

Étude de cas de déploiement de téléphonie IP : Université catholique australienne

Contenu

[Introduction](#)

[AARNet](#)

[Topologie d'AARNet](#)

[Qualité de service](#)

[Passerelles](#)

[Plans de composition](#)

[Garde-porte](#)

[Réseau de Téléphonie sur IP ACU](#)

[Topologie du réseau ACU](#)

[QoS dans le campus](#)

[QoS dans le RNO](#)

[Passerelles](#)

[Plan de composition](#)

[Cisco CallManager](#)

[Messagerie vocale](#)

[Ressources en medias](#)

[Télécopie et prise en charge de modem](#)

[Versions de logiciel](#)

[Informations connexes](#)

Introduction

Le réseau australien d'universitaire et de recherches (AARNet) est un réseau IP ultra-rapide national qui interconnecte 37 universités australiennes aussi bien qu'organisation pour la recherche scientifique et industrielle du Commonwealth (la CSIRO).

AARNet a été au commencement construit comme réseau de données, mais il a porté la voix sur ip (VoIP) depuis début 2000. Le réseau VoIP actuellement déployé est une solution de contournement-contournement qui porte des appels VoIP entre les universités et les PBX automatiques CSIRO (PABX). Il fournit également les passerelles du réseau téléphonique public commuté (PSTN) qui permettent au PSTN pour sauter à cloche-pied outre tout au plus du point rentable. Par exemple, un appel d'un téléphone PABX à Melbourne à un téléphone PSTN à Sydney est porté comme VoIP de Melbourne à la passerelle PSTN de Sydney. Il est là connecté au PSTN.

L'université catholique australienne (ACU) est l'une des universités qui se connecte à AARNet. Vers la fin de 2000, l'ACU a commencé un déploiement de Téléphonie sur IP qui a déployé approximativement 2,000 Téléphones IP à travers six campus universitaires.

Cette étude de cas couvre le déploiement de Téléphonie sur IP ACU. Le projet est terminé. Cependant, il y a les questions architecturales significatives à adresser dans le circuit principal d'AARNet si le réseau est de mesurer quand d'autres universités suivent dans les pas de l'ACU. Ce document décrit ces questions et propose et discute de diverses solutions. Le déploiement de Téléphonie sur IP ACU est susceptible d'être ajusté plus tard afin de tomber en conformité avec l'architecture recommandée par finale.

Remarque: L'université de Deakin était la première université australienne pour déployer la Téléphonie sur IP. Cependant, l'université de Deakin n'emploie pas AARNet pour porter le trafic de Téléphonie sur IP.

AARNet

Les universités et la CSIRO australiennes ont construit AARNet en 1990 par Committee des vice-présidents australiens (AVCC). Quatre-vingt-dix-neuf pour cent du trafic Internet australien étaient aux membres fondateurs pendant les années premières. Un peu de trafic commercial était des organismes qui ont eu une association étroite avec le secteur tertiaire et de recherches. L'utilisation de l'userbase de non-AARNet a augmenté à 20 pour cent de tout le trafic de 1994 en retard.

L'AVCC a vendu la base de clients commerciale d'AARNet à Telstra en juillet de 1995. Cet événement a engendré ce qui était par la suite de devenir Telstra BigPond. Ceci a stimulé davantage de croissance de l'utilisation commerciale et privée de l'Internet en Australie. Le transfert de la propriété intellectuelle et de l'expertise a eu comme conséquence le développement de l'Internet en Australie. Autrement, ceci ne se serait pas produit à une vitesse si rapide.

L'AARNet2 développé par AVCC début 1997. C'était une autre amélioration de l'Internet en Australie, qui emploie des liens et des services Internet atmosphère de bande passante élevée dans le cadre d'un contrat avec Cable & Wireless Optus (CWO) Limited. Le déploiement rapide des Services IP par CWO pour répondre aux exigences AARNet2 était dû en partie du transfert de la connaissance et de l'expertise à partir d'AARNet.

ACU

L'ACU est une université publique qui a été fondée en 1991. L'université a approximativement 10,000 étudiants et personnel 1,000. Il y a six campus sur la Côte Est de l'Australie. Cette table affiche les campus ACU et leurs emplacements :

| Campus | Ville | État |
|-----------------|----------------|---|
| Support St Mary | Strathfield | La Nouvelle-Galles du Sud (NSW) |
| MacKillop | Sydney du nord | La Nouvelle-Galles du Sud (NSW) |
| Patrick | Melbourne | Victoria (carte d'interface virtuelle) |
| Aquinas | Ballarat | Victoria (carte d'interface virtuelle) |
| Signadou | Canberra | Territoire capitale de l'Australie (ACTE) |
| McAuley | Brisbane | Le Queensland (QLD) |

L'ACU s'est fondée sur une solution de spectre de Telstra (centre) avant le lancement de la solution de Téléphonie sur IP que cette étude de cas décrit. Le mouvement à la Téléphonie sur IP a été piloté principalement par le désir de réduire le coût.

LA CSIRO

La CSIRO a le personnel approximativement 6,500 à de nombreux sites en Australie. Recherche d'attitudes CSIRO dans les zones telles que l'agriculture, les minerais, l'énergie, la fabrication, les transmissions, la construction, les santés, et l'environnement.

La CSIRO était la première organisation pour utiliser AARNet pour le VoIP. L'organisation a frayé un chemin les premiers travaux effectués dans cette zone.

[AARNet](#)

Le circuit principal d'AARNet est un élément important dans n'importe quel déploiement de Téléphonie sur IP d'université. Il fournit à l'interconnexion des universités deux services de canalisation dans la zone de Voix :

- Transport des paquets de protocole de transmission en temps réel VoIP (RTP) avec la garantie du Qualité de service (QoS) appropriée pour exprimer
- Point bon marché de hopoff aux PSTN dans le pays

Cette section décrit l'architecture en cours d'AARNet et comment elle fournit ces services. Il trace les grandes lignes également de certains des problèmes d'évolutivité qui surgissent pendant que plus d'universités déploient la solution de Téléphonie sur IP. En conclusion, il discute les solutions possibles pour ces problèmes d'évolutivité.

[Topologie d'AARNet](#)

AARNet se compose d'un BRUIT simple (point de présence) dans chaque état. Les bruits désigné sous le nom des exploitations réseau régionales (RNOs). Les universités se connectent au RNO dans leur état respectif. Le RNOs à leur tour sont interconnectés par un maillage complet d'ATM PVC d'Optus. Ensemble ils constituent AARNet.

Le RNO typique se compose d'un commutateur ATM de Cisco LS1010 et d'un routeur Atmosphère-relié. Le routeur RNO se connecte à chaque routeur d'université par un PVC atmosphère simple à travers une liaison par micro-ondes d'E3. Chaque routeur RNO a également un maillage complet d'ATM PVC que le réseau atmosphère d'Optus fournit à tout autre RNOs. Ce diagramme représente la topologie du Général AARNet du réseau :

Il y a de nombreuses exceptions à la topologie. Certains d'entre eux sont significatifs d'un point de vue de Voix. Ce sont quelques exceptions :

- Le RNO dans Victoria emploie l'IP sur ATM classique (RFC 1577) au lieu de PVCs pour connecter les universités au RNO.
- Les universités rurales se connectent typiquement de nouveau au RNO par le Relais de trames ou le RNIS.
- Quelques grandes universités ont plus d'un lien de nouveau au RNO.

Cette table affiche les états et les territoires qui ont actuellement un RNO. La table inclut capitales pour les lecteurs qui ne sont pas au courant de la zone géographique australienne.

| État | Capitale | RNO ? | Connexions de campus |
|-------------------------------------|-----------|-------|----------------------|
| La Nouvelle-Galles du Sud | Sydney | Oui | À déterminer |
| Victoria | Melbourne | Oui | À déterminer |
| Le Queensland | Brisbane | Oui | À déterminer |
| Australie du sud | Adelaïde | Oui | À déterminer |
| Australie occidentale | Perth | Oui | À déterminer |
| Territoire de capitale australienne | Canberra | Oui | À déterminer |
| Territoire du nord | Darwin | Non | -- |
| La Tasmanie | Hobart | Non | -- |

Qualité de service

Des parties d'AARNet QoS-sont déjà activées pour la Voix en raison du projet de contournement-contournement VoIP. QoS est nécessaire pour le trafic vocal afin de fournir ces caractéristiques, qui réduisent le retard et instabilité et éliminent la perte de paquets :

- Maintien de l'ordre — Marquez en bas du trafic vocal des sources non-faites confiance.
- Queue — La Voix doit être accordée la priorité au-dessus de tout autre trafic pour réduire le retard pendant l'encombrement de liaison.
- Fonction Link Fragmentation and Interleaving (LFI) — Des paquets de données doivent être fragmentés et des paquets vocaux être intercalés sur les liens lents.

Le trafic doit être classifié correctement pour maintenir l'ordre et aligner des paquets vocaux. Cette section décrit comment la classification est faite sur AARNet. Les chapitres ultérieurs décrivent l'implémentation de maintien de l'ordre et de queue.

Classification

Non tout le trafic obtient le même QoS. Le trafic est classifié dans ces catégories pour fournir sélectivement QoS :

- Données
- Voix de connaître et sources sûres
- Voix des provenances inconnues

Seulement des périphériques de confiance sont donnés QoS de haute qualité sur AARNet. Ces périphériques sont principalement des passerelles identifiées par l'adresse IP. Une liste de contrôle d'accès (ACL) est utilisée pour identifier ces sources sûres de Voix.

```
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 Voix a une Priorité IP de 5.

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

Combinez les exemples précédents pour identifier des paquets d'une source sûre.

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

Employez les mêmes principes pour identifier des paquets vocaux d'une provenance inconnue.

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

Maintien de l'ordre

Le trafic vocal d'une source non-faite confiance est classifié et marqué en bas de quand le trafic arrive sur une interface. Ces deux exemples affichent comment maintenant l'ordre est exécuté selon quel type de trafic est prévu d'arriver sur une interface donnée :

Le routeur recherche non-a fait confiance à des paquets vocaux et change leur Priorité IP à 0 si là sont de confiance des sources de Voix 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 change leur Priorité IP à 0 s'il n'y a aucune source connue de Voix 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 dans AARNet était contournement-contournement jusque récemment. Cette condition a comme conséquence relativement peu de points finaux VoIP. La conception en cours de Mise en file d'attente distingue les interfaces qui ont l'en aval et les interfaces d'appareils voip qui ne font pas. Cette section discute s'aligner sur les interfaces non-VoIP.

Une interface non vocale est configurée pour le Mise en file d'attente pondérée (WFQ) ou le Détection précoce directe pondérée (WRED). Ceux-ci 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 la rendre facile de changer le mécanisme de mise en file d'attente sur un type d'interface donnée. Il y a une carte de stratégie par type d'interface. Ceci reflète le fait que non tous les mécanismes de mise en file d'attente sont 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 reliées aux interfaces respectives et sont spécifiques aux types d'interface. Par exemple, ceci simplifie le processus de changer le mécanisme de mise en file d'attente sur les ports Ethernet (basés sur VIP) processeur Processeur d'interface souple de WRED à WFQ. Il exige un changement simple de la carte de stratégie. Les modifications sont apportées à toutes les interfaces Ethernet basées sur 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
```

Basse Mise en file d'attente de latence

N'importe quelle interface qui en aval-a fait confiance à des appareils voip est configurée pour le Fonction Low Latency Queuing (LLQ). N'importe quel paquet qui le fait par la classification d'interface entrante et retient une priorité de 5 est sujet à un LLQ. N'importe quel autre paquet est sujet à WFQ ou à un WRED. Ceci dépend du type d'interface.

Des cartes distinctes de stratégie sont créées pour chaque type d'interface afin de faciliter QoS pour gérer. C'est semblable à la conception non vocale de Mise en file d'attente. Cependant, les plusieurs cartes de stratégie existent pour chaque type d'interface. C'est parce que la capacité des types d'interface pour porter le trafic vocal varie selon la vitesse de liaison, des configurations PVC, et ainsi de suite. Le nombre dans le map name de stratégie reflète le nombre d'appels a couvert 30 appels, 60 appels, et ainsi de suite.

```
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 reliées aux interfaces respectives. Dans cet exemple, la carte de stratégie est spécifique à un type d'interface. Actuellement aucun traitement spécial n'est donné pour exprimer la signalisation. Les cartes de stratégie peuvent facilement être modifiées dans un endroit si ceci devient une condition requise ultérieurement sur un type d'interface donnée. La modification prend l'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 a quelques problèmes d'évolutivité. Le problème principal est qu'il se fonde sur connaître l'adresse IP de chaque appareil VoIP de confiance dans le réseau. C'était une limite raisonnable dans le passé où il y avait un nombre limité de passerelles VoIP manipulant le contournement-contournement. Le nombre de points finaux VoIP augmente considérablement, et il devient de plus en plus irréaliste avec le déploiement de la Téléphonie sur IP. L'ACLs deviennent trop long et trop difficile de gérer.

L'ACLs ont été ajoutés pour faire confiance au trafic d'un sous-réseau spécifique IP de Voix à chaque campus ACU dans le cas de l'ACU. C'est une solution intermédiaire. Ces solutions plus à long terme sont étudiées :

- H.323 proxy
- Maintien de l'ordre d'entrée de QoS

L'idée principale derrière H.323 la solution de proxy est de faire entrer dans tout le trafic de RTP AARNet d'un campus donné au moyen d'un proxy. AARNet voit tout le trafic de RTP d'un campus donné avec une adresse IP simple, car ce diagramme affiche :

Le nombre d'entrées dans le QoS ACLs est limité à une ligne par campus si ce schéma est déployé uniformément. Ce schéma a toujours le potentiel d'ajouter à 100 entrées ou plus puisqu'il y a 37 universités avec de plusieurs campus. Ce n'est pas non plus extensible. Il pourrait être nécessaire de se déplacer à une conception avec un simple ou au nombre limité de superbe-proxys partagés à chaque RNO. Ceci réduit le nombre d'adresses IP de confiance à six. Cependant, ceci ouvrent une question de Réglementation QoS sur le chemin du campus au proxy au RNO.

Remarque: Les joncteurs réseau d'intercluster de Cisco CallManager ne fonctionnent pas actuellement par H.323 un proxy parce que la signalisation d'intercluster n'est pas H.225 indigène.

Le maintien de l'ordre d'entrée de QoS est une solution alternative. Une borne de confiance est établie au point où le campus se connecte au RNO à cette conception. Trafiquez qui entre dans AARNet est maintenu l'ordre par la caractéristique de Fonction Committed Access Rate (CAR) de Cisco IOS® à cette borne. Une université qui utilise AARNet pour le VoIP s'abonne à une bande passante d'AARNet QoS. Le trafic de moniteurs de CAR puis qui entre dans AARNet. Le trafic excédentaire a la Priorité IP marquée vers le bas à 0 si la quantité du trafic de RTP avec la Priorité IP 5 dépasse la bande passante abonnée.

Ce diagramme affiche une configuration du CAR :

Cet exemple affiche comment une configuration du CAR manipule ce maintien de l'ordre :

```
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
```

Ce sont quelques avantages d'une approche de configuration du CAR :

- Le noyau ne doit plus manipuler le maintien de l'ordre. Il est maintenant manipulé à la borne de confiance. Par conséquent, le LLQ au centre n'a pas besoin de savoir les adresses IP de confiance. N'importe quel paquet avec une Priorité IP de 5 au centre peut sans risque être sujet à un LLQ parce qu'il a déjà passé le maintien de l'ordre au d'entrée.
- Aucune supposition n'est faite au sujet de l'architecture, du matériel, et des protocoles VoIP

que les différentes universités choisissent. Une université peut choisir de déployer un Protocole SIP (Session Initiation Protocol) ou le Protocole MGCP (Media Gateway Control Protocol) qui ne fonctionne pas avec H.323 des proxys. Les paquets VoIP reçoivent le QoS approprié au centre tant que ils ont une Priorité IP de 5.

- Le CAR est résilient contre des attaques du Déni de service de QoS (DOS). Une attaque DoS de QoS qui provient d'une université ne peut pas endommager le noyau. Le CAR limite l'attaque, qui ne peut pas générer plus de trafic que ce qui est présent quand le nombre maximal d'appels permis VoIP est en activité. Le VoIP appelle à ou de ce campus peut souffrir pendant une attaque. Cependant, il appartient à l'université individuelle pour se protéger intérieurement. L'université peut serrer le CAR ACLs sur le routeur de sorte que tout sauf des sous-réseaux sélectionnés VoIP aient la Priorité IP marquée vers le bas. Chaque campus a une borne interne de confiance au point où les utilisateurs se connectent au RÉSEAU LOCAL de campus dans la conception finale. Trafiquez avec une Priorité IP de 5 que cette borne de confiance reçoit est limitée à 160 Kbps par port de commutateur, ou à deux G.711 appels VoIP. Le trafic au-dessus de ce débit est marqué vers le bas. L'implémentation de ce schéma exige des Commutateurs ou quelque chose de Catalyst 6500 semblables avec la fonctionnalité de limitation de débit.
- Le ravitaillement de bande passante simplifie au centre pendant que chaque université s'abonne à une quantité déterminée de bande passante de QoS. Ceci rend également l'affichage de QoS simple parce que chaque université peut payer un forfait mensuel plat basé sur un abonnement de bande passante de QoS.

La faiblesse principale dans cette conception est que la borne de confiance se trouve au routeur d'université, ainsi les universités doivent pouvoir gérer correctement le CAR. La borne de confiance est tirée de nouveau dans le RNO. le matériel RNO-géré manipule le maintien de l'ordre dans la conception finale. Cette conception exige la limitation de débit réalisée par matériel telle que le commutateur du Catalyst 6000 ou un processeur de Moteur de services réseau de Cisco 7200 (Cisco 7200 NSE-1). Cependant, il donne le contrôle complet d'AARNet et de RNOs au-dessus de la Réglementation QoS. Ce diagramme affiche cette conception :

[Fragmentation de liaison et interfoliage](#)

Le VoIP seulement est porté à travers les circuits virtuels ATM relativement ultra-rapides (VCs). Par conséquent, aucun LFI n'est exigé. Le VoIP peut également être transporté à travers le Forum Frame Relay (FRF) ou les lignes louées aux universités rurales à l'avenir. Ceci exige des mécanismes LFI tels que le PPP à liaisons multiples (MLP) avec l'entrelacement ou le FRF.12.

[Passerelles](#)

Il y a deux genres de Passerelles H.323 dans AARNet :

- PSTN — PSTN à la passerelle VoIP
- PABX — PABX à la passerelle VoIP

La distinction entre une passerelle PSTN et PABX est principalement fonctionnelle. Les passerelles PSTN fournissent la Connectivité au PSTN. Les passerelles PABX connectent un PABX d'université au circuit principal VoIP. La même case physique agit en tant que PSTN et passerelle PABX dans de nombreux cas. Il y a actuellement 31 passerelles dans la solution de Téléphonie sur IP ACU. La plupart de ces passerelles sont des serveurs d'accès universel de Cisco AS5300. Les autres passerelles sont des Routeurs de gamme Cisco 3600 ou des Routeurs de gamme Cisco 2600. On s'attend à ce qu'un minimum de dix passerelles supplémentaires

soient ajoutées pendant le Q2CY01. AARNet a porté approximativement 145,000 appels VoIP en avril de 2001.

AARNet a déployé des Passerelles H.323 PSTN-relées à la plupart des villes importantes, car ce diagramme affiche :

Les universités peuvent utiliser ces passerelles pour faire des appels sortants au PSTN. Les universités doivent mettre à jour leurs propres joncteurs réseau pour des appels d'arrivée parce qu'elles ne sont pas actuellement prises en charge. AARNet peut être en pourparlers très un prix concurrentiel avec le transporteur en raison du volume d'appels qui passent par ces passerelles. Des appels peuvent également être abandonnés outre tout au plus du point rentable. Par exemple, quelqu'un à Sydney qui demande un numéro de Perth peut utiliser la passerelle de Perth et seulement être facturé un appel local. Ceci est également connu comme saut de fin hors fonction (TEHO).

Un garde-porte simple est déployé pour exécuter E.164 à la résolution d'adresse IP. Tous les appels au PSTN sont envoyés au garde-porte, qui renvoie alors l'adresse IP de la passerelle la plus appropriée. Référez-vous aux sections de [Plans de composition](#) et de [garde-porte](#) pour plus d'informations détaillées sur des garde-portes.

[Facturation et comptabilité](#)

Les passerelles PSTN utilisent le RAYON et l'Authentification, autorisation et comptabilité (AAA) pour l'affichage. Chaque appel par une passerelle génère un article mouvement d'appel (CDR) pour chaque tronçon d'appel. Ces CDR sont signalés au serveur de RAYON. L'adresse IP du Cisco CallManager dans le CDR identifie seulement l'université et s'assure que l'interlocuteur correct est affiché.

[Sécurité de passerelle](#)

La protection des passerelles PSTN contre des attaques DoS et la fraude est un souci important. H.323 les clients sont largement - disponibles. La Microsoft NetMeeting est empaquetée avec le Microsoft Windows 2000, ainsi il est relativement facile pour un utilisateur non technicien de placer des appels gratuits par ces passerelles. Configurez un ACL d'arrivée qui permet à la signalisation H.225 des adresses IP de confiance pour protéger ces passerelles. Cette approche a tous les mêmes problèmes d'évolutivité que la section de [QoS](#) décrit. Le nombre d'entrées dans l'ACL se développe pendant que le nombre de confiance H.323 de points finaux se développe.

H.323 les proxys offrent de l'allègement dans cette zone. La nécessité d'ACLs de passerelle de permettre une adresse IP par campus universitaire si tous les appels par la passerelle PSTN traversent un proxy de campus. Deux adresses IP comme proxy redondant est désirable dans la plupart des cas. Même avec des proxys, l'ACL peut contenir plus de 100 entrées.

Le proxy doit être protégé par l'intermédiaire d'ACLs puisque H.323 peut installer un appel par le proxy. L'ACL de proxy doit permettre des périphériques de gens du pays H.323 pendant que la stratégie locale exige puisque ceci est fait sur une base de par-campus.

Les adresses IP des deux Cisco CallManagers doivent être incluses dans la passerelle ACLs si un campus veut permettre seulement à des appels des Téléphones IP pour utiliser les passerelles PSTN d'AARNet. Les proxys n'ajoutent aucune valeur dans cette situation. Le nombre de rubriques de liste ACL exigés est deux l'un ou l'autre de manière.

Notez que les appels téléphone-à-IP IP d'intercampus n'ont pas besoin de traverser le proxy.

Plans de composition

Le Plan de composition du courant VoIP est simple. Les utilisateurs peuvent placer ces deux types d'appels d'un point de vue de passerelle VoIP :

- Appelez un téléphone à un campus différent mais à la même université.
- Appelez un téléphone PSTN ou un téléphone à une université différente.

Les homologues de numérotation de passerelle reflètent le fait qu'il y a seulement deux types d'appels. Fondamentalement il y a deux types de pair de cadran VoIP, comme indiqué dans 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 pair de cadran est utilisé si quelqu'un appelle l'extension 7... à un autre campus dans cet exemple. Cet appel est conduit directement à l'adresse IP de la passerelle distante. Puisque le garde-porte est évité, le contrôle d'admission d'appel (CAC) n'est pas exécuté.

Le deuxième pair de cadran est utilisé quand l'appel est pour un nombre PSTN. Ceci peut être l'un ou l'autre un de ces éléments :

- Le nombre d'un téléphone dans le PSTN
- Le nombre plein-qualifié PSTN d'un téléphone à une université différente

L'appel est envoyé au garde-porte au moyen d'un message de la demande d'admission (ARQ) dans le premier cas. Le garde-porte renvoie l'adresse IP de la meilleure passerelle PSTN dans une admission confirment le message (ACF).

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

Garde-porte

AARNet actionne actuellement un garde-porte simple. L'objectif unique de ce garde-porte est d'effectuer le routage d'appels sous forme d'E.164 à la résolution d'adresse IP. Le garde-porte n'exécute pas le CAC. Le nombre de joncteurs réseau PABX s'est connecté aux passerelles limite le nombre d'appels simultanés. La principale bande passante couvre tous les joncteurs réseau en service immédiatement. Ceci change avec le lancement de la Téléphonie sur IP à l'ACU et à d'autres universités. Il n'y a aucune limite naturelle sur le nombre d'appels simultanés VoIP dans lesquels peut être originaire ou hors d'un campus donné dans ce nouvel environnement. La bande passante disponible de QoS peut être oversubscribed si trop d'appels sont initiés. Tous les appels peuvent souffrir de la mauvaise qualité dans cette condition. Utilisez le garde-porte pour fournir le CAC.

La taille distribuée de nature et de potentiel du réseau voix d'université se prête à une architecture distribuée de garde-porte. Une solution possible est d'avoir une conception hiérarchique à deux

étages de garde-porte dans laquelle chaque université met à jour son propre garde-porte. Ce garde-porte d'université désigné sous le nom d'un garde-porte du niveau 2. AARNet actionne un garde-porte de *répertoire* qui désigné sous le nom d'un garde-porte du niveau 1.

Les universités doivent employer cette approche à deux étages pour utiliser un garde-porte pour le routage d'appels entre les batteries de Cisco CallManager. Le garde-porte conduit des appels basés sur des 4 ou une extension 5-digit dans ce scénario. Chaque université exige son propre garde-porte. C'est parce que les plages d'extensions superposent entre les universités puisque c'est un espace d'adressage local-géré.

Les garde-portes du niveau 2 d'université exécutent le CAC pour des appels à et de cette université seulement. Il exécute également la résolution E.164 pour des appels entre seulement les campus de cette université. L'appel est conduit par le garde-porte du niveau 2 au garde-porte du niveau 1 au moyen d'un message de la demande d'emplacement (LRQ) si quelqu'un appelle un téléphone IP à une autre université ou appelle le PSTN par une passerelle d'AARNet. Le LRQ est expédié au garde-porte du niveau 2 de cette université si l'appel est pour une autre université. Ce garde-porte renvoie alors un message ACF au garde-porte du niveau 2 à l'université où l'appel commence. Les deux garde-portes du niveau 2 exécutent le CAC. Ils poursuivent seulement l'appel s'il y a bande passante suffisante disponible à chacun des deux appeler et les zones appelées.

AARNet peut choisir de traiter les passerelles PSTN d'AARNet comme ceux de n'importe quelle université. Leur propre garde-porte du niveau 2 s'occupe de eux. Le garde-porte du niveau 1 peut également agir en tant que garde-porte du niveau 2 pour ces passerelles si autorisation de chargement et de représentation.

Chacun des garde-portes (garde-porte y compris de répertoire d'AARNet) doit être répliqué parce que les passerelles sont un tel élément essentiel. Chaque université doit avoir deux garde-portes. Il est possible que les passerelles de Cisco IOS aient les garde-portes alternatifs, comme dans le cas du Logiciel Cisco IOS version 12.0(7)T. Cependant, ceci n'est H.323 actuellement pris en charge par Cisco CallManager ou aucun autre périphérique de tierce partie. N'utilisez pas cette caractéristique à ce moment. Utilisez une solution (basée sur hsrp) basée sur des protocoles de routeur de secours immédiat simple à la place. Ceci exige que les deux garde-portes s'asseyent sur le même sous-réseau IP. Le HSRP détermine quel garde-porte est en activité.

Réseau de Téléphonie sur IP ACU

Cette table affiche le nombre approximatif de Téléphones IP installé aux campus de l'ACU :

| Campus | Ville | Téléphones IP approximatifs |
|-----------------|----------------|-----------------------------|
| Support St Mary | Strathfield | 400 |
| MacKillop | Sydney du nord | 300 |
| Patrick | Melbourne | 400 |
| Aquinas | Ballarat | 100 |
| Signadou | Canberra | 100 |
| McAuley | Brisbane | 400 |
| | Total : | 1700 |

L'ACU a récemment déployé une solution de Téléphonie sur IP. La solution se compose d'une batterie de deux Cisco CallManagers, d'une passerelle de Cisco 3640 à chaque campus, et des Téléphones IP. AARNet interconnecte les campus. Ce diagramme dépeint la topologie de haut niveau et les divers composants du réseau de Téléphonie sur IP ACU :

Topologie du réseau ACU

Ce diagramme affiche un campus typique ACU. Chaque campus a trois couches de Commutateurs de Catalyst. L'armoire de câblage loge les Commutateurs plus anciens de Catalyst 1900. Les Commutateurs de Catalyst 1900 se connectent de nouveau au commutateur du Catalyst 3500XL au moyen de tramage étendu. Ceux-ci se connectent de nouveau à un commutateur simple du Catalyst 6509 au moyen de Gigabit Ethernet (GE). Un routeur simple du Cisco 7200 VXR connecte le campus à AARNet par un circuit virtuel atmosphère aux gens du pays RNO.

La méthode de Connectivité au RNO diffère légèrement de l'état pour énoncer, car cette table affiche. Victoria est basée sur l'IP sur ATM classique (RFC 1577). L'autre RNOs ont un PVC droit installé avec l'encapsulation RFC 1483. Le Protocole OSPF (Open Shortest Path First) est le protocole de routage utilisé entre l'ACU et le RNOs.

| Campus | État | Connectivité à RNO | Protocole de routage |
|-----------------|-----------------------------|-------------------------------|----------------------|
| Support St Mary | NSW | PVC RFC 1483 | OSPF |
| MacKillop | NSW | PVC RFC 1483 | OSPF |
| Patrick | carte d'interface virtuelle | IP sur ATM classique RFC 1577 | OSPF |
| Aquinas | carte d'interface virtuelle | IP sur ATM classique RFC 1577 | OSPF |
| Signadou | ACTE | PVC RFC 1483 | OSPF |
| McAuley | QLD | PVC RFC 1483 | OSPF |

Les Commutateurs de gamme Catalyst 1900 prennent en charge la jonction sur les liaisons ascendantes seulement. Par conséquent, tous les Téléphones IP et les PC sont dans un grand VLAN. En fait, le campus entier est un grand domaine VLAN et d'émission. Des sous-réseaux secondaires IP sont utilisés en raison de le grand nombre de périphériques. Les Téléphones IP sont sur un sous-réseau IP, et les PC sont sur des autres. Le noyau d'AARNet fait confiance au sous-réseau de téléphone IP, et le trafic à et de ce sous-réseau IP est sujet à un LLQ.

Les artères de routeur de Cisco 7200 entre les sous-réseaux primaires et secondaires IP. La carte de fonction de commutateur de Mutilayer (MSFC) dans le commutateur de Catalyst 6500 n'est pas actuellement utilisée.

Les Commutateurs du Catalyst 3500XL et du Catalyst 6500 ont des caractéristiques de QoS, mais ils ne sont pas actuellement activés.

QoS dans le campus

La conception campus en cours n'est pas conforme aux directives de conception Cisco-recommandées pour la Téléphonie sur IP. Ce sont quelques soucis concernant QoS :

- Le domaine d'émission est très grand. Les émissions excessives peuvent affecter la représentation des Téléphones IP, qui doivent les traiter.
- Les Commutateurs de Catalyst 1900 ne sont pas QoS-capables. Si un téléphone IP et un PC sont connectés au même port de commutateur, des paquets vocaux peuvent être lâchés si le PC reçoit des données à un haut débit.

Remodelez les parties de l'infrastructure de campus pour réaliser des améliorations significatives. Une mise à niveau matérielle n'est pas exigée. Ce diagramme montre les principes derrière la reconception recommandée :

Le campus doit être coupé en Voix VLAN et données VLAN. Les téléphones et les PC qui se connectent à un commutateur de Catalyst 1900 doivent maintenant se connecter à différents ports afin de réaliser la séparation VLAN. Une liaison ascendante supplémentaire de chaque commutateur de Catalyst 1900 au commutateur de Cisco 3500XL est ajoutée. Une des deux liaisons ascendantes est un membre de la Voix VLAN. L'autre liaison ascendante est un membre des données VLAN. N'utilisez pas la jonction de l'InterSwitch Link (ISL) comme alternative à deux liaisons ascendantes. Ceci ne fournit pas au trafic voix et de données des files d'attente séparées. Les liens de GE du commutateur du Catalyst 3500XL au commutateur du Catalyst 6000 doivent également être convertis en joncteurs réseau de 802.1Q de sorte que la Voix et les données VLAN puissent être portées à travers ce principal commutateur.

Les ports sur le Catalyst 3500XL commutent qui sont dans les données VLAN ont un Classe de service (Cos) par défaut de zéro. Les ports qui sont des membres de la Voix VLAN ont le cos par défaut de 5. en conséquence, le trafic vocal est correctement donné la priorité une fois qu'il arrive au noyau du Catalyst 3500 ou du Catalyst 6500. Les configurations de port de commutateur de QoS du Catalyst 3500 varient légèrement selon quel port de commutateur VLAN est un membre, comme indiqué dans 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 commutateur arrière sur le téléphone IP dans le rare cas que les Téléphones IP connectent directement à un commutateur du Catalyst 3500XL. Les Téléphones IP se connectent au commutateur au moyen d'un joncteur réseau de 802.1Q dans ce cas. Ceci permet à la Voix et aux paquets de données pour voyager sur des VLAN distincts, et vous pouvez donner à des paquets le cos correct au d'entrée. Remplacez les Commutateurs de Catalyst 1900 par des Commutateurs du Catalyst 3500XL ou d'autres Commutateurs QoS-capables comme ils atteignent la fin de la vie. Cette topologie devient alors la méthode standard de connecter des Téléphones IP et des PC au réseau. Ce scénario affiche la configuration QoS de commutateur du Catalyst 3500XL :

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



```
switchport priority extend 0
```

En conclusion, les deux ports qui se connectent aux deux Cisco CallManagers devraient avoir le cos codé en dur à 3. que le Cisco CallManager place la Priorité IP à 3 dans des tous les paquets de signalisation de Voix. Cependant, le lien du Cisco CallManager au commutateur du Catalyst 3500XL n'utilise pas 801.1p. Par conséquent, la valeur CoS est forcée au comme indiqué dans cet exemple de commutateur :

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

L'obstacle principal avec cette conception est que deux ports de commutateur sont exigés à l'appareil de bureau. Le campus de Patrick pourrait exiger des ports de commutateur des frais supplémentaires 400 pour 400 Téléphones IP. Des Commutateurs supplémentaires du Catalyst 3500XL doivent être déployés si les ports suffisants ne sont pas disponibles. Seulement un port de commutateur du Catalyst 3500XL est exigé pour chaque deux ports de commutateur manquants de Catalyst 1900.

Les Commutateurs de Catalyst 6500 ACU de courant ont des capacités de QoS, mais ils ne sont pas actuellement activés. Ces modules sont présents dans le commutateur du Catalyst 6000 ACU avec ces capacités de mise en file d'attente :

| Emplacement | 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 | | |

Terminez-vous ces étapes pour lancer les caractéristiques appropriées de QoS sur le commutateur du Catalyst 6000 :

1. Dites le commutateur de fournir à QoS sur une base par-VLAN cette commande

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

2. Dites le commutateur de faire confiance aux valeurs CoS reçues du commutateur du

```
Catalyst 3500XL avec cette commande :Cat6K>(enable) set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos
```

Le cos doit maintenant être placé au mappage de point de code de Différenciation de services (DSCP). Ceci est exigé parce que le commutateur du Catalyst 6000 réécrit la valeur DSCP dans l'en-tête IP basée sur la valeur CoS reçue. Les paquets de signalisation VoIP doivent avoir le cos de 3, réécrit avec un DSCP d'AF31 (26). Les paquets de RTP doivent avoir le cos de 5, réécrit avec un DSCP d'E-F (46). Émettez la commande suivante :

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

Employez cet exemple pour vérifier le mappage de CoS-to-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 le MSFC pour conduire entre les divers sous-réseaux IP.

QoS dans le RNO

La conception du courant RNO n'est pas conforme aux directives de conception Cisco recommandées pour la Téléphonie sur IP. Ces soucis existent en vue de QoS :

- LLQ n'est pas appliqué sur le routeur WAN de gamme 7200 ACU de Cisco.
- Les campus de Patrick et d'Aquinas se connectent au RNO au moyen de VCs commuté par atmosphère (SVC). LLQ n'est pas pris en charge sur des SVC.

Un routeur de Cisco 7200 Ethernet-relie Fast connecte le campus à un RNO au moyen d'un lien 34 atmosphères du Mbits/s E4. Le trafic peut potentiellement aligner sortant sur les liens de 34M en raison des 4M contre la non-concordance de vitesse de 100M. Par conséquent, il est nécessaire de donner la priorité au trafic vocal. Utilisation LLQ. La configuration de routeur de Cisco 7200 est semblable 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 le $N \times 24Kbps$, où N est le nombre G.729 d'appels simultanés.

Installez un PVC de chacun des Routeurs de Cisco 7200 de Patrick et d'Aquinas au routeur d'AARNet. Les atmosphères SVC dans Victoria RNO ne prennent en charge pas LLQ, car elles sont basées sur l'IP sur ATM classique (RFC 1577). Les autres universités dans Victoria RNO peuvent continuer à utiliser RFC 1577 pour l'instant. Cependant, remplacez par la suite l'infrastructure classique d'IP sur ATM.

Passerelles

Chacun des campus ACU a un routeur de Cisco 3640 qui agit en tant que passerelle H.323. Ces passerelles se connectent au PSTN au moyen de RNIS. Le nombre d'accès primaires (PRIs) et de canaux B dépend de la taille du campus. Ce tableau présente le nombre de PRIs et des canaux B pour chaque campus :

| Campus | Quantité PRI | Quantité de canal B |
|-----------------|--------------|---------------------|
| Support St Mary | 2 | 30 |
| MacKillop | 2 | 50 |
| Patrick | 2 | 50 |
| Aquinas | 1 | 20 |
| Signadou | 1 | 20 |

| | | |
|---------|---|----|
| McAuley | 1 | 30 |
|---------|---|----|

Ces passerelles sont utilisées seulement en tant que passerelles secondaires pour DOD (prise directe du réseau). Les passerelles d'AARNet sont les passerelles principales. Les passerelles ACU sont toujours utilisées pour ONT FAIT (sélection directe à l'arrivée).

Plan de composition

Le Plan de composition est basé sur les numéros de poste à 4 chiffres. L'extension est également les quatre derniers chiffres du a numéroté. Ce tableau présente les plages d'extensions et A FAIT des nombres pour chaque campus :

| Campus | Extension | A FAIT |
|-----------------|-----------|-----------------|
| Support St 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 |

Un entrée num-exp simple sur les passerelles tronquent a numéroté à l'extension à 4 chiffres avant qu'elle la transmette au Cisco CallManager. Par exemple, la passerelle de campus de Patrick a cette entrée :

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

Les utilisateurs composent zéro pour sélectionner un fil extérieur. Ce principal zéro est transmis à la passerelle. Un homologue de numérotation POTS simple conduit l'exigence que le port RNIS a basée sur le principal zéro.

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

Les appels entrant emploient cet entrée num-exp pour transformer le numéro appelé à une extension à 4 chiffres. L'appel apparie alors les deux pairs de cadran VoIP. Basé sur la préférence inférieure, il préfère cette artère à l'abonné de 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

Chacun des campus a une batterie qui se compose de deux serveurs Cisco CallManagers. Les serveurs Cisco CallManagers sont un mélange du serveur 7835 (MCS-7835) de convergence de medias et le serveur 7820 (MCS-7820) de convergence de medias. Les deux serveurs ont exécuté 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 primaire pour tous les Téléphones IP. Ce tableau présente le matériel déployé à chaque campus :

| Campus | Plate-forme | CallManagers |
|-----------------|-------------|--------------|
| Support St 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 batterie est configurée avec deux régions :

- On pour l'intracampus appelle (G.711)
- On pour l'intercampus appelle (G.729)

Le CAC géolocalisé n'est pas approprié pour l'ACU parce que tous les Téléphones IP servis par chaque batterie sont sur un campus simple. Il y a des mérites à un CAC garde-porte garde-porte pour des appels d'intercampus, mais ceci n'est pas actuellement mis en application. Cependant, il y a des plans à faire tellement dans un avenir proche.

Chaque Cisco CallManager est configuré avec 22 Passerelles H.323. Ceci se compose de joncteurs réseau d'intercluster aux cinq autres batteries de Cisco CallManager, à six passerelles PSTN d'AARNet, et à une passerelle ACU à chaque campus.

| H.323 type de périphérique | Quantité |
|----------------------------|------------|
| CallManager d'Intercampus | 2 x 5 = 10 |
| Passerelle PSTN d'AARNet | 6 |
| Passerelle PSTN ACU | 6 |
| Total : | 22 |

Des listes de routage et les groupes d'artère sont utilisés pour ranger les passerelles PSTN. Par exemple, cette table affiche comment les appels du Cisco CallManager de Patrick à Melbourne au PSTN de Sydney peuvent utiliser les quatre passerelles pour attacher les appels ainsi qu'un groupe d'artère.

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

Les Cisco CallManagers sont configurés avec approximativement 30 modèles d'artère, car cette table affiche. Les modèles d'artère sont conçus tellement là sont les correspondances spécifiques pour tous les nombres australiens domestiques. De cette façon, les utilisateurs ne doivent pas attendre le délai interchiffre pour expirer avant que le Cisco CallManager initie l'appel. Le caractère générique « ! » est utilisé seulement dans le modèle d'artère pour des numéros internationaux. Les utilisateurs doivent attendre jusqu'à ce que le délai interchiffre (par défaut 10 secondes) expire avant les progressions de l'appel quand ils composent une destination internationale. Les utilisateurs peuvent également ajouter le modèle "0.0011!#" d'artère. Les utilisateurs peuvent alors entrer dans « # » après que le dernier chiffre pour indiquer au Cisco CallManager que le numéro composé est complet. Cette action accélère la composition internationale.

| Modèle d'artère | Description |
|-----------------|--|
| | Appel local |
| 0.00 | Appel au secours - si l'utilisateur oublie composé 0 pour le fil extérieur |
| 0.000 | Appel au secours |
| 0.013 | Aide du dossier |
| 0.1223 | |
| 0.0011 ! | Appels internationaux |
| | Appels vers la Nouvelle-Galles du Sud |
| | Appels à Victoria |
| | Appels aux téléphones portables |
| | Appels vers le Queensland |
| | Appels à l'Australie occidentale |
| | Appels vers l'Australie du sud et le territoire du nord |
| | Appels à 1800 xxx xxx de xxx xxx et 1900 |
| 0.1144X | Urgence |
| 0.119[4-6] | Temps et temps |
| 0.1245X | Répertoire |
| 0.13[1-9]XXX | Appels aux nombres 13xxxx |
| | Appels à 1300 nombres xxx xxx |
| 2[0-1]XX | Appels inter-cluster à Signadou |
| 3[0-4]XX | Appels inter-cluster à Patrick |
| 5[3-4]XX | Appels inter-cluster à Aquinas |
| 7[2-5]XX | Appels inter-cluster à McAuley |
| 8[0-3]XX | Appels inter-cluster à MacKillop |
| 9[3-4]XX | Appels inter-cluster pour monter St Mary |
| 9[6-7]XX | Appels inter-cluster pour monter St Mary |

Le nombre de passerelles, de groupes d'artère, de listes de routage, et de modèles d'artère configurés sur les Cisco CallManagers ACU a le potentiel de devenir un grand nombre. Si une nouvelle passerelle RNO est déployée, chacune des cinq batteries de Cisco CallManager doit être modifiée avec une passerelle supplémentaire. Encore plus mauvais, des centaines de passerelles

doivent être ajoutées si l'artère VoIP de Cisco CallManagers ACU appelle directement à toutes autres universités et sautent le PSTN totalement. Clairement ceci ne mesure pas très bien.

La solution est de rendre les Cisco CallManagers garde-porte garde-porte. Vous devez seulement mettre à jour le garde-porte quand une nouvelle passerelle ou Cisco CallManager est ajoutée quelque part dans l'AARNet. Chaque Cisco CallManager doit avoir seulement la passerelle locale de campus et le périphérique configuré anonyme quand ceci se produit. Vous pouvez penser à ce périphérique comme joncteur réseau point-à-multipoint. Il retire la nécessité pour les joncteurs réseau engrenés de PPP dans le modèle de Plan de composition de Cisco CallManager. Un seul groupe d'artère indique au périphérique anonyme comme passerelle préférée et la passerelle locale comme passerelle de sauvegarde. La passerelle PSTN locale est utilisée pour certains appels locaux et également pour le hors fonction-net général appelle si le garde-porte devient indisponible. Actuellement, le périphérique anonyme peut être intercluster ou H.225, mais pas tous deux en même temps.

Le Cisco CallManager a besoin de moins modèles d'artère avec un garde-porte qu'il a maintenant. En principe, le Cisco CallManager a besoin seulement d'un modèle simple d'artère de « ! » indication le garde-porte. En réalité, la manière dans laquelle des appels sont conduits doit être plus spécifique pour ces raisons :

- Quelques appels (tels que des appels à 1-800 ou des numéros d'urgence) doivent être conduits par une passerelle géographiquement locale. Quelqu'un à Melbourne qui compose la police ou une chaîne de restaurant telle que Pizza Hut ne veut pas être connecté à la police ou au Pizza Hut à Perth. Les modèles spécifiques d'artère sont nécessaires que point directement à la passerelle PSTN locale de campus pour ces nombres. Les universités qui prévoient d'exécuter de futurs déploiements de Téléphonie sur IP peuvent choisir de compter seulement sur les passerelles d'AARNet et de ne pas gérer leurs propres passerelles locales. Ces nombres doivent avoir code postal virtuel ajouté au début par Cisco CallManager avant de l'envoyer au garde-porte afin de faire ce travail de conception pour les appels qui doivent être abandonnés hors fonction localement. Par exemple, le Cisco CallManager peut ajouter 003 au début aux appels d'un téléphone basé sur Melbourne au nombre de Pizza Hut 1-800. Ceci permet au garde-porte pour conduire l'appel à une passerelle basée sur Melbourne d'AARNet. La passerelle décolle les 003 principaux avant qu'elle place l'appel dans le PSTN.
- Des modèles d'artère d'utilisation avec les correspondances spécifiques pour tous les nombres domestiques afin d'éviter d'avoir l'attente d'utilisateur le délai interchiffre avant l'appel est initiés.

Cette table affiche les modèles d'artère pour un Cisco CallManager garde-porte garde-porte :

| Modèle d'artère | Description | Artère | Garde-porte |
|-----------------|------------------|-------------------|-------------|
| | Appel local | Liste de routage | AARNet |
| 0.00 | Appel au secours | Passerelle locale | Aucun |
| 0.000 | Appel au secours | Passerelle locale | Aucun |
| 0.013 | Aide du dossier | Passerelle | Aucun |

| | | | |
|--------------|---|-------------------|--------|
| | | locale | |
| 0.1223 | | Passerelle locale | Aucun |
| 0.0011 ! | Appels internationaux | Liste de routage | AARNet |
| 0.0011!# | Appels internationaux | Liste de routage | AARNet |
| | Appels en Nouvelle-Galles du Sud, Victoria, et téléphones portables | Liste de routage | AARNet |
| | Appels vers l'Australie du sud, l'Australie occidentale, et le territoire du nord | Liste de routage | AARNet |
| | Appels à 1800 xxx xxx de xxx xxx et 1900 | Passerelle locale | Aucun |
| 0.1144X | Urgence | Passerelle locale | Aucun |
| 0.119[4-6] | Temps et temps | Passerelle locale | Aucun |
| 0.13[1-9]XXX | Appels aux nombres 13xxxx | Passerelle locale | Aucun |
| | Appels à 1300 nombres xxx xxx | Passerelle locale | Aucun |
| [2-3]XXX | Appels à Signadou | Liste de routage | ACU |
| 5XXX | Appels à Aquinas | Liste de routage | ACU |
| [7-9]XXX | Appels à McAuley, à MacKillop, et à support St Mary | Liste de routage | ACU |

Le garde-porte conduit les appels internationaux, qui ne sont pas envoyés par la passerelle locale. C'est significatif parce qu'AARNet peut déployer les passerelles internationales à l'avenir. Si une passerelle est déployée aux Etats-Unis, une modification de configuration du contrôleur d'accès simple permet à des universités pour placer des appels aux USA aux débits domestiques des USA.

Le garde-porte exécute le routage d'appel inter-cluster basé sur l'extension à 4 chiffres ACU. Cet espace d'adressage superpose très probablement avec d'autres universités. Ceci dicte que l'ACU gèrent son propre garde-porte et utilisent le garde-porte d'AARNet en tant que *garde-porte de répertoire*. La colonne de garde-porte dans cette table indique si le routage d'appels est effectué par le garde-porte ACU ou le garde-porte d'AARNet.

Remarque: La mise en garde unique avec la solution proposée de garde-porte est que le périphérique anonyme peut actuellement être intercluster ou H.225, mais pas chacun des deux en même temps. Le Cisco CallManager se fonde sur le garde-porte pour conduire des appels aux deux passerelles (H.225) et d'autres Cisco CallManagers (intercluster) avec la conception proposée. Le contournement pour cette question est pas à l'utilisation le garde-porte pour le routage d'intercluster ou pour traiter tous les appels par l'intermédiaire du garde-porte comme H.225. Le dernier contournement signifie que quelques caractéristiques supplémentaires pourraient être indisponibles sur des appels inter-cluster.

Messagerie vocale

L'ACU a eu trois serveurs de messagerie vocale de l'esprit OS/2-based de Voix active avec les panneaux dialogiques de téléphone avant le transfert à la Téléphonie sur IP. Le plan est de réutiliser ces serveurs dans l'environnement de Téléphonie sur IP. Une fois mis en application, chaque serveur d'esprit se connecte à un Cisco CallManager au moyen d'un Simplified Message Desk Interface (SMDI) et d'une carte du Foreign Exchange Station 24-Port du Catalyst 6000 (FXS). Ceci fournit la messagerie vocale pour trois des six campus, qui quitte trois campus sans messagerie vocale. Il n'est pas possible de partager correctement un serveur d'esprit entre les utilisateurs sur deux batteries de Cisco CallManager parce qu'il n'y a aucune manière de propager l'indicateur de message en attente (MWI) à travers d'intercluster le joncteur réseau H.323.

L'ACU pourrait acheter trois serveurs de Cisco Unity pour les campus qui restent. Ces serveurs sont basés sur maigre, ainsi aucune passerelle n'est exigée. Ce tableau présente les solutions de messagerie vocale au cas où l'ACU achèterait les serveurs supplémentaires de messagerie vocale :

| Campus | Système de messagerie voix | Passerelle |
|-----------------|----------------------------|---------------------------|
| Support St Mary | Esprit de Voix active | Catalyst 6000 24-port FXS |
| MacKillop | Esprit de Voix active | Catalyst 6000 24-port FXS |
| Patrick | Esprit de Voix active | Catalyst 6000 24-port FXS |
| Aquinas | Cisco Unity | |
| Signadou | Cisco Unity | |
| McAuley | Cisco Unity | |

Les six serveurs de messagerie vocale fonctionnent en tant qu'îles d'isolement de messagerie vocale dans ce plan. Il n'y a aucun réseau de messagerie vocale.

Ressources en medias

Les processeurs de signaux numériques de matériel (DSP) ne sont pas actuellement déployés à l'ACU. Les Conférences utilisent la passerelle articulée autour d'un logiciel de conférence sur le Cisco CallManager. Des Conférences d'Intercluster ne sont pas actuellement prises en charge.

Le transcodage n'est pas actuellement exigé. Seulement G.711 et G.729 des codeur-décodeurs sont utilisés, et ils sont pris en charge par tous les périphériques déployés d'extrémité.

Télécopie et prise en charge de modem

La télécopie et le trafic de modem n'est pas actuellement prise en charge par le réseau de Téléphonie sur IP ACU. L'université prévoit d'utiliser la carte du Catalyst 6000 24-Port FXS à cet effet.

Versions de logiciel

Ce tableau présente l'ACU de versions de logiciel utilisée au moment de cette publication :

| Plate-forme | Fonction | Version de logiciel |
|--------------------------|--------------------------------------|---------------------|
| CallManager | IP-PBX | 3.0(10) |
| Catalyst 3500XL | Commutateur de distribution | 12.0(5.1)XP |
| Catalyst 6500 | Principal commutateur | 5.5(5) |
| Catalyst 1900 | Commutateurs des armoires de câblage | |
| Processeur de Cisco 7200 | Routeur WAN | 12.1(4) |
| Routeur de 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](#)