Implementatie van IP-telefonie voor casestudy-studies - ACU

Inhoud

Inleiding

Het Australische Academisch en onderzoeksnetwerk (AARNet) is een nationaal hogesnelheidsnetwerk dat 37 Australische universiteiten onderling verbindt, evenals de Commonwealth Scientific and Industrial Research Organisation (CSIRO).

AARNet werd aanvankelijk gebouwd als een gegevensnetwerk, maar heeft Voice-over-IP (VoIP) sinds begin 2000 overgedragen. Het VoIP-netwerk dat momenteel wordt ingezet, is een omzeilende oplossing waarmee VoIP-gesprekken tussen universiteiten en de CSIRO privé-filiaalbeurzen (PABX's) mogelijk worden gemaakt. Het voorziet ook in openbare PSTN-gateways (telefoonnetwerk) die PSTN in staat stellen op het meest kosteneffectieve punt uit te stappen. Zo wordt een telefoontje van een PABX-telefoon in Melbourne naar een PSTN-telefoon in Sydney bijvoorbeeld vervoerd als VoIP van Melbourne naar de Sydney PSTN-poort. Het is daar verbonden met het PSTN.

De Australische Katholieke Universiteit (ACU) is een van de universiteiten die verbonden is met AARNet. Eind 2000 startte ACU een uitrol van IP-telefonie die ongeveer 2.000 IP-telefoons over zes universiteitscampussen uitzette.

Deze casestudy bestrijkt de implementatie van ACU IP-telefonie. Het project is voltooid. In de AARNet-backbone moeten echter belangrijke architectonische kwesties worden aangepakt als het netwerk moet schaalbaar zijn wanneer andere universiteiten in de voetsporen van ACU treden. In dit document worden deze kwesties beschreven en worden verschillende oplossingen voorgesteld en besproken. De plaatsing van de ACU IP-telefonie zal waarschijnlijk later worden aangepast om in lijn met de laatste aanbevolen architectuur te vallen.

Opmerking: Deakin University was de eerste Australische universiteit die IP-telefonie implementeerde. De universiteit van Deakin gebruikt AARNet echter niet om IP-telefonieverkeer te transporteren.

AARNet

De Australische universiteiten en CSIRO bouwden AARNet in 1990 op door middel van het Comité van vice-kanseliers van Australië (AVCC). In de eerste jaren werd 99 procent van het Australische internetverkeer naar de oprichters gebracht. Een kleine hoeveelheid commercieel verkeer kwam van organisaties die nauw verbonden waren met de tertiaire en onderzoekssector. Het gebruik door niet-luchtvaartgebonden gebruikers is eind 1994 toegenomen tot 20 procent van het totale verkeer.

In juli 1995 verkocht de AVCC de commerciële klantenbasis van AARNet aan Telstra. Deze gebeurtenis schiep wat uiteindelijk Telstra BigPond zou worden. Dit stimuleerde een verdere groei van het commerciële en particuliere gebruik van internet in Australië. De overdracht van intellectuele eigendom en expertise resulteerde in de ontwikkeling van het internet in Australië. Anders zou dit niet zo snel zijn gegaan.

De AVCC ontwikkelde AARNet2 begin 1997. Het was een verdere verfijning van het internet in Australië, dat grote bandbreedte heeft voor ATM-verbindingen en internetdiensten in het kader van een contract met Cable & Wireless Optus (CWO) Limited. De snelle inzet van IP-diensten door CWO om aan de eisen van AARNet2 te voldoen, was gedeeltelijk te danken aan de overdracht van kennis en expertise van AARNet.

ACU

ACU is een openbare universiteit die in 1991 werd opgericht. De universiteit heeft ongeveer 10.000 studenten en 1.000 medewerkers. Er zijn zes campussen aan de oostkust van Australië. In deze tabel worden de ACU-campussen en hun locaties getoond:

Campus	Stad	Staat
Mount Saint Mary	Strathfield	Nieuw-Zuid-Wales (NSW)
MacKillop	Noord Sydney	Nieuw-Zuid-Wales (NSW)
Patrick	Melbourne	Victoria (VIC)
Achinas	Ballarat	Victoria (VIC)
Signadou	Canberra	Australië - Kapitaalgebied (ACT)
McAuley	Brisbane	Queensland (QLD)

ACU was afhankelijk van een Telstra Spectrum (Centrex) oplossing vóór de uitrol van de oplossing van de IP Telephony die deze casestudy beschrijft. De stap naar IP-telefonie was voornamelijk het gevolg van de wens de kosten te verlagen.

CSIRO

CSIRO heeft ongeveer 6.500 medewerkers op talloze locaties in Australië. CSIRO voert onderzoek uit op gebieden zoals landbouw, mineralen, energie, productie, communicatie, bouw, gezondheid en het milieu.

CSIRO was de eerste organisatie die AARNet voor VoIP gebruikte. De organisatie was de eerste stap in het werk dat op dit gebied werd verricht.

AARNet

De backbone van AARNet is een belangrijk onderdeel in elke installatie van IP-telefonie op de universiteit. Het voorziet in de koppeling van universiteiten met twee belangrijke diensten op het gebied van spraaktelefonie:

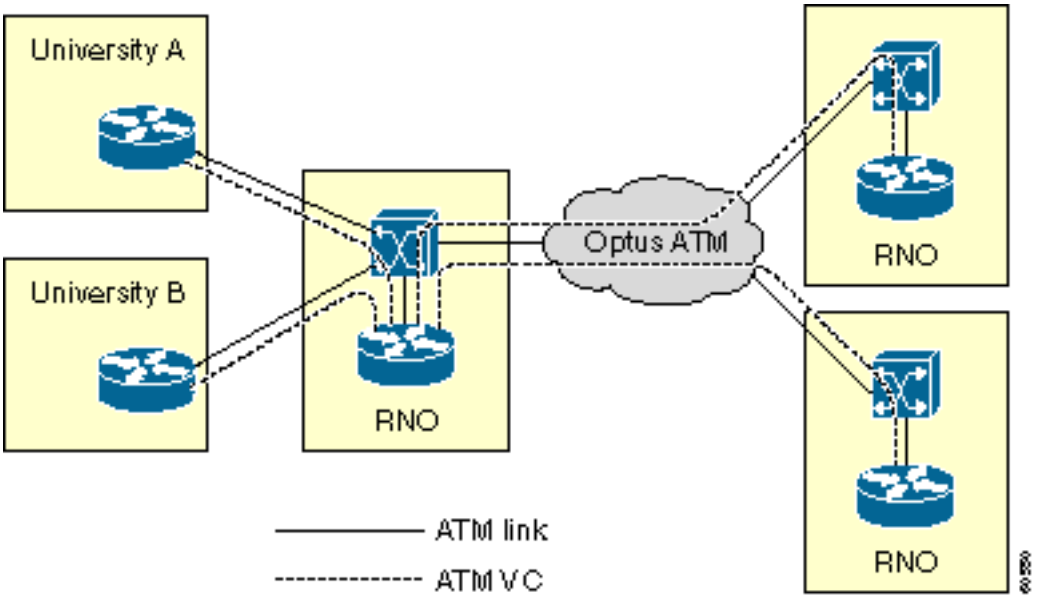
- Transport van VoIP Realtime Transport Protocol (RTP)-pakketten met de garantie van Quality of Service (QoS) geschikt voor spraak
- Lage kosten springen in de richting van de PSTN's in het hele land

In dit deel wordt de huidige AARNet - architectuur beschreven en beschreven hoe deze diensten worden geleverd. Het schetst ook een paar van de schaalbaarheidskwesties die zich voordoen als meer universiteiten de oplossing voor IP-telefonie implementeren. Tenslotte worden de mogelijke oplossingen voor deze schaalbaarheidskwesties besproken.

AARNet-topologie

AARNet bestaat uit één POP (presentiepunt) in elke staat. De POP's worden regionale netwerkoperaties genoemd. Universiteiten verbinden zich met de RNO in hun respectievelijke staat. De RNOs zijn op hun beurt onderling verbonden door een volledige maaswijdte van Optus ATM PVCs. Samen vormen ze AARNet.

Het typische RNO bestaat uit één Cisco LS1010 ATM-switch en één ATM-verbonden router. De RNO-router sluit zich aan op elke universiteitsrouter door één ATM PVC via een E3-microgolflengte. Elke RNO-router heeft ook een volledig netwerk van ATM PVC’s dat het Optus ATM-netwerk aan alle andere RNO’s biedt. Dit diagram vertegenwoordigt de algemene AARNet topologie van het netwerk:



Er zijn talrijke uitzonderingen op de topologie. Sommige zijn belangrijk vanuit een spraakperspectief. Dit zijn een paar uitzonderingen:

- RNO in Victoria gebruikt klassieke IP over ATM (RFC 1577) in plaats van PVC's om de universiteiten aan de RNO te verbinden.
- Plattelandsuniversiteiten verbinden zich normaal gesproken terug met RNO door Frame Relay of ISDN.
- Sommige grote universiteiten hebben meer dan één link terug naar de RNO.

Deze tabel laat de staten en gebieden zien die momenteel een RNO hebben. De tabel bevat kapitaalsteden voor lezers die niet bekend zijn met de geografie van Australië.

Staat	Hoofdstad	RNO?	Campus-verbindingen
Nieuw-Zuid-Wales	Sydney	Ja	TBD
Victoria	Melbourne	Ja	TBD
Queensland	Brisbane	Ja	TBD
Zuid-Australië	Adelaide	Ja	TBD
West-Australië	Perth	Ja	TBD
Australische kapitaalgebieden	Canberra	Ja	TBD
Noordelijk Gebied	Darwin	Nee	—
Tasmanie	Hobart	Nee	—

Quality-of-Service

De delen van AARNet zijn al QoS-enabled voor spraak als resultaat van het VoIP tolomweg-project. QoS is nodig voor spraakverkeer om deze functies te kunnen bieden, waardoor vertragingen worden geminimaliseerd en pakketverlies wordt voorkomen:

- Toezicht-Mark op spraakverkeer van niet-vertrouwde bronnen.

- Wachtrij-spraak moet voorrang hebben op al het andere verkeer om vertraging tijdens verbindingscongestie te minimaliseren.
- Link Fragmentation and Interleaving (LFI) - Data-pakketten moeten worden gefragmenteerd en spraakpakketten worden onderbroken op langzame koppelingen.

Het verkeer moet worden geclassificeerd naar de juiste politie- en rijstempakketten. In dit deel wordt beschreven hoe de classificatie op AARNet wordt uitgevoerd. De volgende hoofdstukken beschrijven de implementatie van het toezicht en de wachtrij.

Classificatie

Niet alle verkeer krijgt dezelfde QoS. Het verkeer wordt in deze categorieën ingedeeld om selectief QoS te verstrekken:

- Gegevens
- Voice-over-bekende bronnen
- Spraak via onbekende bronnen

Alleen vertrouwde apparaten krijgen QoS van hoge kwaliteit op AARNet. Deze apparaten zijn voornamelijk gateways die geïdentificeerd zijn door IP-adres. Een toegangscontrolelijst (ACL) wordt gebruikt om deze vertrouwde bronnen van spraak te identificeren.

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

IP voorrang wordt gebruikt om spraakverkeer van gegevensverkeer te onderscheiden. Voice heeft een IP-voorrang van 5.

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

Combineer de vorige voorbeelden om pakketten van een vertrouwde bron te identificeren.

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

Gebruik de zelfde beginselen om spraakpakketten van een onbekende bron te identificeren.

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

Toezicht

Spraakverkeer vanaf een niet-vertrouwde bron wordt geclassificeerd en gemarkeerd als het verkeer op een interface aankomt. Deze twee voorbeelden laten zien hoe de controle wordt uitgevoerd afhankelijk van welk type verkeer op een gegeven interface zal aankomen:

De router kijkt naar onvertrouwde spraakpakketten en verandert hun IP voorrang in 0 als er stroomafwaarts vertrouwde spraakbronnen zijn.

```
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
```

De router kijkt naar alle spraakpakketten en verandert hun IP voorrang in 0 als er geen bekende spraakbronnen stroomafwaarts zijn.

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

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

Wachtrij zonder spraak

Alle VoIP in AARNet was tot voor kort omzeilen van tol. Deze voorwaarde resulteert in relatief weinig VoIP-eindpunten. Het huidige ontwerp van de wachtrij maakt onderscheid tussen interfaces die VoIP-apparaten stroomafwaarts hebben en interfaces die dat niet doen. In dit gedeelte worden wachtrijen op niet-VoIP-interfaces besproken.

Een niet-Voice-interface is geconfigureerd voor ofwel gewogen fair lange wachtrijen (WFQ) of Weighted Random Early Detection (WRED). Deze kunnen rechtstreeks op de interface worden ingesteld. Het wachtrijmechanisme wordt echter toegepast door middel van een beleidskaart om het voor een bepaald interfacetype gemakkelijk te maken het wachtrijmechanisme te wijzigen. Er is één beleidskaart per interfacetype. Dit weerspiegelt het feit dat niet alle wachtrijen mechanismen op alle interfaces worden ondersteund.

```
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
```

De beleidskaarten zijn aan de respectieve interfaces gehecht en zijn specifiek voor interfacetypen. Dit vereenvoudigt bijvoorbeeld het proces om het wachtend mechanisme te veranderen op veelzijdige Ethernet-poorten (op VIP gebaseerd) van WRED naar WFQ. Het vereist één enkele

verandering in de beleidsplanning. De wijzigingen worden aangebracht in alle op VIP gebaseerde Ethernet-interfaces.

```
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
```

Low Latency Queuing

Elke interface met downstream-vertrouwde VoIP-apparaten is ingesteld voor Low Latency Queuing (LLQ). Elk pakket dat het door de inkomende interfaceklasse maakt en een voorrang van 5 behoudt is aan LLQ onderworpen. Elk ander pakket is aan WFQ of WRED onderworpen. Dit is afhankelijk van het interfacetype.

Voor elk interfacetype worden afzonderlijke beleidskaarten gecreëerd om het beheer van QoS te vergemakkelijken. Dit is gelijk aan het ontwerp van de wachtrij voor een andere stem. Er bestaan echter voor elk interfacetype meerdere beleidskaarten. Dit komt doordat de capaciteit van de interfacetypen voor het transporteren van spraakverkeer afhankelijk is van de snelheid van de link, PVC-instellingen enzovoort. Het nummer in de beleidskaartnaam weerspiegelt het aantal oproepen dat voor 30 oproepen, 60 oproepen, enzovoort is geprogrammeerd.

```
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
```

De beleidskaarten zijn aan de respectieve interfaces gehecht. In dit voorbeeld is de beleidskaart specifiek voor een interfacetype. Momenteel wordt geen speciale behandeling gegeven aan spraaksignalering. De beleidskaarten kunnen gemakkelijk op één plaats worden gewijzigd, als dit in een later stadium op een bepaald interfacetype een vereiste wordt. De verandering heeft invloed op alle interfaces van dat type.

```
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
```

LLQ-schaalbaarheid

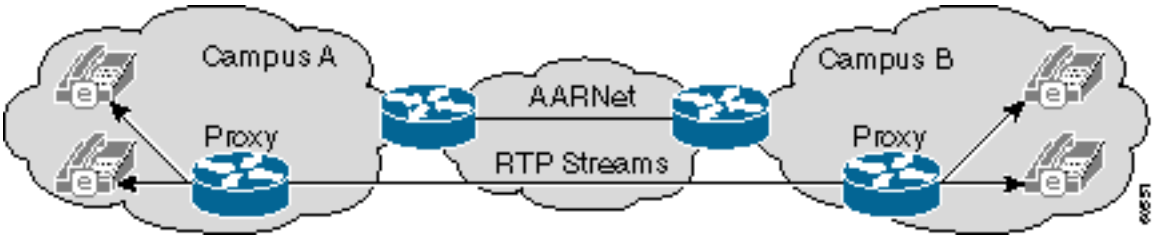
Het Wachtend mechanisme heeft een aantal schaalbaarheidsproblemen. Het belangrijkste probleem is dat het afhankelijk is van het weten van het IP-adres van elk vertrouwd VoIP-apparaat in het netwerk. Dit was een redelijke beperking in het verleden, toen er een beperkt aantal VoIP-gateways was die tolomweg hielden. Het aantal VoIP-endpoints wordt dramatisch verhoogd, en het wordt steeds onpraktisch bij de implementatie van IP-telefonie. De ACL's worden te lang en te moeilijk te beheren.

ACL’s zijn toegevoegd om verkeer te vertrouwen vanaf een specifiek IP-subnetwerk op elke ACU-campus in het geval van ACU. Dit is een tussenoplossing. Deze langetermijnoplossingen worden onderzocht:

- H.323-proxy
- Toezicht QoS-toegangscontrole

Het belangrijkste idee achter de H.323-proxy-oplossing is om alle RTP-verkeer vanaf een

bepaalde campus via een proxy naar AARNet te laten vliegen. AARNet ziet al RTP verkeer van een bepaalde campus met één enkel IP adres, zoals dit diagram toont:

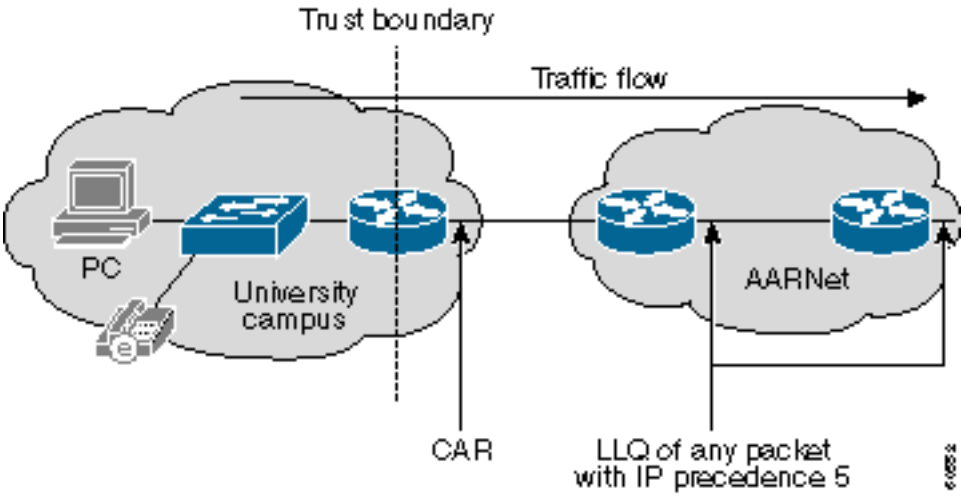


Het aantal lemma's in QoS ACL's is beperkt tot één lijn per campus als dit schema consequent wordt toegepast. Deze regeling heeft nog steeds de mogelijkheid om 100 of meer inzendingen op te tellen, aangezien er 37 universiteiten zijn met meerdere campussen. Ook dit is niet schaalbaar. Het kan nodig zijn om bij elke RNO over te stappen op een ontwerp met één of een beperkt aantal gedeelde superproxy's. Dit beperkt het aantal vertrouwde IP-adressen tot zes. Dit opent echter een QoS-politieprobleem op het pad van de campus naar de proxy bij de RNO.

Opmerking: Cisco CallManager interclusterstammen werken momenteel niet via een H.323-proxy omdat de intercluster signalering geen native H.225 is.

QoS-toezicht op de toegang is een alternatieve oplossing. Op het punt waar de campus met dit ontwerp verbonden is, wordt een vertrouwensgrens vastgesteld. Het verkeer dat AARNet ingaat wordt gecontroleerd door de optie Cisco IOS® Committed Access Rate (CAR) aan deze grens. Een universiteit die AARNet voor VoIP gebruikt abonneert op een bepaalde hoeveelheid AARNet QoS bandbreedte. CAR controleert dan verkeer dat AARNet ingaat. Het overmatige verkeer heeft IP voorrang verminderd tot 0 als de hoeveelheid RTP verkeer met IP voorrang 5 de geabonneerde bandbreedte overschrijdt.

In dit schema is een CAR-configuratie opgenomen:



Dit voorbeeld laat zien hoe een CAR-configuratie met dit toezicht omgaat:

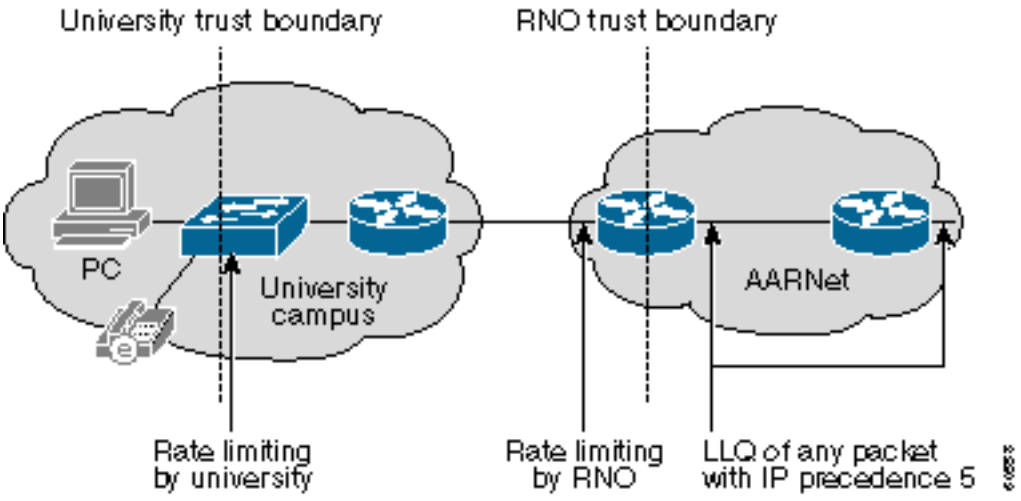
```
Interface a1/0.100
rate-limit input access-group 100 2400000 0 0 conform-action set-prec-transmit 5
exceed-action set-prec-transmit 0

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

Dit zijn enkele voordelen van een CAR configuratie benadering:

- De kern hoeft zich niet langer met de politie bezig te houden. Het wordt nu op de grens van het vertrouwen behandeld. Daarom hoeft de LLQ in de kern niet te weten over de vertrouwde IP-adressen. Elk pakje met een IP-voorrang van 5 in de kern kan veilig aan LLQ worden onderworpen omdat het al het toezicht bij de ingang heeft doorlopen.
- Er worden geen aannames gemaakt over de VoIP architectuur, apparatuur en protocollen die individuele universiteiten kiezen. Een universiteit kan ervoor kiezen om een Session Initiation Protocol (SIP) of Media Gateway Control Protocol (MGCP) te implementeren die niet werkt met H.323-proxy. VoIP-pakketten ontvangen de juiste QoS in de kern zolang ze een IP-voorrang van 5 hebben.
- CAR is veerkrachtig tegen QoS Denial of Service (DoS)-aanvallen. Een QoS DoS-aanval die afkomstig is van een universiteit kan de kern niet beschadigen. CAR beperkt de aanval, die niet meer verkeer kan genereren dan wat er is wanneer het maximum aantal toegestane VoIP aanroepen actief is.VoIP-oproepen naar of van die campus kunnen lijden tijdens een aanval. Maar het is aan de individuele universiteit om zichzelf intern te beschermen. De universiteit kan CAR ACLs op de router aanscherpen zodat alle behalve geselecteerde VoIP subnetwerken het IP voorrang ingedrukt hebben.Elke campus heeft een interne vertrouwensgrens op het punt waar gebruikers in het uiteindelijke ontwerp een verbinding maken met het campus LAN. Verkeer met een IP-voorrang van 5 dat deze vertrouwensgrens wordt ontvangen is beperkt tot 160 kbps per switch poort, of twee G.711 VoIP-oproepen. Het verkeer dat dit tarief te boven gaat, wordt gemarkeerd. De implementatie van deze regeling vereist Catalyst 6500 switches of iets dergelijks met de functie voor snelheidsbeperking.
- Bandbreedtereservering in de kern vereenvoudigt zoals elke universiteit op een vaste hoeveelheid QoS-bandbreedte abonneert. Dit maakt de facturering van QoS ook eenvoudig omdat elke universiteit een vlakke maandelijkse vergoeding kan betalen gebaseerd op een QoS bandbreedte abonnement.

De belangrijkste zwakte van dit ontwerp is dat de vertrouwensgrens zich op de universiteitsrouter bevindt, zodat de universiteiten in staat moeten zijn de CAR correct te beheren. De vertrouwensgrens wordt teruggetrokken in de RNO. Door RNO bestuurde apparatuur regelt de politie in het uiteindelijke ontwerp. Dit ontwerp vereist hardware-Based Rate-limitering zoals de Catalyst 6000 switch of een Cisco 7200 Network Services Engine (Cisco 7200 NSE-1) processor. Het geeft AARNet en RNOs echter volledige controle over QoS-toezicht. In dit schema is dit ontwerp te zien:



Link Fragmentation and Interleaving

VoIP wordt alleen uitgevoerd via virtuele circuits (VC's) van relatief snelle ATM-circuits. Daarom is

geen LFI vereist. VoIP kan in de toekomst ook via Frame Relay Forum (FRF) of huurlijnen naar landelijke universiteiten worden getransporteerd. Dit vereist LFI-mechanismen zoals Multilink PPP (MLP) met Interleaving of FRF.12.

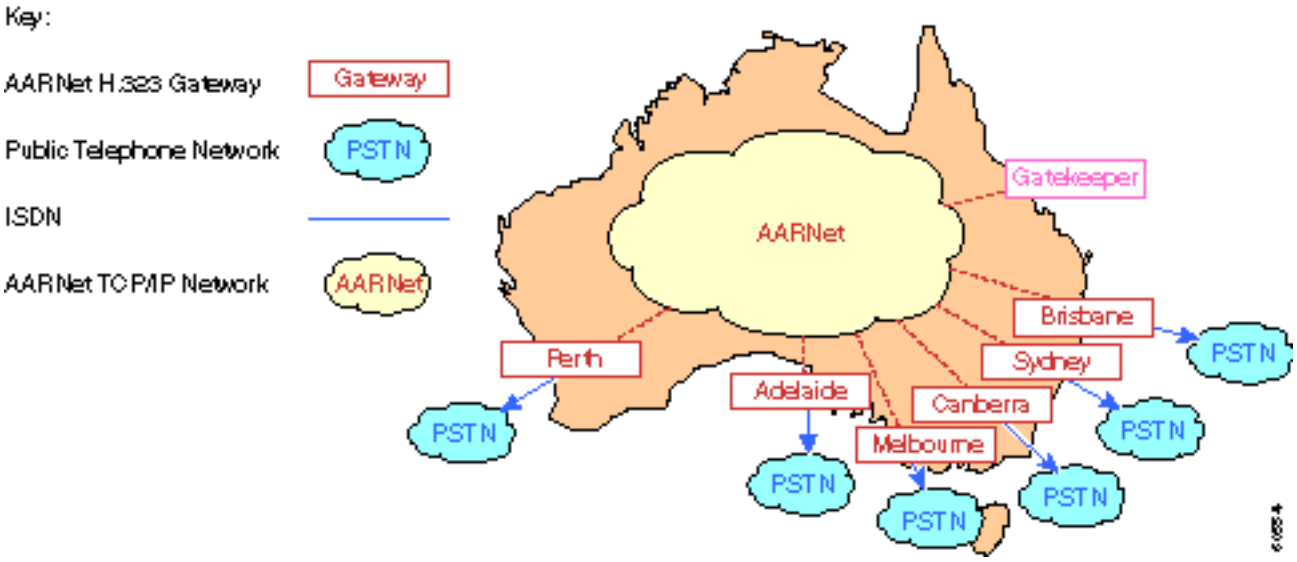
Gateways

Er zijn twee soorten H.323 gateways in AARNet:

- PSTN-PSTN naar VoIP-gateway
- PABX—PABX naar VoIP-gateway

Het onderscheid tussen een PSTN- en een PABX-poort is voornamelijk functioneel. PSTN-gateways bieden connectiviteit op het PSTN. De PABX-gateways verbinden een PABX-universiteit met de VoIP-backbone. Het zelfde fysieke doosje werkt als zowel een PSTN als een PABX gateway in veel gevallen. Er zijn momenteel 31 gateways in de ACU IP-telefonieoplossing. De meeste van deze gateways zijn Cisco AS5300 Universele toegangsservers. De andere gateways zijn Cisco 3600 Series routers of Cisco 2600 Series routers. Tijdens Q2CY01 worden ten minste tien extra gateways verwacht. AARNet heeft in april 2001 ongeveer 145.000 VoIP-oproepen aan boord.

AARNet heeft PSTN-aangesloten H.323 gateways in de meeste grote steden ingezet, zoals dit diagram toont:



Universiteiten kunnen deze gateways gebruiken om uitgaande oproepen naar het PSTN te maken. Universiteiten moeten hun eigen trunks voor inkomende oproepen behouden omdat ze op dit moment niet worden ondersteund. AARNet kan met de luchtvaartmaatschappij onderhandelen over een zeer concurrerende prijs vanwege de omvang van de gesprekken die door deze gateways lopen. De oproepen kunnen ook op het meest kosteneffectieve punt worden afgebroken. Iemand in Sydney bijvoorbeeld die een Perth-nummer aanroept, kan de Perth-poort gebruiken en alleen aanrekenen voor een lokaal gesprek. Dit staat ook bekend als Tail End Hop Off (TEHO).

Er wordt één poorts ingezet om E.164 uit te voeren naar IP-adresresolutie. Alle oproepen naar het PSTN worden naar de poortwachter gestuurd, die dan het IP-adres van de meest geschikte gateway teruggeeft. Raadpleeg de Kiesschema's en de Gatekeeper secties voor meer informatie over gatekeeper.

facturering en accounting

De PSTN-gateways maken gebruik van RADIUS- en authenticatie-, autorisatie- en accounting (AAA) voor factureringsdoeleinden. Elke vraag door een gateway genereert een Call Detail Record (CDR) voor elke aanroep. Deze CDR's worden op de RADIUS-server geplaatst. Het IP-adres van Cisco CallManager in de CDR identificeert de universiteit en garandeert dat de juiste partij wordt gefactureerd.

Gatewaybeveiliging

Het beschermen van de PSTN-gateways tegen VVV-aanvallen en fraude is een belangrijke zorg. De H.323-cliënten zijn op grote schaal beschikbaar. Microsoft NetMeeting is gebundeld met Microsoft Windows 2000, dus is het voor een niet-technische gebruiker relatief eenvoudig om gratis oproepen door deze gateways te plaatsen. Configureer een inkomende ACL die H.225 signalering toestaat van vertrouwde IP-adressen om deze gateways te beschermen. Deze benadering heeft alle dezelfde schaalbaarheidskwesties die in het QoS-gedeelte worden beschreven. Het aantal items in ACL groeit terwijl het aantal vertrouwde H.323-endpoints toeneemt.

H.323-proxy's bieden in dit gebied enige verlichting. De gateway ACL's moeten één IP-adres per universiteitscampus toestaan als alle oproepen via de PSTN-gateway door een campus-proxy lopen. In de meeste gevallen is het wenselijk twee IP-adressen als redundante proxy aan te wijzen. Zelfs met proxy's kan ACL meer dan 100 items bevatten.

De proxy moet via ACL's zijn beveiligd, aangezien elke H.323 een oproep via de proxy kan instellen. De volmacht ACL moet lokale H.323-apparaten toestaan zoals het lokale beleid vereist aangezien dit per campus gebeurt.

De IP adressen van de twee CallManager van Cisco moeten in de gateway ACLs worden opgenomen als een campus slechts vraag van IP telefoons wil toestaan om de AARNet PSTN gateways te gebruiken. De gevolmachtigden voegen in deze situatie geen enkele waarde toe. Het aantal vereiste ACL-items is twee kanten.

Merk op dat intercampus IP telefoon-naar-IP aanroepen niet door de proxy hoeft te gaan.

Kiesschema's

Het huidige VoIP-kiesschema is eenvoudig. De gebruikers kunnen deze twee types van vraag vanuit een perspectief van VoIP plaatsen:

- Bel een telefoon op een andere campus, maar op dezelfde universiteit.
- Bel een PSTN-telefoon of een telefoon aan een andere universiteit.

De toegangskiezerpeers geven het feit aan dat er slechts twee soorten oproepen zijn. Basilicum zijn er twee VoIP dial peer types, zoals dit voorbeeld toont:

```
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
```

De eerste kiestoon wordt gebruikt als iemand verlenging 7... roept op een andere campus in dit voorbeeld. Deze vraag wordt rechtstreeks naar het IP-adres van de externe gateway gestuurd.

Aangezien de poortwachter is omzeild, wordt Call Admission Control (CAC) niet uitgevoerd.

De tweede dial peer wordt gebruikt wanneer de vraag voor een PSTN aantal is. Dit kan een van deze items zijn:

- Het aantal telefoons in het PSTN
- Het volledig gekwalificeerde PSTN-nummer van een telefoon op een andere universiteit

De oproep wordt naar de poortwachter gestuurd door middel van een bericht van toegangsaanvraag (ARQ) in het eerste geval. De poortwachter geeft het IP-adres van de beste PSTN-poort terug in een ACF-bericht (toegangsbevestiging).

De oproep wordt ook naar de poortwachter gestuurd door middel van een ARQ - bericht in het tweede geval. Echter, de poortwachter geeft een ACF-bericht terug met het IP-adres van de VoIP-poort op de universiteit die de oproep ontvangt.

Gatekeeper

AARNet exploiteert momenteel één poortwachter. Het enige doel van deze poortwachter is het routeren van oproepen in de vorm van E.164 naar IP adresresolutie uit te voeren. De poortwachter voert geen CAC uit. Het aantal PABX-trunks dat op de gateways is aangesloten beperkt het aantal gelijktijdige oproepen. De kern bandbreedte omvat voor alle stammen in gebruik tegelijkertijd. Dit verandert door de uitrol van IP-telefonie op ACU en andere universiteiten. Er is geen natuurlijke beperking in het aantal gelijktijdige VoIP-oproepen die in of vanuit een bepaalde campus in deze nieuwe omgeving kunnen worden gegenereerd. De beschikbare QoS-bandbreedte kan worden overschreden als te veel oproepen worden geïnitieerd. Alle oproepen kunnen onder deze omstandigheden van slechte kwaliteit zijn. Gebruik de poortwachter om CAC te leveren.

De gedistribueerde aard en de potentiële omvang van het spraaknetwerk van de universiteit leent zich aan een gedistribueerde poortwarenarchitectuur. Eén mogelijke oplossing is een hiërarchisch gatekeeper-ontwerp op twee niveaus, waarin elke universiteit haar eigen poortwachter handhaaft. Deze universitaire poortwachter wordt aangeduid als de tweede poortwachter. AARNet exploiteert een *directory* gatekeeper dat wordt aangeduid als een tier 1-poortwachter.

Universiteiten moeten deze benadering op twee niveaus gebruiken om een gatekeeper te gebruiken voor oproeproutering tussen Cisco CallManager clusters. De poortwachter-routes roepen op basis van een 4- of 5-cijferig extensie in dit scenario. Iedere universiteit heeft haar eigen poortwachter nodig. Dit komt doordat de verlengingsmarges overlappen tussen universiteiten omdat dit een lokaal bestuurde adresruimte is.

De gatekeepers van het universiteitsniveau 2 voeren CAC uit voor gesprekken van en naar deze universiteit. Het voert ook een E.164 resolutie uit voor gesprekken tussen alleen de campussen van die universiteit. De oproep wordt door de tweede poortwachter van de lijst naar de tweede gatekeeper geleid door middel van een LRQ-bericht (Location request) indien iemand een IP-telefoon aanroept bij een andere universiteit of het PSTN via een AARNet-poort belt. Het LRQ wordt naar de tweede poortwachter van die universiteit gestuurd als er een andere universiteit nodig is. Deze poortwachter geeft een ACF-bericht terug naar de poorts op de tweede klas van de universiteit waar de oproep vandaan komt. Beide niveaus 2 gatekeeper-gatekeeper-gen voeren CAC uit. Ze gaan alleen verder met de oproep als er voldoende bandbreedte beschikbaar is bij zowel de oproepende als de opgeroepen zones.

AARNet kan ervoor kiezen de AARNet PSTN-gateways te behandelen zoals die van elke universiteit. Hun eigen niveau 2 poortwachter zorgt voor de zorg. De op lijst 1 opgenomen

poortwachter kan ook optreden als de op lijst 2 opgenomen poortwachter voor deze gateways indien belasting en prestaties dit toelaten.

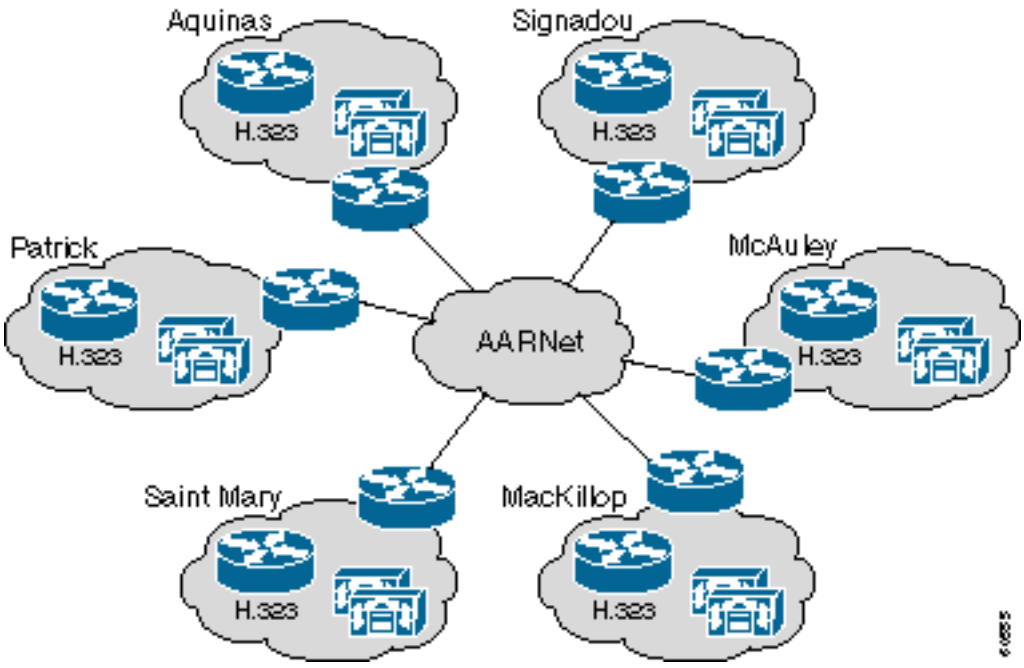
Elk van de poortwachter (met inbegrip van de AARNet folder gatekeeper) moet worden gerepliceerd omdat de gateways zo'n cruciaal onderdeel zijn. Elke universiteit heeft twee gatekeeper nodig. Het is mogelijk voor Cisco IOS-gateways om wisselaars te hebben, zoals in het geval van Cisco IOS-softwarerelease 12.0(7)T. Dit wordt echter niet ondersteund door Cisco CallManager of een ander H.323-apparaat van derden. Gebruik deze optie momenteel niet. Gebruik in plaats daarvan een eenvoudige op HSRP gebaseerde oplossing (Hot Standby Router Protocol). Dit vereist dat beide gatekeeper op hetzelfde IP subnetwerk zit. HSRP bepaalt welke gatekeeper actief is.

ACU IP-telefonienetwerk

In deze tabel wordt het geschatte aantal IP-telefoons weergegeven dat op de campussen van ACU is geïnstalleerd:

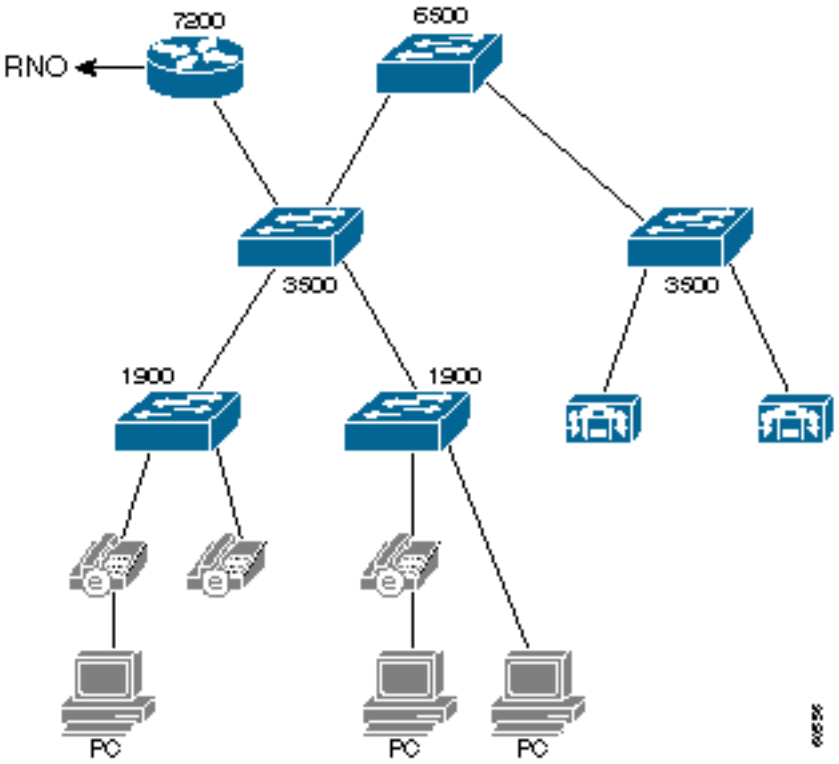
Campus	Stad	IP-telefoons van benadering
Mount Saint Mary	Strathfield	400
MacKillop	Noord Sydney	300
Patrick	Melbourne	400
Achinas	Ballarat	100
Signadou	Canberra	100
McAuley	Brisbane	400
	Totaal:	*1700*

ACU heeft onlangs een oplossing voor IP-telefonie ingezet. De oplossing bestaat uit een cluster van twee CallManager, een gateway van Cisco 3640 op elke campus, en IP-telefoons. AARNet verbindt de campussen onderling. In dit diagram worden de topologie op hoog niveau en de verschillende componenten van het ACU IP-telefonienetwerk weergegeven:



ACU-netwerktopologie

In dit schema is een typische ACU-campus te zien. Elke campus heeft drie lagen Catalyst switches. De kast van de bedrading huisvest de oudere switches van Catalyst 1900. De Catalyst 1900 switches verbinden zich terug tot de Catalyst 3500XL switch door middel van Extended Framing. Deze verbinden terug aan één enkele Catalyst 6509 switch door middel van Gigabit Ethernet (GE). Een enkele Cisco 7200 VXR router sluit de campus aan op AARNet door een ATM VC aan de lokale RNO.



De aansluitingsmethode op de RNO verschilt enigszins van de staat tot de staat, zoals in deze tabel wordt weergegeven. Victoria is gebaseerd op klassieke IP over ATM (RFC 1577). De andere RNOs hebben een rechte PVC opstelling met RFC 1483 insluiting. Open Snelste pad (OSPF) is het routingprotocol dat tussen ACU en RNOs wordt gebruikt.

Campus	Staat	Connectiviteit met RNO	Routing Protocol
Mount Saint Mary	NSW	RFC 1483 PVC	OSPF
MacKillop	NSW	RFC 1483 PVC	OSPF
Patrick	VIC	RFC 1577 klassieke IP-over-ATM	OSPF
Achinas	VIC	RFC 1577 klassieke IP-over-ATM	OSPF
Signadou	HANDELEN	RFC 1483 PVC	OSPF
McAuley	QLD	RFC 1483 PVC	OSPF

De Catalyst 1900 Series switches ondersteunen alleen trunking op de uplinks. Daarom zijn de IP-telefoons en PC's allemaal in één groot VLAN. In feite is de gehele campus één groot VLAN en

een uitgezonden domein. Secundaire IP-subnetwerken worden gebruikt vanwege het grote aantal apparaten. De IP-telefoons bevinden zich op één IP-subnetwerk en de PC's op een andere. De kern van AARNet vertrouwt op het IP telefoon subnetwerk, en het verkeer naar en van dit IP subnetwerk is onderworpen aan LLQ.

De Cisco 7200 routerroutes tussen de primaire en secundaire IP subnetwerken. De functiekaart voor meerlaagse Switch (MSFC) in de Catalyst 6500 switch wordt momenteel niet gebruikt.

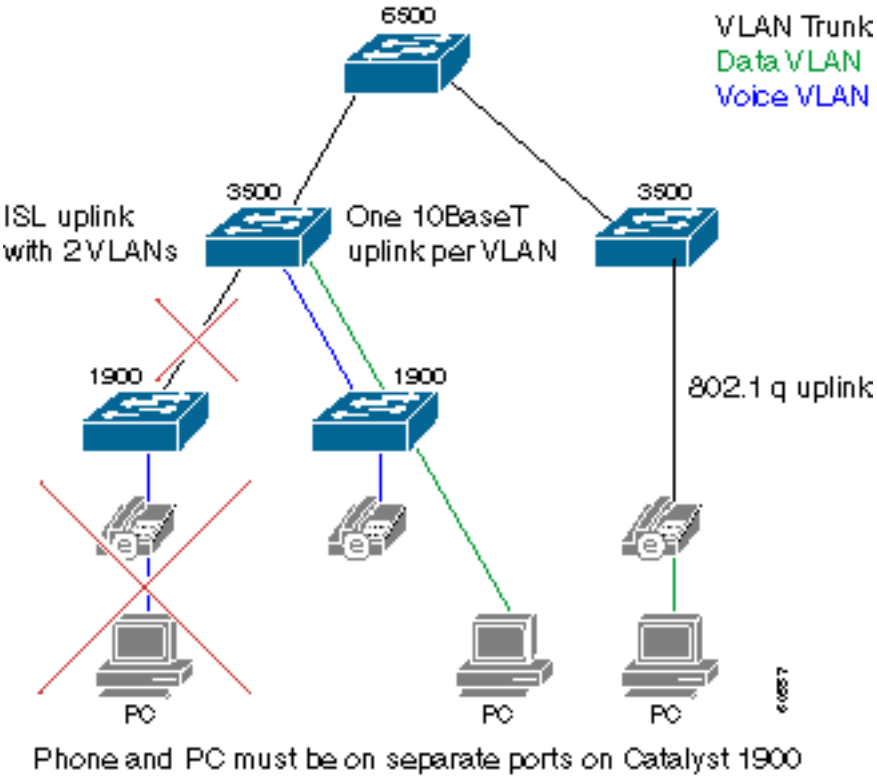
Catalyst 3500XL en Catalyst 6500 switches hebben QoS functies, maar ze zijn op dit moment niet ingeschakeld.

QoS op de campus

Het huidige campus-ontwerp voldoet niet aan de Cisco-aanbevolen ontwerprichtlijnen voor IP-telefonie. Dit zijn een paar zorgen over QoS:

- Het uitgezonden domein is erg groot. De buitensporige uitzendingen kunnen de prestaties van IP telefoons beïnvloeden, die hen moeten verwerken.
- De Catalyst 1900 switches zijn niet geschikt voor QoS. Als een IP-telefoon en een PC op dezelfde switch poort zijn aangesloten, kunnen spraakpakketten worden verzonden als de PC gegevens met een hoog tempo ontvangt.

Herontwerp onderdelen van de campus-infrastructuur om belangrijke verbeteringen te realiseren. Een hardwareupgrade is niet vereist. Dit schema illustreert de principes achter het aanbevolen nieuwe ontwerp:



De campus moet in een spraak-VLAN en een gegevensVLAN worden gesplitst. Telefoons en PC's die aan een Catalyst 1900 switch verbinden moeten nu met verschillende poorten verbinden om de VLAN-scheiding te bereiken. Er wordt een extra uplinks toegevoegd van elke Catalyst 1900-switch aan de Cisco 3500XL switch. Eén van de twee uplinks is lid van de stem VLAN. De andere uplink is een lid van het data-VLAN. Gebruik InterSwitch Link (ISL)-trunking niet als alternatief voor twee uplinks. Dit voorziet niet in het spraak- en gegevensverkeer van afzonderlijke

wachtrijen. De GE links van de Catalyst 3500XL switch naar de Catalyst 6000 switch moeten ook worden geconverteerd naar 802.1q stammen zodat zowel spraak- als gegevensVLAN over deze kernswitch kan worden gedragen.

poorten op Catalyst 3500XL switch die in het data-VLAN zijn hebben een standaard serviceklasse (CoS) van nul. Havens die leden van de stem VLAN zijn hebben een standaard CoS van 5. Als resultaat hiervan, wordt het stemverkeer correct geprioriteerd wanneer het bij Catalyst 3500 of Catalyst 6500 kern aankomt. De Catalyst 3500 QoS switch poortconfiguraties variëren lichtjes afhankelijk van welke VLAN switch poort een lid is, zoals dit voorbeeld toont:

```
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
```

U kunt een PC aan de achterhaven van de switch op de IP telefoon in het zeldzame geval aansluiten dat IP telefoons direct op een Catalyst 3500XL switch verbinden. De IP-telefoons verbinden met de switch in dit geval met een 802.1q stam. Dit staat stem en gegevenspakketten toe om op afzonderlijke VLAN's te reizen, en u kunt pakketten de juiste CoS bij ingress geven. Vervang Catalyst 1900 switches met Catalyst 3500XL switches of andere QoS-enabled switches wanneer ze aan het einde van hun leven komen. Deze topologie wordt dan de standaardmethode om IP telefoons en PCs aan het netwerk te verbinden. Dit scenario toont de Catalyst 3500XL switch QoS configuratie:

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

Tenslotte zouden de twee poorten die aan de twee Cisco CallManager-beheerders verbinden de CoS aan 3 moeten hebben. Cisco CallManager stelt de IP voorrang aan 3 in alle spraak signaleringspakketten in. Echter, de verbinding van Cisco CallManager naar Catalyst 3500XL switch gebruikt geen 801.1p. Daarom wordt de CoS-waarde bij de switch gedwongen, zoals uit dit voorbeeld blijkt:

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

De belangrijkste hindernis bij dit ontwerp is dat er twee switch-poorten vereist zijn op het bureaublad. De Patrick campus kan een extra 400 switch poorten nodig hebben voor 400 IP-telefoons. Aanvullende Catalyst 3500XL switches moeten worden ingezet als er niet voldoende poorten beschikbaar zijn. Er is slechts één Catalyst 3500XL switch poort vereist voor elke twee ontbrekende Catalyst 1900 switch poorten.

De huidige ACU Catalyst 6500 switches hebben QoS mogelijkheden, maar zijn op dit moment niet ingeschakeld. Deze modules zijn aanwezig in de ACU Catalyst 6000 switch met deze wachtrijen mogelijkheden:

sleuf	Module	Poorten	RX-wachtrijen	TX-wachtrijen
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	—	—

Voltooi deze stappen om de juiste QoS-functies te activeren op de Catalyst 6000 switch:

1. Vertel de switch om QoS op een basis per-VLAN van deze opdracht te voorzien:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 vlan-based
   ```

2. Vertel de switch om de CoS waarden te vertrouwen die van de Catalyst 3500XL switch met deze opdracht worden ontvangen:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos
   ```

De CoS moet nu worden ingesteld op gedifferentieerde services code point (DSCP) mapping. Dit is vereist omdat de Catalyst 6000 switch de DSCP waarde in de IP header herschrijft op basis van de ontvangen CoS-waarde. VoIP-signaleringspakketten moeten zijn voorzien van een CoS van 3, herschreven met een DSCP van AF 31 (26). RTP-pakketten moeten een CoS van 5 hebben, herschreven met een DSCP van EF (46). Deze opdracht geven:

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

Gebruik dit voorbeeld om de CoS-to-DSCP afbeelding te controleren.

```
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
```

Configuratie van de MSFC om tussen de verschillende IP subnetwerken te leiden.

QoS in het RNO

Het huidige RNO-ontwerp voldoet niet aan de door Cisco aanbevolen ontwerprichtlijnen voor IP-telefonie. Deze bezorgdheid bestaat ten aanzien van QoS:

- LLQ wordt niet toegepast op Cisco ACU 7200 Series WAN-router.
- De campussen Patrick en Aquinas verbinden met RNO door middel van ATM Switched VC's (SVC's). LLQ wordt niet ondersteund op SVC's.

Een Fast Ethernet-verbonden Cisco 7200 router sluit de campus aan op een RNO door middel van een 34 Mbps E4 ATM-link. Het verkeer kan zich in de rij bevinden aan de kant van de 34M links vanwege de 4M versus de 100M snelle mismatch. Daarom is het noodzakelijk om prioriteit te geven aan het spraakverkeer. Gebruik LLQ. De Cisco 7200 routerconfiguratie is vergelijkbaar met dit voorbeeld:

```
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
```

De bandbreedte die aan LLQ wordt toegewezen moet *N x 24 Kbps* zijn, waar N het aantal gelijktijdige G.729-oproepen is.

Stel één PVC in van elk van de routers van Patrick en Achinas Cisco 7200 naar de AARNet router. ATM SVC's in het Victoriaans RNO ondersteunen LLQ niet, omdat dit is gebaseerd op klassieke IP over ATM (RFC 1577). De andere universiteiten in het Victoriagebied RNO kunnen voorlopig RFC 1577 blijven gebruiken. Vervang echter uiteindelijk de klassieke IP over ATM-infrastructuur.

Gateways

Elk van de ACU campussen heeft een Cisco 3640 router die als H.323 gateway fungeert. Deze gateways verbinden met het PSTN door middel van ISDN. Het aantal Primaire Rate Interfaces (PRI's) en B-kanalen is afhankelijk van de grootte van de campus. Deze tabel bevat het aantal PRI's en B-kanalen voor elke campus:

Campus	PRI-hoeveelheid	B-kanaalhoeveelheid
Mount Saint Mary	2	30
MacKillop	2	50
Patrick	2	50
Achinas	1	20
Signadou	1	20
McAuley	1	30

Deze gateways worden uitsluitend gebruikt als secundaire poorten voor DOD (Direct Outward Dialing). De AARNet-gateways zijn de primaire gateways. De ACU-gateways worden altijd gebruikt voor DID (Direct Inward Dialing).

Kiesschema

Het kiesschema is gebaseerd op de uitbreidingsnummers met 4 cijfers. De verlenging is ook de laatste vier cijfers van het DID-nummer. In deze tabel worden de bereik- en DID-nummers voor elke campus vermeld:

Campus	Uitbreiding	DID
Mount Saint Mary	9 xxx	02 9764 9xxx
MacKillop	8xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Achinas	5 xxx	03 530 5xxx
Signadou	2xxx	02 6123 2xxx
McAuley	7 xxx	07 354 7xxx

Een eenvoudige `num-exp` ingang op de gateways bekraakt het DID nummer aan de 4-cijferig extensie voordat dit op Cisco CallManager wordt doorgegeven. De poort van Patrick campus heeft bijvoorbeeld dit nummer:

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

De gebruikers draaien 0 om een buitenlijn te selecteren. Deze loods nul wordt doorgegeven naar de poort. Eén enkele POTS-kiestoon routeert de ISDN-poort op basis van de toonaangevende nul.

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

Inkomende gesprekken gebruiken deze num-exp invoer om het aangeroepen partijnummer om te zetten in een 4-cijferige extensie. De vraag past dan beide VoIP kiespeers aan. Gebaseerd op de lagere voorkeur, verkiest het deze route naar de abonnee van Cisco CallManager:

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

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

Cisco CallManager

Elk van de campussen heeft een cluster die uit twee servers van Cisco CallManager bestaat. De Cisco CallManager-servers zijn een mix van Media Convergence Server 7835 (MCS-7835) en Media Convergence Server 7820 (MCS-7820). Beide servers runden versie 3.0(10) ten tijde van deze publicatie. Eén Cisco CallManager is de *uitgever* en de andere Cisco CallManager is de *abonnee*. De abonnee treedt op als de primaire Cisco CallManager voor alle IP-telefoons. Deze

tabel toont de hardware die op elke campus is ingezet:

Campus	platform	CallManager
Mount Saint Mary	MCS-7835	2
MacKillop	MCS-7835	2
Patrick	MCS-7835	2
Achinas	MCS-7820	2
Signadou	MCS-7820	2
McAuley	MCS-7835	2

Elke cluster is geconfigureerd met twee regio's:

- 1 voor intracampus-oproepen (G.711)
- Eén voor intercampus-oproepen (G.729)

Op locatie gebaseerde CAC is niet geschikt voor ACU omdat alle IP-telefoons die door elke cluster worden gediend, zich op één campus bevinden. Er zijn voordelen aan een op gatekeeper gebaseerde CAC voor intercampus telefoontjes, maar deze worden momenteel niet geïmplementeerd. Er zijn echter plannen om dat in de nabije toekomst te doen.

Elke Cisco CallManager is geconfigureerd met 22 H.323 gateways. Dit bestaat uit intercluster stammen naar de vijf andere clusters van Cisco CallManager, zes AARNet PSTN gateways, en één ACU gateway op elke campus.

H.323 Apparaattype	Hoeveelheid
Intercampus CallManager	2 x 5 = 10
Aironet PSTN-gateway	6
ACU PSTN-gateway	6
Totaal:	*22*

Routerlijsten en routegroepen worden gebruikt om de PSTN-gateways te rangschikken. Bijvoorbeeld, deze tabel toont hoe de vraag van Patrick Cisco CallManager in Melbourne aan Sydney PSTN de vier gateways kan gebruiken om de vraag samen met een routegroep te verbinden.

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

De Cisco CallManager wordt geconfigureerd met ongeveer 30 routepatronen, zoals in deze tabel wordt weergegeven. De routepatronen zijn zo ontworpen dat er specifieke overeenkomsten zijn voor alle Australische binnenlandse getallen. Op deze manier hoeven de gebruikers niet te wachten tot de tijdelijke versie tussen de cijfers verloopt voordat Cisco CallManager de oproep start. Het teken van de wildkaart "!" uitsluitend in het routepatroon voor internationale nummers wordt gebruikt. De gebruikers moeten wachten tot de onderbreking van meerdere cijfers (standaard 10 seconden) verstrijkt voordat de vraag vordert wanneer zij een internationale

bestemming draaien. De gebruikers kunnen het routepatroon ook toevoegen "0.0011!#". De gebruikers kunnen dan een "#" na het laatste cijfer in om aan Cisco CallManager aan te geven dat het gedialineerde aantal volledig is. Deze actie bevordert de internationale dialoog.

Routepatroon	Beschrijving
0[2-9]XXXXXXX	Bel
0.00	Noodoproep - als de gebruiker vergeet om 0 voor de buitenlijn te bellen
0.000	Noodnummer
0.013	Bijdrage van mappen
0.1223	—
0.0011!	Internationale oproepen
0,02XXXXXX	doet een beroep op New South Wales
0,03XXXXXX	Roept naar Victoria
0,04XXXXXX	Aanroepen naar mobiele telefoons
0,07XXXXXX	riepen naar Queensland
0,086XXXXX	roept op tot West-Australië
0,08XXXXXX	doet een beroep op Zuid-Australië en Noord-gebieden
0,1[8-9]XXXXXXXX	Bel 1800 xxx en 1900 xxx
0,1144x	noodgeval
0,119[4-6]	Tijd en weer
0,1245X	Map
0,13[1-9]XXX	Bel 13xxxx-nummers
0,130XXXXX	Bel 1300 xxx-nummers
2[0-1]XX	Intercluster-oproepen naar Signadou
3[0-4]XX	Intercluster-oproepen aan Patrick
5[3-4]XX	Intercluster-oproepen naar Achinas
7[2-5]XX	Intercluster-oproepen naar McAuley
8[0-3]XX	Intercluster-oproepen naar MacKillop
9[3-4]XX	Intercluster-oproepen naar Mount Saint Mary
9[6-7]XX	Intercluster-oproepen naar Mount Saint Mary

Het aantal gateways, routegroepen, routekaarten, en routepatronen die op de ACU Cisco CallManagers zijn geconfigureerd heeft het potentieel om aan een groot aantal te groeien. Als een nieuwe RNO-gateway wordt ingezet, moeten alle vijf Cisco CallManager-clusters opnieuw worden geconfigureerd met een extra poort. Erger nog, honderden gateways moeten worden toegevoegd als de route VoIP van Cisco CallManager van de ACU rechtstreeks naar alle andere universiteiten belt en het PSTN in zijn geheel voorbijgaat. Dit schaadt duidelijk niet zo goed.

De oplossing is om de gatekeeper-gecontroleerd van Cisco CallManager te maken. U moet de gatekeeper alleen bijwerken als er een nieuwe gateway of Cisco CallManager ergens in de AARNet wordt toegevoegd. Elke Cisco CallManager moet alleen de lokale campus gateway en het anonieme apparaat hebben die ingesteld worden wanneer dit gebeurt. Je kan dit apparaat zien als een point-to-multipoint stam. Het verwijdert de noodzaak voor de gekoppelde PPP-trunks in het Cisco CallManager-kiesschema-model. Eén enkele routegroep wijst naar het anonieme apparaat als de voorkeurstoegang en naar de lokale gateway als de reservegateway. De lokale PSTN-gateway wordt gebruikt voor bepaalde lokale oproepen en ook voor algemene off-net gesprekken als de poortwachter niet beschikbaar wordt. Op dit moment kan het anonieme apparaat intercluster of H.225 zijn, maar niet beide tegelijkertijd.

Cisco CallManager heeft minder routepatronen met een gatekeeper nodig dan nu. In principe heeft Cisco CallManager alleen één routepatroon van "!" nodig. naar de poortwachter te wijzen. In werkelijkheid moet de manier waarop oproepen worden gestuurd om deze redenen specifieker zijn:

- Sommige oproepen (zoals oproepen naar 1-800 of noodnummers) moeten door een geografisch lokale poort worden geleid. Iemand in Melbourne die de politie of een restaurantketen zoals Pizza Hut inhuurt, wil niet verbonden zijn met de politie of de Pizza Hut in Perth. De specifieke routepatronen zijn nodig die rechtstreeks naar de lokale PSTN-gateway van de campus voor deze nummers.Universiteiten die van plan zijn om toekomstige IP Telephony implementaties uit te voeren kunnen ervoor kiezen om uitsluitend op de AARNet gateways te vertrouwen en hun eigen lokale gateways niet te beheren. Deze getallen moeten een virtuele gebiedscode hebben die door Cisco CallManager wordt voorbereid voordat ze naar de poortwachter worden verzonden om dit ontwerp te kunnen maken voor oproepen die lokaal moeten worden afgezet. Bijvoorbeeld, kan Cisco CallManager 003 voorbereiden om van een op Melbourne gebaseerde telefoon naar het Pizza Hut 1-800 aantal te bellen. Dit laat de poortwachter toe om de verbinding naar een AARNet-poort op Melbourne te leiden. De poort stopt van het voorjaar 2003 voordat het de oproep naar het PSTN plaatst.
- Gebruik routepatronen met specifieke overeenkomsten voor alle binnenlandse getallen om te vermijden dat de gebruiker op de cijfer tijd wacht voordat de oproep wordt gestart.

Deze tabel toont de routepatronen voor een door gatekeeper gecontroleerde Cisco CallManager:

Routepatroon	Beschrijving	Routeswitch	Gatekeeper
0[2-9]XXXXXXX	Bel	Routelijst	AARNet
0.00	Noodnummer	Lokale poort	None
0.000	Noodnummer	Lokale poort	None
0.013	Bijdrage van mappen	Lokale poort	None
0.1223	—	Lokale poort	None
0.0011!	Internationale oproepen	Routelijst	AARNet
0,0011!#	Internationale oproepen	Routelijst	AARNet
0,0[2-	Roept op naar	Routelijst	AARNet

4]XXXXXXXX	Nieuw-Zuid-Wales, Victoria en mobiele telefoons		
0,0[7-8]XXXXXXXX	roept op tot Zuid-Australië, West-Australië en Noord-Land	Routelijst	AARNet
0,1[8-9]XXXXXXXX	Bel 1800 xxx en 1900 xxx	Lokale poort	None
0,1144x	noodgeval	Lokale poort	None
0,119[4-6]	Tijd en weer	Lokale poort	None
0,13[1-9]XXX	Bel 13xxxx-nummers	Lokale poort	None
0,130XXXXX	Bel 1300 xxx-nummers	Lokale poort	None
[2-3]XXX	Aanroepen naar Signadou	Routelijst	ACU
5 XXX	Aanroepen naar Achinas	Routelijst	ACU
[7-9]XXX	Roept naar McAuley, MacKillop en Mount Saint Mary	Routelijst	ACU

De poortwachter routeert internationale gesprekken, die niet via de lokale poort worden verstuurd. Dit is van belang omdat AARNet in de toekomst internationale gateways kan inzetten. Als er een 'poort' wordt uitgerold in de Verenigde Staten, kan een simpele verandering van de gatekeeper configuratie universiteiten toestaan om gesprekken naar de VS te plaatsen tegen binnenlandse tarieven van de VS.

De gatekeeper voert interclusteroproerouting uit op basis van de 4-cijferige ACU-extensie. Dit betreft de ruimte die waarschijnlijk overlappingen vertoont met andere universiteiten. Dit dicteert dat ACU zijn eigen poortwachter beheert en de AARNet gatekeeper als *gatekeeper* gebruikt. De gatekeeper kolom in deze tabel geeft aan of de oproeproutering wordt uitgevoerd door de ACU poortwachter of de AARNet gatekeeper.

Opmerking: Het enige voorbehoud met de voorgestelde gatekeeper-oplossing is dat het anonieme apparaat momenteel ofwel intercluster of H.225 kan zijn, maar niet beide tegelijk. Cisco CallManager maakt gebruik van de gatekeeper om oproepen naar zowel gateways (H.225) en andere Cisco CallManager (intercluster) met het voorgestelde ontwerp te sturen. De oplossing voor deze kwestie is om ofwel de gatekeeper niet te gebruiken voor interclusterrouting of om alle oproepen via de gatekeeper te behandelen als H.225. De laatste werkronden betekenen dat sommige aanvullende functies niet beschikbaar zijn voor interclusteroproepen.

Spraakmail

ACU had drie op Active Voice Reparte OS/2-gebaseerde spraakmailservers met analoge telefoonborden voordat werd overgeschakeld op IP-telefonie. Het plan is om deze servers te hergebruiken in de IP-telefonie-omgeving. Wanneer geïmplementeerd, sluit elke omgekeerde server zich aan op een Cisco CallManager door middel van een vereenvoudigde berichtdesk interface (SMDI) en een Catalyst 6000 24-poorts Deviezenstation (FXS) kaart. Dit voorziet voicemail voor drie van de zes campussen, wat drie campussen zonder voicemail laat. Het is niet mogelijk om één Reparte server tussen gebruikers op twee clusters van Cisco CallManager behoorlijk te delen omdat er geen manier is om de berichtwachtindicator (MWI) over de intercluster H.323 boomstam te verspreiden.

ACU kan drie Cisco Unity-servers aanschaffen voor de resterende campussen. Deze servers zijn op Skinny gebaseerd, dus er zijn geen gateways vereist. In deze tabel worden de spraakpostoplossingen vermeld voor het geval dat ACU de extra spraakmailservers koopt:

Campus	Spraakmailsysteem	Gateway
Mount Saint Mary	Active Voice Reparation	Catalyst 6000 24-poorts FXS-module
MacKillop	Active Voice Reparation	Catalyst 6000 24-poorts FXS-module
Patrick	Active Voice Reparation	Catalyst 6000 24-poorts FXS-module
Achinas	Cisco Unity	—
Signadou	Cisco Unity	—
McAuley	Cisco Unity	—

De zes spraakmailservers opereren in dit plan als geïsoleerde voicemail-eilanden. Er is geen voicemail-netwerk.

Mediabronnen

Hardware digitale signaalprocessors (DSP's) worden momenteel niet ingezet bij ACU. Conferencing gebruikt de op software gebaseerde Conference Bridge op Cisco CallManager. Interclusterconferencing wordt momenteel niet ondersteund.

Op dit moment is een transcodering niet vereist. Alleen G.711- en G.729-coder-decoders worden gebruikt, en zij worden ondersteund door alle gebruikte eindapparaten.

Ondersteuning van fax en modem

Fax en modemverkeer worden momenteel niet ondersteund door het ACU IP-telefonienetwerk. De universiteit is van plan om de Catalyst 6000 24-poorts FXS kaart voor dit doel te gebruiken.

Softwareversies

In deze tabel worden de softwareversies weergegeven die op het moment van deze publicatie worden gebruikt:

platform	Functie	Softwareversie
CallManager	IP-PBX	3.0(10)
Catalyst 3500XL switch	Switch voor distributie	12.0(5.1)XP
Catalyst 6500	Core switch	5.5(5)
Catalyst 1900	Switch van kabelkast	—
Cisco 7200 Series processor	WAN-router	12.1(4)
Cisco 3640 router	H.323-gateway	12.1(3a)XI6

Gerelateerde informatie

- Ondersteuning voor spraaktechnologie
- Productondersteuning voor spraak- en IP-communicatie
- Probleemoplossing voor Cisco IP-telefonie
- Technische ondersteuning en documentatie – Cisco Systems