Caso aziendale: implementazione della telefonia IP - ACU

Sommario

Introduzione

L'Australian Academic and Research Network (AARNet) è una rete IP ad alta velocità che interconnette 37 università australiane e la Commonwealth Scientific and Industrial Research Organization (CSIRO).

AARNet è stato inizialmente costruito come rete dati, ma ha trasportato la tecnologia Voice over IP (VoIP) dall'inizio del 2000. La rete VoIP attualmente installata è una soluzione di toll-bypass che trasmette chiamate VoIP tra le università e i CSIRO private automatic branch exchange (PABX). Fornisce inoltre gateway PSTN (Public Switched Telephone Network) che consentono a PSTN di interrompersi nel punto più conveniente. Ad esempio, una chiamata da un telefono PABX di Melbourne a un telefono PSTN di Sydney viene effettuata come VoIP da Melbourne al gateway PSTN di Sydney. È collegato alla rete PSTN.

L'Australian Catholic University (ACU) è una delle università collegate ad AARNet. Verso la fine del 2000, ACU ha iniziato un'implementazione di telefonia IP che ha distribuito circa 2.000 telefoni IP in sei campus universitari.

Questo caso aziendale riguarda l'implementazione della telefonia IP ACU. Il progetto è completato. Tuttavia, ci sono importanti problemi architetturali da affrontare nella backbone di AARNet se la rete è scalabile quando altre università seguono le orme di ACU. Questo documento descrive questi problemi e propone e discute varie soluzioni. È probabile che l'implementazione di telefonia IP ACU venga modificata in un secondo momento per allinearsi all'architettura finale consigliata.

Nota: Deakin University è stata la prima università australiana a implementare la telefonia IP. Tuttavia, la Deakin University non utilizza ARNet per trasportare il traffico di telefonia IP.

AARNet

Le università australiane e il CSIRO hanno costruito AARNet nel 1990 attraverso l'Australian Vice-Chancellors' Committee (AVCC)'. Il 99% del traffico Internet australiano è stato diretto ai membri fondatori durante i primi anni. Una piccola quantità di traffico commerciale proveniva da organizzazioni che avevano una stretta associazione con il settore terziario e della ricerca. L'uso da parte di utenti non ARNet è aumentato fino al 20% del traffico totale entro la fine del 1994.

Nel luglio 1995 l'AVCC ha venduto a Telstra la base clienti commerciale di ARNet. Questo evento generò quello che sarebbe poi diventato Telstra BigPond. Questo ha stimolato l'ulteriore crescita dell'uso commerciale e privato di Internet in Australia. Il trasferimento della proprietà intellettuale e delle competenze ha portato allo sviluppo di Internet in Australia. Altrimenti, non sarebbe successo a un ritmo così rapido.

L'AVCC ha sviluppato ARNet2 all'inizio del 1997. È stato un ulteriore perfezionamento di Internet in Australia, che impiega collegamenti ATM ad alta larghezza di banda e servizi Internet sotto un contratto con Cable & Wireless Optus (CWO) Limited. La rapida implementazione dei servizi IP da parte di CWO per soddisfare i requisiti AARNet2 è dovuta in parte al trasferimento di conoscenze e competenze da AARNet.

ACU

ACU è un'università pubblica fondata nel 1991. L'università ha circa 10.000 studenti e 1.000 dipendenti. Ci sono sei campus sulla costa orientale dell'Australia. La tabella mostra i campus ACU e la loro ubicazione:

Campus	Città	State
Monte Santa Maria	Strathfield	Nuovo Galles del Sud (NSW)
MacKillop	North Sydney	Nuovo Galles del Sud (NSW)
Patrick	Melbourne	Victoria (VIC)
Aquino	Ballarat	Victoria (VIC)
Signadou	Canberra	Australia Capital Territory (ACT)
McAuley	Brisbane	Queensland (QLD)

ACU si è basata su una soluzione Telstra Spectrum (Centrex) prima del lancio della soluzione di telefonia IP descritta nel presente caso di studio. Il passaggio alla telefonia IP è stato dettato principalmente dal desiderio di ridurre i costi.

CSIRO

Il CSIRO ha circa 6.500 dipendenti in numerosi siti in Australia. Il CSIRO conduce ricerche in settori come l'agricoltura, i minerali, l'energia, il manifatturiero, le comunicazioni, l'edilizia, la salute e l'ambiente.

Il CSIRO è stato la prima organizzazione a utilizzare AARNet per il VoIP. L'organizzazione è stata tra le prime a lavorare in questo campo.

AARNet

La backbone AARNet è un componente importante in tutte le implementazioni di telefonia IP delle università. Fornisce l'interconnessione delle università con due servizi principali nel settore vocale:

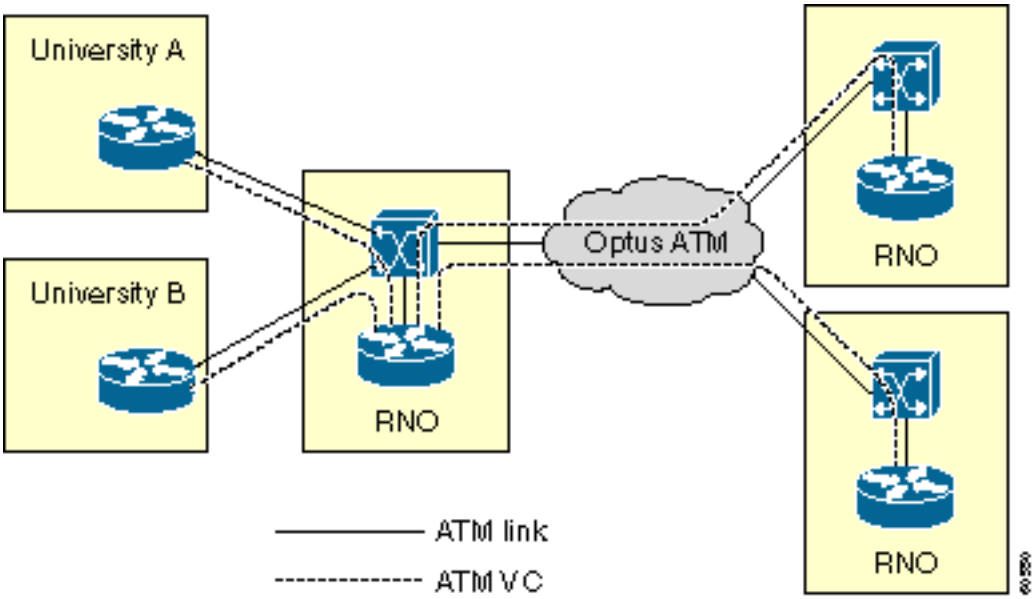
- Trasporto di pacchetti VoIP Realtime Transport Protocol (RTP) con garanzia QoS (Quality of Service) appropriata per la voce
- L'ipocrisia dei netizen locali

In questa sezione viene descritta l'architettura ARNet corrente e la relativa modalità di erogazione dei servizi. Inoltre, vengono evidenziati alcuni dei problemi di scalabilità che possono sorgere quando un maggior numero di università implementa la soluzione di telefonia IP. Infine, vengono descritte le possibili soluzioni per questi problemi di scalabilità.

Topologia ARNet

ARNet è costituito da un singolo punto di presenza (POP) in ogni stato. I POP sono definiti operazioni di rete regionali (RNO). Le università si connettono all'RNO nel loro rispettivo stato. Gli RNO sono a loro volta interconnessi da una rete completa di PVC ATM Optus. Insieme costituiscono AARNet.

L'RNO standard è composto da uno switch Cisco LS1010 ATM e da un router collegato ad ATM. Il router RNO si connette a ciascun router universitario tramite un singolo PVC ATM su un collegamento a microonde E3. Ogni router RNO ha anche una mesh completa di PVC ATM che la rete ATM Opto fornisce a tutti gli altri RNO. Il diagramma mostra la topologia AARNet generale della rete:



Esistono numerose eccezioni alla topologia. Alcuni di essi sono significativi dal punto di vista della voce. Queste sono alcune eccezioni:

- L'RNO di Victoria utilizza l'IP classico su ATM (RFC 1577) al posto dei PVC per collegare le università all'RNO.
- Le università rurali in genere si connettono all'RNO tramite Frame Relay o ISDN.
- Alcune grandi università hanno più di un collegamento con il RNO.

La tabella mostra gli stati e i territori che attualmente hanno un RNO. La tabella include le capitali per i lettori che non conoscono la geografia australiana.

State	Capitale	NO?	Connessioni al campus
Nuovo Galles del Sud	Sydney	Sì	Da definire
Victoria	Melbourne	Sì	Da definire
Queensland	Brisbane	Sì	Da definire
Australia meridionale	Adelaide	Sì	Da definire
Australia occidentale	Perth	Sì	Da definire
Territorio della capitale australiana	Canberra	Sì	Da definire
Territorio del Nord	Darwin	No	—
Tasmania	Hobart	No	—

Quality of Service (QoS)

Parti di AARNet sono già abilitate per QoS per la voce come risultato del progetto di toll-bypass VoIP. QoS è necessario per il traffico vocale al fine di fornire queste funzionalità, che riducono al minimo il ritardo e l'effetto jitter ed eliminano la perdita dei pacchetti:

- Sorveglianza: contrassegna il traffico vocale proveniente da fonti non attendibili.
- Accodamento: per ridurre al minimo il ritardo durante la congestione del collegamento, la voce deve avere la priorità su tutto il resto del traffico.
- Link Fragmentation and Interleaving (LFI): i pacchetti dati devono essere frammentati e i pacchetti voce devono essere interlacciati su collegamenti lenti.

Il traffico deve essere classificato in modo da sorvegliare e mettere in coda correttamente i pacchetti voce. In questa sezione viene descritto come eseguire la classificazione in ARNet. I capitoli successivi descrivono l'implementazione del policing e dell'accodamento.

Classificazione

Non tutto il traffico ottiene lo stesso QoS. Il traffico viene classificato in queste categorie per fornire QoS in modo selettivo:

- Dati

- Voce proveniente da fonti note e attendibili
- Voce da origini sconosciute

Ad ARNet vengono fornite funzionalità QoS di alta qualità solo ai dispositivi attendibili. Questi dispositivi sono principalmente gateway identificati da indirizzi IP. Un elenco di controllo di accesso (ACL) viene usato per identificare queste fonti vocali attendibili.

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

La precedenza IP viene utilizzata per distinguere il traffico vocale dal traffico dati. La voce ha una precedenza IP di 5.

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

Combinare gli esempi precedenti per identificare i pacchetti provenienti da una fonte attendibile.

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

Utilizzare gli stessi principi per identificare i pacchetti voce da un'origine sconosciuta.

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

Traffic policing

Il traffico vocale proveniente da una fonte non attendibile viene classificato e contrassegnato quando arriva su un'interfaccia. Questi due esempi mostrano come viene eseguito il policing a seconda del tipo di traffico che si prevede arriverà su una determinata interfaccia:

Il router cerca i pacchetti voce non attendibili e modifica la loro precedenza IP su 0 se a valle esistono origini voce attendibili.

```
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
```

Il router cerca tutti i pacchetti voce e cambia la loro precedenza IP su 0 se non ci sono origini voce conosciute a valle.

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

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

Accodamento non vocale

Tutti i servizi VoIP di AARNet sono stati toll-bypass fino a poco tempo fa. Questa condizione determina un numero relativamente basso di endpoint VoIP. La struttura corrente delle code distingue tra le interfacce che hanno dispositivi VoIP downstream e le interfacce che non ne hanno. In questa sezione viene descritto come eseguire l'accodamento su interfacce non VoIP.

Un'interfaccia non vocale è configurata per WFQ (Weighted Fair Queuing) o WRED (Weighted Random Early Detection). Questi parametri possono essere configurati direttamente sull'interfaccia. Tuttavia, il meccanismo di coda viene applicato tramite una mappa dei criteri per semplificare la modifica del meccanismo di coda su un determinato tipo di interfaccia. Esiste una mappa dei criteri per ogni tipo di interfaccia. Ciò riflette il fatto che non tutti i meccanismi di coda sono supportati su tutte le interfacce.

```
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
```

Le mappe dei criteri sono associate alle rispettive interfacce e sono specifiche dei tipi di interfaccia. Ad esempio, ciò semplifica il processo di modifica del meccanismo di accodamento sulle porte Ethernet basate su Versatile Interface Processor (basate su VIP) da WRED a WFQ. Richiede un singolo cambiamento nella mappa politica. Le modifiche vengono apportate a tutte le interfacce Ethernet basate su 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
```

Accodamento a bassa latenza

Qualsiasi interfaccia che dispone di dispositivi VoIP attendibili a valle è configurata per LLQ (Low Latency Queuing). Tutti i pacchetti che passano attraverso la classificazione dell'interfaccia in ingresso e mantengono la precedenza di 5 sono soggetti a LLQ. Tutti gli altri pacchetti sono soggetti a WFQ o WRED. Dipende dal tipo di interfaccia.

Per ciascun tipo di interfaccia vengono creati mapping dei criteri distinti per semplificare l'amministrazione del servizio QoS. Analogamente alla progettazione delle code non vocali. Per ogni tipo di interfaccia esistono tuttavia più mapping di criteri. Infatti, la capacità dei tipi di interfaccia per il trasporto del traffico vocale varia a seconda della velocità del collegamento, delle impostazioni del PVC e così via. Il numero nel nome della mappa dei criteri riflette il numero di chiamate gestite per 30, 60 e così via.

```
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
```

Le mappe politiche sono collegate alle rispettive interfacce. In questo esempio, la mappa dei criteri

è specifica di un tipo di interfaccia. Al momento non viene riservato alcun trattamento speciale alla segnalazione vocale. Le mappe delle politiche possono essere facilmente modificate in una posizione se ciò diventa un requisito in una fase successiva di un determinato tipo di interfaccia. La modifica avrà effetto su tutte le interfacce di quel tipo.

```
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
```

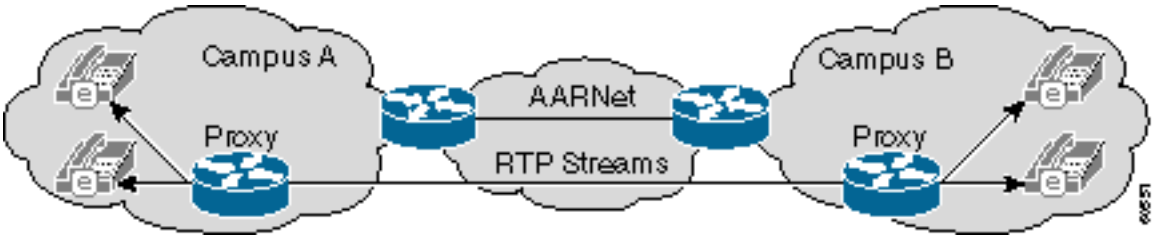
Scalabilità LLQ

Il meccanismo di accodamento presenta alcuni problemi di scalabilità. Il problema principale è che dipende dalla conoscenza dell'indirizzo IP di ogni dispositivo VoIP attendibile nella rete. Questa era una limitazione ragionevole in passato, quando c'era un numero limitato di gateway VoIP che gestivano i toll-bypass. Il numero di endpoint VoIP aumenta in modo significativo e l'implementazione della telefonia IP diventa sempre più impraticabile. Gli ACL diventano troppo lunghi e difficili da gestire.

Nel caso dell'ACU, gli ACL sono stati aggiunti per considerare attendibile il traffico proveniente da una sottorete Voice IP specifica in ciascun campus ACU. Si tratta di una soluzione provvisoria. Sono allo studio le seguenti soluzioni a lungo termine:

- Proxy H.323
- Ingress Policing QoS

L'idea principale della soluzione proxy H.323 è che tutto il traffico RTP entri in ARNet da un determinato campus tramite un proxy. ARNet rileva tutto il traffico RTP da un determinato campus con un unico indirizzo IP, come mostrato nel diagramma:

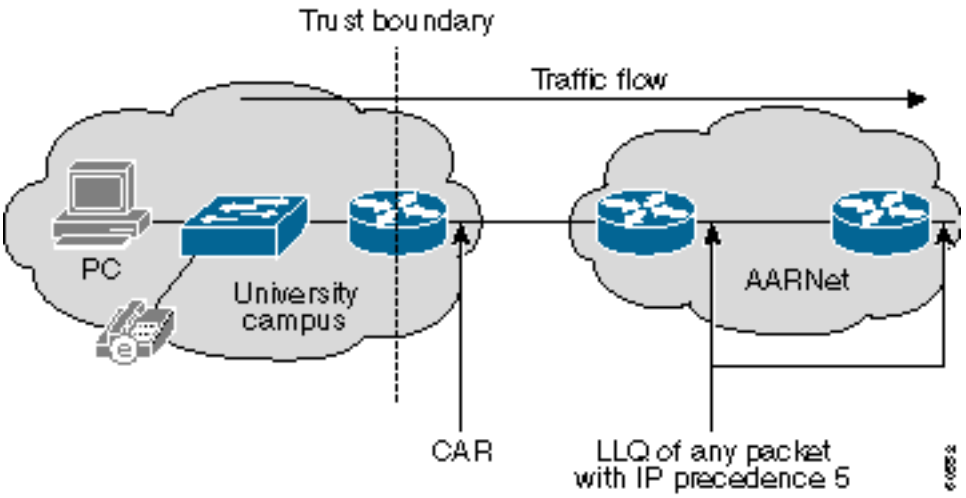


Se lo schema viene implementato in modo coerente, il numero di voci negli ACL QoS è limitato a una riga per campus. Questo progetto ha ancora il potenziale di aggiungere fino a 100 o più ingressi dato che ci sono 37 università con più campus. Anche questo non è scalabile. Potrebbe essere necessario passare a un progetto con un numero singolo o limitato di super-proxy condivisi ad ogni RNO. In questo modo il numero di indirizzi IP attendibili viene ridotto a sei. Tuttavia, questo apre un problema di sorveglianza QoS sul percorso dal campus al proxy all'RNO.

Nota: i trunk intercluster di Cisco CallManager non funzionano attualmente tramite un proxy H.323 perché la segnalazione intercluster non è un H.225 nativo.

La funzione QoS Ingress Policing è una soluzione alternativa. Un limite di trust viene stabilito nel punto in cui il campus si connette all'RNO con questo progetto. Il traffico che entra in AARNet è controllato dalla funzione Cisco IOS® Committed Access Rate (CAR) su questo limite. Un'università che utilizza AARNet per la sottoscrizione di VoIP su una determinata quantità di larghezza di banda QoS AARNet. CAR controlla quindi il traffico che entra in ARNet. Il traffico in eccesso ha la precedenza IP ridotta a 0 se la quantità di traffico RTP con la precedenza IP 5 supera la larghezza di banda sottoscritta.

Il diagramma mostra una configurazione CAR:



Nell'esempio viene mostrato come una configurazione CAR gestisce questo criterio:

```
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
```

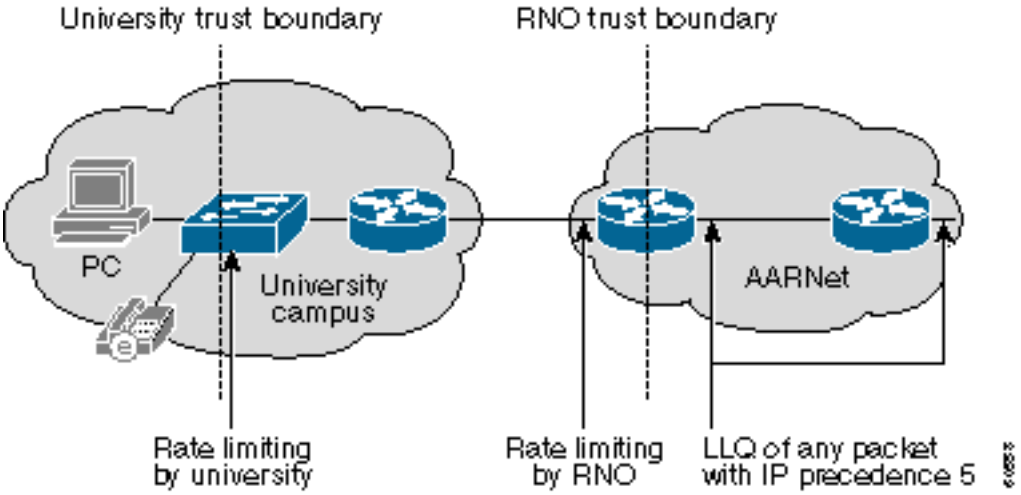
Di seguito sono riportati alcuni vantaggi di un approccio di configurazione CAR:

- Il core non deve più gestire le attività di sorveglianza. Viene ora gestito in corrispondenza del limite di trust. Pertanto, l'LLQ nel nucleo non ha bisogno di conoscere gli indirizzi IP attendibili. Qualsiasi pacchetto con una precedenza IP di 5 nel core può essere soggetto a LLQ in quanto ha già superato il controllo in entrata.
- Non vengono fatte ipotesi sull'architettura VoIP, le apparecchiature e i protocolli scelti dalle singole università. Un'università può scegliere di implementare un SIP (Session Initiation Protocol) o MGCP (Media Gateway Control Protocol) che non funziona con i proxy H.323. I pacchetti VoIP ricevono la QoS appropriata nel core, a condizione che abbiano una precedenza IP di 5.
- CAR è resistente agli attacchi QoS Denial of Service (DoS). Un attacco QoS DoS proveniente da un'università non può danneggiare il core. CAR limita l'attacco, che non può generare più traffico di quello presente quando è attivo il numero massimo di chiamate VoIP consentite.Le chiamate VoIP da e verso il campus possono subire danni durante un attacco. Spetta tuttavia alle singole università tutelarsi internamente. L'università può stringere gli ACL CAR sul router in modo che tutte le sottoreti VoIP tranne quelle selezionate abbiano la precedenza IP

contrassegnata verso il basso.Ogni campus dispone di un confine di trust interno nel punto in cui gli utenti si connettono alla LAN del campus nel progetto finale. Il traffico con precedenza IP pari a 5 ricevuto dal limite di trust è limitato a 160 kbps per porta dello switch o a due chiamate VoIP G.711. Il traffico che supera questa velocità viene contrassegnato per difetto. L'implementazione di questo schema richiede switch Catalyst 6500 o simile con funzionalità di limitazione delle velocità.

- Il provisioning della larghezza di banda nel core semplifica l'accesso di ogni università a una quantità fissa di larghezza di banda QoS. Questo rende anche la fatturazione QoS semplice perché ogni università può pagare un canone mensile fisso basato su un abbonamento QoS larghezza di banda.

Il punto debole di questo progetto è che il confine del trust si trova sul router dell'università, quindi le università devono essere in grado di amministrare correttamente CAR. Il limite del trust viene reinserito nell'RNO. Le apparecchiature amministrate da RNO gestiscono le attività di sorveglianza nel progetto finale. Per questa progettazione è necessaria una limitazione della velocità basata su hardware, ad esempio uno switch Catalyst 6000 o un processore Cisco 7200 Network Services Engine (Cisco 7200 NSE-1). Tuttavia, fornisce ad ARNet e alle RNO il controllo completo sulla sorveglianza QoS. Il diagramma mostra il seguente schema:



Frammentazione dei collegamenti e interfoliazione

Il protocollo VoIP viene trasmesso solo su circuiti virtuali ATM (VC) ad alta velocità. Pertanto, non è richiesto alcun LFI. In futuro, il VoIP potrà anche essere trasferito attraverso Frame Relay Forum (FRF) o linee affittate verso università rurali. Ciò richiede meccanismi LFI come Multilink PPP (MLP) con Interleave o FRF.12.

Gateway

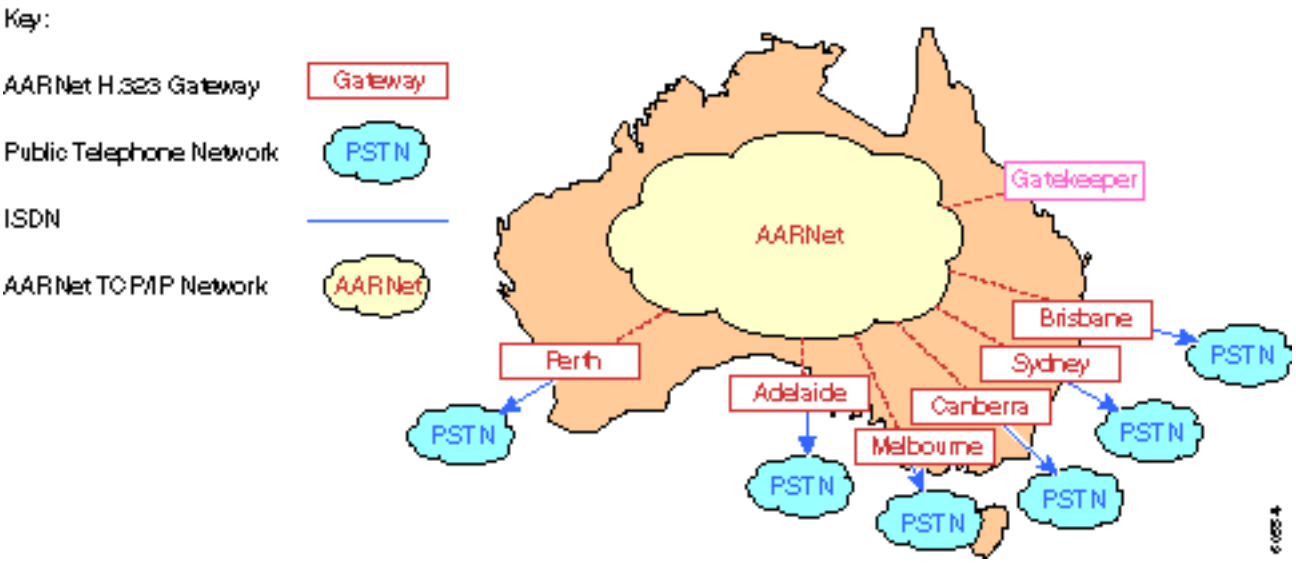
Esistono due tipi di gateway H.323 in AARNet:

- PSTN: da PSTN a gateway VoIP
- PABX: da PABX a gateway VoIP

La distinzione tra gateway PSTN e PABX è principalmente funzionale. I gateway PSTN forniscono connettività alla rete PSTN. I gateway PABX collegano un PABX universitario alla backbone VoIP. In molti casi la stessa casella fisica funge sia da PSTN che da gateway PABX. Attualmente la soluzione di telefonia IP ACU include 31 gateway. La maggior parte di questi gateway sono server Cisco AS5300 Universal Access. Gli altri gateway sono router Cisco serie 3600 o router Cisco serie 2600. Si prevede che nel secondo trimestre del 2001 verranno aggiunti almeno dieci

gateway. Nell'aprile 2001 AARNet ha effettuato circa 145.000 chiamate VoIP.

ARNet ha implementato gateway H.323 con connessione PSTN nella maggior parte delle principali città, come mostrato nel diagramma:



Le università possono utilizzare questi gateway per effettuare chiamate in uscita verso la rete PSTN. Le università devono mantenere i propri trunk per le chiamate in entrata perché non sono attualmente supportate. ARNet può negoziare un prezzo molto competitivo con il vettore a causa del volume di chiamate che passano attraverso questi gateway. Le chiamate possono anche essere interrotte nel punto più conveniente. Ad esempio, una persona di Sydney che chiama un numero Perth può utilizzare il gateway Perth e pagare solo per una chiamata locale. Questo processo è noto anche come TEHO (Tail End Hop Off).

Viene implementato un singolo gatekeeper per eseguire E.164 per la risoluzione degli indirizzi IP. Tutte le chiamate alla PSTN vengono inviate al gatekeeper, che restituisce quindi l'indirizzo IP del gateway più appropriato. Fare riferimento alle sezioni Dial Plans e Gatekeeper per informazioni più dettagliate sui gatekeeper.

Fatturazione e contabilità

I gateway PSTN utilizzano RADIUS e autenticazione, autorizzazione e accounting (AAA) a scopo di fatturazione. Ogni chiamata eseguita tramite un gateway genera un record CDR (Call Detail Record) per ogni tappa. Questi CDR vengono inviati al server RADIUS. L'indirizzo IP di Cisco CallManager nel CDR identifica in modo univoco l'università e garantisce che venga fatturata la parte corretta.

Sicurezza gateway

La protezione dei gateway PSTN dagli attacchi DoS e dalle frodi è una delle principali preoccupazioni. i client H.323 sono ampiamente disponibili. Microsoft NetMeeting viene fornito con Microsoft Windows 2000, quindi è relativamente semplice per un utente senza una specifica preparazione tecnica effettuare chiamate gratuite attraverso questi gateway. Configurare un ACL in entrata che consenta la segnalazione H.225 da indirizzi IP attendibili per proteggere i gateway. Questo approccio presenta gli stessi problemi di scalabilità descritti nella sezione QoS. Il numero di voci nell'ACL aumenta con l'aumentare del numero di endpoint H.323 attendibili.

I proxy H.323 sono particolarmente rilevanti in questo contesto. Gli ACL del gateway devono

autorizzare un indirizzo IP per campus universitario se tutte le chiamate attraverso il gateway PSTN passano attraverso un proxy del campus. Nella maggior parte dei casi è consigliabile utilizzare due indirizzi IP come proxy ridondante. Anche con i proxy, l'ACL può contenere più di 100 voci.

Il proxy deve essere protetto tramite ACL poiché qualunque H.323 può impostare una chiamata attraverso il proxy. L'ACL proxy deve consentire l'uso di dispositivi H.323 locali come richiesto dalle policy locali, in quanto questa operazione viene effettuata per singolo campus.

Se un campus desidera consentire l'uso dei gateway PSTN solo per le chiamate da telefoni IP, gli indirizzi IP dei due Cisco CallManager devono essere inclusi negli ACL del gateway. I proxy non aggiungono alcun valore in questa situazione. Il numero di voci ACL richieste è duplice.

Si noti che le chiamate IP da telefono a IP tra campus non devono passare attraverso il proxy.

Piani di composizione

Il dial plan VoIP corrente è semplice. Gli utenti possono effettuare questi due tipi di chiamate dalla prospettiva di un gateway VoIP:

- Chiama un telefono in un altro campus ma nella stessa università.
- Chiama un telefono PSTN o un telefono in un'altra università.

I peer di composizione del gateway riflettono il fatto che esistono solo due tipi di chiamate. Fondamentalmente esistono due tipi di peer di connessione VoIP, come mostrato nell'esempio:

```
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
```

Il primo peer di composizione viene utilizzato se qualcuno chiama l'estensione 7... in un altro campus in questo esempio. Questa chiamata viene indirizzata direttamente all'indirizzo IP del gateway remoto. Poiché il gatekeeper viene ignorato, il controllo di ammissione di chiamata (CAC) non viene eseguito.

Il secondo peer di composizione viene utilizzato quando la chiamata è per un numero PSTN. Può essere uno dei seguenti elementi:

- Numero di un telefono nella rete PSTN
- Numero PSTN completo di un telefono in un'altra università

La chiamata viene inviata al gatekeeper tramite un messaggio di richiesta di ammissione (ARQ) nel primo caso. Il gatekeeper restituisce l'indirizzo IP del miglior gateway PSTN in un messaggio di conferma dell'ammissione (ACF).

La chiamata viene inoltre inviata al gatekeeper tramite un messaggio ARQ nel secondo caso. Tuttavia, il gatekeeper restituisce un messaggio ACF con l'indirizzo IP del gateway VoIP dell'università che riceve la chiamata.

Gatekeeper

AARNet gestisce attualmente un solo gatekeeper. L'unico scopo di questo gatekeeper è eseguire il routing delle chiamate sotto forma di E.164 alla risoluzione degli indirizzi IP. Il gatekeeper non esegue CAC. Il numero di trunk PABX connessi ai gateway limita il numero di chiamate simultanee. La larghezza di banda centrale è adatta a tutti i trunk in uso contemporaneamente. Questo cambia con il lancio della telefonia IP presso ACU e altre università. Non esiste un limite naturale al numero di chiamate VoIP simultanee che possono essere inviate o ricevute da un determinato campus in questo nuovo ambiente. La larghezza di banda QoS disponibile può essere sovrascritta se vengono avviate troppe chiamate. Tutte le chiamate possono soffrire di scarsa qualità in questa condizione. Usare il gatekeeper per fornire CAC.

La natura distribuita e le dimensioni potenziali della rete vocale dell'università si prestano a un'architettura distribuita di gatekeeper. Una possibile soluzione è avere un gatekeeper gerarchico a due livelli in cui ogni università mantiene il proprio gatekeeper. Questo gatekeeper universitario è denominato gatekeeper di livello 2. ARNet gestisce un gatekeeper di *directory* denominato gatekeeper di livello 1.

Le università devono utilizzare questo approccio a due livelli per utilizzare un gatekeeper per il routing delle chiamate tra cluster Cisco CallManager. In questo scenario, il gatekeeper instrada le chiamate in base a un'estensione di 4 o 5 cifre. Ogni università ha bisogno del proprio gatekeeper. Questo accade perché gli intervalli di estensione si sovrappongono tra le università poiché si tratta di uno spazio di indirizzi amministrato localmente.

I gatekeeper di livello 2 dell'università eseguono CAC solo per le chiamate da e verso tale università. Esegue anche la risoluzione E.164 per chiamate tra solo i campus di quella università. La chiamata viene instradata dal gatekeeper di livello 2 al gatekeeper di livello 1 tramite un messaggio LRQ (Location Request) se qualcuno chiama un telefono IP di un'altra università o chiama la PSTN tramite un gateway AARNet. L'LRQ viene inoltrato al gatekeeper di livello 2 di quell'università se la chiamata è per un'altra università. Questo gatekeeper restituisce quindi un messaggio ACF al gatekeeper di livello 2 dell'università da cui ha origine la chiamata. Entrambi i gatekeeper di livello 2 eseguono CAC. Continuano con la chiamata solo se è disponibile una larghezza di banda sufficiente sia nella zona chiamante che in quella chiamata.

ARNet può scegliere di trattare i gateway PSTN di ARNet come quelli di qualsiasi università. Il loro gatekeeper di livello 2 si prende cura di loro. Il gatekeeper di livello 1 può anche fungere da gatekeeper di livello 2 per questi gateway se il carico e le prestazioni lo consentono.

Ciascun gatekeeper (incluso il gatekeeper della directory AARNet) deve essere replicato perché i gateway sono componenti così critici. Ogni università deve avere due guardiani. I gateway Cisco IOS possono avere gatekeeper alternativi, come nel caso del software Cisco IOS versione 12.0(7)T. Tuttavia, al momento non è supportato da Cisco CallManager o da altri dispositivi H.323 di terze parti. Non utilizzare questa funzionalità in questo momento. In alternativa, è possibile utilizzare una semplice soluzione basata su HSRP (Hot Standby Router Protocol). Ciò richiede che entrambi i gatekeeper si trovino sulla stessa sottorete IP. HSRP determina il gatekeeper attivo.

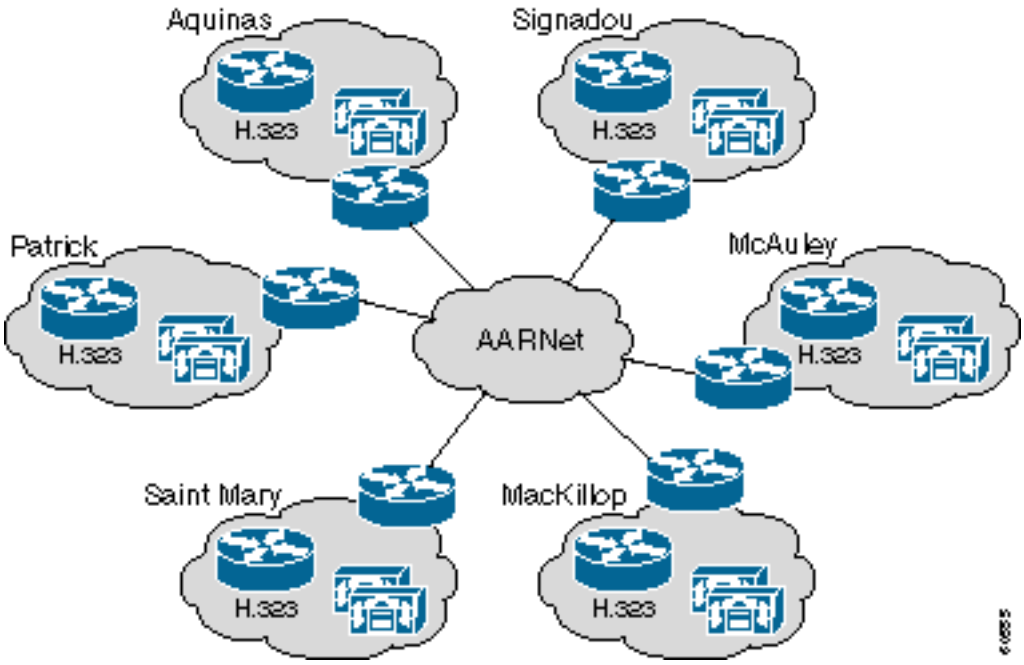
ACU IP Telephony Network

La tabella mostra il numero approssimativo di telefoni IP installati nei campus di ACU:

Campus	Città	Approssimativamente telefoni IP

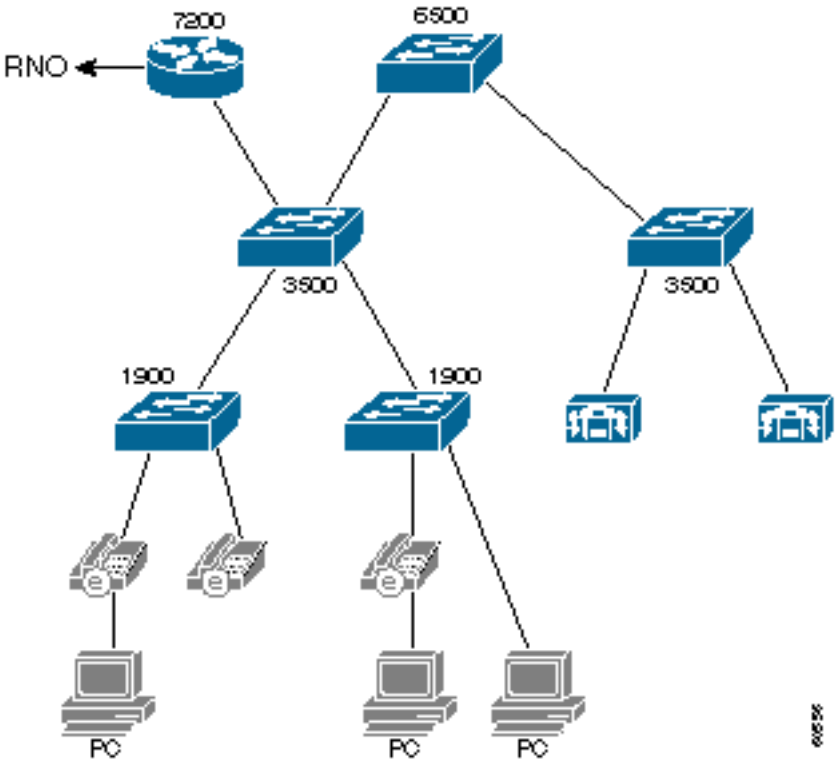
Monte Santa Maria	Strathfield	400
MacKillop	North Sydney	300
Patrick	Melbourne	400
Aquino	Ballarat	100
Signadou	Canberra	100
McAuley	Brisbane	400
	Totale:	*1700*

ACU ha recentemente implementato una soluzione di telefonia IP. La soluzione consiste in un cluster di due Cisco CallManager, un gateway Cisco 3640 in ogni campus e telefoni IP. ARNet interconnette i campus. Il diagramma mostra la topologia di alto livello e i vari componenti della rete di telefonia IP ACU:



Topologia di rete ACU

Il diagramma mostra un tipico campus ACU. Ogni campus è dotato di tre livelli di switch Catalyst. L'armadio dei cavi ospita i vecchi switch Catalyst 1900. Gli switch Catalyst 1900 si connettono nuovamente allo switch Catalyst 3500XL tramite il frame esteso. Questi switch possono essere collegati a un singolo switch Catalyst 6509 tramite Gigabit Ethernet (GE). Un singolo router Cisco 7200 VXR connette il campus ad ARNet da un VC ATM all'RNO locale.



Il metodo di connettività all'RNO varia leggermente da stato a stato, come illustrato nella tabella seguente. Victoria è basata su Classical IP over ATM (RFC 1577). Gli altri RNO sono dotati di una configurazione semplice del PVC con incapsulamento RFC 1483. Open Shortest Path First (OSPF) è il protocollo di routing utilizzato tra ACU e RNO.

Campus	State	Connettività a RNO	Protocollo di routing
Monte Santa Maria	NSW	RFC 1483 - PVC	OSPF
MacKillop	NSW	RFC 1483 - PVC	OSPF
Patrick	VIC	RFC 1577 - IP classico su ATM	OSPF
Aquino	VIC	RFC 1577 - IP classico su ATM	OSPF
Signadou	ACT	RFC 1483 - PVC	OSPF
McAuley	QLD	RFC 1483 - PVC	OSPF

Gli switch Catalyst serie 1900 supportano il trunking solo sugli uplink. Pertanto, i telefoni IP e i PC si trovano tutti in una grande VLAN. Infatti, l'intero campus è una grande VLAN e dominio di broadcast. Le sottoreti IP secondarie vengono utilizzate a causa del numero elevato di dispositivi. I telefoni IP si trovano su una sottorete IP, i PC su un'altra. Il core AARNet considera attendibile la sottorete telefonica IP e il traffico da e verso questa sottorete IP è soggetto a LLQ.

Il router Cisco 7200 collega le sottoreti IP primaria e secondaria. Il modulo Multilayer Switch Feature Card (MSFC) nello switch Catalyst 6500 non è attualmente in uso.

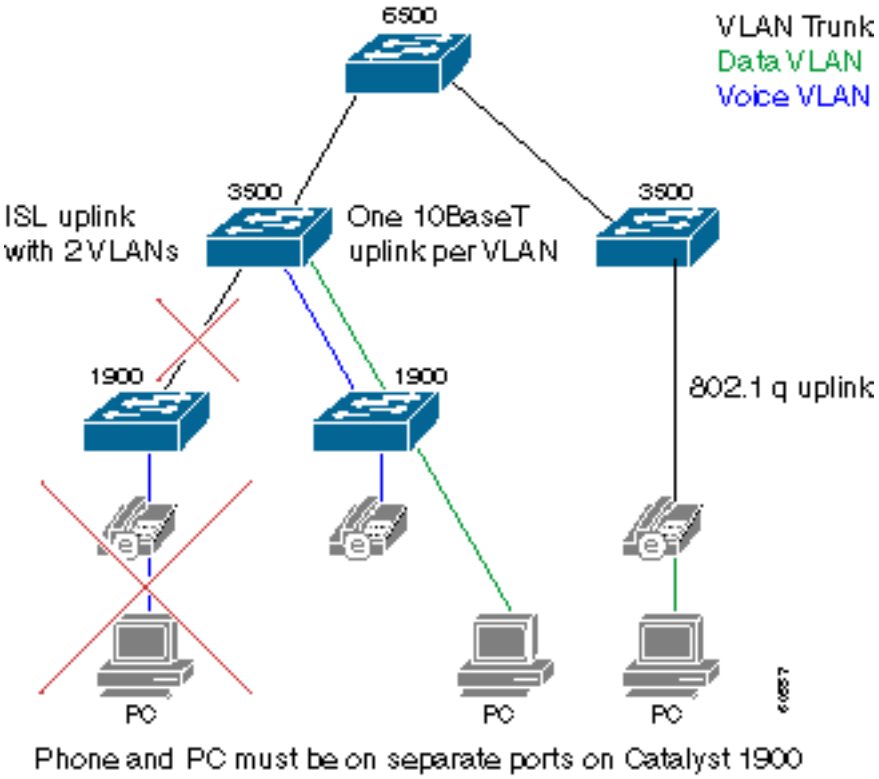
Gli switch Catalyst 3500XL e Catalyst 6500 hanno funzionalità QoS, ma non sono attualmente abilitati.

QoS nel campus

La struttura del campus corrente non è conforme alle linee guida di progettazione consigliate da Cisco per la telefonia IP. Queste sono alcune delle preoccupazioni relative alla QoS:

- Il dominio di trasmissione è molto grande. Trasmissioni eccessive possono compromettere le prestazioni dei telefoni IP, che devono quindi elaborarli.
- Gli switch Catalyst 1900 non supportano QoS. Se un telefono IP e un PC sono collegati alla stessa porta dello switch, i pacchetti voce possono essere scartati se il PC riceve i dati ad alta velocità.

Riprogettare parti dell'infrastruttura del campus per ottenere miglioramenti significativi. Non è necessario un aggiornamento hardware. In questo diagramma vengono illustrati i principi alla base della riprogettazione consigliata:



Il campus deve essere suddiviso in una VLAN voce e in una VLAN dati. I telefoni e i PC che si connettono a uno switch Catalyst 1900 devono ora connettersi a porte diverse per ottenere la separazione della VLAN. Viene aggiunto un uplink aggiuntivo da ciascuno switch Catalyst 1900 allo switch Cisco 3500XL. Uno dei due uplink è un membro della VLAN vocale. L'altro uplink è membro della VLAN dati. Non utilizzare il trunking ISL (InterSwitch Link) in alternativa a due uplink. In questo modo, il traffico voce e dati non viene fornito con code separate. Anche i collegamenti GE tra lo switch Catalyst 3500XL e lo switch Catalyst 6000 devono essere convertiti in trunk 802.1q in modo che sia la VLAN voce che la VLAN dati possano essere trasmesse sullo switch core.

Le porte dello switch Catalyst 3500XL nella VLAN dati hanno un valore predefinito CoS (Class of Service) pari a zero. Le porte che sono membri della VLAN voce hanno un CoS predefinito di 5. Di conseguenza, al traffico vocale viene assegnata correttamente la priorità quando arriva al core Catalyst 3500 o Catalyst 6500. Le configurazioni delle porte dello switch Catalyst 3500 QoS variano leggermente a seconda della porta dello switch VLAN di cui fanno parte, come mostrato nell'esempio:

```
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
```

Èpossibile collegare un PC alla porta posteriore dello switch sul telefono IP nel raro caso in cui i telefoni IP si connettano direttamente a uno switch Catalyst 3500XL. In questo caso, i telefoni IP si connettono allo switch tramite un trunk 802.1q. In questo modo, i pacchetti voce e dati possono viaggiare su VLAN separate ed è possibile fornire ai pacchetti il CoS corretto in entrata. Sostituire gli switch Catalyst 1900 con gli switch Catalyst 3500XL o con altri switch con funzionalità QoS quando raggiungono la fine del ciclo di vita. Questa topologia diventa quindi il metodo standard per la connessione di telefoni IP e PC alla rete. In questo scenario viene mostrata la configurazione QoS dello switch Catalyst 3500XL:

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

Infine, le due porte che si connettono ai due Cisco CallManager devono avere il codice hardcoded CoS su 3. Cisco CallManager imposta la precedenza IP su 3 in tutti i pacchetti di segnalazione vocale. Tuttavia, il collegamento tra Cisco CallManager e lo switch Catalyst 3500XL non utilizza 801.1p. Di conseguenza, il valore CoS viene forzato sullo switch come mostrato nell'esempio:

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

L'ostacolo principale con questo design è che sul desktop sono necessarie due porte dello switch. Il campus di Patrick potrebbe richiedere 400 porte aggiuntive per gli switch con 400 telefoni IP. Se non sono disponibili porte sufficienti, è necessario implementare altri switch Catalyst 3500XL. Per ogni due porte dello switch Catalyst 1900 mancanti, è richiesta solo una porta dello switch Catalyst 3500XL.

Gli switch ACU Catalyst 6500 attuali dispongono di funzionalità QoS, ma non sono attualmente abilitati. Questi moduli sono presenti nello switch ACU Catalyst 6000 con le seguenti funzionalità di accodamento:

Slot	Modulo	Porte	Code RX	Code 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	—	—

Completare questi passaggi per attivare le funzionalità QoS appropriate sullo switch Catalyst 6000:

1. Indicare allo switch di fornire la funzionalità QoS per VLAN con questo comando:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 vlan-based
   ```

2. Indicare allo switch di considerare attendibili i valori CoS ricevuti dallo switch Catalyst 3500XL con questo comando:
   ```
   Cat6K>(enable)set port qos 1/1-2,3/1-8,4/1-8 trust trust-cos
   ```

Èora necessario impostare il CoS sul mapping del punto di codice dei servizi differenziati (DSCP). Questa operazione è necessaria perché lo switch Catalyst 6000 riscrive il valore DSCP nell'intestazione IP in base al valore CoS ricevuto. I pacchetti di segnalazione VoIP devono avere un CoS di 3, riscritto con un DSCP di AF31 (26). I pacchetti RTP devono avere un CoS di 5, riscritto con un DSCP di EF (46). Immettere questo comando

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

Utilizzare questo esempio per verificare il mapping da CoS a 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
```

Configurare l'MSFC per il routing tra le diverse sottoreti IP.

QoS nell'RNO

Il progetto RNO corrente non è conforme alle linee guida di progettazione consigliate da Cisco per la telefonia IP. Queste preoccupazioni sussistono in relazione alla QoS:

- LLQ non è applicato sui router WAN Cisco ACU serie 7200.
- I campus Patrick e Aquinas si connettono alla RNO per mezzo di bancomat (SVC). LLQ non è supportato sugli SVC.

Un router Cisco 7200 Fast Ethernet collega il campus a una RNO tramite un collegamento E4 ATM a 34 Mbps. Il traffico può potenzialmente mettere in coda il traffico in uscita sui collegamenti a 34 m a causa della mancata corrispondenza della velocità di 4 m rispetto a 100 m. È quindi necessario assegnare la priorità al traffico vocale. Utilizzare LLQ. La configurazione del router Cisco 7200 è simile a questo esempio:

```
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 larghezza di banda assegnata a LLQ deve essere *N x 24 Kbps*, dove N è il numero di chiamate G.729 simultanee.

Configurare un PVC da ciascuno dei router Patrick e Aquinas Cisco 7200 al router Aironet. Gli SVC ATM nel Victoria RNO non supportano LLQ, in quanto è basato su Classical IP over ATM (RFC 1577). Le altre università della Victoria RNO possono continuare ad utilizzare per ora la RFC 1577. Tuttavia, alla fine sostituirà l'infrastruttura IP classica su ATM.

Gateway

Ogni campus ACU è dotato di un router Cisco 3640 che funge da gateway H.323. Questi gateway si connettono alla PSTN tramite ISDN. Il numero di PRI (Primary Rate Interfaces) e di B-channel dipende dalle dimensioni del campus. In questa tabella viene elencato il numero di PRI e di B-channel per ogni campus:

Campus	Quantità PRI	Quantità del canale B
Monte Santa Maria	2	30
MacKillop	2	50
Patrick	2	50
Aquino	1	20
Signadou	1	20
McAuley	1	30

Questi gateway vengono utilizzati solo come gateway secondari per DOD (Direct Outward Dialing). I gateway AARNet sono i gateway principali. I gateway ACU vengono sempre utilizzati per DID (Direct Inward Dialing).

Piano di composizione

Il dial plan è basato su numeri di estensione di 4 cifre. L'estensione è anche le ultime quattro cifre del numero DID. Nella tabella seguente vengono elencati gli intervalli di estensione e i numeri DID per ogni campus:

Campus	Interno	DID
Monte Santa Maria	9xxx	02 9764 9xxx
MacKillop	8xxx	02 9463 8xxx
Patrick	3xxx	03 8413 3xxx
Aquino	5xxx	03 5330 5xxx
Signadou	2xxx	02 6123 2xxx
McAuley	7xxx	07 3354 7xxx

Una semplice voce `num-exp` sui gateway tronca il numero DID all'estensione di 4 cifre prima di passarlo a Cisco CallManager. Ad esempio, il gateway di Patrick campus contiene la seguente voce:

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

Gli utenti compongono zero per selezionare una linea esterna. Lo zero iniziale viene passato al gateway. Un singolo dial peer POTS instrada la chiamata verso la porta ISDN in base allo zero iniziale.

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

Le chiamate in arrivo utilizzano questa voce num-exp per trasformare il numero della parte chiamata in un'estensione di 4 cifre. La chiamata quindi corrisponde a entrambi i peer della connessione VoIP. In base alla preferenza inferiore, preferisce questa route al destinatario predefinito 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

Ogni campus dispone di un cluster costituito da due server Cisco CallManager. I server Cisco CallManager sono una combinazione di Media Convergence Server 7835 (MCS-7835) e Media Convergence Server 7820 (MCS-7820). Entrambi i server eseguivano la versione 3.0(10) al momento della pubblicazione. Un Cisco CallManager è l'*editore* e l'altro Cisco CallManager è il *sottoscrittore*. Il sottoscrittore agisce come Cisco CallManager primario per tutti i telefoni IP. In questa tabella sono elencati i componenti hardware distribuiti in ogni campus:

Campus	Piattaforma	CallManager
Monte Santa Maria	MCS-7835	2
MacKillop	MCS-7835	2
Patrick	MCS-7835	2
Aquino	MCS-7820	2
Signadou	MCS-7820	2
McAuley	MCS-7835	2

Ogni cluster è configurato con due aree:

- Uno per chiamate intracampus (G.711)
- Uno per le chiamate intercampus (G.729)

Il CAC basato sulla posizione non è appropriato per ACU perché tutti i telefoni IP forniti da ciascun cluster si trovano in un singolo campus. Un CAC basato su gatekeeper può essere utile per le chiamate intercampus, ma attualmente non è implementato. Tuttavia, si prevede di farlo nel prossimo futuro.

Ogni Cisco CallManager è configurato con 22 gateway H.323. È composto da trunk intercluster verso gli altri cinque cluster Cisco CallManager, sei gateway AARNet PSTN e un gateway ACU in ogni campus.

Tipo di dispositivo H.323	Quantità
Intercampus CallManager	2 x 5 = 10
Gateway ARNet PSTN	6
ACU PSTN Gateway	6
Totale:	*22*

Gli elenchi e i gruppi di route vengono utilizzati per classificare i gateway PSTN. In questa tabella viene ad esempio illustrato come le chiamate dal CallManager Patrick Cisco di Melbourne alla rete PSTN di Sydney possono utilizzare i quattro gateway per collegare le chiamate con un gruppo di route.

Gateway	Priority
ARNet Sydney	1
ACU Sydney	2
ARNet Melbourne	3
ACU Melbourne	4

I CallManager Cisco sono configurati con circa 30 modelli di route, come mostrato nella tabella seguente. I modelli di route sono progettati in modo che ci siano corrispondenze specifiche per tutti i numeri nazionali australiani. In questo modo, gli utenti non devono attendere la scadenza del timeout internumerico prima che Cisco CallManager avvii la chiamata. Carattere jolly "!" viene utilizzato solo nel modello di route per i numeri internazionali. Gli utenti devono attendere la scadenza del timeout di intercifra (impostazione predefinita 10 secondi) prima che la chiamata progredisca quando compongono una destinazione internazionale. Gli utenti possono anche aggiungere il modello di percorso "0.0011!#". Gli utenti possono quindi immettere un "#" dopo l'ultima cifra per indicare a Cisco CallManager che il numero composto è completo. Questa azione accelera la composizione internazionale.

Pattern route	Descrizione
0.[2-9]XXXXXXX	Chiamata locale
0.00	Chiamata di emergenza - se l'utente dimentica di comporre 0 per la linea esterna
0.000	Chiamata di emergenza
0.013	Assistenza directory
0.1223	—
0.0011!	Chiamate internazionali
0,02XXXXXXX	Chiamate al Nuovo Galles del Sud
0,03XXXXXXX	Chiamate a Victoria

0,04XXXXXXXX	Chiamate a telefoni cellulari
0,07XXXXXXXX	Chiamate al Queensland
0,086XXXXX	Chiamate all'Australia Occidentale
0,08XXXXXXXX	Chiamate per l'Australia Meridionale e il Territorio del Nord
0.1[8-9]XXXXXXXX	Chiamate ai numeri 1800 xxx xxx e 1900 xxx xxx
0,1144X	Emergenza
0.119[4-6]	Ora e tempo
0,1245X	Directory
0.13[1-9]XXX	Chiamate ai numeri 13xxxx
0.130XXXXX	Chiamate ai numeri 1300 xxx xxx
2[0-1]XX	Chiamate intercluster a Signadou
3[0-4]XX	Chiamate intercluster a Patrick
5[3-4]XX	Chiamate intercluster ad Aquinas
7[2-5]XX	Chiamate intercluster a McAuley
8[0-3]XX	Chiamate intercluster a MacKillop
9[3-4]XX	Chiamate intercluster al Monte Santa Maria
9[6-7]XX	Chiamate intercluster al Monte Santa Maria

Il numero di gateway, gruppi di route, elenchi di route e modelli di route configurati sui Cisco CallManager ACU può aumentare fino a raggiungere un numero elevato. Se viene implementato un nuovo gateway RNO, tutti e cinque i cluster Cisco CallManager devono essere riconfigurati con un gateway aggiuntivo. Ancora peggio, se i CallManager ACU Cisco instradano le chiamate VoIP direttamente a tutte le altre università e aggirano completamente la PSTN, è necessario aggiungere centinaia di gateway. È evidente che le proporzioni non sono molto buone.

La soluzione è rendere i Cisco CallManager gatekeeper controllati. È necessario aggiornare il gatekeeper solo quando si aggiunge un nuovo gateway o Cisco CallManager in un punto qualsiasi di AARNet. In ogni Cisco CallManager deve essere configurato solo il gateway del campus locale e il dispositivo anonimo. Questo dispositivo può essere considerato come un trunk point-to-multipoint. Elimina la necessità dei trunk PPP a rete nel modello di dial plan di Cisco CallManager. Un singolo gruppo di route punta al dispositivo anonimo come gateway preferito e al gateway locale come gateway di backup. Il gateway PSTN locale viene utilizzato per determinate chiamate locali e anche per chiamate fuori rete generali se il gatekeeper non è disponibile. Al momento, il dispositivo anonimo può essere intercluster o H.225, ma non entrambi contemporaneamente.

Cisco CallManager richiede un numero di modelli di percorso con gatekeeper inferiore a quello attuale. In linea di principio, Cisco CallManager richiede un solo modello di percorso di "!" puntando verso il gatekeeper. In realtà, il modo in cui le chiamate vengono instradate deve essere più specifico per i seguenti motivi:

- Alcune chiamate (come le chiamate al numero 1-800 o i numeri di emergenza) devono essere instradate attraverso un gateway geograficamente locale. Qualcuno a Melbourne che chiama la polizia o una catena di ristoranti come Pizza Hut non vuole essere collegato alla polizia o al Pizza Hut di Perth. Per questi numeri sono necessari i modelli di percorso specifici che

puntano direttamente al gateway PSTN del campus locale.Le università che prevedono di implementare la telefonia IP in futuro possono scegliere di affidarsi esclusivamente ai gateway AARNet e di non amministrare i propri gateway locali. Prima di inviare questi numeri al gatekeeper, Cisco CallManager deve anteporre un indicativo di località virtuale in modo da consentire il corretto funzionamento di questa struttura per le chiamate che devono essere interrotte localmente. Ad esempio, Cisco CallManager può anteporre 003 alle chiamate da un telefono di Melbourne al numero 1-800 del Pizza Hut. Questo consente al gatekeeper di indirizzare la chiamata a un gateway Aironet di Melbourne. Il gateway rimuove lo 003 iniziale prima di inserire la chiamata nella PSTN.

- Usare modelli di route con corrispondenze specifiche per tutti i numeri nazionali per evitare che l'utente aspetti il timeout tra cifre prima di iniziare la chiamata.

Nella tabella seguente vengono riportati i modelli di percorso di un Cisco CallManager controllato da gatekeeper:

Pattern route	Descrizione	Percorso	Gatekeeper
0.[2-9]XXXXXXX	Chiamata locale	Elenco route	AARNet
0.00	Chiamata di emergenza	Gateway locale	Nessuna
0.000	Chiamata di emergenza	Gateway locale	Nessuna
0.013	Assistenza directory	Gateway locale	Nessuna
0.1223	—	Gateway locale	Nessuna
0.0011!	Chiamate internazionali	Elenco route	AARNet
0,0011!#	Chiamate internazionali	Elenco route	AARNet
0.0[2-4]XXXXXXX	Chiamate a New South Wales, Victoria e telefoni cellulari	Elenco route	AARNet
0.0[7-8]XXXXXXX	Chiamate per Australia meridionale, Australia occidentale e Territorio del Nord	Elenco route	AARNet
0.1[8-9]XXXXXXX	Chiamate ai numeri 1800 xxx xxx e 1900 xxx xxx	Gateway locale	Nessuna
0,1144X	Emergenza	Gateway locale	Nessuna
0.119[4-6]	Ora e tempo	Gatew	Nessuna

		ay locale	
0.13[1-9]XXX	Chiamate ai numeri 13xxxx	Gateway locale	Nessuna
0.130XXXXX	Chiamate ai numeri 1300 xxx xxx	Gateway locale	Nessuna
[2-3]XXX	Chiamate a Signadou	Elenco route	ACU
5XXX	Chiamate ad Aquino	Elenco route	ACU
[7-9]XXX	Chiamate a McAuley, MacKillop e Mount Saint Mary	Elenco route	ACU

Il gatekeeper instrada le chiamate internazionali, che non vengono inviate attraverso il gateway locale. Questo è significativo perché ARNet può implementare gateway internazionali in futuro. Se negli Stati Uniti viene implementato un gateway, una semplice modifica alla configurazione del gatekeeper consente alle università di effettuare chiamate verso gli Stati Uniti alle tariffe nazionali degli Stati Uniti.

Il gatekeeper esegue il routing delle chiamate tra cluster in base all'estensione ACU a 4 cifre. Questo spazio di indirizzamento molto probabilmente si sovrappone ad altre università. Questo impone all'ACU di amministrare il proprio gatekeeper e di usare il gatekeeper AARNet come *gatekeeper delle directory*. La colonna gatekeeper in questa tabella indica se il routing delle chiamate viene eseguito dal gatekeeper ACU o dal gatekeeper AARNet.

Nota: l'unico problema della soluzione gatekeeper proposta è che il dispositivo anonimo può essere attualmente intercluster o H.225, ma non entrambi contemporaneamente. Con la progettazione proposta, Cisco CallManager si affida al gatekeeper per indirizzare le chiamate a entrambi i gateway (H.225) e ad altri Cisco CallManager (intercluster). Per risolvere questo problema, non utilizzare il gatekeeper per il routing tra cluster o gestire tutte le chiamate tramite il gatekeeper come H.225. In questo modo, alcune funzionalità supplementari potrebbero non essere disponibili nelle chiamate tra cluster.

Casella vocale

ACU disponeva di tre server di posta vocale basati su Active Voice Repartee OS/2 con schede telefoniche Dialogic prima della migrazione alla telefonia IP. Si prevede di riutilizzare questi server nell'ambiente di telefonia IP. Quando implementato, ogni server Repartee si connette a un Cisco CallManager tramite un'interfaccia SMDI (Message Desk Interface) semplificata e una scheda Catalyst 6000 FXS (Foreign Exchange Station) a 24 porte. Questo fornisce la segreteria telefonica per tre dei sei campus, lasciando tre campus senza segreteria telefonica. Non è possibile condividere correttamente un server Repartee tra utenti su due cluster Cisco CallManager perché non è possibile propagare l'indicatore MWI (Message Wait Indicator) sul trunk H.323 dell'intercluster.

ACU potrebbe acquistare tre server Cisco Unity per i campus rimanenti. Questi server sono basati su Skinny, quindi non sono necessari gateway. In questa tabella sono elencate le soluzioni di posta vocale nel caso in cui ACU acquisti i server di posta vocale aggiuntivi:

Campus	Sistema di posta vocale	Gateway
Monte Santa Maria	Active Voice Repartee	Catalyst 6000 FXS a 24 porte
MacKillop	Active Voice Repartee	Catalyst 6000 FXS a 24 porte
Patrick	Active Voice Repartee	Catalyst 6000 FXS a 24 porte
Aquino	Cisco Unity	—
Signadou	Cisco Unity	—
McAuley	Cisco Unity	—

In questo piano, i sei server di posta vocale funzionano come isole di posta vocale isolate. Nessuna rete di posta vocale.

Risorse multimediali

I DSP (Digital Signal Processor) hardware non sono attualmente installati presso ACU. Le conferenze utilizzano il Conference Bridge basato su software su Cisco CallManager. La conferenza tra cluster non è attualmente supportata.

La trascodifica non è attualmente richiesta. Vengono utilizzati solo i decoder G.711 e G.729, supportati da tutti i dispositivi terminali installati.

Supporto fax e modem

Il traffico fax e modem non è attualmente supportato dalla rete di telefonia IP ACU. A tale scopo, l'università intende utilizzare la scheda FXS Catalyst 6000 a 24 porte.

Versioni software

Nella tabella seguente vengono elencate le versioni software di ACU utilizzate al momento della pubblicazione:

Piattaforma	Funzione	Versione del software
CallManager	IP-PBX	3.0(10)
Catalyst 3500XL	Switch di distribuzione	12.0(5.1)XP
Catalyst 6500	Switch core	5.5(5)
Catalyst 1900	Interruttore armadio cavi	—
Processore Cisco 7200	router WAN	12.1(4)
Cisco 3640 router	H.323 gateway	12.1(3a)XI6

Informazioni correlate

- Supporto alla tecnologia vocale
- Supporto dei prodotti per le comunicazioni voce e IP
- Risoluzione dei problemi di Cisco IP Telephony
- Documentazione e supporto tecnico – Cisco Systems