

Étude de cas Déploiement de la téléphonie IP - ACU

Contenu

[Introduction](#)

[AARNet](#)

[Topologie AARNet](#)

[Qualité de service](#)

[Passerelles](#)

[Plans de numérotation](#)

[portier](#)

[Réseau de téléphonie IP ACU](#)

[Topologie du réseau ACU](#)

[QoS sur le campus](#)

[QoS dans le RNO](#)

[Passerelles](#)

[Plan de numérotation](#)

[Cisco CallManager](#)

[Messagerie vocale](#)

[Ressources multimédia](#)

[Support fax et modem](#)

[Versions logicielles](#)

[Informations connexes](#)

Introduction

L'Australian Academic and Research Network (AARNet) est un réseau de propriété intellectuelle à haut débit à l'échelle nationale qui relie 37 universités australiennes ainsi que l'Organisation de recherche scientifique et industrielle du Commonwealth (CSIRO).

AARNet a été initialement créé en tant que réseau de données, mais il transporte la voix sur IP (VoIP) depuis le début de l'année 2000. Le réseau VoIP actuellement déployé est une solution de contournement téléphonique qui achemine les appels VoIP entre les universités et les PABX (Private Automatic Branch Exchange) CSIRO. Il fournit également des passerelles de réseau téléphonique public commuté (RTPC) qui permettent au RTPC de s'arrêter au point le plus économique. Par exemple, un appel d'un téléphone PABX à Melbourne vers un téléphone RTPC à Sydney est acheminé en tant que VoIP de Melbourne vers la passerelle RTPC de Sydney. Il est connecté au RTPC.

L'Université Catholique Australienne (ACU) est l'une des universités qui se connecte à AARNet. À la fin de 2000, ACU a commencé un déploiement de téléphonie IP qui a déployé environ 2 000 téléphones IP sur six campus universitaires.

Cette étude de cas porte sur le déploiement de la téléphonie IP ACU. Le projet est terminé. Cependant, il y a des problèmes architecturaux importants à résoudre dans le réseau fédérateur AARNet si le réseau doit évoluer lorsque d'autres universités suivent les traces de l'ACU. Ce document décrit ces problèmes et propose et discute de diverses solutions. Il est probable que le déploiement de la téléphonie IP ACU sera ajusté ultérieurement afin de s'aligner sur l'architecture recommandée finale.

Remarque : Deakin University a été la première université australienne à déployer la téléphonie IP. Cependant, l'université de Deakin n'utilise pas AARNet pour transporter le trafic de téléphonie IP.

AARNet

Les universités australiennes et le CSIRO ont construit AARNet en 1990 par l'intermédiaire du Comité des vice-chanceliers australiens (AVCC). Quatre-vingt-dix-neuf pour cent du trafic Internet australien était destiné aux membres fondateurs au cours des premières années. Un petit volume de trafic commercial provenait d'organisations étroitement liées au secteur tertiaire et à la recherche. L'utilisation par la base d'utilisateurs non AARNet a augmenté à 20 % du trafic total vers la fin de 1994.

L'AVCC a vendu la base de clients commerciaux d'AARNet à Telstra en juillet 1995. Cet événement a donné naissance à ce qui allait devenir Telstra BigPond. Cela a stimulé la croissance de l'utilisation commerciale et privée d'Internet en Australie. Le transfert de propriété intellectuelle et de compétences a permis le développement d'Internet en Australie. Sinon, cela ne se serait pas produit à un rythme aussi rapide.

L'AVCC a développé AARNet2 au début de 1997. Il s'agissait d'une amélioration supplémentaire de l'Internet en Australie, qui utilise des liaisons ATM à large bande passante et des services Internet dans le cadre d'un contrat passé avec Cable & Wireless Optus (CWO) Limited. Le déploiement rapide des services IP par l'Adjud pour répondre aux exigences d'AARNet2 était dû en partie au transfert de connaissances et d'expertise d'AARNet.

ACU

L'ACU est une université publique qui a été créée en 1991. L'université compte environ 10 000 étudiants et 1 000 employés. Il y a six campus sur la côte est de l'Australie. Ce tableau présente les campus ACU et leurs emplacements :

Campus	Ville	Province
Le mont Saint-Mary	Strathfield	Nouvelle-Galles du Sud
MacKillop	North Sydney	Nouvelle-Galles du Sud
Patrick	Melbourne	Victoria (VIC)
Aquinas	Ballarat	Victoria (VIC)
Signadou	Canberra	Territoire de la capitale australienne (ACT)
McAuley	Brisbane	Queensland (QLD)

L'ACU s'est appuyée sur une solution Centrex (Telstra Spectrum) avant le déploiement de la solution de téléphonie IP décrite dans cette étude de cas. Le passage à la téléphonie IP est principalement motivé par le désir de réduire les coûts.

CSIRO

Le CSIRO compte environ 6 500 employés dans de nombreux sites en Australie. Le CSIRO mène des recherches dans des domaines comme l'agriculture, les minéraux, l'énergie, la fabrication, les communications, la construction, la santé et l'environnement.

CSIRO a été la première entreprise à utiliser AARNet pour VoIP. L'organisation a été à l'avant-garde des premiers travaux réalisés dans ce domaine.

AARNet

Le réseau fédérateur AARNet est un composant important de tout déploiement de téléphonie IP universitaire. Il assure l'interconnexion des universités avec deux services principaux dans la zone vocale :

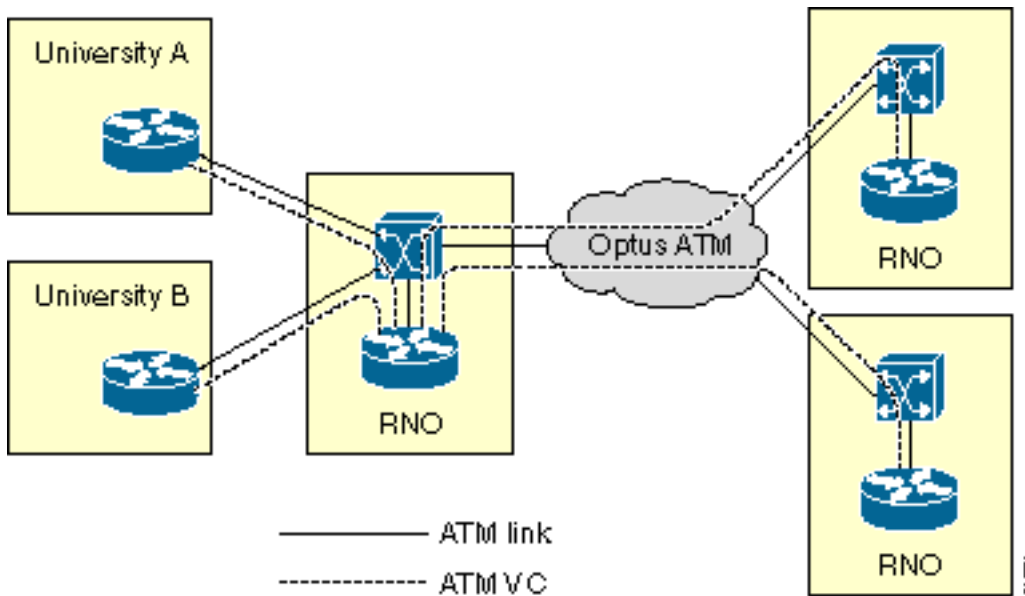
- Transport de paquets RTP (VoIP Realtime Transport Protocol) avec garantie de qualité de service (QoS) adaptée à la voix
- Point d'arrêt économique vers les RTPC dans tout le pays

Cette section décrit l'architecture AARNet actuelle et la manière dont elle fournit ces services. Il présente également quelques-uns des problèmes d'évolutivité qui surviennent lorsque de plus en plus d'universités déploient la solution de téléphonie IP. Enfin, il traite des solutions possibles à ces problèmes d'évolutivité.

Topologie AARNet

AARNet se compose d'un point de présence unique dans chaque état. Les POP sont appelés RNO (Regional Network Operations). Les universités se connectent au RNO dans leur état respectif. Les RNO sont à leur tour interconnectés par un maillage complet de circuits virtuels permanents ATM Optus. Ensemble, ils constituent AARNet.

Le RNO type se compose d'un commutateur ATM Cisco LS1010 et d'un routeur ATM. Le routeur RNO se connecte à chaque routeur d'université par un seul circuit virtuel permanent ATM via une liaison micro-ondes E3. Chaque routeur RNO possède également un maillage complet de circuits virtuels permanents ATM que le réseau ATM Optus fournit à tous les autres RNO. Ce schéma représente la topologie AARNet générale du réseau :



Il existe de nombreuses exceptions à la topologie. Certaines sont significatives du point de vue de la voix. Voici quelques exceptions :

- Le RNO de Victoria utilise le protocole IP classique sur ATM (RFC 1577) au lieu de PVC pour connecter les universités au RNO.
- Les universités rurales se connectent généralement au RNO par le relais de trames ou le RNIS.
- Certaines grandes universités ont plus d'un lien vers le RNO.

Ce tableau présente les états et territoires qui ont actuellement un RNO. Le tableau inclut les capitales pour les lecteurs qui ne connaissent pas la géographie australienne.

Province	Ville capitale	RNO ?	Connexions de campus
Nouvelle-Galles du Sud	Sydney	Oui	À déterminer
Victoria	Melbourne	Oui	À déterminer
Queensland	Brisbane	Oui	À déterminer
Australie du Sud	Adélaïde	Oui	À déterminer
Australie occidentale	Perth	Oui	À déterminer
Territoire de la capitale australienne	Canberra	Oui	À déterminer
Territoire du Nord	Darwin	Non	—
Tasmanie	Hobart	Non	—

Qualité de service

Certaines parties d'AARNet sont déjà compatibles QoS pour la voix à la suite du projet de contournement de la VoIP. La QoS est nécessaire pour le trafic vocal afin de fournir ces fonctionnalités, qui réduisent le délai et la gigue et éliminent la perte de paquets :

- Réglementation : marque le trafic vocal provenant de sources non fiables.

- Mise en file d'attente : la voix doit être prioritaire sur tout autre trafic afin de minimiser le retard lors de l'encombrement de la liaison.
- Fragmentation et entrelacement de liaison (LFI) : les paquets de données doivent être fragmentés et les paquets de voix entremêlés sur des liaisons lentes.

Le trafic doit être classifié pour contrôler correctement et mettre en file d'attente les paquets vocaux. Cette section décrit comment la classification est effectuée sur AARNet. Les chapitres suivants décrivent la mise en oeuvre de la réglementation et de la mise en file d'attente.

Classification

Tous les trafics ne reçoivent pas la même QoS. Le trafic est classé dans ces catégories pour fournir de manière sélective la qualité de service :

- Données
- Voix provenant de sources connues et fiables
- Voix provenant de sources inconnues

Seuls les périphériques fiables reçoivent une qualité de service élevée sur AARNet. Ces périphériques sont principalement des passerelles identifiées par adresse IP. Une liste de contrôle d'accès (ACL) est utilisée pour identifier ces sources de voix fiables.

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

La priorité IP est utilisée pour distinguer le trafic vocal du trafic de données. La priorité IP de la voix est 5.

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

Combinez les exemples précédents pour identifier les paquets provenant d'une source fiable.

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

Utilisez les mêmes principes pour identifier les paquets vocaux d'une source inconnue.

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

Contrôle

Le trafic vocal provenant d'une source non fiable est classifié et marqué comme étant inactif lorsque le trafic arrive sur une interface. Ces deux exemples montrent comment la réglementation est appliquée en fonction du type de trafic attendu sur une interface donnée :

Le routeur recherche les paquets vocaux non fiables et modifie leur priorité IP sur 0 s'il existe des sources vocales de confiance en aval.

```
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
```

Le routeur recherche tous les paquets vocaux et modifie leur priorité IP sur 0 s'il n'existe aucune source vocale connue en aval.

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

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

Mise en file d'attente non vocale

Tout le VoIP d'AARNet était contourné jusqu'à récemment. Cette condition entraîne relativement peu de terminaux VoIP. La conception actuelle de la mise en file d'attente fait la distinction entre les interfaces qui ont des périphériques VoIP en aval et les interfaces qui ne le font pas. Cette section traite de la mise en file d'attente sur les interfaces non VoIP.

Une interface non vocale est configurée pour la mise en file d'attente pondérée (WFQ) ou pour la détection WRED (Weighted Random Early Detection). Ils peuvent être configurés directement sur l'interface. Cependant, le mécanisme de mise en file d'attente est appliqué au moyen d'une carte de stratégie afin de faciliter la modification du mécanisme de mise en file d'attente sur un type d'interface donné. Il existe une carte de stratégie par type d'interface. Cela reflète le fait que tous les mécanismes de mise en file d'attente ne sont pas pris en charge sur toutes les interfaces.

```
policy-map OUTPUT-DATA-ATM
class class-default
fair-queue

policy-map OUTPUT-DATA-VIP-ATM
class class-default
random-detect

policy-map OUTPUT-DATA-ETHERNET
class class-default
fair-queue

policy-map OUTPUT-DATA-VIP-ETHERNET
class class-default
random-detect

policy-map OUTPUT-DATA-SERIAL
class class-default
fair-queue

policy-map OUTPUT-DATA-VIP-SERIAL
class class-default
random-detect
```

Les cartes de stratégie sont associées aux interfaces respectives et sont spécifiques aux types d'interface. Par exemple, cela simplifie le processus de modification du mécanisme de mise en file d'attente sur les ports Ethernet VIP (Versatile Interface Processor) de WRED à WFQ. Il nécessite

un seul changement dans la carte de stratégie. Les modifications sont apportées à toutes les interfaces Ethernet VIP.

```
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
```

Mise en file d'attente à faible latence

Toute interface dotée de périphériques VoIP de confiance en aval est configurée pour la mise en file d'attente à faible latence (LLQ). Tout paquet qui passe par la classification d'interface entrante et conserve une priorité de 5 est soumis à LLQ. Tout autre paquet est soumis à WFQ ou WRED. Cela dépend du type d'interface.

Des cartes de stratégie distinctes sont créées pour chaque type d'interface afin de faciliter l'administration de la qualité de service. Ceci est similaire à la conception de mise en file d'attente non vocale. Cependant, il existe plusieurs mappages de politiques pour chaque type d'interface. En effet, la capacité des types d'interface pour le transport du trafic vocal varie en fonction de la vitesse de liaison, des paramètres PVC, etc. Le numéro du nom de la carte de stratégie reflète le nombre d'appels traités pour 30 appels, 60 appels, etc.

```
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
```

Les cartes de stratégie sont associées aux interfaces respectives. Dans cet exemple, la carte de stratégie est spécifique à un type d'interface. Actuellement, aucun traitement spécial n'est accordé à la signalisation vocale. Les cartes de stratégie peuvent facilement être modifiées à un endroit si cela devient une exigence à un stade ultérieur sur un type d'interface donné. La modification prend effet pour toutes les interfaces de ce type.

```
Interface ATM0/0
service-policy output OUTPUT-VOICE-ATM-30
```

```
interface ATM1/0/0
service-policy output OUTPUT-VOICE-VIP-ATM-30
```

```
interface Ethernet2/0
service-policy output OUTPUT-VOICE-ETHERNET-60
```

```
interface Ethernet3/0/0
service-policy output OUTPUT-VOICE-VIP-ETHERNET-60
```

```
interface Serial4/0
service-policy output OUTPUT-VOICE-SERIAL-30
```

```
interface Serial5/0/0
service-policy output OUTPUT-VOICE-VIP-SERIAL-60
```

[Évolutivité LLQ](#)

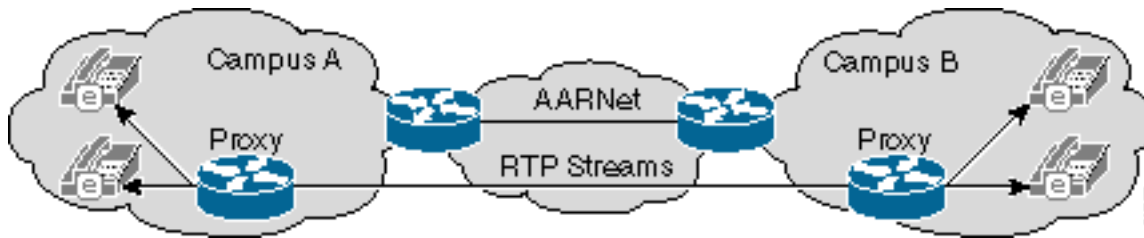
Le mécanisme de mise en file d'attente présente des problèmes d'évolutivité. Le principal problème est qu'il repose sur la connaissance de l'adresse IP de chaque périphérique VoIP de confiance du réseau. Il s'agissait d'une limitation raisonnable dans le passé, alors qu'un nombre limité de passerelles VoIP géraient le contournement des interurbains. Le nombre de terminaux VoIP augmente de manière spectaculaire et devient de plus en plus difficile avec le déploiement de la téléphonie IP. Les listes de contrôle d'accès deviennent trop longues et trop difficiles à gérer.

Les listes de contrôle d'accès ont été ajoutées pour faire confiance au trafic provenant d'un sous-réseau IP voix spécifique sur chaque campus ACU dans le cas d'ACU. Il s'agit d'une solution provisoire. Ces solutions à plus long terme font l'objet d'une étude :

- Proxy H.323
- Contrôle d'entrée QoS

L'idée principale derrière la solution proxy H.323 est de faire entrer tout le trafic RTP dans AARNet

à partir d'un campus donné au moyen d'un proxy. AARNet voit tout le trafic RTP d'un campus donné avec une adresse IP unique, comme le montre ce schéma :

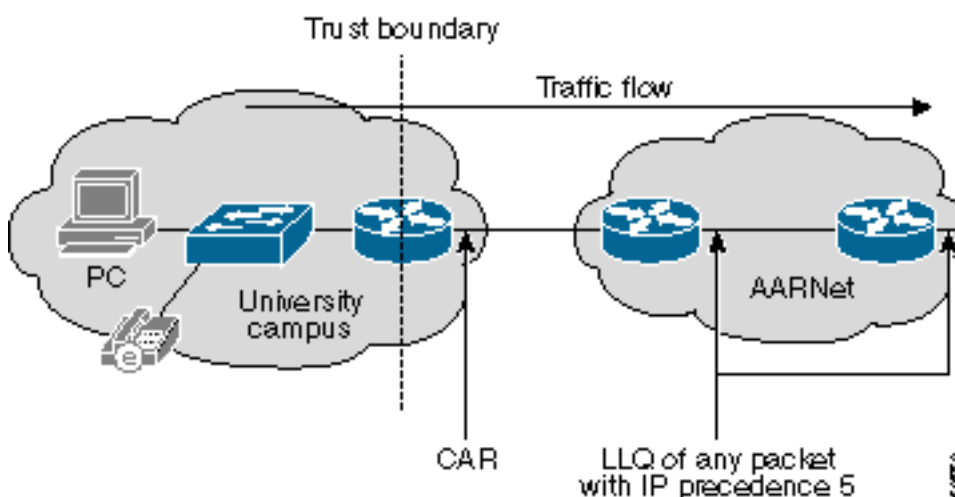


Le nombre d'entrées dans les listes de contrôle d'accès QoS est limité à une ligne par campus si ce schéma est déployé de manière cohérente. Ce programme a encore le potentiel d'ajouter au moins 100 inscriptions puisqu'il y a 37 universités avec plusieurs campus. Cela non plus n'est pas évolutif. Il peut être nécessaire de passer à une conception avec un nombre unique ou limité de super-proxies partagés à chaque RNO. Cela réduit le nombre d'adresses IP de confiance à six. Cependant, cela ouvre un problème de réglementation de QoS sur le chemin du campus au proxy au niveau du RNO.

Remarque : les liaisons interclusters Cisco CallManager ne fonctionnent pas actuellement via un proxy H.323, car la signalisation intercluster n'est pas native H.225.

La réglementation d'entrée de QoS est une solution alternative. Une frontière de confiance est établie au point où le campus se connecte au RNO avec cette conception. Le trafic entrant dans AARNet est réglementé par la fonctionnalité CAR (Committed Access Rate) de Cisco IOS® à cette limite. Une université qui utilise AARNet pour VoIP s'abonne à une certaine quantité de bande passante QoS AARNet. CAR surveille ensuite le trafic entrant dans AARNet. Le trafic excédentaire a une priorité IP marquée à 0 si la quantité de trafic RTP avec la priorité IP 5 dépasse la bande passante abonnée.

Ce schéma présente une configuration CAR :



Cet exemple montre comment une configuration CAR gère cette réglementation :

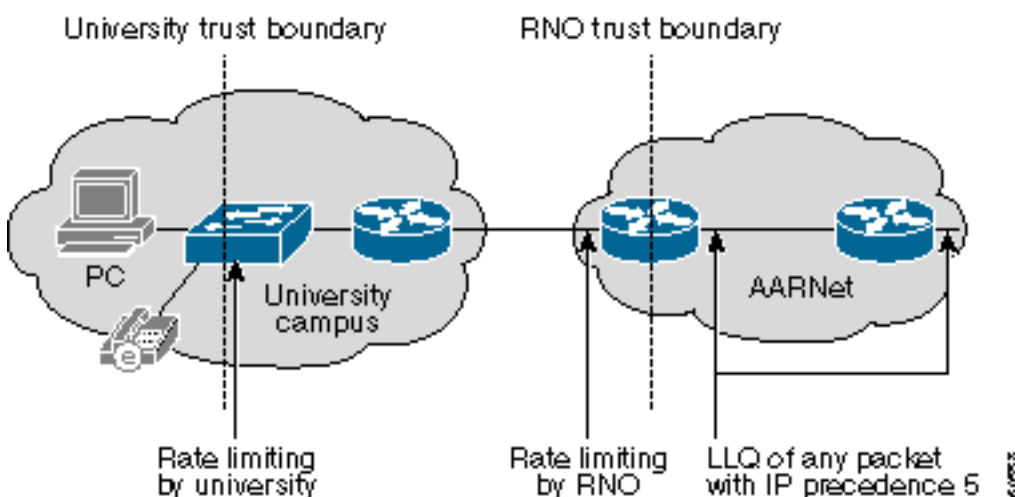
```
Interface a1/0.100
rate-limit input access-group 100 2400000 0 0 conform-action set-prec-transmit 5
exceed-action set-prec-transmit 0

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

Voici quelques avantages d'une approche de configuration CAR :

- Le noyau n'a plus besoin de gérer la police. Il est maintenant géré à la frontière de confiance. Par conséquent, la LLQ du coeur n'a pas besoin de connaître les adresses IP de confiance. Tout paquet ayant une priorité IP de 5 dans le coeur peut être soumis en toute sécurité à LLQ car il a déjà passé la réglementation en entrée.
- Aucune hypothèse n'est faite au sujet de l'architecture, de l'équipement et des protocoles VoIP choisis par chaque université. Une université peut choisir de déployer un protocole SIP (Session Initiation Protocol) ou MGCP (Media Gateway Control Protocol) qui ne fonctionne pas avec les proxy H.323. Les paquets VoIP reçoivent la QoS appropriée dans le coeur tant qu'ils ont une priorité IP de 5.
- CAR est résistant contre les attaques de déni de service (DoS) QoS. Une attaque DoS QoS provenant d'une université ne peut pas endommager le coeur. CAR limite l'attaque, qui ne peut pas générer plus de trafic que ce qui est présent lorsque le nombre maximal d'appels VoIP autorisés est actif. Les appels VoIP à destination ou en provenance de ce campus peuvent souffrir lors d'une attaque. Cependant, il appartient à chaque université de se protéger en interne. L'université peut resserrer les listes de contrôle d'accès CAR sur le routeur de sorte que tous les sous-réseaux VoIP, sauf certains, aient la priorité IP marquée. Chaque campus a une limite de confiance interne au point où les utilisateurs se connectent au LAN du campus dans la conception ultime. Le trafic avec une priorité IP de 5 que cette limite d'approbation reçoit est limité à 160 kbits/s par port de commutateur, ou deux appels VoIP G.711. Le trafic supérieur à ce débit est marqué comme étant en baisse. La mise en oeuvre de ce schéma nécessite des commutateurs Catalyst 6500 ou une fonctionnalité similaire de limitation de débit.
- La mise en service de la bande passante au coeur de réseau simplifie la tâche car chaque université s'abonne à une quantité fixe de bande passante QoS. Cela simplifie également la facturation de la QoS, car chaque université peut payer des frais mensuels forfaitaires basés sur un abonnement à la bande passante de la QoS.

La principale faiblesse de cette conception est que la limite de confiance est située sur le routeur de l'université, de sorte que les universités doivent être en mesure d'administrer correctement le CAR. La limite de confiance est retirée dans le RNO. L'équipement administré par RNO gère la police dans sa conception ultime. Cette conception nécessite une limitation de débit basée sur le matériel, telle que le commutateur Catalyst 6000 ou un processeur Cisco 7200 Network Services Engine (Cisco 7200 NSE-1). Cependant, il donne à AARNet et RNO le contrôle total de la réglementation QoS. Ce diagramme montre cette conception :



Fragmentation et entrelacement des liaisons

La VoIP n'est transportée que sur des circuits virtuels ATM à relativement haut débit. Par conséquent, aucune IFL n'est requise. La VoIP peut également être transportée à l'avenir via le Forum Frame Relay (FRF) ou des lignes louées vers des universités rurales. Cela nécessite des mécanismes LFI tels que MLP (1Multilink PPP2) avec Interleave ou FRF.

Passerelles

Il existe deux types de passerelles H.323 dans AARNet :

- RTPC : passerelle RTPC vers VoIP
- PABX : passerelle PABX vers VoIP

La distinction entre une passerelle RTPC et PABX est principalement fonctionnelle. Les passerelles RTPC fournissent la connectivité au RTPC. Les passerelles PABX connectent un PABX universitaire au réseau fédérateur VoIP. Dans de nombreux cas, la même boîte physique agit à la fois comme une passerelle RTPC et PABX. Il existe actuellement 31 passerelles dans la solution de téléphonie IP ACU. La plupart de ces passerelles sont des serveurs d'accès universel Cisco AS5300. Les autres passerelles sont des routeurs de la gamme Cisco 3600 ou Cisco 2600. Au moins dix passerelles supplémentaires devraient être ajoutées au cours du deuxième trimestre 2001. AARNet a transporté environ 145 000 appels VoIP en avril 2001.

AARNet a déployé des passerelles H.323 RTPC dans la plupart des grandes villes, comme le montre ce schéma :

Key:

AARNet H.323 Gateway

Gateway

Public Telephone Network

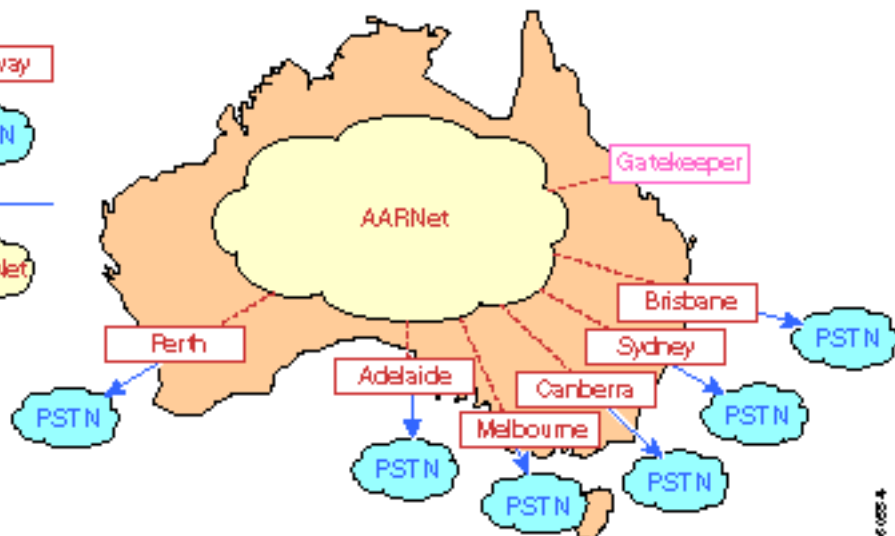
PSTN

ISDN

ISDN

AARNet TCP/IP Network

AARNet



Les universités peuvent utiliser ces passerelles pour passer des appels sortants vers le RTPC. Les universités doivent gérer leurs propres agrégations pour les appels entrants car elles ne sont pas prises en charge actuellement. AARNet peut négocier un prix très compétitif avec l'opérateur en raison du volume d'appels passant par ces passerelles. Les appels peuvent également être supprimés au point le plus économique. Par exemple, une personne de Sydney qui appelle un numéro Perth peut utiliser la passerelle Perth et ne peut être facturée que pour un appel local. On parle également de Tail End Hop Off (TEHO).

Un seul contrôleur d'accès est déployé pour effectuer la résolution d'adresses E.164 vers IP. Tous les appels destinés au RTPC sont envoyés au contrôleur d'accès, qui renvoie ensuite l'adresse IP de la passerelle la plus appropriée. Reportez-vous aux sections [Plans de numérotation](#) et [garde-barrière](#) pour plus d'informations sur les contrôleurs d'accès.

Facturation et comptabilité

Les passerelles RTPC utilisent RADIUS et AAA (Authentication, Authorization and Accounting) à des fins de facturation. Chaque appel via une passerelle génère un enregistrement détaillé des appels (CDR) pour chaque segment d'appel. Ces CDR sont affichés sur le serveur RADIUS. L'adresse IP de Cisco CallManager dans le CDR identifie de manière unique l'université et s'assure que la personne correcte est facturée.

Sécurité de la passerelle

La protection des passerelles RTPC contre les attaques par déni de service (DoS) et les fraudes est une préoccupation majeure. Les clients H.323 sont largement disponibles. Microsoft NetMeeting est fourni avec Microsoft Windows 2000, il est donc relativement facile pour un utilisateur non technique de passer des appels gratuits via ces passerelles. Configurez une liste de contrôle d'accès entrante qui autorise la signalisation H.225 à partir d'adresses IP de confiance pour protéger ces passerelles. Cette approche présente tous les mêmes problèmes d'évolutivité que ceux décrits dans la section [QoS](#). Le nombre d'entrées dans la liste de contrôle d'accès augmente à mesure que le nombre de terminaux H.323 fiables augmente.

Les proxies H.323 offrent un certain soulagement dans cette zone. Les listes de contrôle d'accès de passerelle doivent autoriser une adresse IP par campus universitaire si tous les appels via la passerelle RTPC passent par un proxy de campus. Deux adresses IP en tant que proxy redondant sont souhaitables dans la plupart des cas. Même avec des proxies, la liste de contrôle d'accès peut contenir plus de 100 entrées.

Le proxy doit être protégé par des listes de contrôle d'accès, car n'importe quel H.323 peut configurer un appel via le proxy. La liste de contrôle d'accès proxy doit autoriser les périphériques H.323 locaux, comme le requiert la politique locale, car cela est fait par campus.

Les adresses IP des deux Cisco CallManager doivent être incluses dans les listes de contrôle d'accès de la passerelle si un campus souhaite autoriser uniquement les appels des téléphones IP à utiliser les passerelles RTPC AARNet. Les proxies n'ajoutent aucune valeur dans cette situation. Le nombre d'entrées de liste de contrôle d'accès requises est de deux façons.

Notez que les appels IP de téléphone IP entre campus n'ont pas besoin de passer par le proxy.

Plans de numérotation

Le plan de numérotation VoIP actuel est simple. Les utilisateurs peuvent passer ces deux types d'appels du point de vue de la passerelle VoIP :

- Appelez un téléphone sur un autre campus mais dans la même université.
- Appelez un téléphone RTPC ou un téléphone dans une autre université.

Les terminaux de numérotation dial-peer de la passerelle reflètent le fait qu'il n'existe que deux types d'appels. En gros, il existe deux types de terminaux de numérotation dial-peer VoIP, comme le montre cet exemple :

```
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
```

Le premier terminal de numérotation dial-peer est utilisé si quelqu'un appelle le poste 7... sur un autre campus dans cet exemple. Cet appel est acheminé directement vers l'adresse IP de la passerelle distante. Puisque le contrôleur d'accès est contourné, le contrôle d'admission d'appel (CAC) n'est pas effectué.

Le second terminal de numérotation dial-peer est utilisé lorsque l'appel porte sur un numéro RTPC. Il peut s'agir de l'un des éléments suivants :

- Numéro d'un téléphone dans le RTPC
- Numéro RTPC complet d'un téléphone d'une autre université

L'appel est envoyé au contrôleur d'accès par un message ARQ (demande d'admission) dans le premier cas. Le contrôleur d'accès renvoie l'adresse IP de la meilleure passerelle RTPC dans un message de confirmation d'admission (ACF).

L'appel est également envoyé au contrôleur d'accès au moyen d'un message ARQ dans le deuxième cas. Cependant, le contrôleur d'accès renvoie un message ACF avec l'adresse IP de la passerelle VoIP de l'université qui reçoit l'appel.

portier

AARNet gère actuellement un seul contrôleur d'accès. Le seul objectif de ce contrôleur d'accès est d'effectuer le routage des appels sous la forme de résolution d'adresse IP E.164 vers IP. Le contrôleur d'accès n'exécute pas CAC. Le nombre de faisceaux PABX connectés aux passerelles limite le nombre d'appels simultanés. La bande passante principale prend en charge toutes les agrégations utilisées en même temps. Cela change avec le déploiement de la téléphonie IP à l'ACU et dans d'autres universités. Il n'y a aucune limite naturelle au nombre d'appels VoIP simultanés pouvant être émis ou reçus sur un campus donné dans ce nouvel environnement. La bande passante QoS disponible peut être surabondante si trop d'appels sont initiés. Tous les appels peuvent souffrir d'une mauvaise qualité dans ce cas. Utilisez le contrôleur d'accès pour fournir CAC.

La nature distribuée et la taille potentielle du réseau vocal de l'université se prêtent à une architecture de garde-barrière distribuée. Une solution possible est d'avoir un contrôleur d'accès hiérarchique à deux niveaux dans lequel chaque université gère son propre contrôleur d'accès. Ce contrôleur d'accès universitaire est appelé contrôleur d'accès de niveau 2. AARNet gère un contrôleur d'accès *de répertoire* appelé contrôleur d'accès de niveau 1.

Les universités doivent utiliser cette approche à deux niveaux pour utiliser un contrôleur d'accès pour le routage des appels entre les clusters Cisco CallManager. Le contrôleur d'accès achemine les appels en fonction d'un poste à 4 ou 5 chiffres dans ce scénario. Chaque université a besoin de son propre portier. En effet, les plages de numéros de poste se chevauchent entre les universités, car il s'agit d'un espace d'adresses géré localement.

Les contrôleurs d'accès de niveau 2 de l'université exécutent CAC uniquement pour les appels à destination et en provenance de cette université. Il exécute également la résolution E.164 pour les appels entre les campus de cette université uniquement. L'appel est acheminé par le contrôleur d'accès de niveau 2 vers le contrôleur d'accès de niveau 1 au moyen d'un message de demande d'emplacement (LRQ) si quelqu'un appelle un téléphone IP d'une autre université ou appelle le RTPC via une passerelle AARNet. Le LRQ est transmis au contrôleur d'accès de niveau 2 de

cette université si l'appel concerne une autre université. Ce contrôleur d'accès renvoie ensuite un message ACF au contrôleur d'accès de niveau 2 de l'université d'où provient l'appel. Les deux contrôleurs d'accès de niveau 2 exécutent CAC. Ils ne procèdent à l'appel que s'il y a suffisamment de bande passante disponible dans les zones d'appel et d'appel.

AARNet peut choisir de traiter les passerelles RTPC AARNet comme celles de n'importe quelle université. Leur propre contrôleur d'accès de niveau 2 s'occupe d'eux. Le contrôleur d'accès de niveau 1 peut également agir en tant que contrôleur d'accès de niveau 2 pour ces passerelles si la charge et les performances le permettent.

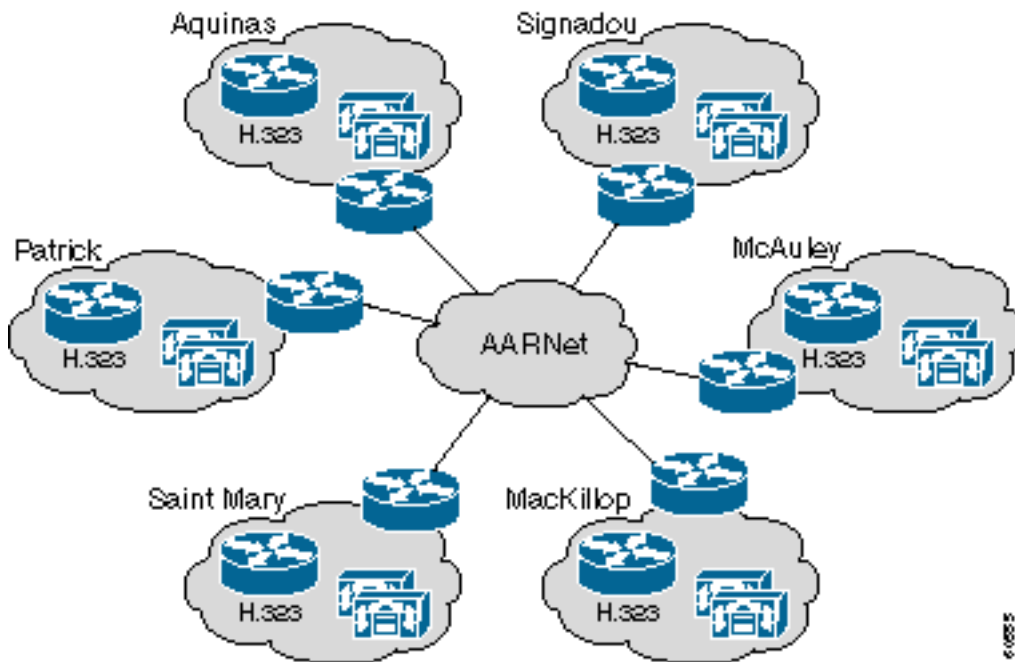
Chacun des contrôleurs d'accès (y compris le contrôleur d'accès du répertoire AARNet) doit être répliqué car les passerelles sont un composant essentiel. Chaque université a besoin de deux gardiens. Il est possible que les passerelles Cisco IOS aient d'autres contrôleurs d'accès, comme dans le cas du logiciel Cisco IOS Version 12.0(7)T. Cependant, ceci n'est actuellement pas pris en charge par Cisco CallManager ou tout autre périphérique H.323 tiers. N'utilisez pas cette fonctionnalité pour le moment. Utilisez plutôt une solution simple basée sur le protocole HSRP (Hot Standby Router Protocol). Cela nécessite que les deux contrôleurs d'accès soient installés sur le même sous-réseau IP. Le protocole HSRP détermine le contrôleur d'accès actif.

Réseau de téléphonie IP ACU

Ce tableau indique le nombre approximatif de téléphones IP installés sur les campus de l'ACU :

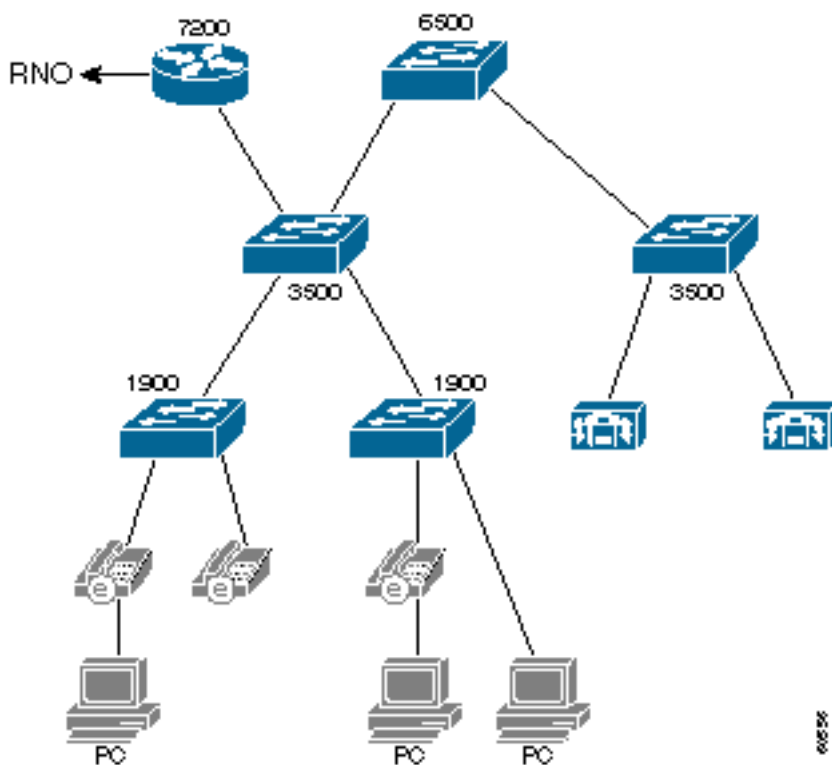
Campus	Ville	Téléphones IP approximatifs
Le mont Saint-Mary	Strathfield	400
MacKillop	North Sydney	300
Patrick	Melbourne	400
Aquinas	Ballarat	100
Signadou	Canberra	100
McAuley	Brisbane	400
	Total :	1700

ACU a récemment déployé une solution de téléphonie IP. La solution se compose d'un cluster de deux Cisco CallManager, d'une passerelle Cisco 3640 sur chaque campus et de téléphones IP. AARNet interconnecte les campus. Ce schéma présente la topologie de haut niveau et les différents composants du réseau de téléphonie IP ACU :



Topologie du réseau ACU

Ce diagramme montre un campus ACU typique. Chaque campus comporte trois couches de commutateurs Catalyst. Le local technique héberge les anciens commutateurs Catalyst 1900. Les commutateurs Catalyst 1900 se connectent de nouveau au commutateur Catalyst 3500XL par le biais d'un verrouillage de trame étendu. Ils se connectent à un commutateur Catalyst 6509 au moyen de Gigabit Ethernet (GE). Un seul routeur Cisco 7200 VXR connecte le campus à AARNet par un circuit virtuel ATM au RNO local.



La méthode de connectivité au RNO diffère légèrement d'état en état, comme le montre ce tableau. Victoria est basée sur le protocole IP classique sur ATM (RFC 1577). Les autres RNO ont une configuration PVC droite avec encapsulation RFC 1483. OSPF (Open Shortest Path First) est le protocole de routage utilisé entre ACU et RNO.

Campus	Province	Connectivité à RNO	Protocole de routage
Le mont Saint-Mary	NSW	PVC RFC 1483	OSPF
MacKillop	NSW	PVC RFC 1483	OSPF
Patrick	VIC	RFC 1577 Classical IP over ATM	OSPF
Aquinas	VIC	RFC 1577 Classical IP over ATM	OSPF
Signadou	ACTE	PVC RFC 1483	OSPF
McAuley	QLD	PVC RFC 1483	OSPF

Les commutateurs de la gamme Catalyst 1900 prennent uniquement en charge l'agrégation sur les liaisons ascendantes. Par conséquent, les téléphones IP et les PC se trouvent tous dans un grand VLAN. En fait, l'ensemble du campus est un grand VLAN et un domaine de diffusion. Les sous-réseaux IP secondaires sont utilisés en raison du grand nombre de périphériques. Les téléphones IP se trouvent sur un sous-réseau IP et les PC sur un autre. Le coeur d'AARNet fait confiance au sous-réseau du téléphone IP et le trafic en provenance et à destination de ce sous-réseau IP est soumis à la LLQ.

Le routeur Cisco 7200 achemine les routes entre les sous-réseaux IP principal et secondaire. La carte MSFC (Multilayer Switch Feature Card) du commutateur Catalyst 6500 n'est pas utilisée actuellement.

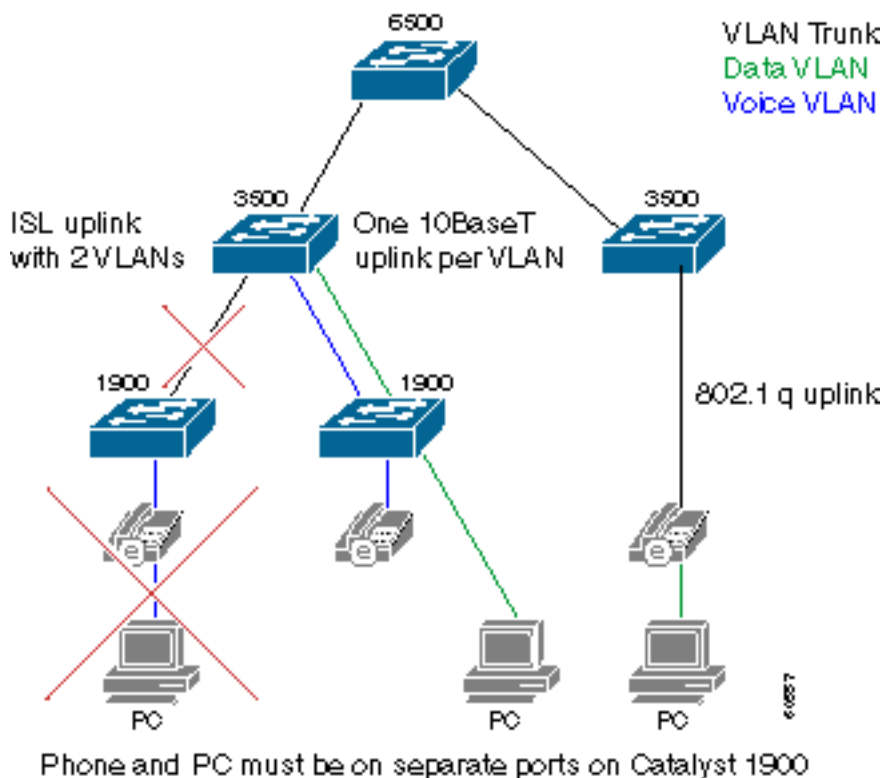
Les commutateurs Catalyst 3500XL et Catalyst 6500 ont des fonctionnalités QoS, mais ils ne sont pas actuellement activés.

[QoS sur le campus](#)

La conception actuelle du campus n'est pas conforme aux directives de conception recommandées par Cisco pour la téléphonie IP. Voici quelques préoccupations concernant la qualité de service :

- Le domaine de diffusion est très grand. Les diffusions excessives peuvent affecter les performances des téléphones IP, qui doivent les traiter.
- Les commutateurs Catalyst 1900 ne sont pas compatibles QoS. Si un téléphone IP et un PC sont connectés au même port de commutateur, les paquets vocaux peuvent être supprimés si le PC reçoit des données à un débit élevé.

Reconcevoir certaines parties de l'infrastructure du campus pour obtenir des améliorations significatives. Aucune mise à niveau matérielle n'est requise. Ce diagramme illustre les principes qui sous-tendent la refonte recommandée :



Le campus doit être divisé en un VLAN voix et un VLAN de données. Les téléphones et les PC qui se connectent à un commutateur Catalyst 1900 doivent désormais se connecter à différents ports afin d'obtenir la séparation VLAN. Une liaison ascendante supplémentaire entre chaque commutateur Catalyst 1900 et le commutateur Cisco 3500XL est ajoutée. L'une des deux liaisons ascendantes est membre du VLAN voix. L'autre liaison ascendante est membre du VLAN de données. N'utilisez pas l'agrégation ISL (InterSwitch Link) comme alternative à deux liaisons ascendantes. Cela ne fournit pas de files d'attente distinctes au trafic voix et données. Les liaisons GE du commutateur Catalyst 3500XL au commutateur Catalyst 6000 doivent également être converties en liaisons 802.1q afin que les VLAN voix et données puissent être transportés sur ce commutateur principal.

Les ports du commutateur Catalyst 3500XL qui se trouvent dans le VLAN de données ont une classe de service (CoS) par défaut égale à zéro. Les ports qui sont membres du VLAN voix ont une CoS par défaut de 5. Par conséquent, le trafic vocal est correctement hiérarchisé une fois qu'il arrive au cœur des Catalyst 3500 ou Catalyst 6500. Les configurations des ports du commutateur Catalyst 3500 QoS varient légèrement en fonction du port du commutateur VLAN membre, comme le montre cet exemple :

```
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
```

Vous pouvez connecter un PC au port de commutation arrière du téléphone IP dans le rare cas où les téléphones IP se connectent directement à un commutateur Catalyst 3500XL. Les téléphones IP se connectent au commutateur au moyen d'une agrégation 802.1q dans ce cas. Cela permet aux paquets voix et données de circuler sur des VLAN distincts, et vous pouvez donner aux paquets la CoS correcte en entrée. Remplacez les commutateurs Catalyst 1900 par des

commutateurs Catalyst 3500XL ou d'autres commutateurs compatibles QoS lorsqu'ils arrivent en fin de vie. Cette topologie devient alors la méthode standard de connexion des téléphones IP et des PC au réseau. Ce scénario présente la configuration QoS du commutateur Catalyst 3500XL :

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

Enfin, les deux ports qui se connectent aux deux Cisco CallManager doivent avoir le code CoS en dur sur 3. Cisco CallManager définit la priorité IP sur 3 dans tous les paquets de signalisation vocale. Cependant, la liaison entre Cisco CallManager et le commutateur Catalyst 3500XL n'utilise pas 801.1p. Par conséquent, la valeur CoS est forcée au niveau du commutateur comme le montre cet exemple :

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

L'obstacle principal de cette conception est que deux ports de commutateur sont requis sur le bureau. Le campus Patrick peut nécessiter 400 ports de commutation supplémentaires pour 400 téléphones IP. Des commutateurs Catalyst 3500XL supplémentaires doivent être déployés si des ports suffisants ne sont pas disponibles. Un seul port de commutateur Catalyst 3500XL est requis pour deux ports de commutateur Catalyst 1900 manquants.

Les commutateurs ACU Catalyst 6500 actuels ont des fonctionnalités QoS, mais ils ne sont pas actuellement activés. Ces modules sont présents dans le commutateur ACU Catalyst 6000 avec les fonctionnalités de mise en file d'attente suivantes :

Logement	module	Ports	Files d'attente RX	Files d'attente TX
1	WS-X6K-SUP1A-2GE	2	1p1q4t	1p2q2t
3	WS-X6408-GBIC	8	1q4t	2q2t
4	WS-X6408-GBIC	8	1q4t	2q2t
5	WS-X6248-RJ-45	48	1q4t	2q2t
15	WS-F6K-MSFC	0	—	—

Exécutez les étapes suivantes pour activer les fonctions QoS appropriées sur le commutateur Catalyst 6000 :

1. Indiquez au commutateur de fournir la QoS par VLAN avec cette commande :

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

2. Demandez au commutateur de faire confiance aux valeurs CoS reçues du commutateur Catalyst 3500XL avec cette commande :

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

La CoS doit maintenant être définie sur le mappage de point de code de services différenciés (DSCP). Cela est nécessaire car le commutateur Catalyst 6000 réécrit la valeur DSCP dans l'en-

tête IP en fonction de la valeur CoS reçue. Les paquets de signalisation VoIP doivent avoir une CoS de 3, réécrite avec un DSCP de AF31 (26). Les paquets RTP doivent avoir une CoS de 5, réécrite avec un DSCP de EF (46). Émettez la commande suivante :

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

Utilisez cet exemple pour vérifier le mappage CoS-DSCP.

```
Cat6K> (enable) show qos map run CoS-DSCP-map
```

```
CoS - DSCP map:
```

```
CoS DSCP
```

```
--- ----
```

```
0 0
1 8
2 16
3 26
4 32
5 46
6 48
7 56
```

Configurez la carte MSFC pour le routage entre les différents sous-réseaux IP.

QoS dans le RNO

La conception RNO actuelle n'est pas conforme aux directives de conception recommandées par Cisco pour la téléphonie IP. Ces préoccupations concernent la qualité de service :

- La LLQ n'est pas appliquée sur les routeurs WAN de la gamme Cisco ACU 7200.
- Les campus Patrick et Aquinas se connectent au RNO au moyen de circuits virtuels commutés ATM (SVC). LLQ n'est pas pris en charge sur les circuits virtuels commutés.

Un routeur Cisco 7200 connecté à Fast Ethernet connecte le campus à un RNO au moyen d'une liaison ATM E4 34 Mbits/s. Le trafic peut potentiellement mettre en file d'attente vers le haut sur les liaisons 34 M en raison d'une non-correspondance de vitesse de 4 M par rapport à 100 M. Par conséquent, il est nécessaire de hiérarchiser le trafic vocal. Utiliser LLQ. La configuration du routeur Cisco 7200 est similaire à cet exemple :

```
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
```

La bande passante allouée à LLQ doit être $N \times 24$ Kbits/s, où N est le nombre d'appels G.729

simultanés.

Configurez un circuit virtuel permanent entre chacun des routeurs Patrick et Aquinas Cisco 7200 et le routeur AARNet. Les circuits virtuels commutés ATM du Victoria RNO ne prennent pas en charge LLQ, car ils sont basés sur IP classique sur ATM (RFC 1577). Les autres universités du Victoria RNO peuvent continuer à utiliser le document RFC 1577 pour le moment. Cependant, remplacez finalement l'infrastructure IP sur ATM classique.

Passerelles

Chaque campus ACU dispose d'un routeur Cisco 3640 qui agit comme une passerelle H.323. Ces passerelles se connectent au RTPC par le biais d'un RNIS. Le nombre d'interfaces PRI (Primary Rate Interfaces) et de canaux B dépend de la taille du campus. Ce tableau répertorie le nombre de PRI et de canaux B pour chaque campus :

Campus	Quantité PRI	Quantité canal B
Le mont Saint-Mary	2	30
MacKillop	2	50
Patrick	2	50
Aquinas	1	20
Signadou	1	20
McAuley	1	30

Ces passerelles sont utilisées uniquement comme passerelles secondaires pour DOD (Direct Outward Dialing). Les passerelles AARNet sont les passerelles principales. Les passerelles ACU sont toujours utilisées pour DID (Direct Inward Dialing).

Plan de numérotation

Le plan de numérotation est basé sur des numéros de poste à 4 chiffres. Le numéro de poste correspond également aux quatre derniers chiffres du numéro DID. Ce tableau répertorie les plages de postes et les numéros DID de chaque campus :

Campus	Extension	DIEU
Le mont Saint-Mary	9xxx	02 9764 9xxx
MacKillop	8xxx	02 9463 8xxx
Patrick	3 xxx	03 8413 3xxx
Aquinas	5xxx	03 5330 5xxx
Signadou	2 xxx	02 6123 2xxx
McAuley	7xxx	07 3354 7xxx

Une simple entrée num-exp sur les passerelles relie le numéro DID au poste à 4 chiffres avant de le

transmettre à Cisco CallManager. Par exemple, la passerelle du campus Patrick a cette entrée :

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

Les utilisateurs composent zéro pour sélectionner une ligne externe. Ce zéro de début est transmis à la passerelle. Un seul terminal de numérotation dial-peer POTS achemine l'appel vers le port RNIS en fonction du zéro de début.

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

Les appels entrants utilisent cette entrée num-exp pour transformer le numéro de l'appelé en un poste à 4 chiffres. L'appel correspond ensuite aux deux homologues de numérotation VoIP. En fonction de la préférence inférieure, il préfère cette route à l'abonné Cisco CallManager :

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

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

[Cisco CallManager](#)

Chaque campus comporte un cluster composé de deux serveurs Cisco CallManager. Les serveurs Cisco CallManager sont un mélange de Media Convergence Server 7835 (MCS-7835) et Media Convergence Server 7820 (MCS-7820). Les deux serveurs exécutaient la version 3.0(10) au moment de cette publication. Un Cisco CallManager est l'*éditeur* et l'autre Cisco CallManager est l'*abonné*. L'abonné agit en tant que Cisco CallManager principal pour tous les téléphones IP. Ce tableau répertorie le matériel déployé sur chaque campus :

Campus	Plateforme	AppelsGestionnaires
Le mont Saint-Mary	MCS-7835	2
MacKillop	MCS-7835	2
Patrick	MCS-7835	2
Aquinas	MCS-7820	2
Signadou	MCS-7820	2
McAuley	MCS-7835	2

Chaque cluster est configuré avec deux régions :

- Un pour les appels intracampus (G.711)
- Un pour les appels intercampus (G.729)

Le CAC basé sur l'emplacement n'est pas approprié pour ACU, car tous les téléphones IP desservis par chaque grappe se trouvent sur un seul campus. Un CAC basé sur un contrôleur d'accès présente des avantages pour les appels intercampus, mais ce n'est pas le cas

actuellement. Toutefois, il est prévu de le faire dans un avenir proche.

Chaque Cisco CallManager est configuré avec 22 passerelles H.323. Il se compose de liaisons interclusters vers les cinq autres clusters Cisco CallManager, six passerelles RTPC AARNet et une passerelle ACU sur chaque campus.

Type de périphérique H.323	Quantité
CallManager intercampus	2 x 5 = 10
Passerelle RTPC AARNet	6
Passerelle RTPC ACU	6
Total :	22

Les listes de routage et les groupes de routage sont utilisés pour classer les passerelles PSTN. Par exemple, ce tableau montre comment les appels de Patrick Cisco CallManager à Melbourne vers le RTPC de Sydney peuvent utiliser les quatre passerelles pour relier les appels à un groupe de routage.

Passerelle	Priorité
AARNet Sydney	1
ACU Sydney	2
AARNet Melbourne	3
ACU Melbourne	4

Les Cisco CallManager sont configurés avec environ 30 modèles de routage, comme le montre ce tableau. Les modèles de route sont conçus de sorte qu'il y ait des correspondances spécifiques pour tous les numéros australiens nationaux. De cette manière, les utilisateurs n'ont pas à attendre l'expiration du délai d'attente entre les chiffres avant que Cisco CallManager ne lance l'appel. Caractère générique « ! » est utilisé uniquement dans le modèle de route pour les numéros internationaux. Les utilisateurs doivent attendre que le délai d'attente entre les chiffres (10 secondes par défaut) expire avant que l'appel ne progresse lorsqu'ils composent une destination internationale. Les utilisateurs peuvent également ajouter le modèle de route « 0.0011 !# » . Les utilisateurs peuvent ensuite saisir un "#" après le dernier chiffre pour indiquer à Cisco CallManager que le numéro composé est terminé. Cette action accélère la numérotation internationale.

Schéma de routage	Description
0.[2-9]XXXXXXX	Appel local
0.00	Appel d'urgence : si l'utilisateur oublie de composer le 0 pour la ligne externe
0.000	Appel d'urgence
0.013	Assistance par répertoire
0.1223	—
0.0011!	Appels internationaux
0,02XXXXXXXXX	Appels en Nouvelle-Galles du Sud
0,03XXXXXXXXX	Appels vers Victoria
0,04XXXXXXXXX	Appels vers les téléphones

	portables
0,07XXXXXXXX	Appels au Queensland
0,086XXXXX	Appels en Australie occidentale
0,08XXXXXXXX	Appels en Australie du Sud et dans le Territoire du Nord
0,1[8-9]XXXXXXXX	Appels vers 1800 xxx xxx et 1900 xxx xxx
0,1144X	Urgence
0,119[4-6]	Temps et temps
0,1245X	Répertoire
0,13[1-9]XXX	Appels vers des numéros 13xxxx
0,130XXXXX	Appels vers 1300 xxx xxx numéros
2[0-1]XX	Appels interclusters vers Signadou
3[0-4]XX	Appels interclusters vers Patrick
5[3-4]XX	Appels interclusters vers l'quinas
7[2-5]XX	Appels interclusters vers McAuley
8[0-3]XX	Appels interclusters vers MacKillop
9[3-4]XX	Appels interclusters vers le mont Saint Mary
9[6-7]XX	Appels interclusters vers le mont Saint Mary

Le nombre de passerelles, de groupes de routage, de listes de routage et de modèles de routage configurés sur l'ACU Cisco CallManager peut augmenter pour atteindre un grand nombre. Si une nouvelle passerelle RNO est déployée, les cinq clusters Cisco CallManager doivent être reconfigurés avec une passerelle supplémentaire. Pire encore, des centaines de passerelles doivent être ajoutées si ACU Cisco CallManagers achemine les appels VoIP directement vers toutes les autres universités et contourne complètement le RTPC. Il est clair que cela ne s'étend pas très bien.

La solution consiste à contrôler le contrôleur d'accès Cisco CallManagers. Vous ne devez mettre à jour le contrôleur d'accès que lorsqu'une nouvelle passerelle ou Cisco CallManager est ajoutée quelque part dans AARNet. Chaque Cisco CallManager doit avoir uniquement la passerelle de campus locale et le périphérique anonyme configurés lorsque cela se produit. Vous pouvez considérer ce périphérique comme une agrégation point à multipoint. Il supprime la nécessité des liaisons PPP maillées dans le modèle de plan de numérotation Cisco CallManager. Un groupe de routes unique pointe vers le périphérique anonyme comme passerelle préférée et vers la passerelle locale comme passerelle de secours. La passerelle RTPC locale est utilisée pour certains appels locaux et également pour les appels hors réseau généraux si le contrôleur d'accès devient indisponible. Actuellement, le périphérique anonyme peut être intercluster ou H.225, mais pas les deux en même temps.

Cisco CallManager a besoin de moins de modèles de routage avec un contrôleur d'accès que maintenant. En principe, Cisco CallManager n'a besoin que d'un seul modèle de route de « ! » pointant vers le contrôleur d'accès. En réalité, la manière dont les appels sont acheminés doit être plus spécifique pour les raisons suivantes :

- Certains appels (tels que les appels vers 1-800 ou les numéros d'urgence) doivent être acheminés via une passerelle locale géographique. Quelqu'un à Melbourne qui compose la

police ou une chaîne de restaurants comme Pizza Hut ne veut pas être connecté à la police ou à la Pizza Hut à Perth. Les modèles de route spécifiques qui pointent directement vers la passerelle RTPC du campus local pour ces numéros sont nécessaires. Les universités qui envisagent de déployer de futures solutions de téléphonie IP peuvent choisir de s'appuyer uniquement sur les passerelles AARNet et de ne pas administrer leurs propres passerelles locales. Ces numéros doivent avoir un code de zone virtuelle préfixé par Cisco CallManager avant de l'envoyer au contrôleur d'accès pour que cette conception fonctionne pour les appels qui doivent être abandonnés localement. Par exemple, Cisco CallManager peut prépasser 003 pour les appels d'un téléphone basé à Melbourne vers le numéro Pizza Hut 1-800. Cela permet au contrôleur d'accès d'acheminer l'appel vers une passerelle AARNet basée à Melbourne. La passerelle retire le 003 principal avant de passer l'appel dans le RTPC.

- Utilisez des modèles de routage avec des correspondances spécifiques pour tous les numéros domestiques afin d'éviter que l'utilisateur attende le délai d'attente entre les chiffres avant le début de l'appel.

Ce tableau présente les modèles de route pour un Cisco CallManager contrôlé par un contrôleur d'accès :

Schéma de routage	Description	Route	portier
0.[2-9]XXXXXXX	Appel local	Liste des routes	AARN et
0.00	Appel d'urgence	Passerelle locale	Aucune
0.000	Appel d'urgence	Passerelle locale	Aucune
0.013	Assistance par répertoire	Passerelle locale	Aucune
0.1223	—	Passerelle locale	Aucune
0.0011!	Appels internationaux	Liste des routes	AARN et
0,0011 !#	Appels internationaux	Liste des routes	AARN et
0,0[2-4]XXXXXXX	Appels vers la Nouvelle-Galles du Sud, Victoria et téléphones portables	Liste des routes	AARN et
0,0[7-8]XXXXXXX	Appels vers l'Australie du Sud, l'Australie occidentale et le Territoire du Nord	Liste des routes	AARN et
0,1[8-	Appels vers 1800 xxx	Passerelle	Aucune

9]XXXXXXXX	xxx et 1900 xxx xxx	Ile locale	e
0,1144X	Urgence	Passerelle locale	Aucune
0,119[4-6]	Temps et météo	Passerelle locale	Aucune
0,13[1-9]XXX	Appels vers des numéros 13xxxx	Passerelle locale	Aucune
0,130XXXXX	Appels vers 1300 xxx xxx numéros	Passerelle locale	Aucune
[2-3]XXX	Appels à Signadou	Liste des routes	ACU
5 XXX	Appels à l'quinas	Liste des routes	ACU
[7-9]XXX	Appels à McAuley, MacKillop et Mount Saint Mary	Liste des routes	ACU

Le contrôleur d'accès achemine les appels internationaux qui ne sont pas envoyés par la passerelle locale. Cela est important car AARNet pourra déployer des passerelles internationales à l'avenir. Si une passerelle est déployée aux États-Unis, un simple changement de configuration des contrôleurs d'accès permet aux universités de passer des appels vers les États-Unis aux tarifs intérieurs américains.

Le contrôleur d'accès effectue le routage des appels interclusters en fonction du poste ACU à 4 chiffres. Cet espace d'adressage chevauche très probablement d'autres universités. Cela signifie que l'ACU gère son propre contrôleur d'accès et utilise le contrôleur d'accès AARNet comme *contrôleur d'accès de répertoire*. La colonne du contrôleur d'accès de cette table indique si le routage des appels est effectué par le contrôleur d'accès ACU ou le contrôleur d'accès AARNet.

Remarque : La seule mise en garde avec la solution de contrôleur d'accès proposée est que le périphérique anonyme peut actuellement être intercluster ou H.225, mais pas les deux en même temps. Cisco CallManager s'appuie sur le contrôleur d'accès pour acheminer les appels vers les deux passerelles (H.225) et vers d'autres Cisco CallManager (intercluster) avec la conception proposée. La solution de contournement de ce problème consiste à ne pas utiliser le contrôleur d'accès pour le routage intercluster ou à traiter tous les appels via le contrôleur d'accès comme H.225. Cette dernière solution de contournement signifie que certaines fonctionnalités supplémentaires peuvent ne pas être disponibles sur les appels interclusters.

Messagerie vocale

Avant la migration vers la téléphonie IP, l'ACU disposait de trois serveurs de messagerie vocale OS/2 avec cartes téléphoniques Dialogic. Il est prévu de réutiliser ces serveurs dans l'environnement de téléphonie IP. Lorsqu'il est mis en oeuvre, chaque serveur Réparte se connecte à Cisco CallManager au moyen d'une interface SMDI (Message Desk Interface)

simplifiée et d'une carte FXS (Foreign Exchange Station) Catalyst 6000 à 24 ports. Cela fournit la messagerie vocale pour trois des six campus, ce qui laisse trois campus sans messagerie vocale. Il n'est pas possible de partager correctement un serveur Réparé entre les utilisateurs sur deux clusters Cisco CallManager, car il n'y a aucun moyen de propager l'indicateur de message en attente (MWI) sur la liaison H.323 intercluster.

ACU peut acheter trois serveurs Cisco Unity pour les campus restants. Ces serveurs sont basés sur Skinny, donc aucune passerelle n'est requise. Ce tableau répertorie les solutions de messagerie vocale dans le cas où l'ACU achète les serveurs de messagerie vocale supplémentaires :

Campus	Système de messagerie vocale	Passerelle
Le mont Saint-Mary	Réparation vocale active	Catalyst 6000 24 ports FXS
MacKillop	Réparation vocale active	Catalyst 6000 24 ports FXS
Patrick	Réparation vocale active	Catalyst 6000 24 ports FXS
Aquinas	Cisco Unity	—
Signadou	Cisco Unity	—
McAuley	Cisco Unity	—

Les six serveurs de messagerie vocale fonctionnent comme des îlots de messagerie vocale isolés dans ce plan. Il n'y a pas de réseau de messagerie vocale.

[Ressources multimédia](#)

Les processeurs de signal numérique (DSP) matériels ne sont pas actuellement déployés sur ACU. La conférence utilise le pont de conférence logiciel sur Cisco CallManager. La conférence intercluster n'est pas prise en charge actuellement.

Le transcodage n'est pas requis actuellement. Seuls les codeurs-décodeurs G.711 et G.729 sont utilisés et ils sont pris en charge par tous les périphériques finaux déployés.

[Support fax et modem](#)

Le trafic fax et modem n'est pas pris en charge par le réseau de téléphonie IP ACU. L'université prévoit d'utiliser la carte Catalyst 6000 FXS 24 ports à cette fin.


[Versions logicielles](#)

Ce tableau répertorie les versions logicielles de l'ACU utilisées au moment de cette publication :

Plateforme	Fonction	Version du logiciel
CallManager	PBX IP	3.0(10)
Catalyst 3500XL	Commutateur de distribution	12.0(5.1)XP

Catalyst 6500	Commutateur principal	5.5(5)
Catalyst 1900	Commutateur de local technique	—
Processeur Cisco 7200	Routeur WAN	12.1(4)
Routeur Cisco 3640	Passerelle H.323	12.1(3a)XI6

[Informations connexes](#)

- [Assistance technique concernant la technologie vocale](#)
- [Support produit pour Voix et Communications IP](#)
- [Dépannage des problèmes de téléphonie IP Cisco](#) 
- [Support et documentation techniques - Cisco Systems](#)