Implementierung von IP-Telefonie im Anwenderbericht: Australische Katholische Universität

Inhalt

Einführung

Das Australian Academic and Research Network (AARNet) ist ein landesweites Hochgeschwindigkeits-IP-Netzwerk, das 37 australische Universitäten sowie die Commonwealth Scientific and Industrial Research Organization (CSIRO) miteinander verbindet.

AARNet wurde ursprünglich als Datennetzwerk konzipiert, wurde aber seit Anfang 2000 über VoIP (Voice over IP) übertragen. Das derzeit eingesetzte VoIP-Netzwerk ist eine Umgehungslösung, die VoIP-Anrufe zwischen den Universitäten und den CSIRO PABX (Private Automatic Branch Exchange) überträgt. Darüber hinaus stehen PSTN-Gateways (Public Switched Telefone Network, PSTN) zur Verfügung, die es dem PSTN ermöglichen, am kostengünstigsten Ort abzuheben. Beispielsweise wird ein Anruf von einem PABX-Telefon in Melbourne an ein PSTN-Telefon in Sydney als VoIP von Melbourne an das PSTN-Gateway von Sydney weitergeleitet. Es ist dort mit dem PSTN verbunden.

Die Australian Catholic University (ACU) ist eine der Universitäten, die mit AARNet verbunden ist.

Ende 2000 begann die ACU mit der Bereitstellung von IP-Telefonie, bei der etwa 2.000 IP-Telefone an sechs Universitätsgeländen bereitgestellt wurden.

In diesem Anwenderbericht wird die ACU IP-Telefonie-Bereitstellung behandelt. Das Projekt ist abgeschlossen. Im AARNet-Backbone müssen jedoch erhebliche Architekturprobleme gelöst werden, wenn das Netzwerk skaliert werden soll, wenn andere Universitäten die ACU unterstützen. In diesem Dokument werden diese Probleme beschrieben, und es werden verschiedene Lösungen vorgeschlagen und erörtert. Die ACU-IP-Telefonie-Bereitstellung wird wahrscheinlich später angepasst, um sie an die empfohlene Architektur anzupassen.

Hinweis: Die Deakin University war die erste australische Universität, die IP-Telefonie bereitstellte. Die Deakin University verwendet jedoch kein AARNet, um IP-Telefonie-Datenverkehr zu übertragen.

AARNet

Die australischen Universitäten und CSIRO bauten AARNet 1990 über das Australian Vice-Bundeskanzlerausschuss (AVCC) auf. Neunundneunzig Prozent des australischen Internetdatenverkehrs erfolgten in den ersten Jahren über die Gründungsmitglieder. Ein kleiner Teil des kommerziellen Datenverkehrs stammte von Organisationen, die eng mit dem Tertiär- und Forschungssektor verbunden waren. Die Nutzung durch Benutzer ohne AARNet stieg bis Ende 1994 auf 20 Prozent des gesamten Datenverkehrs an.

Die AVCC verkaufte den kommerziellen Kundenstamm von AARNet im Juli 1995 an Telstra. Diese Veranstaltung löste das aus, was letztendlich zu Telstra BigPond wurde. Dies stimulierte das Wachstum der kommerziellen und privaten Nutzung des Internets in Australien. Der Transfer von geistigem Eigentum und Fachwissen führte zur Entwicklung des Internets in Australien. Andernfalls wäre dies nicht so schnell geschehen.

Der AVCC entwickelte Anfang 1997 AARNet2. Es war eine weitere Verbesserung des Internets in Australien, das im Rahmen eines Vertrags mit Cable & Wireless Optus (CWO) Limited bandbreitenintensive ATM-Links und Internet-Services verwendet. Die schnelle Bereitstellung von IP-Services durch CWO zur Erfüllung der AARNet2-Anforderungen war zum Teil auf den Wissens- und Erfahrungsaustausch von AARNet zurückzuführen.

ACU

ACU ist eine öffentliche Universität, die 1991 gegründet wurde. Die Universität hat etwa 10.000 Studenten und 1.000 Mitarbeiter. Es gibt sechs Campus an der Ostküste Australiens. Diese Tabelle zeigt die ACU-Standorte und deren Standorte:

Campus	Stadt	Staat
Monte Saint Mary	Strathfield	New South Wales (NSW)
MacKillop	North Sydney	New South Wales (NSW)
Patrick	Melbourne	Victoria (VIC)
Quinas	Ballarat	Victoria (VIC)
Signadou	Canberra	Hauptstadt Australien (ACT)
McAuley	Brisbane	Queensland (QLD)

Vor der Einführung der IP-Telefonielösung, die in diesem Anwenderbericht beschrieben wird, hat sich die ACU auf eine Lösung für das Telstra Spectrum (Centrex) verlassen. Der Umstieg auf IP-Telefonie war hauptsächlich auf die Kostensenkung zurückzuführen.

CSIRO

CSIRO beschäftigt an zahlreichen Standorten in Australien ca. 6.500 Mitarbeiter. CSIRO forscht in Bereichen wie Landwirtschaft, Mineralien, Energie, Produktion, Kommunikation, Bauwesen, Gesundheit und Umwelt.

CSIRO war die erste Organisation, die AARNet für VoIP nutzte. Die Organisation war Pionier in der frühen Arbeit in diesem Bereich.

AARNet

Der AARNet-Backbone ist eine wesentliche Komponente jeder IP-Telefonie-Bereitstellung an einer Universität. Es bietet die Verbindung von Universitäten mit zwei Hauptdiensten im Bereich Sprachkommunikation:

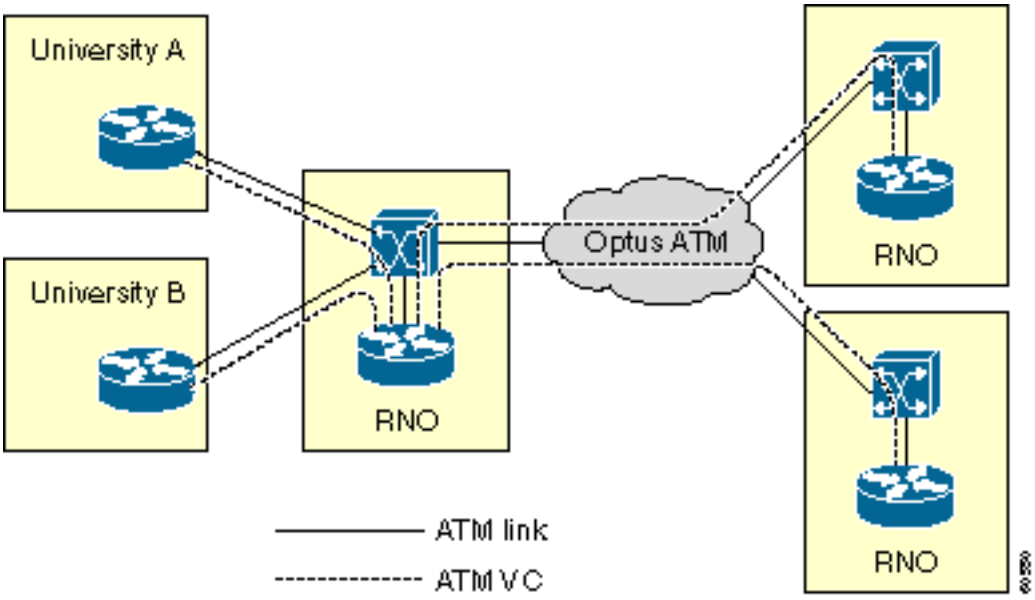
- Transport von VoIP Realtime Transport Protocol (RTP)-Paketen mit der Gewährleistung einer für Sprache geeigneten Quality of Service (QoS)
- Low-Cost-Hoffnungsschimmer zu den PSTNs im ganzen Land

In diesem Abschnitt wird die aktuelle AARNet-Architektur und deren Bereitstellung beschrieben. Darüber hinaus werden einige Probleme hinsichtlich der Skalierbarkeit umrissen, die auftreten, wenn mehr Universitäten die IP-Telefonielösung bereitstellen. Schließlich werden die möglichen Lösungen für diese Skalierbarkeitsprobleme erörtert.

AARNet-Topologie

AARNet besteht aus einem einzigen PoP (Point of Presence) in jedem Staat. Die POPs werden auch als Regional Network Operations (RNOs) bezeichnet. Universitäten stellen Verbindungen zum RNO in ihrem jeweiligen Bundesstaat her. Die RNO wiederum sind durch ein Full-Mesh von Optus ATM PVCs verbunden. Gemeinsam bilden sie AARNet.

Das typische RNO besteht aus einem Cisco LS1010 ATM-Switch und einem ATM-angeschlossenen Router. Der RNO-Router ist über eine ATM-PVC über eine E3-Mikrowellenverbindung mit jedem Universitäts-Router verbunden. Jeder RNO-Router verfügt außerdem über ein vollständiges Netz an ATM-PVCs, die das Optus ATM-Netzwerk allen anderen RNOs zur Verfügung stellt. Dieses Diagramm stellt die allgemeine AARNet-Topologie des Netzwerks dar:



Es gibt zahlreiche Ausnahmen für die Topologie. Einige davon sind aus sprachlicher Sicht von Bedeutung. Dies sind einige Ausnahmen:

- Das RNO in Victoria verwendet für die Verbindung der Universitäten mit dem RNO klassische IP over ATM (RFC 1577) anstelle von PVCs.
- Ländliche Universitäten verbinden sich normalerweise per Frame Relay oder ISDN mit dem RNO.
- Einige große Universitäten haben mehr als eine Verbindung zurück zum RNO.

Diese Tabelle zeigt die Staaten und Gebiete, die derzeit über ein RNO verfügen. Die Tabelle enthält die Hauptstädte für Leser, die nicht mit der australischen Geografie vertraut sind.

Staat	Hauptstadt	RNO?	Campus-Verbindungen
New South Wales	Sydney	Ja	Noch nicht festgelegt
Victoria	Melbourne	Ja	Noch nicht festgelegt
Queensland	Brisbane	Ja	Noch nicht festgelegt
Südafrika	Adelaid	Ja	Noch nicht festgelegt
Westaustralien	Perth	Ja	Noch nicht festgelegt
Australisches Hauptstadtrevier	Canberra	Ja	Noch nicht festgelegt
Nördliches Gebiet	Darwin	Nein	—
Tasmanie	Hobart	Nein	—

Quality of Service

Teile von AARNet sind aufgrund des VoIP-Projekts zur Umgehung von Telefongebühren bereits QoS-fähig. QoS ist für Sprachdatenverkehr erforderlich, um diese Funktionen bereitzustellen, die Verzögerungen und Jitter minimieren und Paketverluste vermeiden:

- Richtlinienvergabe - Markierung des Sprachdatenverkehrs von nicht vertrauenswürdigen Quellen.
- Queuing (Warteschlangenverwaltung) - Sprache muss gegenüber dem gesamten anderen Datenverkehr Priorität erhalten, um Verzögerungen während einer Verbindungsüberlastung zu minimieren.
- Link Fragmentation and Interleaving (LFI) - Datenpakete müssen fragmentiert und Sprachpakete auf langsamen Verbindungen verschachtelt werden.

Der Datenverkehr muss für die ordnungsgemäße Überwachung und Warteschlangenverwaltung von Sprachpaketen klassifiziert werden. In diesem Abschnitt wird beschrieben, wie die Klassifizierung auf AARNet vorgenommen wird. In den folgenden Kapiteln wird die Implementierung von Richtlinien und Warteschlangen beschrieben.

Klassifizierung

Nicht der gesamte Datenverkehr erhält dieselbe QoS. Der Datenverkehr wird in die folgenden Kategorien klassifiziert, um eine selektive QoS bereitzustellen:

- Daten
- Sprache aus bekannten und vertrauenswürdigen Quellen
- Sprache aus unbekannten Quellen

Nur vertrauenswürdige Geräte erhalten eine qualitativ hochwertige QoS auf AARNet. Diese Geräte sind hauptsächlich Gateways, die durch die IP-Adresse identifiziert werden. Eine Zugriffskontrollliste (ACL) wird verwendet, um diese vertrauenswürdigen Sprachquellen zu identifizieren.

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

IP-Rangfolge wird verwendet, um Sprachverkehr von Datenverkehr zu unterscheiden. Voice hat eine IP-Priorität von 5.

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

Kombinieren Sie die vorherigen Beispiele, um Pakete von einer vertrauenswürdigen Quelle zu identifizieren.

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

Verwenden Sie dieselben Prinzipien, um Sprachpakete von einer unbekannten Quelle zu identifizieren.

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

Richtlinienvergabe

Sprachdatenverkehr von einer nicht vertrauenswürdigen Quelle wird klassifiziert und markiert, wenn der Datenverkehr an einer Schnittstelle eingeht. In diesen beiden Beispielen wird

veranschaulicht, wie die Richtlinienvergabe in Abhängigkeit davon durchgeführt wird, welche Art von Datenverkehr auf einer bestimmten Schnittstelle erwartet wird:

Der Router sucht nach nicht vertrauenswürdigen Sprachpaketen und ändert seine IP-Priorität auf 0, wenn nachgeschaltete vertrauenswürdige Sprachquellen vorhanden sind.

```
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
```

Der Router sucht nach allen Sprachpaketen und ändert seine IP-Rangfolge auf 0, wenn im Downstream keine bekannten Sprachquellen vorhanden sind.

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

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

Warteschlangen ohne Sprachübertragung

Bis vor kurzem war das gesamte VoIP in AARNet gebührenpflichtig. Diese Bedingung führt zu relativ wenigen VoIP-Endpunkten. Beim aktuellen Warteschlangendesign wird zwischen Schnittstellen mit Downstream-VoIP-Geräten und Schnittstellen unterschieden, die dies nicht tun. In diesem Abschnitt wird die Warteschlangenverwaltung für Nicht-VoIP-Schnittstellen erläutert.

Eine Nicht-Sprachschnittstelle wird für Weighted Fair Queuing (WFQ) oder Weighted Random Early Detection (WRED) konfiguriert. Diese können direkt auf der Schnittstelle konfiguriert werden. Der Warteschlangenmechanismus wird jedoch mithilfe einer Richtlinienzuordnung angewendet, um das Ändern des Warteschlangenmechanismus für einen bestimmten Schnittstellentyp zu vereinfachen. Pro Schnittstellentyp gibt es eine Richtlinienzuordnung. Dies spiegelt die Tatsache wider, dass nicht alle Warteschlangenmechanismen auf allen Schnittstellen unterstützt werden.

```
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
```

Die Richtlinienzuordnungen sind den jeweiligen Schnittstellen zugeordnet und beziehen sich auf Schnittstellentypen. So wird beispielsweise der Prozess zum Ändern des Warteschlangenmechanismus für VIP-basierte (VIP-basierte) Ethernet-Ports von WRED auf WFQ vereinfacht. Sie erfordert eine einzige Änderung in der Richtlinienzuordnung. Die Änderungen werden an allen VIP-basierten Ethernet-Schnittstellen vorgenommen.

```
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

Jede Schnittstelle mit Downstream-vertrauenswürdigen VoIP-Geräten ist für Low Latency Queuing (LLQ) konfiguriert. Jedes Paket, das die eingehende Schnittstellenklassifizierung durchläuft und eine Priorität von 5 behält, unterliegt der LLQ. Jedes andere Paket unterliegt entweder WFQ oder WRED. Dies hängt vom Schnittstellentyp ab.

Für jeden Schnittstellentyp werden separate Richtlinienzuordnungen erstellt, um die QoS-Verwaltung zu vereinfachen. Dies ähnelt dem Design für Warteschlangen ohne Sprachübertragung. Für jeden Schnittstellentyp stehen jedoch mehrere Richtlinienzuordnungen zur Verfügung. Dies liegt daran, dass die Kapazität der Schnittstellentypen für die Sprachübertragung je nach Verbindungsgeschwindigkeit, PVC-Einstellungen usw. variiert. Die Nummer im Richtlinienzuordnungsnamen gibt die Anzahl der Anrufe an, die für 30 Anrufe, 60 Anrufe usw. bereitgestellt werden.

```
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
```

Die Richtlinienzuordnungen sind den entsprechenden Schnittstellen zugeordnet. In diesem Beispiel ist die Richtlinienzuordnung spezifisch für einen Schnittstellentyp. Derzeit wird die Sprachsignalisierung nicht besonders behandelt. Die Richtlinienzuordnungen können problemlos an einem Ort geändert werden, wenn dies zu einem späteren Zeitpunkt für einen bestimmten Schnittstellentyp erforderlich wird. Die Änderung wirkt sich auf alle Schnittstellen dieses Typs aus.

```
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
```

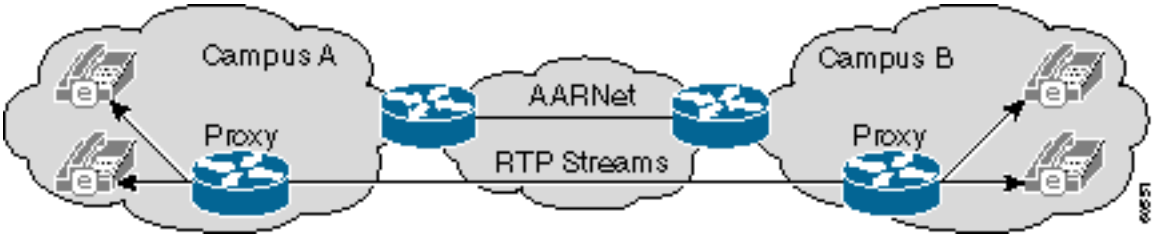
LLQ-Skalierbarkeit

Der Warteschlangenmechanismus weist einige Skalierbarkeitsprobleme auf. Das Hauptproblem besteht darin, dass die IP-Adresse jedes vertrauenswürdigen VoIP-Geräts im Netzwerk bekannt ist. Dies war in der Vergangenheit eine vernünftige Einschränkung, als es eine begrenzte Anzahl von VoIP-Gateways gab, die die Umgehung von Mautgebühren umsetzten. Die Anzahl der VoIP-Endpunkte nimmt drastisch zu und wird bei der Bereitstellung von IP-Telefonie immer unpraktischer. Die Zugriffskontrolllisten sind zu lang und zu schwer zu verwalten.

Die ACLs wurden angehängt, um Datenverkehr aus einem spezifischen Sprach-IP-Subnetz an jedem ACU-Campus im Fall von ACU zu vertrauen. Dies ist eine Zwischenlösung. Diese längerfristigen Lösungen werden derzeit geprüft:

- H.323-Proxy
- QoS-Eingangsüberwachung

Die Hauptidee der H.323-Proxy-Lösung besteht darin, den gesamten RTP-Datenverkehr über einen Proxy von einem bestimmten Campus in AARNet zu leiten. AARNet sieht den gesamten RTP-Verkehr von einem bestimmten Campus mit einer einzigen IP-Adresse, wie das folgende Diagramm zeigt:

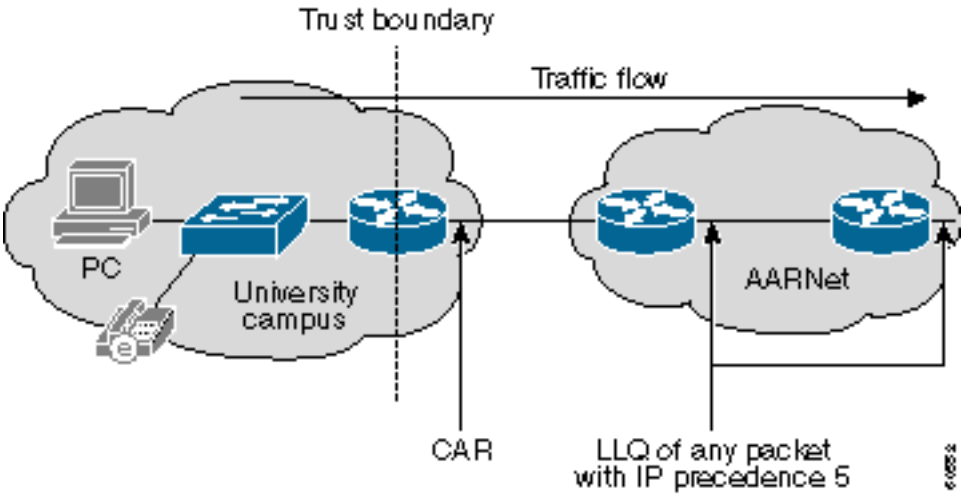


Die Anzahl der Einträge in den QoS-ACLs ist auf eine Zeile pro Campus beschränkt, wenn dieses Schema konsistent bereitgestellt wird. Dieses Programm kann noch bis zu 100 oder mehr Einträge enthalten, da es 37 Universitäten mit mehreren Universitäten gibt. Auch das ist nicht skalierbar. Es kann erforderlich sein, an jedem RNO ein Design mit einer einzigen oder einer begrenzten Anzahl gemeinsam genutzter Superproxys zu implementieren. Dadurch wird die Anzahl der vertrauenswürdigen IP-Adressen auf sechs reduziert. Dies führt jedoch zu einem Problem bei der QoS-Richtlinienvergabe auf dem Pfad vom Campus zum Proxy am RNO.

Hinweis: Cisco CallManager-Intercluster-Trunks funktionieren derzeit nicht über einen H.323-Proxy, da die Intercluster-Signalisierung kein natives H.225 ist.

Die QoS-Eingangsüberwachung ist eine alternative Lösung. An dem Punkt, an dem der Campus mit diesem Design eine Verbindung zum RNO herstellt, wird eine Vertrauensgrenze festgelegt. Der Datenverkehr, der in AARNet eingeht, wird an dieser Grenze durch die Cisco IOS® Committed Access Rate (CAR)-Funktion geregelt. Eine Universität, die AARNet für VoIP nutzt, zeichnet sich durch eine bestimmte AARNet-QoS-Bandbreite aus. Die CAR überwacht anschließend den Datenverkehr, der in AARNet eingeht. Bei überschüssigem Datenverkehr ist die IP-Priorität auf 0 herabgesetzt, wenn die Menge des RTP-Datenverkehrs mit der IP-Priorität 5 die abonnierte Bandbreite überschreitet.

Dieses Diagramm zeigt eine CAR-Konfiguration:



Dieses Beispiel zeigt, wie eine CAR-Konfiguration diese Richtlinien behandelt:

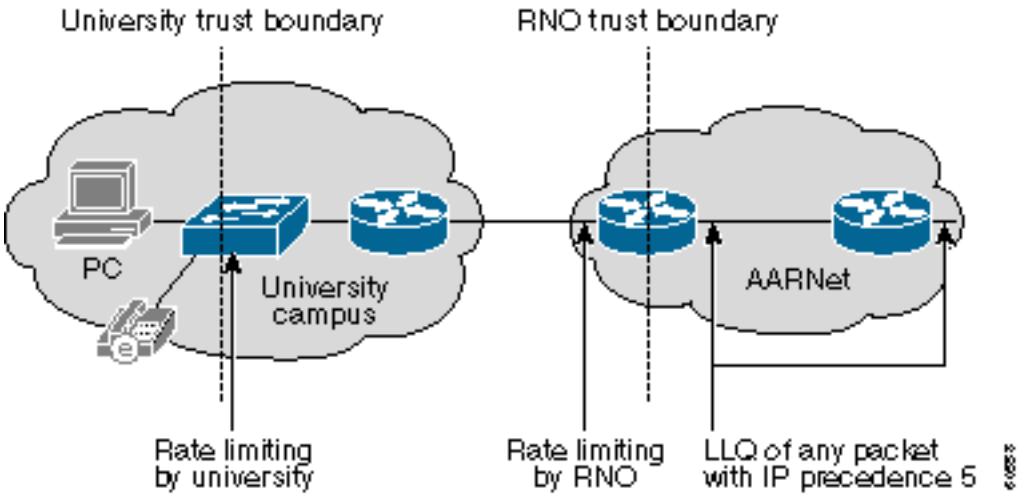
```
Interface a1/0.100
rate-limit input access-group 100 2400000 0 0 conform-action set-prec-transmit 5
exceed-action set-prec-transmit 0

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

Dies sind einige Vorteile eines CAR-Konfigurationsansatzes:

- Der Core muss nicht mehr mit der Richtlinienvergabe umgehen. Sie wird nun an der Vertrauensgrenze behandelt. Aus diesem Grund muss das LLQ im Core keine Informationen über vertrauenswürdige IP-Adressen enthalten. Jedes Paket mit einer IP-Priorität von 5 im Core kann sicher einem LLQ unterzogen werden, da es die Richtlinienvergabe bereits am Eingang bestanden hat.
- Über die VoIP-Architektur, die Geräte und die Protokolle, die von den einzelnen Universitäten ausgewählt werden, wird keine Aussage getroffen. Eine Universität kann entweder ein Session Initiation Protocol (SIP) oder ein Media Gateway Control Protocol (MGCP) bereitstellen, das nicht mit H.323-Proxys kompatibel ist. VoIP-Pakete erhalten die entsprechende QoS im Core, solange sie eine IP-Priorität von 5 haben.
- Die CAR ist gegen QoS-Denial-of-Service (DoS)-Angriffe gewappnet. Ein QoS-DoS-Angriff, der von einer Universität ausgeht, kann den Kern nicht beschädigen. CAR begrenzt den Angriff, der nicht mehr Datenverkehr erzeugen kann als der, der vorhanden ist, wenn die maximale Anzahl zulässiger VoIP-Anrufe aktiv ist.VoIP-Anrufe an oder von diesem Campus können während eines Angriffs leiden. Es ist jedoch Aufgabe der einzelnen Universität, sich intern zu schützen. Die Universität kann die CAR-ACLs auf dem Router straffen, sodass die IP-Priorität für alle VoIP-Subnetzwerke bis auf ausgewählte VoIP-Subnetzwerke markiert ist.Jeder Campus verfügt über eine interne Vertrauensgrenze, an der die Benutzer im ultimativen Design mit dem Campus-LAN verbunden sind. Datenverkehr mit einer IP-Rangfolge von 5, der von dieser Vertrauensgrenze empfangen wird, ist auf 160 Kbit/s pro Switch-Port oder zwei G.711-VoIP-Anrufe beschränkt. Datenverkehr, der diesen Tarif überschreitet, wird entsprechend gekennzeichnet. Für die Implementierung dieses Schemas sind Catalyst 6500-Switches oder ähnliche Funktionen mit Ratenbegrenzungsfunktionen erforderlich.
- Die Bandbreitenbereitstellung im Core vereinfacht die Bereitstellung, da jede Universität eine feste Menge an QoS-Bandbreite abonniert. Dies vereinfacht auch die QoS-Abrechnung, da jede Universität eine pauschale monatliche Gebühr auf der Grundlage eines QoS-Bandbreitenabonnements zahlen kann.

Die Hauptschwäche bei diesem Design besteht darin, dass sich die Vertrauensgrenze am Universitätsrouter befindet, sodass die Universitäten die CAR korrekt verwalten können müssen. Die Vertrauensgrenze wird wieder in das RNO zurückgezogen. RNO-verwaltete Geräte übernehmen die Richtlinienvergabe im ultimativen Design. Für dieses Design ist eine hardwarebasierte Ratenbegrenzung erforderlich, z. B. für den Catalyst 6000-Switch oder einen Cisco 7200 Network Services Engine (Cisco 7200 NSE-1)-Prozessor. Sie bietet AARNet und RNOs jedoch die vollständige Kontrolle über die QoS-Richtlinienvergabe. Dieses Diagramm zeigt dieses Design:



Link-Fragmentierung und -Verschachtelung

VoIP wird nur über relativ schnelle ATM Virtual Circuits (VCs) übertragen. Daher ist kein LFI erforderlich. VoIP kann auch über das Frame Relay Forum (FRF) übertragen oder später an ländliche Universitäten geleast werden. Hierfür sind LFI-Mechanismen wie Multilink PPP (MLP) mit Interleave oder FRF.12 erforderlich.

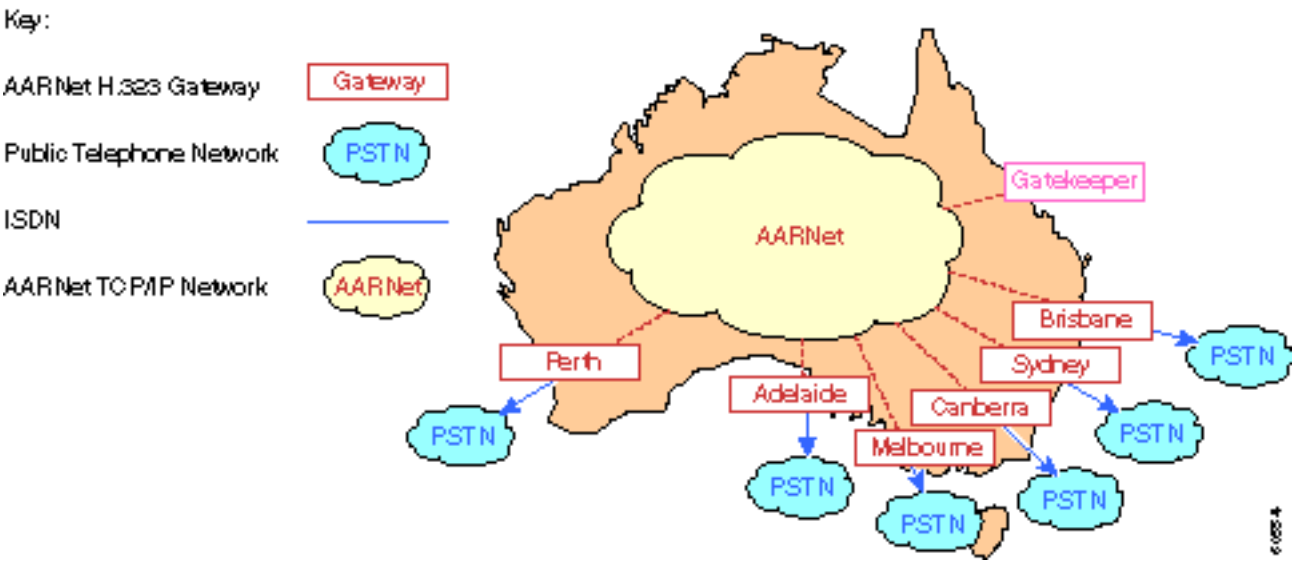
Gateways

Es gibt zwei Arten von H.323-Gateways in AARNet:

- PSTN - PSTN an VoIP-Gateway
- PABX - PABX an VoIP-Gateway

Die Unterscheidung zwischen einem PSTN- und einem PABX-Gateway ist in erster Linie funktionstüchtig. PSTN-Gateways stellen Verbindungen zum PSTN her. Die PABX-Gateways verbinden ein Universitäts-PABX mit dem VoIP-Backbone. In vielen Fällen fungiert dieselbe physische Box als PSTN- und PABX-Gateway. Die ACU IP-Telefonielösung umfasst derzeit 31 Gateways. Die meisten dieser Gateways sind Cisco AS5300 Universal Access Server. Die anderen Gateways sind Cisco Router der Serie 3600 oder Router der Serie 2600. Es wird erwartet, dass im 2. Quartal des Kalenderjahres 2001 mindestens zehn zusätzliche Gateways hinzugefügt werden. AARNet führte im April 2001 etwa 145.000 VoIP-Anrufe durch.

AARNet hat in den meisten Großstädten PSTN-verbundene H.323-Gateways bereitgestellt, wie das folgende Diagramm zeigt:



Universitäten können diese Gateways für ausgehende Anrufe an das PSTN verwenden. Universitäten müssen ihre eigenen Trunks für eingehende Anrufe verwalten, da sie derzeit nicht unterstützt werden. AARNet kann mit dem Betreiber einen sehr wettbewerbsfähigen Preis aushandeln, da die Anzahl der Anrufe über diese Gateways steigt. Anrufe können auch am kosteneffektivsten Ort abgebrochen werden. Beispielsweise kann jemand in Sydney, der eine Perth-Nummer anruft, das Perth-Gateway verwenden und nur für einen Ortsgespräch in Rechnung gestellt werden. Dies wird auch als Tail End Hop Off (TEHO) bezeichnet.

Es wird ein einziger Gatekeeper bereitgestellt, um die Auflösung von E.164- zu IP-Adressen durchzuführen. Alle Anrufe an das PSTN werden an den Gatekeeper gesendet, der dann die IP-Adresse des am besten geeigneten Gateways zurückgibt. Weitere Informationen zu Gatekeepers finden Sie in den Abschnitten Wählpläne und Gatekeeper.

Rechnungsstellung

Die PSTN-Gateways verwenden RADIUS und AAA (Authentication, Authorization, Accounting) für die Abrechnung. Jeder Anruf über ein Gateway generiert einen CDR (Call Detail Record) für jede Anrufkomponente. Diese CDRs werden auf dem RADIUS-Server bereitgestellt. Die IP-Adresse des Cisco CallManager im CDR identifiziert die Universität eindeutig und stellt sicher, dass die richtige Partei in Rechnung gestellt wird.

Gateway-Sicherheit

Der Schutz der PSTN-Gateways vor DoS-Angriffen und -Betrug ist ein wichtiges Anliegen. H.323-Clients sind weit verbreitet. Microsoft NetMeeting ist mit Microsoft Windows 2000 gebündelt, sodass es für nicht-technische Benutzer relativ einfach ist, über diese Gateways kostenlose Anrufe zu tätigen. Konfigurieren Sie eine eingehende ACL, die die H.225-Signalisierung von vertrauenswürdigen IP-Adressen zulässt, um diese Gateways zu schützen. Dieser Ansatz weist dieselben Skalierbarkeitsprobleme auf wie im QoS-Abschnitt beschrieben. Die Anzahl der Einträge in der ACL nimmt mit wachsender Anzahl vertrauenswürdiger H.323-Endpunkte zu.

H.323 Proxies bieten in diesem Bereich einige Erleichterung. Die Gateway-ACLs müssen eine IP-Adresse pro Universitätsgelände zulassen, wenn alle Anrufe über das PSTN-Gateway über einen Campus-Proxy geleitet werden. Zwei IP-Adressen als redundanter Proxy sind in den meisten Fällen wünschenswert. Selbst bei Proxys kann die ACL mehr als 100 Einträge enthalten.

Der Proxy muss über ACLs geschützt werden, da jedes H.323-Gerät einen Anruf über den Proxy

einrichten kann. Die Proxy-ACL muss lokale H.323-Geräte entsprechend den lokalen Richtlinien zulassen, da dies pro Campus geschieht.

Die IP-Adressen der beiden Cisco CallManager müssen in die Gateway-ACLs aufgenommen werden, wenn ein Campus nur Anrufe von IP-Telefonen zur Verwendung der AARNet-PSTN-Gateways zulassen möchte. Die Proxys fügen in dieser Situation keinen Wert hinzu. Die Anzahl der erforderlichen ACL-Einträge ist in beiden Richtungen gleich.

Beachten Sie, dass IP-Telefon-zu-IP-Anrufe zwischen Campus-Geräten nicht über den Proxy weitergeleitet werden müssen.

Wählpläne

Der aktuelle VoIP-Wählplan ist einfach. Benutzer können diese beiden Anrufe aus Sicht eines VoIP-Gateways tätigen:

- Rufen Sie ein Telefon an einem anderen Campus an, aber an derselben Universität.
- Rufen Sie ein PSTN-Telefon oder ein Telefon an einer anderen Universität an.

Die Gateway-DFÜ-Peers spiegeln die Tatsache wider, dass es nur zwei Arten von Anrufen gibt. Im Grunde gibt es zwei VoIP-DFÜ-Peer-Typen, wie im folgenden Beispiel gezeigt:

```
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
```

Der erste DFÜ-Peer wird verwendet, wenn jemand die Durchwahl 7 anruft.. an einem anderen Campus in diesem Beispiel. Dieser Anruf wird direkt an die IP-Adresse des Remote-Gateways weitergeleitet. Da der Gatekeeper umgangen wird, wird die Anrufzugangskontrolle (Call Admission Control, CAC) nicht ausgeführt.

Der zweite DFÜ-Peer wird verwendet, wenn es sich um einen Anruf für eine PSTN-Nummer handelt. Dabei kann es sich um eines der folgenden Elemente handeln:

- Die Nummer eines Telefons im PSTN
- Die vollqualifizierte PSTN-Nummer eines Telefons an einer anderen Universität

Der Anruf wird dem Gatekeeper im ersten Fall über eine Eintrittsanfrage (ARQ)-Nachricht zugestellt. Der Gatekeeper gibt die IP-Adresse des besten PSTN-Gateways in einer ACF-Nachricht (Admission confirm) zurück.

Der Anruf wird im zweiten Fall auch über eine ARQ-Nachricht an den Gatekeeper gesendet. Der Gatekeeper gibt jedoch eine ACF-Nachricht mit der IP-Adresse des VoIP-Gateways an der Universität zurück, die den Anruf empfängt.

Gatekeeper

AARNet betreibt derzeit einen einzigen Gatekeeper. Der einzige Zweck dieses Gatekeeper besteht in der Anrufweiterleitung in Form von E.164-IP-Adressen. Der Gatekeeper führt kein CAC aus. Die Anzahl der mit den Gateways verbundenen PABX-Trunks begrenzt die Anzahl

gleichzeitiger Anrufe. Die Kernbandbreite deckt alle gleichzeitig verwendeten Trunks ab. Dies ändert sich mit der Einführung von IP-Telefonie an der ACU und anderen Universitäten. Die Anzahl gleichzeitiger VoIP-Anrufe, die in einer bestimmten Campus-Umgebung ein- oder ausgelagert werden können, ist nicht natürlich begrenzt. Die verfügbare QoS-Bandbreite kann überbelegt werden, wenn zu viele Anrufe initiiert werden. Unter dieser Bedingung können alle Anrufe von schlechter Qualität sein. Verwenden Sie den Gatekeeper, um CAC bereitzustellen.

Die verteilte Struktur und potenzielle Größe des Sprachnetzwerks der Universität sind eine verteilte Gatekeeper-Architektur. Eine mögliche Lösung ist ein zweistufiges hierarchisches Gatekeeper-Design, in dem jede Universität ihren eigenen Gatekeeper unterhält. Dieser Gatekeeper an einer Universität wird als Tier-2-Gatekeeper bezeichnet. AARNet betreibt einen *Directory* Gatekeeper, der als Tier-1-Gatekeeper bezeichnet wird.

Universitäten müssen diesen zweistufigen Ansatz verwenden, um einen Gatekeeper für die Anrufweiterleitung zwischen Cisco CallManager-Clustern zu verwenden. Der Gatekeeper leitet in diesem Szenario Anrufe basierend auf einer 4- oder 5-stelligen Durchwahl weiter. Jede Universität benötigt einen eigenen Gatekeeper. Dies liegt daran, dass sich die Durchwahlbereiche zwischen Universitäten überschneiden, da es sich um einen lokal verwalteten Adressbereich handelt.

Die Stufe-2-Gatekeeper der Universität führen CAC nur für Anrufe an und von dieser Universität aus. Es führt auch eine E.164-Auflösung für Anrufe zwischen nur den Universitätsgeländen durch. Der Anruf wird vom Tier-2-Gatekeeper über eine LRQ-Nachricht (Location Request) an den Tier-1-Gatekeeper weitergeleitet, wenn jemand ein IP-Telefon an einer anderen Universität anruft oder das PSTN über ein AARNet-Gateway anruft. Der LRQ wird an den Tier-2-Gatekeeper der Universität weitergeleitet, wenn der Anruf für eine andere Universität eingeht. Dieser Gatekeeper gibt dann eine ACF-Nachricht an den Tier-2-Gatekeeper an der Universität zurück, von der der Anruf stammt. Beide Tier-2-Gatekeeper führen CAC durch. Sie nehmen den Anruf nur dann weiter vor, wenn für die anrufende und die angerufene Zone eine ausreichende Bandbreite verfügbar ist.

AARNet kann die AARNet-PSTN-Gateways wie die aller Universitäten behandeln. Ihr eigener Tier-2-Gatekeeper kümmert sich um sie. Der Tier-1-Gatekeeper kann auch als Tier-2-Gatekeeper für diese Gateways fungieren, wenn die Last und Leistung dies zulässt.

Jeder Gatekeeper (einschließlich des Verzeichnisgatekeeper AARNet) muss repliziert werden, da die Gateways eine so wichtige Komponente sind. Jede Universität muss über zwei Gatekeeper verfügen. Cisco IOS-Gateways können alternative Gatekeeper verwenden, wie z. B. bei Cisco IOS Software Release 12.0(7)T. Dies wird jedoch derzeit nicht von Cisco CallManager oder einem anderen H.323-Gerät eines Drittanbieters unterstützt. Verwenden Sie diese Funktion derzeit nicht. Verwenden Sie stattdessen eine einfache HSRP-basierte (Hot Standby Router Protocol-basierte) Lösung. Dazu müssen beide Gatekeeper im gleichen IP-Subnetz sitzen. HSRP bestimmt, welcher Gatekeeper aktiv ist.

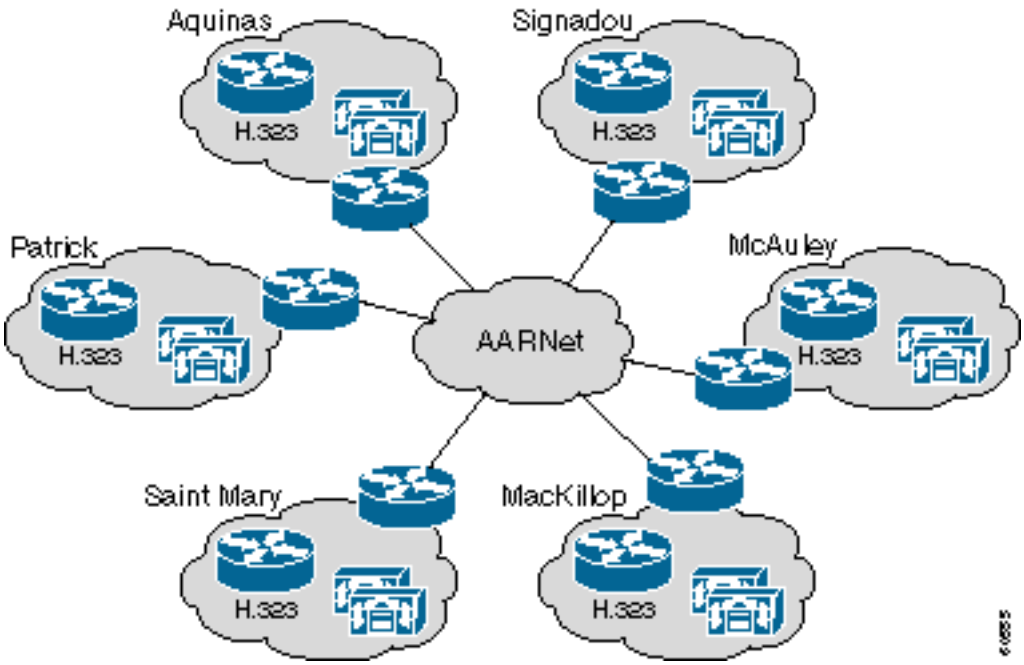
ACU IP-Telefonnetzwerk

Diese Tabelle zeigt die ungefähre Anzahl von IP-Telefonen, die auf den Campus der ACU installiert sind:

Campus	Stadt	Ungefähre IP-Telefone
Monte Saint Mary	Strathfield	400

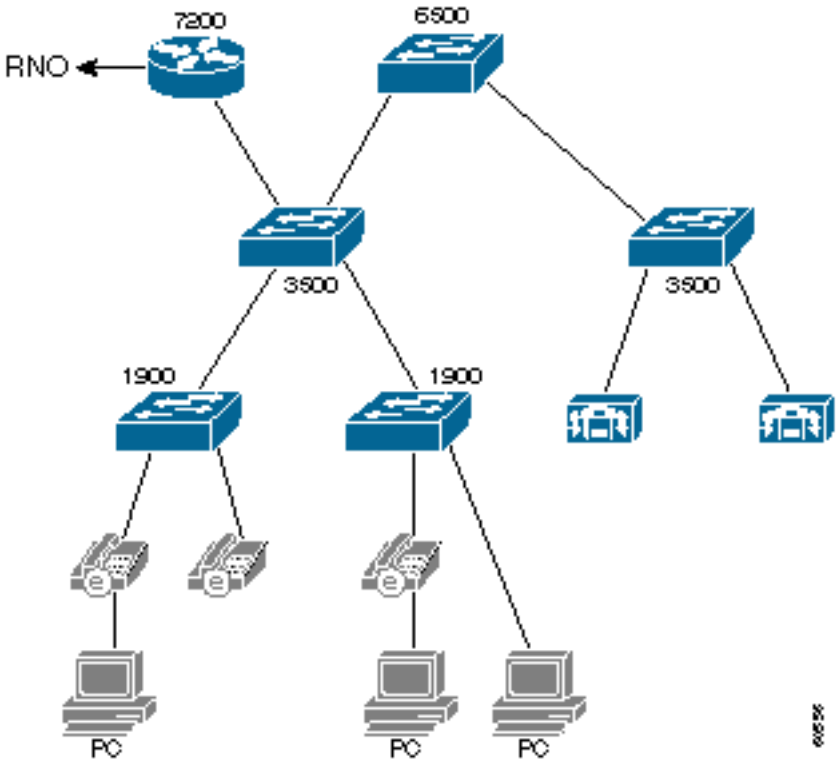
MacKillop	North Sydney	300
Patrick	Melbourne	400
Quinas	Ballarat	100
Signadou	Canberra	100
McAuley	Brisbane	400
	Gesamt:	***1700***

Die ACU hat kürzlich eine IP-Telefonielösung bereitgestellt. Die Lösung besteht aus einem Cluster aus zwei Cisco CallManagers, einem Cisco 3640-Gateway auf jedem Campus und IP-Telefonen. AARNet verbindet die Campus-Netzwerke. Dieses Diagramm zeigt die Topologie auf höchster Ebene und die verschiedenen Komponenten des ACU IP-Telefonienetzwerks:



ACU-Netzwerktopologie

Dieses Diagramm zeigt einen typischen ACU-Campus. Jeder Campus verfügt über drei Ebenen von Catalyst Switches. Im Verteilerschrank sind die älteren Catalyst 1900 Switches untergebracht. Die Catalyst 1900-Switches werden mittels Extended Framing wieder mit dem Catalyst 3500XL-Switch verbunden. Diese verbinden sich mittels Gigabit Ethernet (GE) mit einem einzigen Catalyst 6509 Switch. Ein einziger Cisco 7200 VXR-Router verbindet den Campus über eine ATM-VC mit der lokalen RNO mit dem AARNet.



Die Verbindungsmethode zum RNO unterscheidet sich je nach Zustand geringfügig, wie die folgende Tabelle zeigt. Victoria basiert auf dem klassischen IP over ATM (RFC 1577). Die anderen RNOs verfügen über eine gerade PVC-Konfiguration mit RFC 1483-Kapselung. Open Shortest Path First (OSPF) ist das Routing-Protokoll, das zwischen der ACU und den RNOs verwendet wird.

Campus	Staat	Verbindung mit RNO	Routing-Protokoll
Monte Saint Mary	NSW	RFC 1483 PVC	OSPF
MacKillop	NSW	RFC 1483 PVC	OSPF
Patrick	VIC	RFC 1577 Classical IP over ATM	OSPF
Quinas	VIC	RFC 1577 Classical IP over ATM	OSPF
Signadou	AKT	RFC 1483 PVC	OSPF
McAuley	QLD	RFC 1483 PVC	OSPF

Die Catalyst Switches der Serie 1900 unterstützen nur Trunking auf den Uplinks. Aus diesem Grund befinden sich die IP-Telefone und PCs alle in einem großen VLAN. Der gesamte Campus ist eine große VLAN- und Broadcast-Domäne. Aufgrund der großen Anzahl von Geräten werden sekundäre IP-Subnetze verwendet. Die IP-Telefone befinden sich in einem IP-Subnetz, die PCs in einem anderen. Der AARNet-Core vertraut dem Subnetz des IP-Telefons, und der Datenverkehr zu und von diesem IP-Subnetz unterliegt dem LLQ.

Der Cisco 7200 Router routet zwischen dem primären und dem sekundären IP-Subnetz. Die

Multilayer Switch Feature Card (MSFC) auf dem Catalyst 6500-Switch wird derzeit nicht verwendet.

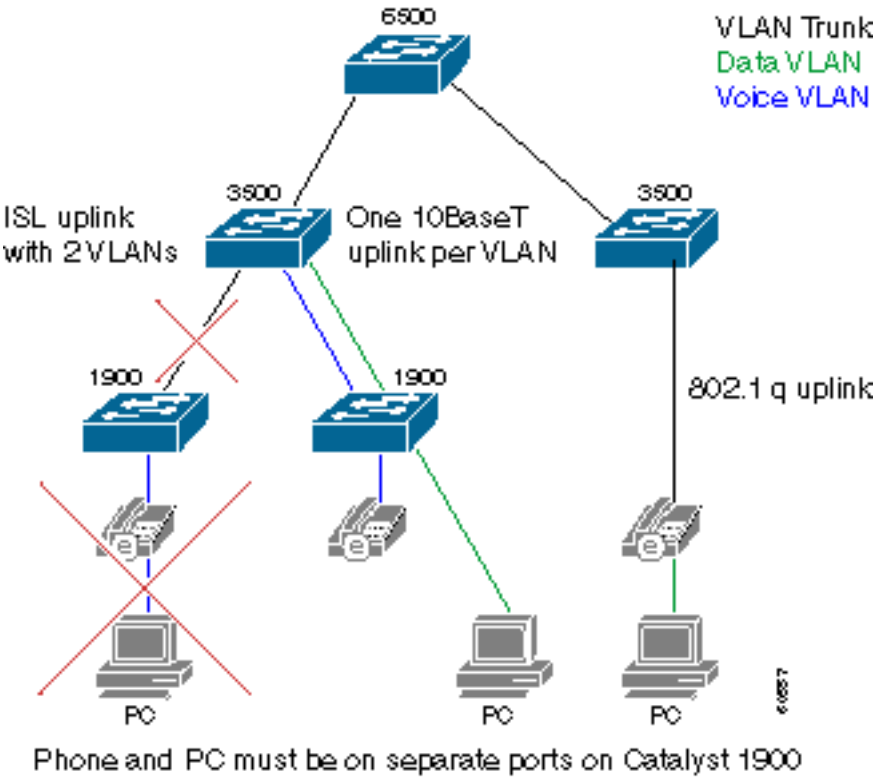
Die Catalyst Switches der Serien 3500XL und 6500 verfügen über QoS-Funktionen, sind jedoch derzeit nicht aktiviert.

QoS im Campus

Das aktuelle Campus-Design entspricht nicht den von Cisco empfohlenen Design-Richtlinien für IP-Telefonie. Dies sind einige Bedenken hinsichtlich QoS:

- Die Broadcast-Domäne ist sehr groß. Übermäßige Übertragungen können die Leistung von IP-Telefonen beeinträchtigen, die diese verarbeiten müssen.
- Die Catalyst 1900-Switches sind nicht QoS-fähig. Wenn ein IP-Telefon und ein PC mit demselben Switch-Port verbunden sind, können Sprachpakete verworfen werden, wenn der PC Daten mit hoher Geschwindigkeit empfängt.

Umgestaltung von Teilen der Campus-Infrastruktur, um deutliche Verbesserungen zu erzielen Ein Hardware-Upgrade ist nicht erforderlich. Dieses Diagramm veranschaulicht die Prinzipien, die der empfohlenen Umgestaltung zugrunde liegen:



Der Campus muss in ein Sprach-VLAN und ein Daten-VLAN aufgeteilt werden. Telefone und PCs, die mit einem Catalyst 1900-Switch verbunden sind, müssen nun mit verschiedenen Ports verbunden werden, um die VLAN-Trennung zu erreichen. Ein zusätzlicher Uplink von jedem Catalyst 1900-Switch zum Cisco 3500XL-Switch wird hinzugefügt. Einer der beiden Uplinks ist Teil des Sprach-VLANs. Der andere Uplink ist Mitglied des Daten-VLANs. Verwenden Sie kein InterSwitch Link (ISL)-Trunking als Alternative zu zwei Uplinks. Der Sprach- und Datenverkehr wird nicht über separate Warteschlangen bereitgestellt. Die GE-Verbindungen vom Catalyst 3500XL-Switch zum Catalyst 6000-Switch müssen ebenfalls in 802.1q-Trunks konvertiert werden, damit Sprach- und Daten-VLAN über diesen Core-Switch übertragen werden können.

Ports am Catalyst 3500XL-Switch, die sich im Daten-VLAN befinden, haben eine CoS-

Standardeinstellung (Class of Service) von Null. Ports, die Mitglieder des Sprach-VLANs sind, haben eine standardmäßige CoS von 5. Als Ergebnis wird der Sprachverkehr korrekt priorisiert, sobald er den Catalyst 3500- oder Catalyst 6500-Kern erreicht. Die Konfigurationen der Catalyst 3500 QoS-Switch-Ports variieren je nach Mitglied leicht, wie das folgende Beispiel zeigt:

```
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
```

Sie können einen PC an den hinteren Switch-Port des IP-Telefons anschließen, in seltenen Fällen, wenn IP-Telefone direkt mit einem Catalyst 3500XL-Switch verbunden werden. Die IP-Telefone werden in diesem Fall über einen 802.1q-Trunk mit dem Switch verbunden. Dadurch können Sprach- und Datenpakete auf separaten VLANs übertragen werden, und Sie können Paketen beim Eingang die richtige CoS zuweisen. Ersetzen Sie Catalyst 1900-Switches durch Catalyst 3500XL-Switches oder andere QoS-fähige Switches, sobald diese das Ende des Lebenszyklus erreicht haben. Diese Topologie wird dann zur Standardmethode für die Verbindung von IP-Telefonen und PCs mit dem Netzwerk. Dieses Szenario zeigt die Catalyst 3500XL Switch QoS-Konfiguration:

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

Schließlich sollte für die beiden Ports, die mit den beiden Cisco CallManager verbunden sind, die CoS auf 3 hardcodiert sein. Cisco CallManager legt die IP-Priorität in allen Sprachsignalisierungspaketen auf 3 fest. Die Verbindung vom Cisco CallManager zum Catalyst 3500XL-Switch verwendet jedoch nicht 801.1p. Daher wird der CoS-Wert am Switch erzwungen, wie im folgenden Beispiel gezeigt wird:

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

Die größte Hürde bei diesem Design besteht darin, dass am Desktop zwei Switch-Ports erforderlich sind. Der Patrick Campus benötigt möglicherweise zusätzliche 400 Switch-Ports für 400 IP-Telefone. Zusätzliche Catalyst 3500XL-Switches müssen bereitgestellt werden, wenn keine ausreichenden Ports verfügbar sind. Pro zwei fehlenden Catalyst 1900-Switch-Ports ist nur ein Catalyst 3500XL-Switch-Port erforderlich.

Die aktuellen ACU Catalyst Switches der Serie 6500 verfügen über QoS-Funktionen, sind jedoch derzeit nicht aktiviert. Diese Module sind im ACU Catalyst 6000 Switch mit folgenden Warteschlangenfunktionen vorhanden:

Steckplatz	Modul	Ports	RX-Warteschlangen	TX-Warteschlangen
1	WS-X6K-	2	1p1q4t	1p2q2t

	SUP1A-2GE			
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	—	—

Gehen Sie wie folgt vor, um die entsprechenden QoS-Funktionen auf dem Catalyst 6000 zu aktivieren:

1. Weisen Sie den Switch an, mit diesem Befehl QoS auf VLAN-basierter Basis bereitzustellen:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 vlan-based
   ```

2. Weisen Sie den Switch an, den CoS-Werten zu vertrauen, die er vom Catalyst 3500XL-Switch mit dem folgenden Befehl erhält:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos
   ```

Für die CoS muss jetzt die DSCP-Zuordnung (Differentiated Services Code Point) festgelegt werden. Dies ist erforderlich, da der Catalyst 6000-Switch den DSCP-Wert auf Basis des empfangenen CoS-Werts in den IP-Header umschreibt. VoIP-Signalisierungspakete müssen eine CoS von 3 haben, die mit einem DSCP von AF31 (26) neu geschrieben wird. RTP-Pakete müssen eine CoS von 5 haben, die mit einem DSCP von EF (46) neu geschrieben wird. Geben Sie den folgenden Befehl ein:

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

Verwenden Sie dieses Beispiel, um die Zuordnung von CoS zu DSCP zu überprüfen.

```
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
```

Konfigurieren Sie die MSFC für die Weiterleitung zwischen den verschiedenen IP-Subnetzwerken.

QoS im RNO

Das aktuelle RNO-Design entspricht nicht den von Cisco empfohlenen Design-Richtlinien für IP-Telefonie. Diese Bedenken bestehen in Bezug auf QoS:

- LLQ wird auf dem WAN-Router der Cisco ACU 7200-Serie nicht angewendet.

- Die Campus-Standorte Patrick und Aquinas verbinden sich mit dem RNO über ATM Switched VCs (SVCs). LLQ wird auf SVCs nicht unterstützt.

Ein Fast Ethernet-verbundener Cisco 7200-Router verbindet den Campus über eine E4 ATM-Verbindung mit 34 Mbit/s mit einem RNO. Der Datenverkehr kann an den 34-Millionen-Verbindungen möglicherweise in die Warteschlange nach oben gestellt werden, da die Geschwindigkeit 4 im Vergleich zu 100 Millionen nicht übereinstimmt. Daher muss der Sprachverkehr priorisiert werden. LLQ verwenden. Die Konfiguration des Cisco 7200-Routers ähnelt dem folgenden Beispiel:

```
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
```

Die dem LLQ zugewiesene Bandbreite muss *N x 24 Kbit/s* sein, wobei N die Anzahl gleichzeitiger G.729-Anrufe ist.

Richten Sie von jedem Patrick- und Aquinas-Cisco 7200-Router eine PVC zum AARNet-Router ein. ATM SVCs im Victoria RNO unterstützen LLQ nicht, da es auf dem klassischen IP over ATM (RFC 1577) basiert. Die anderen Universitäten im Victoria RNO können weiterhin RFC 1577 verwenden. Ersetzen Sie jedoch letztendlich die klassische IP over ATM-Infrastruktur.

Gateways

Jeder ACU-Standort verfügt über einen Cisco 3640-Router, der als H.323-Gateway fungiert. Diese Gateways verbinden sich über ISDN mit dem PSTN. Die Anzahl der primären Rate Interfaces (PRIs) und B-Kanäle hängt von der Größe des Campus ab. In dieser Tabelle ist die Anzahl der PRIs und B-Kanäle für jeden Campus aufgeführt:

Campus	PRI-Menge	B-Channel-Menge
Monte Saint Mary	2	30
MacKillop	2	50
Patrick	2	50
Quinas	1	20
Signadou	1	20
McAuley	1	30

Diese Gateways werden nur als sekundäre Gateways für DOD (Direct Outward Dialing) verwendet. Die AARNet-Gateways sind die primären Gateways. Die ACU-Gateways werden immer für DID (Direct Inward Dialing) verwendet.

Wählplan

Der Wählplan basiert auf vierstelligen Durchwahlnummern. Die Durchwahl ist auch die letzten vier Ziffern der DID-Nummer. In dieser Tabelle sind die Durchwahlbereiche und die DID-Nummern für jeden Campus aufgeführt:

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

Ein einfacher `Num-Exp`-Eintrag auf den Gateways spaltet die DID-Nummer auf die vierstellige Durchwahl ab, bevor sie an Cisco CallManager weitergeleitet wird. Der Patrick Campus Gateway hat beispielsweise folgenden Eintrag:

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

Benutzer wählen 0, um eine externe Leitung auszuwählen. Diese führende Null wird an das Gateway weitergegeben. Ein einzelner POTS-DFÜ-Peer leitet den Anruf auf Basis der führenden Null an den ISDN-Port weiter.

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

Eingehende Anrufe verwenden diesen Num-Exp-Eintrag, um die Nummer des angerufenen Teilnehmers in eine vierstellige Durchwahl umzuwandeln. Der Anruf stimmt dann mit beiden VoIP-DFÜ-Peers überein. Basierend auf der niedrigeren Präferenz wird diese Route dem Cisco CallManager-Teilnehmer vorgezogen:

```
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

Jeder Campus verfügt über einen Cluster, der aus zwei Cisco CallManager-Servern besteht. Die Cisco CallManager-Server sind eine Kombination aus Media Convergence Server 7835 (MCS-7835) und Media Convergence Server 7820 (MCS-7820). Beide Server hatten zum Zeitpunkt dieser Veröffentlichung Version 3.0(10). Ein Cisco CallManager ist der *Publisher*, der andere Cisco CallManager der *Subscriber*. Der Teilnehmer fungiert als primärer Cisco CallManager für alle IP-Telefone. In dieser Tabelle ist die Hardware aufgeführt, die auf den einzelnen Campus bereitgestellt wird:

Campus	Plattform	CallManager
Monte Saint Mary	MCS-7835	2
MacKillop	MCS-7835	2
Patrick	MCS-7835	2
Quinas	MCS-7820	2
Signadou	MCS-7820	2
McAuley	MCS-7835	2

Jeder Cluster ist mit zwei Regionen konfiguriert:

- Einer für Intracampus-Anrufe (G.711)
- Eine für standortübergreifende Anrufe (G.729)

Die standortbasierte CAC eignet sich nicht für die ACU, da sich alle von den einzelnen Clustern bedienten IP-Telefone auf einem einzigen Campus befinden. Eine auf Gatekeeper basierende CAC für Anrufe zwischen Campus-Geräten bietet Vorteile, ist jedoch derzeit nicht implementiert. Dies ist jedoch in naher Zukunft geplant.

Jeder Cisco CallManager ist mit 22 H.323-Gateways konfiguriert. Diese besteht aus Intercluster-Trunks zu den fünf anderen Cisco CallManager-Clustern, sechs AARNet-PSTN-Gateways und einem ACU-Gateway an jedem Campus.

Gerätetyp H.323	Menge
Intercampus CallManager	2 x 5 = 10
AARNet-PSTN-Gateway	6
ACU PSTN-Gateway	6
Gesamt:	*22*

Routenlisten und Routengruppen werden zum Rangieren der PSTN-Gateways verwendet. Diese Tabelle zeigt beispielsweise, wie Anrufe vom Patrick Cisco CallManager in Melbourne beim Sydney PSTN die vier Gateways nutzen können, um die Anrufe mit einer Routengruppe zu verknüpfen.

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

Die Cisco CallManager werden mit ca. 30 Weiterleitungsmustern konfiguriert, wie in der folgenden

Tabelle dargestellt. Die Routenmuster sind so konzipiert, dass es für alle nationalen australischen Nummern spezifische Übereinstimmungen gibt. Auf diese Weise müssen die Benutzer nicht warten, bis die Zeitüberschreitung zwischen den Ziffern abläuft, bevor der Anruf von Cisco CallManager initiiert wird. Das Platzhalterzeichen "!" wird nur im Routenmuster für internationale Nummern verwendet. Benutzer müssen warten, bis die Zeitüberschreitung zwischen den Ziffern (Standard-10 Sekunden) abläuft, bevor der Anruf weitergeht, wenn sie ein internationales Ziel wählen. Benutzer können auch das Routenmuster "0.0011!#" hinzufügen. Benutzer können dann nach der letzten Ziffer ein "#" eingeben, um Cisco CallManager mitzuteilen, dass die gewählte Nummer vollständig ist. Dadurch wird der internationale Wählvorgang beschleunigt.

Routenmuster	Beschreibung
0.[2-9]XXXXX	Lokaler Anruf
0.00	Notruf - wenn der Benutzer vergessen hat, die 0 für eine Amtsleitung zu wählen
0.000	Notruf
0.013	Verzeichnisunterstützung
0.1223	—
0.0011!	Auslandsgespräche
0,02XXXXXXX	Anrufe an New South Wales
0,03XXXXXXX	Anrufe nach Victoria
0,04XXXXXXX	Anrufe an Mobiltelefone
0,07XXXXXXX	Anrufe nach Queensland
0,086XXXXXX	Anrufe nach Westaustralien
0,08 XXXXXXX	Anrufe nach Südaustralien und Nord-Territorium
0,1[8-9]XXXXX	Anrufe an die Nummern 1800 xxx xxx und 1900 xxx xxx
0,144 x	Notfall
0,119[4-6]	Zeit und Wetter
0,1245 x	Verzeichnis
0,13[1-9]XXX	Anrufe an 13xxxx Nummern
0,130 XXXXXX	Anrufe an 1300 xxx xxx Nummern
2[0-1]XX	Clusterübergreifende Anrufe an Signadou
3[0-4]XX	Clusterübergreifende Anrufe an Patrick
5[3-4]XX	Clusterübergreifende Anrufe an Aquinas
7[2-5]XX	Clusterübergreifende Anrufe an McAuley
8[0-3]XX	Clusterübergreifende Anrufe an MacKillop
9[3-4]XX	Clusterübergreifende Anrufe an Mount Saint Mary
9[6-7]XX	Clusterübergreifende Anrufe an Mount Saint Mary

Die Anzahl der Gateways, Routengruppen, Weiterleitungslisten und Weiterleitungsmuster, die für die Cisco ACU CallManager konfiguriert wurden, kann auf eine große Anzahl von Geräten erweitert werden. Wenn ein neues RNO-Gateway bereitgestellt wird, müssen alle fünf Cisco CallManager-Cluster mit einem zusätzlichen Gateway neu konfiguriert werden. Noch schlimmer: Hunderte von Gateways müssen hinzugefügt werden, wenn ACU Cisco CallManager VoIP-Anrufe direkt an alle anderen Universitäten weiterleiten und das PSTN vollständig umgehen. Dies ist eindeutig nicht sehr gut skalierbar.

Die Lösung besteht darin, die Cisco CallManager Gatekeeper-Kontrolle zu erlangen. Sie müssen den Gatekeeper nur aktualisieren, wenn irgendwo im AARNet ein neues Gateway oder ein neuer Cisco CallManager hinzugefügt wird. Jeder Cisco CallManager darf nur das lokale Campus-Gateway und das anonyme Gerät konfigurieren, wenn dies geschieht. Sie können sich dieses Gerät als Punkt-zu-Mehrpunkt-Trunk vorstellen. Damit entfällt die Notwendigkeit vernetzter PPP-Trunks im Cisco CallManager-Wählplanmodell. Eine Routengruppe verweist auf das anonyme Gerät als bevorzugtes Gateway und auf das lokale Gateway als Backup-Gateway. Das lokale PSTN-Gateway wird für bestimmte lokale Anrufe sowie für allgemeine Off-Net-Anrufe verwendet, wenn der Gatekeeper nicht verfügbar ist. Derzeit kann das anonyme Gerät entweder intercluster oder H.225 sein, aber nicht beides gleichzeitig.

Cisco CallManager benötigt weniger Weiterleitungsmuster mit einem Gatekeeper als bisher. Grundsätzlich benötigt der Cisco CallManager nur ein einziges Routenmuster von "!" mit dem Gatekeeper. Tatsächlich muss die Art und Weise, wie Anrufe weitergeleitet werden, aus den folgenden Gründen genauer bestimmt werden:

- Einige Anrufe (z. B. Anrufe an 1-800 oder Notrufnummern) müssen über ein geografisch örtliches Gateway weitergeleitet werden. Jemand in Melbourne, der die Polizei wählt, oder eine Restaurantkette wie Pizza Hut will nicht mit der Polizei oder der Pizza Hut in Perth verbunden werden. Es werden spezifische Weiterleitungsmuster benötigt, die für diese Nummern direkt auf das PSTN-Gateway des lokalen Campus verweisen.Universitäten, die künftige IP-Telefoniebereitstellungen planen, können sich ausschließlich auf die AARNet-Gateways verlassen und keine eigenen Gateways verwalten. Diese Nummern müssen über eine virtuelle Ortsvorwahl verfügen, die von Cisco CallManager vorangestellt wird, bevor sie an den Gatekeeper gesendet werden, damit dieses Design für Anrufe funktioniert, die lokal abgebrochen werden müssen. Beispielsweise kann Cisco CallManager 003 für Anrufe von einem Melbourne-basierten Telefon an die Pizza Hut 1-800-Nummer vorleiten. Dadurch kann der Gatekeeper den Anruf an ein Melbourne-basiertes AARNet-Gateway weiterleiten. Das Gateway trennt die Nummer 003, bevor es den Anruf in das PSTN leitet.
- Verwenden Sie Weiterleitungsmuster mit spezifischen Übereinstimmungen für alle Inlandsnummern, um zu verhindern, dass der Benutzer vor der Initiierung des Anrufs auf das Interdigit-Timeout wartet.

Diese Tabelle zeigt die Weiterleitungsmuster für einen vom Gatekeeper gesteuerten Cisco CallManager:

Routenmuster	Beschreibung	Route	Gatekeeper
0.[2-9]XXXX	Lokaler Anruf	Routenliste	AARNet
0.00	Notruf	Lokales Gateway	None
0.000	Notruf	Lokales	None

		Gateway	
0.013	Verzeichnisunterstützung	Lokales Gateway	None
0.1223	—	Lokales Gateway	None
0.0011!	Auslandsgespräche	Routenliste	AARNet
0,0011!#	Auslandsgespräche	Routenliste	AARNet
0,0[2-4]XXXXXX	Anrufe an New South Wales, Victoria und Mobiltelefone	Routenliste	AARNet
0,0[7-8]XXXXXX	Anrufe nach Südaustralien, Westaustralien und Nordterritorium	Routenliste	AARNet
0,1[8-9]XXXXXX	Anrufe an die Nummern 1800 xxx xxx und 1900 xxx xxx	Lokales Gateway	None
0,144 x	Notfall	Lokales Gateway	None
0,119[4-6]	Uhrzeit und Wetter	Lokales Gateway	None
0,13[1-9]XXX	Anrufe an 13xxxx Nummern	Lokales Gateway	None
0,130 XXXXXXX	Anrufe an 1300 xxx xxx Nummern	Lokales Gateway	None
[2-3]XXX	Anrufe an Signadou	Routenliste	ACU
5. XXX	Anrufe an Aquinas	Routenliste	ACU
[7-9]XXX	Anrufe an McAuley, MacKillop und Mount Saint Mary	Routenliste	ACU

Der Gatekeeper leitet internationale Anrufe weiter, die nicht über das lokale Gateway gesendet werden. Dies ist wichtig, da AARNet in Zukunft internationale Gateways bereitstellen kann. Wenn in den Vereinigten Staaten ein Gateway bereitgestellt wird, können Universitäten dank einer einfachen Änderung der Gatekeeper-Konfiguration Anrufe zu US-Inlandstarifen in die USA tätigen.

Der Gatekeeper führt die clusterübergreifende Anrufweiterleitung basierend auf der vierstelligen ACU-Durchwahl durch. Dieser Adressbereich überschneidet sich höchstwahrscheinlich mit anderen Universitäten. Dies setzt voraus, dass die ACU einen eigenen Gatekeeper verwaltet und den AARNet-Gatekeeper als *Directory Gatekeeper* verwendet. Die Spalte Gatekeeper in dieser Tabelle gibt an, ob die Anrufweiterleitung vom ACU-Gatekeeper oder vom AARNet-Gatekeeper durchgeführt wird.

Hinweis: Der einzige Nachteil der vorgeschlagenen Gatekeeper-Lösung besteht darin, dass das anonyme Gerät derzeit entweder clusterübergreifend oder H.225 sein kann, aber nicht beide gleichzeitig. Cisco CallManager ist darauf angewiesen, dass der Gatekeeper Anrufe mit dem vorgeschlagenen Design an beide Gateways (H.225) und andere Cisco CallManager (Intercluster) weiterleitet. Die Lösung für dieses Problem besteht darin, entweder den Gatekeeper nicht für die clusterübergreifende Weiterleitung zu verwenden oder alle Anrufe über den Gatekeeper als H.225 zu behandeln. Die letztgenannte Problemumgehung bedeutet, dass bei clusterübergreifenden Anrufen möglicherweise einige zusätzliche Funktionen nicht verfügbar sind.

Voicemail

Die ACU verfügte vor der Migration zu IP-Telefonie über drei aktive Voice Reparate OS/2-basierte Voicemail-Server mit Dialogic-Telefonboards. Diese Server sollen in der IP-Telefonie-Umgebung wiederverwendet werden. Nach der Implementierung stellt jeder Repartee-Server über eine vereinfachte Message Desk Interface (SMDI) und eine Catalyst 6000 24-Port Foreign Exchange Station (FXS)-Karte eine Verbindung zu einem Cisco CallManager her. Auf diese Weise werden drei der sechs Campus Voicemail-Nachrichten erhalten, die drei Campus ohne Voicemail verlassen. Es ist nicht möglich, einen Repartee-Server zwischen den Benutzern in zwei Cisco CallManager-Clustern korrekt freizugeben, da es nicht möglich ist, die Nachrichtenanzeige (MWI) über den Intercluster-H.323-Trunk weiterzugeben.

Die ACU kann drei Cisco Unity-Server für die verbleibenden Standorte erwerben. Da diese Server auf Skinny-Basis betrieben werden, sind keine Gateways erforderlich. In dieser Tabelle sind die Voicemail-Lösungen für den Fall aufgeführt, dass die ACU die zusätzlichen Voicemail-Server erwirbt:

Campus	Voicemail-System	Gateway
Monte Saint Mary	Aktiver Sprach-Reparatur	Catalyst 6000 FXS mit 24 Ports
MacKillop	Aktiver Sprach-Reparatur	Catalyst 6000 FXS mit 24 Ports
Patrick	Aktiver Sprach-Reparatur	Catalyst 6000 FXS mit 24 Ports
Quinas	Cisco Unity	—
Signadou	Cisco Unity	—
McAuley	Cisco Unity	—

Die sechs Voicemail-Server fungieren in diesem Plan als isolierte Voicemail-Inseln. Es gibt kein Voicemail-Netzwerk.

Medienressourcen

Hardware-Digital-Signal-Prozessoren (DSPs) werden derzeit bei der ACU nicht bereitgestellt. Bei Konferenzen wird die softwarebasierte Konferenzbrücke im Cisco CallManager verwendet. Intercluster-Konferenzen werden derzeit nicht unterstützt.

Eine Umkodierung ist derzeit nicht erforderlich. Es werden nur G.711- und G.729-Codierer

verwendet, die von allen bereitgestellten Endgeräten unterstützt werden.

Fax- und Modemunterstützung

Fax- und Modemverkehr wird derzeit nicht vom ACU IP-Telefonienetzwerk unterstützt. Zu diesem Zweck plant die Universität die Verwendung der Catalyst 6000 FXS-Karte mit 24 Ports.

Softwareversionen

In dieser Tabelle sind die zum Zeitpunkt dieser Veröffentlichung verwendeten Softwareversionen aufgeführt:

Plattform	Funktion	Software-Version
CallManager	IP-Telefonanlage	3.0(10)
Catalyst 3500XL	Distribution-Switch	12.0(5.1)XP
Catalyst 6500	Core-Switch	5.5(5)
Catalyst 1900	Verteilerschrank-Switch	—
Cisco 7200-Prozessor	WAN-Router	12.1(4)
Cisco Router 3640	H.323-Gateway	12.1(3a)XI6

Zugehörige Informationen

- Unterstützung von Sprachtechnologie
- Produkt-Support für Sprach- und IP-Kommunikation
- Fehlerbehebung bei Cisco IP-Telefonie
- Technischer Support und Dokumentation für Cisco Systeme