Caso práctico de instrumentación de telefonía IP: Australian Catholic University

Contenido

Introducción

El Academic y la red de investigación australianos (AARNet) es una red del IP de alta velocidad a escala nacional que interconecta 37 universidades australianas así como la organización de la científica de la Commonwealth y de investigación industrial (CSIRO).

El AARNet fue construido inicialmente como red de datos, pero ha llevado la voz sobre IP (VoIP) desde principios de 2000. La red VoIP desplegada actualmente es una solución del Toll Bypass que lleva las llamadas VoIP entre las universidades y las centrales telefónicas automáticas privadas CSIRO (PABX). También proporciona los gatewayes del Public Switched Telephone Network (PSTN) que permiten el PSTN al punto rentable del saltar a lo más. Por ejemplo, una llamada de un teléfono PABX en Melbourne a un teléfono PSTN en Sydney se lleva como VoIP de Melbourne al gateway PSTN Sydney. Allí está conectada con el PSTN.

El Australian Catholic University (ACU) es una de las universidades que conecta con el AARNet. En finales de 2000, el ACU comenzó un despliegue de la Telefonía IP que desplegó aproximadamente 2,000 Teléfonos IP a través de seis campus de la universidad.

Este caso práctico cubre el despliegue de la Telefonía IP ACU. Se completa el proyecto. Sin embargo, hay problemas arquitectónicos significativos a dirigir en la estructura básica AARNet si la red es escalar cuando otras universidades siguen en los pasos del ACU. Este documento describe estos problemas y propone y discute las diversas soluciones. El despliegue de la Telefonía IP ACU es probable ser ajustado más adelante para bajar conforme a la arquitectura recomendada final.

Nota: El La universidad de Deakin era la primera universidad australiana para desplegar la Telefonía IP. Sin embargo, el La universidad de Deakin no utiliza el AARNet para llevar el tráfico de la Telefonía IP.

AARNet

Las universidades australianas y el CSIRO construyeron el AARNet en 1990 con el Australian Vice-Chancellors' Committee (AVCC). El noventa y nueve por ciento de tráfico de Internet australiano estaba a los miembros fundadores durante los años iniciales. Un muy poco de tráfico comercial era de las organizaciones que tenían una asociación cercana con el sector terciario y de la investigación. Utilice por el userbase del NON-AARNet creciente al 20 por ciento del tráfico total en finales de 1994.

El AVCC vendió la base de cliente comercial del AARNet a Telstra en julio de 1995. Este evento spawn/generó cuál era eventual convertirse en Telstra BigPond. Esto crecimiento posterior estimulado del uso comercial y privado de Internet en Australia. La transferencia de la propiedad intelectual y de la experiencia dio lugar al desarrollo de Internet en Australia. Si no, esto no habría ocurrido a tal velocidad tan rápida.

El AVCC desarrolló AARNet2 a principios de 1997. Era otro refinamiento de Internet en Australia, que emplea los vínculos ATM y los servicios de Internet del ancho de banda alto bajo contrato con Cable & Wireless Optus (CWO) Limited. La instrumentación rápida de los Servicios IP por el CWO para cumplir los requisitos AARNet2 era debida en la parte a la transferencia del conocimiento y de la experiencia del AARNet.

ACU

El ACU es una universidad pública que fue establecida en 1991. La universidad tiene aproximadamente 10,000 estudiantes y el personal 1,000. Hay seis campus en la Costa Este de Australia. Esta tabla muestra los campus ACU y sus ubicaciones:

Campus	Ciudad	Estado
Santa María del soporte	Strathfield	Nuevo Gales del Sur (NSW)
MacKillop	Sydney del Norte	Nuevo Gales del Sur (NSW)
Patrick	Melbourne	Victoria (VIC)
Aquinas	Ballarat	Victoria (VIC)
Signadou	Canberra	Australia Capital Territory (ACTO)
McAuley	Brisbane	Queensland (QLD)

El ACU confió en la solución a Telstra Spectrum (Centrex) antes del rollout de la solución de telefonía IP que este caso práctico describe. El movimiento a la Telefonía IP fue conducido

principalmente por el deseo de reducir el coste.

CSIRO

El CSIRO tiene personal aproximadamente 6,500 en los sitios numerosos en Australia. El CSIRO conduce la investigación en las áreas tales como agricultura, minerales, energía, fabricación, comunicaciones, construcción, salud, y el entorno.

El CSIRO era la primera organización para utilizar el AARNet para el VoIP. La organización promovió el trabajo inicial hecho en esta área.

AARNet

La estructura básica AARNet es un componente importante en cualquier despliegue de la Telefonía IP de la universidad. Proporciona la interconexión de universidades con dos servicios principales en el área de la Voz:

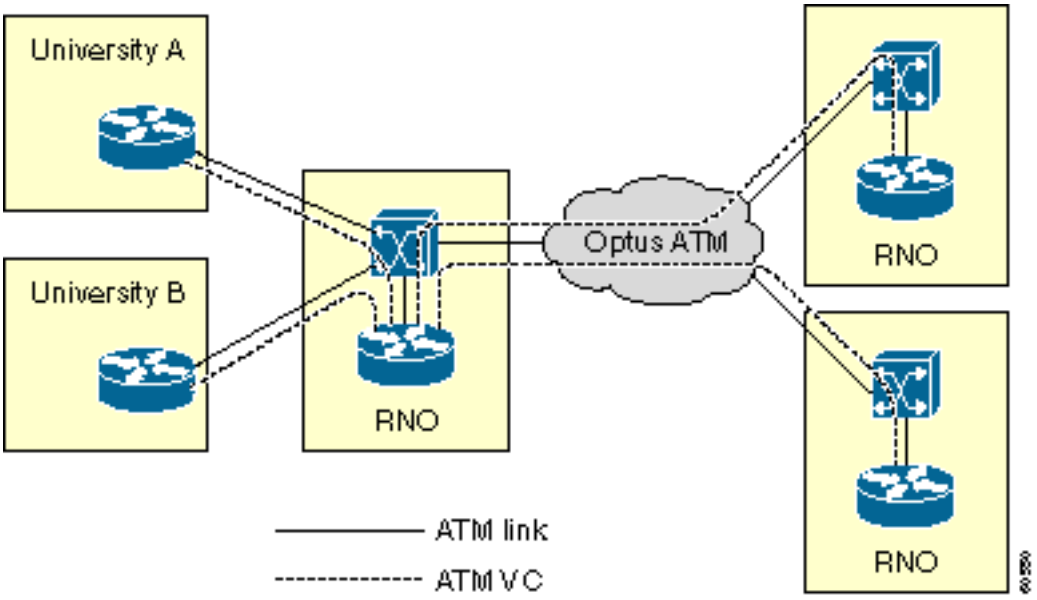
- Transporte de los paquetes en tiempo real del (RTP) del Transport Protocol VoIP con la garantía del Calidad de Servicio (QoS) apropiada expresar
- Punta barata del hopoff a los PSTN alrededor del país

Esta sección describe la arquitectura actual de AARNet y cómo entrega estos servicios. También delinea algunos de los problemas de ampliación que se presentan mientras que más universidades despliegan la solución de telefonía IP. Finalmente, discute las Soluciones posibles por estos problemas de ampliación.

Topología AARNet

El AARNet consiste en un solo POP (Point of Presence) en cada estado. Los estallidos se refieren como operaciones de la red regional (RNO). Las universidades conectan con el RNO en su estado respectivo. Los RNO a su vez son interconectados por una interconexión total del ATM PVC de Optus. Juntos constituyen el AARNet.

El RNO típico consiste en un switch ATM de Cisco LS1010 y un router conectado a ATM adjunto. El router RNO conecta con cada router de universidad por una sola atmósfera PVC a través de un link de microondas E3. Cada router RNO también tiene una interconexión total del ATM PVC que la red ATM de Optus proporcione al resto de los RNO. Este diagrama representa la topología de AARNet general de la red:



Hay excepciones múltiples a la topología. Algunas de ellas son significativas de una perspectiva de la Voz. Éstas son algunas excepciones:

- El RNO en las aplicaciones de Victoria IP clásica sobre la atmósfera (RFC 1577) en vez de los PVC de conectar las universidades con el RNO.
- Las universidades rurales conectan típicamente de nuevo al RNO por el Frame Relay o el ISDN.
- Algunas universidades grandes tienen más de un link de nuevo al RNO.

Esta tabla muestra los estados y los territorios que tienen actualmente un RNO. La tabla incluye a las Ciudades Capitales para los lectores que no son familiares con la geografía australiana.

Estado	Ciudad Capital	¿RNO?	Conexiones campus
Nuevo Gales del Sur	Sydney	Sí	TBD
Victoria	Melbourne	Sí	TBD
Queensland	Brisbane	Sí	TBD
Sur de Australia	Adelaide	Sí	TBD
Australia del oeste	Perth	Sí	TBD
Territorio capital de Australia	Canberra	Sí	TBD
Territorio del norte	Darwin	No	--
Tasmania	Hobart	No	--

Calidad del servicio

El AARNet de las partes de QoS-se habilita ya para la Voz como resultado del proyecto del Toll Bypass VoIP. QoS es necesario para el tráfico de voz para proporcionar estas características, que minimizan la fluctuación y retraso y eliminan la pérdida del paquete:

- Vigilancia — Marque abajo del tráfico de voz de las fuentes no confiables.
- Espera — La Voz se debe dar la prioridad sobre el resto del tráfico para minimizar el retardo durante la congestión de link.
- Link Fragmentation and Interleaving (LFI) — Los paquetes de datos se deben ser hechos fragmentos y los paquetes de voz interpolar en los links lentos.

El tráfico se debe clasificar para limpiar y para hacer cola correctamente los paquetes de voz. Esta sección describe cómo la clasificación se hace en el AARNet. Los Los capítulos subsiguientes describen el policing y la implementación de envío a cola.

Clasificación

No todo el tráfico consigue el mismo QoS. El tráfico se clasifica en estas categorías para proporcionar selectivamente QoS:

- Datos
- Voz de sabido y fuentes confiables
- Voz de las fuentes desconocidas

Solamente los dispositivos confiables se dan QoS de alta calidad en el AARNet. Estos dispositivos son principalmente gatewayes identificados por la dirección IP. Un Access Control List (ACL) se utiliza para identificar estas fuentes confiables de Voz.

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

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

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

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

```
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 una fuente no confiable se clasifica y se marca abajo de cuando el tráfico llega en una interfaz. Estos dos ejemplos muestran cómo la vigilancia se realiza dependiendo de qué tipo de tráfico se espera llegar en una interfaz dada:

El router busca los paquetes de voz no confiables y cambia su Prioridad IP a 0 si hay fuentes confiadas en de la Voz rio abajo.

```
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 Prioridad IP a 0 si no hay fuentes sabidas de la Voz rio abajo.

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

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

Datos en espera de la NON-Voz

Todo el VoIP en el AARNet era Toll Bypass hasta hace poco tiempo. Esta condición da lugar a relativamente pocos puntos finales de VoIP. El diseño de envío a cola actual distingue entre las interfaces que tienen dispositivos de VoIP rio abajo y las interfaces que no lo hacen. Esta sección discute el hacer cola en las interfaces NON-VoIP.

Una interfaz de la NON-Voz se configura para el Espera equitativa ponderada (WFQ) o el Weighted Random Early Detection (WRED). Éstos se pueden configurar directamente en la interfaz. Sin embargo, el Mecanismo para formar la cola es aplicado mediante una correspondencia de políticas para hacerla fácil cambiar el Mecanismo para formar la cola en un tipo de interfaz dada. Hay una correspondencia de políticas por el tipo de interfaz. Esto refleja el hecho de que no todos los Mecanismos para formar la cola están 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
```

Las correspondencias de políticas se asocian a las interfaces respectivas y son específicas a los tipos de interfaz. Por ejemplo, esto simplifica el proceso de cambiar el Mecanismo para formar la cola en los accesos de Ethernet (VIP basados) basados en el procesador de la Interfaz versátil del WRED al WFQ. Requiere un solo cambio en la correspondencia de políticas. Los cambios se realizan a todas las interfaces de Ethernet VIP basadas.

```
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 baja latencia

Cualquier interfaz que tenga dispositivos de VoIP rio abajo-de confianza se configura para el Low Latency Queuing (LLQ). Cualquier paquete que la haga con la clasificación de la interfaz entrante y conserva una precedencia de 5 está conforme al LLQ. Cualquier otro paquete está conforme al WFQ o al WRED. Esto depende del tipo de interfaz.

Las correspondencias de la política diferenciados se crean para cada tipo de interfaz para hacer QoS más fácil administrar. Esto es similar al diseño de envío a cola de la NON-Voz. Sin embargo, las correspondencias de las políticas múltiples existen para cada tipo de interfaz. Esto es porque la capacidad de los tipos de interfaz para llevar el tráfico de voz varía dependiendo de la velocidad del link, las configuraciones PVC, y así sucesivamente. El número en el nombre de correspondencia de políticas refleja el número de llamadas abasteció 30 llamadas, 60 llamadas, y así sucesivamente.

```
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
```

Las correspondencias de políticas se asocian a las interfaces respectivas. En este ejemplo, la correspondencia de políticas es específica a un tipo de interfaz. No se da actualmente ningún tratamiento especial a la señalización de voz. Las correspondencias de políticas se pueden enmendar fácilmente en un lugar si esto se convierte en un requisito ulteriormente en un tipo de interfaz dada. El cambio toma la influencia para 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
```

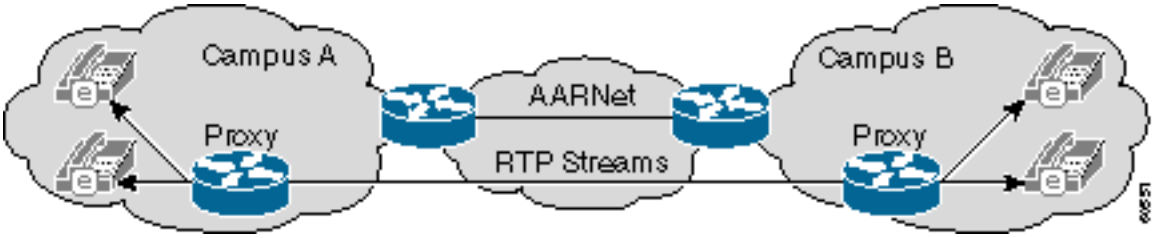
Escalabilidad LLQ

El Mecanismo para formar la cola tiene algunos problemas de ampliación. La cuestión principal es que confía en conocer la dirección IP de cada dispositivo de VoIP de confianza en la red. Esto era un impedimento razonable en el pasado en que había un número limitado de gatewayes de VoIP que manejaban el Toll Bypass. El número de puntos finales de VoIP aumenta dramáticamente, y llega a ser cada vez más poco práctico con el despliegue de la Telefonía IP. Los ACL llegan a ser demasiado largos y demasiado duros de manejar.

Los ACL se han añadido al final del fichero para confiar en el tráfico de un red secundario específico IP de la Voz en cada campus ACU en el caso del ACU. Esto es una solución interina. Se están investigando estas soluciones más a largo plazo:

- Proxy de H.323
- Vigilancia de calidad de servicio (Qos) de ingreso

La idea principal detrás de la solución proxy de H.323 es hacer que todo el tráfico RTP ingrese el AARNet de un campus dado mediante un proxy. El AARNet ve todo el tráfico RTP de un campus dado con una sola dirección IP, pues este diagrama muestra:

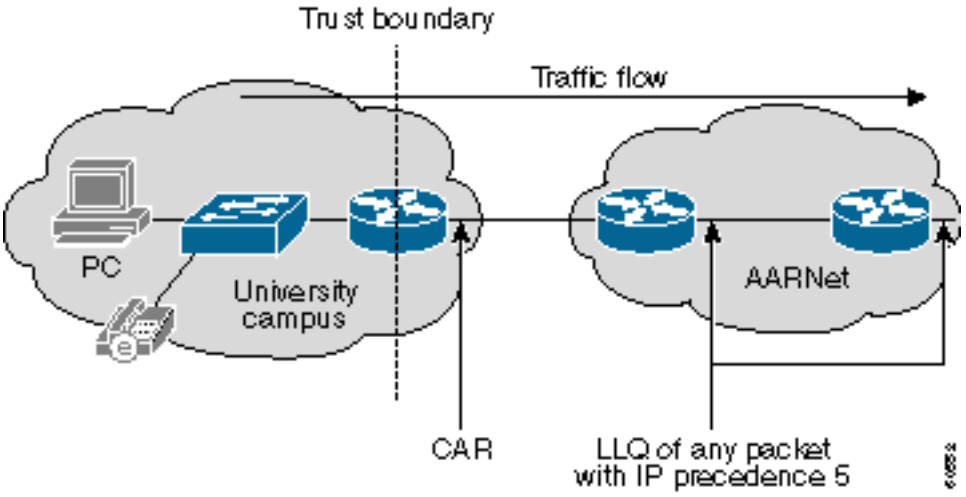


El número de entradas en el QoS ACL se limita a una línea por el campus si este esquema se despliega constantemente. Este esquema todavía tiene el potencial para agregar hasta 100 o más entradas puesto que hay 37 universidades con las oficinas centrales múltiples. Esto no es también scalable. Puede ser que sea necesario moverse a un diseño con un solo o al número limitado de estupendo-proxys compartidos en cada RNO. Esto reduce el número de IP Addresses de confianza a seis. Sin embargo, esto abre un problema de la Supervisión de QoS en la trayectoria del campus al proxy en el RNO.

Nota: Los troncos entre clústers del Cisco CallManager no funcionan actualmente con un proxy de H.323 porque la señalización entre clústers no es H.225 nativo.

La vigilancia de calidad de servicio (Qos) de ingreso es una solución alternativa. Un límite de confianza se establece en la punta donde el campus conecta con el RNO con este diseño. Trafique que ingresa el AARNet es limpiado por la característica del Committed Access Rate (CAR) de Cisco IOS® en este límite. Una universidad que utiliza el AARNet para el VoIP inscribe a una determinada cantidad ancho de banda de la Calidad de servicio (QoS) de AARNet. El CAR entonces monitorea el tráfico que ingresa el AARNet. El tráfico en exceso tiene Prioridad IP marcada abajo a 0 si la cantidad de tráfico RTP con la Prioridad IP 5 excede el ancho de banda inscrito.

Este diagrama muestra una configuración CAR:



Este ejemplo muestra cómo una configuración CAR dirige este policing:

```
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
```

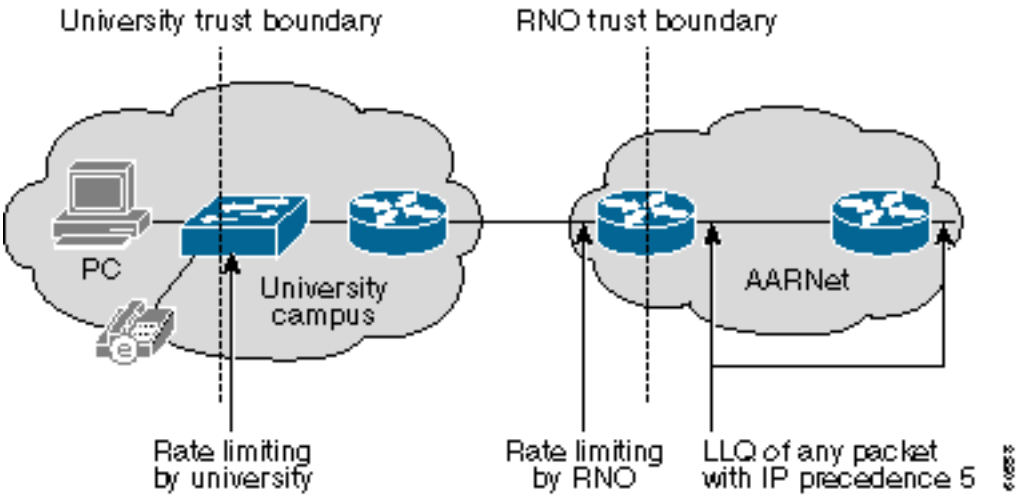
Éstas son algunas ventajas de un acercamiento de la configuración CAR:

- La base necesita no más dirigir el policing. Ahora se dirige en el límite de confianza. Por lo

tanto, el LLQ en la base no necesita saber sobre los IP Addresses de confianza. Cualquier paquete con una Prioridad IP de 5 en la base puede con seguridad estar conforme al LLQ porque ha pasado ya el policing en el ingreso.

- No se hace ningunas suposiciones sobre la arquitectura de VoIP, el equipo, y los protocolos que las universidades en particular eligen. Una universidad puede elegir desplegar un Session Initiation Protocol (SIP) o el Media Gateway Control Protocol (MGCP) que no trabaja con los proxys de H.323. Los paquetes de VoIP reciben el QoS apropiado en la base mientras tengan una Prioridad IP de 5.
- El CAR es resistente contra los ataques de la negación de servicio de QoS (DOS). Un ataque DOS de QoS que origina de una universidad no puede dañar la base. El CAR limita el ataque, que no puede generar más tráfico que cuál es presente cuando el número máximo de llamadas VoIP permitidas es activo.Las llamadas VoIP a o desde ese campus pueden sufrir durante un ataque. Sin embargo, está hasta la universidad en particular para protegerse internamente. La universidad puede apretar el CAR ACL en el router de modo que toda sino los redes secundarios seleccionados VoIP tenga la Prioridad IP marcada abajo.Cada campus tiene un límite de confianza interno en la punta donde los usuarios conectan con el LAN de oficina central en el último diseño. Trafique con una Prioridad IP de 5 que este límite de confianza reciba se limite a 160 dos de G.711 llamadas VoIP del kbps por el puerto del switch, o. El tráfico superior a esta tarifa se marca abajo. La implementación de este esquema requiere los Catalyst 6500 Switch o algo similares con la tarifa que limita las funciones.
- El aprovisionamiento del ancho de banda en la base simplifica mientras que cada universidad inscribe a una cantidad fija de ancho de banda de QoS. Esto también hace cargar en cuenta de QoS simple porque cada universidad puede pagar una tarifa mensual plana basada en una suscripción al ancho de banda de calidad de servicio (QoS).

La debilidad principal en este diseño es que el límite de confianza está situado en el router de universidad, así que las universidades deben poder administrar correctamente el CAR. El límite de confianza se tira nuevamente dentro del RNO. el equipo RNO-administrado dirige el policing en el último diseño. Este diseño requiere la tarifa basado en hardware que limita por ejemplo el Catalyst 6000 Switch o un procesador del Network Services Engine del Cisco 7200 (Cisco 7200 NSE-1). Sin embargo, da el control total del AARNet y RNO sobre la Supervisión de QoS. Este diagrama muestra este diseño:



Fragmentación de link e interpolación

El VoIP se está llevando solamente a través relativamente ATM de alta velocidad de los circuitos

virtuales (VCs). Por lo tanto, no se requiere ningún LFI. El VoIP se puede también transportar a través del foro de Frame Relay (FRF) o de las líneas arrendadas a las universidades rurales en el futuro. Esto requiere los mecanismos LFI tales como Multilink PPP (MLP) con la interpolación o el FRF.12.

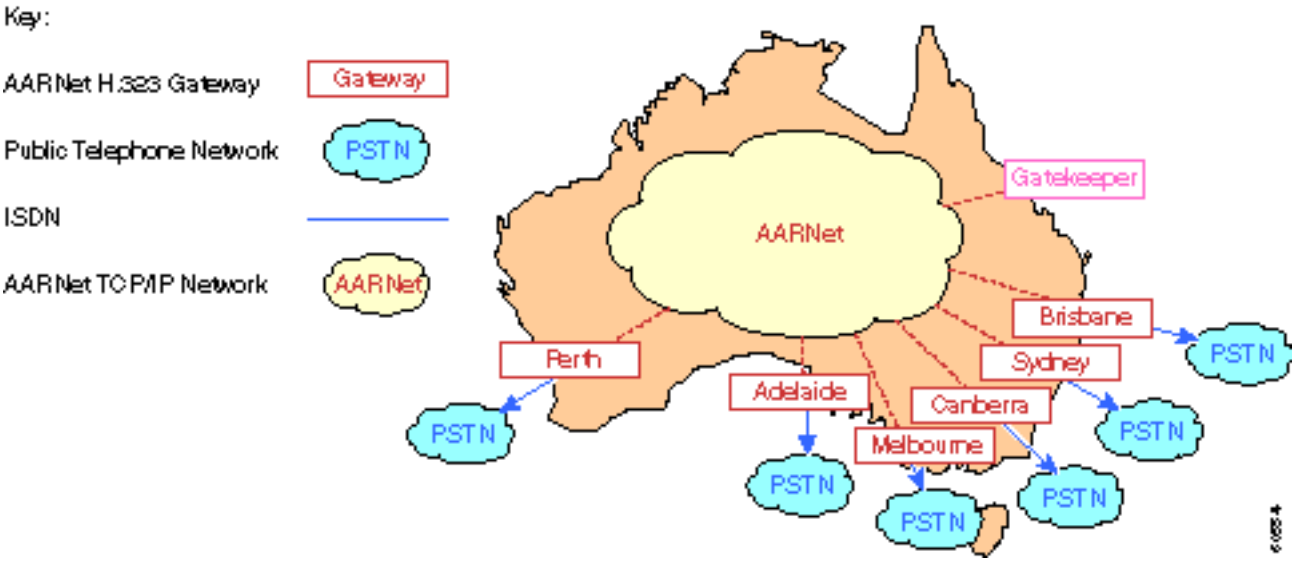
Gateways

Hay dos clases de Gateways H.323 en el AARNet:

- PSTN — PSTN al gateway de VoIP
- PABX — PABX al gateway de VoIP

La distinción entre un PSTN y un gateway de PABX es principalmente funcional. Los gatewayes PSTN proporcionan la Conectividad al PSTN. Los gatewayes de PABX conectan una universidad PABX con la estructura básica de VoIP. El mismo cuadro físico actúa como un PSTN y gateway de PABX en muchos casos. Hay actualmente 31 gatewayes en la solución de telefonía IP ACU. La mayor parte de estos gatewayes son Cisco AS5300 Universal Access Servers. Los otros gatewayes son Cisco 3600 Series Router o Cisco 2600 Series Router. Se espera que los gatewayes adicionales del mínimo de diez sean agregados durante el Q2CY01. El AARNet llevó aproximadamente 145,000 llamadas VoIP en abril de 2001.

El AARNet ha desplegado Gateways H.323 PSTN-asociado en la mayoría de las ciudades importantes, pues este diagrama muestra:



Las universidades pueden utilizar estos gatewayes para hacer las llamadas de salida al PSTN. Las universidades tienen que mantener sus propios trunks para las llamadas entrantes porque no se soportan actualmente. El AARNet puede negociar mismo un precio competitivo con el portador debido al volumen de llamadas que pasen a través de estos gatewayes. Las llamadas se pueden también caer a lo más del punto rentable. Por ejemplo, alguien en Sydney que llame un número de Perth puede utilizar el gateway de Perth y ser cargada solamente para una Llamada local. Esto también se conoce como saltar del fin de cola (TEHO).

Despliegan a un solo gatekeeper para realizar el E.164 a la resolución de la dirección IP. Todas las llamadas al PSTN se envían al portero, que entonces vuelve la dirección IP del gateway más apropiado. Refiera a las secciones de los Planes de marcado y del portero para información más detallada sobre los porteros.

Factura y estadísticas

Los gatewayes PSTN utilizan el RADIUS y el Authentication, Authorization, and Accounting (AAA) para los fines de facturación. Cada llamada a través de un gateway genera un registro de detalles de la llamada (CDR) para cada tramo de llamada. Estos CDR se fijan al servidor de RADIUS. La dirección IP del Cisco CallManager en el CDR identifica únicamente la universidad y se asegura de que el partido correcto está cargado en cuenta.

Seguridad de gateway

La protección de los gatewayes PSTN contra los ataques y el fraude DOS es una preocupación principal. Los clientes de H.323 están extensamente - disponibles. El NetMeeting de Microsoft se lía con el Microsoft Windows 2000, así que es relativamente fácil que un usuario no técnico ponga las llamadas libres a través de estos gatewayes. Configure un ACL entrante que permita que la señalización H.225 de los IP Addresses de confianza proteja estos gatewayes. Este acercamiento tiene aun así problemas de ampliación que la sección de QoS describa. El número de entradas en el ACL crece mientras que el número de puntos finales de confianza de H.323 crece.

Los proxys de H.323 ofrecen un cierto alivio en esta área. El ACLs del gateway necesita permitir una dirección IP por el campus de la universidad si todas las llamadas a través del paso del gateway PSTN con un Proxy campus. Dos IP Addresses como a proxy redundante son deseables en la mayoría de los casos. Incluso con los proxys, el ACL puede contener más de 100 entradas.

El proxy se debe proteger vía los ACL puesto que cualquier H.323 puede configurar una llamada con el proxy. El proxy ACL debe permitir los dispositivos locales de H.323 mientras que la política local requiere puesto que esto se hace sobre una base del por-campus.

Los IP Addresses de los dos Ciscos CallManageres se deben incluir en el ACLs del gateway si un campus quiere permitir que solamente las llamadas de los Teléfonos IP utilicen los gatewayes PSTN AARNet. Los proxys no agregan ningún valor en esta situación. El número de entradas ACL requeridas es dos cualquier manera.

Observe que las llamadas teléfono-a-IP IP del intercampus no necesitan pasar con el proxy.

Planes de marcado

El Plan de marcado actual VoIP es directo. Los usuarios pueden poner estos dos tipos de llamadas de una perspectiva del gateway de VoIP:

- Llame un teléfono en un diverso campus pero en la misma universidad.
- Llame un teléfono PSTN o un teléfono en una diversa universidad.

Los gateway dial peer reflejan el hecho de que hay solamente dos tipos de llamadas. Básicamente hay dos tipos del voip dial peer, pues este ejemplo muestra:

```
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
```

Utilizan al primer dial peer si alguien llama la extensión 7… en otro campus en este ejemplo. Esta llamada se rutea directamente a la dirección IP del gateway remoto. Puesto que desvían al portero, el control de admisión de llamadas (CAC) no se realiza.

Utilizan al segundo dial peer cuando la llamada está para un número PSTN. Éste puede ser cualquiera uno de estos elementos:

- El número de un teléfono en el PSTN
- El número calificado completamente PSTN de un teléfono en una diversa universidad

La llamada se envía al portero mediante un mensaje de petición de admisión (ARQ) en el primer caso. El portero vuelve la dirección IP del mejor gateway PSTN de un mensaje del Admission Confirm (ACF).

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

Gatekeeper

El AARNet actúa actualmente a un solo gatekeeper. El único propósito de este portero es realizar el ruteo de llamadas bajo la forma de E.164 a la resolución de la dirección IP. El portero no realiza el CAC. El número de trunks PABX conectó con los gatewayes limita el número de llamadas simultáneas. El ancho de banda de la base abastece todos los trunks funcionando inmediatamente. Esto cambia con el rollout de la Telefonía IP en el ACU y otras universidades. No hay límite natural en el número de llamadas VoIP simultáneas en las cuales pueda ser originado o fuera de un campus dado en este nuevo entorno. El ancho de banda de QoS disponible puede ser oversubscribed si se inician demasiadas llamadas. Todas las llamadas pueden sufrir de la baja calidad bajo esta condición. Utilice al portero para proporcionar el CAC.

La naturaleza distribuida y el tamaño potencial de la red de voz de la universidad se presta a una arquitectura del gatekeeper distribuida. Una Solución posible es tener un diseño del gatekeeper jerárquico de dos niveles en el cual cada universidad mantenga a su propio portero. Refieren a este gatekeeper de la universidad como portero de la grada 2. El AARNet actúa a un *gatekeeper de directorio* que se refiera como portero de la grada 1.

Las universidades deben utilizar este acercamiento de dos niveles para utilizar a un portero para el ruteo de llamadas entre los clústeres del Cisco CallManager. El portero rutea las llamadas basadas en 4 o una extensión 5-digit en este escenario. Cada universidad requiere a su propio portero. Esto es porque los rangos de internos solapan entre las universidades puesto que esto es un espacio de la dirección local-administrado.

Los porteros de la universidad de nivel 2 realizan el CAC para las llamadas a y desde esa universidad solamente. También realiza la resolución E.164 para las llamadas entre solamente los campus de esa universidad. La llamada es ruteada por el portero de la grada 2 al portero de la grada 1 mediante un mensaje del Location Request (LRQ) si alguien llama un teléfono del IP en otra universidad o llama el PSTN a través de un gateway de AARNet. El LRQ se remite al portero de la grada 2 de esa universidad si la llamada está para otra universidad. Este portero entonces devuelve un mensaje ACF al portero de la grada 2 en la universidad en donde la llamada origina. Ambos porteros de la grada 2 realizan el CAC. Proceden solamente con la llamada si hay ancho de banda suficiente disponible en ambos la llamada y las zonas llamadas.

El AARNet puede elegir tratar los gatewayes PSTN AARNet como los de cualquier universidad. Su propio portero de la grada 2 se ocupa los. El portero de la grada 1 puede también actuar como el portero de la grada 2 para estos gatewayes si la carga y el funcionamiento permiten.

Cada uno de los porteros (gatekeeper de directorio incluyendo del AARNet) necesita ser replicado

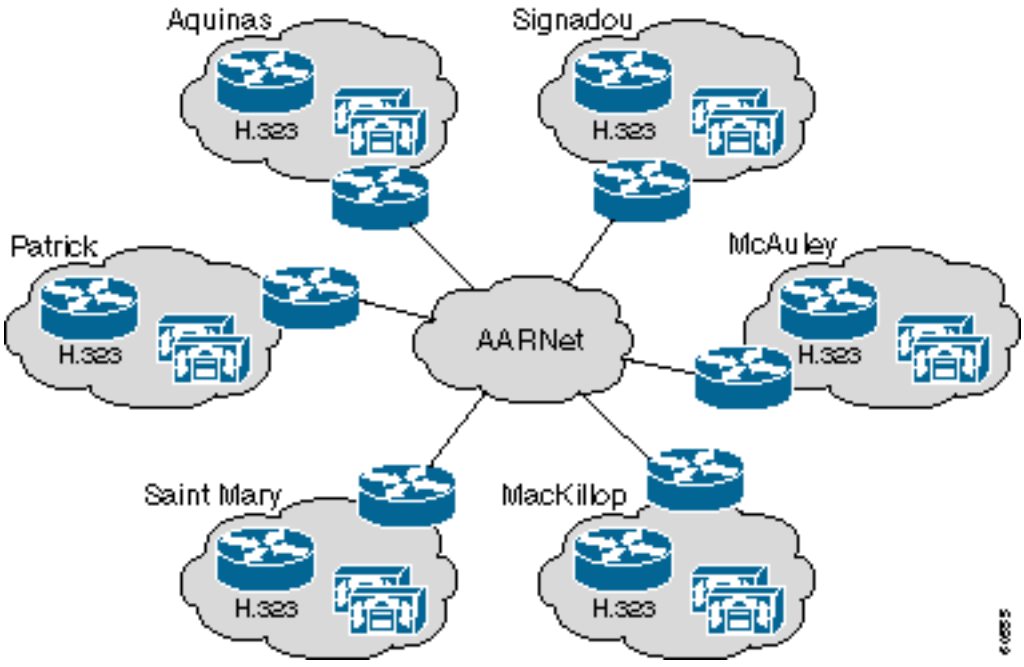
porque los gatewayes son tal componente crítico. Cada universidad necesita tener dos porteros. Es posible que los gatewayes del Cisco IOS tengan los gatekeeperes alternativos, como en el caso del Cisco IOS Software Release 12.0(7)T. Sin embargo, esto no es soportada actualmente por el Cisco CallManager o ningún otro dispositivo de tercera persona de H.323. No utilice esta característica ahora. Utilice una solución (HSRP-basada) basada en protocolos del router simple de la espera en caliente en lugar de otro. Esto requiere que ambos porteros se sienten en el mismo red secundario IP. El HSRP determina qué portero es activo.

Red de ACU IP Telephony

Esta tabla muestra el número aproximado de Teléfonos IP instalado en los campus del ACU:

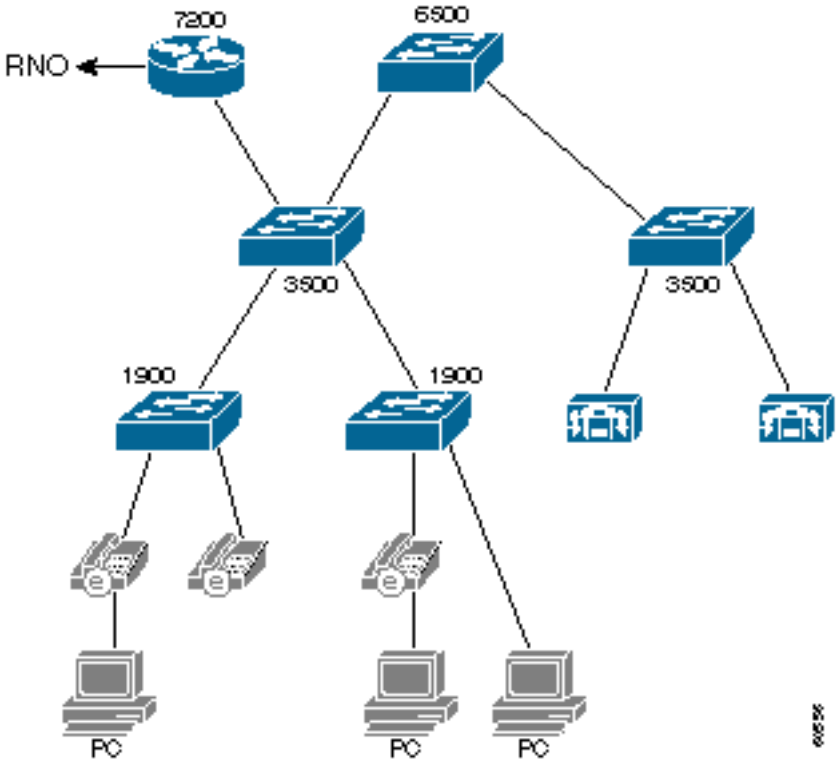
Campus	Ciudad	Teléfonos IP aproximados
Santa María del soporte	Strathfield	400
MacKillop	Sydney del Norte	300
Patrick	Melbourne	400
Aquinas	Ballarat	100
Signadou	Canberra	100
McAuley	Brisbane	400
	Total:	*1700*

El ACU desplegó recientemente una solución de telefonía IP. La solución consiste en un cluster de dos Ciscos CallManageres, de un gateway del Cisco 3640 en cada campus, y de los Teléfonos IP. El AARNet interconecta los campus. Este diagrama representa 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 tiene tres capas de switches de Catalyst. El Wiring Closet contiene los más viejos Catalyst 1900 Switch. Los Catalyst 1900 Switch conectan de nuevo al Catalyst 3500XL Switch mediante el Extended Framing. Éstos conectan de nuevo a un solo Catalyst 6509 Switch mediante el Gigabit Ethernet (GE). Un solo router del Cisco 7200VXR conecta el campus con el AARNet por un VC atmósfera con el RNO local.



El método de conectividad al RNO diferencia levemente del estado para estado, pues esta tabla muestra. Victoria se basa encendido IP clásica sobre la atmósfera (RFC 1577). Los otros RNO tienen un PVC recto puesto con la encapsulación del RFC 1483. El Open Shortest Path First (OSPF) es el Routing Protocol usado entre el ACU y los RNO.

Campus	Estado	Conectividad al RNO	Protocolo de ruteo
Santa María del soporte	NSW	RFC 1483 PVC	OSPF
MacKillop	NSW	RFC 1483 PVC	OSPF
Patrick	VIC	RFC 1577 IP clásica sobre la atmósfera	OSPF
Aquinas	VIC	RFC 1577 IP clásica sobre la atmósfera	OSPF
Signadou	ACTO	RFC 1483 PVC	OSPF
McAuley	QLD	RFC 1483 PVC	OSPF

El enlace del soporte de los Catalyst 1900 Series Switch en el uplinks solamente. Por lo tanto, los Teléfonos IP y los PC son todos en un VLA N grande. De hecho, el campus entero es un VLA N y dominio de broadcast grandes. Los redes secundarios secundarios IP se utilizan debido al número grande de dispositivos. Los Teléfonos IP están en un red secundario IP, y los PC están en otro. La base del AARNet confía en el red secundario del teléfono del IP, y el tráfico a y desde este red secundario IP está conforme al LLQ.

Las rutas del Cisco 7200 Router entre los redes secundarios primarios y secundarios IP. El

(MSFC) del Mutilayer Switch Feature Card en el Catalyst 6500 Switch no se utiliza actualmente.

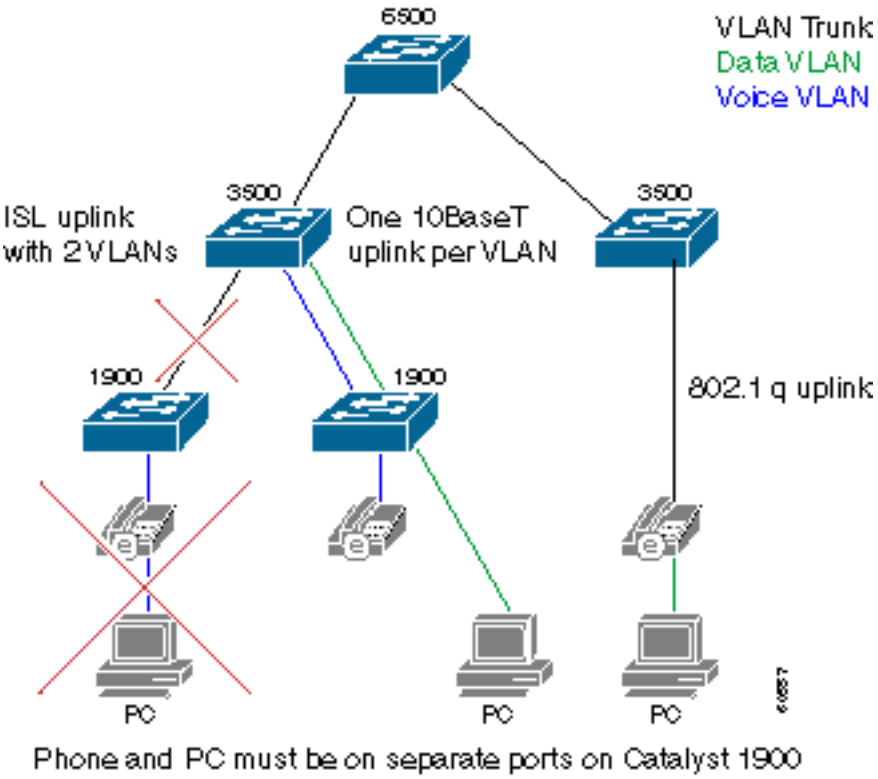
El Catalyst 3500XL y los Catalyst 6500 Switch tienen características de QoS, pero no se habilitan actualmente.

QoS (Calidad de servicio) en el Campus

El diseño para oficinas centrales actual no cumple con las pautas de diseño Cisco-recomendadas para la Telefonía IP. Éstas son algunas preocupaciones por QoS:

- El dominio de broadcast es muy grande. Los broadcastes excesivos pueden afectar al funcionamiento de los Teléfonos IP, que tienen que procesarlos.
- Los Catalyst 1900 Switch no son QoS-capaces. Si un teléfono del IP y un PC están conectados con el mismo puerto del switch, los paquetes de voz pueden ser caídos si el PC recibe los datos a una alta velocidad.

Partes del reajuste la infraestructura del campus para alcanzar las mejoras importantes. Una actualización de hardware no se requiere. Este diagrama ilustra los principios detrás del reajuste recomendado:



El campus se debe partir en un VLA N de la Voz y un VLAN de dato. Los teléfonos y los PC que conectan con un Catalyst 1900 Switch deben ahora conectar con diversos puertos para alcanzar la separación de VLAN. Un uplink adicional de cada Catalyst 1900 Switch al Cisco 3500XL Switch se agrega. Uno de los dos uplinks es un miembro del VLA N de la Voz. El otro uplink es un miembro del VLAN de dato. No utilice el enlace del InterSwitch Link (ISL) como alternativa a dos uplinks. Esto no proporciona el tráfico de voz y de datos con las colas aparte. Los links de GE del Catalyst 3500XL Switch al Catalyst 6000 Switch se deben también convertir a los trunks 802.1q para poder llevar Voz y el VLAN de dato a través de este switch del núcleo.

Los puertos en el Catalyst 3500XL Switch que están en el VLAN de dato tienen una clase predeterminada de (CoS) del servicio de cero. Los puertos que son miembros del VLA N de la Voz tienen CoS predeterminado de 5. como consecuencia, el tráfico de voz se dan prioridad

correctamente una vez que llega la base del Catalyst 3500 o del Catalyst 6500. Las configuraciones de puerto de switch de QoS del Catalyst 3500 varían levemente dependiendo de qué puerto del switch del VLA N es un miembro, pues este ejemplo muestra:

```
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
```

Usted puede conectarse un PC al puerto del switch posterior en el teléfono del IP en el caso poco probable que los Teléfonos IP conectan directamente con un Catalyst 3500XL Switch. Los Teléfonos IP conectan con el Switch mediante un tronco 802.1q en este caso. Esto permite que los paquetes de voz y datos viajen en los VLAN distintos, y usted puede dar a los paquetes CoS correcto en el ingreso. Substituya los Catalyst 1900 Switch por los Catalyst 3500XL Switch o el otro Switches QoS-capaz como alcanzan el fin de la vida útil. Esta topología entonces se convierte en el método estándar de conectar los Teléfonos IP y los PC con la red. Este escenario muestra la configuración de QoS del Catalyst 3500XL Switch:

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

Finalmente, los dos puertos que conectan con los dos Ciscos CallManageres deben tener el CoS codificado a 3. que el Cisco CallManager fija la Prioridad IP a 3 en todos los paquetes de la señalización de voz. Sin embargo, el link del Cisco CallManager al Catalyst 3500XL Switch no utiliza 801.1p. Por lo tanto, el valor de CoS es forzado en el Switch mientras que este ejemplo muestra:

```
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 dos puertos del switch están requeridos en el escritorio. El campus Patrick pudo requerir los puertos adicionales de un 400 Switch para 400 Teléfonos IP. Los Catalyst 3500XL Switch adicionales deben ser desplegados si los suficientes puertos no están disponibles. Solamente un puerto del Catalyst 3500XL Switch se requiere para cada dos puertos que falta del Catalyst 1900 Switch.

Los Catalyst 6500 Switch actuales ACU tienen capacidades de Calidad de servicio (QoS), pero no se habilitan actualmente. Estos módulos están presentes en el Catalyst 6000 Switch ACU con estas capacidades de colocación en cola:

Ranura	Módulo	Puertos	Colas de administración del tráfico RX	Colas de administración del tráfico 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 características apropiadas de QoS en el Catalyst 6000 Switch:

1. Diga el Switch proporcionar QoS sobre una base del por el VLAN con este comando:`Cat6K>(enable)`**`set port qos 1/1-2,3/1-8,4/1-8 vlan-based`**
2. Diga el Switch confiar en los valores de CoS recibidos del Catalyst 3500XL Switch con este comando:`Cat6K>(enable)`**`set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos`**

CoS se debe ahora fijar a asociar del Differentiated Services Code Point (DSCP). Se requiere esto porque el Catalyst 6000 Switch reescribe el valor DSCP en el encabezado IP basado en el valor recibido de CoS. Los paquetes de señalización de VoIP deben tener CoS de 3, reescrito con un DSCP de AF31 (26). Los paquetes RTP deben tener 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 mapeo 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 el MSFC para rutear entre los diversos redes secundarios IP.

QoS (Calidad de servicio) en RNO

El diseño actual RNO no cumple con las pautas de diseño Cisco-recomendadas para la Telefonía IP. Estas preocupaciones existen con respecto a QoS:

- El LLQ no se aplica en el router de WAN del Cisco ACU 7200 Series.
- Los campus del Patrick y de Aquinas conectan con el RNO mediante VCs conmutado atmósfera (SVC). El LLQ no se soporta en los SVC.

Un Cisco 7200 Router adjunto a Ethernet rápido conecta el campus con un RNO mediante un vínculo ATM del 34 Mbps E4. El tráfico puede potencialmente hacer cola para arriba saliente en los links de los 34M debido a los 4M contra la discrepancia de velocidad del 100M. Por lo tanto, es necesario dar prioridad al tráfico de voz. Utilice el LLQ. La configuración del Cisco 7200 Router 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 afectado un aparato al LLQ debe ser *N x 24Kbps*, donde está el número N de llamadas simultáneas de G.729.

Configure un PVC de cada uno del Patrick y de los Cisco 7200 Router de Aquinas al router AARNet. Las atmósferas SVC en Victoria RNO no soportan el LLQ, pues se basan encendido IP clásica sobre la atmósfera (RFC 1577). Las otras universidades en Victoria RNO pueden continuar utilizando el RFC 1577 por ahora. Sin embargo, substituya eventual IP clásica encima la infraestructura ATM.

Gateways

Cada uno de los campus ACU tiene un Cisco 3640 Router que actúe como gateway de H.323. Estos gateways conectan con el PSTN mediante el ISDN. El número de las interfaces de la velocidad primaria (PRI) y de Canales B depende del tamaño del campus. Esta tabla enumera el número de PRI y de Canales B para cada campus:

Campus	Cantidad PRI	Cantidad del Canal B
Santa María del soporte	2	30
MacKillop	2	50
Patrick	2	50
Aquinas	1	20
Signadou	1	20
McAuley	1	30

Estos gateways se utilizan solamente como gateways secundaria para DOD (Marcado directo saliente). Los gateways de AARNet son los gateways principales. Los gateways ACU se utilizan siempre para HICIERON (Direct Inward Dialing).

Plan de marcado

El Plan de marcado se basa en los números de interno de 4 dígitos. La extensión es también el últimos cuatro dígitos del numeró. Esta tabla enumera los rangos de internos e HIZO los números para cada campus:

Campus	Extensión	HIZO
Santa María del soporte	9xxx	02 9764 9xxx
MacKillop	8xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Aquinas	5xxx	03 5330 5xxx
Signadou	2xxx	02 6123 2xxx
McAuley	el 7xxx	07 3354 7xxx

`Un entrada Num-Exp` simple en los gateways trunca numeró a la extensión de 4 dígitos antes de que la pase encendido al Cisco CallManager. Por ejemplo, el gateway de campus Patrick tiene esta entrada:

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

Los usuarios marcan cero para seleccionar una línea exterior. Este cero al principio se pasa encendido al gateway. Un solo POTS dial peer rutea el decir en voz alta que el puerto ISDN basó en el cero al principio.

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

Las llamadas entrantes utilizan este entrada Num-Exp para transformar el número de la parte llamada a una extensión de 4 dígitos. La llamada entonces hace juego a ambos voip dial peer. De acuerdo con la preferencia menor, prefiere esta ruta al suscriptor del 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 cluster que consista en dos Cisco Callmanager servers. El Cisco Callmanager servers es una mezcla del Media Convergence Server 7835 (MCS-7835) y el Media Convergence Server 7820 (MCS-7820). Ambos servidores funcionaron con la versión 3.0(10) a la hora de esta publicación. Un Cisco CallManager es el *editor* y el otro Cisco CallManager es el *suscriptor*. El suscriptor actúa como el CallManager primario de Cisco para todos los Teléfonos IP. Esta tabla enumera el hardware desplegado en cada campus:

Campus	Plataforma	CallManageres
Santa María del soporte	MCS-7835	2
MacKillop	MCS-7835	2
Patrick	MCS-7835	2
Aquinas	MCS-7820	2
Signadou	MCS-7820	2
McAuley	MCS-7835	2

Cada cluster se configura con dos regiones:

- Uno para el intracampus llama (G.711)
- Uno para las llamadas entre campus (G.729)

El CAC basado en la ubicación no es apropiado para el ACU porque todos los Teléfonos IP servidos por cada cluster están en un solo campus. Hay méritos a un CAC portero-basado para las llamadas entre campus, pero esto no se implementa actualmente. Sin embargo, hay planes a hacer tan en un futuro próximo.

Cada Cisco CallManager se configura con 22 Gateways H.323. Esto se compone de los troncos entre clústers a los cinco otros clústeres del Cisco CallManager, a seis gatewayes PSTN AARNet, y a un gateway ACU en cada campus.

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

Utilizan las listas y a los Grupos de Routes de la ruta para alinear los gatewayes PSTN. Por ejemplo, esta tabla muestra cómo las llamadas del Cisco CallManager del Patrick en Melbourne a la Sydney PSTN pueden utilizar los cuatro gatewayes para atar las llamadas así como un Grupo de Routes.

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

Los Ciscos CallManageres se configuran con aproximadamente 30 patrones de ruta, pues esta tabla muestra. Diseñan a los patrones de ruta tan allí son coincidencias específicas para todos los números australianos nacionales. Esta manera, los usuarios no tiene que esperar el tiempo de espera entre dígitos para expirar antes de que el Cisco CallManager inicie la llamada. El carácter comodín “!” se utiliza solamente en el patrón de ruta para los números internacionales. Los usuarios deben esperar hasta que el tiempo de espera entre dígitos (valor por defecto 10 segundos) expire antes de los progresos de la llamada cuando marcan un destino internacional. Los usuarios pueden también agregar al patrón de ruta el "0.0011!#". Los usuarios pueden entonces ingresar “#” después de que el último pasado para indicar al Cisco CallManager que el Número marcado es completo. Esta acción apresura el Marcado internacional.

Patrón de ruta	Descripción
	Llamada local
0.00	Llamada de emergencia - si el usuario olvida marca 0 para la línea exterior
0.000	Llamada de emergencia
0.013	Asistencia para directorio
0.1223	
¡0.0011!	Llamadas internacionales
	Llama a Nuevo Gales del Sur
	Llama a Victoria
	Llama a los teléfonos celulares
	Llama a Queensland
	Llama a la Australia del oeste
	Llamadas al sur de Australia y al territorio del norte
	Llamadas a 1800 xxx del xxx y al xxx 1900 del xxx
0.1144X	Emergencia

0.119[4-6]	Tiempo y tiempo
0.1245X	Directorio
0.13[1-9]XXX	Llama a los números 13xxxx
	Llama a 1300 xxx del xxx los números
2[0-1]XX	Llamadas entre clústers a Signadou
3[0-4]XX	Llamadas entre clústers al Patrick
5[3-4]XX	Llamadas entre clústers a Aquinas
7[2-5]XX	Llamadas entre clústers a McAuley
8[0-3]XX	Llamadas entre clústers a MacKillop
9[3-4]XX	Llamadas entre clústers para montar a la Santa María
9[6-7]XX	Llamadas entre clústers para montar a la Santa María

El número de gatewayes, los Grupos de Routes, ruta enumera, y los patrones de ruta configurados en los Ciscos CallManageres ACU tienen el potencial para venir un número grande. Si se despliega un nuevo gateway RNO, los cinco clústeres del Cisco CallManager se deben configurar de nuevo con un gateway adicional. Incluso peor, los cientos de gateways necesitan ser agregados si los Ciscos CallManageres ACU rutean las llamadas VoIP directamente al resto de las universidades y desvían el PSTN en conjunto. Esto no escala claramente muy bien.

La solución es hacer el gatekeeper controlado de los Ciscos CallManageres. Usted debe poner al día solamente al portero cuando un nuevo gateway o Cisco CallManager se agrega en alguna parte en el AARNet. Cada Cisco CallManager debe tener solamente el gateway del campus local y el dispositivo anónimo configurados cuando sucede éste. Usted puede pensar en este dispositivo como trunk de la punta a de múltiples puntos. Quita la necesidad para los trunks enredados PPP en el modelo del Plan de marcado del Cisco CallManager. Un grupo de la solo ruta señala al dispositivo anónimo como gateway preferida y al gateway local como el gateway de backup. El gateway PSTN local es con certeza Llamadas locales usadas y también para las llamadas fuera de red generales si el portero hace inasequible. Actualmente, el dispositivo anónimo puede ser intercluster o H.225, pero no ambos al mismo tiempo.

El Cisco CallManager necesita a menos patrones de ruta con un portero que ahora tiene. En principio, el Cisco CallManager necesita solamente un modelo de la solo ruta de “!” el señalar al portero. En la realidad, la manera de la cual se rutean las llamadas necesita ser más específica por estas razones:

- Algunas llamadas (tales como llamadas a 1-800 o números de emergencia) necesitan ser ruteadas a través geográficamente de un gateway local. Alguien en Melbourne que marque la policía o una cadena de restaurantes tal como Pizza Hut no quiere ser conectada con la policía o Pizza Hut en Perth. Los patrones de ruta específicos son necesarios que punta directamente al gateway PSTN del campus local para estos números.Las universidades que planean realizar las implementaciones futuras de la Telefonía IP pueden elegir confiar solamente en los gatewayes de AARNet y no administrar sus propios gatewayes locales. Estos números deben tener un código de área virtual prepended por el Cisco CallManager antes de enviarlo al portero para hacer este trabajo del diseño para las llamadas que necesitan ser caídas apagado localmente. Por ejemplo, el Cisco CallManager puede prepend 003 a las llamadas de un teléfono Melbourne-basado al número de Pizza Hut 1-800. Esto permite que el portero rutee la llamada a un gateway de AARNet Melbourne-basado. El

gateway pela los 003 principales antes de que ponga la llamada en el PSTN.
- Utilice a los patrones de ruta con las coincidencias específicas para todos los números nacionales para evitar tener la espera del usuario para el tiempo de espera entre dígitos antes de que se inicie la llamada.

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

Patrón de ruta	Descripción	Rutear	Gatekeeper
	Llamada local	Lista de la ruta	AARNet
0.00	Llamada de emergencia	Gateway local	Ninguno
0.000	Llamada de emergencia	Gateway local	Ninguno
0.013	Asistencia para directorio	Gateway local	Ninguno
0.1223		Gateway local	Ninguno
¡0.0011!	Llamadas internacionales	Lista de la ruta	AARNet
0.0011!#	Llamadas internacionales	Lista de la ruta	AARNet
	Llama a Nuevo Gales del Sur, a Victoria, y a los teléfonos celulares	Lista de la ruta	AARNet
	Llama al sur de Australia, a la Australia del oeste, y al territorio del norte	Lista de la ruta	AARNet
	Llamadas a 1800 xxx del xxx y al xxx 1900 del xxx	Gateway local	Ninguno
0.1144X	Emergencia	Gateway local	Ninguno
0.119[4-6]	Tiempo y tiempo	Gateway local	Ninguno
0.13[1-9]XXX	Llama a los números 13xxxx	Gateway local	Ninguno
	Llama a 1300 xxx del xxx los números	Gateway local	Ninguno
[2-3]XXX	Llama a Signadou	Lista de la ruta	ACU
5XXX	Llama a Aquinas	Lista de la	ACU

		ruta	
[7-9]XXX	Llama a McAuley, a MacKillop, y a la Santa María del soporte	Lista de la ruta	ACU

El portero rutea las llamadas internacionales, que no se envían a través del gateway local. Esto es significativo porque el AARNet puede desplegar los gatewayes internacionales en el futuro. Si un gateway se despliega en los Estados Unidos, un cambio de configuración de control de acceso simple permite que las universidades pongan las llamadas a los E.E.U.U. a las tarifas nacionales E.E.U.U.

El portero realiza la encaminamiento de la llamada entre clústers basada en la extensión ACU de 4 dígitos. Este espacio de la dirección solapa muy probablemente con otras universidades. Esto dicta que el ACU administra a su propio portero y utiliza al gatekeeper AARNet como *gatekeeper de directorio*. La columna de gatekeeper en esta tabla indica si el ruteo de llamadas es realizado por el gatekeeper ACU o el gatekeeper AARNet.

Nota: La advertencia única con la solución propuesta del portero es que el dispositivo anónimo pueda actualmente ser intercluster o H.225, pero no ambos al mismo tiempo. El Cisco CallManager confía en el portero para rutear las llamadas a ambos gatewayes (H.225) y a otros Ciscos CallManageres (intercluster) con el diseño propuesto. La solución alternativa para este problema es no al uso el portero para el ruteo entre clústers o tratar todas las llamadas vía el portero como H.225. La última solución alternativa significa que algunas características suplementarias pudieron ser inasequibles en las llamadas entre clústers.

Correo de voz

El ACU tenía tres servidores de correo de voz de la grabación de conversaciones de voz activa OS/2-based con las tarjetas dialogales del teléfono antes de la migración a la Telefonía IP. El plan es reutilizar estos servidores en entorno de telefonía IP. Cuando está implementado, cada servidor para la grabación de conversaciones conecta con un Cisco CallManager mediante un Simplified Message Desk Interface (SMDI) y un indicador luminoso LED amarillo de la placa muestra gravedad menor de la Estación de intercambio remota (FXS) 24-Port del Catalyst 6000. Esto proporciona el correo de voz para tres de los seis campus, que sale de tres campus sin el correo de voz. No es posible compartir correctamente a un servidor para la grabación de conversaciones entre los usuarios en dos clústeres del Cisco CallManager porque no hay manera de propagar el indicador de mensaje en espera (MWI) a través del trunk de H.323 del intercluster.

El ACU pudo comprar tres servidores del Cisco Unity para los campus que permanecen. Estos servidores son Flaco basados, así que no se requiere ningunos gatewayes. Esta tabla enumera las soluciones del correo de voz en caso que el ACU compre a los servidores de correo de voz adicionales:

Campus	Sistema de correo de voz	Gateway
Santa María del soporte	Grabación de conversaciones de voz activa	Catalyst 6000 24-port FXS
MacKillop	Grabación de conversaciones de voz activa	Catalyst 6000 24-port FXS
Patrick	Grabación de	Catalyst 6000

	conversaciones de voz activa	24-port FXS
Aquinas	Cisco Unity	
Signadou	Cisco Unity	
McAuley	Cisco Unity	

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

Recursos de medios

Los procesadores de señales digitales del hardware (DSPs) no se despliegan actualmente en el ACU. La Conferencia utiliza el Bridge de conferencia basado en software en el Cisco CallManager. La Conferencia entre clústers no se soporta actualmente.

La transcodificación no se requiere actualmente. Se utilizan los decodificadores del codificador solamente de G.711 y de G.729, y son soportados por todos los dispositivos extremos desplegados.

Soporte de fax y módem

El fax y el tráfico del módem no es soportado actualmente por la red de telefonía IP ACU. Los planes de la universidad para utilizar el para este propósito del indicador luminoso LED amarillo de la placa muestra gravedad menor del Catalyst 6000 24-Port FXS.

'Versiones de software'

Esta tabla enumera las versiones de software ACU usadas a la hora de esta publicación:

Plataforma	Función	Versión del software
CallManager	IP-PBX	3.0(10)
Catalyst 3500XL	Switch de distribución	12.0(5.1)XP
Catalyst 6500	Switch del núcleo	5.5(5)
Catalyst 1900	Switch del Wiring Closet	
Procesador del Cisco 7200	Router de WAN	12.1(4)
Cisco 3640 Router	Gateway de 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