SIP ain't SIMPLE

Rodney McDuff
Strategic Technologies Group
Information Technology Services
The University of Queensland

- About UQ.
- Some Business Drivers.
- SIP Prelude.
- SIP Bestiary.
- Where have we been today?
- Issues along the way.
- Where do we want to go tomorrow?

About UQ

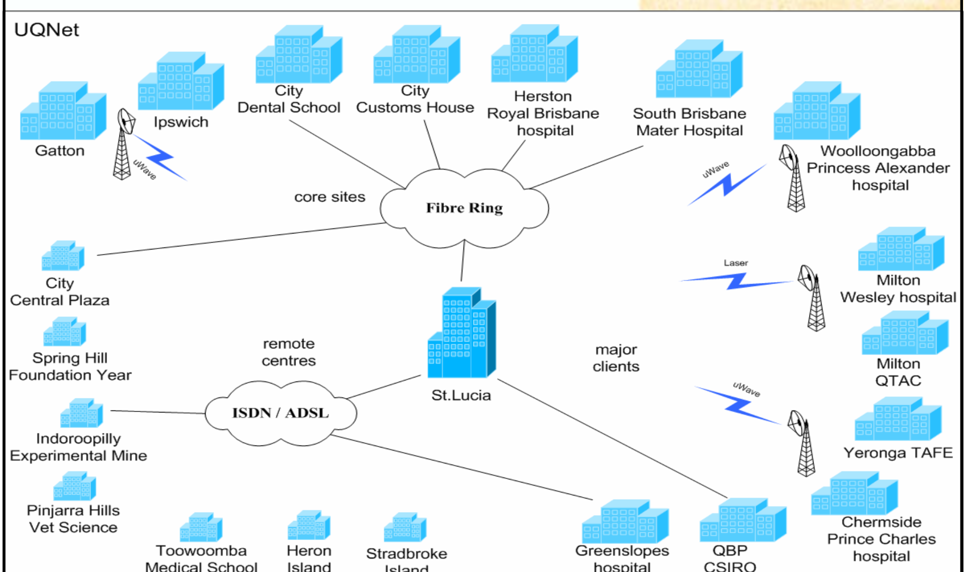
- 37K student.
  - 17% international students (from 121 countries).
  - 26% Postgrads.
- 5250 Staff.
  - 2191 Academics.
  - 3059 General Staff.
  - Approx. 7000 Fringe Dwellers.
- 3 main campuses.
  - St. Lucia, Ipswich and Gatton.
  - Operates about 50 other sites.
- 18000+ computers.
  - 30+ routers, 700+ switches, 200+ AP.
  - 11K phone extensions.

About UQconnect

- UQ's ISP focused at staff, students and alumni's residential and personal needs.
  - Over 10K customers.
  - Dialup, ADSL, iBurst, Web Hosting.

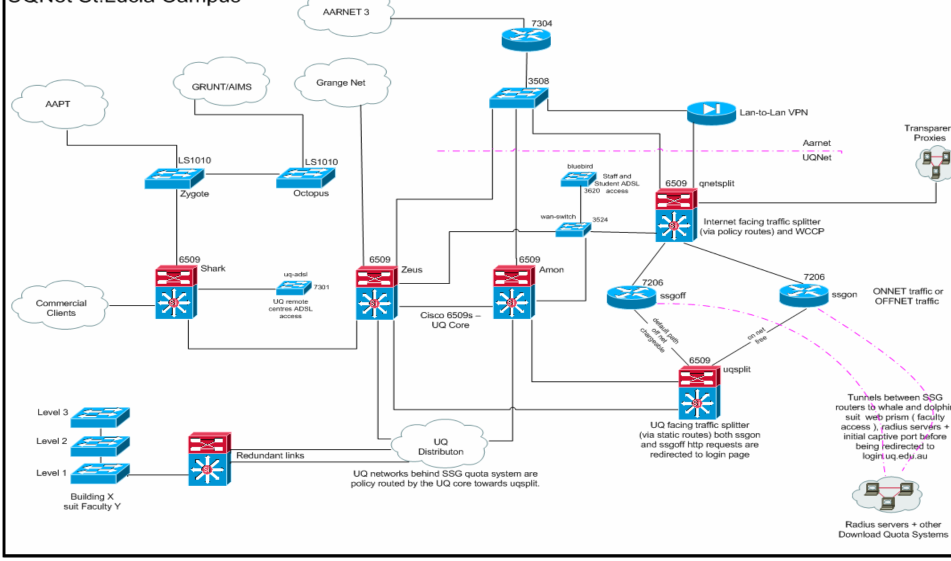
About UQ: UQ Network

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES



About UQ: UQ Network

UQNet St.Lucia Campus



About UQ: Voice Network

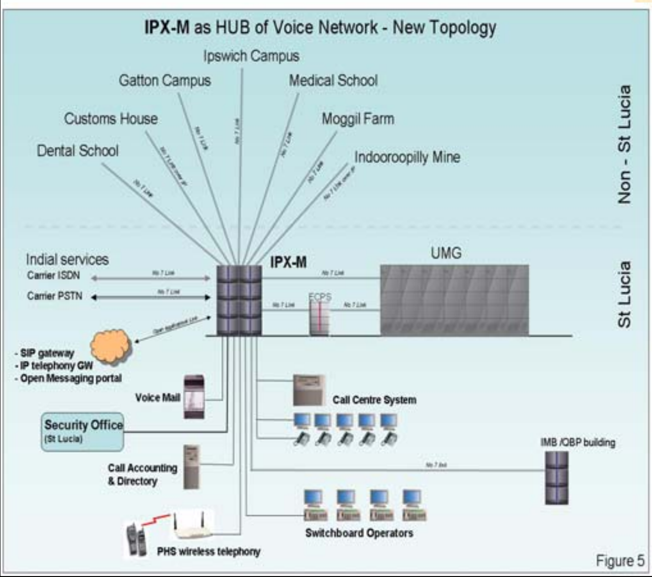


Figure 5

TOTAL: 11K exts

- St. Lucia:
  - UMG 7100 exts
  - IPX-M 380 exts
  - IMB 620 exts
- Ipswich: 470 exts
- Gatton:
  - Campus 775 exts
  - Hall of Residence 560 exts
- Medical School: 735 exts
- Other: 369 exts

PRAs

- 510 channels in
- 240 channels out

Voicemail

- 7K users
- 5K messages/day
- 10K hits/day

What we want to do

- Construct an *open* flexible scalable *multi-modal* communication solution.
- Based on suitable freely available and commercial products.
- Use converged communications identifier ie email address.
- Revolutionize the work place and the campus community through an integrated collaboration infrastructure based on video, instant messaging and presence enabled services and information exchange.

Drivers

- Old, unsupported PBX.
  - NEC 2400 Ultra Module Group (UMG).
  - 1988 technology.
    - 50% 16 years old.
    - 25% 13 years old.
  - Unsupported since 31/12/2005.
  - Mitigated some risk with IPX-M.
- Want to move virtually everything to VoIP.

Drivers

- **Cost savings**
  - **Cheaper calls? Maybe.**
    - SIP-to-SIP voice call data charges cost 0.4 cent/min thru AARNet.
    - If there was any one out there to call.
  - **Cheaper Infrastructure? Maybe.**
    - One network rather than two. But network needs. major work for QoS, redundancy and DR.
  - **Cheaper Operational Costs? Possibly.**
    - Cheaper maintenance and management.
    - Cheaper and faster moves, adds and changes.

Drivers

- **Cost savings**
  - **Less PSTN and mobile calls? Maybe.**
    - Edith Cowen University.
  - **Less staff? Maybe.**
    - Dartmouth College <http://www.educause.edu/LIVE056>.
  - **Greater efficiencies? Definitely!!**

    From surveys completed by Sage Research and Forrester Consulting.
    - Save 32 min/day reaching coworkers.
    - Save 43 min/day from using unified messaging.
    - Save 31 min/day by using IM.
    - 25% say projects halt until key decision makers found.
    - 37% say save 15-30 min/day reaching coworker with single address.
    - 37% say presence would significantly streamline communications.

www.its.uq.edu.au

THE UNIVERSITY OF QUEENSLAND AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

Drivers

- Network management
  - Students want to use Skype and other IMs.
  - Staff want to use Skype and other IMs to collaborate.
  - But good network ~~fascists~~ managers want:
    - To know who is using their networks.
      - Staff and students to be accountable for their (mis)deeds.
    - To know that nice, well behaved applications are being used on their networks.
    - To eliminate Skype from their networks (because it too good at the evil things its does).
      - P2P. Endpoint defined by login but IP.
      - Constantly evolving to bypass firewalls, NATs and access control.
      - Heavily obfuscated and encrypted.
      - Application-to-Application communication through Skype.
  - But need to replace Skype and IMs with friendlier apps.
    - Can't leave a vacuum.

www.its.uq.edu.au

THE UNIVERSITY OF QUEENSLAND AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

Drivers

- VoIP is inevitable.
  - Only a question of when you deploy.
- Our duty to grease the wheels of collaboration.
  - Intra-institution.
  - Inter-institution.
    - eScience grants favouring inter-institution collaboration and federation.

Drivers

- VoIP for UQconnect.
  - Over 1200 ADSL customers and growing.
  - Over 100 iBurst customers and growing fast.
  - Need VoIP product to help maintain growth.
    - Provide DID numbers to staff, students and alumni. for residential and personal use.
    - DIDs follow students from house to house.
    - Enable home and remote workers.
    - Cheap PSTN calls for all.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

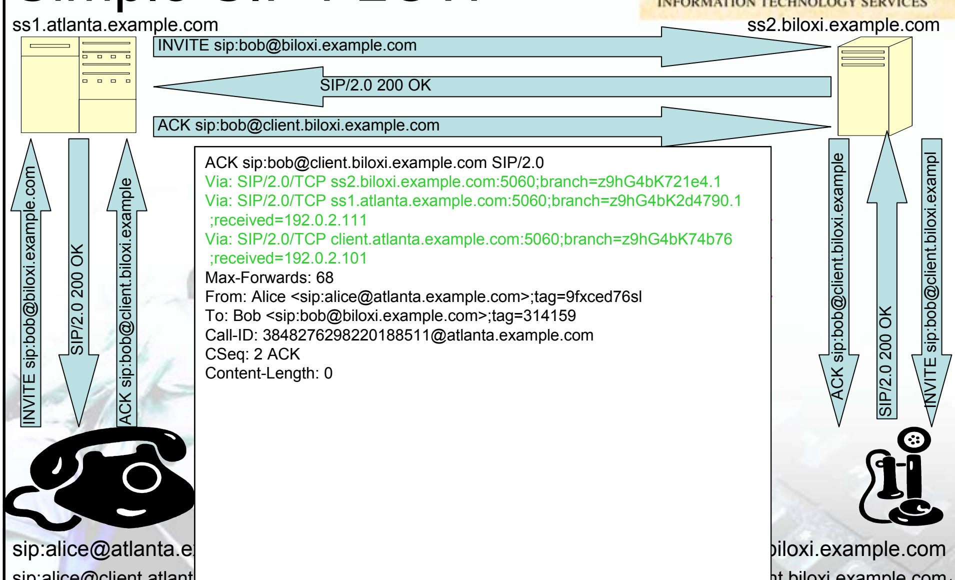
Session Initiation Protocol (SIP)

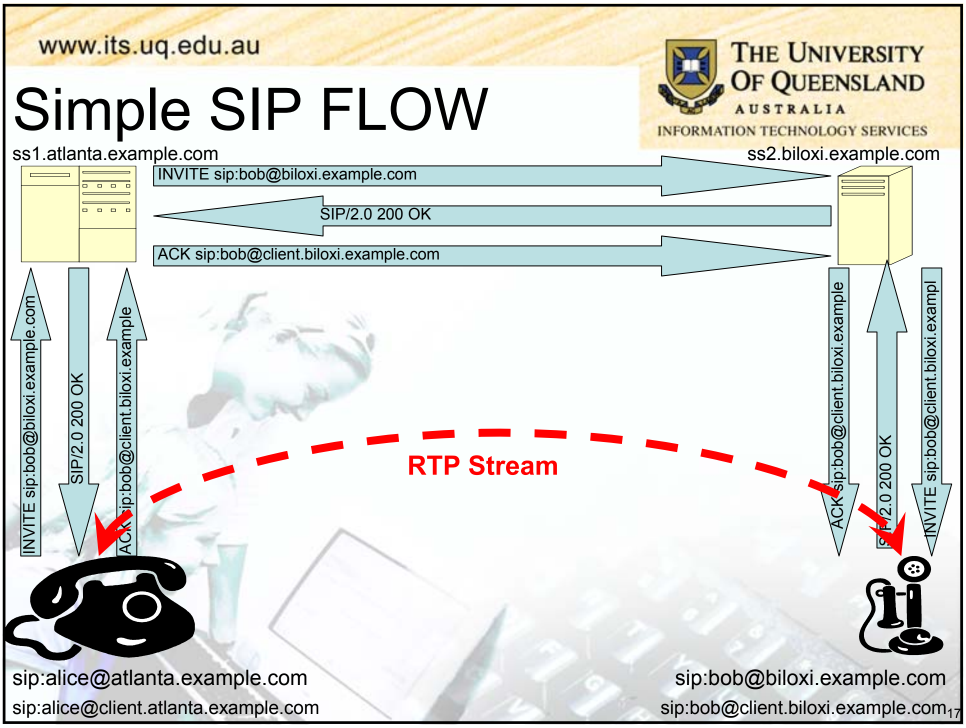
- **HTTP like protocol over UDP, TCP, TLS or SCTP**
  - Originally described in RFC 2543, obsoleted by RFC 3261.
  - Consists of:
    - Headers and Bodies.
    - Request and Responses.
  - Signaling protocol for creating, modifying, and terminating sessions with one or more participants.
- **Requests:**
  - REGISTER, INVITE, ACK, BYE, CANCEL, OPTIONS (RFC 3261) .
  - PRACK (RFC 3262).
  - SUBSCRIBE, NOTIFY (RFC 3265).
  - INFO (RFC 2976).
  - REFER (RFC 3515).
  - MESSAGE (RFC 3428).
  - UPDATE (RFC 3311).
  - PUBLISH (RFC 3903).
  - SERVICE, BENOTIFY (Microsoft Proprietary).

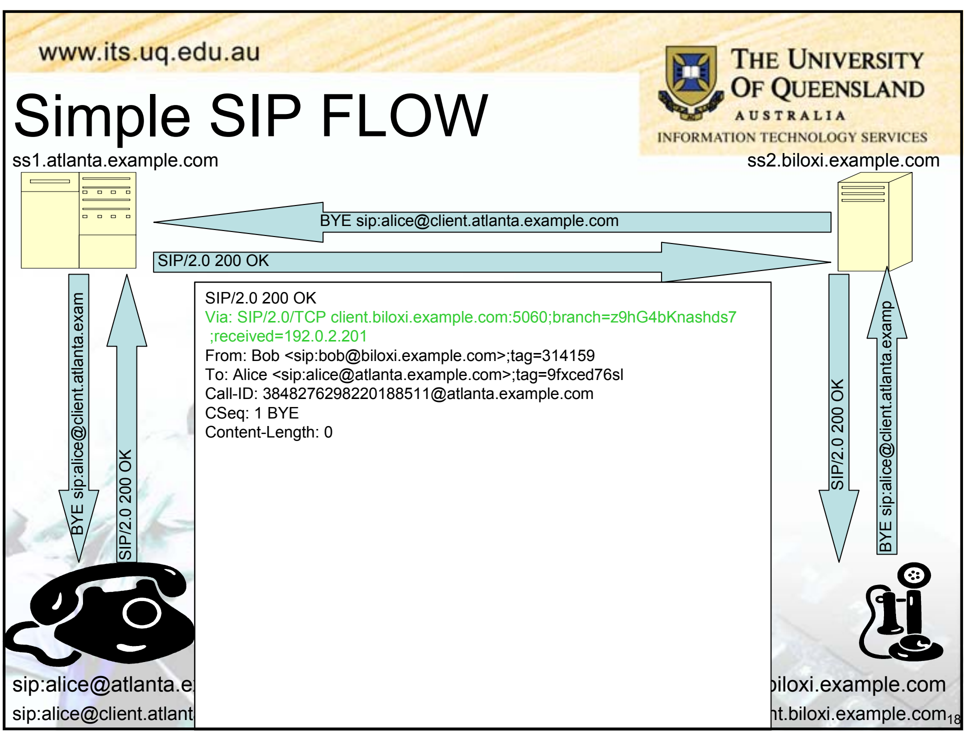
Session Initiation Protocol (SIP)

- **Reponses.**
  - 1xx Informational.
    - 100 Trying, 180 Ringing, 183 Session Progress.
  - 2xx Successful.
    - 200 OK, 202 Accepted.
  - 3xx Redirection.
    - 301 Moved Permanently, 302 Moved Temporarily.
  - 4xx Request Failure.
    - 401 Unauthorized , 404 Not Found, 407 Proxy Authentication Required , 482 Loop Detected.
  - 5xx Server Failure.
    - 501 Not Implemented.
  - 6xx Global Failure.
    - 603 Decline.

Simple SIP FLOW




www.its.uq.edu.au
Simple SIP FLOW
THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES
ss1.atlanta.example.com
ss2.biloxi.example.com
INVITE sip:bob@biloxi.example.com
SIP/2.0 200 OK
ACK sip:bob@client.biloxi.example.com
INVITE sip:bob@biloxi.example.com
SIP/2.0 200 OK
ACK sip:bob@client.biloxi.example
ACK sip:bob@client.biloxi.example
SIP/2.0 200 OK
INVITE sip:bob@client.biloxi.exampl
RTP Stream
sip:alice@atlanta.example.com
sip:alice@client.atlanta.example.com
sip:bob@biloxi.example.com
sip:bob@client.biloxi.example.com
17


www.its.uq.edu.au
Simple SIP FLOW
THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES
ss1.atlanta.example.com
ss2.biloxi.example.com
BYE sip:alice@client.atlanta.example.com
SIP/2.0 200 OK
SIP/2.0 200 OK
Via: SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7
;received=192.0.2.201
From: Bob <sip:bob@biloxi.example.com>;tag=314159
To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 BYE
Content-Length: 0
BYE sip:alice@client.atlanta.exam
SIP/2.0 200 OK
SIP/2.0 200 OK
BYE sip:alice@client.atlanta.examp
sip:alice@atlanta.e
sip:alice@client.atlant
biloxi.example.com
nt.biloxi.example.com
18

RTP, SRTP and ZRTP

- Media Transport Protocol.
  - Audio and Video Codecs.
- RTP – Realtime Transport Protocol (RFC 3550).
  - Over UDP.
  - 2 streams. Media and Control (RTCP).
- SRTP – Secure Realtime Transport Protocol (RFC 3711).
  - sdescriptions.
    - Key exchange in SDP payloads.
    - Security requires SIP exchange over TLS.
  - MIKEY – Multimedia Internet KEYing (RFC 3830).
    - Key exchange by IKE.
- ZRTP (IETF Internet Draft draft-zimmermann-avt-zrtp-01.txt).
  - Zfone <http://www.philzimmermann.com/EN/zfone/index.html>.
  - Shim in network stack.
  - Key exchange by Diffie-Hellman.
- See next session: "Enable Secure Realtime Media with SIP"
  Robert Dolphin.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

Codecs

Number	Bit rate (kbps)	Sampling rate (kHz)	Frame size (ms)	MOS (Mean Opinion Score) 1-5	Ethernet Bandwith (kbps)
G.711	64	8	Sampling	4.1	87.2
G.721	32	8	Sampling		
G.722	64	16	Sampling		79.6
G.722.1	24/32	16	20		
G.723	24/40	8	Sampling		
G.723.1	5.6/6.3	8	30	3.8-3.9	21.9
G.726	16/24/32/40	8	Sampling	3.85	55.2
G.728	16	8	2.5	3.61	31.5
G.729	8	8	10	3.92	31.2
GSM	13	8	22.5	3.7	30
Speex	8, 16, 32	2.15-24.6 (NB) 4-44.2 (WB)	30 (NB) 34 (WB)		24.8
iLBC	8	13.3	30	3.85	27.7

Instant Messaging and Presence

- Instant Messaging:
  - MESSAGE method defined in RFC 3428.
  - Page-based messaging. SMS Like.
- Presence:
  - Presence Information Data Format (PIDF) RFC 3863.
    - Consists of two basic states, OPEN and CLOSE.
    - Rich Presence in extension status.
  - Peer-to-Peer.
    - Watcher SUBSCRIBEs to Presence User Agent for Presentity status.
    - PUA NOTIFYs Watcher when status changes.
    - Watcher aggregates forked replies.
  - Presence Agent.
    - PUA(s) PUBLISH status to Presence Agent.
    - Watcher SUBSCRIBEs to Presence Agent.
    - Presence Agent NOTIFYs Watcher when status changes.
    - PA aggregates status from PUA(s).

Instant Messaging and Presence

- SIMPLE.
  (SIP Instant Messaging and Presence Leveraged Extensions.)
  - Still just an 4 RFCs and a set of Internet Drafts.
  - Session-based IM. Ie. Group Chats
    - Setup via INVITE and SDP payload.
    - Message Session Relay Protocol (MSRP) between end-points.
    - Session can offer multi-modal communication types. Voice, video, text,…
  - Extended Presence Data Model.
  - Partial PUBLISH and NOTIFY.
- XMPP.
  (Extensible Messaging and Presence Protocol.)
  - RFC 392[0-3] since 2004. (Adaptation of Jabber protocol.)
  - Underlies GoogleTalk. Transports for AIM, MSN, Yahoo, ICQ, IRC, …
  - Federated like SIP.
  - Next IM and Presence contender?

SIP Bestiary: User Agents (UA):

- Devices that end users actually use to send and receive calls.
  - User Agent Client (UAC).
  - User Agent Server (UAS).
    - Listens typically on port 5060 TCP/UDP.
      - Some UAs choose port automatically.
    - Various Firewall Issues.
      - SIP Keep-a-lives. Frequent OPTIONS and REGISTER.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

SIP Bestiary: User Agents (UA):

Softphones: Software application.

X-Lite

SJPhone

MS Messenger V5.1

eyeBeam

Kapanga

Office Communicator

SIP Bestiary: User Agents (UA):

Handsets: Looks and feels like a phone.

Cisco 7960

Nec DTERMs

Hitachi Wireless IP3000/5000

Cisco 7961

NetComm V85

Analog Telephone Adapters (ATA)

SIP Bestiary: SIP Proxies

- Primarily plays the role of routing and enforcing policy.
  - Usually only modify requests/responses for routing purposes.
  - Generally do not participate in RTP streams.
- Other Optional Functions.
  - Registrar.
    - Authenticates UACs.
  - User Location Service.
    - Translates AOR URI to Contact URI(s).
  - Redirect Service.
    - Handle events like call forwarding.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

SIP Bestiary: SIP Proxies

- Examples:
  - SER/OpenSER:
    - Actively developed open source proxy.
    - Standards based.
    - Rich feature set like:
      - SIP over UDP/TCP/TLS, SIMPLE, SIMPLE2Jabber, LCR, ENUM, Radius/database integration and many more
      - SBC feature like FW/NAT transversal, RTP proxy, DoS mitigation
    - fine control and manipulation of SIP packets.
      - Allows protocol repair.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

SIP Bestiary: SIP Proxies

- Examples:
  - NEC SV 7000:
    - NEC's Enterprise Telephony Solution.
    - Only believe in numbers.
    - Only believes in UDP.
    - SRTP by MIKEY variant.
    - IMHO. Just replacing copper with IP and SIP.
      - Seems a lot of Telephony Vendors do this.

SIP Bestiary: SIP Proxies

- Examples:
  - Microsoft Live Communications Server 2005:
    - Marketed as “standards based collaboration suite that leverages Instant Messaging and Presence” which also is capable of voice and video communications over SIP.
      - (In marketing, truth is the first casualty.)
    - Tight integration with Exchange, Outlook, Office Products etc.
      - (One might even say restrictive.)
    - Only works with Office Communicator and Windows Messenger V5.1 UAs.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

SIP Bestiary: B2BUAs Back-to-Back User Agents

- Concatenation of a UAC and UAS.
- Receives requests, processes them and generate new requests.
  - Signaling terminates one on side and regenerates on the other. (Different Call-IDs.)
  - Optionally RTP may terminate one on side and regenerates on the other.
    - Possible different codecs. Ie. transcoding.
    - Can monitor the media stream and provide features based on DMTF signaling.
  - Maintains dialog state.

SIP Bestiary: B2BUAs
Back-to-Back User Agents

- Examples:
  - Asterisk:
    - actively developed open source software PABX.
    - features a high quality voicemail system, conference room, IVR and phone queue.
    - only supports SIP over UDP.
      - SRTP in v1.4, TCP/TLS as patch.
    - Can't have multiple user REGISTrations.
      - Asterisk is NOT a Proxy.

SIP Bestiary: B2BUAs
Back-to-Back User Agents

- Examples:
  - Cisco Call Manager v5.
    - An enterprise IP telephony call-processing solution that is scalable, distributable and highly available.
    - Packaged as an appliance. Single firmware image (Linux).
    - Call Admission Control (CAC) thru RSVP.
    - Manage/Provision Cisco and third party SIP phones.
    - Supports KPML (Keypad Markup Language) ID draft-ietf-sipping-kpml.
    - Still undergoing evaluation…

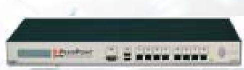
SIP Bestiary: SIP Gateways

- Protocol Transcoders
  - Signaling: SIP into H.323/SCCP/SS7.
  - Media: RTP into TDM.
  - SIP and RTP flows initiate/terminate on device.
- Examples:
  - Cisco 2821 Integrated Services Router:
    With High-Density Analog and Digital Extension Module
    for Voice and Fax.

  - Asterisk:
    With various E1 cards. Digium, Sangoma,…
    - SIP/PSTN, SIP/IAX, SIP/H.323, SIP/SCCP, SIP/MGCP.
    - Currently only SIP over UDP.

SIP Bestiary: SBCs
Session Border Controllers

- **Firewall for VoIP. (Usually takes the form of a B2BUA.**)
  - An RTP Proxy and help stop service theft.
  - Repair and fixes protocol problems.
  - Aid NAT transversal for UAs .
  - Perform protocol transcoding both in the signaling and data channels.
  - Hide SIP topology behind it.
  - Security and hardening again DoS
  - Call Admission Control.
  - QoS enforcement.
  - Create and control firewall pinholes to allow VoIP access into the network.
- **Examples:**
  - Jasomi Peerpoint C100.

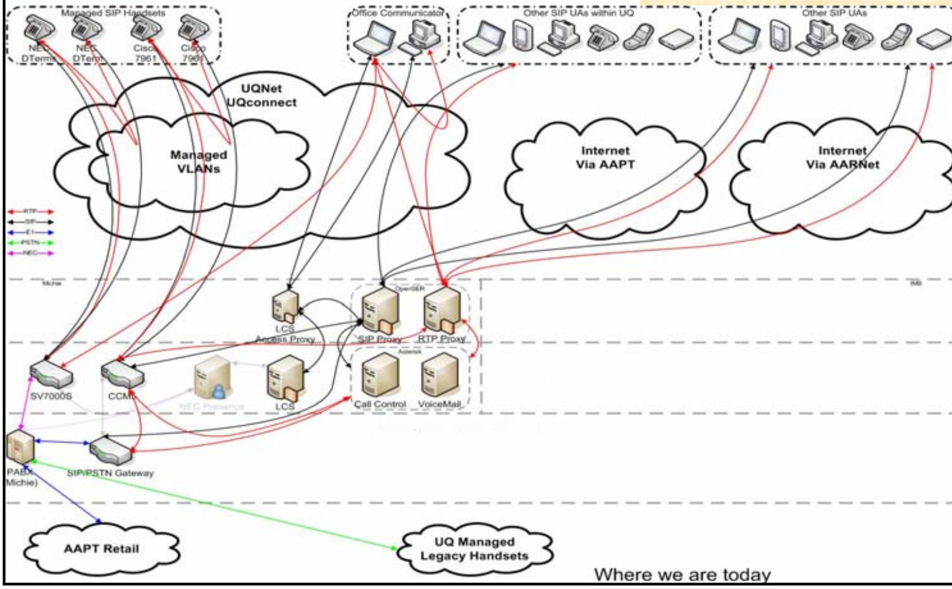


  - Cisco Multiservice IP-to-IP Gateway.

www.its.uq.edu.au

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

Where We are Today

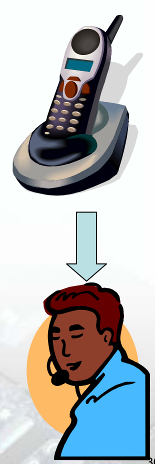


Where we are today

www.its.uq.edu.au

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

Issues: Prologue



PSTN is a MATURE technology

SIP is still evolving!!

Issues: Firewalls

- **SIP is not firewall friendly.**
  - SIP/RTP paths can be different.
  - BYE/ACK may go point-to-point
- **UQ has > 50 firewalls within network**
  - Many varieties. PIX, FreeBSD,…
- **UQ has Quotient FW around everything.**
  - Quotient == UQ in-house IMS based on Cisco SSG.
  - Nothing get in or out until user authenticates.
    - SIP setups session (INVITE/200 OK/ACK) thru one path.
    - RTP wants to go point-to-point but can't.
    - Everyone hears the sounds of silence.

Issues: Firewalls

- Solutions:
  - SBC at network perimeter.
    - Won't help with internal firewalls.
  - SIP-aware or UPnP firewalls.
    - Need to replace a lot of firewalls.
  - RTP proxy.
    - SER/OpenSER has a module for this.
    - Still wont help with internal firewalls.
      - Need to develop minimal set of static rules.
      - Need to control range of ports UAs listen to.

Issues: NATs

- SIP is not NAT friendly.
  - IPs in Headers and SDP inconsistent with source/destination addresses.
    - Use UAs that determine their external facing IPs
      - STUN (Simple Traversal of UDP Through NATs). RFC 3489.
      - TURN (Traversal Using Relay NAT) ID draft-rosenberg-midcom-turn.
      - ICE (Interactive Connectivity Establishment) ID draft-rosenberg-sipping-ice.
    - Use SIP Proxies/SBC fix up inconsistencies on the fly.
      - SER/OpenSER has modules for this.

Issues: Converged SIP Identities

- Want a converged communications identifier
  - sip:r.mcduff@uq.edu.au.
  - mailto:r.mcduff@uq.edu.au.
  - pres:r.mcduff@uq.edu.au
  - im:r.mcduff@uq.ed.au
- But 12 digit key pads will be around for a long time.
- Need SIP aliases. Like email aliases.
- Issue user a number-like URI aliased to their AOR as well.
- SER/OpenSER support aliases.

Issues: Quality of Service

- Poor voice quality mainly due to:
  - Packet latency, jitter and loss.
    - Mitigated by Network QoS.
  - Echo. Analog X-fed at remote end-point.
    - Mitigated by hardware/software echo cancellers.
- State of UQ Network.
  - Core is QoS ready today.
  - Rest of network is another story.
  - Long and costly venture to upgrade.
  - Still going to proceed anyway (in a staged approach).

Issues: Quality of Service

- VoIP servers on 802.1P VLANs in CORE network.
- Managed 802.1P VLANs only for Managed Handsets.
  - Users expect something that looks like a telephone to have telephone quality.
- Everything else overwrite user set DSCP as soon as possible.
  - QoS tag everything that looks like a SIP/RTP packet.
    - Destination or source is SIP server or RTP proxy.
  - Keep fingers crossed.
- Retag DSCP when peering with AARNet CAC system.

Issues: Live Communications Server

- Standards are good.
  - Aids interoperability between products.
    - Gives choices to the customer.
      - IMHO, this is the last thing certain vendors want.
- RFC 3261:
  - MUST support SIP over UDP. SHOULD should TCP/TLS.
    - LCS only supports SIP over TCP/TLS.
  - MUST support Digest method of authentication
    - LCS only supports proprietary NTLM and Kerberos methods.
- SIMPLE:
  - LCS doesn't support PUBLISH method. Uses SERVICE method for same purpose.
  - Uses BENOTIFY rate than NOTIFY.
- Just the tip of the iceberg.

Issues: Live Communications Server

- I **need** to support Office Communicator and other UAs.
- If I could use LCS to do this I would.
  - Tight integration with Outlook, Exchange, etc
    - a powerfully argument you can't ignore.
  - Plus it would drive "lesser" standards-based clients.
    - SIP Handsets, third party softphones, ATAs, ADSL Modems,…
- Only one choice.
  - Support 2 (or more) separate SIP infrastructures.
  - Still need to integrate them all.
    - LCS make this hard as well.
  - This somewhat confuses my unified communications identifier.
- Bottom Line. MS business arrogance is causing me pain.
  - Thank you Bill.

Issues: SIP Security

- Inherits all the attacks on layer 2,3,4.
  - ARP poisoning, IP spoofing, malformed packets, TCP/UDP floods/replays, DDoS, …
- SIP vulnerable to many attacks on layer 7.
  - Confidentiality:
    - Man-in-the-Middle, Tools like VOMIT, Oreka.
  - Integrity:
    - Spoofed headers, RTP tampering/insertion, DHCP/TFTP insertion attacks.
    - Attacker masquerading as legitimate user.
  - Availability:
    - REGISTER/INVITE floods, CANCEL/BYE attacks. Malformed requests/responses.
- And then there's SPIT.
  - SPam over Internet Telephony.

Issues: SIP Security

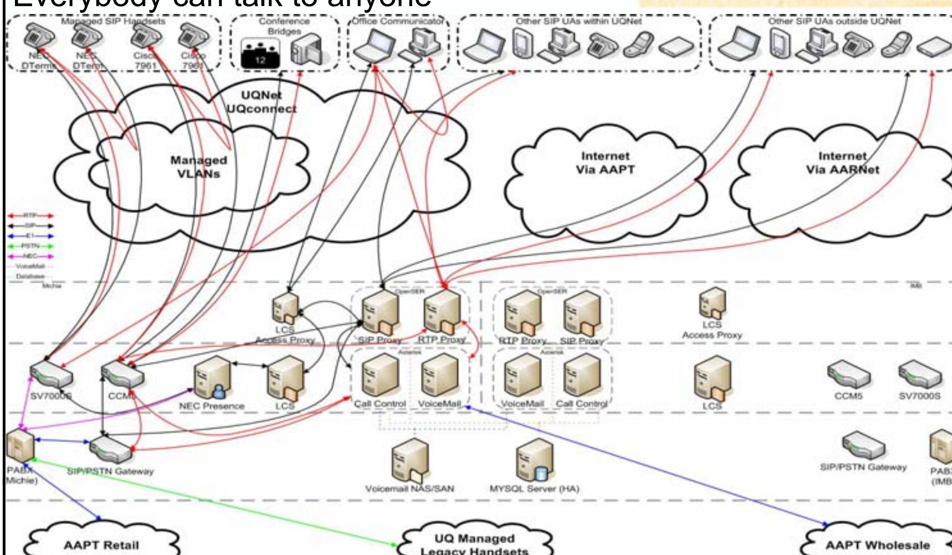
- What to do?
  - Enforcing outbound proxy and authenticate all requests.
    - Atleast you'll know whose account has been compromised.
  - Use SIP over TLS and SRTP where possible.
    - Hop-to-Hop integrity and confidentiality.
    - Requires transitive trust of SIP proxies.
  - Use S/MIME of SIP bodies (defined in RFC 3261).
    - End-to-End integrity and (some) confidentiality.
    - Doesn't protect headers unless using Tunneled SIP.
      - Still can't protect some headers. Via. Record-Route, Caller-ID, Cseq.
    - Needs personal PKI and associated infrastructure.
    - S/MIME for SIP has not been as widely deployed.
  - Hope for the future.
    - SIP SAML Profile and Binding (ID draft-ietf-sip-saml)

Issues: SIP Security

- What to do?
  - Use a SBC or its ilk.
  - Use Access Lists.
    - Only peer with domains you trust.
  - Use SIP vulnerability tests/security tools:
    - SiVuS.
      <http://www.vopsecurity.org/html/sivus.html>
    - PROTOS C07-SIP test suite.
      <http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip>
    - SFTF.
      <http://www.sipfoundry.org/sftf>
    - Codenomicon SIP Test Tool.
      <http://www.codenomicon.com/products/telecommunications/sip>
    - Unfortunately these types of tools still in their infancy.
- Don’t worry. Be happy!!!

A Glimpse of a Possible Future

Everybody can talk to anyone



The Big Picture

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
INFORMATION TECHNOLOGY SERVICES

Question?