

# ケーススタディ IP テレフォニーの導入 – ACU

## 内容

[概要](#)

[AARNet](#)

[AARNet のトポロジ](#)

[Quality of Service](#)

[ゲートウェイ](#)

[ダイヤルプラン](#)

[ゲートキーパー](#)

[ACU IP テレフォニー ネットワーク](#)

[ACU ネットワーク トポロジ](#)

[キャンパスにおける QoS](#)

[RNO における QoS](#)

[ゲートウェイ](#)

[ダイヤルプラン](#)

[Cisco CallManager](#)

[ボイス メール](#)

[メディア リソース](#)

[FAX とモデムのサポート](#)

[ソフトウェアのバージョン](#)

[関連情報](#)

## 概要

オーストラリア学術研究ネットワーク (AARNet) は、37 のオーストラリアの大学とオーストラリア連邦科学産業研究機構 (CSIRO) を相互接続する国際的な高速 IP ネットワークです。

AARNet は当初データ ネットワークとして構築されましたが、2000 年代前半から Voice over IP (VoIP) を伝送しています。現在導入されている VoIP ネットワークは、大学と CSIRO の自動式構内交換機 (PABX) の間で VoIP コールを伝送するトールバイパスソリューションです。また、公衆電話交換網 (PSTN) が最もコスト効率の高いポイントでホップオフできるようにする PSTN ゲートウェイも提供します。たとえば、メルボルンの PABX 電話機からシドニーの PSTN 電話機へのコールは、メルボルンからシドニーの PSTN ゲートウェイへの VoIP として伝送されます。このゲートウェイで PSTN に接続されます。

オーストラリア カトリック大学 (ACU) は、AARNet に接続する大学の 1 つです。ACU は 2000 年の後半に IP テレフォニー導入に着手し、6 か所の大学キャンパスに約 2,000 台の IP フォンを導入しました。

このケーススタディでは、ACU の IP テレフォニーの導入について説明します。このプロジェクトは完了しています。ただし、他の大学が ACU の先例にならい、ネットワークを拡張する場合、AARNet バックボーンで解決すべきアーキテクチャ上の重要な問題があります。このドキュメ

ントでは、これらの問題について説明し、さまざまな解決策を提示して説明します。ACU の IP テレフォニー導入環境は、最終的な推奨アーキテクチャに合わせて今後調整される可能性があります。

注：ディーキン大学は、オーストラリアで初めて IP テレフォニーを導入した大学です。ただし、ディーキン大学は IP テレフォニー トราフィックの伝送に AARNet を使用していません。

## AARNet

オーストラリアの各大学と CSIRO は 1990 年、オーストラリア大学学長評議会 ( AVCC ) により AARNet を構築しました。最初の数年間は、オーストラリアのインターネット トラフィックの 99% は、設立メンバーによるものでした。わずかな商用トラフィックは、教育研究分野と密接に関係する組織からのものでした。1994 年後半までに、AARNet 以外のユーザベースによる使用量は、トラフィック全体の 20% に増加しました。

AVCC は 1995 年 7 月に AARNet の商用顧客ベースを Telstra に売却しました。これが、最終的に Telstra Bigpond となる組織の始まりです。これにより、オーストラリアにおけるインターネットの商用利用と個人利用の増加が促進されました。この知的財産と専門知識の移転によって、オーストラリアのインターネットが発展しました。この移転がなければ、これほど急速な発展を遂げることはなかったでしょう。

AVCC は、1997 年前半に AARNet2 を開発しました。これによりオーストラリアのインターネットはさらに洗練され、広帯域幅 ATM リンクと、Cable & Wireless Optus (CWO) Limited との契約によるインターネット サービスが採用されました。AARNet2 の要件に対応するために CWO が迅速に IP サービスを導入できた理由の 1 つに、AARNet からの専門知識の移転があります。

## ACU

ACU は 1991 年に設立された公立大学です。約 10,000 名の学生と 1,000 名のスタッフが在籍しています。オーストラリア東海岸に 6 つのキャンパスがあります。次の表に、ACU のキャンパスとその所在地を示します。

キャンパス	都市	都道府県
Mount Saint Mary	ストラスフィールド	New South Wales ( NSW )
MacKillop	North Sydney	New South Wales ( NSW )
Patrick	メルボルン	ビクトリア ( VIC )
Aquinas	バララット	ビクトリア ( VIC )
Signadou	キャンベラ	オーストラリア首都特別地域 ( ACT )
McAuley	ブリスベン	クイーンズランド ( QLD )

ACU は、このケース スタディで解説する IP テレフォニーのロールアウト前には Telstra Spectrum ( Centrex ) ソリューションを利用していました。IP テレフォニーへの移行が推進された主な理由は、コスト削減が求められていたことにあります。

## CSIRO

CSIRO は、オーストラリア国内の多数の施設を擁し、6,500 名のスタッフが在籍しています。CSIRO は農業、鉱業、エネルギー、製造業、通信、建設、保健、環境といったさまざまな分野の研究を進めています。

CSIRO は、VoIP に AARNet を使用した初の機関です。CSIRO は、この分野での初期の開発に先駆的に取り組みました。

## AARNet

AARNet バックボーンは、大学における IP テレフォニー導入の重要な構成要素です。音声分野の 2 つの主要なサービスにより、大学間の相互接続を実現します。

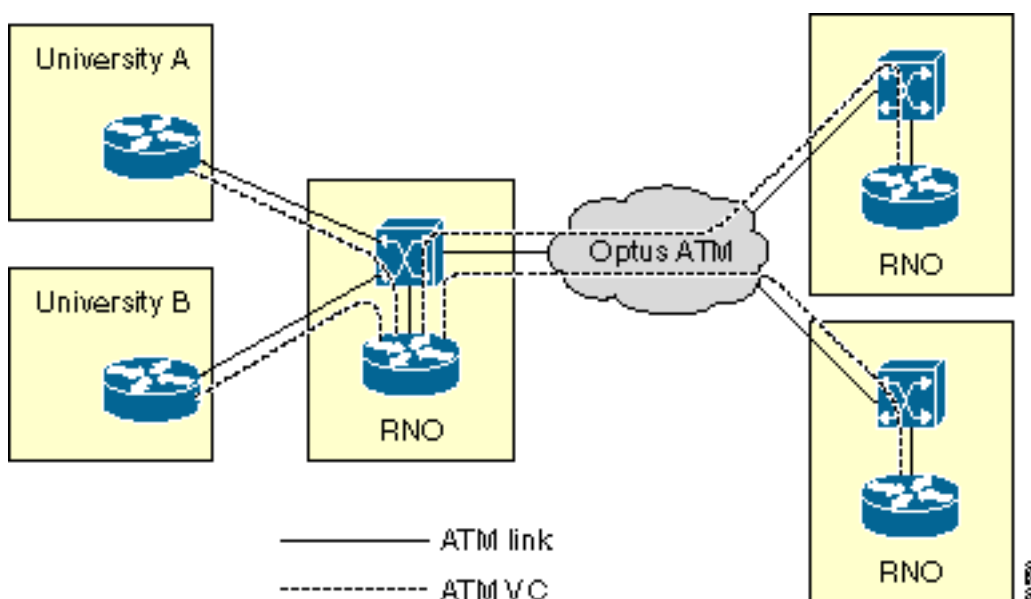
- 音声に適した Quality of Service ( QoS ) を保証する VoIP Realtime Transport Protocol ( RTP ) パケット転送
- 国内の PSTN への低コスト ホップオフ ポイント

ここでは、現在の AARNet アーキテクチャと、このアーキテクチャでこれらのサービスがどのように提供されるかについて説明します。また、IP テレフォニーソリューションを導入する大学の増加に伴って発生するスケーラビリティの問題の一部についても概説します。最後に、これらのスケーラビリティの問題に対する解決策について説明します。

## AARNet のトポロジ

AARNet は、州ごとに 1 つの POP ( Point of Presence ) で構成されています。POP は Regional Network Operations ( RNO ) とも呼ばれます。各大学は当該州の RNO に接続しています。各 RNO は、Optus ATM PVC からなるフル メッシュによって相互接続されます。これらが AARNet を構成しています。

典型的な RNO は、1 台の Cisco LS1010 ATM スイッチと 1 台の ATM 接続ルータで構成されます。RNO ルータは、E3 マイクロ波リンクを介して 1 つの ATM PVC により各大学のルータに接続します。各 RNO ルータは、Optus ATM ネットワークがその他のすべての RNO に提供する ATM PVC からなるフル メッシュにも接続しています。次の図に、このネットワークの一般的な AARNet トポロジを示します。



このトポロジにはさまざまな例外があります。一部の例外は、音声の点で重要です。いくつかの例外について次に説明します。

- ビクトリア州の RNO は、各大学を RNO に接続するために PVC ではなく Classical IP over ATM ( RFC 1577 ) を採用しています。
- 地方の大学は通常、フレーム リレーまたは ISDN により RNO に接続します。
- 一部の大規模な大学では、RNO へ複数のリンクで接続しています。

次の表に、現在 RNO が導入されている州および準州を示します。この表には、オーストラリアの地理について詳しくない読者のために州都も記載されています。

都道府県	州都	RNO ?	キャンパスの接続
ニューサウスウェールズ	シドニー	Yes	TBD
ビクトリア	メルボルン	Yes	TBD
クィーンズランド	ブリスベン	Yes	TBD
サウスオーストラリア	Adelaide	Yes	TBD
ウェスタンオーストラリア	Perth	Yes	TBD
オーストラリア首都特別地域	キャンベラ	Yes	TBD
ノーザンテリトリー	Darwin	No	—
タスマニア	Hobart	No	—

## Quality of Service

AARNet の一部では、VoIP トール バイパス プロジェクトにより、すでに音声 QoS に対応しています。QoS は、遅延やジッタを最小限に抑え、パケット損失を排除する次の機能を提供するために、音声トラフィックで必要です。

- ポリシング：信頼できない発信元からの音声トラフィックをマークダウンします。
- キューイング：リンク輻輳発生時に遅延を最小限に抑えるため、その他のすべてのトラフィックよりも音声優先される必要があります。
- Link Fragmentation and Interleaving ( LFI )：低速リンクでは、データ パケットはフラグメント化され、音声パケットはインターリーブされる必要があります。

音声パケットを適切にポリシングおよびキューイングするため、トラフィックを分類する必要があります。ここでは、AARNet でどのように分類が行われるかを説明します。後続の章では、ポリシングとキューイングの実装について説明します。

## 分類

すべてのトラフィックに同一の QoS が適用されるわけではありません。QoS を選択的に提供するため、トラフィックは次のカテゴリに分類されます。

- Data
- 既知の信頼できる発信元からの音声
- 不明な発信元からの音声

AARNet では、信頼されているデバイスだけに高品質 QoS が提供されます。これらのデバイスは主に、IP アドレスにより識別されるゲートウェイです。アクセスコントロール リスト

( ACL ) を使用して、これらの信頼できる音声発信元を識別します。

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

IP プレシデンスを使用して、データトラフィックと音声トラフィックを区別します。音声の IP プレシデンスは 5 です。

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

前述の例を組み合わせて、信頼できる発信元からのパケットを識別します。

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

不明な発信元からの音声パケットの識別にも同じ原則が適用されます。

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

## ポリシング

信頼できない発信元からの音声トラフィックは、インターフェイスに着信した時点で分類され、マークダウンされます。次の 2 つの例では、特定のインターフェイスで着信が予期されるトラフィックのタイプに応じて、どのようにポリシングが実行されるかを示しています。

信頼できる音声発信元がダウンストリームにある場合、ルータは信頼できない音声パケットを検索し、それらのパケットの IP プレシデンスを 0 に変更します。

```
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
```

既知の音声発信元がダウンストリームにない場合、ルータはすべての音声パケットを検索し、それらのパケットの IP プレシデンスを 0 に変更します。

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

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

## 音声以外のキューイング

AARNet では、最近まですべての VoIP がツールバイパスでした。このため、VoIP エンドポイントの数が比較的少数でした。現在のキューイングの設計では、VoIP デバイスがダウンストリーム

にあるインターフェイスと、そうでないインターフェイスが区別されます。ここでは、非 VoIP インターフェイスでのキューイングについて説明します。

音声以外のインターフェイスは、重み付け均等化キューイング (WFQ) または重み付けランダム早期検出 (WRED) のいずれかに対応して設定されています。これらは、インターフェイス上で直接設定できます。ただし、特定のインターフェイスタイプでキューイングメカニズムを容易に変更できるようにするため、キューイングメカニズムはポリシーマップを使用して適用されます。インターフェイスタイプごとに1つのポリシーマップがあります。これは、すべてのキューイングメカニズムがすべてのインターフェイスでサポートされるわけではないことを反映しています。

```
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
```

ポリシーマップはインターフェイスタイプに固有であり、該当するインターフェイスに関連付けられています。たとえば、このことにより、WRED から WFQ への Versatile Interface Processor ベース (VIP ベース) イーサネットポートにおけるキューイングメカニズム変更プロセスが簡素化されます。このためには、ポリシーマップで1つの変更を行う必要があります。変更はすべてのVIPベースイーサネットインターフェイスに反映されます。

```
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
```

## 低遅延キューイング

ダウンストリームに信頼される VoIP デバイスがあるインターフェイスはすべて、低遅延キューイング (LLQ) に対して設定されます。着信インターフェイス分類を通過し、プレシデンス 5 を維持するパケットはすべて、LLQ の対象となります。その他のパケットはすべて WFQ または WRED の対象となります。これはインターフェイスのタイプによって異なります。

QoS の管理を容易にするため、インターフェイス タイプごとに個別のポリシー マップが作成されます。これは、音声以外のキューイングの設計と似ています。ただし、インターフェイス タイプごとに複数のポリシー マップが存在します。これは、各インターフェイス タイプの音声トラフィック伝送キャパシティが、リンク速度、PVC 設定などに応じて異なるためです。ポリシー マップ名の番号は、処理するコールの数 (30 コール、60 コールなど) を反映しています。

```
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
```

ポリシー マップは該当するインターフェイスに関連付けられています。次の例では、ポリシー マップが 1 つのインターフェイス タイプに限定されています。現時点では、音声シグナリングには特別な処理は行われません。今後、特定のインターフェイス タイプでこれが必須となる場合には、ポリシー マップを 1 か所で容易に変更できます。この変更は、そのタイプのすべてのインター

フェイスに反映されます。

```
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
```

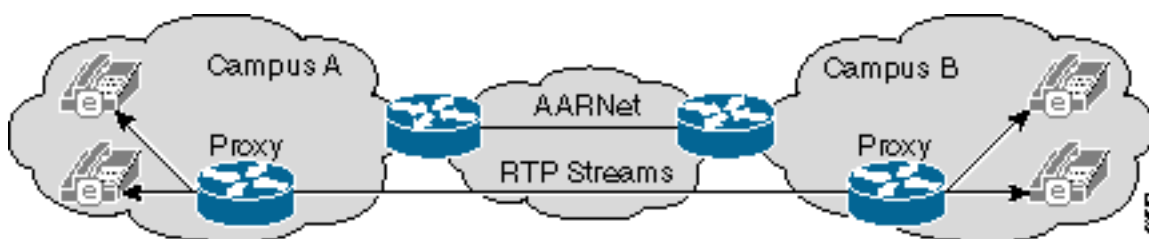
## LLQ の拡張性

キューイング メカニズムには、拡張性の問題がいくつかあります。主な問題は、このメカニズムが、ネットワーク上の信頼できるすべての VoIP デバイスの IP アドレスを認識していることを前提としている点です。これは、過去にトールバイパスを処理する VoIP ゲートウェイの数が限られていた状況では、妥当な制約事項でした。VoIP エンドポイントの数が飛躍的に増加しており、また IP テレフォニーの導入に伴ってこれは非現実的になってきています。ACL が大きくなりすぎ、管理が困難になります。

ACU のケースでは、ACU の各キャンパスにおける特定の音声 IP サブネットワークからのトラフィックを信頼するため、ACL が付加されました。これは暫定的な解決策です。次の長期的な解決策が現在調査検討されています。

- H.323 プロキシ
- QoS 入力ポリシング

H.323 プロキシによる解決策は、特定のキャンパスからのすべての RTP トラフィックを、プロキシ経由で AARNet に流入させるという構想に基づいています。次の図に示すように、AARNet では、特定のキャンパスからのすべての RTP トラフィックは 1 つの IP アドレスで認識されます。



この方式を一貫して導入する場合、QoS ACL のエントリの数は、キャンパスあたり 1 行に制限されます。ただしこの方式でも、37 の大学が複数のキャンパスを抱えている状況では、エントリの数が 100 以上になる可能性があります。この方式にも拡張性がありません。各 RNO に 1 つまたは限られた数の共有スーパープロキシを導入する設計に移行することが必要となる可能性があります。これにより、信頼できる IP アドレスの数が 6 に減ります。ただしこの方法では、キャンパスから RNO のプロキシまでのパスで QoS ポリシングの問題が発生する可能性があります。

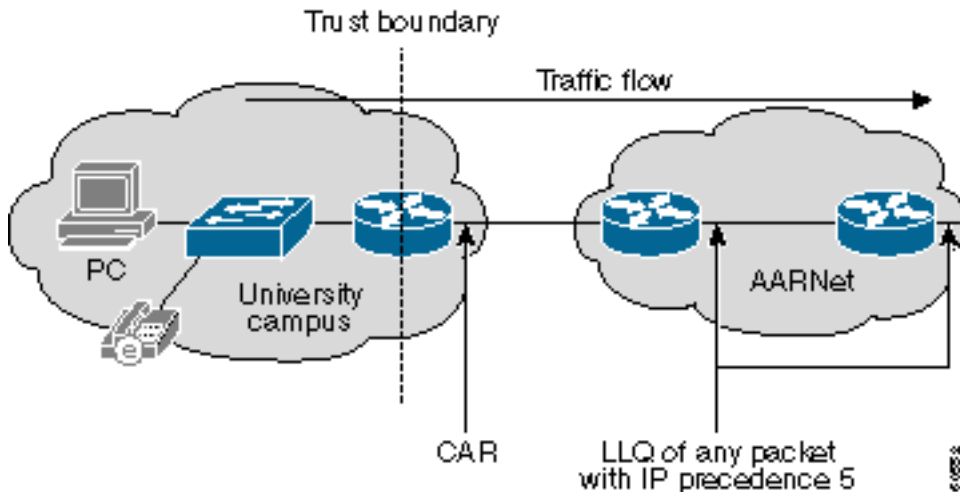
注：Cisco CallManager クラスタ間トランクは、現在、H.323 プロキシを介して動作しません。こ



これは、クラスタ間シグナリングがネイティブH.225ではないためです。

その代替となる解決策は QoS 入力ポリシングです。この設計では、キャンパスが RNO に接続するポイントで信頼境界が確立されます。AARNetに入るトラフィックは、この境界でCisco IOS® Committed Access Rate(CAR)機能によってポリシングされます。VoIP に AARNet を利用する大学は、一定量の AARNet QoS 帯域幅をサブスクライブします。CAR は AARNet に流入するトラフィックをモニタします。IP プレシデンスが 5 の RTP トラフィックの量がサブスクライブされた帯域幅を超えると、超過トラフィックの IP プレシデンスは 0 にマークダウンされます。

次の図に、CAR 構成を示します。



次の例に、CAR 構成によるこのポリシングの処理方法を示します。

```
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
```

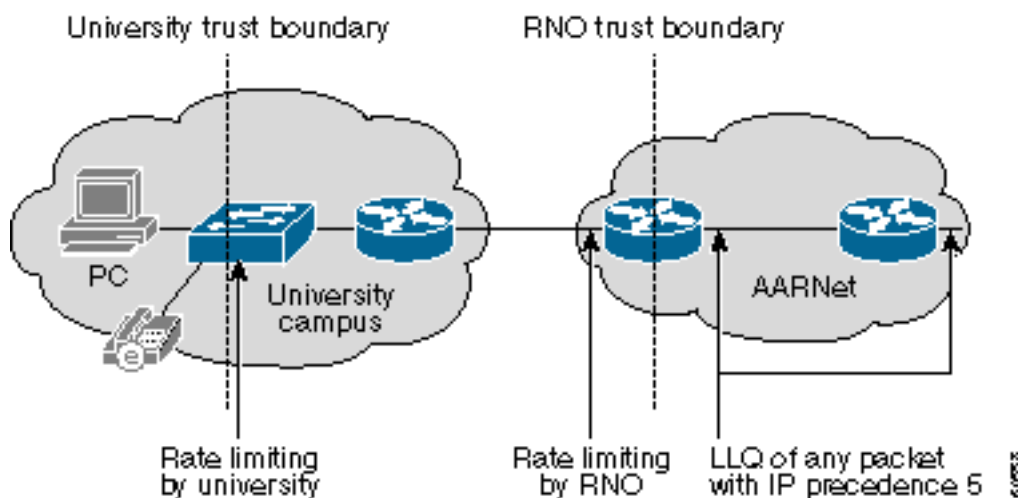
CAR 構成アプローチのメリットを次に示します。

- コアでポリシングを処理する必要がありません。これは信頼境界で処理されます。したがって、コアの LLQ が信頼できる IP アドレスを認識する必要はありません。コアの IP プレシデンス 5 のパケットはすべて、安全に LLQ の対象にできます。これは、そのようなパケットはすでに入力時にポリシングを通過しているためです。
- 各大学が選定する VoIP アーキテクチャ、機器、プロトコルについての前提条件はありません。各大学は、H.323 プロキシでは機能しない Media Gateway Control Protocol ( MGCP ) や Session Initiation Protocol ( SIP ) を導入することを選択できます。VoIP パケットの IP プレシデンスが 5 である限り、その VoIP パケットにはコアで適切な QoS が適用されます。
- CAR は、QoS サービス妨害 ( DoS ) 攻撃に対する回復力があります。大学から発生した QoS DoS 攻撃によってコアが損害を受けることはありません。CAR によりこの攻撃が制限されるため、最大数の許可 VoIP コールがアクティブな場合のトラフィック量を超えるトラフィックが生成されることはありません。攻撃中は、キャンパスから発信される VoIP またはキャンパスに着信する VoIP が影響を受けることがあります。ただし、内部での保護は各大学に委ねられています。大学は、選択されている VoIP サブネットワーク以外のすべての VoIP サブネットワークの IP プレシデンスをマークダウンするために、ルータの CAR ACR

を制限できます。各キャンパスの内部信頼境界は、最終的な設計においてユーザがキャンパス LAN に接続するポイントにあります。この信頼境界で受信される IP プレシデンス 5 のトラフィックは、スイッチポートあたり 160 kbps、または 2 つの G.711 VoIP コールに制限されています。このレートを超えるトラフィックはマークダウンされます。この方式を導入するには、Catalyst 6500 スイッチまたはレート制限機能を備えた類似のスイッチが必要です。

- 各大学が一定量の QoS 帯域幅をサブスクライブするため、コアでの帯域幅プロビジョニングが簡素化されます。また、各大学は QoS 帯域幅サブスクリプションに基づく月次定額料金を支払うことができるため、QoS に関する請求が簡素化されます。

この設計における主な弱点は、信頼境界が各大学のルータに位置しているため、各大学が CAR を正しく管理できなければならない点です。信頼境界は RNO に戻されます。最終的な設計では、RNO により管理される機器でポリシングが処理されます。この設計では、ハードウェアベースのレート制限 (Catalyst 6000 スイッチまたは Cisco 7200 Network Services Engine (Cisco 7200 NSE-1) プロセッサなど) を必要とします。ただし、AARNet と RNO が QoS ポリシングを完全に制御できます。この設計を次の図に示します。



## [Link Fragmentation and Interleaving](#)

VoIP は、比較的高速な ATM 仮想回線 (VC) でのみ伝送されます。したがって LFI は必要ありません。今後、VoIP はフレームリレーフォーラム (FRF) または専用回線で地方の大学へ伝送可能になります。このためには、LFI メカニズム (インターリーブまたは FRF.12 によるマルチリンク PPP (MLP) など) が必要です。

## [ゲートウェイ](#)

AARNet には 2 種類の H.323 ゲートウェイがあります。

- PSTN : VoIP ゲートウェイへの PSTN
- PABX : VoIP ゲートウェイへの PABX

PSTN ゲートウェイと PABX ゲートウェイの違いは、主にその機能にあります。PSTN ゲートウェイは、PSTN への接続を提供します。PABX ゲートウェイは、大学の PABX を VoIP バックボーンに接続します。多くの場合、1 つの物理ボックスが、PSTN ゲートウェイおよび PABX ゲートウェイの両方として機能します。ACU の IP テレフォニーソリューションでは、現在 31 のゲートウェイが導入されています。これらのゲートウェイのほとんどは、Cisco AS5300 ユニバーサルアクセスサーバです。他のゲートウェイは Cisco 3600 シリーズルータまたは Cisco 2600 シリーズルータです。2001年第2四半期には、ゲートウェイの追加が10件以上予定されています。AARNetは、2001年4月に約145,000件のVoIPコールを伝送しました。

次の図に示すように、AARNet では、ほとんどの主要都市に PSTN 接続 H.323 ゲートウェイを導入しています。

Key:

AARNet H.323 Gateway

Gateway

Public Telephone Network

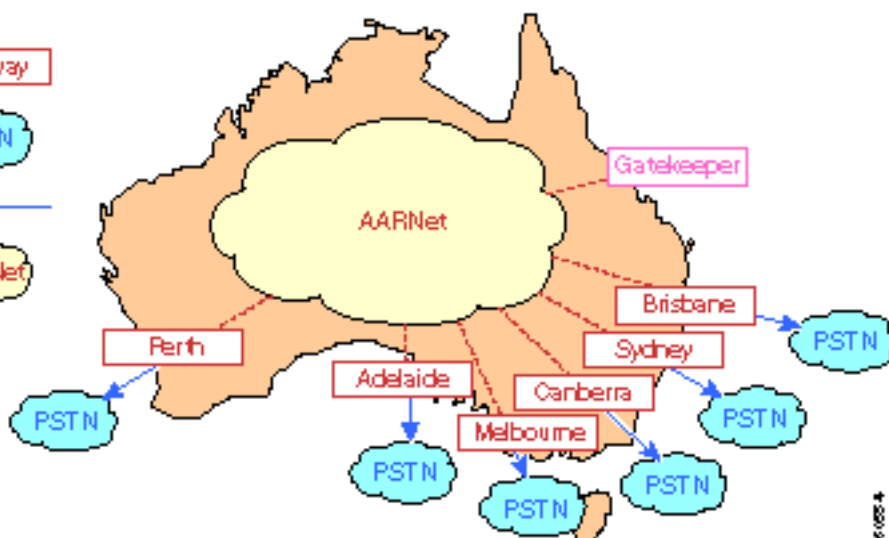
PSTN

ISDN

ISDN

AARNet TCP/IP Network

AARNet



各大学はこれらのゲートウェイを使用して PSTN に発信コールを実行できます。着信コール用のトランクは現在サポートされていないため、各大学は着信コール用に各自のトランクを維持する必要があります。AARNet は、これらのゲートウェイを通過するコールの量から、通信事業者との間で非常に優れた価格を交渉できます。コスト効率が高いポイントでは、コールガドロップオフする可能性もあります。たとえば、シドニーのユーザがパースの電話番号をコールする場合、パースのゲートウェイを使用することで、請求される通話料が市内通話料金になります。これはテール エンド ホップ オフ (TEHO) とも呼ばれます。

IP アドレス解決のために E.164 を実行する目的で、1 つのゲートキーパーが導入されています。PSTN へのコールはすべてこのゲートキーパーに送信され、このゲートキーパーから最も適切なゲートウェイの IP アドレスが返されます。ゲートキーパーの詳細については、[「ダイヤルプラン」](#)と[「ゲートキーパー」](#)の項を参照してください。

## [請求とアカウントティング](#)

PSTN ゲートウェイは、RADIUS と認証、認可、およびアカウントティング (AAA) を請求処理に使用します。ゲートウェイを経由する各コールは、コール レッグごとにコール詳細レコード (CDR) を生成します。これらの CDR は RADIUS サーバに送信されます。CDR の Cisco CallManager の IP アドレスは大学を一意に識別し、これにより正しい当事者に対して請求が行われます。

## [ゲートウェイ セキュリティ](#)

DoS 攻撃や不正行為からの PSTN ゲートウェイの保護は、大きな課題です。H.323 クライアントが広く利用されています。Microsoft NetMeeting は Microsoft Windows 2000 にバンドルされています。したがって、技術的な知識がないユーザでも、これらのゲートウェイを経由して比較的容易に無料通話をかけることができます。これらのゲートウェイを保護するため、信頼できる IP アドレスからの H.225 シグナリングを許可する着信 ACL を設定します。この方法には、[「QoS」の項で説明する拡張性の問題があります](#)。信頼できる H.323 エンドポイントの増加に伴い、ACL のエントリの数が増加します。

H.323 プロキシにより、この問題がやや緩和されます。PSTN ゲートウェイ経由のすべてのコールがキャンパス プロキシをパススルーする場合、ゲートウェイ ACL では、大学キャンパスごとに 1 つの IP アドレスを許可する必要があります。ほとんど場合、冗長プロキシとして 2 つの IP

アドレスを使用することが適しています。プロキシを使用する場合でも、ACL のエントリ数が 100 を超えることがあります。

H.323 ではプロキシ経由でコールを設定できるため、プロキシを ACL によって保護する必要があります。これはキャンパス単位で行われるため、ローカル ポリシーの要件に従い、プロキシ ACL ではローカル H.323 デバイスを許可する必要があります。

キャンパスで IP フォンからのコールだけが AARNet PSTN ゲートウェイを使用することが求められる場合は、2 つの Cisco CallManager の IP アドレスをゲートウェイ ACL に含める必要があります。この状況では、プロキシは値を追加しません。いずれの場合でも必要な ACL エントリの数は 2 です。

キャンパス間での IP フォンから IP へのコールは、プロキシをパススルーする必要がない点に注意してください。

## ダイヤルプラン

現在の VoIP ダイヤルプランは単純です。VoIP ゲートウェイの観点から、ユーザは 2 種類のコールを発信できます。

- 同じ大学内の別のキャンパスの電話へのコール。
- PSTN フォンまたは別の大学の電話へのコール。

ゲートウェイ ダイヤル ピアは、コールはこの 2 種類だけであることを反映しています。基本的には、次の例に示すように 2 種類の VoIP ダイヤル ピアがあります。

```
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
```

この例の 1 番目のダイヤル ピアは、別のキャンパスの内線番号 7... がコールされる場合に使用されます。このコールはリモート ゲートウェイの IP アドレスに直接ルーティングされます。ゲートキーパーをバイパスするため、コール アドミッション制御 (CAC) は実行されません。

2 番目のダイヤル ピアは、PSTN 番号へのコールの場合に使用されます。これは次のいずれかの番号です。

- PSTN 内の電話の番号。
- 別の大学の電話の完全修飾 PSTN 番号

1 番目のケースでは、コールはアドミッション要求 (ARQ) メッセージによりゲートキーパーに送信されます。ゲートキーパーは、アドミッション確認 (ACF) メッセージで最適な PSTN ゲートウェイの IP アドレスを返します。

2 番目のケースでも、コールは ARQ メッセージによりゲートキーパーに送信されます。ただしゲートキーパーは、コールを受信した大学の VoIP ゲートウェイの IP アドレスを含む ACF メッセージを返します。

## ゲートキーパー

現在、AARNet は 1 つのゲートキーパーを運用しています。このゲートキーパーの唯一の目的は、コールルーティングを E.164 から IP アドレスへの解決の形で実行することです。ゲートキーパーは CAC を実行しません。ゲートウェイに接続する PABX トランクの数により、同時コールの数が制限されます。コアの帯域幅は、使用中のすべてのトランクに同時に対応できます。これは、ACU およびその他の大学での IP テレフォニーのロールアウトに伴って変化します。この新しい環境では、特定のキャンパス内外から発信される同時 VoIP コールの数に自然の制限はありません。発信コールの数が多すぎると、使用可能な QoS 帯域幅のオーバーサブスクライブが発生することがあります。この状況では、すべてのコールが低品質の影響を受ける可能性があります。ゲートキーパーを使用して CAC を提供します。

大学の音声ネットワークは、その分散型特性と想定される規模から、分散型ゲートキーパーアーキテクチャに適しています。考えられる解決策の 1 つとして、各大学が各自のゲートキーパーを運用する 2 階層の階層型ゲートキーパー設計を導入することがあります。この大学ゲートキーパーは Tier 2 ゲートキーパーと呼ばれます。AARNet は Tier 1 ゲートキーパーと呼ばれるディレクトリゲートキーパーを運用します。

各大学は、Cisco CallManager クラスタ間のコールルーティングにゲートキーパーを使用するために、この 2 階層方式を採用する必要があります。このシナリオでは、ゲートキーパーは 4 ~ 5 桁の内線番号に基づいてコールをルーティングします。各大学には専用のゲートキーパーが必要です。これは、内線番号の範囲は、ローカルで管理されるアドレス空間であり、大学間で重複しているためです。

大学の Tier 2 ゲートキーパーは、その大学で発信/着信するコールに対してのみ CAC を実行します。また、大学内のキャンパス間のコールに対してのみ E.164 解決を実行します。ユーザが別の大学の IP フォンにコールするか、または AARNet ゲートウェイ経由で PSTN にコールする場合、そのコールは、ロケーション要求 (LRQ) メッセージにより Tier 2 ゲートキーパーから Tier 1 ゲートキーパーにルーティングされます。別の大学へのコールの場合、LRQ がその大学の Tier 2 ゲートキーパーに転送されます。このゲートキーパーは、コール発信元の大学の Tier 2 ゲートキーパーに ACF メッセージを返します。両方の Tier 2 ゲートキーパーが CAC を実行します。発信ゾーンと着信ゾーンの両方で十分な帯域幅が利用可能な場合にだけ、ゲートキーパーはコールの処理を進めます。

AARNet では、AARNet PSTN ゲートウェイを大学のゲートウェイと同様に扱うかどうかを選択できます。ゲートウェイの Tier 2 ゲートキーパーがゲートウェイを管理します。負荷とパフォーマンスの面で対応可能な場合には、Tier 1 ゲートキーパーが、これらのゲートウェイの Tier 2 ゲートキーパーとして機能することもできます。

ゲートウェイは重要な構成要素であるため、各ゲートキーパー (AARNet ディレクトリゲートキーパーを含む) を複製する必要があります。各大学には 2 台のゲートキーパーが必要です。Cisco IOS ソフトウェア リリース 12.0(7)T の場合、Cisco IOS ゲートウェイが代替ゲートキーパーを使用できます。ただし現在、Cisco CallManager やその他のサードパーティの H.323 デバイスでは、これはサポートされていません。現時点ではこの機能を使用しないでください。代わりに、単純な Hot Standby Router Protocol ベース (HSRP ベース) のソリューションを使用します。このためには、両方のゲートキーパーが同じ IP サブネットワーク内に導入されている必要があります。HSRP により、アクティブなゲートキーパーが判別されます。

## [ACU IP テレフォニー ネットワーク](#)

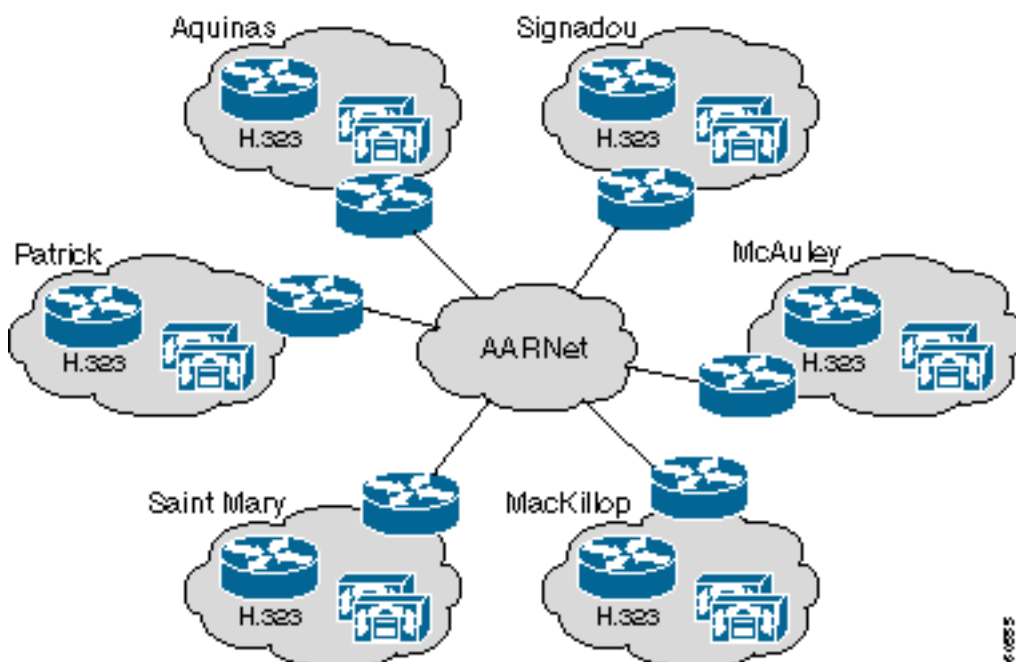
次の表に、ACU の各キャンパスに導入されている IP フォンの概数を示します。

キャンパス	都市	IP フォンの概数
-------	----	-----------



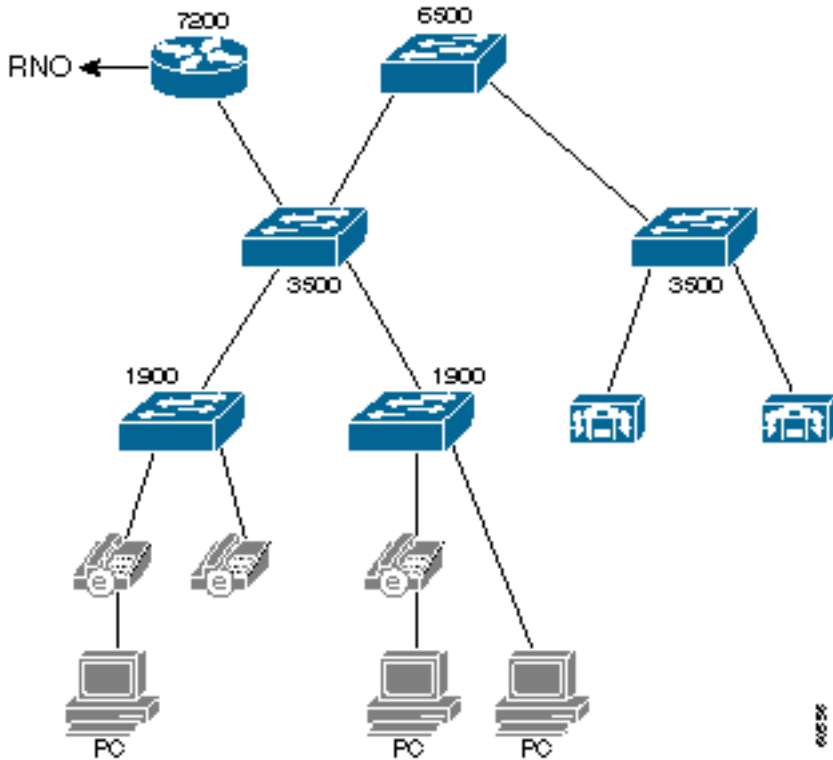
Mount Saint Mary	ストラスフィールド	400
MacKillop	North Sydney	300
Patrick	メルボルン	400
Aquinas	バララット	100
Signadou	キャンベラ	100
McAuley	ブリズベン	400
	<b>合計：</b>	<b>1700</b>

ACU は最近、IP テレフォニー ソリューションを導入しました。このソリューションは、2つの Cisco CallManager からなるクラスター、各キャンパスに導入されている Cisco 3640 ゲートウェイ、および IP フォンで構成されています。AARNet によってキャンパスが相互接続されます。次の図に、ACU IP テレフォニー ネットワークの全体的なトポロジと各種コンポーネントを示します。



## ACU ネットワーク トポロジ

次の図に、ACU の典型的なキャンパスを示します。各キャンパスには、Catalyst スイッチからなる 3 つの階層があります。古い Catalyst 1900 スイッチはワイヤリング クローゼットに格納されています。Catalyst 1900 スイッチは、Extended Framing によって Catalyst 3500XL スイッチに接続します。これらのスイッチはギガビット イーサネット (GE) によって 1 台の Catalyst 6509 スイッチに接続します。1 台の Cisco 7200 VXR ルーターが、ローカル RNO への ATM VC によってキャンパスを AARNet に接続します。



次の表に示すように、RNO への接続方式は州によって多少異なります。ビクトリア州は Classical IP over ATM ( RFC 1577 ) に基づいています。その他の RNO は、RFC 1483 カプセル化を使用した単純な PVC セットアップです。ACU と RNO の間で使用されるルーティング プロトコルは Open Shortest Path First ( OSPF ) です。

キャンパス	都道府県	RNO への接続	ルーティングプロトコル
Mount Saint Mary	NSW	RFC 1483 PVC	OSPF
MacKillop	NSW	RFC 1483 PVC	OSPF
Patrick	VIC	RFC 1577 Classical IP over ATM	OSPF
Aquinas	VIC	RFC 1577 Classical IP over ATM	OSPF
Signadou	ACT	RFC 1483 PVC	OSPF
McAuley	QLD	RFC 1483 PVC	OSPF

Catalyst 1900 シリーズ スイッチは、アップリンクでのトランキングだけをサポートしています。したがって、IP フォンと PC がすべて 1 つの大規模 VLAN に接続しています。実際には、キャンパス全体が 1 つの大規模な VLAN およびブロードキャスト ドメインです。デバイスの数が多いため、セカンダリ IP サブネットワークが使用されます。IP フォンは 1 つの IP サブネットワークに接続し、PC は別の IP サブネットワークに接続しています。AARNet コアは、IP フォン サブネットワークを信頼し、この IP サブネットワークを出入りするトラフィックは LLQ の対象となります。

Cisco 7200 ルータは、プライマリ IP サブネットワークとセカンダリ IP サブネットワーク間のル

ーディングを行います。現在、Catalyst 6500 のマルチレイヤ スイッチ フィーチャ カード ( MSFC ) は使用されていません。

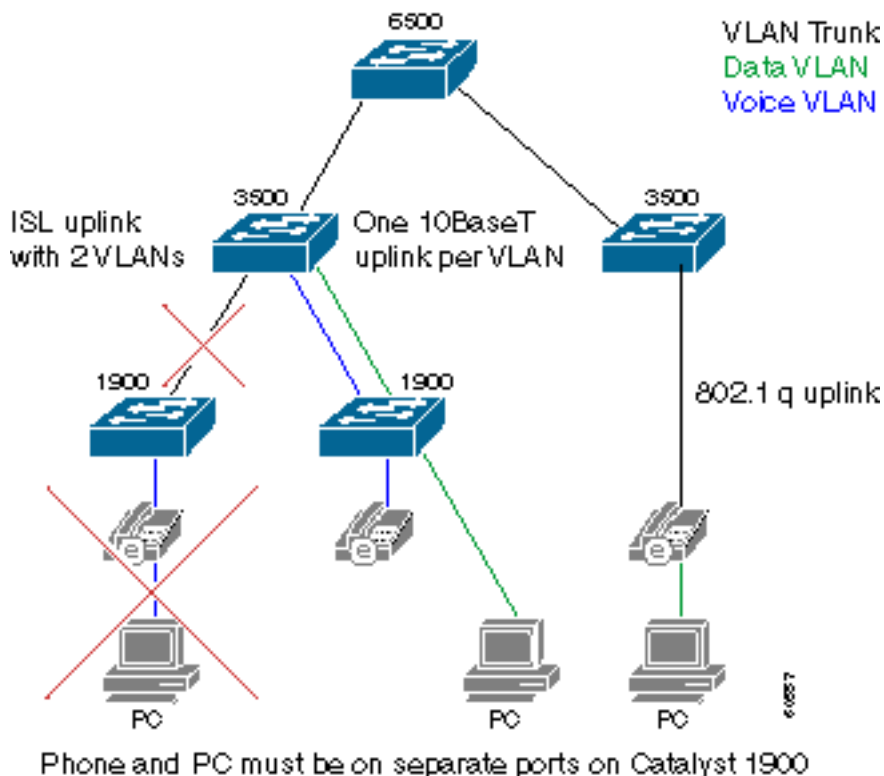
Catalyst 3500XL および Catalyst 6500 スイッチには QoS 機能が組み込まれていますが、現在この機能は有効ではありません。

## キャンパスにおける QoS

現在のキャンパス設計は、IP テレフォニーに関するシスコ推奨の設計ガイドラインに準拠していません。QoS に関するいくつかの懸念事項があります。

- ブロードキャスト ドメインが非常に大規模である。過剰なブロードキャストが、そのブロードキャストを処理する必要がある IP フォンのパフォーマンスに影響する可能性があります。
- Catalyst 1900 スイッチが QoS に対応していない。IP フォンと PC が同じスイッチ ポートに接続しており、PC がデータを高速で受信する場合、音声パケットがドロップされることがある。

大幅な改善を実現するため、キャンパス インフラストラクチャの一部を再設計します。ハードウェアのアップグレードは不要です。次の図に、推奨される再設計の原理を示します。



キャンパスを音声 VLAN とデータ VLAN に分割する必要があります。VLAN の切り離しのため、Catalyst 1900 スイッチに接続している PC と電話をそれぞれ別のポートに接続する必要があります。各 Catalyst 1900 スイッチから Cisco 3500XL スイッチへのアップリンクが追加されました。2つのアップリンクのうち1つは音声 VLAN のメンバーです。もう1つのアップリンクはデータ VLAN のメンバーです。2つのアップリンクの代わりにスイッチ間リンク ( ISL ) を使用しないでください。この場合、音声トラフィックとデータトラフィックに個別のキューが提供されません。Catalyst 3500XL スイッチから Catalyst 6000 スイッチへの GE リンクも、802.1q トランクに変換される必要があります。これにより、音声 VLAN とデータ VALN の両方を、このコアスイッチを介して伝送できます。

データ VLAN の Catalyst 3500XL スイッチのポートのデフォルト サービス クラス ( CoS ) は 0 です。音声 VLAN のメンバーであるポートのデフォルト CoS は 5 です。このため、音声トラフ



イックは Catalyst 3500 または Catalyst 6500 コアに到着した時点で正しく優先順位付けされます。次の例に示すように、Catalyst 3500 QoS スイッチ ポート構成は、どの VLAN スイッチ ポートがメンバーであるかによって多少異なります。

```
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
```

IP フォンが Catalyst 3500XL スイッチに直接接続されているという稀な状況では、IP フォンの背面スイッチ ポートに PC を接続できます。この場合、IP フォンは 802.1q トランクを使用してスイッチに接続します。これにより、音声パケットとデータパケットがそれぞれ個別の VLAN 上を移動し、入力時にパケットに正しい CoS を設定できます。Catalyst 1900 スイッチのサポートが間もなく終了するため、Catalyst 1900 スイッチを Catalyst 3500XL スイッチまたはその他の QoS 対応スイッチに交換してください。このトポロジは、IP フォンと PC をネットワークに接続する標準方式となります。このシナリオでは、Catalyst 3500XL スイッチの QoS 設定を示します。

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

最後に、2 つの Cisco CallManager に接続する 2 つのポートには、CoS が 3 としてハードコーディングされている必要があります。Cisco CallManager は、すべての音声シグナリングパケットの IP プレシデンスを 3 に設定します。ただし、Cisco CallManager から Catalyst 3500XL スイッチへのリンクでは 801.1p は使用されません。したがって CoS 値は、この例に示すようにスイッチで強制的に適用されます。

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

この設計の主な課題は、デスクトップに 2 つのスイッチポートが必要な点です。Patrick キャンパスでは、400 台の IP フォン用に 400 台のスイッチが追加が必要となります。十分な数のポートが使用可能ではない場合は、Catalyst 3500XL スイッチを追加で導入する必要があります。不足している Catalyst 1900 スイッチポート 2 つに対し、Catalyst 3500XL スイッチポートが 1 つ必要です。

現在の ACU の Catalyst 6500 スイッチには QoS 機能が搭載されていますが、これらのスイッチは現在有効ではありません。ACU の Catalyst 6000 スイッチには、次のキューイング機能を備えた次のモジュールが装着されています。

スロット	モジュール	ポート	RX キュー	TX キュー
1	WS-X6K-SUP1A-2GE	0	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	—	—
----	-------------	---	---	---

Catalyst 6000 スイッチで適切な QoS 機能をアクティブにするには、次の手順を実行します。

1. 次のコマンドを使用して、スイッチに対し、VLAN ごとに QoS を指定するよう指示します

```
。
Cat6K>(enable) set port qos 1/1-2,3/1-8,4/1-8 vlan-based
```

2. 次のコマンドを使用して、スイッチに対し、Catalyst 3500XL スイッチから受信した CoS 値を信頼するよう指示します。

```
Cat6K>(enable) set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos
```

CoS は、DiffServ コードポイント ( DSCP ) マッピングに設定されている必要があります。これは、Catalyst 6000 スイッチが、受信した CoS 値に基づいて IP ヘッダーの DSCP 値を書き換えるために必要です。VoIP シグナリング パケットでは CoS が 3 に設定されている必要があります ( DSCP AF31 ( 26 ) で書き換え )。RTP パケットでは CoS が 5 に設定されている必要があります ( DSCP EF ( 46 ) で書き換え )。次のコマンドを実行します。

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

次の例を使用して CoS/DSCP マッピングを確認します。

```
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
```

さまざまな IP サブネットワーク間をルーティングするように MSFC を設定します。

## [RNO における QoS](#)

RNO の現在の設計は、シスコ推奨の IP テレフォニー設計ガイドラインに準拠していません。この問題は QoS に関連しています。

- LLQ は Cisco ACU 7200 シリーズ WAN ルータには適用されません。
- Patrick キャンパスと Aquinas キャンパスは、ATM 相手先選択 VC ( SVC ) によって RNO に接続しています。LLQ は SVC ではサポートされません。

ファストイーサネットに接続した Cisco 7200 ルータにより、キャンパスと RNO が 34 Mbps E4 ATM リンクで接続されています。4M と 100M という速度の不一致が原因で、トラフィックが 34M リンク上でアウトバウンドでキューイングされる可能性があります。そのため、音声トラフィックを優先する必要があります。LLQ を使用します。Cisco 7200 ルータの設定は次の例に似ています。

```
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
```

LLQ に割り当てられた帯域幅は  $N \times 24\text{Kbps}$  でなければなりません。この  $N$  は、同時 G.729 コールの数です。

Patrick および Aquinas の各 Cisco 7200 ルータと AARNet ルータの間で 1 つの PVC を設定します。ビクトリア州の RNO の ATM SVC は、Classical IP over ATM ( RFC 1577 ) に基づいているため、LLQ をサポートしていません。現時点では、ビクトリア州の RNO に接続する他の大学は、引き続き RFC 1577 を使用できます。ただし、Classical IP over ATM インフラストラクチャは最終的には交換される予定です。

## ゲートウェイ

ACU の各キャンパスには、H.323 ゲートウェイとして機能する Cisco 3640 ルータが導入されています。これらのゲートウェイは、ISDN 経由で PSTN に接続します。1 次群速度インターフェイス ( PRI ) と B チャネルの数は、キャンパスの規模に応じて異なります。次の表に、各キャンパスの PRI および B チャネルの数を示します。

キャンパス	PRI の数	B チャネルの数
Mount Saint Mary	0	30
MacKillop	0	50
Patrick	0	50
Aquinas	1	20
Signadou	1	20
McAuley	1	30

これらのゲートウェイは、DOD (ダイヤルアウト方式) のセカンダリゲートウェイとしてのみ使用されます。AARNet のゲートウェイはプライマリゲートウェイです。ACU のゲートウェイは常に DID (ダイヤルイン方式) に使用されます。

## ダイヤルプラン

ダイヤルプランは、4 桁の内線番号に基づいています。この内線番号は、DID 番号の最後の 4 桁でもあります。次の表に、各キャンパスの内線番号の範囲と DID 番号を示します。

キャンパス	Extension	DID
Mount Saint Mary	9xxx	02 9764 9xxx

MacKillop	8xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Aquinas	5xxx	03 5330 5xxx
Signadou	2xxx	02 6123 2xxx
McAuley	7xxx	07 3354 7xxx

ゲートウェイでの単純な num-exp Cisco CallManager DID DID 4 たとえば、Patrick キャンパスのゲートウェイには次のエントリがあります。

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

ユーザが、外線を選択するためゼロをダイヤルします。先頭のゼロがゲートウェイに渡されます。1つの POTS ダイヤルピアが、先頭のゼロに基づいてコールを ISDN ポートヘルパーティングします。

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

着信コールでは、着信者番号を4桁の内線番号に変換するため、この num-exp エントリが使用されます。次にコールが両方の VoIP ダイヤルピアに一致します。優先順位に基づき、このルートが Cisco CallManager サブスクライバよりも優先されます。

```
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](#)

各キャンパスには、2台の Cisco CallManager サーバで構成されるクラスタがあります。Cisco CallManager サーバは、Media Convergence Server 7835 (MCS-7835) と Media Convergence Server 7820 (MCS-7820) の組み合わせです。このドキュメントの発行時点では、この両方のサーバはバージョン 3.0(10) で稼働していました。1つの Cisco CallManager がパブリッシャであり、もう1つの Cisco CallManager がサブスクライバです。サブスクライバは、すべての IP フォンに対しプライマリ Cisco CallManager として機能します。次の表に、各キャンパスに導入されているハードウェアを示します。

キャンパス	Platform	CallManager
Mount Saint Mary	MCS-7835	0
MacKillop	MCS-7835	0

Patrick	MCS-7835	0
Aquinas	MCS-7820	0
Signadou	MCS-7820	0
McAuley	MCS-7835	0

各クラスタには 2 つの領域が設定されています。

- キャンパス内コール ( G.711 ) のための領域
- キャンパス間コール ( G.729 ) のための領域

ACU では、各クラスタで処理されるすべての IP フォンが 1 つのキャンパス内にあるため、ロケーションベースの CAC は適切ではありません。キャンパス間コールにゲートキーパーベースの CAC を使用するメリットがありますが、これは現在実装されていません。ただし、近い将来に実装する予定です。

各 Cisco CallManager は、22 台の H.323 ゲートウェイを使用して設定されています。これは、その他の 5 つの Cisco CallManager クラスタへのクラスタ間トランク、6 台の AARNet PSTN ゲートウェイ、および各キャンパスの 1 つの ACU ゲートウェイで構成されます。

H.323 デバイス タイプ	数量
キャンパス間 CallManager	2 x 5 = 10
AARNet PSTN ゲートウェイ	6
ACU PSTN ゲートウェイ	6
<b>合計 :</b>	<b>22</b>

ルートリストとルートグループは、PSTN ゲートウェイのランク付けに使用されます。たとえば、メルボルンの Patrick キャンパスにある Cisco CallManager からシドニーの PSTN へのコールで、4 つのゲートウェイを使用してコールをルートグループに結合する方法を次の表に示します。

ゲートウェイ	優先順位
AARNet シドニー	1
ACU シドニー	0
AARNet メルボルン	3
ACU メルボルン	4

次の表に示すように、Cisco CallManager では約 30 のルートパターンが設定されています。ルートパターンは、オーストラリア国内のすべての番号に対し、一致が存在するように設計されています。このため、ユーザは Cisco CallManager がコールを開始する前に、桁間タイムアウトが経過するまで待つ必要はありません。ワイルドカード文字「!」は、国際電話番号のルートパターンでのみ使用されます。ユーザは国際電話番号をダイヤルするときに、コールの処理を進める前に、桁間タイムアウト ( デフォルトでは 10 秒 ) が経過するまで待つ必要があります。ユーザはルートパターン「0.0011!#」も追加できます。ユーザは、最後の数字の後に「#」を入力して、Cisco CallManager に対して着信番号が完了したことを通知することもできます。このアクションにより、国際通話が迅速に処理されます。

ルートパターン	説明
0.[2-9]XXXXXXX	ローカルコール
0.00	緊急コール : ユーザが外線通話のため

	の 0 をダイヤルし忘れた場合
0.000	緊急コール
0.013	番号案内
0.1223	—
0.0011!	国際コール
0.02XXXXXXXXX	ニュー サウス ウェールズ州へのコール
0.03XXXXXXXXX	ビクトリア州へのコール
0.04XXXXXXXXX	携帯電話へのコール
0.07XXXXXXXXX	クイーンズランド州へのコール
0.086XXXXXXXXX	ウェスタン オーストラリア州へのコール
0.08XXXXXXXXX	サウス オーストラリア州および北部準州へのコール
0.1[8-9]XXXXXXXXX	1800 xxx xxx および 1900 xxx xxx へのコール
0.1144X	緊急
0.119[4-6]	時刻と天気
0.1245X	ディレクトリ
0.13[1-9]XXX	13xxxx 番号へのコール
0.130XXXXXXXXX	1300 xxx xxx 番号へのコール
2[0-1]XX	Signadou へのクラスタ間コール
3[0-4]XX	Patrick へのクラスタ間コール
5[3-4]XX	Aquinas へのクラスタ間コール
7[2-5]XX	McAuley へのクラスタ間コール
8[0-3]XX	MacKillop へのクラスタ間コール
9[3-4]XX	Mount Saint Mary へのクラスタ間コール
9[6-7]XX	Mount Saint Mary へのクラスタ間コール

ACU の Cisco CallManager で設定されているゲートウェイ、ルート グループ、ルート リスト、およびルート パターンの数が大幅に増加する可能性があります。新しい RNO ゲートウェイを導入する場合は、追加したゲートウェイを使用して、5 つの Cisco CallManager クラスタすべてを再設定する必要があります。さらに、ACU の Cisco CallManager により VoIP コールがその他のすべての大学に直接ルーティングされ、PSTN がバイパスされる場合は、数百台のゲートウェイを追加する必要があります。明らかにこれは適切に拡張されません。

この解決策として、Cisco CallManager をゲートキーパーにより制御します。新しいゲートウェイまたは Cisco CallManager が AARNet 上に追加される場合に行う必要がある操作は、ゲートキーパーの更新だけです。この操作が行われる場合には、各 Cisco CallManager でローカル キャンパス ゲートウェイと匿名デバイスだけが設定されている必要があります。このデバイスはポイントツーマルチポイント トランクと見なすことができます。これにより、Cisco CallManager ダイアル プラン モデルでメッシュ PPP トランクの必要性が排除されます。1 つのルート グループが匿名デバイスを優先ゲートウェイとして指し示し、ローカル ゲートウェイをバックアップ ゲートウェイとして指し示します。ローカル PSTN ゲートウェイは特定のローカル コールに使用されます。また、ゲートキーパーが使用できない状態になった場合には一般的なオフネット コールにも

使用されます。現在、匿名デバイスは、クラスタ間または H.225 のいずれかにできますが、同時にクラスタ間と H.225 の両方にすることはできません。

ゲートキーパーを使用する場合、Cisco CallManager に必要なルート パターンの数は、現在 Cisco CallManager に含まれる数よりも少なくなります。基本的に、Cisco CallManager に必要なルートパターンは、ゲートキーパーを指し示すルート パターン (「!」) だけです。実際には、次に示す理由からコールのルーティング方法をより詳細にする必要があります。

- 一部のコール ( 1-800 番号や緊急番号などへのコール ) は、地理的にローカルなゲートウェイを経由してルーティングする必要があります。メルボルンのユーザが警察やピザハットなどのレストランチェーンにダイヤルする場合、パースの警察やピザハットに接続することは求められません。これらの番号の場合、ローカル キャンパスの PSTN ゲートウェイを直接指し示す特定のルート パターンが必要です。今後 IP テレフォニーの導入を予定している大学は、AARNet ゲートウェイだけを利用し、各自のローカル ゲートウェイを管理しないことを選択できます。ローカルでドロップオフする必要があるコールの場合でもこの設計が有効であるようにするため、これらの番号には、Cisco CallManager によりゲートキーパーへの送信前に仮想エリア コードが先頭に付加されている必要があります。たとえば、Cisco CallManager はメルボルンの電話からのピザハットの 1-800 番号へのコールの先頭に 003 を付加できます。これにより、ゲートキーパーはこのコールをメルボルンの AARNet ゲートウェイにルーティングできます。ゲートウェイは、先頭の 003 を削除してから、PSTN へこのコールを発信します。
- コールを開始する前にユーザが桁間タイムアウトを待つ必要がないようにするため、すべての国内電話番号に正確に一致するルート パターンを使用します。

次の表に、ゲートキーパーにより制御される Cisco CallManager のルート パターンを示します。

ルート パターン	説明	ルート	ゲートキーパー
0.[2-9]XXXXXX XX	ローカル コール	ルート リスト	AARNet
0.00	緊急コール	ローカル ゲートウェイ	なし
0.000	緊急コール	ローカル ゲートウェイ	なし
0.013	番号案内	ローカル ゲートウェイ	なし
0.1223	—	ローカル ゲートウ	なし

		エイ	
0.0011!	国際コール	ルー トリ スト	AARNe t
0.0011!#	国際コール	ルー トリ スト	AARNe t
0.0[2-4]XXXXX XXX	ニュー サウス ウェールズ州、ビクトリア州、および携帯電話へのコール	ルー トリ スト	AARNe t
0.0[7-8]XXXXX XXX	サウス オーストラリア州、ウエスタン オーストラリア州、および北部準州へのコール	ルー トリ スト	AARNe t
0.1[8-9]XXXXX XXX	1800 xxx xxx および 1900 xxx xxx へのコール	ロー カル ゲー トウ エイ	なし
0.1144X	緊急	ロー カル ゲー トウ エイ	なし
0.119[4-6]	時刻と天気	ロー カル ゲー トウ エイ	なし
0.13[1-9]XXX	13xxxx 番号へのコール	ロー カル ゲー トウ エイ	なし
0.130XX XXXXX	1300 xxx xxx 番号へのコール	ロー カル ゲー トウ エイ	なし
[2-3]XXX	Signadou へのコール	ルー トリ スト	ACU
5XXX	Aquinas へのコール	ルー トリ スト	ACU
[7-9]XXX	McAuley、MacKillop、および Mount Saint Mary へのコール	ルー トリ スト	ACU

ゲートキーパーは、ローカル ゲートウェイ経由で送信されない国際コールをルーティングします。AARNet では将来、国際ゲートウェイが導入可能になるため、これは重要です。ゲートウェイ



が米国内に導入されている場合、ゲートキーパー設定の簡単な変更を行うことで、大学は米国の国内通話料金で米国へコールできます。

ゲートキーパーは ACU の 4 桁の内線番号に基づいて、クラスタ間コール ルーティングを実行します。このアドレス空間は、他の大学と重複している可能性が高いです。このため、ACU は専用のゲートキーパーを管理し、AARNet のゲートキーパーをディレクトリゲートキーパーとして使用します。この表のゲートキーパーのカラムは、コール ルーティングが ACU のゲートキーパーまたは AARNet のゲートキーパーのいずれによって実行されるかを示します。

注：ご提案するゲートキーパーのソリューションに関する唯一の注意点は、匿名デバイスは現在、クラスタ間または H.225 のいずれかにできますが、両方を同時に使用することはできません。Cisco CallManager は、推奨される設計でゲートウェイ ( H.225 ) およびその他の Cisco CallManager ( クラスタ間 ) の両方にコールをルーティングするときに、ゲートキーパーを使用します。この問題の回避策は、クラスタ間ルーティングにゲートキーパーを使用しないか、ゲートキーパー経由のすべてのコールを H.225 として扱うことです。後者の回避策は、クラスタ間コールで一部の補足機能が使用できない可能性があります。

## ボイス メール

ACU では、IP テレフォニーへの移行前は、Dialogic 電話ボードを備えた Active Voice Repartee OS/2 ベースのボイス メール サーバが 3 台導入されていました。IP テレフォニー環境でこれらのサーバを再利用する予定です。実装時には、各 Repartee サーバが Simplified Message Desk Interface ( SMDI ) および Catalyst 6000 24 ポート Foreign Exchange Station ( FXS ) カードを使用して Cisco CallManager に接続します。これにより、6 つのキャンパスのうち 3 つにボイス メールが導入され、残りの 3 つにはボイス メールが導入されません。クラスタ間の H.323 トランクを渡るメッセージ待機インディケータ ( MWI ) を伝搬させることはできないため、2 つの Cisco CallManager クラスタのユーザ間で Repartee サーバを正常に共有することは不可能です。

ACU では、残りのキャンパスのために 3 台の Cisco Unity サーバを購入する可能性があります。これらのサーバは Skinny ベースであるため、ゲートウェイは不要です。次の表に、ACU が追加のボイス メール サーバを購入した場合のボイス メール ソリューションを示します。

キャンパス	ボイス メール システム	ゲートウェイ
Mount Saint Mary	Active Voice Repartee	Catalyst 6000 24 ポート FXS
MacKillop	Active Voice Repartee	Catalyst 6000 24 ポート FXS
Patrick	Active Voice Repartee	Catalyst 6000 24 ポート FXS
Aquinas	Cisco Unity	—
Signadou	Cisco Unity	—
McAuley	Cisco Unity	—

この計画では、6 台のボイス メール サーバが、独立したボイス メール アイランドとして機能します。ボイス メール ネットワーキングはありません。

## メディア リソース

ハードウェア デジタル シグナル プロセッサ ( DSP ) は、現在 ACU には導入されていません。電

話会議では、Cisco CallManager 上のソフトウェア ベースの会議ブリッジが使用されます。現在、クラスタ間電話会議はサポートされていません。

現在、トランスコーディングは不要です。G.711 および G.729 コーダ/デコーダだけが使用されます。これらのコーダ/デコーダは、導入されているすべてのエンド デバイスでサポートされています。

## FAX とモデムのサポート


FAX とモデムのトラフィックは、ACU IP テレフォニー ネットワークでは現在サポートされていません。同大学では、この目的で Catalyst 6000 24 ポート FXS カードを使用することを予定しています。

## ソフトウェアのバージョン

次の表に、このドキュメントの発行時点で ACU が使用していたソフトウェアのバージョンを示します。

Platform	機能	[Software Version]
CallManager	IP-PBX	3.0(10)
Catalyst 3500XL	ディストリビューション スイッチ	12.0(5.1)XP
Catalyst 6500	コアスイッチ	5.5(5)
Catalyst 1900	ワイヤリング クローゼット スイッチ	—
Cisco 7200 プロセッサ	WAN ルータ	12.1(4)
Cisco 3640 ルータ	H.323 ゲートウェイ	12.1(3a)XI6

## 関連情報

- [音声に関する技術サポート](#)
- [音声と IP 通信製品サポート](#)
- [Cisco IP Telephony のトラブルシューティング](#) 
- [テクニカル サポートとドキュメント – Cisco Systems](#)