

Recommendation H.350.4 Directory Services Architecture for SIP

Summary

This Recommendation describes an LDAP directory services architecture for multimedia conferencing using SIP. In particular, it defines an LDAP schema to represent SIP User Agents (UAs) on the network and associate those endpoints with users.

This Recommendation is intended to supplement the CommObject directory architecture as discussed in H.350, and not intended to be used as a stand-alone architecture. The implementation of this LDAP schema, together with the use of the H.350 CommObject architecture, facilitates the integration of SIP User Agents and conferencing devices into existing Enterprise Directories, thus allowing the user to perform white page lookups and access clickable dialling supported by SIP devices. The primary reasons for implementing this schema are identical to those listed in H.350 (the CommObject class definition) as they apply specifically to the use of SIP UAs.

Keywords

LDAP, Directory Services, H.323, H.320, H.235, SIP

Table of Contents

1	Scope	3
1.1	Extending the Schema	3
2	References.....	3
2.1	Normative References	3
2.2	Non-Normative References	4
3	Definitions	4
4	Abbreviations.....	5
5	Conventions	5
6	Object Class Definitions	5
6.1	SIPIIdentity	5
6.2	SIPIIdentitySIPURI	5
6.3	SIPIIdentityRegistrarAddress	6
6.4	SIPIIdentityProxyAddress	6
6.5	SIPIIdentityAddress.....	7
6.6	SIPIIdentityPassword.....	7
6.7	SIPIIdentityUserName.....	8
6.8	SIPIIdentityServiceLevel.....	9
7	SIPIIdentity LDIF Files	9
A	Annex A Indexing Profile.....	12
I	Electronic Attachment	13

Full text only in electronic version

1 Scope

This Recommendation describes an LDAP directory services architecture for multimedia conferencing using SIP. In particular, it defines an LDAP schema to represent SIP User Agents (UAs) on the network and associate those endpoints with users.

This Recommendation is intended to supplement the CommObject directory architecture as discussed in H.350, and not intended to be used as a stand-alone architecture. The implementation of this LDAP schema, together with the use of the H.350 CommObject architecture, facilitates the integration of SIP User Agents and conferencing devices into existing Enterprise Directories, thus allowing the user to perform white page lookups and access clickable dialling supported by SIP devices. The primary reasons for implementing this schema include those listed in H.350 (the CommObject class definition) as they apply specifically to the use of SIP UAs, and to facilitate vendors making SIP services more readily available to their users.

The Scope of this Recommendation includes recommendations for the architecture to integrate endpoint information for endpoints using SIP into existing enterprise directories and white pages.

The scope of this Recommendation does not include normative methods for the use of the LDAP directory itself or the data it contains. The purpose of the schema is not to represent all possible data elements in the SIP protocol, but rather to represent the minimal set required to accomplish the design goals enumerated in H.350.

Note that SIP provides well defined methods for discovering registrar addresses and locating users on the network. Some of the attributes defined here are intended for more trivial or manual implementations and may not be needed for all applications. For example, SIPIdentityRegistrarAddress and SIPIdentityAddress may not be needed for many applications, but are included here for completeness. Thus, SIPIdentitySIPURI is the primary attribute of interest that will be served out, especially for white page directory applications.

1.1 Extending the Schema

The SIPIdentity classes may be extended as necessary for specific implementations. See the base H.350 document for a discussion on schema extension.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation

2.1 Normative References

- ITU-T Recommendation H.350 (2003), *Directory Services Architecture for Multimedia Conferencing*.

- IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification*.
- IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.
- IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

2.2 Non-Normative References

- IETF RFC 3263 (2002), *Session Initiation Protocol (SIP): Locating SIP Servers*.
- Timothy A. Howes, PhD, Mark C. Smith, Gordon S. Good, New Riders Publishing (1999), ISBN: 1578700701, *Understanding And Deploying LDAP Directory Services*.
- Timothy A. Howes, PhD, Mark C. Smith, New Riders Publishing (1997), ISBN: 1578700000, *LDAP Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*.

3 Definitions

The following terms used throughout the document:

Client: a SIP client is a network device that initiates SIP requests and receives SIP responses on a network.

commObject: An LDAP object class defined in ITU-T H.350 that represents generic multimedia conferencing endpoints.

endpoint: a logical device that provides video and/or voice media encoding/decoding, and signalling functions. Examples include:

1. a group teleconferencing appliance that is located in a conference room
2. an IP telephone.
3. a software program that takes video and voice from a camera and microphone and encodes it and applies signalling using a host computer.

Note that from the perspective of most signalling protocols, gateways and MCUs are special cases of endpoints.

enterprise directory: A canonical collection of information about users in an organization. Typically this information is collected from a variety of organizational units to create a whole. For example, Human Resources may provide name and address, Telecommunications may provide the telephone number, Information Technology may provide the email address, etc. For the purposes of this architecture, it is assumed that an enterprise directory is accessible via LDAP.

gateway: A device that translates from one protocol to another. Often gateways translate between the IP network and the public switched voice network to allow integration of the two.

MCU: Multipoint Control Unit. A device capable of mixing audio/video from multiple endpoints to create a virtual meeting space.

Proxy Server, SIP Proxy: a server that acts as both a client and a server to make requests on behalf of another user agent. The primary role of a proxy server is to ensure that a request generated by a UA is passed to another entity that is closer to the destination user.

Registrar: a registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.

SIP URI: a type of Uniform Resource Identifier that identifies a communication resource in SIP. A SIP URI usually contains a user name and a host name and is similar in format to an email address.

User Agent (UA): a device that can function as both a user agent client and server.

White Pages: An application that allows end users to look up the address of another user.

4 Abbreviations

LDAP: Lightweight Directory Access Protocol as defined in RFC 3377.

5 Conventions

In this Recommendation, the following conventions are used:

"Shall" indicates a mandatory requirement.

"Should" indicates a suggested but optional course of action.

"May" indicates an optional course of action rather than a recommendation that something take place.

References to clauses, sub clauses, annexes and appendices refer to those items within this Recommendation unless another specification is explicitly listed.

6 Object Class Definitions

The SIPIdentity object class represents SIP User Agents (UAs). It is an auxiliary class and is derived from the commObject class, which is defined in the ITU-T H.350 Recommendation.

6.1 SIPIdentity

```
OID: 0.0.8.350.1.1.6.2.1
objectclasses: (0.0.8.350.1.1.6.2.1
NAME 'SIPIdentity'
DESC 'SIPIdentity object'
SUP top AUXILIARY
MAY ( SIPIdentitySIPURI $ SIPIdentityRegistrarAddress $
    SIPIdentityProxyAddress $ SIPIdentityUserName $
    SIPIdentityPassword $ SIPIdentityServiceLevel $
    userSMIMECertificate )
)
```

6.2 SIPIdentitySIPURI

```
OID: 0.0.8.350.1.1.6.1.1
attributetypes: (0.0.8.350.1.1.6.1.1
NAME 'SIPIdentitySIPURI'
DESC 'Universal Resource Indicator of the SIP UA'
EQUALITY caseExactMatch
SUBSTR caseExactSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Application utility class

standard

Number of values

multi

Definition

Uniform Resource Identifier that identifies a communication resource in SIP- usually contains a user name and a host name and is often similar in format to an email address.

Permissible values (if controlled)

Notes

This URI may institute SIP or SIPS (secure). In the event that SIPS is instituted, the URI must reflect that it is using SIPS as opposed to SIP. See Examples below.

Semantics

Example applications for which this attribute would be useful

Online representation of most current listing of a user's SIP(S) UA.

Example

```
SIPIdentitySIPURI: sip:alice@foo.com // SIP example
SIPIdentitySIPURI: sip:alice@152.2.158.212 // SIP example
SIPIdentitySIPURI: sips:bob@birmingham.edu // SIPS example
```

6.3 SIPIdentityRegistrarAddress

```
OID: 0.0.8.350.1.1.6.1.2
attributetypes: (0.0.8.350.1.1.6.1.2
NAME 'SIPIdentityRegistrarAddress'
DESC 'specifies the location of the registrar'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Application utility class

Standard

Number of values

multi

Definition

Address for the domain to which the server that handles REGISTER requests and forwarding to the location server for a particular domain belongs.

Permissible values (if controlled)

Notes

Note that RFC 3261 states that user agents can discover their registrar address by configuration, using the address-of-record, or by multicast. The first scenario, by configuration, is noted as out of scope for RC 3261. This attribute may be used for the first scenario. It can be accomplished manually, (e.g. a web page that displays a user's correct registrar address) or automatically with an H.350.4 aware user agent.

Semantics

Example applications for which this attribute would be useful

white pages, a web page that displays a user's correct configuration information.

Example (LDIF fragment)

```
SIPIdentityRegistrarAddress: 152.2.15.22 //IP address example
SIPIdentityRegistrarAddress: sipregistrar.unc.edu //FQDN example
```

6.4 SIPIdentityProxyAddress

```
OID: 0.0.8.350.1.1.6.1.3
attributetypes: (0.0.8.350.1.1.6.1.3
NAME 'SIPIdentityProxyAddress'
DESC 'Specifies the location of the SIP Proxy'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Application utility class

Standard

Number of values

multi

Definition

Address which specifies the domain location of SIP proxy within a domain. RFC 3261 defines the role of the SIP proxy.

Permissible values (if controlled)

Notes

SIP User Agents are not REQUIRED to use a proxy, but will in many cases.

Semantics

Example applications for which this attribute would be useful

white pages, a web page that displays a user's correct configuration information.

Example (LDIF fragment)

```
SIPIIdentityProxyAddress: 172.2.13.234 //IP address example
SIPIIdentityProxyAddress: sipproxy.unc.edu //FQDN example
```

6.5 SIPIIdentityAddress

```
OID: 0.0.8.350.1.1.6.1.4
attributetypes: (0.0.8.350.1.1.6.1.4
NAME 'SIPIIdentityAddress'
DESC 'IP address or FQDN of the UA'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Application utility class

standard

Number of values

multi

Definition

Specifies the IP address or fully qualified domain name of the UA.

Permissible values (if controlled)

Notes

This attribute may be useful for applications in which UA to UA communication is direct, not involving a proxy or registrar.

Example applications for which this attribute would be useful

A web page that displays a user's proper user agent configuration information.

Example (LDIF fragment)

```
SIPIIdentityAddress: 152.2.121.36 // IP address example
SIPIIdentityAddress: ipPhone.foo.org // FQDN example
```

6.6 SIPIIdentityPassword

```
OID: 0.0.8.350.1.1.6.1.5
attributetypes: (0.0.8.350.1.1.6.1.5
NAME 'SIPIIdentityPassword'
```

```
DESC 'The user agent SIP password '  
EQUALITY octetStringMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

Application utility class

Standard

Number of values

multi

Definition

The SIP user agent's password, used for the HTTP digest authentication scheme as defined in RFC 2617.

Permissible values (if controlled)

Notes

Because RFC 2069, which was made obsolete by RFC 2617, was used as the basis for HTTP Digest in RFC 2543, any SIP servers supporting RFC 2617 must ensure backward compatibility with RFC 2069.

This SIPIdentityUserName, together with SIPIdentityPassword, are reserved for the purpose of use with Digest Access Authentication, and not intended for use with Basic Authentication methods.

LDAP provides one method to store user passwords for reference. If passwords are stored in LDAP it makes the LDAP server a particularly valuable target for attack. Implementers are encouraged to exercise caution and implement appropriate security procedures such as encryption, access control, and transport layer security for access to this attribute.

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

```
SIPIdentityPassword: 36zxJmCIB18dM0FVAj
```

6.7 SIPIdentityUserName

```
OID: 0.0.8.350.1.1.6.1.6  
attributetypes: (0.0.8.350.1.1.6.1.6  
NAME 'SIPIdentityUserName'  
DESC 'The user agent user name.'  
EQUALITY caseIgnoreMatch  
SUBSTR caseIgnoreSubstringsMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Application utility class

Standard

Number of values

multi

Definition

The SIP user agent's user name, used for the HTTP digest authentication scheme as defined in RFC 2617.

Permissible values (if controlled)

Notes

Because RFC 2069, which was made obsolete by RFC 2617, was used as the basis for HTTP Digest Authentication in RFC 2543, any SIP servers supporting HTTP Digest Authentication as defined in RFC 2617 must ensure backward compatibility with RFC 2069.

This SIPIdentityUserName, together with SIPIdentityPassword, are reserved for the purpose of use with Digest Access Authentication, and not intended for use with Basic Authentication methods.

Note that in many cases the user name will be parsed from the user@proxy.domain portion of the SIP URI. In that case it may not be necessary to populate this attribute.

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

```
SIPIdentityUserName: nelkhour
```

6.8 SIPIdentityServiceLevel

OID: 0.0.8.350.1.1.6.1.7

attributetypes: (0.0.8.350.1.1.6.1.7

NAME 'SIPIdentityServiceLevel'

DESC 'To define services that a user can belong to.'

EQUALITY caseIgnoreIA5Match

SUBSTR caseIgnoreIA5SubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.26)

Application utility class

Standard

Number of values

multi

Definition

This describes the level of services a user can belong to.

Permissible values (if controlled)

Notes

This attribute does not represent a data element found in SIP. SIP itself does not support distinctions in service levels. Instead, this attribute provides a mechanism for the storage of service level information directly in LDAP. This mapping allows service providers to adapt to an existing LDAP directory without changing the values of the SIPIdentityServiceLevel instances in the directory.

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

```
SIPIdentityServiceLevel: premium
```

7 SIPIdentity LDIF Files

This section contains a schema configuration file for SIPIdentity that can be used to configure an LDAP server to support this class

```
# SIPIdentity Object Schema
```

```
#
# Schema for representing SIPIdentity Object in an LDAP Directory
#
# Abstract
#
# This document defines the schema for representing SIPIdentity
# object in an LDAP directory [LDAPv3]. It defines schema elements
# to represent an SIPIdentity object [SIPIdentity].
#
#           .1 = Communication related work
#           .1.6 = SIPIdentity
#           .1.6.1 = attributes
#           .1.6.2 = objectclass
#           .1.6.3 = syntax
#
#
# Attribute Type Definitions
#
#   The following attribute types are defined in this document:
#
#   SIPIdentitySIPURI
#   SIPIdentityRegistrarAddress
#   SIPIdentityProxyAddress
#   SIPIdentityAddress
#   SIPIdentityPassword
#   SIPIdentityUserName
#   SIPIdentityServiceLevel
dn: cn=schema
changetype: modify
#
# if you need to change the definition of an attribute,
#           then first delete and re-add in one step
#
# if this is the first time you are adding the SIPIdentity
# objectclass using this LDIF file, then you should comment
# out the delete attributetypes modification since this will
# fail. Alternatively, if your ldapmodify has a switch to continue
# on errors, then just use that switch -- if you're careful
#
delete: attributetypes
attributetypes: (0.0.8.350.1.1.6.1.1 NAME 'SIPIdentitySIPURI' )
attributetypes: (0.0.8.350.1.1.6.1.2 NAME 'SIPIdentityRegistrarAddress' )
attributetypes: (0.0.8.350.1.1.6.1.3 NAME 'SIPIdentityProxyAddress' )
attributetypes: (0.0.8.350.1.1.6.1.4 NAME 'SIPIdentityAddress' )
attributetypes: (0.0.8.350.1.1.6.1.5 NAME 'SIPIdentityPassword' )
attributetypes: (0.0.8.350.1.1.6.1.6 NAME 'SIPIdentityUserName' )
attributetypes: (0.0.8.350.1.1.6.1.7 NAME 'SIPIdentityServiceLevel' )
-
#
# re-add the attributes -- in case there is a change of definition
#
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.6.1.1
  NAME 'SIPIdentitySIPURI'
  DESC 'Universal Resource Indicator of the SIP UA'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.6.1.2
```

```
NAME 'SIPIdentityRegistrarAddress'
DESC 'specifies the location of the registrar'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.6.1.3
NAME 'SIPIdentityProxyAddress'
DESC 'Specifies the location of the SIP Proxy'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.6.1.4
NAME 'SIPIdentityAddress'
DESC 'IP address of the UA'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.6.1.5
NAME 'SIPIdentityPassword'
DESC 'The user agent SIP password '
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
attributetypes: (0.0.8.350.1.1.6.1.6
NAME 'SIPIdentityUserName'
DESC 'The user agent user name.'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.6.1.7
NAME 'SIPIdentityServiceLevel'
DESC 'To define services that a user can belong to.'
EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
-
# Object Class Definitions
#
# The following object class is defined in this document:
#
# SIPIdentity
#
# SIPIdentity
#
delete: objectclasses
objectclasses: (0.0.8.350.1.1.6.2.1 NAME 'SIPIdentity' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.6.2.1
NAME 'SIPIdentity'
DESC 'SIPIdentity object'
SUP top AUXILIARY
MAY ( SIPIdentitySIPURI $ SIPIdentityRegistrarAddress $
SIPIdentityProxyAddress $ SIPIdentityAddress $
SIPIdentityPassword $ SIPIdentityUserName $
SIPIdentityServiceLevel $ userSMIMECertificate )
)
-
#
# end of LDIF
#
```

Annex A: Indexing Profile

A Annex A Indexing Profile

Indexing of attributes is an implementation-specific activity and depends upon the desired application. Non-indexed attributes can result in search times sufficiently long to render some applications unusable. Notably, user and alias lookup should be fast. The Annex A Indexing Profile describes an indexing configuration for SIPIdentity directories that will be optimised for use in directory of directories applications. Use of this profile is optional.

SIPIdentitySIPURI: equality

SIPIdentityRegistrarAddress: no recommendation

SIPIdentityProxyAddress: no recommendation

SIPIdentityAddress: equality

SIPIdentityUserName: equality

SIPIdentityPassword: no recommendation

SIPIdentityServiceLevel: equality

Appendix I Electronic Attachment

I Electronic Attachment

The attached file `sipIdentity.ldif.txt` contains a text only version of the LDIF file described in section 7.



`sipIdentity.ldif.txt`
