4 dígitos. La extensión es también los últimos cuatro dígitos del número DID. Esta tabla enumera los rangos de extensión y los números DID para cada campus:

Campus	Extensión	DID
Monte Saint Mary	9xxx	02 9764 9xxx
MacKillop	8 xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Aquinas	5xxx	03 5330 5xxx
Signadou	2xxx	02 6123 2xxx
McAuley	7xxx	07 3354 7xxx

Una simple entrada `num-exp` en las gateways trunca el número DID a la extensión de 4 dígitos antes de pasarlo a Cisco CallManager. Por ejemplo, el gateway de campus Patrick tiene esta entrada:

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

Los usuarios marcan cero para seleccionar una línea externa. Este cero principal se transfiere al gateway. Un único par de marcado POTS dirige la llamada hacia el puerto ISDN basado en el cero principal.

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

Las llamadas entrantes utilizan esta entrada num-exp para transformar el número de la persona a la que se llama en una extensión de 4 dígitos. A continuación, la llamada coincide con ambos pares de marcado VoIP. Según la preferencia inferior, prefiere esta ruta al suscriptor de 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
```

CallManager de Cisco

Cada uno de los campus tiene un clúster que consta de dos servidores Cisco CallManager. Los servidores Cisco CallManager son una combinación de Media Convergence Server 7835 (MCS-7835) y Media Convergence Server 7820 (MCS-7820). Ambos servidores ejecutaban la versión 3.0(10) en el momento de esta publicación. Un Cisco CallManager es el *editor* y el otro Cisco CallManager es el *suscriptor*. El suscriptor actúa como el Cisco CallManager primario para todos los teléfonos IP. Esta tabla enumera el hardware implementado en cada campus:

Campus	Platform	CallManagers
Monte 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 clúster se configura con dos regiones:

- Uno para llamadas dentro de la red (G.711)
- Uno para llamadas entre campus (G.729)

El CAC basado en la ubicación no es apropiado para ACU porque todos los teléfonos IP que sirven cada clúster se encuentran en un solo campus. Hay ventajas para un CAC basado en el gatekeeper para llamadas entre campus, pero esto no se implementa actualmente. Sin embargo, se prevé hacerlo en un futuro próximo.

Cada Cisco CallManager se configura con 22 gateways H.323. Se compone de troncales entre

clústeres a los otros cinco clústeres de Cisco CallManager, seis gateways PSTN AARNet y un gateway ACU en cada campus.

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

Las listas de rutas y los grupos de rutas se utilizan para clasificar los gateways PSTN. Por ejemplo, esta tabla muestra cómo las llamadas de Patrick Cisco CallManager en Melbourne al Sydney PSTN pueden utilizar las cuatro puertas de enlace para vincular las llamadas con un grupo de rutas.

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

Los Cisco CallManagers se configuran con aproximadamente 30 patrones de ruta, como se muestra en esta tabla. Los patrones de ruta están diseñados de modo que haya coincidencias específicas para todos los números nacionales australianos. De esta manera, los usuarios no tienen que esperar a que caduque el tiempo de espera entre dígitos antes de que Cisco CallManager inicie la llamada. El carácter comodín "!" se utiliza sólo en el patrón de ruta para los números internacionales. Los usuarios deben esperar hasta que caduque el tiempo de espera entre dígitos (predeterminado, 10 segundos) antes de que la llamada progrese cuando marquen un destino internacional. Los usuarios también pueden agregar el patrón de ruta "0.0011!#". Los usuarios pueden entonces ingresar un "#" después del último dígito para indicar a Cisco CallManager que el número marcado está completo. Esta acción acelera la marcación internacional.

Patrón de ruta	Descripción
0.[2-9]XXXXXXX	Llamada local
0.00	Llamada de emergencia: si el usuario olvida marcar 0 para una línea externa
0.000	Llamada de emergencia
0.013	Asistencia de directorio
0.1223	—
0.0011!	Llamadas internacionales
0,02XXXXXXX	Llamadas a Nueva Gales del Sur
0,03XXXXXXX	Llamadas a Victoria
0,04XXXXXXX	Llamadas a teléfonos móviles
0,07XXXXXXX	Llamadas a Queensland
0,086XXXXXX	Llamadas a Australia Occidental
0,08XXXXXXX	Llamadas al sur de Australia y al

	territorio norte
0.1[8-9]XXXXXXXX	Llamadas al 1800 xxx xxx y al 1900 xxx xxx xxx
0,1144 X	Emergencia
0,119[4-6]	Tiempo y tiempo
0,1245 veces	Directorio
0.13[1-9]XXX	Llamadas a números 13xxxx
0,130XXXXXXX	Llamadas a los números 1300 xxx xxx xxx
2[0-1]XX	Llamadas de interclúster a Signadou
3[0-4]XX	Llamadas entre clústers a Patrick
5[3-4]XX	Llamadas de interclúster a Aquinas
7[2-5]XX	Llamadas entre clústers a McAuley
8[0-3]XX	Llamadas de interclúster a MacKillop
9[3-4]XX	Llamadas interraciales al Monte Santa María
9[6-7]XX	Llamadas interraciales al Monte Santa María

El número de gateways, grupos de rutas, listas de rutas y patrones de ruta configurados en los Cisco CallManagers de ACU tiene el potencial de aumentar a un gran número. Si se implementa un nuevo gateway RNO, los cinco clústeres de Cisco CallManager deben reconfigurarse con un gateway adicional. Peor aún, es necesario agregar cientos de gateways si los Cisco CallManagers de ACU enrutan las llamadas VoIP directamente a todas las demás universidades y omiten por completo la PSTN. Claramente, esto no se escala muy bien.

La solución es hacer que el gatekeeper de Cisco CallManagers esté controlado. Sólo debe actualizar el gatekeeper cuando se agrega una nueva gateway o Cisco CallManager en algún lugar de AARNet. Cada Cisco CallManager debe tener solamente el gateway de campus local y el dispositivo anónimo configurados cuando esto ocurra. Puede pensar en este dispositivo como un tronco punto a multipunto. Elimina la necesidad de los troncales PPP mallados en el modelo de plan de marcado de Cisco CallManager. Un único grupo de rutas señala al dispositivo anónimo como gateway preferido y al gateway local como gateway de respaldo. La puerta de enlace PSTN local se utiliza para determinadas llamadas locales y también para llamadas generales fuera de la red si el gatekeeper deja de estar disponible. Actualmente, el dispositivo anónimo puede ser intercluster o H.225, pero no ambos al mismo tiempo.

Cisco CallManager necesita menos patrones de ruta con un gatekeeper de los que tiene ahora. En principio, Cisco CallManager sólo necesita un patrón de ruta único de "!" apuntando al gatekeeper. En realidad, la forma en que se enrutan las llamadas debe ser más específica por estas razones:

- Algunas llamadas (como las llamadas al 1-800 o los números de emergencia) deben enrutarse a través de un gateway geográficamente local. Alguien en Melbourne que llama a la policía o a una cadena de restaurantes como Pizza Hut no quiere estar conectado con la policía o el Pizza Hut en Perth. Se necesitan patrones de ruta específicos que apunten directamente al gateway PSTN de campus local para estos números.Las universidades que planean realizar futuras implementaciones de telefonía IP pueden optar por confiar

exclusivamente en los gateways AARNet y no administrar sus propios gateways locales. Estos números deben tener un código de área virtual precedido por Cisco CallManager antes de enviarlo al gatekeeper para hacer que este diseño funcione para las llamadas que deben eliminarse localmente. Por ejemplo, Cisco CallManager puede anteponer 003 a las llamadas de un teléfono basado en Melbourne al número Pizza Hut 1-800. Esto permite al gatekeeper rutear la llamada a un gateway AARNet basado en Melbourne. La puerta de enlace elimina el 003 inicial antes de colocar la llamada en la PSTN.

- Utilice patrones de ruta con coincidencias específicas para todos los números domésticos para evitar que el usuario espere el tiempo de espera entre dígitos antes de que se inicie la llamada.

Esta tabla muestra los patrones de ruta para un Cisco CallManager controlado por gatekeeper:

Patrón de ruta	Descripción	Ruta	Gatekeeper
0.[2-9]XXXXXXX	Llamada local	Lista de rutas	AARNet
0.00	Llamada de emergencia	Gateway local	Ninguno
0.000	Llamada de emergencia	Gateway local	Ninguno
0.013	Asistencia de directorio	Gateway local	Ninguno
0.1223	—	Gateway local	Ninguno
0.0011!	Llamadas internacionales	Lista de rutas	AARNet
0.0011!#	Llamadas internacionales	Lista de rutas	AARNet
0,0[2-4]XXXXXXXX	Llamadas a Nueva Gales del Sur, Victoria y teléfonos móviles	Lista de rutas	AARNet
0,0[7-8]XXXXXXXX	Llamadas a Australia del Sur, Australia Occidental y Territorio del Norte	Lista de rutas	AARNet
0.1[8-9]XXXXXXXX	Llamadas al 1800 xxx xxx y al 1900 xxx xxx xxx	Gateway local	Ninguno
0,1144 X	Emergencia	Gateway	Ninguno

		local	
0,119[4-6]	Tiempo y tiempo	Gateway local	Ninguno
0.13[1-9]XXX	Llamadas a números 13xxxx	Gateway local	Ninguno
0,130XXXXXXX	Llamadas a los números 1300 xxx xxx xxx	Gateway local	Ninguno
[2-3]XXX	Llamadas a Signadou	Lista de rutas	ACU
5XXX	Llamadas a Aquinas	Lista de rutas	ACU
[7-9]XXX	Llamadas a McAuley, MacKillop y Monte Santa María	Lista de rutas	ACU

El gatekeeper enruta las llamadas internacionales, que no se envían a través del gateway local. Esto es significativo porque AARNet puede implementar gateways internacionales en el futuro. Si se implementa un gateway en los Estados Unidos, un simple cambio en la configuración del gatekeeper permite a las universidades realizar llamadas a los Estados Unidos a las tarifas domésticas estadounidenses.

El gatekeeper realiza el ruteo de llamadas entre clústers basado en la extensión ACU de 4 dígitos. Este espacio de dirección se superpone con toda probabilidad con otras universidades. Esto dicta que ACU administre su propio gatekeeper y utilice el gatekeeper AARNet como *gatekeeper de directorio*. La columna Gatekeeper de esta tabla indica si el gatekeeper ACU o el gatekeeper AARNet realizan el ruteo de llamadas.

Nota: La única salvedad con la solución de gatekeeper propuesta es que el dispositivo anónimo puede ser actualmente intercluster o H.225, pero no ambos al mismo tiempo. Cisco CallManager se basa en el gatekeeper para rutear las llamadas a las gateways (H.225) y a otros Cisco CallManagers (intercluster) con el diseño propuesto. La solución temporal para este problema es no utilizar el gatekeeper para el ruteo entre clústers o tratar todas las llamadas a través del gatekeeper como H.225. Esta última solución temporal significa que algunas funciones complementarias podrían no estar disponibles en llamadas entre clústeres.

Correo de voz

ACU tenía tres servidores de correo de voz basados en SO/2 de Active Voice Repartee con placas de teléfono dialógico antes de la migración a telefonía IP. El plan es reutilizar estos servidores en el entorno de telefonía IP. Cuando se implementa, cada servidor Repartee se conecta a Cisco CallManager mediante una interfaz de escritorio de mensajes (SMDI) simplificada y una tarjeta Catalyst 6000 24-Port Foreign Exchange Station (FXS). Esto proporciona correo de voz para tres de los seis campus, que deja tres campus sin correo de voz. No es posible compartir correctamente un servidor Repartee entre los usuarios en dos clústeres de Cisco CallManager porque no hay forma de propagar el indicador de mensaje en espera (MWI) en el

troncal H.323 del interclúster.

ACU podría comprar tres servidores Cisco Unity para los campus que quedan. Estos servidores se basan en Skinny, por lo que no se necesitan puertas de enlace. Esta tabla enumera las soluciones de correo de voz en caso de que ACU compre los servidores de correo de voz adicionales:

Campus	Sistema de buzón de voz	Gateway
Monte Saint Mary	Reparador de voz activo	FXS de 24 puertos Catalyst 6000
MacKillop	Reparador de voz activo	FXS de 24 puertos Catalyst 6000
Patrick	Reparador de voz activo	FXS de 24 puertos Catalyst 6000
Aquinas	Cisco Unity	—
Signadou	Cisco Unity	—
McAuley	Cisco Unity	—

Los seis servidores de correo de voz funcionan como islas aisladas de correo de voz en este plan. No hay red de correo de voz.

Recursos de medios

Los procesadores de señales digitales (DSP) de hardware no se implementan actualmente en ACU. La conferencia utiliza el puente de conferencia basado en software en Cisco CallManager. Actualmente no se admite la conferencia entre clústeres.

La transcodificación no es necesaria actualmente. Solo se utilizan los codificadores decodificadores G.711 y G.729, y todos los dispositivos finales implementados los admiten.

Soporte de fax y módem

La red de telefonía IP de ACU no admite actualmente el tráfico de fax y módem. La universidad planea utilizar la tarjeta FXS Catalyst 6000 de 24 puertos para este fin.

'Versiones de software'

Esta tabla enumera las versiones de software ACU utilizadas en el momento de esta publicación:

Platform	Función	Versión del software
CallManager	IP-PBX	3.0(10)
Catalyst 3500XL	Switch de distribución	12.0(5.1)XP
Catalyst 6500	Switch de núcleo	5.5(5)
Catalyst 1900	Switch de armario de cableado	—

Procesador Cisco 7200	router WAN	12.1(4)
Cisco 3640 router	gateway H.323	12.1(3a)XI6

Información Relacionada

- Soporte de tecnología de voz
- Soporte para productos de comunicaciones IP y por voz
- Troubleshooting de Cisco IP Telephony
- Soporte Técnico y Documentación - Cisco Systems