Advanced SIP topics

H.350: What it is, what it does, why you want it…

20th Apan Meeting, Taipei, Taiwan
August 2005

aarnet
Australia's Academic and Research Network

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

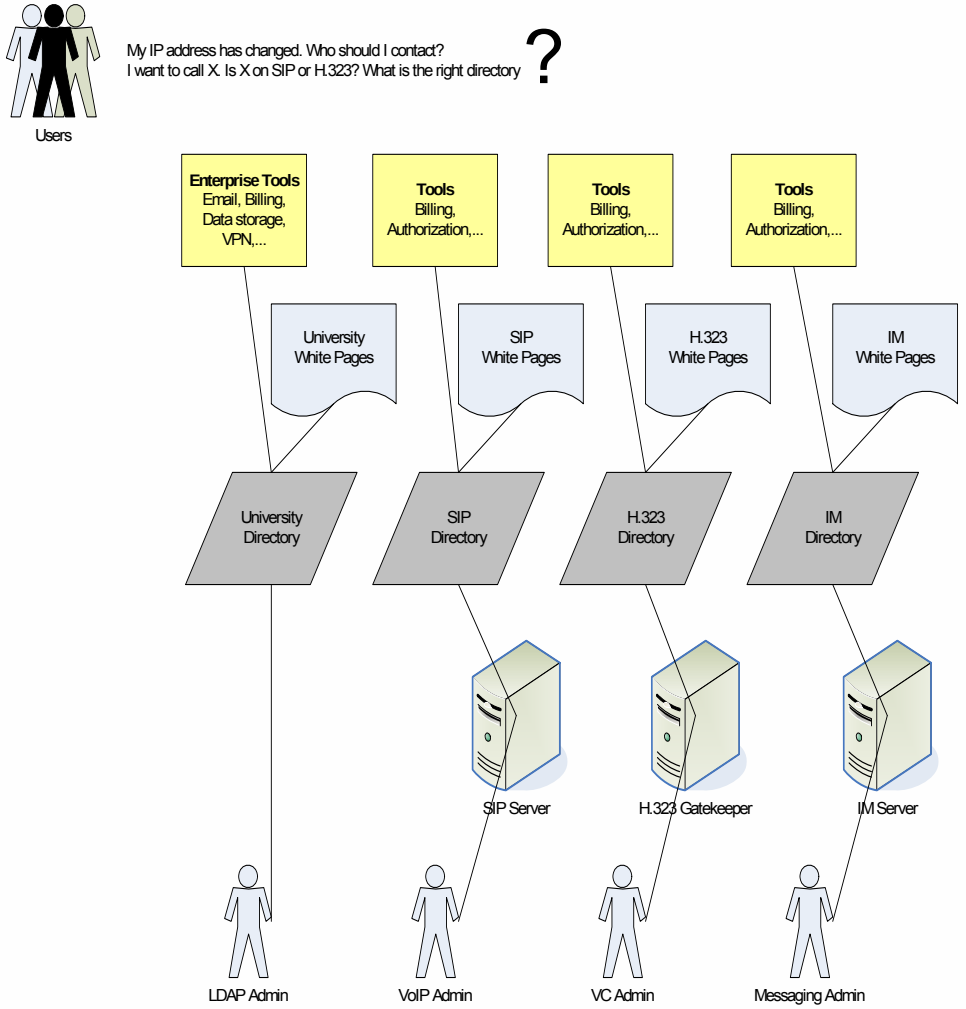
The Problem

- User management and information management is a big issue, once the deployment scales up
  - Need for new Gatekeeper/SIP Proxy entries
  - Update of white pages
  - Reliable billing?
  - Get the ‘working’ configuration for an endpoint
- Resource discovery
  - How do I find users and their endpoints?
    - Is it an H.323 endpoint, a SIP endpoint or something else?
  - How do I find MCUs and Gateways?

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The Problem

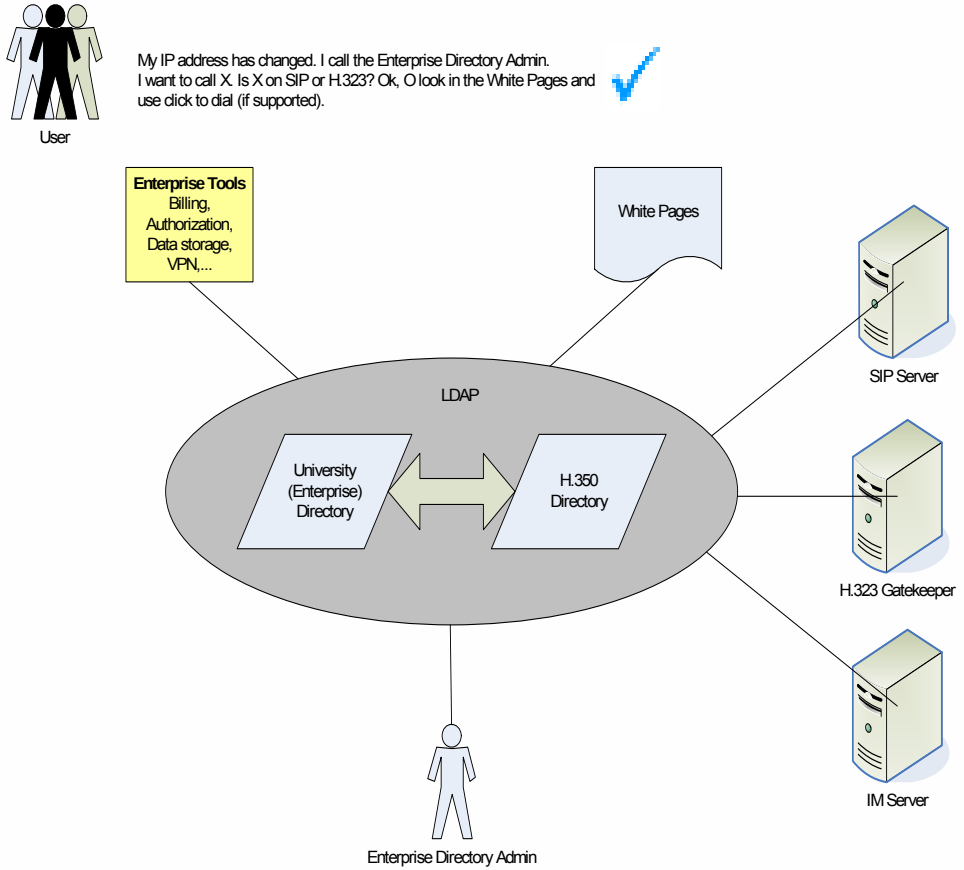
- Redundant information and processes if:
  - A user has entries in more than one directory
- Confuses the user and external parties who need some information
  - Who is the right contact?
- Billing?



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The Solution

- ONLY one ‘directory’ stores all the information, credentials, etc.
- Information is consistent and available → no confusion: where to find what
  - Canonical information
    - Impossible to handle several directories, especially for large scale environments
- No redundancy of tools necessary
  - Billing
  - …



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The Solution

- Enterprise Directory
  - Many Universities/Organizations/Institutions already have a centralized LDAP server
  - Stores information about people associated with institutions
  - Just ONE list → duplicate entries resolved
  - Advantages
    - Correct and current
    - Single place to disable account
    - Single place to change a password
    - …

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The Solution

- LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol)
- Protocol describes message to access data
- Standarzied data model (schemas) for data naming and organization for global unique naming
- Derived from OSI X.500
- LDAP V.3 (IETF RFC3377) includes security enhancements (SSL, TLS, …)
- Centralized name space and identity management
- Flexible and fast (although specialized)
- Can be used for White Pages, Authentication, User/Account management, Endpoint management

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The Solution

- Advantages of a standardized identity management
  - Vendor platform can be changed → Multi vendor service
  - Integration of more than just audio/video (e.g. email, web)
- Leverage existing identity management tools
  - LDAP tools are stable, well developed (due to its 'long' existence, flexible, open (many OpenSource products))

History of H.350

- The Video Middleware working group ‘vidmid-vc’ developed the idea for directory enabled audio/video
- The project was funded by an NSF grant given to the University of Alabama and partners such as CGU, SURFnet, University of North-Carolina Chapel Hill, and RADVISION
- The architecture was proposed to the ITU-T, accepted and ratified as H.350 standard in August 2003

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

Why H.350?

- Today's audio and video applications lack the ability of retrieving their configuration, phonebook, etc. automatically
  - All endpoints need to know an initial IP address of a Gatekeeper, Proxy or Gateway
- Unreliable authentication
  - Who is calling me?
- No authorization
  - (Usually) all user have the same rights
- No security
  - This has been improved over the last year by introducing AES/DES encryption to the endpoints

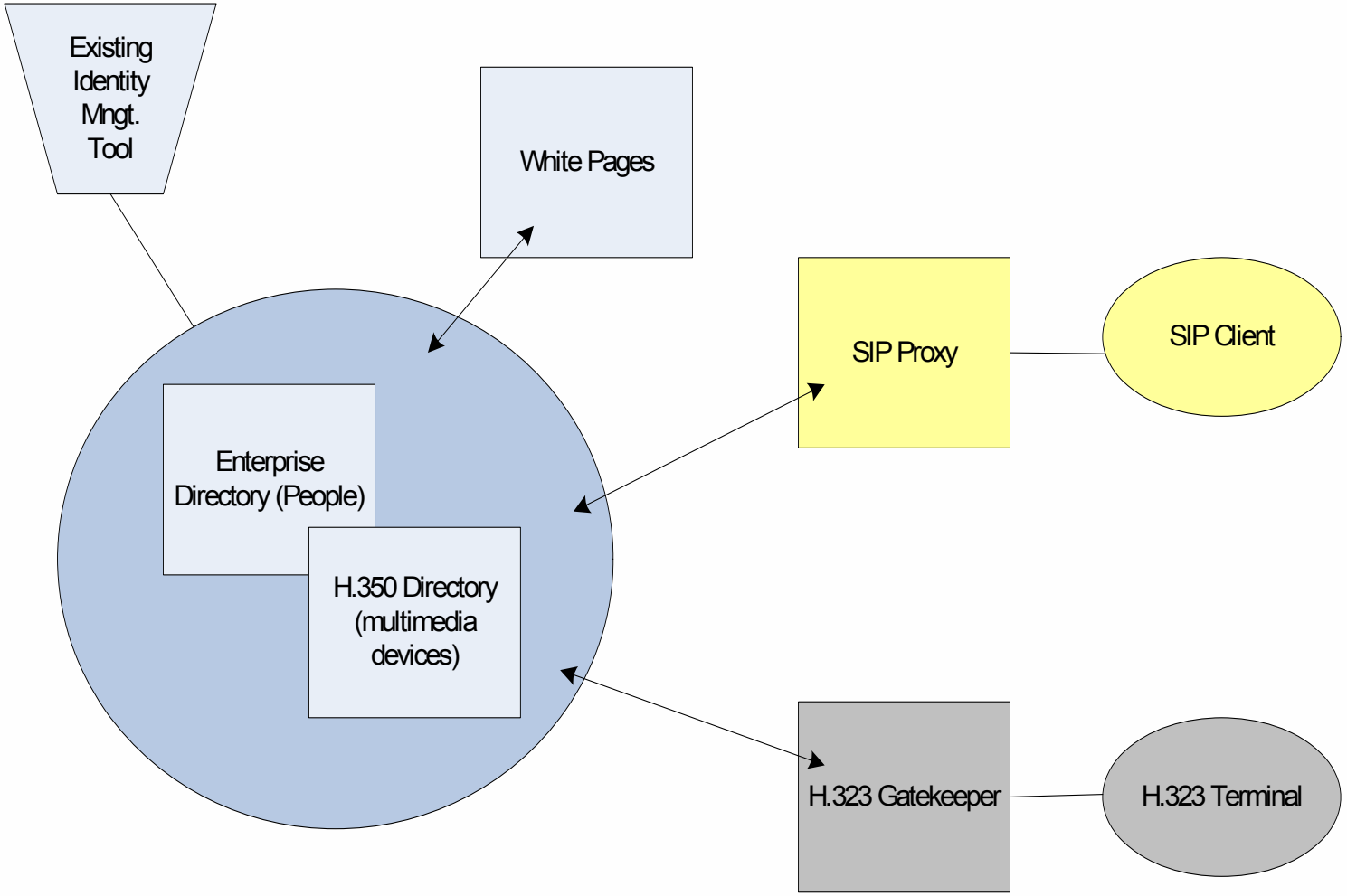
aarnet Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

Why H.350?

- H.350 was designed to support
  - Association of endpoints to users
  - Local/global White Page including search functionality
  - Centralized data storage rather than distributed redundant data distribution over several servers
    - What if a user has a H.323 endpoint, a SIP phone and an IM client?
  - Auto-load of the configuration for the endpoint
  - High scalability
  - 'Lightweight' impact on enterprise directory

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The Architecture



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

What is H.350?

- H.350 is
  - An LDAP scheme
  - Standardized way to store information
  - Basic elements are defined
  - Extensible and scalable
    - It works well for large networks, e.g. 20000+ user
    - Proprietary elements can be included
  - Multi-protocol enabled
    - SIP
    - H.323
    - H.320
    - Generic Protocols (mpeg2 en/decoder)
    - …
- H.350 is not
  - A protocol
  - Just for H-Series protocols

aarnet Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

What is H.350?

- H.350 – Directory services architecture for multimedia conferencing
  - Base architecture
- H.350.1 – Directory services architecture for H.323
- H.350.2 – Directory services architecture for H.235
- H.350.3 – Directory services architecture for H.320
- H.350.4 – Directory services architecture for SIP
- H.350.5 – Directory services architecture for non-standard protocols
- H.350.6 – Directory services architecture for call forwarding and preferences
- H.350.7 – Directory services architecture for Presence information (XMPP)
- H.350 Implementers Guide

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

H.350 and Presence

- "*sip.edu (an Internet2 project) uses presence and didn't think much of H.350….until they scaled up their service and decided configuration storage and auto-configuration were 'good things*'" E. Verharen, SURFnet

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How does H.350 work?

- Each user in the enterprise directory consists of several attributes
  - inetOrgPerson (enhanced by eduperson.schema)
    - Name
    - Address
    - Telephone
    - Email
    - Organization
    - Organization Unit
  - RFC1274
    - userPassword
- Using H.350, the existing user gets a new attribute, the commURI
  - commURI is a pointer to a structure in the commObject (→ next slide)

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How does H.350 work?

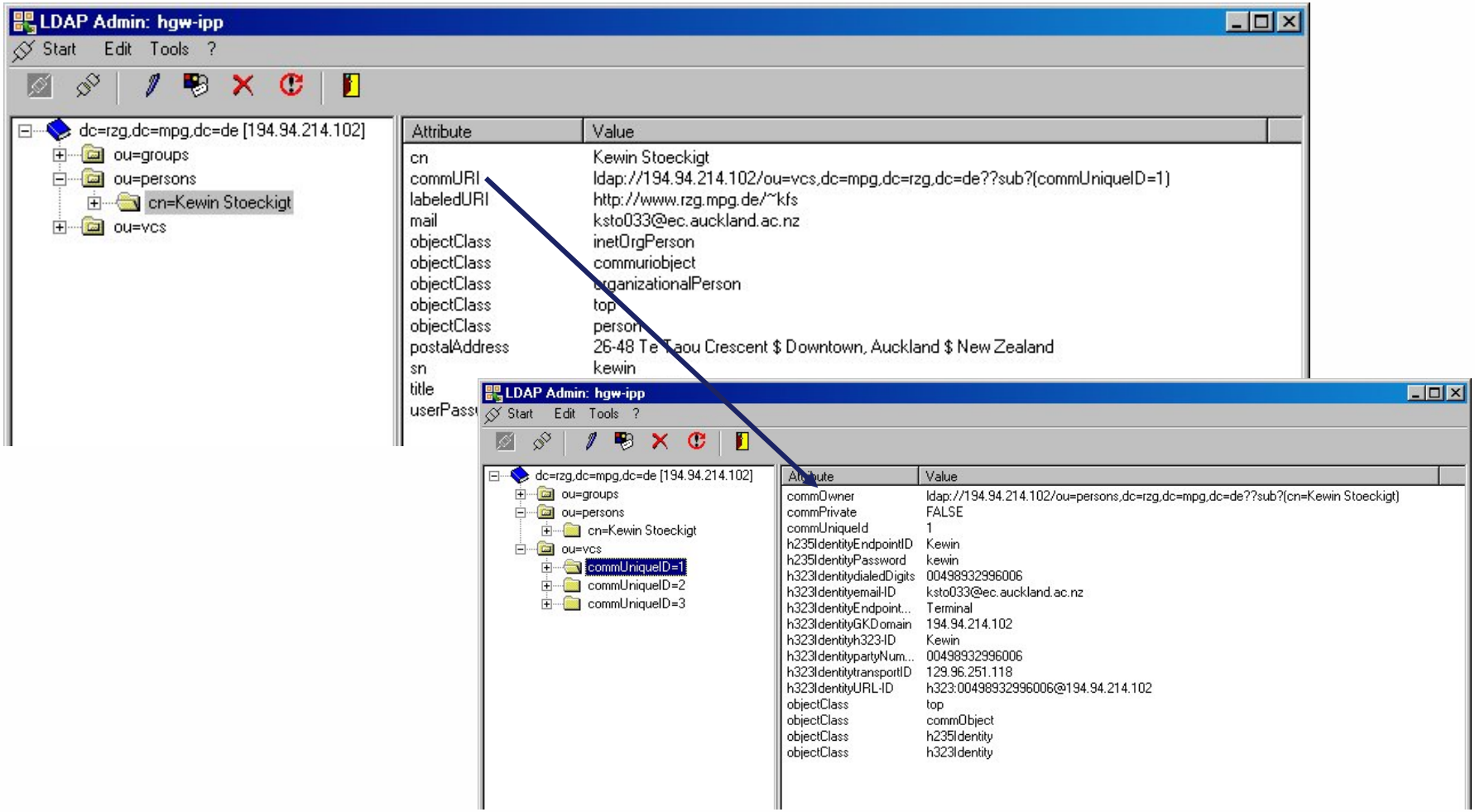
- **Enterprise Directory**
  - inetOrgPerson
    - Name (dn)
    - Address
    - Telefphone
    - Email
    - Organization
    - Organizational unit
    - commURI
  - RFC
    - userPassword

- **H.350 Directory**
  - commObject
    - commUniqueID
    - commOwner
    - commPrivate
  - SIPidentity
    - SIPIdentitySIPURI
    - SIPIdentityRegistrarAddress
    - SIPIdentityemailProxyAddress
    - SIPIdentityAddress
    - SIPIdentityPassword
    - SIPIdentityUsername
    - SIPIdentityServiceLevel

They reference each other using ‘pointer’

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

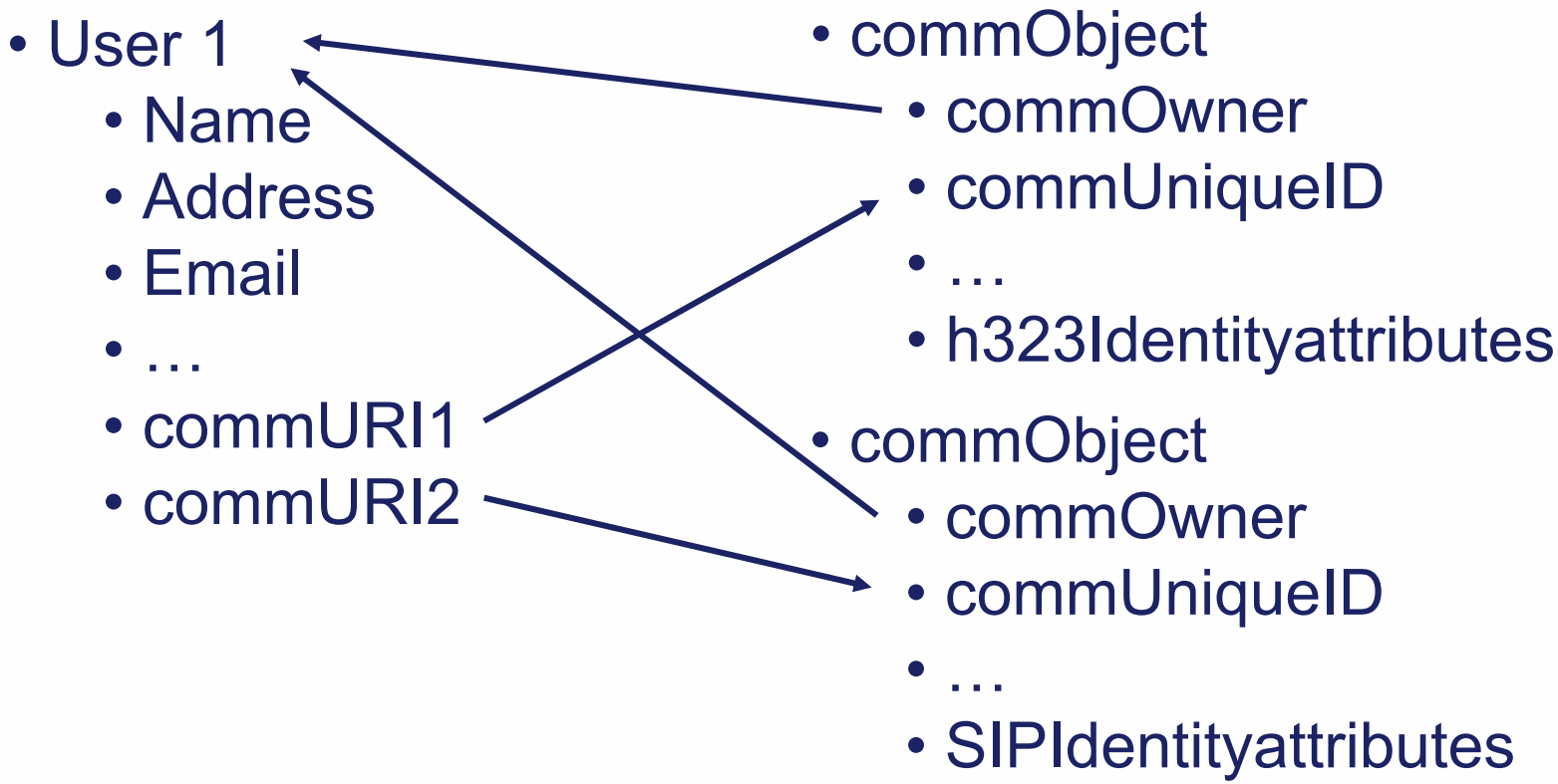
How does H.350 work?



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How does H.350 work?

- The relation commURI ↔ commUniqueID is highly flexible, because a user can have multiple commURIs'
  - One user (account) : multiple devices



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How does H.350 work?

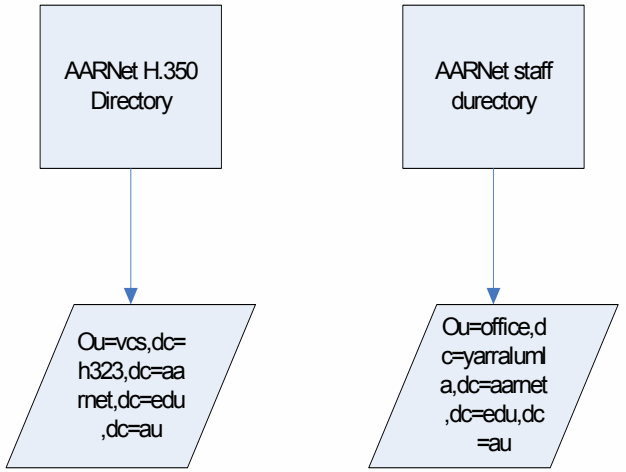
- The architecture and the use of LDAP makes H.350 ready for a flexible deployment
  - Enterprise and H.350 directory can be on the same LDAP, but in different branches (e.g. Flinders University, Videnet)
  - Enterprise and H.350 directory can be two different administered domains (AARNet, UAB)
    - Enterprise directory needs just the commURI

ldap://<ip|dns-name>/<ldapDN>??sub(commUniqueID=X)>

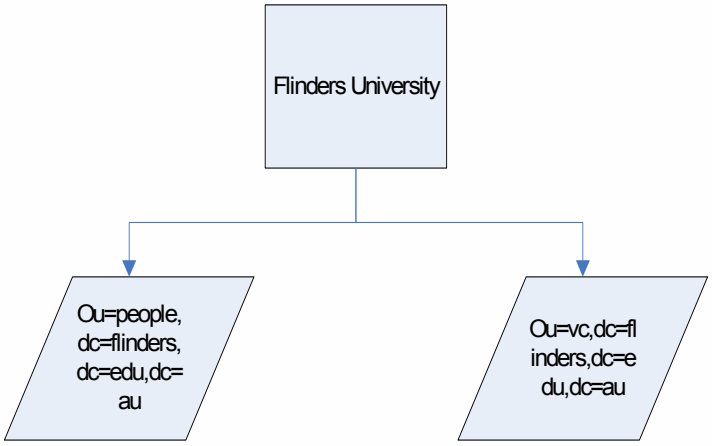
Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How does H.350 work?

- Two different domains



- One LDAP domain, but two different branches



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How does H.350 work?

- Call forwarding and preferences (H.350.6)
  - The URI points to a forwarding address
  - A label specifies the type of forwarding and the waiting time until the call is forwarded
  - Possible types of forwards
    - A different number
    - mailto:
    - A web form
    - …

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How does H.350 work?

- What about rooms?
  - The problem with room is, who should authenticate?
    - The device
    - The conference moderator
    - Everyone in the conference
    - All of the above

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How is H.350 currently used?

Enterprise Directory

H.323 Directory Service

Jill B Gemmill

Phonebook alias:	jgemmill
Internet Email address:	JGemmill@uab.edu
University department:	Academic Computing
University job title:	Asst Dir Academic Computing
Physical location of office:	Administration Building AB 719
Paper mail address of office:	1530 3RD AVE S BIRMINGHAM AL 35294-0107
Office telephone number:	(205) 975-2850
Office hours:	9-6
Current project(s):	Internet2, Secure Internet videoconferencing, Grid Computing
Other colleges attended:	Antioch College
URL for WWW use:	http://www.dpo.uab.edu/~jgemmill/
Fraternity or sorority:	never have liked them much
Degrees earned:	B.A.; M.S. ; MSEE
UAB	ALUMNI

Multimedia contact info:

- [H323] My Desktop
- [H323] AB 7th Floor Room Unit
- [H323] Jill's Desktop

Phonebook UAB, J. Gemmill
http://www.uab.edu/phonebook

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How is H.350 currently used?

- White Pages at ‘My Videnet’
- Search functionality
  - A country wide search in Australia results in 16 unique users
    - University of Queensland
    - AARNet
    - University of Newcastle
    - Charles Darwin University
    - Swinburne University of Technology
    - …

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

How is H.350 currently used?

- Northwestern University
  - Large SIP client network
  - SER SIP Server (iptel.org)
- Large company in Germany with 200+ VCon endpoints and an MXM Gatekeeper
- AARNet
  - Deployment is on the way (I hope you join)
  - Country GK will use H.350 for endpoint authentication (~Q3/2005)

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

What are the advantages of H.350?

- H.350 enabled endpoints can
  - Lookup and retrieve their correct working configuration → Reduces the necessary user support
  - It does not matter what protocol (H.320/H.323/SIP/genereic) you use, and the vendor does not matter either, you always have the necessary data available in a well managed way
  - White Page search (click to dial if supported), retrieve phonebook, etc.
- If the endpoint also/only supports H.235, it can all the above mentioned

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

What are the advantages of H.350?

- A H.350 enabled Callserver can
  - Retrieve information from a canonical store
    - Solve manual input problem
    - Conversion to propriety format can be done on the fly
  - Use a XIdentityServiceLevel to provide different levels of authorization (no international calls, no use of PSTN, etc.)
  - Scale up Voice/Video operations

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

What Hardware/Software currently supports H.350?

- The H.350 schema are currently available for
  - OpenLDAP
  - Sun iPlanet
  - Novell LDAP
  - Microsoft Active Directory
- H.350 aware H.323 systems
  - Radvision Endpoint and Gatekeeper
  - GnuGK → I am going to talk about this later
  - VCon clients and MXM Gatekeeper
  - Aethra systems
- H.350 aware SIP systems
  - SIP user agent CGU (it's not available for download anymore)
  - SIP Proxy Server HCL
  - Northwestern University uses a Perl Script to interface between SER and H.350
- H.350 aware infrastructure management systems
  - Tandberg TMS 8.0

Resources about H.350

- ViDe H.350 cookbook (Current version 2.0)
  - Available in print, pdf and html
  - Contains detailed descriptions of H.350 as well as several configuration samples and tools

    A VERY VALUABLE SOURCE

- J. Gemmill, “H.323 and Approaches to Authentication”, http://www.dpo.uab.edu/%7Ejgemmill/Presentations/Year_2002/Internet2AUthNZ2002.pdf
- J. Gemmill, “Secure Videoconferencing”, http://www.vide.net/conferences/spr2003/presentations/day_one/jill_gemmill
- E. Verharen, “European VC services and GDS and H.350” http://www.carnet.hr/CUC/tnc-cuc2003/program/slides/s6a1.pdf
- K. Stoeckigt, E. Verharen, Slides from the Real-time communication workshop, 19th Apan Meeting, http://www.rzg.mpg.de/vc/docs/apan/
- K. Stoeckigt, “H.350: Everything OpenSource and solving the H.323 Firewall problem”, Internet2 Member Meeting, Arlington, USA, http://www.internet2.edu/

aarnet

Australia's Academic
and Research Network