

Authentication

→ SIP Workshop
Centrelink

By Stephen Kingham

Stephen.Kingham@kingtech.com.au



©Stephen Kingham

→ Authentication in SIP

- Both ends must know the same secret password (key).
- The password is used to encrypt certain information such as the user's password.
- Originated from HTTP (WWW) and often called HTTP digest, Digest Authentication is described by RFC 2671.
- RFC 3261 (SIP) describes how Digest Authentication is applied to SIP.

→ SIP REGISTER with Digest Authentication

UA

Proxy Server

REGISTER bruce@uni.edu.au (with out credentials)

407 Proxy Authentication Required

ask user for a password

REGISTER bruce@uni.edu.au (password encrypted with key)

200 OK

→ SIP INVITE with Digest Authentication

UA

Proxy Server

UA

INVITE fred@uni.edu.au (with out credentials)



407 Proxy Authentication Required



ACK



ask user for a password

INVITE fred@uni.edu.au (with encrypted password)



100 TRYING



INVITE fred@uni.edu.au (password removed)



→ Secure SIP

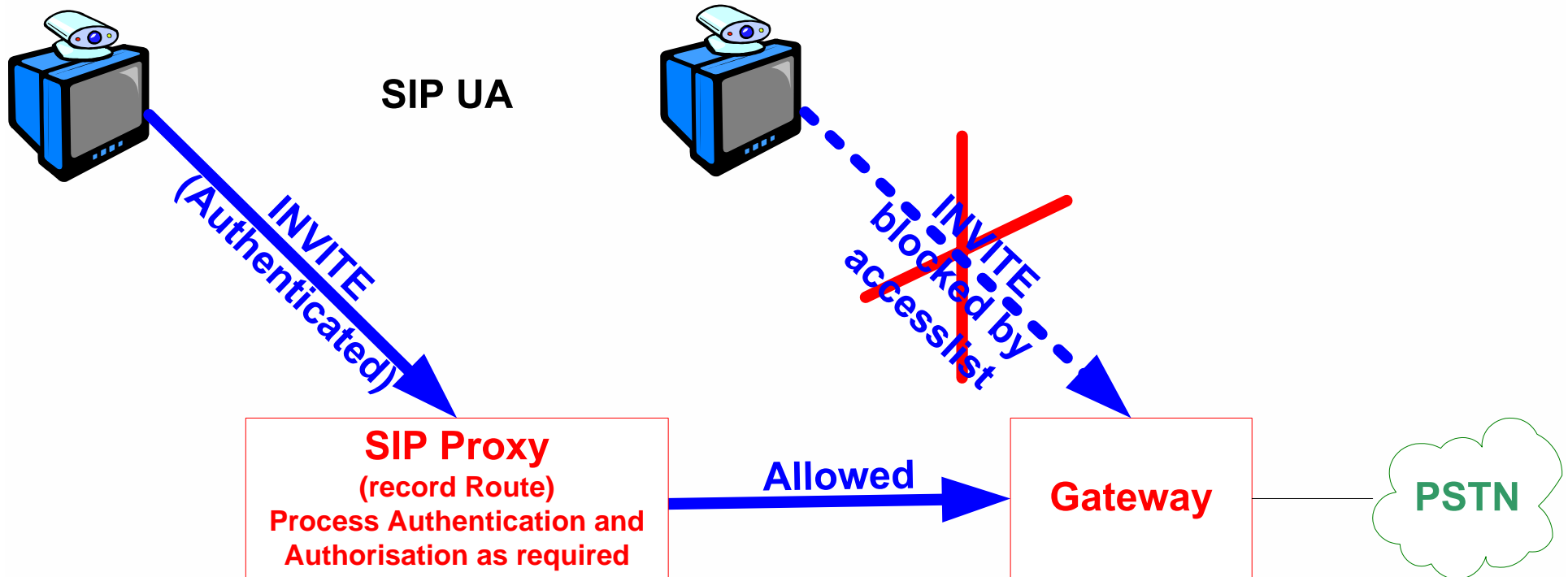
- SIPS, a close cousin of SIP, is a good and low cost means of encryption soon to be widely deployed. It specifies TLS (transport layer security) over TCP and is not subject to bid down attacks. This means a SIPS call will fail rather than complete insecurely.

→ Two interesting drafts

- <http://www.ietf.org/internet-drafts/draft-ietf-sip-identity-03.txt>
Abstract The existing security mechanisms in the Session Initiation Protocol are inadequate for cryptographically assuring the identity of the end users that originate SIP requests, especially in an interdomain context. This document recommends practices and conventions for identifying end users in SIP messages, and proposes a way to distribute cryptographically-secure authenticated identities.
- <http://www.ietf.org/internet-drafts/draft-peterson-message-identity-00.txt>
This document provides an overview of the concept of identity in Internet messaging systems as a means of preventing impersonation. It describes the architectural roles necessary to provide identity, and details some approaches to the generation of identity assertions and the transmission of such assertions within messages. The trade-offs of various design decisions are explained.

→ Protect Gateways from un-authorized use

- Use a Proxy Server in front of your Gateways, turn on Record Route so ALL SIP control is via Proxy.
- Configure gateways so that they only respond to SIP from your SIP Proxy.
 - Filter TCP and UDP traffic to port 5060 on the Gateway.
 - Also do the same for H.323, TCP traffic to port 1720 on the gateway.



Future of telephony

→ VoIP Workshop
Terena 2005 Poznan Poland

By Stephen Kingham

<mailto:Stephen.Kingham@aarnet.edu.au>

<sip:Stephen.Kingham@aarnet.edu.au>



©Stephen Kingham

→ Copyright Stephen Kingham 2004

This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

→ Outline and Objectives

- Leading up to today
- Telephone revolution powered by SIP
- What to do now in NRENS and back home
 - SIP GDS – “SGDS”
 - Private ENUM trees
 - “eduPhone”
 - Signed SIP calls to stop SPIT

→ Telephones BEFORE the 80s see note



- Basic Telephone service
- In Universities it was provided by “Buildings and Grounds” departments in Universities.
- Generally provided by Carriers, usually on Carrier recommended PBX vendors.

Note: Starting with telephone services based on stored programme controlled TDM based switches.

→ Telephones in the 80s - deregulation

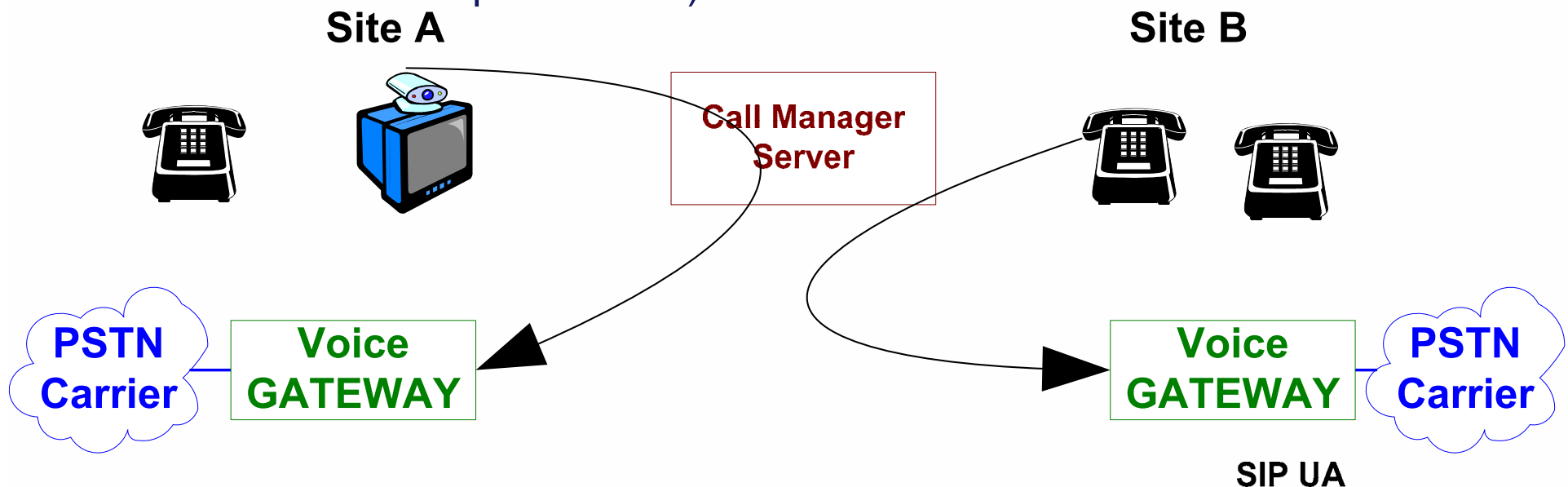
- Still Basic Telephone service
- (Tele)Communications Section created by bringing the Voice and Data Communications together under one management group, but still separate sections.
- Structured (shared) cabling between LAN and Telephone
- Generally still provided by Carriers. Some private networks using TDM and some compression.
- More choice of PABX platform.

→ Telephones in 2000-2004 – here comes H.323

- VoIP toll bypass based on H.323. Huge success in AARNet – 20,000 calls per day – extremely cheap, more stable and simpler than TDM networking.
- Proprietary IP Telephones deployments:
 - H.323 too hard (although Avaya did it).
 - whole University Campuses (some of the largest Universities in Australia).
 - Some hybrids (some PABX left) and some entirely IP Telephony.
 - IP Telephony based on top of solid VoIP network.
- VoIP needed WAN Section to work with Voice Section to provide low latency, loss and jitter. Voice now sharing WAN.
- IP Telephony needed LAN Section to work with Voice Section to provide VLAN design/management plus good quality network. Voice now on shared active LAN infrastructure.

→ IP Telephones in 2000-2004 – Emergency Services

- Provide POTS phones as power fail/emergency phones. Connected Analogue Terminal Adaptors with SIP Servers and Gateways to the PSTN at each Site.
- Ask how complicated it is to make sure Emergency phone calls are sent to local gateway (easy with new generation PBXs, eg SLIPPER and SER use exception and rules set routing and can use the source ip address?)



→ Telephones in 2005+ SIP and 3rd party Carriers The revolution begins!

1. Explosion of SIP UAs into the market.
2. Many 3rd party providers of sip: accounts.
3. Some proprietary solutions (eg Skype) plus some who lock customer in (eg MSN).
4. All the IP Phone and traditional PABX vendors are moving to SIP.
5. SIP based PBXs with exceptional capabilities and features, at a fraction of traditional TDM switches.
6. Control given back to the user.

I think we will now see the introduction of the Unix System Administrator (and programmer) skills into the Voice Section.

→ Affordable SIP products (NOT H.323)
SIP is cheaper because it is easier to build and support

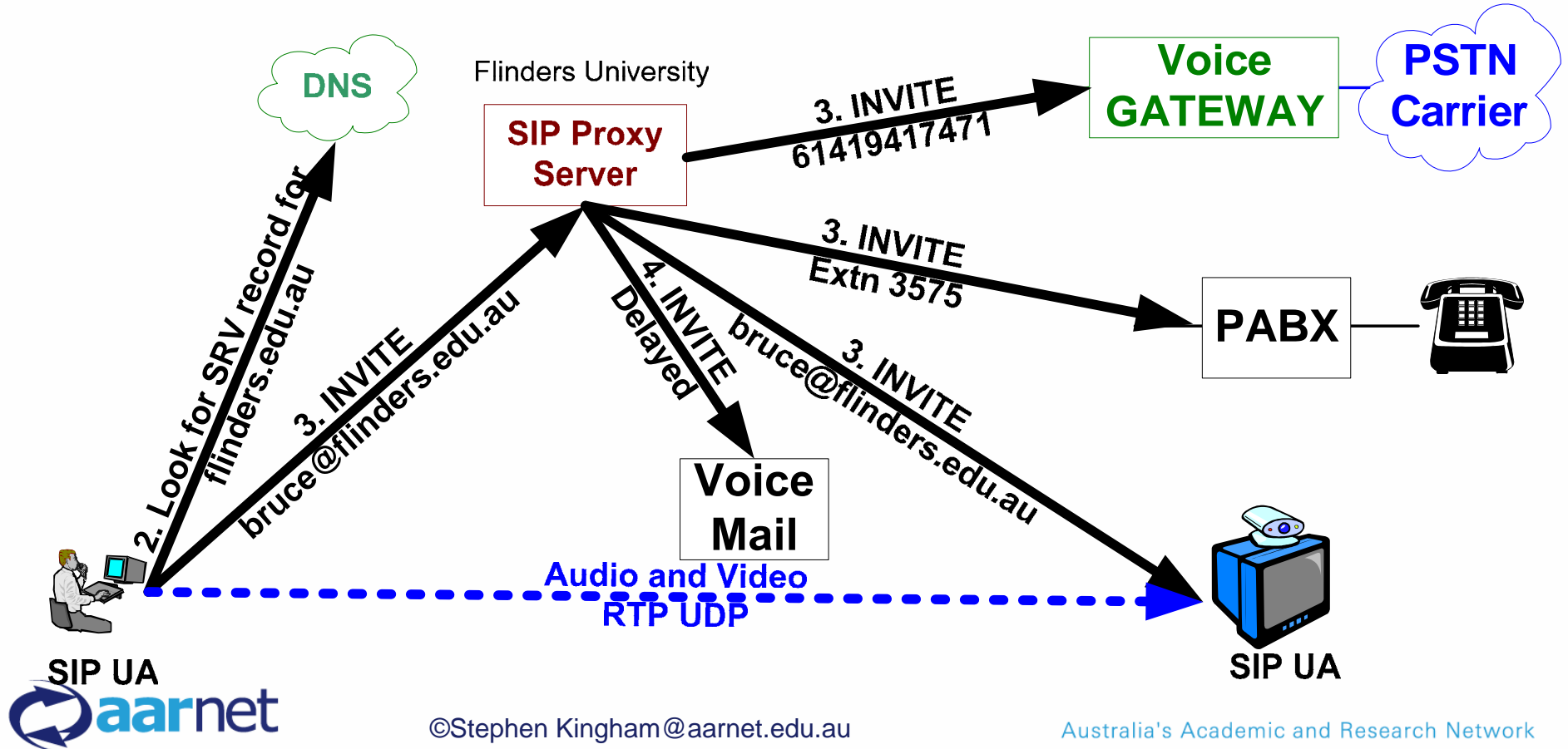
- Basic SIP IP phones below A\$150
- 802.11 phones
- video phones
- Speakerphones
- PDAs with SIP software
- MAC, Unix. and MSoft.



Combination of Stephen Kingham and Quincy Wu's talk, www.apan.net Cairns 2004

→ SIP FORKING (native to SIP)

Never need to forward phones to other phones again!!!!
This is a big change.



→ providers of sip: accounts

Provide sip accounts like hotmail provides email accounts.

- www.iptel.org (home of Open Source SIP Server SER)
- Free World Dial (fwd) fwd.pulver.com
- And many many more impossible to estimate the number

Providers of closed sip accounts

(is this unproductive behaviour?):

- MSN
- Skype is NOT SIP – and has serious implications (kazaar)!

Could Universities start loosing their customers to 3rd party providers?

Has this already started?

→ Vendors moving to SIP (a sample for discussion)

- NEC
- Avaya
- Cisco new Call Manager is SIP in the core not skinny
- Nortel
- Microsoft

With SIP it is easy to inter-work

→ SIP based PBXs

Some of these offer features and capacities that leave the traditional big vendors looking very inadequate (note: presenter's opinion open to be convinced otherwise)

- SIP Express Router (SER) Open Source from www.iptel.org.
 - 1 config file and mysql
- SIPx (Open Source) is making a big impact
- Asterisk is not really SIP or H.323
 - does some nasty things to the codec negotiations
 - but it is very popular.
 - Great for H323-SIP GW, IVR, and Voice Mail.
 - Many config files.
- There is the start of an explosion of very good quality SIP PBXs.
- What does the audience have?

→ Slipper HelperApp: a full Voicemail System in perl:

```
#!/usr/bin/perl -w
use strict;
use Slipper::HelperApp;
my $stream = Slipper::HelperApp -> new_stream (shift, shift);
if (! ref $stream) {
    print $stream . "\n";
    exit 0;
}
my $return = $stream -> find_vm_target;
if ($return !~ /^200/) {
    print $return;
    exit 0;
}
$stream -> report_port;
$stream -> play_audio ($stream -> {'VM Greeting'});
$stream -> play_audio ('vm/pling.au');
my ($dtmf, $message) = $stream -> record_audio;
exit 0 if (! defined $message);
$stream -> send_vm ($message);
exit 0;
```

→ Slipper Rulesets

- Input Filter
- Group / Authenticate
- Canonify
- Authorise
- Expand
- Route (done by exception)
- Destination Group
- Codec
- Various header mappings
- Output Filter

→ PROPOSAL 1: eduPhone

It is to create a Service similar to fwd and skype.

A Voice, Video, Presence, Instant Messaging Service with PSTN connectivity, and Voice Mail, for the people in the AREN community.

Members then encourage staff etc to use the University's approved service that can be secured and supported.

Consider using eduRoam radius Authentication to provide sip accounts to anyone who is eduRoam enabled.

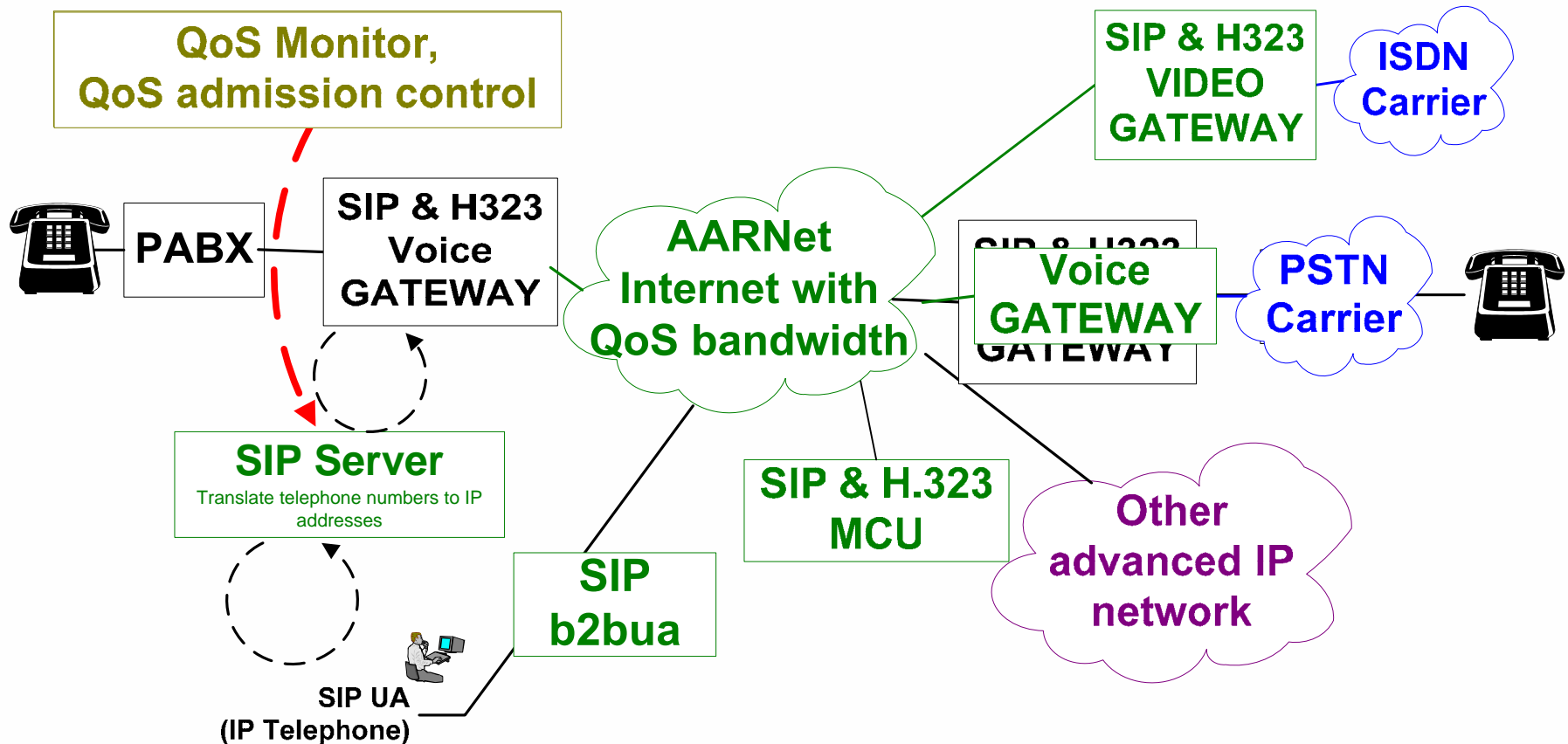
→ SIP.edu: Benefits and Open Issues

- Benefits:
 - Employees of an organization can be reached worldwide by a SIP client via their email-address
 - After the realization of SIP.edu, the organization is ready to build an organization-wide IP Telephony infrastructure (IM, Presence, Video) because the basic components are already available
 - ENUM can be easily integrated
 - SIP to SIP calls are open and always possible
- Open issues so far:
 - Call forking to multiple location should be implemented (office phone and registered SIP clients)
 - The claim that email addresses should converge to voice identities is not completely right
 - what about inbound integration with PSTN?
 - ENUM is there and I still have to remember an E.164 number as long as PSTN exists (for a long time) if I am calling from a PSTN phone (let's use ENUM for this)
 - It is a closed environment
 - what about people not employed in the organization that do not have a number (students for example)?
 - what about outbound calls to PSTN?

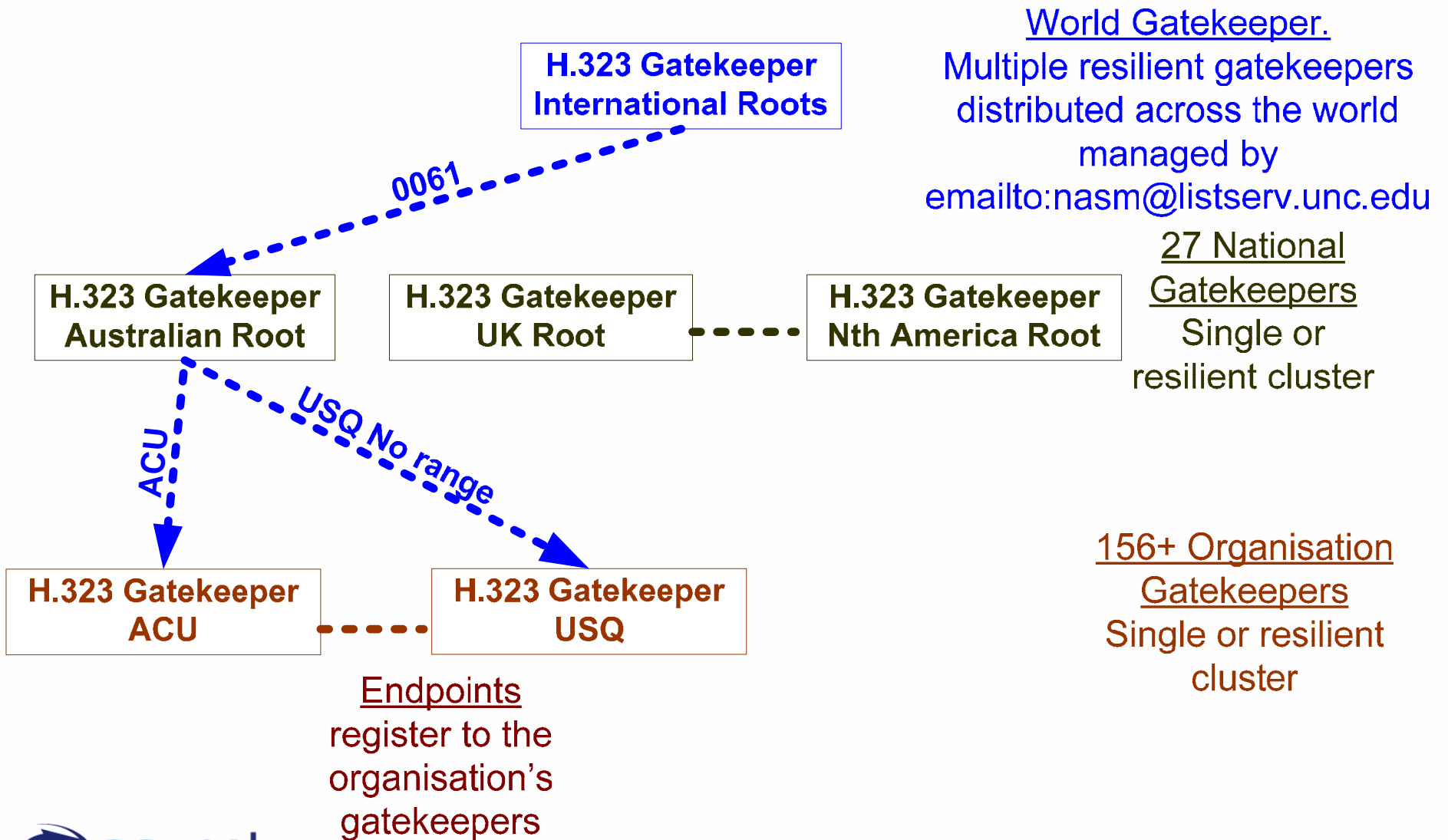
→ AARNet SIP & H.323 network – where/how to put eduPhone

It is the QoS Admission control that enables AARNet connect 20,000 commodity telephone calls per day, started in 1999.

See lattice.act.aarnet.net.au/VoIPMonitor



→ The GDS: H.323 routing (all static configuration)



→ PROPOSAL 2: SGDS to accomplish e164 routing.

- SIP Global Dialling Scheme (SGDS). A hierarchy of SIP Redirect Servers.
 - Several International roots
 - One Root per country
 - Organisation (open to the public) per to Country
 - Each with static routing entries for E164.
 - Based on the success of GDS (H.323 hierarchy of H.323 Gatekeepers)
- An alternative/addition/enhancement is a Private ENUM root run by the ARENs, such as e164.edu (rather than e164.arpa). The administrators of the existing International GDS Roots might take on administration of the e164.edu applying the same administration processes.
 - Add some SIP Proxies that will do the ENUM look up as a public service
(eg sip:+<country code><number>@redirect.SipEduEnum.pulver.com:5062)

→ CONCLUSION

- Need to keep supporting H.323 but
- Do not undertake any large projects without implementing SIP.
- Get one or more SIP Proxy Servers going (get a SysAdmin and Voice person together).
 - SIPx might be a great choice (I do not know it's strengths yet)
 - SER for routing and users – configuration is a programme
 - Mix an match SIP products (use Asterisk for IVR and Voice Mail)
 - Consider commercial products with similar open architectures, such as one like Slipper.
- SIP.edu enable your University
- Join the working groups:
- Internet2 WGs (VoIP, SIP.edu, and PIC) and APAN siph323 WG – is there one in Terena?

→ The Revolution has started

- SIP enabled IP Telephony and VoIP and VIDEOoIP with Presence and Instant Messaging.
- Mobility, freedom, cheap, flexible.
- **Will have a larger Social and Economic impact than http!**
- Innovation today comes from the worlds ARENs.
- This community needs to work on SIP enablement of their infrastructure and do some leading together with Carriers.

How then do we proceed?

→ Discussion and hands on

- Who would like to peer??????
- How then do we peering NREN VoIP domains
 - SGDS
 - ENUM
 - Private ENUM
 - TRIP
- eduPhone use eduRoam radius infrastructure for use authentication
- PSTN hop off

→ References used in this talk

- Internet2 SIP.edu initiative <http://voip.internet2.edu/SIP.edu/> take a look at the CookBook.
- <http://www.iptel.org/> home of The SIP Express Router (SER)
- www.fwd.pulver.com 3rd party carrier
- SIP Tutorials and Workshops run by AARNet <http://www.aarnet.edu.au/events/conferences/2004/sip/>