STANDARDS AND INFORMATION DOCUMENTS

Call for comment on DRAFT AES standard for audio applications of networks - Requirements for Media Network Directories and Directory Services

This document was developed by a writing group of the Audio Engineering Society Standards Committee (AESSC) and has been prepared for comment according to AES policies and procedures. It has been brought to the attention of International Electrotechnical Commission Technical Committee 100. Existing international standards relating to the subject of this document were used and referenced throughout its development.

Address comments by E-mail to standards@aes.org, or by mail to the AESSC Secretariat, Audio Engineering Society, PO Box 731, Lake Oswego OR 97034. **Only comments so addressed will be considered**. E-mail is preferred. **Comments that suggest changes must include proposed wording.** Comments shall be restricted to this document only. Send comments to other documents separately. Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

This document will be approved by the AES after any adverse comment received within **six weeks** of the publication of this call on http://www.aes.org/standards/comments/, **2019-10-09** has been resolved. Any person receiving this call first through the *JAES* distribution may inform the Secretariat immediately of an intention to comment within a month of this distribution.

Because this document is a draft and is subject to change, no portion of it shall be quoted in any publication without the written permission of the AES, and all published references to it must include a prominent warning that the draft will be changed and must not be used as a standard.

The AES Standards Committee is the organization responsible for the standards program of the Audio Engineering Society. It publishes technical standards, information documents and technical reports. Working groups and task groups with a fully international membership are engaged in writing standards covering fields that include topics of specific relevance to professional audio. Membership of any AES standards working group is open to all individuals who are materially and directly affected by the documents that may be issued under the scope of that working group.

Complete information, including working group scopes and project status is available at http://www.aes.org/standards. Enquiries may be addressed to standards@aes.org

The AES Standards Committee is supported in part by those listed below who, as Standards Sustainers, make significant financial contribution to its operation.

Standards Sustainer Gold

NETFLIX, Focusrite, DOLBY

Standards Sustainer Silver

LECTROSONICS, 21ST CENTURY FOX, Audio precision, WAVES, SHURE, fulcrum ACOUSTIC, ROSS LIVING LIVE!, Eventide, PreSonus, ADAMSON, THE TELOS ALLIANCE, SENNHEISER, BOSE, MUSIC TRIBE

Standards Sustainer

NHK, NTi AUDIO, MQA, audio-technica, CLAIR, WEISS, LAWO, AEA, USOUND, THAT Corporation, NBCUniversal, Control4, WorldCast Systems, Fraunhofer IIS, PRO AUDIO TECHNOLOGY, MERGING, RAVENNA, steinberg, XPERI, ATTERO TECH, HARMAN, KLIPPEL, NEUTRIK, dbx-tv

This list is current as of 2019/9/30

AES standard for audio applications of networks - Requirements for Media Network Directories and Directory Services

Published by
Audio Engineering Society, Inc.

Abstract

This document sets forth technical recommendations for media network directories and directory-related services and mechanisms such as network discovery. It is hoped that this document will inform future industry directory and directory services standards that cover at least the following topics:

1. Registration, query, and administration protocols;
2. Security mechanisms;
3. Directory data model;
4. Query language and related semantics; and
5. Scalability strategies.

Audio Engineering Society Inc. 551 Fifth Avenue, Room 1225, New York, NY, US.
www.aes.org/standards - standards@aes.org

2019-12-16 printing

Contents

Foreword

This foreword is not part of this document, AES74, *AES standard for audio applications of networks - requirements for Media Network Directories and Directory Services.*

A media network contains two primary sets of services: (1) a *media transport set*, which is responsible for transporting synchronous media samples, and a (2) *system control set*, which is responsible for the remote control of devices and the control of media transport traffic.

These primary service sets require at least two support services: (a) a *time* service, which allows synchronization of samples between devices, and (b) a *directory*, which allows devices, device services, and media streams to be recorded in a common database that may be queried as required for network operation.

This standard specifies a set of functional requirements for media network directories in professional audio applications in the fields of sound reinforcement, public address, sound recording, electronic music, broadcasting, and cinema. The standard does not address consumer, automotive, or telecommunications applications.

The principal writing group members who contributed to this document were: F. Bergholtz, R. Cabot, J. Berryman, S. Jones, A. Kuzub, M. Lave, G. Linis, S. Price, A. Rosen, S. Scott, G. Shay, M. Smaak, P. Stevens, P. Treleaven, and P. Waddell. Additional contributions were received from the OCA Alliance Technical Committee and SMPTE TC34cs.

J. Berryman led the writing group.

Morten Lave
Chair, working group SC-02-12

2019-10-28

Note on normative language

In AES standards documents, sentences containing the word “shall” are requirements for compliance with the document. Sentences containing the verb “should” are strong suggestions (recommendations). Sentences giving permission use the verb “may”. Sentences expressing a possibility use the verb “can”.

AES standard for Audio applications of networks - Requirements for Media Network Directories and Directory Services

0. Introduction

0.1. General

This document specifies technical requirements for media network directories and directory-related services. It has been compiled from various sources, and the contents have been offered for public comment via a Call for Comment document first circulated by the AES in 2017.

Media network directories are application-layer mechanisms that collect, store and disseminate information about devices, application services, and other elements of media networks. They are used for connection management, network supervision, and other purposes.

0.2. Document conventions

Numerical values are decimal unless otherwise stated.

A `Courier typeface` is used to identify programmatic names to distinguish them from regular text.

Where a term is first introduced in body text, the term will be set in an *italic typeface*.

When references are cited in the text they are [enclosed in brackets].

1. Scope

The requirements given here address the following aspects of media network directories:

This document is a requirements guide. It does not specify implementation design.

- Data model;
- Registration;
- Querying;
- Administration;
- Scalability;
- Security.

The scope of this document excludes directory service implementation architectures, application protocols for accessing the Directory data, and internal mechanisms the services may use to maintain the directory data.

Also excluded is connection management. In this context, "connection management" means the protocols and processes in a media network by which signal flows are set up, monitored, and taken down. Although directories are *used* by connection management, connection management mechanisms themselves are outside this document's scope.

2. Normative references

AES67 *AES67-2015: AES standard for audio applications of networks - High-performance streaming audio-over-IP interoperability.* Audio Engineering Society (AES), 2015.

RFC 1034 *Domain Names - Concepts and Facilities*. Internet Engineering Task Force (IETF), 1987.

RFC 1035 *Domain Names - Implementation and Specification*. Internet Engineering Task Force (IETF), 1987.

RFC 2131 *Dynamic Host Configuration Protocol.* Internet Engineering Task Force (IETF), 1997.

RFC 2606 *Reserved Top Level DNS Names*. Internet Engineering Task Force (IETF), 1999.

RFC 2782 *A DNS RR for specifying the location of services (DNS SRV).* Internet Engineering Task Force (IETF), 2000.

RFC 2818 *HTTP Over TLS*. Internet Engineering Task Force (IETF), 2000.

RFC 3986 *Uniform Resource Identifier (URI): Generic Syntax.* Internet Engineering Task Force (IETF), 2005

RFC 4566 *SDP: Session Description Protocol*. Internet Engineering Task Force (IETF), 2006

RFC 6455 *The WebSocket Protocol***.** Internet Engineering Task Force (IETF), 2011

RFC 6762 *Multicast DNS*. Internet Engineering Task Force (IETF), 2013.

RFC 7230 *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.* Internet Engineering Task Force (IETF), 2014.

RFC 7231 *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.* Internet Engineering Task Force (IETF), 2014

RFC 7232 *Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests*. Internet Engineering Task Force (IETF), 2014.

RFC 7233 *Hypertext Transfer Protocol (HTTP/1.1): Range Requests.* Internet Engineering Task Force (IETF), 2014.

RFC 7234 *Hypertext Transfer Protocol (HTTP/1.1): Caching*. Internet Engineering Task Force (IETF), 2014.

RFC 7235 *Hypertext Transfer Protocol (HTTP/1.1): Authentication.* Internet Engineering Task Force (IETF), 2014

RFC 8259 *The JavaScript Object Notation (JSON) Data Interchange Format.* Internet Engineering Task Force (IETF), 2017.

XML Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C, 2008/11/26, https://www.w3.org/TR/2008/REC-xml-20081126/

MQTT Client Server publish/subscribe messaging transport protocol, version 5.0, 2019/03/07 Standard Organization for the Advancement of Structured Information Standards (OASIS), https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.docx

3. Definitions

3.1. Application Program Interface (API)

set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.

3.2. Application network

set of devices and related software elements interconnected by a data network for a common purpose.

3.3. Client

software component that interacts with a server.

3.4. Data network

telecommunications network for transport of digital data of various kinds. Synonym of "computer network".

3.5. Database

formally organized collection of data that allows query and update.

> Note: This document uses "database" in the abstract Computing Science sense, to mean a set of objects and operations defined by a schema. No particular database management system (e.g. MySQL) is expected or implied.

3.6. Deregister (entity)

delete an entity's entry from a directory.

3.7. Device

container for a logically-related set of functions within a networked media infrastructure, usually implemented by a physical device connected to the media network, or a software virtualization of such a device running on a computer connected to the media network.

3.8. Directory

database that contains directory entries.

3.9. Directory access protocol

network protocol that clients use to access directory services.

3.10. Directory service

network service that provides access to a directory.

3.11. Discovery

set of directory functions that support automation of directory updating. These functions typically include:

- Autonomous self-registration of entities;
- Automatic detection of new or departing entities;
- Support of persisting queries;
- Ongoing supervision and verification mechanisms to ensure that the directory data is always accurate.

Note: Some directory services do not offer discovery functions. .

3.12. Entity

functional element of a media network.

Note: Entities are described by directory entries. An entity can be a network host, or a software element running in a network host, or a network service, or some other element with an identity in the network. A directory is itself an entity.

3.13. Entity attribute

data value that is part of an entry. For example, entity name is an entity attribute.

3.14. Entity connection data

entity attributes that provide information used for making media network connections to the entity in question.

3.15. Entity name

unique name of an entity within a directory.

3.16. Entity name resolution

process by which entity name or entity path of an entity is used to retrieve its entity attributes, particularly its entity connection data.

3.17. Entity path

unique identifier of an entity within a hierarchy of nested directories. See 7.

3.18. Entity type

logical nature or function of an entity.

Note: Typical entities are: device, function within a device, media stream.

3.19. Entry

database record in a directory that describes an entity.

3.20. Media network

application network that communicates audio and video signals and related control, monitoring, data, and time-synchronization traffic.

3.21. Network service

network-attached set of software functions that can be used by clients, together with the policies that control its usage.

3.22. Persisting query

query that includes a subscription to subsequent changes involving entries that match the query.

Note 1: Persisting queries allow entities to maintain continuously accurate knowledge of a directory's population, or more precisely, knowledge of the subset of the population the subscriber cares about.

Note 2: Executing queries or persistent queries is sometimes called "browsing" in networking standards language.

3.23. Query

(noun) precise request for retrieving one or more entries from a directory.

(verb) apply a (noun) query.

3.24. Query language

specification that defines the syntax and semantics of a query.

3.25. Register (entity)

add an entity's entry to a directory.

3.26. Server

computing resource that runs one or more network services.

3.27. Simple media network

media network that operates entirely on a single subnet that is not shared with any other media network.

3.28. Subnet

logical, visible division of a data network. For IP networks, a subnet is an IP "broadcast domain", i.e. the set of IP nodes reachable by a single broadcast message from any of those nodes.

3.29. Subscription

a relationship between entities that provides automatic notifications to the initiating entity *("subscriber")* whenever query results change in the other entity *("subscribee")* .

4. Functionality

4.1. Registration / deregistration

It shall be possible for entities to be registered in, and deregistered from, the directory.

A directory should provide a networkAPI for registration of entities.

Each entity described by a directory shall have its own entry.

4.2. Querying

Querying may be used by:

- Any client that needs to identify and monitor the entities in the media network;
- Entities, in order to confirm their registration status;
- Media network management processes, for updating and reporting of entities and editing of other data such as security parameters and access permissions.

The directory service shall provide querying functions sufficient for all of these activities.

Different directory implementations may offer differing levels of query service, but in all cases, it shall be possible to retrieve sufficient information for communicating devices to attempt establishing connections with the entities involved.

Queries shall be expressed in a query language defined by the directory standard. The same language shall be used for all compliant implementations. However, the standard may define some query features as optional.

4.3. Subscriptions

The directory service may support subscription, a mechanism by which clients are automatically notified of directory additions, changes, and deletions. Subscriptions, if supported, may be added or deleted at any time, subject to access control restrictions, if any.

4.4. Persisting queries

The directory may support persisting queries. By definition, persisting queries include subscriptions that generate notifications for creation, modification, and deletion of entries that match the query.

4.5. Discovery

The directory service may support discovery. If supported, discovery:

1. Shall accept entity self-registration and de-registration;
2. Shall support queries;
3. Should support persisting queries, particularly including queries that detect entries added to or deleted from the Directory;
4. Should provide timely automatic detection of entity departure from the media network.

Note 1: The quantitative meaning of "timely" is an implementation decision.

Note 2: Automatic detection of entity departure will normally require either periodic probe messages to be issued by the directory service or periodic notifications to be issued by each registered entity. Design of such methods is an implementation decision.

4.6. Representational capability

The same directory services shall work for all kinds of entities, including media transport, connection management, and device control.

A directory shall be able to describe multiple entity types.

A compliant directory standard shall define:

- A schema that describes the complete set of standard entity types;
- The minimum subset of entity types a directory must be able to support in order to comply with the standard;
- A means by which implementations may extend the schema to support additional nonstandard entity types without compromising interoperability.

Directories shall offer flexible entity attribute support.

- Entity types shall be capable of providing entity attribute names and values that can clients can use for presentation or filtering of query results.
- The schema for an entity shall constitute the definition of its entity type.
- Entity type definitions shall be configurable by application network administrators.

5. Directory access

5.1. Directory services

Directories are accessed via directory services. A typical directory service will:

- implement standard directory data models and processing rules;
- publish one or more protocol interfaces;
- use entity names as defined by this document.

A given directory implementation may support multiple directory services. All of these directory services shall access the same directory database, but may provide alternative means of doing so.

Note: Examples of multiple directory services include:

1. Media network protocol architectures that specify multiple services for directory access. For example, NMOS defines separate directory services for registration and query;
2. Directories that must support legacy schemes (e.g. DNS-SD) alongside newer standards. In such cases, there may be different directory services for legacy and current clients.

5.2. Directory access protocols

A given directory service may support multiple directory access protocols to suit a variety of clients. These protocols may use various protocol logic rules, protocol data unit formats, data encodings, and data transport methods.

6. Coexistence of multiple directories

It should be possible for multiple directories to coexist within a given application network. The number of directories and what each one contains shall be implementation decisions, out of scope of this document.

7. Nested directories

A directory should allow registration of other directories as entities. A directory so registered is called a *nested directory*, and the directory holding the registration is called the *parent directory*. A directory in a chain of nested directories that ultimately leads to an entity is called an *ancestor* of that entity; the entity itself is called a *descendant* of all its ancestors.

No directory shall be registered in any of its descendants.

> Note: In common discourse, a nested directory may be described as being *contained by* its parent. The term "contained by" is metaphoric, and is not intended to reflect actual implementation structure. The nested directory's entry is contained in the parent, but the nested directory itself may reside anywhere on the media network.

7.1. Entity path

An unambiguous identifier of an entity may be constructed by prepending to the entity's name the set of names of its ancestors, starting with the entity name of the parent, proceeding to the left, and ending with the entity name of the outermost ancestor. Each element of the identifier shall be separated by a delimiter character. such an identifier shall be termed an *entity path*.

Entity path syntax shall be defined by the IETF URI scheme described in [RFC 3986]. The URI scheme has various options from which the final directory standard shall select.

An example entity path might be as follows:

```
ODA:/MyCompany/Operations/PagingSys/LoadingDock/Amp1
```

7.2. Multiple ancestry

Some directory implementations may allow entities to have more than one ancestry and hence more than one entity path. When entities are allowed to have multiple ancestries, the directory scheme is said to support *multiple ancestry*.

Whether to support multiple ancestry is a directory implementation decision that is outside the scope of this standard.

7.3. Entity name resolution

For entity name resolution, directory services shall provide various query functions, depending on the query specified, as follows:

- If the query specifies an entity path, a direct lookup shall be made in the designated directories as specified by the entity names in the entity path;
- If the query specifies only a simple entity name, a lookup in the client's parent directory shall be attempted; if it is not found there, the lookup shall fail;
- If the query specifies multiple entity attributes, the lookup shall generally proceed according to the rules of the query language.

8. Data network considerations

8.1. Data network type independence

Directory standards shall not assume a particular data network type (e.g. IP network), and shall include features that allow implementations to operate over a range of data network types, including use cases that include multiple data networks of differing kinds in a single application network.

8.2. Data network topology independence

Specific entity name and entity path values shall not depend on the topologies of the underlying data network infrastructures, and entity name and entity path values shall survive changes to addressing strategies and routing topologies of the data networks involved.

8.3. Minimal effect on infrastructure

Directory changes, including:

- adding/changing/deleting new directory entries; and
- adding/changing/deleting new media networks and their directories

should require minimal (ideally zero) infrastructure administration (e.g. IT department) activity.

Directory operations shall not compromise the integrity of the underlying data network infrastructure.

8.4. Shared data networks

A compliant directory standard shall allow for use cases in which multiple independent media networks owned by different organizational units share a common data network.

In such cases:

- The directories of the respective media networks shall function independently of each other;
- One media network's directory shall not be detectable or accessible by another media network's entities unless specific permissions to that effect have been granted;
- Given suitable permissions, an entity may be registered simultaneously in more than one directory;
- Adding and deleting entities and their directory entries shall be secure, straightforward, and not error-prone.

Note: When a directory implementation supports automatic self-registration of entities, and where multiple directories exist in the common data network, a mechanism will be required to ensure that each new entity joining the network registers itself in the correct directory or directories.

8.5. Discoverability

Directory services shall be discoverable by the normal service discovery mechanisms the data network provides.

9. Security and access control

9.1. Security

Security is an infrastructure mechanism that prevents harm, theft, and unauthorized use.

In practice, the level of security is an application decision. Directory services shall support security measures consistent with the overall application security level.

In a typical secure implementation:

- Directory service clients authenticate the directory service, i.e. to ensure that the addressed directory service is indeed the desired one;
- Directory services authenticate connected clients;
- Directory service traffic is safe from eavesdropping and tampering.

9.2. Access control

Directory services may provide access control features.

Access control determines the scope of user directory interactions that a given user may perform. A user may be a person, a device, or an instance of a software system.

Specific access control mechanisms and rules are application-dependent, and are out of scope of this standard.

10. Scalability

A directory should support:

- Both local and wide-area applications;
- Network populations ranging from two to many thousands of entities;
- Network infrastructures at all levels of complexity, ranging from simple single-subnet cases to complex cases with many subnets.

Plug-and-play, zero-administration operation shall not be required for larger networks.

Note 1: It is acknowledged that some directory implementations will forever be confined to small environments and need not be scalable. However, scalable designs should be used wherever possible, to forestall future integration problems.

Note 2: Polling implementations are strongly discouraged in all cases.

10.1. Performance

Quantitative directory service performance criteria may vary from application network to application network, but in general, directory service performance shall be satisfactory in the following functional areas:

- Distribution of an update to many persistent query subscribers;
- Servicing many simultaneous queries (this is particularly important for system startup);
- Recovering from loss of the active directory service.

In all cases, directory services shall be stable under extreme conditions, such as data network bandwidth deficiency, high data transmission error rates, and massive bursts of transaction traffic of all kinds.

10.2. Centralized and distributed implementations

A directory may be implemented in a centralized or distributed manner. In this context, "distributed" shall mean implemented in multiple physical sections usually stored in diverse network hosts.

The distribution of a directory shall generally be transparent to directory clients.

Implementation details of directory distribution are outside the scope of this document.

11. Reliability and robustness

It shall be possible to implement high-reliability directories sufficient to support life-safety and other mission-critical systems, and sufficient to be certified by safety authorities. Directory standards shall not prevent this.

High-reliability directory implementations should provide:

- Proactive methods for instability prevention;
- Reactive methods for recovery from existing instability;
- The ability to recover automatically from loss of the active directory.

Where directory redundancy is required, it is recommended that the solution be structured as a single directory with a redundant implementation, rather than as multiple sets of directories. Implementation redundancy should be invisible to directory service clients.

12. Ease of use

Setting up and managing directory services for simple media networks shall not require advanced network administration skills.

The directory standard may define, for simple media networks, a plug-and-play mode requiring zero pre-configuration by users and no dedicated directory server.

Annex A. (normative) IP-based directories

This Annex gives recommendations specifically for directories supporting media networks running on IP data networks.

A.1. Directory addressing

An IP-based directory service should :

- Be capable of operating with either IPv4 or IPv6 addressing;
- Use Dynamic Host Configuration Protocol (DHCP) (see [RFC 2131]) to determine its own IP address(es);
- Register its hostname(s) in the IP Domain Name Service (DNS) (see [RFC 1035]);
- Provide a service name that can be used to register DNS SRV records as per [RFC 2782].

A.2. Entity addressing

Entries in an IP-based directory should address their respective entities using hostnames, not specific IP addresses.

Note: Following this rule allows validity of Entries to survive a network reset.

A.3. Serverless operation

To support small networks that do not include server devices, directory implementations may offer a serverless option, in which entries are stored in devices in a distributed fashion, and directory operations are performed via multicasting. A common example of this approach is Multicast DNS ("mDNS") - see [RFC 6762].

A.4. Multiple directories in the same network

To avoid conflicts when multiple directory services share the same IP network, each directory service shall have a unique DNS domain, e.g.

- `directory1.example.com`
- `directory2.example.com`

Domains are described and defined in [RFC 1034], [RFC 1035] and [RFC 2606]..

A.5. Directory access protocol agility

Directory Services may be implemented that offer options for accessing directory data. Such services are described as being directory *access protocol agile*.

In this context, "directory access protocol" means a combination of a message transport protocol, an application protocol logic, and a data representation.

An access protocol agile directory service:

1. Shall provide a means for the client to indicate the directory access protocol it uses.
2. Shall provide a means to specify what directory access protocols are supported.

Message transport protocol options include:

- HTTP - see [RFC 7230-7235];
- HTTPS - see [RFC 2818];
- WebSocket - see [RFC 6455];
- MQTT- see [MQTT].

Data encoding options include:

- JSON - see [RFC 8259];
- XML - see [XML];
- A byte-efficient format of some kind.

A.6. SDP media profiles

Connection data in entries for entities that support Session Description Protocol (SDP) (see [RFC 4566]) shall include one or more recommended media profiles expressed as partial or full SDP documents.

Note: SDP is used by [ACIP] and [AES67].

Annex B. Bibliography

ACIP *EBU – TECH 3326: Audio contribution over IP*. European Broadcast Union (EBU), 2008.