

# 사례 연구 IP 텔레포니 구축 - ACU

## 목차

[소개](#)

[AARNet](#)

[AARNet 토폴로지](#)

[QoS\(Quality of Service\)](#)

[게이트웨이](#)

[다이얼 플랜](#)

[게이트키퍼](#)

[ACU IP 텔레포니 네트워크](#)

[ACU 네트워크 토폴로지](#)

[캠퍼스의 QoS](#)

[RNO의 QoS](#)

[게이트웨이](#)

[다이얼 플랜](#)

[Cisco CallManager](#)

[음성 메일](#)

[미디어 리소스](#)

[팩스 및 모뎀 지원](#)

[소프트웨어 버전](#)

[관련 정보](#)

## 소개

AARNet(Australian Academic and Research Network)는 37개의 호주 대학과 CSIRO(Commonwealth Scientific and Industrial Research Organization)를 연결하는 전국적인 고속 IP 네트워크입니다.

AARNet은 처음에는 데이터 네트워크로 구축되었지만 2000년 초부터 VoIP(Voice over IP)를 사용했습니다. 현재 구축된 VoIP 네트워크는 대학과 CSIRO PABX(Private Automatic Branch Exchange) 간에 VoIP 통화를 전달하는 유료 바이패스 솔루션입니다. 또한 PSTN이 가장 비용 효율적인 지점에서 하프(hop)할 수 있는 PSTN(Public Switched Telephone Network) 게이트웨이를 제공합니다. 예를 들어 멜버른의 PABX 전화기에서 시드니의 PSTN 전화기로 가는 통화는 멜버른에서 시드니 PSTN 게이트웨이로 VoIP로 전달됩니다. PSTN에 연결되어 있습니다.

ACU(Australian Catholic University)는 AARNet과 연결되는 대학 중 하나입니다. 2000년 말, ACU는 6개 대학 캠퍼스에 약 2,000개의 IP 전화를 구축하는 IP 텔레포니 구축을 시작했습니다.

이 사례 연구에서는 ACU IP 텔레포니 구축을 다룹니다. 프로젝트가 완료되었습니다. 그러나 다른 대학들이 ACU의 뒤를 이을 때 네트워크를 확장하려면 AARNet 백본에서 해결해야 할 중요한 아키텍처 문제가 있습니다. 이 문서에서는 이러한 문제에 대해 설명하고 다양한 솔루션을 제안하며 설명합니다. ACU IP 텔레포니 구축은 최종 권장 아키텍처에 맞게 나중에 조정될 가능성이 높습니다.

**참고:** Deakin University는 IP 텔레포니를 구축한 최초의 호주 대학이었습니다. 그러나 Deakin University는 AARNet을 사용하여 IP 텔레포니 트래픽을 전달하지 않습니다.

## AARNet

호주 대학과 CSIRO는 1990년 AARNet을 호주 부총장협의회(AVCC)를 통해 설립했습니다. 호주 인터넷 트래픽의 99%가 처음 몇 년 동안 창업자들에게 전달되었습니다. 3차 및 연구 부문과 밀접한 관련이 있는 조직에서 소규모의 커머셜 트래픽이 발생했습니다. 비 AARNet 사용자 기반의 사용은 1994년 말에 전체 트래픽의 20%까지 증가했습니다.

AVCC는 1995년 7월 AARNet의 상용 고객 기반을 Telstra에 매각했습니다. 이 사건은 결국 텔스트라 빅 연못이 될 것을 낳았습니다. 이것은 호주에서 인터넷의 상업적 그리고 민간 사용의 성장을 촉진시켰다. 지적 재산과 전문 기술의 이전으로 호주의 인터넷 개발이 이루어졌습니다. 그렇지 않았다면 이런 빠른 속도로 일어난 것은 아닐 것이다.

AVCC는 1997년 초에 AARNet2를 개발했습니다. 이것은 CWO(Cable & Wireless Optus) Limited와의 계약에 따라 고대역폭 ATM 링크와 인터넷 서비스를 사용하는 호주에서 인터넷의 개선이었다. AARNet2 요구 사항을 충족하기 위해 CWO가 IP 서비스를 신속하게 구축하는 것은 AARNet에서 지식과 전문 지식을 이전하기 때문이었습니다.

## ACU

ACU는 1991년에 설립된 공립 대학입니다. 그 대학에는 약 10,000명의 학생과 1,000명의 직원이 있습니다. 호주 동해안에 6개의 캠퍼스가 있다. 다음 표에서는 ACU 캠퍼스 및 위치를 보여 줍니다.

캠퍼스	구/군/시	주/도
세인트 메리 산	스트라스필드	뉴사우스웨일스(NSW)
맥킬롭	시드니 북부	뉴사우스웨일스(NSW)
패트릭	멜버른	빅토리아(VIC)
아퀴나스	발라랏	빅토리아(VIC)
사이나두	캔버라	오스트레일리아 수도 구역 (ACT)
맥컬리	브리즈번	퀸즈랜드(QLD)

ACU는 이 사례 연구에서 설명한 IP 텔레포니 솔루션의 출시에 앞서 Telstra Spectrum(Centrex) 솔루션을 이용했습니다. IP 텔레포니로의 전환은 주로 비용 절감에 기인한 것입니다.

## CSIRO

CSIRO는 오스트레일리아 내 여러 지역에서 약 6,500명의 직원을 보유하고 있습니다. CSIRO는 농업, 광물, 에너지, 제조, 통신, 건설, 건강 및 환경 등의 분야에서 연구를 수행합니다.

CSIRO는 VoIP용 AARNet을 사용한 최초의 조직입니다. 그 단체는 이 지역에서 처음으로 일을 시작했습니다.

## [AARNet](#)

AARNet 백본은 모든 대학 IP 텔레포니 구축에서 중요한 구성 요소입니다. 음성 분야에서는 두 가지 주요 서비스를 대학의 상호 연결성을 제공합니다.

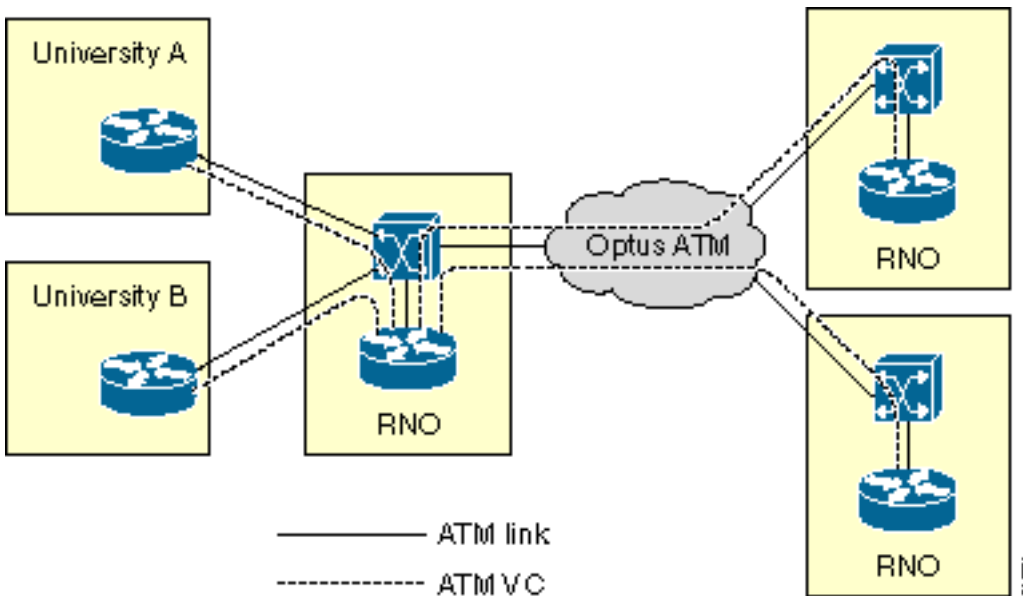
- 음성에 적합한 QoS(Quality of Service)를 보장하는 VoIP RTP(Realtime Transport Protocol) 패킷 전송
- 전국 PSTN을 위한 저렴한 호프오프 지점

이 섹션에서는 현재 AARNet 아키텍처와 이러한 서비스를 제공하는 방법에 대해 설명합니다. 또한 더 많은 대학에서 IP 텔레포니 솔루션을 구축함에 따라 발생하는 몇 가지 확장성 문제에 대해서도 설명합니다. 마지막으로, 이러한 확장성 문제를 해결할 수 있는 솔루션에 대해 설명합니다.

## AARNet 토폴로지

AARNet은 각 상태의 단일 POP(Point of Presence)로 구성됩니다. POP를 RNO(Regional Network Operations)라고 합니다. 대학은 해당 주에서 RNO에 연결됩니다. RNO는 Optus ATM PVC의 풀 메쉬로 상호 연결됩니다. 그들은 함께 AARNet을 구성합니다.

일반적인 RNO는 Cisco LS1010 ATM 스위치 1개와 ATM 연결 라우터 1개로 구성됩니다. RNO 라우터는 E3 전자레인지 링크를 통해 단일 ATM PVC를 통해 각 대학 라우터에 연결됩니다. 또한 모든 RNO 라우터에는 Optus ATM 네트워크가 다른 모든 RNO에 제공하는 ATM PVC의 풀 메쉬가 있습니다. 이 다이어그램은 네트워크의 일반적인 AARNet 토폴로지를 나타냅니다.



토폴로지에는 여러 가지 예외가 있습니다. 음성 관점에서는 상당한 의미가 있습니다. 다음은 몇 가지 예외입니다.

- Victoria의 RNO는 PVCs 대신 기존의 IP over ATM(RFC 1577)을 사용하여 대학을 RNO에 연결합니다.
- 시골 대학은 일반적으로 프레임 릴레이 또는 ISDN에 의한 RNO로 연결됩니다.
- 일부 대형 대학들은 RNO로 연결되는 링크가 두 개 이상 있습니다.

이 표에서는 현재 RNO가 있는 상태 및 영역을 보여 줍니다. 이 표에는 호주 지리에 익숙하지 않은 독자들을 위한 자본 도시가 포함되어 있습니다.

주/도	캐피탈 시티	RNO?	캠퍼스 연결
뉴사우스웨일스	시드니	예	미정
빅토리아	멜버른	예	미정
퀸즐랜드	브리즈번	예	미정
사우스오스트레일리아	애들레이드	예	미정

서호주	퍼스	예	미정
오스트레일리아 수도 구역	캔버라	예	미정
북부 지역	다윈	아니요	—
태즈메이니아	호바트	아니요	—

## QoS(Quality of Service)

VoIP 유료 우회 프로젝트의 결과로 AARNet의 일부가 이미 음성에 대해 QoS가 활성화되었습니다. 지연 및 지터를 최소화하고 패킷 손실을 방지하는 이러한 기능을 제공하려면 QoS가 음성 트래픽에 필요합니다.

- Policing(폴리싱) - 신뢰할 수 없는 소스의 음성 트래픽을 표시합니다.
- Queuing(대기 중) - 링크 혼잡 중 지연을 최소화하려면 음성에 다른 모든 트래픽보다 우선 순위가 부여되어야 합니다.
- LFI(Link Fragmentation and Interleaving) - 데이터 패킷은 프래그먼트화되어야 하며 음성 패킷은 느린 링크에 인터리빙되어야 합니다.

트래픽은 올바른 경찰 및 대기열 음성 패킷으로 분류되어야 합니다. 이 섹션에서는 AARNet에서 분류가 수행되는 방법에 대해 설명합니다. 후속 장에서는 폴리싱 및 큐잉 구현에 대해 설명합니다.

## 분류

모든 트래픽이 동일한 QoS를 얻는 것은 아닙니다. 트래픽은 선택적으로 QoS를 제공하기 위해 다음 범주로 분류됩니다.

- 데이터
- 알려진 소스 및 신뢰할 수 있는 소스의 음성
- 알 수 없는 소스의 음성

신뢰할 수 있는 디바이스에만 AARNet에 고품질 QoS가 제공됩니다. 이러한 디바이스는 주로 IP 주소로 식별되는 게이트웨이입니다. ACL(Access Control List)은 이러한 신뢰할 수 있는 음성 소스를 식별하는 데 사용됩니다.

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

IP 우선 순위는 음성 트래픽과 데이터 트래픽을 구분하는 데 사용됩니다. 음성의 IP 우선 순위는 5입니다.

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

이전 예를 결합하여 신뢰할 수 있는 소스의 패킷을 식별합니다.

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

동일한 원칙을 사용하여 알 수 없는 소스에서 음성 패킷을 식별합니다.

```
class-map match-all VOICE-NOT-GATEWAY
```

```
match class-map VOICE
match not access-group 20
```

## 폴리싱

신뢰할 수 없는 소스의 음성 트래픽은 트래픽이 인터페이스에 도달하면 분류되어 다운된 것으로 표시됩니다. 다음 두 예는 지정된 인터페이스에 도착할 것으로 예상되는 트래픽 유형에 따라 폴리싱을 수행하는 방법을 보여줍니다.

라우터는 신뢰할 수 없는 음성 패킷을 찾고 신뢰할 수 있는 음성 소스가 다운스트림에 있는 경우 IP 우선 순위를 0으로 변경합니다.

```
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
```

라우터는 모든 음성 패킷을 검색하고 알려진 음성 소스가 없는 경우 IP 우선순위를 0으로 변경합니다.

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

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

## 비음성 대기열

AARNet의 모든 VoIP는 최근까지 유료 바이패스였습니다. 이 경우 상대적으로 적은 수의 VoIP 엔드 포인트가 발생합니다. 현재 대기 설계에서는 VoIP 디바이스가 다운스트림에 있는 인터페이스와 다운스트림이 없는 인터페이스를 구분합니다. 이 섹션에서는 비 VoIP 인터페이스에서 대기하는 방법에 대해 설명합니다.

비음성 인터페이스는 WFQ(Weighted Fair Queuing) 또는 WRED(Weighted Random Early Detection)에 대해 구성됩니다. 인터페이스에서 직접 구성할 수 있습니다. 그러나 지정된 인터페이스 유형에서 대기열 메커니즘을 쉽게 변경할 수 있도록 정책 맵을 통해 대기열 지정 메커니즘이 적용됩니다. 인터페이스 유형당 하나의 정책 맵이 있습니다. 이는 모든 대기 메커니즘이 모든 인터페이스에서 지원되지는 않는다는 사실을 반영합니다.

```
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
```

정책 맵은 각 인터페이스에 연결되며 인터페이스 유형에 따라 다릅니다. 예를 들어, VIP 기반 (Versatile Interface Processor-based) 이더넷 포트의 큐잉 메커니즘을 WRED에서 WFQ로 변경하는 프로세스가 간소화됩니다. 정책 맵에서 단일 변경이 필요합니다. 모든 VIP 기반 이더넷 인터페이스가 변경됩니다.

```
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
```

## 짧은 대기 시간 대기

다운스트림 트러스트된 VoIP 디바이스가 있는 인터페이스는 LLQ(Low Latency Queuing)에 대해 구성됩니다. 수신 인터페이스 분류를 통과하고 5의 우선 순위를 유지하는 패킷은 LLQ의 적용을 받습니다. 다른 모든 패킷은 WFQ 또는 WRED의 영향을 받습니다. 이는 인터페이스 유형에 따라 달라집니다.

QoS를 보다 쉽게 관리할 수 있도록 각 인터페이스 유형에 대해 별도의 정책 맵이 생성됩니다. 이는 비음성 대기열 설계와 유사합니다. 그러나 각 인터페이스 유형에 대해 여러 정책 맵이 있습니다. 이는 음성 트래픽을 전달하는 인터페이스 유형의 용량이 링크 속도, PVC 설정 등에 따라 다르기 때문입니다. 정책 맵 이름의 숫자는 30건의 통화, 60건의 통화 발신 등에 맞춘 통화 수를 나타냅니다.

```
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
```

정책 맵은 각 인터페이스에 연결됩니다. 이 예에서 정책 맵은 인터페이스 유형에 따라 다릅니다. 현재 음성 신호에는 특별한 처리가 주어지지 않습니다. 정책 맵은 지정된 인터페이스 유형의 이후 단계에서 요구 사항이 될 경우 한 곳에서 쉽게 수정할 수 있습니다. 변경 사항은 해당 유형의 모든 인터페이스에 적용됩니다.

```
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
```

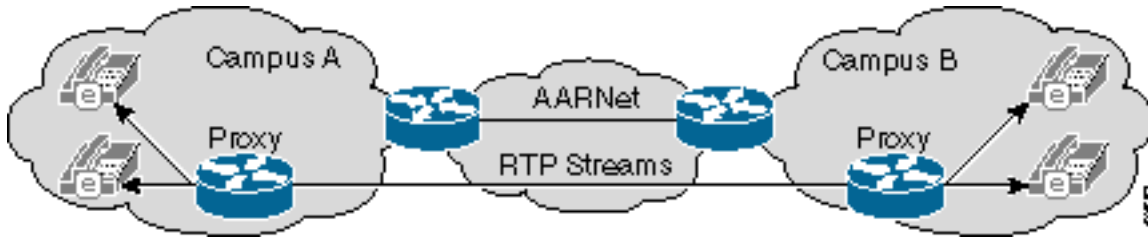
## LLQ 확장성

대기 메커니즘에 확장성 문제가 있습니다. 주요 문제는 네트워크에서 신뢰할 수 있는 모든 VoIP 디바이스의 IP 주소를 파악하는 데 있습니다. 과거에는 유료 우회를 처리하는 VoIP 게이트웨이의 수가 제한적이었지만 이는 합리적인 한계였습니다. VoIP 엔드포인트의 수가 크게 증가하며, IP 텔레포니 구축으로 인해 점점 더 비현실적이 됩니다. ACL이 너무 길어지고 관리하기가 너무 어려워집니다.

ACU의 경우 ACL은 각 ACU 캠퍼스의 특정 음성 IP 하위 네트워크로부터 트래픽을 신뢰하도록 추가되었습니다. 이것은 임시 해결책이다. 이러한 장기적인 솔루션은 다음과 같이 조사됩니다.

- H.323 프록시
- QoS 인그레스 폴리싱

H.323 프록시 솔루션의 주요 목적은 프록시를 통해 지정된 캠퍼스에서 모든 RTP 트래픽이 AARNet에 유입되도록 하는 것입니다. AARNet은 다음 다이어그램에서 보여주는 것처럼 지정된 캠퍼스의 모든 RTP 트래픽을 단일 IP 주소로 확인합니다.

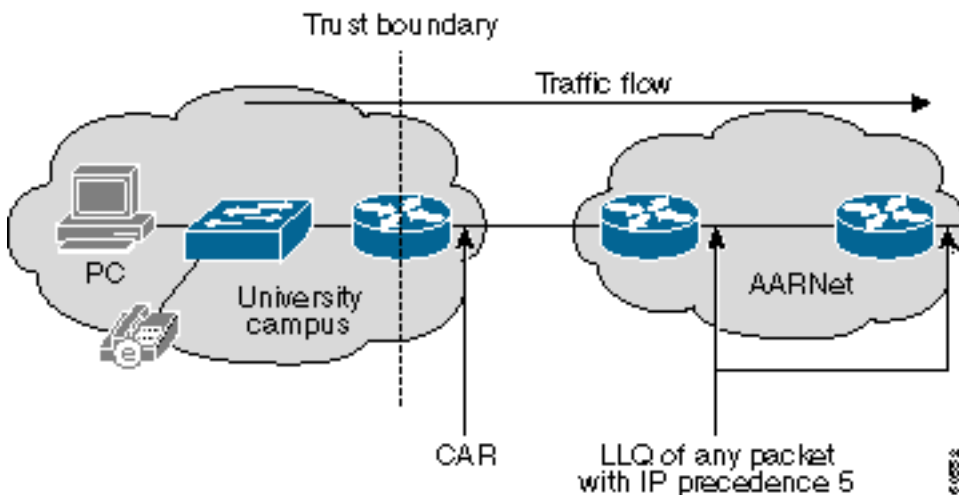


QoS ACL의 항목 수는 이 구성표가 일관되게 구축된 경우 캠퍼스당 한 줄로 제한됩니다. 여러 캠퍼스를 보유한 대학이 37곳이기 때문에 이 체계에는 100개 이상의 엔트리를 추가할 수 있는 가능성이 있습니다. 이 역시 확장성이 없습니다. 각 RNO에서 단일 또는 제한된 수의 공유 수퍼 프록시를 사용하여 설계로 이동해야 할 수 있습니다. 이렇게 하면 신뢰할 수 있는 IP 주소 수가 6개로 줄어듭니다. 그러나 이렇게 하면 캠퍼스에서 RNO의 프록시로의 경로에 대한 QoS 폴리싱 문제가 열립니다.

**참고:** Cisco CallManager 인터클러스터 트렁크는 클러스터 간 신호 처리가 네이티브 H.225가 아니므로 현재 H.323 프록시를 통해 작동하지 않습니다.

QoS 인그레스 폴리싱은 대안적인 솔루션입니다. 이 설계로 캠퍼스가 RNO에 연결되는 지점에서 신뢰 경계가 설정됩니다. AARNet으로 들어오는 트래픽은 이 경계에서 Cisco IOS® CAR(Committed Access Rate) 기능에 의해 폴리싱됩니다. VoIP에 AARNet을 사용하는 대학은 일정 양의 AARNet QoS 대역폭을 구독합니다. 그런 다음 CAR은 AARNet으로 들어오는 트래픽을 모니터링합니다. IP 우선순위 5의 RTP 트래픽 양이 가입한 대역폭을 초과하는 경우 초과 트래픽의 IP 우선 순위는 0으로 표시됩니다.

다음 다이어그램은 CAR 컨피그레이션을 보여줍니다.



다음 예에서는 CAR 컨피그레이션이 이 폴리싱을 처리하는 방법을 보여 줍니다.

```
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
```

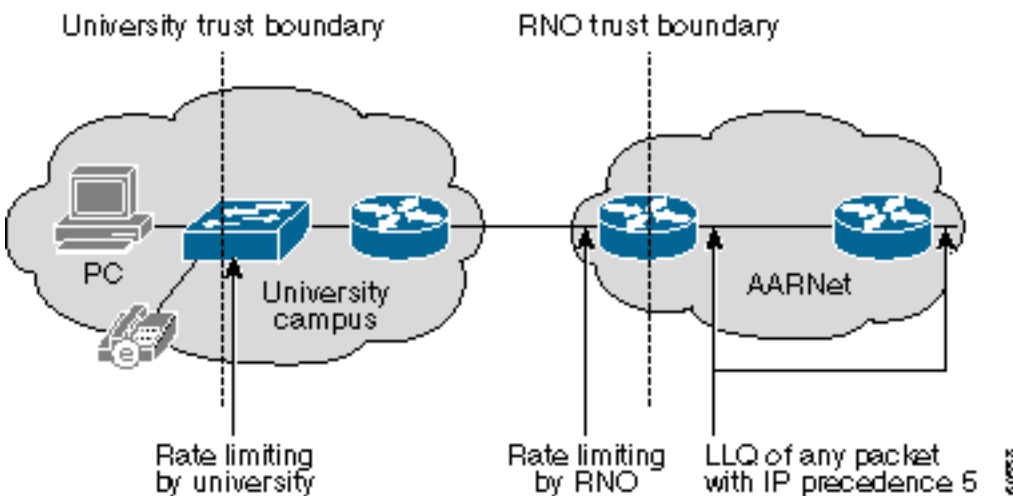


```
access-list 100 permit udp any range 16384 32767 any range
16384 32767 precedence critical
```

다음은 CAR 컨피그레이션 접근 방식의 몇 가지 장점입니다.

- 코어는 더 이상 폴리싱을 처리할 필요가 없습니다. 이제 신뢰 경계에서 처리됩니다. 따라서 코어의 LLQ는 신뢰할 수 있는 IP 주소에 대해 알 필요가 없습니다. 코어에서 IP 우선 순위가 5인 패킷은 인그레스(ingress)에서 이미 폴리싱을 통과했기 때문에 LLQ에 안전하게 적용될 수 있습니다.
- 개별 대학에서 선택하는 VoIP 아키텍처, 장비 및 프로토콜에 대해 어떠한 가정도 이루어지지 않습니다. 대학은 H.323 프록시에서 작동하지 않는 SIP(Session Initiation Protocol) 또는 MGCP(Media Gateway Control Protocol)를 구축하도록 선택할 수 있습니다. VoIP 패킷은 IP 우선 순위가 5인 경우 코어에서 적절한 QoS를 수신합니다.
- CAR은 QoS DoS(Denial of Service) 공격에 대비하여 탄력적으로 작동합니다. 대학에서 시작된 QoS DoS 공격은 코어를 손상시킬 수 없습니다. CAR은 공격을 제한하므로 허용되는 최대 VoIP 통화 수가 활성 상태일 때 현재 트래픽 수보다 많은 트래픽을 생성할 수 없습니다. 해당 캠퍼스를 오가는 VoIP 통화는 공격 중에 발생할 수 있습니다. 그러나 내적으로 스스로를 보호하는 것은 개별 대학의 책임이다. 이 대학은 선택된 모든 VoIP 하위 네트워크가 IP 우선 순위가 아래로 표시되도록 라우터에서 CAR ACL을 조정할 수 있습니다. 각 캠퍼스에는 최종 설계에서 사용자가 캠퍼스 LAN에 연결하는 지점에서 내부 신뢰 경계가 있습니다. 이 신뢰 경계가 수신하는 IP 우선 순위가 5인 트래픽은 스위치 포트당 160kbps 또는 G.711 VoIP 호출 2개로 제한됩니다. 이 속도를 초과하는 트래픽은 다운된 것으로 표시됩니다. 이 체계를 구현하려면 속도 제한 기능이 있는 Catalyst 6500 스위치 또는 이와 유사한 제품이 필요합니다.
- 코어의 대역폭 프로비저닝은 각 대학이 고정된 양의 QoS 대역폭을 구독할 때 간소화됩니다. 따라서 각 대학이 QoS 대역폭 서브스크립션을 기반으로 월 단위 요금을 균등하게 지불할 수 있으므로 QoS 청구 과정이 간단해집니다.

이 설계의 주요 단점은 신뢰 경계가 대학 라우터에 있으므로 대학이 CAR을 올바르게 관리할 수 있어야 한다는 것입니다. 신뢰 경계는 RNO로 다시 폴링됩니다. RNO 관리 장비는 궁극적인 설계에서 폴리싱을 처리합니다. 이 설계에는 Catalyst 6000 스위치 또는 Cisco 7200 Network Services Engine(Cisco 7200 NSE-1) 프로세서와 같은 하드웨어 기반 속도 제한이 필요합니다. 그러나 AARNet 및 RNO는 QoS 폴리싱을 완벽하게 제어할 수 있습니다. 이 다이어그램은 다음 설계를 보여줍니다.



### 링크 조각화 및 인터리빙

VoIP는 상대적으로 고속 ATM VC(Virtual Circuit)를 통해서만 전달됩니다. 따라서 LFI는 필요하지 않습니다. 또한 VoIP는 FRF(Frame Relay Forum)를 통해 전송되거나 향후 지방 대학에 임대 회선

을 제공할 수도 있습니다. 이를 위해서는 Interleave 또는 FRF.12를 사용하는 MLP(Multilink PPP)와 같은 LFI 메커니즘이 필요합니다.

## 게이트웨이

AARNet에는 두 가지 종류의 H.323 게이트웨이가 있습니다.

- PSTN - PSTN-VoIP 게이트웨이
- PABX - PABX-VoIP 게이트웨이

PSTN과 PABX 게이트웨이의 차이점은 주로 기능적입니다. PSTN 게이트웨이는 PSTN에 대한 연결을 제공합니다. PABX 게이트웨이는 대학 PABX를 VoIP 백본에 연결합니다. 대부분의 경우 동일한 물리적 상자가 PSTN 및 PABX 게이트웨이 역할을 합니다. 현재 ACU IP 텔레포니 솔루션에는 31개의 게이트웨이가 있습니다. 이러한 게이트웨이 대부분은 Cisco AS5300 Universal Access Server입니다. 다른 게이트웨이는 Cisco 3600 Series 라우터 또는 Cisco 2600 Series 라우터입니다. 2001년 Q2에는 최소 10개의 추가 게이트웨이가 추가될 예정입니다. 2001년 4월에 약 145,000건의 VoIP 통화가 수행되었습니다.

AARNet은 다음 다이어그램에서 보여주는 것처럼 대부분의 주요 도시에 PSTN 연결 H.323 게이트웨이를 구축했습니다.

Key:

AARNet H.323 Gateway



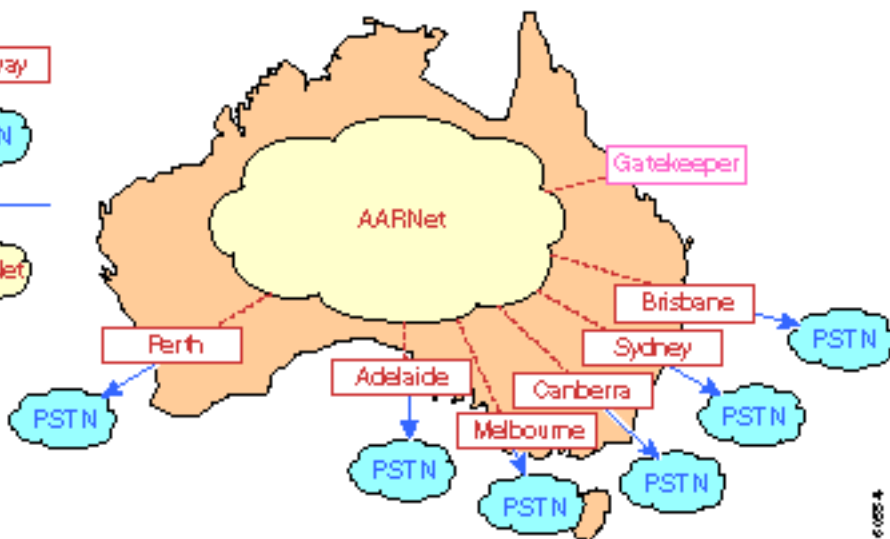
Public Telephone Network



ISDN



AARNet TCP/IP Network



대학은 이러한 게이트웨이를 사용하여 PSTN으로 아웃바운드 전화를 걸 수 있습니다. 대학은 현재 지원되지 않기 때문에 인바운드 통화를 위해 자신의 트렁크를 유지 관리해야 합니다. AARNet은 이러한 게이트웨이를 통과하는 통화 수 때문에 통신사와 매우 경쟁력 있는 가격을 협상할 수 있습니다. 또한 가장 비용 효율적인 지점에서 통화를 취소할 수 있습니다. 예를 들어, 시드니에서 퍼스 번호로 전화를 거는 사람은 퍼스 게이트웨이를 사용할 수 있으며 시내 통화만 요금이 부과됩니다. TEHO(Tail End Hop Off)라고도 합니다.

단일 게이트키퍼가 구축되어 E.164-IP 주소 확인을 수행합니다. PSTN에 대한 모든 통화는 게이트키퍼로 전송되며, 게이트키퍼는 가장 적합한 게이트웨이의 IP 주소를 반환합니다. 게이트키퍼에 대한 자세한 내용은 [다이얼 플랜](#) 및 [게이트키퍼](#) 섹션을 참조하십시오.

## 청구 및 회계

PSTN 게이트웨이는 RADIUS 및 AAA(Authentication, Authorization, and Accounting)를 청구 용도로 사용합니다. 게이트웨이를 통한 각 통화는 각 통화 레그에 대한 CDR(Call Detail Record)을 생성합니다. 이러한 CDR은 RADIUS 서버에 게시됩니다. CDR에 있는 Cisco CallManager의 IP 주소는

해당 대학을 고유하게 식별하고 올바른 당사자가 청구되도록 합니다.

## 게이트웨이 보안

DoS 공격 및 사기 행위로부터 PSTN 게이트웨이를 보호하는 것은 중요한 문제입니다. H.323 클라이언트는 널리 사용 가능합니다. Microsoft NetMeeting은 Microsoft Windows 2000과 함께 번들로 제공되므로, 기술 전문가가 아닌 사용자가 이러한 게이트웨이를 통해 무료 전화를 쉽게 걸 수 있습니다. 이러한 게이트웨이를 보호하기 위해 신뢰할 수 있는 IP 주소에서 H.225 신호 처리를 허용하는 인바운드 ACL을 구성합니다. 이 접근 방식에는 QoS 섹션에서 설명하는 것과 동일한 확장성 문제가 모두 있습니다. 신뢰할 수 있는 H.323 엔드포인트 수가 증가하면 ACL의 항목 수가 증가합니다.

H.323 프록시는 이 지역에서 약간의 안도감을 제공합니다. PSTN 게이트웨이를 통한 모든 통화가 캠퍼스 프록시를 통과하는 경우 게이트웨이 ACL은 대학 캠퍼스당 하나의 IP 주소를 허용해야 합니다. 대부분의 경우 이중화된 프록시로 두 개의 IP 주소를 사용하는 것이 좋습니다. 프록시를 사용하더라도 ACL은 100개 이상의 항목을 포함할 수 있습니다.

H.323에서 프록시를 통해 통화를 설정할 수 있으므로 프록시는 ACL을 통해 보호되어야 합니다. 로컬 정책에 따라 로컬 H.323 디바이스가 캠퍼스별로 수행되므로 프록시 ACL은 로컬 H.323 디바이스를 허용해야 합니다.

캠퍼스에서 AARNet PSTN 게이트웨이를 사용하도록 IP 전화의 통화만 허용하려는 경우 두 Cisco CallManager의 IP 주소가 게이트웨이 ACL에 포함되어야 합니다. 프록시가 이 상황에서 값을 추가하지 않습니다. 필수 ACL 항목의 수는 양방향입니다.

캠퍼스 내 IP Phone-to-IP 통화는 프록시를 통과할 필요가 없습니다.

## 다이얼 플랜

현재 VoIP 다이얼 플랜은 간단합니다. 사용자는 VoIP 게이트웨이 관점에서 다음과 같은 두 가지 유형의 통화를 발신할 수 있습니다.

- 다른 캠퍼스에서 전화를 걸지만 같은 대학에서 전화를 겁니다.
- 다른 대학에서 PSTN 전화나 전화기로 전화하세요.

게이트웨이 다이얼 피어는 두 가지 유형의 통화만 있다는 사실을 반영합니다. 기본적으로 다음 예에서는 두 가지 VoIP 다이얼 피어 유형이 있습니다.

```
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
```

첫 번째 다이얼 피어는 이 예에서 다른 캠퍼스에서 내선 번호 7...을 호출하는 경우 사용됩니다. 이 통화는 원격 게이트웨이의 IP 주소로 직접 라우팅됩니다. 게이트키퍼가 우회되므로 CAC(Call Admission Control)가 수행되지 않습니다.

두 번째 다이얼 피어는 통화가 PSTN 번호용일 때 사용됩니다. 다음 항목 중 하나일 수 있습니다.

- PSTN의 전화 번호
- 다른 대학의 전화기의 정규화된 PSTN 번호

첫 번째 케이스의 ARQ(Admission Request) 메시지를 통해 통화가 게이트키퍼에게 전송됩니다. 게이트키퍼는 ACF(Admission Confirm) 메시지에서 최상의 PSTN 게이트웨이의 IP 주소를 반환합니다.

두 번째 경우에는 ARQ 메시지를 통해 게이트키퍼에게 통화가 전송됩니다. 그러나 게이트키퍼는 통화를 수신하는 대학에서 VoIP 게이트웨이의 IP 주소가 포함된 ACF 메시지를 반환합니다.

## 게이트키퍼

AARNet은 현재 단일 게이트키퍼를 운영합니다. 이 게이트키퍼의 유일한 목적은 E.164-IP 주소 확인 형식으로 통화 라우팅을 수행하는 것입니다. 게이트키퍼는 CAC를 수행하지 않습니다. 게이트웨이에 연결된 PABX 트렁크의 수는 동시 통화 수를 제한합니다. 코어 대역폭은 한 번에 사용 중인 모든 트렁크를 제공합니다. 이는 ACU 및 다른 대학에서 IP 텔레포니를 출시함으로써 변경됩니다. 이 새로운 환경에서 지정된 캠퍼스에서 또는 외부로 소싱할 수 있는 동시 VoIP 통화 수에 대한 자연스러운 제한은 없습니다. 너무 많은 통화가 시작된 경우 사용 가능한 QoS 대역폭을 초과 구독할 수 있습니다. 이런 상태에서는 모든 전화의 품질이 떨어질 수 있다. 게이트키퍼를 사용하여 CAC를 제공합니다.

분산형 특성과 잠재적 규모 덕분에 분산된 게이트키퍼 아키텍처에 도움이 됩니다. 한 가지 가능한 해결책은 각 대학이 자체 게이트키퍼를 유지 관리하는 2계층 게이트키퍼 설계를 사용하는 것입니다. 이 대학 게이트키퍼를 계층 2 게이트키퍼라고 합니다. AARNet은 계층 1 게이트키퍼라고 하는 *디렉토리* 게이트키퍼를 작동합니다.

대학은 Cisco CallManager 클러스터 간 통화 라우팅에 게이트키퍼를 사용하려면 이 2계층 방식을 사용해야 합니다. 게이트키퍼는 이 시나리오에서 4자리 또는 5자리 내선 번호를 기준으로 통화를 라우팅합니다. 각 대학에는 고유의 게이트키퍼가 필요합니다. 이는 로컬에서 관리되는 주소 공간이므로 확장 범위가 대학 간에 겹치기 때문입니다.

대학 Tier 2 게이트키퍼는 해당 대학과의 통화에만 CAC를 수행합니다. 또한 해당 대학의 캠퍼스만 통화할 경우 E.164 해결을 수행합니다. 다른 대학에서 IP 전화를 걸거나 AARNet 게이트웨이를 통해 PSTN을 호출하는 경우, 계층 2 게이트키퍼가 LRQ(Tier 1 게이트키퍼)를 통해 통화를 계층 1 게이트키퍼로 라우팅합니다. 통화가 다른 대학의 경우 LRQ는 해당 대학의 Tier 2 게이트키퍼에게 전달됩니다. 그런 다음 이 게이트키퍼는 통화가 시작되는 대학의 Tier 2 게이트키퍼에게 ACF 메시지를 반환합니다. 두 Tier 2 게이트키퍼는 CAC를 수행합니다. 통화와 호출된 영역 모두에서 사용 가능한 대역폭이 충분한 경우에만 통화를 진행합니다.

AARNet은 AARNet PSTN 게이트웨이를 어떤 대학의 게이트웨이와 같이 처리하도록 선택할 수 있습니다. Tier 2 게이트키퍼가 그들을 돌봅니다. 또한 Tier 1 게이트키퍼는 로드 및 성능이 허용되는 경우 이러한 게이트웨이의 Tier 2 게이트키퍼 역할을 할 수 있습니다.

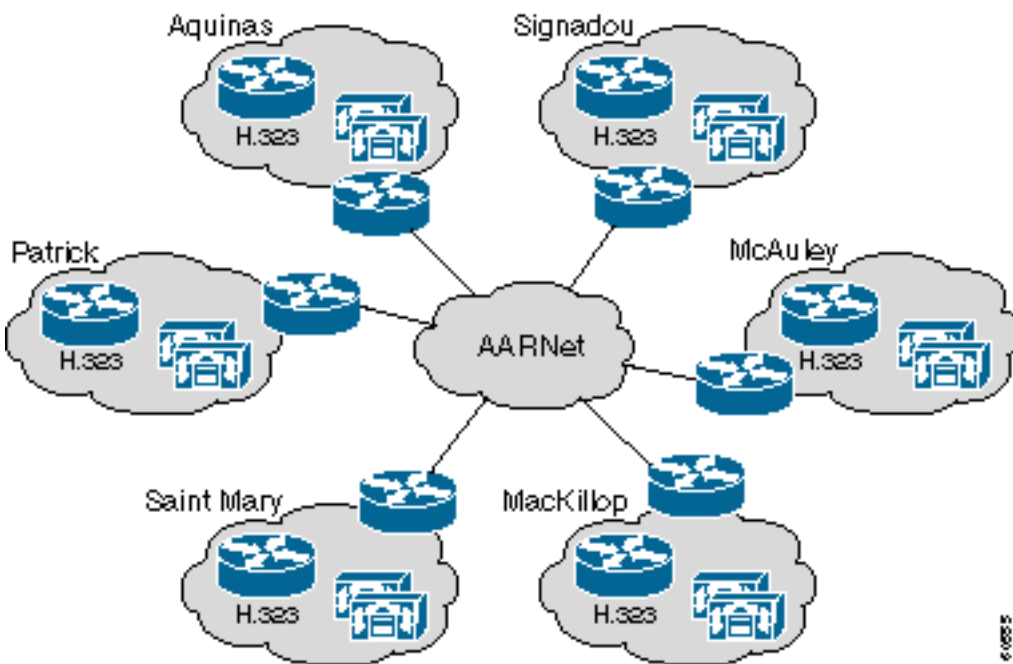
게이트웨이는 매우 중요한 구성 요소이므로 AARNet 디렉토리 게이트키퍼를 포함한 각 게이트키퍼를 복제해야 합니다. 각 대학에는 두 명의 게이트키퍼가 필요합니다. Cisco IOS Software Release 12.0(7)T와 같이 Cisco IOS 게이트웨이에 대체 게이트키퍼가 있을 수 있습니다. 그러나 현재 Cisco CallManager 또는 다른 타사 H.323 디바이스에서 이 기능을 지원하지 않습니다. 지금은 이 기능을 사용하지 마십시오. 대신 간단한 HSRP 기반(Hot Standby Router Protocol-based) 솔루션을 사용하십시오. 이를 위해서는 두 게이트키퍼가 동일한 IP 하위 네트워크에 있어야 합니다. HSRP는 어떤 게이트키퍼가 활성 상태인지 결정합니다.

## ACU IP 텔레포니 네트워크

다음 표는 ACU 캠퍼스에 설치된 IP 전화의 대략적인 수를 보여줍니다.

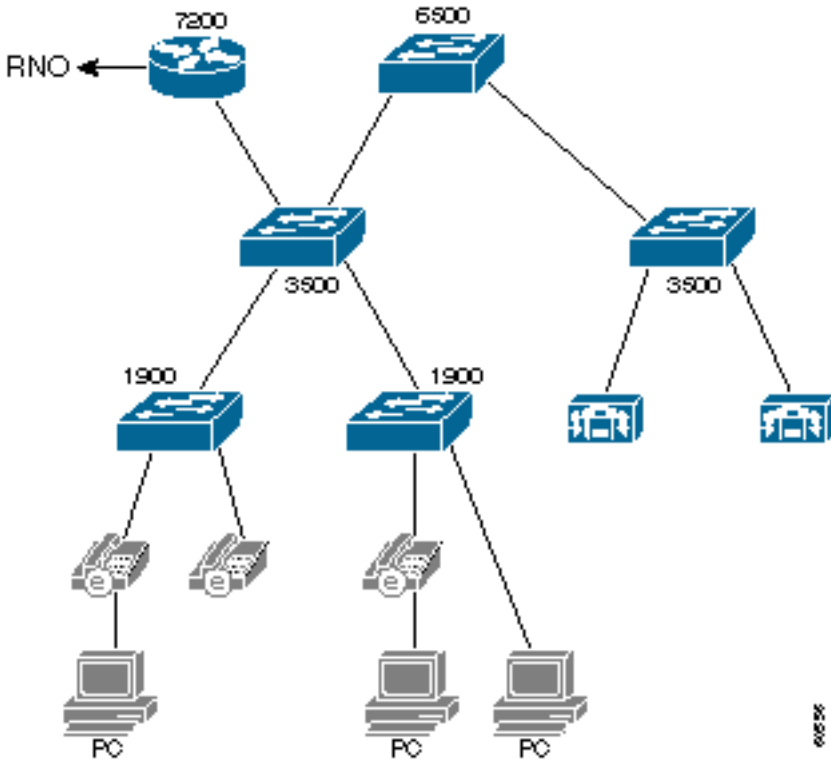
캠퍼스	구/군/시	대략적인 IP 전화
세인트 메리 산	스트라스필드	400
맥킬롭	시드니 북부	300
패트릭	멜버른	400
아퀴나스	발라랏	100
사이나두	캔버라	100
맥컬리	브리즈번	400
	<b>합계:</b>	<b>1700</b>

ACU는 최근 IP 텔레포니 솔루션을 구축했습니다. 이 솔루션은 두 개의 Cisco CallManager, 각 캠퍼스의 Cisco 3640 게이트웨이, IP 전화로 구성된 클러스터로 구성됩니다. AARNet은 캠퍼스를 상호 연결합니다. 다음 다이어그램은 ACU IP 텔레포니 네트워크의 상위 토폴로지 및 다양한 구성 요소를 보여줍니다.



## ACU 네트워크 토폴로지

이 다이어그램은 일반적인 ACU 캠퍼스를 보여줍니다. 각 캠퍼스에는 3개의 Catalyst 스위치 레이어가 있습니다. 와이어링 클로짓에는 이전 Catalyst 1900 스위치가 있습니다. Catalyst 1900 스위치는 확장 프레임밍을 통해 Catalyst 3500XL 스위치에 다시 연결됩니다. 기가비트 이더넷(GE)을 통해 단일 Catalyst 6509 스위치에 다시 연결됩니다. 단일 Cisco 7200 VXR 라우터는 ATM VC를 통해 로컬 RNO에 캠퍼스를 AARNet에 연결합니다.



이 표에 나와 있는 것처럼 RNO에 대한 연결 방법은 상태와 약간 다릅니다. Victoria는 Classic IP over ATM(RFC 1577)을 기반으로 합니다. 다른 RNO에는 RFC 1483 캡슐화를 사용하는 직선 PVC 설정이 있습니다. OSPF(Open Shortest Path First)는 ACU와 RNO 간에 사용되는 라우팅 프로토콜입니다.

캠퍼스	주/도	RNO에 연결	라우팅 프로토콜
세인트 메리산	NSW	RFC 1483 PVC	OSPF
맥킬롭	NSW	RFC 1483 PVC	OSPF
패트릭	VIC	RFC 1577 ATM을 통한 기존 IP	OSPF
아퀴나스	VIC	RFC 1577 ATM을 통한 기존 IP	OSPF
사이나두	법률	RFC 1483 PVC	OSPF
맥컬리	QLD	RFC 1483 PVC	OSPF

Catalyst 1900 시리즈 스위치는 업링크에서만 트렁킹을 지원합니다. 따라서 IP 전화와 PC는 모두 하나의 대규모 VLAN에 있습니다. 실제로 전체 캠퍼스는 하나의 대규모 VLAN 및 브로드캐스트 도메인입니다. 장치 수가 많기 때문에 보조 IP 하위 네트워크가 사용됩니다. IP 전화는 한 IP 하위 네트워크에 있고 PC는 다른 네트워크에 있습니다. AARNet 코어는 IP 전화 하위 네트워크를 신뢰하며, 이 IP 하위 네트워크에서 들어오고 나가는 트래픽은 LLQ의 적용을 받습니다.

Cisco 7200 라우터는 기본 및 보조 IP 하위 네트워크 간에 라우팅됩니다. Catalyst 6500 스위치의 MSFC(Multilayer Switch Feature Card)는 현재 사용되지 않습니다.

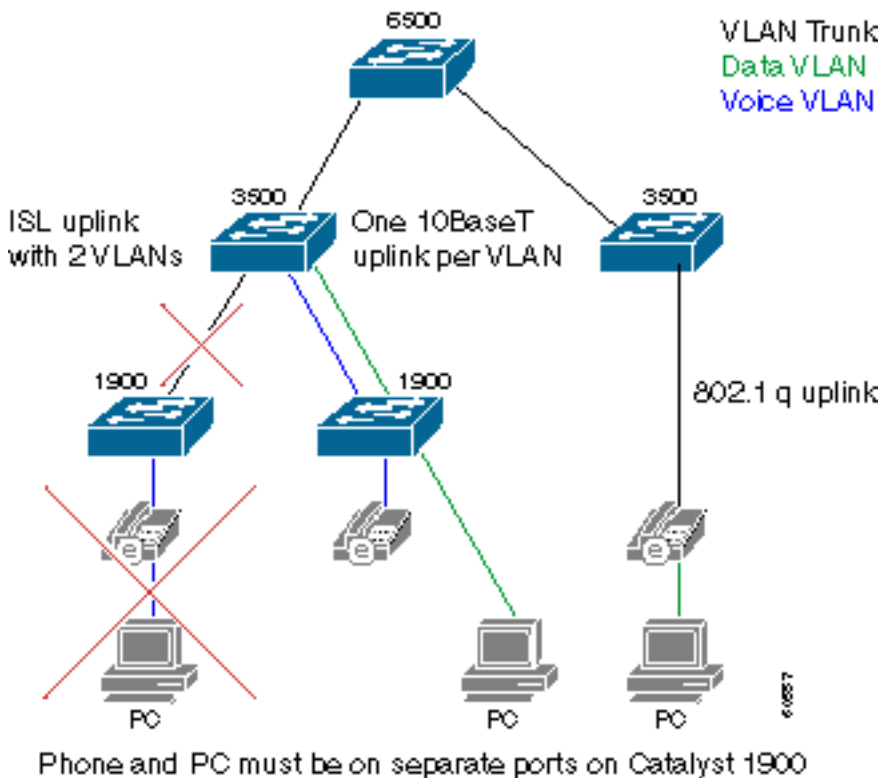
Catalyst 3500XL 및 Catalyst 6500 스위치에는 QoS 기능이 있지만 현재 활성화되어 있지 않습니다.

## 캠퍼스의 QoS

현재 캠퍼스 설계는 IP 텔레포니에 대한 Cisco 권장 설계 지침을 따르지 않습니다. 다음은 QoS에 대한 몇 가지 문제입니다.

- 브로드캐스트 도메인이 매우 큼. 과도한 브로드캐스트는 IP 전화의 성능에 영향을 미칠 수 있으며, 이를 처리해야 합니다.
- Catalyst 1900 스위치는 QoS를 지원하지 않습니다. IP 전화와 PC가 동일한 스위치 포트에 연결된 경우 PC에서 데이터를 높은 속도로 수신하면 음성 패킷이 삭제될 수 있습니다.

캠퍼스 인프라의 일부를 재설계하여 상당한 개선 사항을 달성합니다. 하드웨어 업그레이드가 필요하지 않습니다. 이 다이어그램은 권장 재설계 이면의 원칙을 설명합니다.



캠퍼스는 음성 VLAN 및 데이터 VLAN으로 분할되어야 합니다. 이제 Catalyst 1900 스위치에 연결하는 전화기와 PC를 다른 포트에 연결하여 VLAN을 분리해야 합니다. 각 Catalyst 1900 스위치에서 Cisco 3500XL 스위치의 추가 업링크가 추가됩니다. 두 업링크 중 하나가 음성 VLAN의 멤버입니다. 다른 업링크는 데이터 VLAN의 멤버입니다. 두 업링크 대신 ISL(InterSwitch Link) 트렁킹을 사용하지 마십시오. 이는 음성 및 데이터 트래픽에 별도의 대기열을 제공하지 않습니다. Catalyst 3500XL 스위치에서 Catalyst 6000 스위치로 연결되는 GE 링크도 802.1q 트렁크로 변환하여 음성 및 데이터 VLAN을 이 코어 스위치에서 전달할 수 있어야 합니다.

데이터 VLAN에 있는 Catalyst 3500XL 스위치의 포트는 기본 CoS(Class of Service)가 0입니다. 음성 VLAN의 구성원인 포트에는 기본 CoS가 5입니다. 따라서 음성 트래픽이 Catalyst 3500 또는 Catalyst 6500 코어에 도착하면 음성 트래픽의 우선 순위가 올바르게 지정됩니다. Catalyst 3500 QoS 스위치 포트 구성은 구성원인 VLAN 스위치 포트에 따라 약간 달라집니다. 예를 들면 다음과 같습니다.

```
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 전화가 Catalyst 3500XL 스위치에 직접 연결되는 드문 경우라면 PC를 IP 전화의 후면 스위치 포트에 연결할 수 있습니다. 이 경우 IP 전화는 802.1q 트렁크를 통해 스위치에 연결됩니다. 이렇게 하면 음성 및 데이터 패킷이 별도의 VLAN에서 이동할 수 있으며, 인그레스(ingress)에 올바른 CoS를 패킷에 제공할 수 있습니다. Catalyst 1900 스위치를 Catalyst 3500XL 스위치 또는 기타 QoS 지원 스위치로 교체하십시오. 그런 다음 이 토폴로지는 IP 전화와 PC를 네트워크에 연결하는 표준 방법이 됩니다. 이 시나리오에서는 Catalyst 3500XL 스위치 QoS 컨피그레이션을 보여줍니다.

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

마지막으로 두 Cisco CallManager에 연결하는 두 개의 포트는 CoS를 3으로 하드코딩해야 합니다. Cisco CallManager는 모든 음성 신호 패킷에서 IP 우선순위를 3으로 설정합니다. 그러나 Cisco CallManager에서 Catalyst 3500XL 스위치로의 링크는 801.1p를 사용하지 않습니다. 따라서 다음 예와 같이 스위치에서 CoS 값이 강제 적용됩니다.

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

이 설계의 주요 장애물은 두 개의 스위치 포트가 데스크톱에 필요하다는 것입니다. Patrick 캠퍼스에는 400개의 IP 전화에 추가로 400개의 스위치 포트가 필요할 수 있습니다. 충분한 포트가 없는 경우 추가 Catalyst 3500XL 스위치를 구축해야 합니다. 누락된 Catalyst 1900 스위치 포트 2개마다 하나의 Catalyst 3500XL 스위치 포트만 필요합니다.

현재 ACU Catalyst 6500 스위치는 QoS 기능을 가지고 있지만 현재 활성화되어 있지 않습니다. 이러한 모듈은 ACU Catalyst 6000 스위치에 다음과 같은 대기열 기능을 제공합니다.

슬롯	모듈	포트	RX 큐	TX 큐
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	—	—

Catalyst 6000 스위치에서 적절한 QoS 기능을 활성화하려면 다음 단계를 완료하십시오.

1. 스위치에서 다음 명령을 사용하여 VLAN별로 QoS를 제공하도록 지시합니다.

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

2. 다음 명령을 사용하여 Catalyst 3500XL 스위치에서 받은 CoS 값을 신뢰하도록 스위치에 알립니다.

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

이제 CoS를 차별화된 DSCP(서비스 코드 포인트) 매핑으로 설정해야 합니다. 이는 Catalyst 6000 스위치가 수신된 CoS 값을 기반으로 IP 헤더의 DSCP 값을 다시 쓰기 때문에 필요합니다. VoIP 신호 패킷에는 DSCP의 AF31(26)로 재작성된 3의 CoS가 있어야 합니다. RTP 패킷에는 EF(46)의



DSCP와 함께 재작성된 5의 CoS가 있어야 합니다. 다음 명령을 실행합니다.

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

이 예를 사용하여 CoS-to-DSCP 매핑을 확인합니다.

```
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
```

다양한 IP 하위 네트워크 간에 라우팅하도록 MSFC를 구성합니다.

## RNO의 QoS

현재 RNO 설계는 IP 텔레포니에 대한 Cisco 권장 설계 지침을 따르지 않습니다. QoS와 관련하여 다음과 같은 문제가 있습니다.

- LLQ는 Cisco ACU 7200 Series WAN 라우터에 적용되지 않습니다.
- Patrick 및 Aquinas 캠퍼스는 ATM SVC(Switched VC)를 통해 RNO에 연결됩니다. SVC에서는 LLQ가 지원되지 않습니다.

고속 이더넷에 연결된 Cisco 7200 라우터는 34Mbps E4 ATM 링크를 통해 캠퍼스를 RNO에 연결합니다. 4M과 1억 M의 속도 불일치로 인해 트래픽이 34M 링크에서 아웃바운드를 대기열에 추가할 수 있습니다. 따라서 음성 트래픽의 우선 순위를 지정해야 합니다. LLQ를 사용합니다. Cisco 7200 라우터 컨피그레이션은 다음 예와 유사합니다.

```
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
```

LLQ에 할당된 대역폭은  $N \times 24Kbps$ 여야 합니다. 여기서 N은 동시 G.729 통화 수입입니다.

Patrick 및 Aquinas Cisco 7200 라우터에서 AARNet 라우터로 각각 하나의 PVC를 설정합니다. Victoria RNO의 ATM SVC는 Classic IP over ATM(RFC 1577)을 기반으로 하므로 LLQ를 지원하지

않습니다. Victoria RNO의 다른 대학에서는 당분간 RFC 1577을 계속 사용할 수 있습니다. 그러나 결국 기존 IP over ATM 인프라를 대체합니다.

## 게이트웨이

각 ACU 캠퍼스에는 H.323 게이트웨이 역할을 하는 Cisco 3640 라우터가 있습니다. 이러한 게이트웨이는 ISDN을 통해 PSTN에 연결됩니다. PRI(Primary Rate Interfaces) 및 B 채널 수는 캠퍼스의 크기에 따라 달라집니다. 다음 표에는 각 캠퍼스의 PRI 및 B 채널 수가 나열되어 있습니다.

캠퍼스	PRI 수량	B-channel 수량
세인트 메리 산	2	30
맥킬롭	2	50
패트릭	2	50
아퀴나스	1	20
사이나두	1	20
맥컬리	1	30

이러한 게이트웨이는 DOD(직접 외부 전화 걸기)용 보조 게이트웨이로만 사용됩니다. AARNet 게이트웨이는 기본 게이트웨이입니다. ACU 게이트웨이는 항상 DID(Direct Inward Dialing)에 사용됩니다.

## 다이얼 플랜

다이얼 플랜은 4자리 내선 번호를 기반으로 합니다. 내선 번호는 DID 번호의 마지막 4자리이기도 합니다. 다음 표에는 각 캠퍼스의 확장 범위 및 DID 번호가 나열되어 있습니다.

캠퍼스	내선 번호	DID
세인트 메리 산	9xxx	02 9764 9xxx
맥킬롭	8xxx	02 9463 8xxx
패트릭	3xxx	03 8413 3xxx
아퀴나스	5xxx	03 5330 5xxx
사이나두	2xxx	02 6123 2xxx
맥컬리	7xxx	07 3354 7xxx

게이트웨이의 단순 num-exp 항목은 DID 번호를 Cisco CallManager에 전달하기 전에 4자리 확장자로 자릅니다. 예를 들어 Patrick 캠퍼스 게이트웨이에 다음과 같은 항목이 있습니다.

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

사용자가 0을 눌러 외부 회선을 선택합니다. 이 선행 0이 게이트웨이로 전달됩니다. 단일 POTS 다이얼 피어는 선행 0을 기반으로 ISDN 포트에서 통화를 라우팅합니다.

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

수신 통화에서는 이 num-exp 항목을 사용하여 발신자 번호를 4자리 내선으로 변환합니다. 그러면 통화가 두 VoIP 다이얼 피어와 일치합니다. 낮은 기본 설정에 따라 Cisco CallManager 가입자에게

이 경로를 선호합니다.

```
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

각 캠퍼스에는 2개의 Cisco CallManager 서버로 구성된 클러스터가 있습니다. Cisco CallManager 서버는 Media Convergence Server 7835(MCS-7835) 및 Media Convergence Server 7820(MCS-7820)이 혼합된 서버입니다. 두 서버 모두 이 게시 당시 버전 3.0(10)을 실행했습니다. 한 Cisco CallManager는 *게시자*이고 다른 Cisco CallManager는 *가입자*입니다. 가입자는 모든 IP 전화의 기본 Cisco CallManager 역할을 합니다. 다음 표에는 각 캠퍼스에 구축된 하드웨어가 나열되어 있습니다.

캠퍼스	플랫폼	통화 관리자
세인트 메리 산	MCS-7835	2
맥킬롭	MCS-7835	2
패트릭	MCS-7835	2
아퀴나스	MCS-7820	2
사이나두	MCS-7820	2
맥컬리	MCS-7835	2

각 클러스터는 다음 두 영역으로 구성됩니다.

- Intracampus 통화용 1개(G.711)
- 캠퍼스 내 통화용 1개(G.729)

각 클러스터에서 제공하는 모든 IP 전화가 단일 캠퍼스에 있으므로 위치 기반 CAC는 ACU에 적합하지 않습니다. 캠퍼스 간 통화에 대한 게이트키퍼 기반 CAC의 장점이 있지만 현재 구현되지 않았습니다. 하지만, 가까운 장래에 그렇게 할 계획이 있다.

각 Cisco CallManager는 22 H.323 게이트웨이로 구성됩니다. 이는 5개의 다른 Cisco CallManager 클러스터로의 클러스터 간 트렁크, 6개의 AARNet PSTN 게이트웨이, 각 캠퍼스의 ACU 게이트웨이 1개로 구성됩니다.

H.323 장치 유형	수량
캠퍼스 내 CallManager	2 x 5 = 10
AARNet PSTN 게이트웨이	6
ACU PSTN 게이트웨이	6
<b>합계:</b>	<b>22</b>

경로 목록 및 경로 그룹은 PSTN 게이트웨이의 순위를 지정하는 데 사용됩니다. 예를 들어, 이 표는 멜버른에 있는 Patrick Cisco CallManager에서 시드니 PSTN으로의 통화가 네 개의 게이트웨이를 사용하여 통화를 경로 그룹과 연결하는 방법을 보여줍니다.

게이트웨이	우선 순위
AARNet 시드니	1
ACU 시드니	2
AARNet 멜버른	3
ACU 멜버른	4

이 표에 나와 있는 것처럼 Cisco CallManager는 약 30개의 경로 패턴으로 구성됩니다. 경로 패턴은 모든 국내 호주 번호에 대해 특정 일치 항목이 있도록 설계되었습니다. 이렇게 하면 사용자는 Cisco CallManager가 통화를 시작하기 전에 숫자 시간 제한이 만료될 때까지 기다릴 필요가 없습니다. 와일드카드 문자 "!" 는 국제 번호에 대한 경로 패턴에서만 사용됩니다. 사용자는 국제 대상 전화를 걸 때 통화가 진행되기 전에 숫자 시간 제한(기본값 10초)이 만료될 때까지 기다려야 합니다. 사용자는 경로 패턴 "0.0011!#"을 추가할 수도 있습니다. 그런 다음 마지막 숫자 뒤에 "#"을 입력하여 전화를 건 번호가 완료되었음을 Cisco CallManager에 나타낼 수 있습니다. 이 작업은 국제 전화 걸기를 신속하게 처리합니다.

경로 패턴	설명
0.[2-9]XXXXXXX	로컬 통화
0.00	긴급 통화 - 사용자가 외부 회선에 대해 0으로 전화를 거는 것을 잊은 경우
0.000	긴급 통화
0.013	디렉터리 지원
0.1223	—
0.0011!	국제 전화
0.02XXXXXX	뉴사우스웨일스행 통화
0.03xxxxxx	빅토리아
0.04XXXXXX	휴대폰으로 통화
0.07XXXXXX	퀸즐랜드행 통화
0.086XXXXXXX	웨스턴 오스트레일리아 통화
0.08XXXXXX	호주 남부 및 북부 지역 통화
0.1[8-9]XXXXXX	1800 xxx 및 1900 xxx에 전화
0.1144X	긴급
0.119[4-6]	시간 및 날씨
0.1245X	디렉터리에 저장할 수 있습니다
0.13[1-9]XXX	13xxxx 번호로 통화
0.130XXXXXXX	1300xxx xxx번으로 전화 걸기
2[0-1]XX	Signadou에 대한 클러스터 간 통화
3[0-4]XX	Patrick에 대한 클러스터 간 통화
5[3-4]XX	Aquinas에 대한 클러스터 간 통화
7[2-5]XX	McAuley에 대한 클러스터 간 통화
8[0-3]XX	MacKillop에 대한 클러스터 간 통화
9[3-4]XX	성모 산에 대한 클러스터 간 통화
9[6-7]XX	성모 산에 대한 클러스터 간 통화

ACU Cisco CallManager에 구성된 게이트웨이, 경로 그룹, 경로 목록 및 경로 패턴의 수는 많은 수로 증가할 가능성이 있습니다. 새 RNO 게이트웨이가 구축되면 5개의 Cisco CallManager 클러스터

를 모두 추가 게이트웨이로 재구성해야 합니다. 더욱이 ACU Cisco CallManager가 VoIP 통화를 다른 모든 대학에 직접 라우팅하고 PSTN을 모두 우회할 경우 수백 개의 게이트웨이를 추가해야 합니다. 확실히 이것은 확장성이 좋지 않습니다.

해결책은 Cisco CallManager 게이트키퍼를 제어하기 위한 것입니다. 새 게이트웨이 또는 Cisco CallManager가 AARNet에 추가된 경우에만 게이트키퍼를 업데이트해야 합니다. 각 Cisco CallManager는 로컬 캠퍼스 게이트웨이 및 이 경우 익명 디바이스만 구성해야 합니다. 이 디바이스를 point-to-multipoint 트렁크로 생각할 수 있습니다. Cisco CallManager 다이얼 플랜 모델에서 연결된 PPP 트렁크에 대한 필요성을 제거합니다. 단일 경로 그룹은 기본 게이트웨이로 익명 디바이스를, 로컬 게이트웨이를 백업 게이트웨이로 가리킵니다. 로컬 PSTN 게이트웨이는 특정 로컬 통화에 사용되며 게이트키퍼를 사용할 수 없게 되면 일반 오프넷 통화에도 사용됩니다. 현재 익명 디바이스는 클러스터 간 또는 H.225일 수 있지만 둘 다 동시에 사용할 수는 없습니다.

Cisco CallManager는 현재 보다 게이트키퍼를 사용하는 경로 패턴이 더 적습니다. 원칙적으로 Cisco CallManager는 "Route Pattern" 하나만 있으면 됩니다. 게이트키퍼를 가리킵니다. 실제로 통화가 라우팅되는 방식은 다음과 같은 이유로 더욱 구체화되어야 합니다.

- 일부 통화(예: 1-800 또는 긴급 번호)는 지리적으로 로컬 게이트웨이를 통해 라우팅되어야 합니다. 멜버른에 사는 피자 핫과 같은 음식점 체인점에 전화를 거는 사람은 경찰에 연결되거나 퍼스에 있는 피자 핫과 연결되고 싶어하지 않습니다. 특정 경로 패턴은 이러한 번호에 대한 로컬 캠퍼스 PSTN 게이트웨이를 직접 가리키는 것이 필요합니다. 향후 IP 텔레포니 구축을 수행하려는 대학은 AARNet 게이트웨이에만 의존할 수 있으며 자체 로컬 게이트웨이를 관리하지 않을 수도 있습니다. 이러한 번호에는 로컬로 삭제해야 하는 통화에 대해 이 설계가 작동하도록 하려면 먼저 Cisco CallManager가 가상 영역 코드를 게이트키퍼에게 전송하기 전에 접두사로 추가해야 합니다. 예를 들어 Cisco CallManager는 멜버른 기반 전화기에서 Pizza Hut 1-800 번호로 003을 추가할 수 있습니다. 이를 통해 게이트키퍼는 멜버른 기반 AARNet 게이트웨이로 통화를 라우팅할 수 있습니다. 게이트웨이는 통화를 PSTN에 연결하기 전에 리드 003을 분리합니다.
- 모든 국내 번호에 대해 특정 일치 항목이 있는 경로 패턴을 사용하여 통화가 시작되기 전에 사용자가 숫자 시간 제한을 기다리지 않도록 합니다.

다음 표는 게이트키퍼가 제어하는 Cisco CallManager에 대한 경로 패턴을 보여줍니다.

경로 패턴	설명	경로	게이트키퍼
0.[2-9]XXXXXXX	로컬 통화	경로 목록	AARNet
0.00	긴급 통화	로컬 게이트웨이	없음
0.000	긴급 통화	로컬 게이트웨이	없음
0.013	디렉터리 지원	로컬 게이트웨이	없음
0.1223	—	로컬 게이트웨이	없음
0.0011!	국제 전화	경로 목록	AARNet
0.0011!#	국제 전화	경로 목록	AARNet
0.0[2-4]XXXXXX	뉴사우스웨일스, 빅토리아, 휴대폰 통화	경로 목록	AARNet
0.0[7-	호주 남부, 호주	경로 목록	AARNet

8]XXXXXX	서부 및 북부 지역 통화		
0.1[8-9]XXXXXX	1800 xxx 및 1900 xxx에 전화	로컬 게이트웨이	없음
0.1144X	긴급	로컬 게이트웨이	없음
0.119[4-6]	시간 및 날씨	로컬 게이트웨이	없음
0.13[1-9]XXX	13xxxx 번호로 통화	로컬 게이트웨이	없음
0.130XXXXXX	1300xxx xxx번으로 전화 걸기	로컬 게이트웨이	없음
[2-3]XXX	Signadou에 대한 통화	경로 목록	ACU
5XXX	아퀴나스 전화	경로 목록	ACU
[7-9]XXX	McAuley, MacKillop 및 Mount Saint Mary로 통화	경로 목록	ACU

게이트키퍼는 로컬 게이트웨이를 통해 전송되지 않는 국제 통화를 라우팅합니다. 이는 AARNet이 향후 국제 게이트웨이를 구축할 수 있기 때문에 중요합니다. 미국에 게이트웨이가 구축되면 간단한 게이트키퍼 구성 변경으로 인해 대학들은 미국 국내 요금으로 미국에 전화를 걸 수 있습니다.

게이트키퍼는 4자리 ACU 확장을 기반으로 클러스터 간 통화 라우팅을 수행합니다. 이 주소 공간은 다른 대학과 겹칠 가능성이 가장 높습니다. 따라서 ACU는 자체 게이트키퍼를 관리하고 AARNet 게이트키퍼를 디렉토리 게이트키퍼로 사용해야 합니다. 이 테이블의 게이트키퍼 열은 ACU 게이트키퍼에서 통화 라우팅이 수행되는지 아니면 AARNet 게이트키퍼에서 수행되는지를 나타냅니다.

**참고:** 제안된 게이트키퍼 솔루션의 유일한 주의 사항은 익명 디바이스가 현재 클러스터 간 또는 H.225일 수 있지만 동시에 둘 다 될 수는 없다는 것입니다. Cisco CallManager는 게이트웨이 (H.225) 및 기타 Cisco CallManager(클러스터 간)로 통화를 라우팅하는 데 게이트키퍼를 사용합니다. 이 문제의 해결 방법은 클러스터 간 라우팅에 게이트키퍼를 사용하지 않거나 게이트키퍼를 통해 모든 통화를 H.225로 처리하는 것입니다. 후자의 해결 방법은 클러스터 간 통화에서 일부 보조 기능을 사용할 수 없음을 의미합니다.

## 음성 메일

ACU는 IP 텔레포니로 마이그레이션하기 전에 Dialogic 폰 보드가 장착된 3개의 활성 음성 매개변수 OS/2 기반 음성 메일 서버를 사용했습니다. IP 텔레포니 환경에서 이러한 서버를 재사용할 계획입니다. 구현되면 각 Replete 서버는 간소화된 SMDI(Message Desk Interface) 및 Catalyst 6000 24포트 FXS(Foreign Exchange Station) 카드를 통해 Cisco CallManager에 연결됩니다. 이 기능은 6개 캠퍼스 중 3개 캠퍼스에 음성 메일을 제공합니다. 세 캠퍼스는 음성 메일을 사용하지 않습니다. 클러스터 간 H.323 트렁크에 MWI(메시지 대기 표시기)를 전파할 방법이 없으므로 두 Cisco CallManager 클러스터의 사용자 간에 하나의 Recoverit 서버를 제대로 공유할 수 없습니다.

ACU는 남아 있는 캠퍼스용 Cisco Unity 서버 3대를 구매할 수 있습니다. 이러한 서버는 Skinny 기반이므로 게이트웨이가 필요하지 않습니다. 다음 표에는 ACU가 추가 음성 메일 서버를 구매하는 경우의 음성 메일 솔루션이 나열되어 있습니다.

캠퍼스	음성 메일 시스템	게이트웨이
세인트 메리 산	활성 음성 매개 변수	Catalyst 6000 24포트 FXS
맥길롭	활성 음성 매개 변수	Catalyst 6000 24포트 FXS
패트릭	활성 음성 매개 변수	Catalyst 6000 24포트 FXS
아퀴나스	Cisco Unity	—
사이나두	Cisco Unity	—
맥컬리	Cisco Unity	—

6개의 음성 메일 서버는 이 계획에서 격리된 음성 메일 시스템으로 작동합니다. 음성 메일 네트워킹이 없습니다.

## 미디어 리소스

하드웨어 DSP(디지털 신호 프로세서)는 현재 ACU에 구축되어 있지 않습니다. 컨퍼런싱은 Cisco CallManager의 소프트웨어 기반 컨퍼런스 브리지를 사용합니다. 클러스터 간 회의는 현재 지원되지 않습니다.

트랜스코딩은 현재 필요하지 않습니다. G.711 및 G.729 코더 디코더만 사용되며, 구축된 모든 엔드 디바이스에서 지원됩니다.

## 팩스 및 모뎀 지원


팩스 및 모뎀 트래픽은 현재 ACU IP 텔레포니 네트워크에서 지원되지 않습니다. 이 대학은 Catalyst 6000 24-Port FXS 카드를 이러한 용도로 사용할 계획입니다.

## 소프트웨어 버전

이 표에는 이 게시 시점에 사용된 소프트웨어 버전 ACU가 나열되어 있습니다.

플랫폼	합수	소프트웨어 버전
통화 관리자	IP-PBX	3.0(10)
Catalyst 3500XL	배포 스위치	12.0(5.1)XP
Catalyst 6500	코어 스위치	5.5(5)
Catalyst 1900	와이어링 클로젯 스위치	—
Cisco 7200 프로세서	WAN 라우터	12.1(4)
Cisco 3640 라우터	H.323 게이트웨이	12.1(3a)XI6

## 관련 정보

- [음성 기술 지원](#)
- [음성 및 IP 커뮤니케이션 제품 지원](#)
- [Cisco IP 텔레포니 문제 해결](#) 
- [기술 지원 및 문서 - Cisco Systems](#)