ANSI/TIA-1057- 2006
Approved: April 6, 2006

TIA STANDARD

Telecommunications

IP Telephony Infrastructure

Link Layer Discovery Protocol for Media Endpoint Devices

TIA-1057

April 2006

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Representing the telecommunications industry in association with the Electronic Industries Alliance

Electronic Industries Alliance

NOTICE

TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. The existence of such Standards and Publications shall not in any respect preclude any member or non-member of TIA from manufacturing or selling products not conforming to such Standards and Publications. Neither shall the existence of such Standards and Publications preclude their voluntary use by Non-TIA members, either domestically or internationally.

Standards and Publications are adopted by TIA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(From Standards Proposal No. 3-0185, formulated under the cognizance of the TIA TR-41.4, Subcommittee on IP Telephony Infrastructures).

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Standards and Technology Department
2500 Wilson Boulevard
Arlington, VA 22201 U.S.A.

PRICE: Please refer to current Catalog of
TIA TELECOMMUNICATIONS INDUSTRY ASSOCIATION STANDARDS
AND ENGINEERING PUBLICATIONS
or call Global Engineering Documents, USA and Canada
(1-800-854-7179) International (303-397-7956)
or search online at http://www.tiaonline.org/standards/catalog/

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Engineering Manual ("Manual"), the current and predecessor versions of which are available at http://www.tiaonline.org/standards/procedures/manuals/ TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). TIA does not evaluate, test, verify or investigate the information, accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA disclaims any undertaking to perform any duty owed to or for anyone.

If the Document is identified or marked as a project number (PN) document, or as a standards proposal (SP) document, persons or parties reading or in any way interested in the Document are cautioned that: (a) the Document is a proposal; (b) there is no assurance that the Document will be approved by any Committee of TIA or any other body in its present or any other form; (c) the Document may be amended, modified or changed in the standards development or any editing process.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. TIA makes no search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. TIA takes no position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR. TIA will neither be a party to discussions of any licensing terms or conditions, which are instead left to the parties involved, nor will TIA opine or judge whether proposed licensing terms or conditions are reasonable or non-discriminatory. TIA does not warrant or represent that procedures or practices suggested or provided in the Manual have been complied with as respects the Document or its contents.

If the Document contains one or more Normative References to a document published by another organization ("other SSO") engaged in the formulation, development or publication of standards (whether designated as a standard, specification, recommendation or otherwise), whether such reference consists of mandatory, alternate or optional elements (as defined in the TIA Engineering Manual, 4th edition) then (i) TIA disclaims any duty or obligation to search or investigate the records of any other SSO for IPR or letters of assurance relating to any such Normative Reference; (ii) TIA's policy of encouragement of voluntary disclosure (see Engineering Manual Section 6.5.1) of Essential Patent(s) and published pending patent applications shall apply; and (iii) Information as to claims of IPR in the records or publications of the other SSO shall not constitute identification to TIA of a claim of Essential Patent(s) or published pending patent applications.

TIA does not enforce or monitor compliance with the contents of the Document. TIA does not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NONINFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKES NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTENTS.

Table of Contents

Figures

Tables

Foreword

(This foreword is not part of this Standard.)

This document is a TIA Telecommunications standard produced by Engineering Subcommittee TR41.4, “VoIP Systems – IP Telephony Infrastructure and Endpoints”, of Committee TR-41. This Standard was developed in accordance with TIA procedural guidelines, and represents the consensus position of the subcommittee, which served as the formulating group.

The TR-41.4 subcommittee acknowledges the contribution made by the following individuals in the development of this revision of this standard.

Name	**Representing**
Peter Blatherwick (Editor)	Mitel Networks
Dan Romascanu	Avaya
David Frattura	Enterasys Networks
Manfred Arndt	Hewlett Packard Company
Henning Schulzrinne	Columbia University

Suggestions for improvement of this Standard are welcome. They should be sent to:

Telecommunications Industry Association
Engineering Department
Suite 300
250 Wilson Boulevard
Arlington, VA 22201

1 Introduction

1.1 General

The IEEE Standard 802.1AB™, "Link Layer Discovery Protocol"[1] [1], is designed to provide a multi-vendor solution for the discovery of elements on a data network and how they are connected to each other. The LLDP Standard allows stations attached to an IEEE 802 LAN/MAN to advertise to other stations, attached to the same 802 LAN segment, the functionalities provided by that station. These advertisements can announce fundamental station configuration information such as management address, address of the entities that manage the device, the identification of the end system's point of attachment, or its identity and type. The information distributed via LLDP is generally stored by its recipients in a standard management information base (MIB), making it possible for the information to be accessed by a network management system (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

IEEE 802.1AB can be utilized for many advanced features in a VoIP network environment. These features include basic configuration, network policy configuration, location identification (including for Emergency Call Service / E911), inventory management, and more.

This Standard provides extensions to the IEEE 802.1AB base protocol to allow for these functions, and also provides behavioral requirements for devices implementing the extensions to enable correct multi-vendor interoperation.

1.2 Purpose

This Standard fills a recognized need in the Voice Over IP (VoIP) industry, brought about by the use of equipment supplied by many different manufacturers, along with the need for cost-effective, readily deployable, and easily managed solutions. In particular, the needs for deployment of VoIP equipment into IEEE 802 - based LAN environments are addressed. It will be useful to anyone engaged in the manufacture of VoIP equipment and related products, as well as to those purchasing, operating or using such products. It is internationally applicable.

To fulfill these needs, this Standard provides extensions to IEEE 802.1AB that are specific to the requirements of Media Endpoint Devices in an IEEE 802 LAN environment. Specific usage of the IEEE 802.1AB LLDP base specification is also defined. Interaction behavior between the Media Endpoint Devices and the LAN infrastructure elements are also described where they are relevant to correct operation or multi-vendor interoperability.

LLDP extensions and behavior requirements are described specifically in the areas of network configuration and policy, device location (including for Emergency Call Service / E911), Power over Ethernet management, and inventory management. Extensibility mechanisms to allow for future work in this area are also provided where possible.

[1] The IEEE 802.1AB™ standard is formally titled "IEEE Standard for Local and Metropolitan Networks: Station and Media Access Control Connectivity Discovery", but is commonly referred to as "Link Layer Discovery Protocol" (LLDP). The term LLDP is used interchangeably with IEEE 802.1AB in this Standard. IEEE 802.1AB is a trademark of IEEE, used by permission.

Media Endpoint Devices addressed include, but are not limited to, IP Phones, IP Voice / Media Gateways, IP Media Servers, IP Communications Controllers, and others.

The intent of this standard is to conform to and align with existing IEEE, IETF, ETSI, ITU-T, ANSI, TIA, and other standards; however, it is not the intent to duplicate the efforts of these other organizations. Specifically, this standard makes use of the extension mechanisms designed into IEEE 802.1AB.

1.3 Document Conventions

Two categories of standard requirements are specified in this Standard: mandatory and advisory. The mandatory requirements are designated by the word "shall". Advisory requirements are designated by the words "should", "recommended" or "may".

In addition, where reference is made to requirements set in other standards, or requirements are set drawing directly from those other standards, the word "mandatory" is also used to indicate mandatory requirements, and the words "desirable" or "optional" are also used to indicate advisory requirements. The word "conditional" is used to indicate requirements that are applicable in the described circumstances. These secondary terms hold equal weight with those given in the previous paragraph (i.e. "shall", "should", "recommended" or "may").

NOTE – The definitions of these secondary terms, over and above those generally used in ANSI/TIA standards documents, are intended to align with the definitions in the referenced external standards. Since this Standard makes extensive references to external standards, notably IEEE 802.1AB [1] of which this Standard is largely an extension, it is important to maintain this consistency in the definitions.

The mandatory criteria generally apply to safety and protection, signaling and compatibility. They specify the absolute minimum acceptable functional capability or performance criteria in areas such as protocol conformance, information element content and format, or other criteria required to allow universal interoperability between implementations of this Standard.

Advisory, recommended or desirable criteria represent product goals. In some instances, these criteria are included in an effort to assure universal product compatibility even with equipment and facilities operational in statistically small quantities. In other cases, advisory criteria are presented when their attainment will enhance the general performance of the product in all its contemplated applications, or to align with best current practices.

Where both a mandatory and an advisory level are specified for the same criterion, the advisory level represents a goal currently identifiable as having distinct compatibility or performance advantages, or both, toward which future designs should strive.

2 Scope

This Standard defines a set of organizationally-specific IEEE 802.1AB TLV extensions and a related MIB module, for the purpose of improved deployment properties and multi-vendor interoperability between VoIP endpoint devices and IEEE 802 networking infrastructure elements. Where required for correct multi-vendor interoperation, specific constraints on IEEE 802.1AB protocol behavior, application-level interaction with the protocol elements, as well as constraints on existing IEEE 802.1AB TLVs and related MIB module, are also defined.

This Standard is applicable to all VoIP network edge devices such as (but not limited to) IP Phones, Voice / Media Gateways, Media Servers, IP Communications Controllers or other VoIP devices or servers, as well as to network access elements such as (but not limited to) IEEE 802 LAN Bridges or Wireless Access Points, and L2 or L3 switches or routers which are connected within IEEE 802 LANs.

This Standard specifically addresses usage of LLDP and the extensions defined herein within IEEE 802 LAN environments. This Standard may also be applicable to IEEE 802 MAN environments (IEEE 802.1AB is not specific to this, however there are no defined limits).

This Standard is specifically defined for use between VoIP endpoints and LAN network access elements, and as such is not intended for use on links between LAN infrastructure elements.

This Standard is international in scope.

This Standard conforms to and harmonizes with other existing, referenced TIA, ANSI, ISO, IEEE, IETF, ETSI, ITU-T and other standards. Specifically, this Standard conforms to IEEE 802.1AB [1] and use of the extension mechanisms defined as part of that Standard, as well as to applicable IEEE-defined pre-existing extensions to IEEE 802.1AB as published in Annexes F (802.1 extensions) and Annex G (802.3 extensions) of that Standard.

This Standard does not address interactions between IEEE 802.1AB and other link level protocols such as IEEE 802.1X or IEEE 802.3af.

This Standard is not specific to any particular VoIP control architecture, signaling or other higher-level protocol (e.g. SIP, Megaco / H.248, H.323, etc).

This Standard is not specific to any particular system management architecture, and does not mandate use of SNMP or other particular management protocol.

This Standard does not place any application-level requirements on interaction between system components such as control signaling, setting of policies, gathering of management information, or usage of the information provided.

2.1 Scope of Current Standard Release

In this release of this Standard, the following capabilities are fully specified. More detailed functional descriptions of these capabilities, as well as specific references to implementation sections, are given in section 7, Media Endpoint Discovery Functional Description.

- LAN speed and duplex in use, 2-way advertisement (see section 7.2, LAN Speed and Duplex Discovery).

- Network policy discovery, including VLAN id, 802.1p priority and Diffserv code point (DSCP), 2-way advertisement (see section 7.3, Network Policy Discovery).

- Device location and topology discovery based on LAN-level MAC/port information, 2-way advertisement (see section 7.4, LAN Level Endpoint Location Discovery).

- IP Phone location identification, including emergency call service location, based on IETF and NENA-defined location objects, 1-way advertisement from LAN infrastructure element to endpoint (see section 7.5, Endpoint Location Identification Discovery).

- Endpoint move detection notification from network connectivity device to their associated VoIP management application(s), using SNMP or similar (see section 7.6, Endpoint Move Detection Notification).

- Extended Power over Ethernet (PoE) discovery for fine-grained power management, 2-way advertisement (see section 7.7, Extended Power Via MDI Discovery).

- Extended device identification for inventory management, 1-way advertisement from endpoint to LAN infrastructure element (see section 7.8, Inventory Management Discovery).

- Identification of endpoint-embedded network connectivity capabilities (e.g. multi-port IP Phone with embedded L2 switch or bridge capability), 1-way advertisement from endpoint to LAN infrastructure element (see section 7.9, Embedded Network Connectivity Discovery).

- Application level interactions with the LLDP protocol elements to provide timely startup of LLDP to support rapid availability of Emergency Call Service (see section 7.10, LLDP-MED Fast Start Protocol Behavior).

- Applicability of LLDP-MED to Wireless LAN environments (Informative, see ANNEX B: LLDP-MED Support for Voice over Wireless LAN).

Note that some of these capabilities are based on newly defined TLVs and the related MIB module defined herein, while others of these capabilities are based on previously defined TLVs and related MIB modules from the IEEE 802.1AB base specification [1].

It is considered that future iterations of this Standard can potentially add expanded support in the above or related areas, and also for other types of media endpoints, such as video devices. Refer to section 2.2 Future Considerations for a listing of future items considered, but not specified in this release of this Standard.

2.2 Future Considerations

The following were considered for inclusion in this release of this Standard, but are now considered candidates for future releases, and every effort is made to provide for extensibility to these and other capabilities:

- IP Phone advertisement of its dialable phone number, URI or other callable address.

- Extended device class definitions such as basic IP phone, video phone, web phone, etc.
- Media type(s) supported (voice, video, text conversation, etc).
- Media bandwidth requirement(s) advertise by endpoint.
- Device operational status.
- Device mobility.
- IP Phone advertisement of ECS calls in progress.
- Specific extensions for usage of LLDP-MED in Wireless LAN environments.

3 Normative References

The following references contain provisions, which, through reference in this text, constitute provisions of this Standard.

At the time of publication, the editions indicated were valid. All references are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the references indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

[1] IEEE Std 802.1AB™-2005 Edition, IEEE Standard for Local and Metropolitan Networks: Station and Media Access Control Connectivity Discovery, May 2005.[2]

[2] IEEE Std 802.3af™-2003 Edition, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Layer and Physical Layer Specifications – Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)

[3] IEEE Std 802.1D™-2004 Edition, IEEE Standard for Local and Metropolitan Area Networks -- Media Access Control (MAC) Bridges.

[4] IEEE Std 802.1Q™-2003 Edition, IEEE Standards for Local and Metropolitan Area Networks -- Virtual Bridged Local Area Networks.

[5] IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, Nichols et al, December 1998 (see also RFC3260 [28] and RFC 2475 [27]).

[6] IETF RFC 3825, Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information, Polk et al, July 2004.

[7] IETF RFC 3621, Power Ethernet MIB, Berger & Romascanu, December 2003.

[8] IETF 3410, Introduction and Applicability Statements for Internet Standard Management Framework, Case et al, December 2002.

[9] IETF STD 62, RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, Harrington et al, December 2002.

[10] IETF STD 62, RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), Case et al, December 2002.

[11] IETF STD 62, RFC 3413, Simple Network Management Protocol (SNMP) Applications, Levi et al, December 2002.

[12] IETF STD 62, RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), Blumenthal & Wijnen, December 2002.

[2] The IEEE standards referred to in this Standard are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[13] IETF STD 62, RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), Wijnen et al, December 2002.

[14] IETF STD 62, RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), Presuhn et al, December 2002.

[15] IETF STD 62, RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), Presuhn et al, December 2002.

[16] IETF STD 62, RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Presuhn et al, December 2002.

[17] IETF STD 58, RFC 2578, Structure of Management Information Version 2 (SMIv2), McCloghrie et al, April 1998.

[18] IETF STD 58, RFC 2579, Textual Conventions for SMIv2, McCloghrie et al, April 1998.

[19] IETF STD 58, RFC 2580, Conformance Statements for SMIv2, McCloghrie et al, April 1998.

[20] IETF RFC 2737, Entity MIB (Version 2), McCloghrie & Bierman, December 1999.

[21] NENA TID 07-501, Network Interfaces for E9-1-1 and Emerging Technologies, September 2002.

4 Definitions, Abbreviations and Acronyms

For the purposes of this Standard, the following definitions, abbreviations and acronyms apply.

4.1 Terminology Definitions

Topic-specific terminology, which appears in this Standard, is defined below.

LLDP-MED Device – Any device which implements this Standard.

LLDP-MED Device Type – A specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below.

Network Connectivity Device – An LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices (refer to section 6, Media Endpoint Discovery Reference Model).

Endpoint Device – An LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology. Endpoint Devices may be a member of any of the Endpoint Device Classes defined below.

Endpoint Device Class – Any of the three sub-categories of Endpoint Device defined below (refer to section 6, Media Endpoint Discovery Reference Model).

Generic Endpoint Device (Class I) – The most basic class of Endpoint Device (refer to section 6, Media Endpoint Discovery Reference Model).

Media Endpoint Device (Class II) – The class of Endpoint Device that supports media stream capabilities (refer to section 6, Media Endpoint Discovery Reference Model).

Communication Device Endpoint (Class III) – The class of Endpoint Device that directly supports end users of the IP communication system (refer to section 6, Media Endpoint Discovery Reference Model).

IP Phone – A VoIP telephone or other end-user communication appliance, such as defined in TIA-811-A [22].

IP Voice Gateway / Media Gateway– A device used to bridge from the VoIP media domain to other non-IP domains (e.g. to connect IP-based media streams to PSTN trunking or similar).

IP Media Server – A server used to manipulate IP-based media streams by performing mixing, recording, playback or other similar functions (e.g. conference bridging, announcement servers, etc).

IP Communication Controller – A server providing call control or call control related functions to the endpoints in a VoIP system (e.g. a Megaco / H.248 Media Gateway Controller, H.323 Gatekeeper, or SIP User Agent or Proxy Server).

4.2 Abbreviations and Acronyms

Abbreviations and acronyms, other than in common usage, which appear in this Standard, are defined below.

AP Access Point, such as a wireless Access Point defined by IEEE 802.11 [25].

CAPWAP Control and Provisioning of Wireless Access Points [32].

DHCP Dynamic Host Configuration Protocol [29].

DSCP Diffserv Code Point [5], [27], [28].

ECS Emergency Call Service (e.g. E911 and others), such as defined by TIA [23] or NENA [21].

E911 Enhanced 911 Emergency Call Service applicable in North America.

ELIN Emergency Location Identification Number, a valid North America Numbering Plan format telephone number, supplied to the PSAP for ECS purposes.

IETF Internet Engineering Task Force.

LAN Local Area Network, as defined by the IEEE 802 suite of standards.

LCI Location Configuration Information.

LLDP Link Layer Discovery Protocol, as defined by IEEE 802.1AB [1].

LLDP-MED Link Layer Discovery Protocol Media Endpoint Discovery, the set of capabilities as defined by this Standard.

LLDPDU Link Layer Discovery Protocol Data Unit, as defined in IEEE 802.1AB [1].

MAC Media Access Control (sublayer).

MAN Metropolitan Area Network, as defined by the IEEE 802 suite of standards.

MDI Media Dependent Interface.

MED Media Endpoint Discovery.

MIB Management Information Base, as defined by the Internet-Standard Management Framework, IETF RFC 3410 [31].

NENA National Emergency Number Association, the body responsible for evolution of public ECS architectures in North America.

NMS Network Management System.

OUI Organizationally Unique Identifier.

PoE Power Over Ethernet, as defined by IEEE 802.3af [2].

PVID Port VLAN ID.

RADIUS Remote Authentication Dial In User Service Protocol, as defined by IETF RFC 2865 [33].

SMI Structure of Management Information as defined by IETF RFC 2578 – 2580 [17] - [19].

SNMP Simple Network Management Protocol, as defined by IETF RFC 3410 – 3418 [8] - [16].

TIA Telecommunications Industry Association.

TLV Type Length Value.

VID VLAN ID.

VoIP Voice over Internet Protocol.

VoWLAN Voice over WLAN.

WLAN Wireless LAN such as defined by IEEE 802.11 [25].

5 IEEE 802.1AB LLDP — Overview (Informative)

This section is provided as an informative overview only. See the IEEE 802.1AB specification [1] for definitive details.

Note that later normative sections of this specification add further mandatory requirements on IEEE 802.1AB base behavior, including making some optional aspects of 802.1AB mandatory for LLDP-MED devices to support.

LLDP is a Link-layer protocol that transmits advertisements containing device information, device capabilities and media specific configuration information periodically to neighbors attached to the same network. The LLDP agent operates only in an advertising mode, and hence does not support any means for soliciting information, or keeping state between two LLDP entities. The LLDP agent advertises information over Logical Link-Layer Control frames and records the information received from other agents in IEEE defined MIB modules. (Note that LLDP does not specifically mandate SNMP or any MIB module support, just that the information can be mapped to the objects defined in the MIB modules.)

5.1 LLDP - Frame Format

The information fields in each frame are contained in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of short, variable-length, information elements known as TLVs that each include type, length, and value fields where:

a) Type identifies what kind of information is being sent

b) Length indicates the length of the information string in octets

c) Value is the actual information that needs to be sent

Each LLDPDU includes the four mandatory TLVs listed below plus optional TLVs as selected by network management:

d) Chassis ID TLV

e) Port ID TLV

f) Time-to-live TLV

g) Optional TLVs may be inserted in any order, as allowed by the space limitation of the LLDPDU

h) End-of-LLDPDU TLV

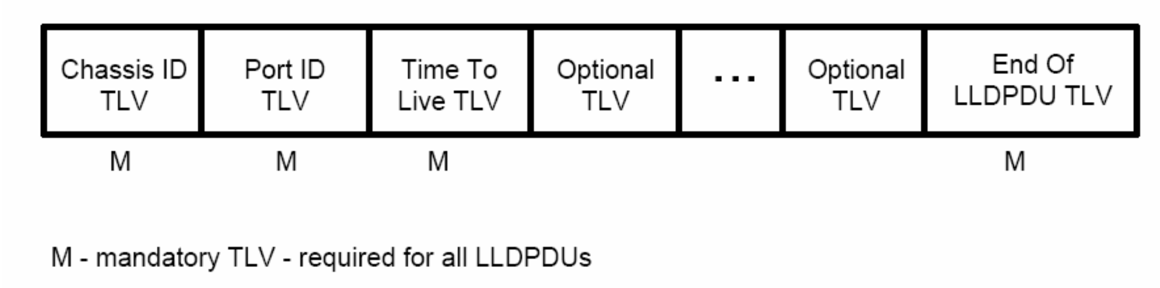

Figure 1 – LLDP PDU Format*

The chassis and port ID TLVs represent the connected system's chassis identification and the identification of the specific port that transmitted the LLDP frame. The receiving LLDP agent combines the Chassis ID and Port ID to represent the entity that sent the LLDPDU. The Time to Live TLV represents for how long information contained in the received LLDPDU shall be valid. The end-of-LLDPDU TLV marks the end of an LLDPDU.

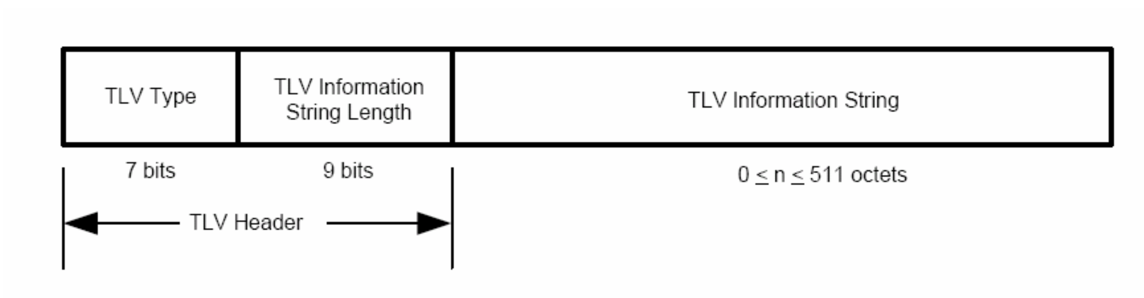

Figure 2 – TLV Format*

The TLV type field occupies the seven most-significant bits of the first octet of the TLV format. The least-significant bit in the first octet of the TLV format is the most-significant bit of the TLV information-string length field.

The TLV type field identifies a specific TLV from the LLDP basic management set or a particular set of TLVs that have been defined by a professional organization or individual vendor. Two classes of TLVs are defined; mandatory and optional.

5.2 LLDP - Optional TLVs

The LLDP standard defines a set of officially recognized optional TLVs. The optional TLVs provide various details about the LLDP agent advertising them. The LLDP agent can advertise one or more of these TLVs in addition to the mandatory TLVs.

a) Port description TLV

b) System name TLV

c) System description TLV

d) System capabilities TLV

e) Management address TLV

The port description TLV is used to identify the port from which the LLDP agent transmitted the frame. The system name TLV represents the system's administratively-assigned name. The system description TLV provides a textual description of the network entity. This value should include the systems name, the hardware version, the operating system level and networking software version. The system capabilities TLV contain a bit-map that defines the primary function(s) of the system. The currently defined capabilities include, among other things, WLAN Access Point, Router and Telephone. The management address TLV represents an address associated with the local LLDP agent that may be used to reach higher layer entities. TLVs in the basic management set are defined in subclause 9.5 of the IEEE 802.1AB-2005 specification [1].

5.3 Organizationally-specific TLV extensions

Organizationally-specific TLVs can be defined by either the professional organizations or the individual vendors that are involved with the particular functionality being implemented within a system.

Because of the TLV structure of LLDP, the protocol is very flexible. The organizationally-specific TLV allows for the creation of many advanced discovery options not originally envisioned during the development of the LLDP standard.

The organizationally-specific TLV category is provided to allow different organizations, such as the TIA, IETF or other standards bodies, as well as individual software and equipment vendors, to define TLVs that advertise information to remote entities attached to the same media, subject to the following restrictions:

a) Information transmitted in a TLV is intended to be a one-way advertisement. The TLV shall not solicit a response and shall not provide an acknowledgement.

b) Information transmitted in a TLV shall be independent from information in a TLV received from a remote port.

c) Information transmitted in one TLV shall not be concatenated with information transmitted in another TLV on the same media in order to provide a means for sending messages that are larger than would fit within a single TLV.

d) Information received in the TLV shall not be explicitly forwarded to other ports in the system.

e) Any other restriction as specified in IEEE 802.1AB.

Each set of organizationally-defined extension TLVs shall include associated LLDP MIB extensions and the associated TLV selection management variables and MIB/TLV cross-reference tables.

Systems that implement LLDP and that also support standard protocols for which organizationally-specific TLV extension sets have been defined shall support all TLVs and the LLDP MIB extensions defined for that particular TLV set.

The basic format for organizationally-defined TLV extensions is shown in Figure 3, below. The TLV type value of 127 shall be used for all organizationally-defined TLVs.

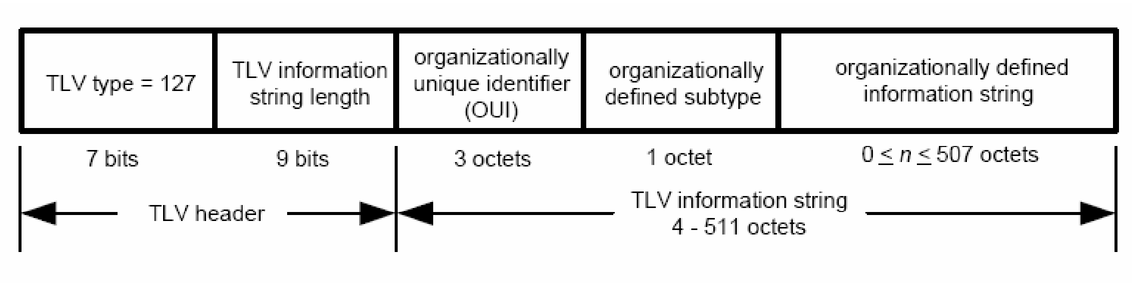

Figure 3 – Basic format for organizationally-defined extension TLVs*

IEEE 802.1AB also defines a set of optional TLVs that may be used to describe the system and/or to assist in the detection of configuration of IEEE 802.1 and IEEE 802.3 information.

The IEEE 802.1 TLV extensions describe various attributes associated with Virtual Local Area Networks. The defined TLVs are as follows:

f) Port VLAN ID TLV

g) Port & Protocol VLAN ID TLV

h) VLAN Name TLV

i) Protocol Identity TLV.

The Port VLAN ID TLV allows a bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames it receives. The Port & Protocol VLAN ID TLV allows a bridge to advertise whether it supports protocol VLANs and, if so, what VLAN IDs these protocols will be associated with. The VLAN Name TLV allows a bridge to advertise the textual name of any VLAN with which it is configured. The Protocol Identity TLV allows the bridge to advertise the particular protocols that are accessible through its port.

The IEEE 802.3 TLV extensions describe various attributes associates with the operation of an 802.3 LAN interface. The defined TLVs are as follows:

* From IEEE Std. 802.1AB 2005 Copyright 2005 IEEE. All rights reserved.

j) MAC/PHY Configuration/Status TLV

k) Power Via MDI TLV

l) Link Aggregation TLV

m) Maximum Frame Size TLV.

The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. The Power-Via-MDI TLV advertises the power-via-MDI capabilities of the sending 802.3 LAN station. The Link-Aggregation TLV advertises whether the link is capable of being aggregated, whether it is currently in an aggregation and if in an aggregation, the port of the aggregation. The Maximum Frame Size TLV advertises the maximum supported 802.3 frame size of the sending station.

6 Media Endpoint Discovery Reference Model and Definitions (Normative)

Figure 4, below, shows the LLDP-Media Endpoint Discovery reference model in diagrammatic form.

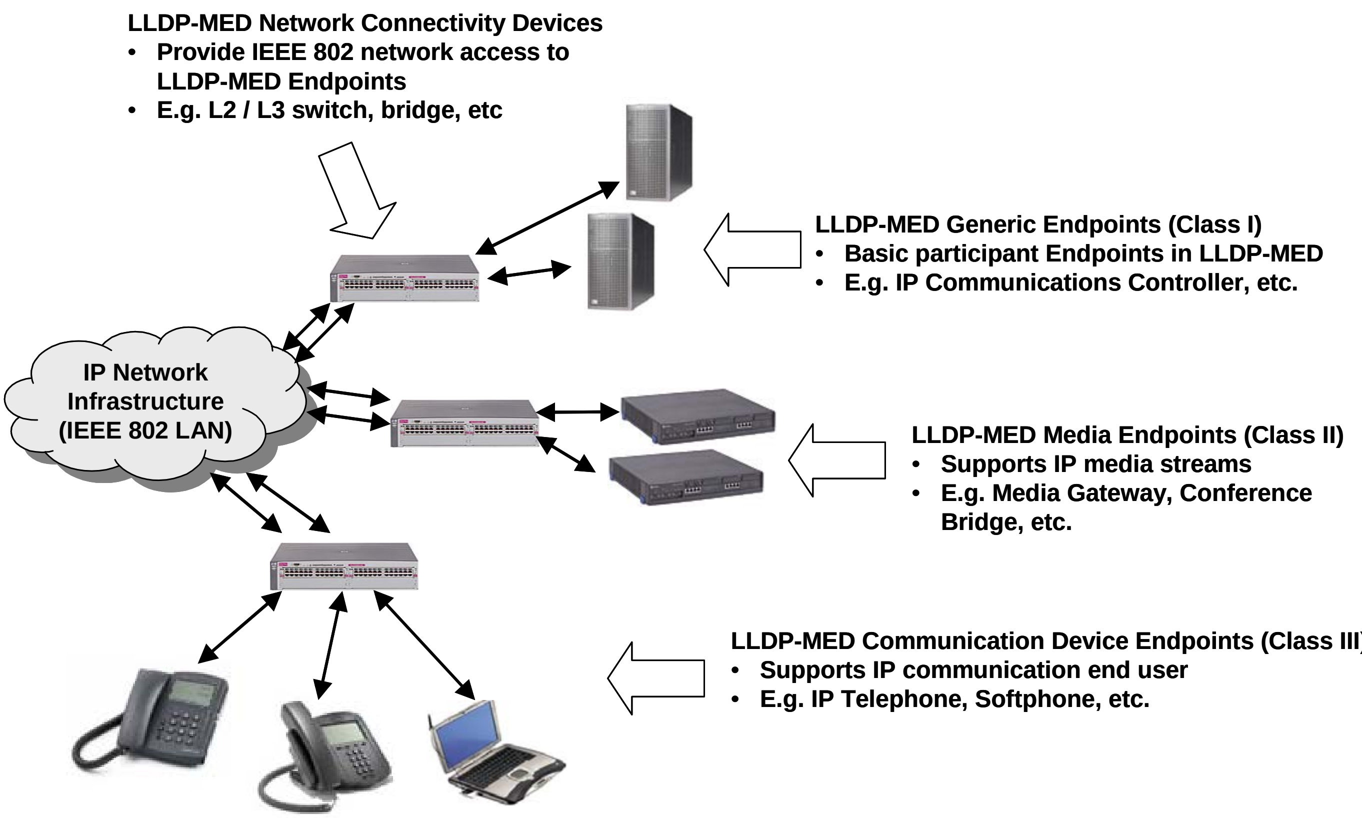

Figure 4 – LLDP-MED Reference Model

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. In turn, Endpoint Devices are composed of three defined sub-types or Classes. These are specifically defined in the following subsections.

6.1 LLDP-MED Network Connectivity Device Definition

This subsection gives a normative definition of LLDP-MED Network Connectivity Devices. All products claiming conformance with this Standard, as an LLDP-MED Network Connectivity Device, shall conform to this definition.

LLDP-MED Network Connectivity Devices, as defined in this Standard, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

Specific requirements that apply to LLDP-MED Network Connectivity Devices are defined in section 8.1, Network Connectivity Device Requirements.

6.2 LLDP-MED Endpoint Device Definition

This subsection gives a normative definition of LLDP-MED Endpoint Devices. All products claiming conformance with this Standard, as an LLDP-MED Endpoint Device, shall conform to this definition.

LLDP-MED Endpoint Devices, as defined in this Standard, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Specific requirements that apply to all LLDP-MED Endpoint Devices are defined in section 8.2, Endpoint Device Requirements.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following subsections. These Class definitions are also normative, such that any product that claims conformance to one or more of these defined Endpoint Device Classes shall conform to all requirements of the claimed Class.

It is important that each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. As such, any particular product implementing this Standard may not require all capabilities, depending on their specific product category. However if a product claims compliance with a particular LLDP-MED Endpoint Device Class, such product shall also be in compliance with all aspects of all underlying Endpoint Device Classes. Specifically, any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) shall also support all aspects of this Standard applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) shall also support all aspects of this Standard applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

NOTE – A product may claim conformance to this Standard as an LLDP-MED Endpoint Device even if it does not specifically conform to any of the specified Endpoint Device Classes defined below, so long as it does meet the general description above as well as the specific requirements given in section 8.2, Endpoint Device Requirements. It is recommended that such products explicitly list or otherwise make available to their customers the specific aspects of this Standard to which they do conform.

6.2.1 LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in this Standard, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in this Standard.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

Specific requirements that apply to all LLDP-MED Generic Endpoint (Class I) Devices are defined in section 8.2.1, Requirements for Generic Endpoints.

6.2.2 LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

Specific requirements that apply to all LLDP-MED Media Endpoint (Class II) Devices are defined in section 8.2.2, Requirements for Media Endpoints.

6.2.3 LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

Specific requirements that apply to all LLDP-MED Communication Endpoint (Class III) Devices are defined in section 8.2.3, Requirements for Communication Device Endpoints.

7 Media Endpoint Discovery Functional Description (Normative)

This section defines, at a functional level, how the various capabilities defined by LLDP-MED are intended to operate, and also sets these capabilities in context to make their purpose and applicability clear. As such, this section forms a "bridge" between the scope statement of LLDP-MED capabilities in this revision of this Standard (section 2.1) and later sections which define exact requirements for each LLDP-MED Device Type as well as the specific TLV and MIB extensions themselves.

Table 1, below, lists the various LLDP-MED discovery functions and their associated TLVs or MIB operations.

Table 1 – Discovery Function / TLV or MIB Cross Reference

Discovery Function	TLV or MIB Procedure	Section Reference
LLDP-MED Capabilities	LLDP-MED Capabilities TLV	10.2.2
LAN Speed and Duplex	IEEE 802.3 MAC/PHY Configuration/Status TLV	9.2.2
Network Policy	Network Policy TLV	10.2.3
LAN Level Endpoint Location	IEEE 802.1AB Chassis ID TLV IEEE 802.1AB Port ID TLV	9.2.3
Endpoint Location Identification	LLDP-MED Location Identification TLV	10.2.4
Endpoint Move Detection	LLDP-MED MIB change notification	12.3
Extended Power via MDI	Extended Power-via-MDI	10.2.5
Inventory Management	Inventory - Hardware Revision Inventory - Firmware Revision Inventory - Software Revision Inventory - Serial Number Inventory - Manufacturer Name Inventory - Model Name Inventory - Asset ID	10.2.6.1 10.2.6.2 10.2.6.3 10.2.6.4 10.2.6.5 10.2.6.6 10.2.6.7
Embedded Network Connectivity		9.2.1

Specific requirements regarding exactly what must be implemented by particular Devices in the LLDP-MED Reference Model, and what aspects are optional, are defined in section 8, LLDP-MED Device Requirements, below.

Pointers to relevant later sections are included to direct the reader to the specific and detailed definitions of new TLV extensions and related MIB objects (in sections 10 and 13), defined usage of the LLDP base protocol (in section 9), and LLDP-MED specific protocol interactions involved in implementing the functionality (in section 11).

7.1 LLDP-MED Capabilities Discovery

LLDP-MED Capabilities Discovery enables efficient discovery of the LLDP-MED TLVs supported by a particular Media Endpoint or Network Connectivity Device, and the LLDP-MED Device Type it belongs to. Since LLDP-MED Capabilities are specific to LLDP-MED Devices, advertisement of this TLV by Endpoints enables LLDP-MED capable Network Connectivity Devices to definitively determine support of LLDP-MED by Endpoints they are connecting to.

Implementation details are defined in section 10.2.2, LLDP-MED Capabilities TLV.

7.2 LAN Speed and Duplex Discovery

LAN Speed and Duplex Discovery enables efficient discovery and diagnosis of mismatch issues in VoIP LAN environments. These capabilities are considered highly useful in VoIP environments, where speed or duplex mismatches are a relatively common issue that can cause bandwidth utilization and voice quality of service degradation.

This Standard defines specific usage of pre-existing IEEE 802.1AB TLVs that allow for discovery of the LAN speed and duplex in use at each end of a LAN link. LLDP-MED makes these TLVs (which are optional in the LLDP base protocol) mandatory for all LLDP-MED devices to both send and receive.

Implementation details are defined in section 9.2.2, IEEE 802.3 MAC/PHY Configuration/Status TLV.

7.3 Network Policy Discovery

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

This TLV is only intended for use with applications that have specific ‘real-time’ network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised in this Standard include:

- Layer 2 VLAN ID (IEEE 802.1Q-2003 [4])
- Layer 2 priority value (IEEE 802.1D-2004 [3])
- Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474 [5])

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed in this revision of this Standard include:

- Voice

- Guest Voice
- Softphone Voice
- Video Conferencing
- Streaming Video
- Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policy TLVs to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Implementation details are defined in section 10.2.3, Network Policy TLV.

7.4 LAN Level Endpoint Location Discovery

LAN Level Endpoint Location Discovery enables network topology discovery and Endpoint Device location and move detection based on network-level connectivity as advertised between Network Connectivity Devices and the Endpoints. This discovery is based on two-way advertisement of mandatory Chassis ID and Port ID elements provided in the IEEE 802.1AB base specification, placing specific constraints on formats and usage of these LLDP elements.

Location-based applications, including Emergency Calling Service (ECS) applications such as defined by TIA-TSB-146 [23], may make use of this capability to enable resolution of an Endpoint Device's physical location based on a wire map or similar network topology data held elsewhere in the system. This Standard does not specify any particular application level usage of this TLV information.

Implementation details are defined in section 9.2.3, IEEE 802.1AB Chassis ID and Port ID TLVs.

7.5 Endpoint Location Identification Discovery

Endpoint Location Identification Discovery enables advertisement of location identifier information to Communication Endpoint Devices, including emergency call service location, based on configuration of the Network Connectivity Device it is connected to. This method of location data distribution is intended to support and harmonize with TIA-TSB-146 Emergency Call Services [23], NENA [21], or other similar standards, as an optional method of providing this information in those applications, but is explicitly not limited to those applications. This Standard does not specify any particular application level usage of this TLV information.

The location identifier data types specifically addressed in this revision of this Standard include:

- Coordinate-based LCI as defined by IETF RFC 3825 [6],

- Civic Address LCI as defined by IETF (refer to ANNEX B),
- Emergency Call Service ELIN number, to support traditional PSAP-based Emergency Call Service in North America, as described for example by NENA TID 07-501 [23].

The provided information is expected to be related to wire map or similar network topology data, such that the configuration of the Network Connectivity Device is able to uniquely identify the physical location of the connected Endpoint Device, hence provide the correct location identifier information for it to use.

Implementation details are defined in section 10.2.4, Location Identification TLV.

NOTE – Location-based applications may also make use of the LAN Level Endpoint Location Discovery capability described in section 7.4. Detection of location changes by VoIP management applications may also be facilitated using the Endpoint Move Detection Notification capability described in section 7.6.

7.6 Endpoint Move Detection Notification

Endpoint move detection notification enables Network Connectivity Devices to efficiently notify their associated VoIP management application(s) of VoIP device moves, using SNMP or similar means. The LLDP-MED MIB module defines the notifications that carry the data reflecting these topology changes, as well as objects to enable or disable transmission of the notifications.

In a VoIP environment, the procedure for endpoint move detection is often based upon an SNMP management application, or similar, periodically polling the network connectivity devices. LinkUp and LinkDown notifications from the network devices are used to improve the performance of the database updates, by letting the management application know proactively about endpoint moves and changes.

However; a large portion of LinkUp / LinkDown and similar notifications can be due to endpoint system reboots or power failures where the endpoint port location did not actually change. Also, many LinkUp / LinkDown notifications may not be related to any endpoint involved in the VoIP system (e.g. may be a printer, PC, etc), hence may not be of any direct interest to the VoIP management application. Even though the endpoint port location did not change, the VoIP management application must respond to the link state notification events from the network device, triggered due to a temporary link loss, and poll the network device to check for location change.

The LLDP-MED mechanism provided in this Standard allows for significantly reduced overhead in device move tracking by providing VoIP-device-specific information only to the VoIP management application, and by providing key information in the notification itself. (Note however that this mechanism cannot entirely eliminate the need for periodic polling the of network connectivity devices, to audit current information, due to the non-guaranteed delivery properties of UDP, generally used as the transport for SNMP.)

Implementation details are defined in section 12.3, Topology Change Notification.

7.7 Extended Power Via MDI Discovery

Extended Power Via MDI Discovery enables detailed power information to be advertised by Media Endpoints and Network Connectivity Devices.

Information provided from the Endpoint Device to the Network Connectivity Device includes:

- Endpoint Device power requirement, in fractions of Watts, in current configuration;
- The Endpoint Device's power priority (which the Network Connectivity Device may use to prioritize which devices will remain in service during power shortages);
- Whether or not the Endpoint is currently operating from an external power source.

Information provided from the Network Connectivity Device to the Endpoint Device includes:

- Power availability from the Network Connectivity Device, in fractions of Watts;
- Current power state of the Network Connectivity Device, including whether it is currently operating from primary power or is on backup power (backup power may indicate to the Endpoint Device that it should move to a power conservation mode).

Extended Power via MDI Discovery is the preferred means for advertising information related to MDI power. Implementation details are defined in section 10.2.5, Extended Power-Via-MDI TLV.

IEEE has also defined a basic Power Via MDI TLV within 802.1AB. The IEEE basic Power Via MDI TLV provides minimal information and is intended primarily to facilitate troubleshooting of basic MDI power issues. Use of the IEEE802.1AB defined TLV is optional in that specification, and is not recommended for LLDP-MED Devices to implement, in order to conserve LLDPDU space. Additional informational discussion on usage of this TLV is provided in section 9.2.4, IEEE 802.3 Power Via MDI TLV (Informational).

7.8 Inventory Management Discovery

Inventory Management Discovery enables tracking and identification of endpoint inventory-related attributes such as manufacturer, model, software version and other pertinent information. The information advertised by the Endpoint is based on the IETF Entity MIB, RFC 2737 [20].

The set of LLDP-MED inventory TLVs defined provide a way of feeding the Endpoint inventory information to the Network Connectivity Devices, allowing for those to become an on-line repository of basic inventory information for connected VoIP Endpoints, while restricting the need for implementing SNMP agents only to the Network Connectivity Devices. This is especially important for inventory management of IP Phones, the majority of which lack support of management protocols such as SNMP, due to cost and complexity pressures that are likely to persist for some time to come. The solution is also more scalable since the management application can receive information from the LLDP-MED MIB in the network Connectivity Device instead of querying SNMP agents in the much larger numbers of Endpoint agents.

Implementation details are defined in section 10.2.6, Inventory Management TLV Set.

7.9 Embedded Network Connectivity Discovery

Embedded Network Connectivity Discovery enables identification of embedded network connectivity capabilities within Communication Endpoint Devices (e.g. multi-port IP Phone with embedded L2 switch or bridge capability, as commonly used in VoIP systems). This functionality makes use of the IEEE 802.1AB optional System Capabilities TLV, and makes specific uses of this TLV mandatory for LLDP-MED Devices. This can assist in network trouble-shooting and detection of potential security issues related to this capability. However, no specific mechanisms to guard against the related security issues are specifically addressed in this release of this Standard (see note below).

Implementation details are defined in section 9.2.1, IEEE 802.1AB System Capabilities TLV.

NOTE – It is clear that Endpoint Devices that contain embedded connectivity capabilities can affect the security posture of LAN environments as they inhibit Network Connectivity Devices from detecting a change in connectivity status of devices connecting through the Endpoint. By not being able to detect the change of connectivity status, a hole in network security could be created whereby the access allowed to an authorized device could be utilized by a non-authorized device when it is connected to a port where an authorized device had been previously connected. Efforts are underway in IEEE to address these issues by the use of port-based authentication and link layer encryption, however these efforts are not yet mature enough for inclusion in this Standard at this time. Hence interaction of LLDP-MED with these future standards, or direct support of these with further LLDP-MED extensions, is for future consideration.

7.10 LLDP-MED Fast Start Protocol Behavior

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. LLDP management variables in the application layer are used to temporarily speed up the protocol and to maintain the stateless one-way advertisement of LLDP.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Implementation details of the application layer to protocol interactions involved in this, both on the Network Connectivity Device side and on the Endpoint Device side, are defined in section 11, LLDP-MED Protocol Interactions (Normative).

8 LLDP-MED Device Requirements (Normative)

This section defines specific, normative requirements for each type of LLDP-MED Device defined by the Media Endpoint Discovery Reference Model of section 6. Forward references to implementation details given in later sections are provided. Organization of this section flows from the Reference Model.

General requirements applicable to all LLDP-MED Devices are given below, and further requirements in addition to these, specific to Network Connectivity Devices and to Endpoint Devices, are given in subsequent subsections.

A system for which conformance to this Standard is claimed shall, for all ports for which support is claimed, include the following capabilities:

a) All LLDP-MED Devices shall conform to the IEEE 802.1AB-2005 specification [1].

   1) All mandatory IEEE 802.1AB protocol behavior, TLVs and management objects shall be supported.

   2) All optional elements of IEEE 802.1AB, including optional TLVs, organizationally-specific extension TLVs, and associated MIBs, are also optional in this Standard, unless specifically overridden by subsequent subclauses.

b) All LLDP-MED Devices shall implement both LLDP transmit and receive as defined in IEEE 802.1AB.

   1) The default LLDP adminStatus value shall be enabledRxTx.

c) The TLV format of all LLDP-MED organizationally-specific extensions defined in this Standard shall use the LLDP-MED OUI value as defined in section 10.1.

d) All LLDP-MED Devices shall support the following TLVs defined in IEEE 802.1AB:

   1) LAN Speed and Duplex Discovery as described in section 9.2.2,

   2) Chassis ID and Port ID, with usage rules specific to LLDP-MED as defined in section 9.2.3.

e) All LLDP-MED Devices shall conform to all mandatory aspects of LLDP extended application to protocol interaction behavior as defined in section 11, LLDP-MED Protocol Interactions (Normative).

f) If SNMP is supported, the LLDP-MED Device shall implement the LLDP-MED MIB as defined in section 13, LLDP-MED MIB Module (Normative).

NOTE – This Standard does not specifically require implementation of SNMP for LLDP-MED Endpoint or Network Connectivity Devices. However, SNMP support is strongly recommended for Network Connectivity Devices.

8.1 Network Connectivity Device Requirements

The general description of LLDP-MED Network Connectivity Devices is given in section 6, Media Endpoint Discovery Reference Model, and Network Connectivity Devices are specifically defined in section 6.1, LLDP-MED Network Connectivity Device Definition, above.

This section defines additional specific requirements pertaining to all Network Connectivity Devices and are in addition to requirements defined in section 8 above that apply to all LLDP-MED Devices.

a) All LLDP-MED Network Connectivity Devices shall support the following LLDP-MED TLVs:

    1) Network Connectivity TLV Set, as defined in section 10.2.1.1, Table 5.

b) LLDP-MED Network Connectivity Devices may optionally implement the following LLDP-MED TLVs:

    1) Inventory Management TLV Set, as defined in section 10.2.1.5, Table 9.

c) LLDP-MED Network Connectivity Devices, which also supports SNMP (or similar), may optionally support Topology Change Notification as defined in section 12.3.

8.2 Endpoint Device Requirements

The general description of LLDP-MED Endpoint Devices and the three defined Endpoint Device Classes (Class I - III) is given in section 6, Media Endpoint Discovery Reference Model, and Endpoint Devices are specifically defined in section 6.2, LLDP-MED Endpoint Device Definition, above.

The following subsections define additional specific requirements pertaining to each Class of Endpoint Device, and are in addition to requirements defined in section 8 above that apply to all LLDP-MED Devices.

8.2.1 Requirements for Generic Endpoints (Class I)

This sub-section defines specific additional requirements applicable to all LLDP-MED Generic Endpoint Devices (Class I), as defined in section 6.2.1, LLDP-MED Generic Endpoint (Class I). As defined in section 6.2, LLDP-MED Endpoint Device Definition, this also implies that any Class II or Class III Endpoint Device shall also meet these requirements.

All products claiming compliance with LLDP-MED as an Endpoint Device Class, or as a Generic Endpoint Device (Class I), or higher Endpoint Device Class, shall be compliant to the following functional requirements.

a) All LLDP-MED Generic Endpoint Devices (Class I) shall support the following LLDP-MED TLVs:

    1) Endpoint Class I TLV Set as defined in section 10.2.1.2, Table 6.

b) LLDP-MED Generic Endpoint Devices (Class I) may optionally implement the following LLDP-MED TLVs:

   1) Inventory Management TLV Set, as defined in section 10.2.1.5, Table 9, For Endpoints that do not support SNMP or the Entity MIB, support of Inventory Management Discovery is recommended.

8.2.2 Requirements for Media Endpoints (Class II)

This sub-section defines specific additional requirements applicable to all LLDP-MED Media Endpoint Devices (Class II), as defined in section 6.2.2, LLDP-MED Media Endpoint (Class II). As defined in section 6.2, LLDP-MED Endpoint Device Definition, this also implies that any Class III Endpoint Device shall also meet these requirements.

All products claiming compliance with LLDP-MED as an Media Endpoint Device (Class II), or higher Endpoint Device Class, shall be compliant to the following functional requirements.

a) All Media Endpoint Devices (Class II) shall support all requirements of Generic Endpoint (Class I) as previously defined, unless specifically over-ridden in this sub-clause.

b) All LLDP-MED Media Endpoint Devices (Class II) shall support the following LLDP-MED TLVs:

   1) Endpoint Class II TLV Set as defined in section 10.2.1.3, Table 7.

c) LLDP-MED Media Endpoint Devices (Class II) may optionally implement the following LLDP-MED TLVs:

   1) Inventory Management TLV Set, as defined in section 10.2.1.5, Table 9. For Endpoints that do not support SNMP or the Entity MIB, support of Inventory Management Discovery is recommended.

8.2.3 Requirements for Communication Device Endpoints (Class III)

This sub-section defines specific additional requirements applicable to all LLDP-MED Communication Device Endpoints (Class III), as defined in section 6.2.3, LLDP-MED Communication Endpoint (Class III).

All products claiming compliance with LLDP-MED as a Communication Device Endpoint (Class III) shall be compliant to the following functional requirements.

a) All Communication Device Endpoints (Class III) shall support all requirements of Media Endpoint (Class II) as previously defined, unless specifically over-ridden in this sub-clause.

b) All LLDP-MED Communication Device Endpoints (Class III) shall support the following LLDP-MED TLVs:

   1) Endpoint Class III TLV Set as defined in section 10.2.1.4,Table 8.

c) All LLDP-MED Communication Device Endpoints (Class III) shall support the following IEEE 802.1AB TLVs (which are optional in IEEE 802.1AB):

   1) IEEE 802.1AB System Capabilities TLV, with specific usage rules for LLDP-MED Devices as defined in sections 9.2.1 and 9.2.1.3.

d) LLDP-MED Communication Device Endpoints (Class III) may optionally implement the following LLDP-MED TLVs:

   1) Inventory Management TLV Set, as defined in section 10.2.1.5, Table 9 For Endpoints that do not support SNMP or the Entity MIB, support of Inventory Management Discovery is recommended.

9 Usage of IEEE 802.1AB Specification (Normative)

This section provides detailed description of those TLVs defined in the IEEE 802.1AB LLDP specification that are used by LLDP-MED implementations. This includes requirements of the LLDP base specification as well as extensions to LLDP as defined in annexes of the IEEE 802.1AB specification. In some cases, optional LLDP TLVs are made mandatory to be included in LLDP-MED LLDPDUs, or constraints on TLV field content are defined.

9.1 Usage of IEEE 802.1AB Specification Mandatory Elements

All mandatory elements of the IEEE 802.1AB specification [1] shall be mandatory for all LLDP-MED implementations.

9.2 Usage of IEEE 802.1AB TLVs

Unless otherwise stated in the following subclauses of this section, all optional TLVs of the IEEE 802.1AB specification [1] shall be optional for all LLDP-MED implementations.

Table 2, below, lists the TLVs defined by IEEE 802.1AB [2] whose usage rules have been updated in LLDP-MED for either Network Connectivity or Endpoint Devices. Subsequent subsections provide further details on usage of each of these TLVs.

Table 2 – IEEE 802.1AB TLV usage requirements in LLDP-MED LLDPDUs

TLV Name	Network Connectivity Device Usage	Endpoint Device Usage	Subclause Reference
System Capabilities	Optional	Optional for Class I and II Mandatory for Class III	9.2.1
MAC/PHY configuration/status	Mandatory	Mandatory	9.2.2
Chassis ID	Mandatory – subtype shall default to MAC address	Mandatory – subtype shall default to Network address	9.2.3
Port ID	Mandatory – subtype shall default to MAC address	Mandatory – subtype shall default to MAC address	9.2.3
Power Via MDI	Not recommended	Not recommended	9.2.4

9.2.1 IEEE 802.1AB System Capabilities TLV

IEEE has defined the System Capabilities TLV to allow for network systems to advertise their embedded system capabilities. This TLV enables Endpoints to advertise whether they contain embedded connectivity capabilities, and also whether they are a telephone device.

The IEEE System Capabilities TLV identifies the primary function(s) of the system and whether or not these primary functions are enabled. Figure 5, below, shows the format of this TLV.

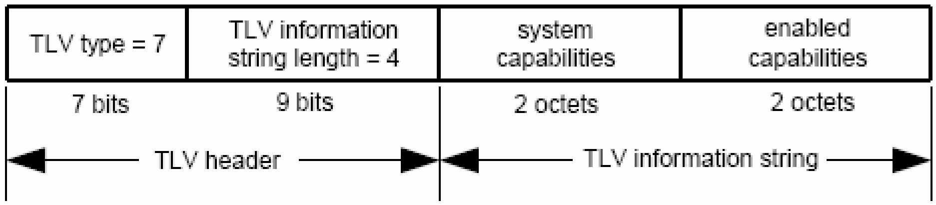

Figure 5 – IEEE 802.1AB System Capabilities TLV*

This TLV is defined in clause 9.5.8 of IEEE 802.1AB-2005 [1].

9.2.1.1 System Capabilities

This field contains a bit-map of the capabilities that define the primary function(s) of the system. The bit position for each function and the associated MIB or standard that are likely, but not guaranteed, to be supported are listed in Table 3, below. A binary one in the associated bit indicates the existence of that capability. Individual systems may indicate more than one implemented functional capability.

Table 3 – System Capability Values*

Bit	Capability	MIB or Std Reference
0	Other	—
1	Repeater	IETF RFC 2108
2	Bridge	IETF RFC 2674
3	WLAN Access Point	IEEE 802.11 MIB
4	Router	IETF RFC 1812
5	Telephone	IETF RFC 2011
6	DOCSIS Cable Device	IETF RFC 2669,RFC 2670
7	Station Only[1]	IETF RFC 2011
8-15	reserved	—

Note 1: The station-only capability is intended for devices that implement only an end-station capability. Bit 7 should not be set in conjunction with any other bits.

9.2.1.2 Enabled Capabilities

This field shall contain a bitmap of the primary functions listed in Table 3, above. A binary one in a position indicates that the function associated with the bit is currently enabled.

9.2.1.3 System Capabilities TLV usage rules in LLDP-MED

An LLDPDU shall not contain more than one system capabilities TLV.

If the system capabilities field does not indicate the existence of a capability that the enabled capabilities field indicates is enabled, the TLV shall be interpreted as containing an error and shall be discarded.

Endpoint Devices that contain embedded connectivity options or implement telephone-like capability (i.e. are Class III Endpoints) shall include this TLV in outgoing LLDP-MED LLDPDUs.

All Class III Endpoint Devices, if they implement telephone-like capability, shall set the value for bit position 5, the Telephone capability, to a binary one.

All Class III Endpoint Devices that contain embedded connectivity devices such as a bridge, router or access point shall set the value of the appropriate bit position to a binary value of one. All Class III Endpoint Devices that contain embedded connectivity capabilities other than the ones defined in the current capabilities bit values shall set bit 0, “other”, to the binary value to 1.

9.2.2 IEEE 802.3 MAC/PHY Configuration/Status TLV

IEEE 802.1AB-2005 [1] Annex G.2, defines the MAC/PHY configuration/status TLV that identifies:

a) The duplex and bit-rate capability of the sending 802.3 LAN node;

b) The current duplex and bit-rate settings of the sending 802.3 LAN node;

c) Whether theses settings are the result of auto-negotiation during the initialization of the link, or of manual set override actions.

All LLDP-MED Devices shall include this TLV in outgoing LLDP-MED LLDPDUs.

9.2.3 IEEE 802.1AB Chassis ID and Port ID TLVs

LAN Level Endpoint Location Discovery specifies mandatory elements for use in network topology discovery, Endpoint Device location and move detection, based on network-level connectivity. This makes use of the mandatory Chassis ID and Port ID TLVs provided in IEEE 802.1AB [1]. This section defines additional specific constraints on usage of those TLVs for the purposes of LLDP-MED.

IEEE 802.1AB defines mandatory TLVs for Chassis ID and Port ID of the advertising device. However, within each of these TLVs, several optional formats for the information provided are defined. For the purpose of LLDP-MED operations, it is highly useful to constrain these optional formats such that the system administrator is always presented with guaranteed globally unique information and this information can be auto-generated by the Device without administrator intervention. This consistency enables guaranteed correct generation of network topology maps as well as detection of device location and device moves, based on correlation of the network-level connectivity information with other administrative data (e.g. a wire map or similar).

All LLDP-MED Devices, both Endpoint Devices and Network Connectivity Devices, shall support the LLDP Chassis ID TLV as defined in IEEE 802.1AB-2005 [1] subclause 9.5.2, as follows:

a) Both the MAC address ID subtype (ID subtype 4) and the Network address ID subtype (ID subtype 5) shall be supported;

b) All LLDP-MED Network Connectivity Devices shall use the MAC address ID subtype (ID subtype 4) by default;

c) All LLDP-MED Endpoint Devices shall use the Network address ID subtype (ID subtype 5) by default:

   1) If a valid IP address of an Endpoint is not yet known (e.g. the Endpoint is starting up and has not yet acquired an IP address through DHCP) it is recommended that the Endpoint should advertise the unspecified IP address of 0.0.0.0 (for IPv4) or 0:0:0:0:0:0:0:0 (for IPv6). Once a valid IP address is determined, that value should then be advertised;

d) Where MAC address subtype is used, the MAC address value advertised shall correspond to the manufacturer-assigned, permanent, primary management interface of the chassis and shall uniquely identify the chassis;

e) By default, all LLDP-MED Devices shall auto-generate the MAC address ID or Network address subtype information as the TLV value, depending on their type, unless overridden by intentional configuration on the part of network administration.

All LLDP-MED Devices, both Endpoint Devices and Network Connectivity Devices, shall support the LLDP Port ID TLV as defined in IEEE 802.1AB [1] subclause 9.5.3, as follows:

f) The MAC address ID subtype (ID subtype 3) shall be supported;

g) The MAC address used shall be the manufacturer-assigned, permanent MAC address of the port and shall uniquely identify the port;

h) By default, all LLDP-MED Devices shall auto-generate this MAC address ID subtype information as the TLV value, unless overridden by intentional configuration on the part of network administration;

i) Those devices which do not have a permanent unique MAC address associated with each port shall default to using ifAlias (ID subtype 1) as the ID basis for Port ID.

9.2.4 IEEE 802.3 Power Via MDI TLV (Informational)

This section provides an informational discussion of the IEEE 802.1AB Optional 802.3 Power via MDI TLV, and is provided for the reference of implementers of LLDP-MED. The definitive specification of this TLV can be found in Annex G, Section G.3 of the IEEE 802.1AB-2005 specification [1].

The IEEE 802.1AB defined basic Power via MDI TLV provides a minimal amount of information and was intended by IEEE primarily to aid in troubleshooting network issues. The information exchanged does not provide additional detail over and above that which is available from the IEEE 802.3af power negotiation process [2]. Hence the IEEE 802.1AB defined Power via MDI TLV is optional for LLDP-MED Endpoints and Network Connectivity Devices to implement. In order to conserve LLDPDU space, transmission of this TLV is not recommended for LLDP-MED Devices.

A more comprehensive Power via MDI TLV has been defined within this Standard, in section 10.2.5, Extended Power-Via-MDI TLV. The LLDP-MED defined TLV enables fine grain power management. It is expected that developers of LLDP-MED will utilize the Extended Power-via-MDI TLV if they implement power via MDI technology.

10 LLDP-MED Organizationally Specific TLVs (Normative)

This section defines new organizationally specific TLVs designed for use by LLDP-MED Endpoint Devices and Network Connectivity Devices, as well as behavioral aspects related to these TLVs.

The extensions defined herein are a subset of those required by LLDP-MED implementations. LLDP-MED Endpoint Devices and Network Connectivity Devices are also required to support some specific TLVs of the LLDP base specification as summarized in section 8, LLDP-MED Device Requirements (Normative), and specified in detail in section 9, Usage of IEEE 802.1AB Specification (Normative).

10.1 LLDP-MED OUI Value

All implementations of LLDP-MED TLV extensions shall utilize the Organizationally Unique Identifier (OUI) 00-12-BB, as assigned by IEEE to TIA for standards use.

NOTE – This OUI is assigned by IEEE to TIA for standards use, and may be used in the context of other standards in the future[3]. Implementers of this Standard are cautioned that it is not correct to imply that a received LLDPDU was sent from an LLDP-MED Device based solely on its containing this OUI value. LLDP-MED Devices may safely deduce that a connected device is LLDP-MED capable by detecting a received, valid LLDP-MED Capabilities TLV, as defined in section 10.2.2.

10.2 LLDP-MED TLV Definitions and Formats

The currently defined LLDP-MED Organizationally Specific TLVs are listed in Table 4, below. Any additions or changes to these TLVs shall be included in future releases of this Standard.

[3] Parties interested in extending the use of this OUI should contact TIA Committee TR-41, User Premises Telecommunications Requirements.

Table 4 – LLDP-MED Organizationally Specific TLVs

LLDP-MED TLV Subtype	TLV Name	Subclause Reference
1	LLDP-MED Capabilities	10.2.2
2	Network Policy	10.2.3
3	Location Identification	10.2.4
4	Extended Power-via-MDI	10.2.5
5	Inventory - Hardware Revision	10.2.6.1
6	Inventory - Firmware Revision	10.2.6.2
7	Inventory - Software Revision	10.2.6.3
8	Inventory - Serial Number	10.2.6.4
9	Inventory - Manufacturer Name	10.2.6.5
10	Inventory - Model Name	10.2.6.6
11	Inventory - Asset ID	10.2.6.7
12 – 255	Reserved for future standardization	—

10.2.1 LLDP-MED TLV Sets Definition

LLDP-MED specifies five TLV sets to ensure interoperability between the various LLDP-MED Devices and to allow implementation of TLVs that are relevant for a given LLDP-MED Device Type.

The mandatory to implement LLDP-MED TLV sets are:

a) Network Connectivity TLV Set

b) Endpoint Class I TLV Set

c) Endpoint Class II TLV Set

d) Endpoint Class III TLV Set

The optional to implement LLDP-MED TLV set is:

e) Optional Inventory TLV Set

An LLDP-MED Device shall support exactly one mandatory LLDP-MED TLV set, corresponding to its LLDP-MED Device Type. In addition, an LLDP-MED Device may implement the Optional Inventory TLV Set.

For every supported LLDP-MED TLV set, support shall be implemented for receipt of all TLVs defined in the set.

For every TLV defined in a set, the following symbols are used to describe requirements for inclusion in outgoing LLDP-MED LLDPDUs.

- **M** Mandatory for this TLV to be included in all outgoing LLDP-MED LLDPDUs,
- **C** Conditionally required, mandatory for this TLV to be included in outgoing LLDP-MED LLDPDUs under the described conditions,
- **O** Optional for this TLV to be included in outgoing LLDP-MED LLDPDUs,
- **R** Recommended for this TLV to be included in outgoing LLDP-MED LLDPDUs.

10.2.1.1 Network Connectivity TLV Set

The Network Connectivity TLV set, defined in Table 5, specifies the usage of LLDP-MED TLVs for Network Connectivity Devices.

Table 5 – Network Connectivity TLV Set

LLDP-MED TLV Subtype	TLV Name	LLDPDU Usage	Subclause Reference
1	LLDP-MED Capabilities	M	10.2.2
2	Network Policy	C[1]	10.2.3
3	Location Identification	C[1]	10.2.4
4	Extended Power-via-MDI	C[2]	10.2.5

Note 1: Transmission of these mandatory TLVs only applies if the associated TLV data contents have been administratively configured and apply on a given port.

Note 2: Extended Power-via-MDI TLV is mandatory for IEEE 802.3af compliant PSE Network Connectivity Devices. This TLV is not applicable for non-PoE capable ports, and should not be included in outgoing LLDP-MED LLDPDUs on such ports.

10.2.1.2 Endpoint Class I TLV Set

The Endpoint Class I TLV set, defined in Table 6, specifies the usage of LLDP-MED TLVs for Generic Endpoint Devices (Class I).

Table 6 – Endpoint Class I TLV Set

LLDP-MED TLV Subtype	TLV Name	LLDPDU Usage	Subclause Reference
1	LLDP-MED Capabilities	M	10.2.2
2	Network Policy	O	10.2.3
4	Extended Power-via-MDI	C[1]	10.2.5

Note 1: Extended Power-via-MDI TLV is mandatory for IEEE 802.3af compliant PD Endpoint Devices. This TLV is not applicable for non-PoE capable ports, and should not be included in outgoing LLDP-MED LLDPDUs on such ports.

10.2.1.3 Endpoint Class II TLV Set

The Endpoint Class II TLV set, defined in Table 7, specifies the usage of LLDP-MED TLVs in LLDPDUs for Media Endpoint Devices (Class II).

Table 7 – Endpoint Class II TLV Set

LLDP-MED TLV Subtype	TLV Name	LLDPDU Usage	Subclause Reference
1	LLDP-MED Capabilities	M	10.2.2
2	Network Policy	M	10.2.3
4	Extended Power-via-MDI	C[1]	10.2.5

Note 1: Extended Power-via-MDI TLV is mandatory for IEEE 802.3af compliant PD Endpoint Devices. This TLV is not applicable for non-PoE capable ports, and should not be included in outgoing LLDP-MED LLDPDUs on such ports.

10.2.1.4 Endpoint Class III TLV Set

The Endpoint Class II TLV set, defined in Table 8, specifies the usage of LLDP-MED TLVs in LLDPDUs for Communication Device Endpoints (Class III).

Table 8 – Endpoint Class III TLV Set

LLDP-MED TLV Subtype	TLV Name	LLDPDU Usage	Subclause Reference
1	LLDP-MED Capabilities	M	10.2.2
2	Network Policy	M	10.2.3
3	Location Identification	O	10.2.4
4	Extended Power-via-MDI	C[1]	10.2.5

Note 1: Extended Power-via-MDI TLV is mandatory for IEEE 802.3af compliant PD Endpoint Devices. This TLV is not applicable for non-PoE capable ports, and should not be included in outgoing LLDP-MED LLDPDUs on such ports.

10.2.1.5 Optional Inventory Management TLV Set

Table 9, below, specifies the usage of the optional to implement LLDP-MED Inventory Management TLV set in LLDPDUs. Note that if any of the Inventory Management TLVs are implemented, then all shall be implemented.

Table 9 – Optional Inventory Management TLV Set

LLDP-MED TLV Subtype	TLV Name	LLDPDU Usage	Subclause Reference
5	Inventory - Hardware Revision	R[1]	10.2.6.1
6	Inventory - Firmware Revision	R[1]	10.2.6.2
7	Inventory - Software Revision	R[1]	10.2.6.3
8	Inventory - Serial Number	R[1]	10.2.6.4
9	Inventory - Manufacturer Name	R[1]	10.2.6.5
10	Inventory - Model Name	R[1]	10.2.6.6
11	Inventory - Asset ID	R[1]	10.2.6.7

Note 1: Recommended that these TLVs be included in outgoing LLDPDUs for LLDP-MED Devices that do not support SNMP or the Entity MIB. These TLVs are not recommended to be included in outgoing LLDPDUs for LLDP-MED Devices that support SNMP and the Entity MIB.

10.2.2 LLDP-MED Capabilities TLV

The LLDP-MED Capabilities TLV allows LLDP-MED Network Connectivity Devices to definitively determine whether particular connected devices do support LLDP-MED, and if so, to discover which specific LLDP-MED TLVs the particular Endpoint Devices are capable of supporting as well as what specific Device Class they belong to.

The LLDP-MED Capabilities TLV also allows LLDP-MED Endpoint Devices to discover which specific LLDP-MED TLVs the Network Connectivity Device they are connected to is capable of supporting.

Figure 6, below, shows the format of this TLV.

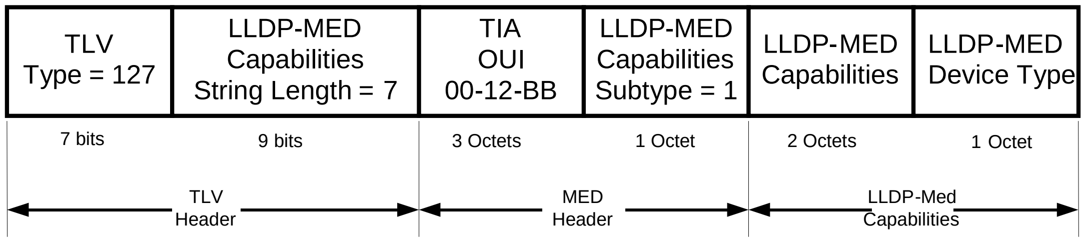

Figure 6 – LLDP-MED Capabilities TLV Format

10.2.2.1 LLDP-MED Capabilities

This field contains a bit-map of the supported set of capabilities that define the primary function(s) of the port. The bit position for each function and the associated bits in the LLDPXMedCapabilities Textual Convention, as defined in section 13, LLDP-MED MIB Module (Normative), are listed in Table 10 below. A binary one in the associated bit indicates the existence of that capability.

NOTE – There is no need to explicitly send the set of enabled capabilities, since the receiver will detect what is enabled by the LLDP-MED TLVs it is receiving. Doing so would provide no additional value and would complicate the frame validation rules in the event of a mismatch.

Individual systems may indicate more than one implemented functional capability, shall indicate all fully implemented capabilities, and shall not indicate any capability that is not implemented. Refer to section 8, LLDP-MED Device Requirements (Normative), for a complete listing of specific support requirements for each LLDP-MED Device Type.

Table 10 – LLDP-MED Capability Values

Bit Position	Capability	LLDPXMedCapabilities TC bit
0	LLDP-MED Capabilities	capabilities(0)
1	Network Policy	networkPolicy(1)
2	Location Identification	location(2)
3	Extended Power via MDI – PSE	extendedPSE(3)
4	Extended Power via MDI – PD	extendedPD(4)
5	Inventory	inventory(5)
6-15	reserved	—

10.2.2.2 LLDP-MED Device Type

This field contains a value that indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, which Endpoint Class it belongs to. The mapping of values to LLDP-MED Device Type is listed in Table 11, below.

Table 11 – LLDP-MED Device Type Values

Value	LLDP-MED Device Type
0	Type Not Defined
1	Endpoint Class I
2	Endpoint Class II
3	Endpoint Class III
4	Network Connectivity
5 – 255	Reserved

10.2.2.3 LLDP-MED Capabilities TLV usage rules

All LLDP-MED LLDPDUs shall contain exactly one LLDP-MED Capabilities TLV, and this TLV shall always be the first LLDP-MED TLV contained in the LLDPDU.

All LLDP-MED Devices shall set the appropriate bit-values in the LLDP-MED Capabilities Field for each LLDP-MED TLV supported.

All LLDP-MED Devices shall set the appropriate value in the LLDP-MED Device Type field to indicate their specific Device Type.

10.2.3 Network Policy TLV

The Network Policy Discovery TLV allows both Network Connectivity Devices and Endpoints to advertise VLAN configuration and associated Layer 2 and Layer 3 attributes that apply for a set of specific applications on that port. In addition, an LLDP-MED Endpoint should advertise this TLV for supported application types, to enable the discovery of specific policy information and diagnosis of network policy configuration mismatch issues.

Every port on a Network Connectivity Device may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

NOTE – Network based authentication technologies such as IEEE 802.1X™ along with RADIUS attributes [33] could be used to determine the appropriate network policies for a given port, however specification of such mechanisms is outside the scope of this standard.

This TLV is only intended for use with application types that have specific real-time network policy requirements, such as interactive voice and/or video services.

This TLV is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link.

The LLDP-MED network policy TLV is a fixed length TLV that allows Network Connectivity Devices and Endpoint Devices to advertise the specific port's VLAN type, VLAN identifier (VID), and both the Layer 2 and Layer 3 priorities associated with a specific set of application types. Figure 7, below, shows the format of this TLV.

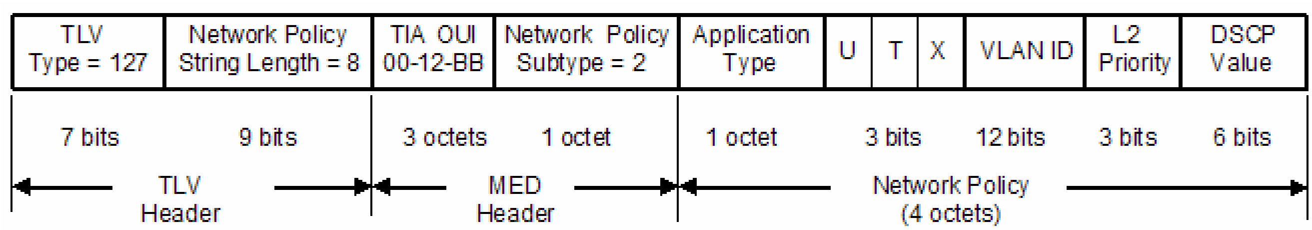

Figure 7 – Network Policy TLV Format

10.2.3.1 Application Type

This field shall contain an integer value indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device, as define in Table 12, below. This allows an Endpoint to support various different application types (e.g. voice and video) by advertising multiple network policy TLVs within an LLDPDU, each having a unique application type value.

Table 12 – Application Type

Application Type Value	Value Meaning
0	Reserved
1	Voice
2	Voice Signaling[1]
3	Guest Voice
4	Guest Voice Signaling[1]
5	Softphone Voice
6	Video Conferencing
7	Streaming Video
8	Video Signaling[1]
9 – 255	Reserved

Note 1: The “signaling” application types are conditional and should not be advertised if all the same network policies apply for signaling/control packets as apply for the related “media” stream.

Intended use of the application types:

- Voice – for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

- Voice Signaling (conditional) – for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice policy TLV.

- Guest Voice – to support a separate “limited feature-set” voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

- Guest Voice Signaling (conditional) – for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice policy TLV.

- Softphone Voice – for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an ‘untagged’ VLAN or a single ‘tagged’ data specific VLAN. When a network policy is defined for use with an ‘untagged’ VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.

- Video Conferencing – for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

- Streaming Video – for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

- Video Signaling (conditional) – for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing policy TLV.

10.2.3.2 Unknown Policy Flag (U)

This field shall contain a 1-bit flag indicating that an Endpoint Device wants to explicitly advertise that this policy is required by the device, but is currently unknown.

A value of 1 indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID, Layer 2 priority and DSCP value fields are ignored.

A value of 0 indicates that this network policy is defined.

10.2.3.3 Tagged Flag (T)

This field shall contain a 1-bit flag indicating whether the specified application type is using a ‘tagged’ or an ‘untagged’ VLAN.

A value of 0 indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003 [4]. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

A value of 1 indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003 [4].

10.2.3.4 Reserved (X)

This 1-bit field is reserved for future standardization.

10.2.3.5 VLAN ID

This field shall contain the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003 [4]. This field is 12 bits in length and may contain a value as defined in Table 13, below.

Table 13 – VLAN ID

VLAN ID Value	Value Meaning
0	Priority Tagged
1 - 4094	VLAN ID
4095	Reserved

A value of 1 through 4094 is used to define a valid VLAN ID.

A value of 0 (Priority Tagged) shall be used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003 [4], meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

A value of 4095 is reserved for implementation use.

10.2.3.6 Layer 2 Priority

This field shall contain the Layer 2 priority to be used for the specified application type. This 3 bit field may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004 [3]. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

10.2.3.7 DSCP Value

This field shall contain the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474 [5]. This 6 bit field may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

NOTE – The class selector DSCP values are backwards compatible for devices that only support the old IP precedence Type Of Service (TOS) format.

10.2.3.8 Network Policy TLV usage rules

All LLDP-MED Network Connectivity Devices and Endpoint Devices should advertise a Network Policy TLV for all network policies that are configured and apply on a given port.

An LLDP-MED Endpoint Device should advertise a network policy with the ‘Unknown Policy’ bit set for an application type that it requires but has not been configured. This also applies for Endpoints that are in the process of auto configuration using DHCP extensions, or other techniques. This is to support efficient diagnosis of network policy configuration errors.

An LLDP-MED Network Connectivity Device shall not advertise a network policy with the ‘Unknown Policy’ bit set, to conserve TLV space.

If more than one Network Policy TLV is defined within an LLDPDU, then the application type shall be different from any other Network Policy TLV application type in the LLDPDU.

If an untagged VLAN is advertised, the endpoint application should use DSCP prioritization; otherwise, the Network Connectivity Device may not be able to prioritize time-sensitive traffic ahead of normal packets. This is due to the fact that deep packet inspection or state-full packet classification required for detecting media traffic streams (e.g. RTP) are outside the scope of this standard.

10.2.4 Location Identification TLV

The Location Identification Discovery extension provides for advertisement of location identifier information to Communication Endpoint Devices (Class III), based on configuration of the Network Connectivity Device it is connected to. This is expected to be related to wire map or similar network topology data, such that the configuration of the Network Connectivity Device is able to uniquely identify the physical location of the connected MED Endpoint, hence the correct location identifier information for it to use.

NOTE – While this extension is intended to be general in nature, able to provide location data applicable to a wide range of location-based applications, Emergency Call Service location is a critically important application. This method of location data distribution is specifically intended to support and harmonize with TIA-TSB-146 Emergency Call Services [23], NENA [21] or other similar standards as an optional method of providing this information within the context of those applications. This Standard does not specify any particular application level usage of this TLV information.

There are three forms this identifier information may be delivered in defined by this Standard:

a) Coordinate-based LCI as defined by IETF RFC 3825 [6],

b) Civic Address LCI as defined by IETF (refer to ANNEX B),

c) Emergency Call Services ELIN, as described for example by NENA TID 07-501 [21].

Future extensions to this TLV are allowed for, however are not specifically defined here.

One or more of these methods is potentially used for delivery of location identifier data to the Communication Endpoint Device, using this TLV, as configured in the LLDP-MED Network Connectivity Device. If multiple location data subtypes are configured in the Network Connectivity Device, all shall be advertised.

The LLDP-MED Location Identification TLV (Location ID) allows the Network Connectivity Devices to advertise the appropriate location identifier information for an Endpoint to use in the context of location-based applications. The format of this TLV is shown in Figure 8, below.

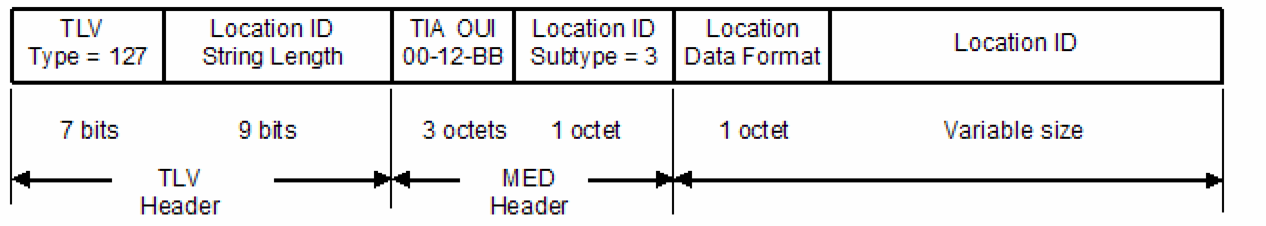

Figure 8 – Location Identification TLV Format

10.2.4.1 Location ID string length

This field shall contain the exact length, in octets, of the Location ID data field + 5.

10.2.4.2 Location data format

This field shall contain an integer octet index indicating the specific Location ID data format being delivered in the Location ID field, as defined in Table 14, below. These specific formats are defined in section 10.2.4.3, below.

Table 14 – Location data format type values

Location data format type value	**Data type provided**	**Location ID data length** (octets)
0	Invalid	Invalid
1	Coordinate-based LCI	16
2	Civic Address LCI	6 to 256
3	ECS ELIN	10 to 25
4 - 255	Reserved for future expansion	Reserved

10.2.4.3 Location ID

Three Location ID data formats are defined in this release of this Standard, for use in the Location ID field.

10.2.4.3.1 Coordinate-based LCI data format

In alignment with directions being taken by NENA [21] and TIA-TSB-146 [23], the IETF Geopriv Coordinate-based Location Configuration Information (Coordinate-based LCI) identifier data format is defined to reuse the relevant sub-fields of the DHCP Option for Coordinate LCI as specified in RFC 3825 [6]. The format of this identifier subtype is shown in Figure 9, below.

0		16	32	39
LaRes (6 bit)		**Latitude** (34 bit)		
LoRes (6 bit)		**Longitude** (34 bit)		
AT (4 bit)	**AltRes** (6 bit)	**Altitude** (30 bit)		
Datum (8 bit)				

Figure 9 – Coordinate-based LCI data format

The precise definitions of all sub-fields within this format shall be as defined in RFC 3825 [6].

The data length of this format is exactly 128 bits, or 16 octets.

10.2.4.3.2 Civic Address LCI data format

In alignment with directions being taken by NENA [21] and TIA-TSB-146 [23], the IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI) identifier data format is defined to reuse the relevant sub-fields of the DHCP Option for Civic Address LCI as specified by IETF (refer to ANNEX B). The format of this identifier subtype is shown in Figure 10, below.

0	8	16	24	31
LCI Length (1 octet)	**What** (1 octet)	**Countrycode** (2 octets)		
CAtype (1 octet)	**CAlength** (1 octet)	**CAvalue** (variable 0 – 250 octets) • • •		

• • • **additional civic address elements** • • •

1 or more civic address elements

Figure 10 – Civic Address LCI data format

The LCI Length sub-field shall contain the total length in octets of all subsequent sub-fields of the Civic Address LCI data format, not including the LCI Length octet itself. The LCI Length sub-field corresponds to the 'N' (option length) field of the DHCPv4 format for Civic Address LCI defined by IETF (refer to ANNEX B) and in turn to the 'Len' field defined for variable length DHCP options in IETF RFC 2132 [30].

The precise definitions of the 'What', 'Countrycode', 'CAtype', 'CALength' and 'CAvalue' sub-fields within this format shall be as defined in the IETF Civic Address LCI (refer to ANNEX B) for the DHCPv4 encoding of those fields.

The value used in the What field shall be set to 2, corresponding to the location of the client device, as defined in the IETF Civic Address LCI (refer to ANNEX B).

The value used in the Countrycode field shall be as defined in the IETF Civic Address LCI (refer to ANNEX B) for the country in which the Endpoint Device is physically located.

The data length of this format is variable, given by the value of the LCI Length field + 1, ranging from a minimum of 6 octets (LCI Length = 5) to a maximum of 256 octets (LCI Length = 255), depending on specific civic address elements included.

NOTE 1 – The IETF Civic Address LCI (refer to ANNEX B) defines both DHCPv4 and DHCPv6 formats. The DHCPv4 format is followed here. These formats differ only in the size of the LCI Length field ('N' field in the DHCP format), which is 2 octets in the DHCPv6 encoding.

NOTE 2 – While the total number of civic address elements theoretically included in this LCI could potentially cause its size to exceed 256 octets, this is not a practical consideration. Since only a limited number of civic address elements are required in most circumstances to adequately specify location, and most are small by definition, it is very unlikely that the limit will be exceeded. The maximum size of 256 octets was chosen for alignment with the DHCPv4 equivalent data as defined in the IETF Civic Address LCI (refer to ANNEX B).

NOTE 3 – Of the numerous civic address element types defined in the IETF Civic Address LCI (refer to ANNEX B), some may be considered critically important for successful operation of applications of this Location Identification TLV subtype. However definition of specific required, recommended or optional elements to be included is outside the scope of this Standard, and left to definition by the specific applications. Implementers and network administrators are strongly urged to consult applicable standards related to applications of this Location Identification TLV subtype for specific requirements on element types to be included. In the specific case of Emergency Call Service applications, it is expected that sufficient civic address elements are needed to specifically and consistently identify the emergency location making the call, to the resolution required by the applicable civic authority.

10.2.4.3.3 ECS ELIN data format

In alignment with directions being taken by NENA [21] and TIA-TSB-146 [23], the Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The data format of this identifier subtype is shown in Figure 11, below.

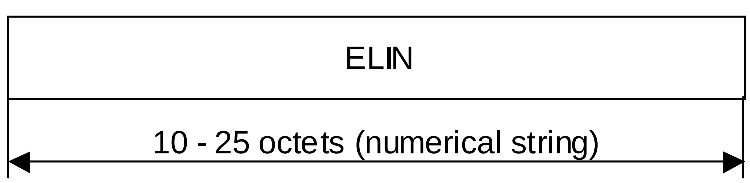

Figure 11 – ECS ELIN data format

This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

The data length of this format is variable, given by the Location ID string length field value - 5, ranging from a minimum of 10 octets (Location ID string length = 15) to a maximum of 25 octets (Location ID string length = 30).

NOTE 1 – While the ELIN number string currently used in North America is 10 digits in length, provision is made here to allow for longer strings for future extensibility purposes. The maximum number length defined for the International ISDN Number plan is 15, as defined by ITU-T Recommendation E.164 [34].

NOTE 2 – Unlike the previously defined location identifier subtypes, the ECS ELIN subtype is expected to be specifically for use in Emergency Call Service applications.

10.2.4.4 Location Identification TLV usage rules

All LLDP-MED Network Connectivity Devices shall advertise exactly one Location Identification TLV for each Location identifier subtype they are configured to support. All LLDP-MED Network Connectivity Devices shall support configuration and transmission of all of Coordinate-based LCI, Civic Address LCI and ECS ELIN identifier subtypes. If a particular Location identifier subtype is supported for configuration in the Network Connectivity Device, but is not configured, the corresponding TLV for this identifier subtype shall not be delivered.

All LLDP-MED Communications Endpoint Devices (Class III) shall support reception of at least three Location Identification TLVs. All LLDP-MED Communications Endpoint Devices (Class III) shall support reception of any or all of Coordinate-based LCI, Civic Address LCI and ECS ELIN identifier subtypes.

NOTE – The intention of allowing multiple Location Identification TLV subtypes to be configured and advertised is to allow arbitrary configuration to support whatever location-based applications are of relevance to the devices involved in the particular network environment. An important use case is the ESC application where, in North America, the NENA standards [21] mandate delivery of all available forms of location data to the PSAP.

LLDP-MED Communications Endpoint Devices (Class III) may transmit Location Identification TLVs if they are capable of either automatically determining their physical location (e.g. by use of GPS, radio beacon or similar) or are capable of being statically configured with this information. Endpoint Devices that are capable of automatically determining their physical location should not transmit the corresponding Location Identification TLV(s) containing this location information until it has been determined to be current and accurate. Such Endpoint Devices should not transmit out-of-date or obsolete location information.

Usage of the data supplied by this TLV to LLDP-MED Endpoint Devices (Class III) or to Network Connectivity Devices is application-specific and not defined here.

10.2.5 Extended Power-Via-MDI TLV

The Extended Power-Via-MDI TLV is intended to enable advanced power management between LLDP-MED Endpoint and Network Connectivity Devices. The Extended Power-Via-MDI TLV allows advertisement of fine grained power requirement details, Endpoint power priority, as well as both Endpoint and Network Connectivity Device power status. For the purpose of advanced power management functions, this TLV provides significantly more value than the IEEE 802.1AB Power Via MDI TLV, referenced in section 9.2.4of this Standard.

The Extended Power-Via-MDI TLV does not provide for power negotiation capabilities between the Endpoint and Network Connectivity Devices. The data carried in this TLV from Endpoint Devices to

Network Connectivity Devices does not set power policy in the Network Connectivity Devices, although the data may be used to influence those policies. Setting of power management policy is outside the scope of this Standard.

The LLDP-MED Extended Power-via-MDI TLV allows the media endpoint to advertise its IEEE 802.3af power related information. The format of this TLV is shown in Figure 12, below.

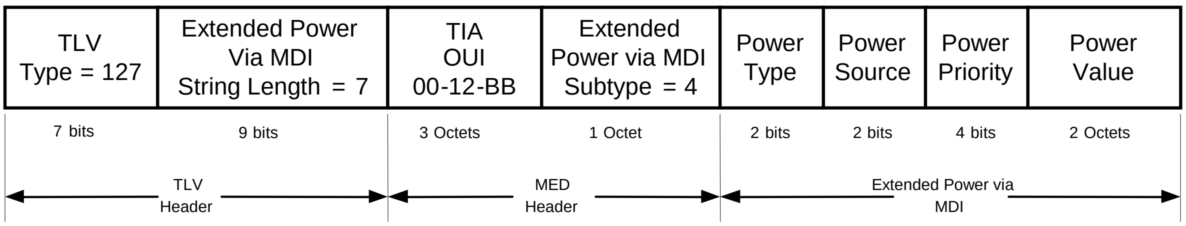

Figure 12 – Extended Power-via-MDI TLV Format

10.2.5.1 Power Type

The Power Type field contains a binary value that represents whether LLDP-MED device transmitting the LLDPDU is a Power Sourcing Entity (PSE) or Power Device (PD). The binary value for each possible device is represented in Table 15, below.

Table 15 – Power-via-MDI Device Type Field Values

Binary Value	Power Type
0 0	PSE Device
0 1	PD Device
1 0	Reserved
1 1	Reserved

10.2.5.2 Power Source

The Power Source field shall contain a binary value that represents the power source being utilized by a PSE or PD device. An LLDP-MED device shall insert information into the Power Source field based on the type of device it is, in accordance with the values listed in Table 16, below.

Table 16 – Power Source Field Values

Binary Value	PD Device Types	PSE Device Types
0 0	Unknown	Unknown
0 1	PSE	Primary Power Source
1 0	Local	Backup Power Source, Power conservation mode
1 1	PSE and Local	Reserved

The value advertised by this field should be used by Endpoint devices to infer the power capability of the Network Connectivity Device it is attaching to. When the Network Connectivity Device advertises that it is using its primary power source, then the Endpoint should assume that they will have uninterrupted access to the power level advertised by the PSE Power Available field. If the Network Connectivity Device advertises that it is using backup power, then the Endpoint should infer that it may not expect continuous power. The Endpoint may additionally choose to power down non-essential subsystems or transition to a power conservation mode for as long a period as the PSE device is advertising that it is operating on backup power.

If a PD device is advertising that it is utilizing a local power source, the PSE device may choose to disable MDI power to the PD device when it is operating on a backup power source.

10.2.5.3 Power Priority

This field shall contain a binary value that represents the priority of the PD type device to the power being supplied by the PSE type device, or the power priority associated with the PSE type device's port that is sourcing the power via MDI. There are three levels of power priority represented by this field, corresponding to the three levels as defined by IETF RFC 3621 [7] in the pethPsePortPowerPriority object. The binary value for each possible power priority level is represented in Table 17, below.

Table 17 – Power Priority Field Values

Binary Value	Power Priority	IETF RFC 3621 MIB Object
0 0 0 0	Unknown	—
0 0 0 1	Critical	pethPsePortPowerPriority=1
0 0 1 0	High	pethPsePortPowerPriority=2
0 0 1 1	Low	pethPsePortPowerPriority=3
0 1 0 0 – 1 1 1 1	Reserved	—

PSE devices shall advertise the power priority configured on each of its ports where Power-Via-MDI services are enabled. If the power priority for a port on a PSE is unknown or not defined, then the PSE Device shall set the Power Priority field to Unknown for that port.

PD devices shall advertise the power priority configured for the device. If a PD device is unable to determine its power priority or it has not been configured, then the PD device shall set the power priority field to Unknown.

A PD device shall not change the Power Priority value it is advertising to match that of the PSE Power Priority value as result of receiving a TLV containing a Power Priority value from a PSE device that is different from the value the PD device has been configured to expect.

In the event that a PSE device receives a TLV containing a Power Priority value from a PD device that is different from the value the PSE device has been configured to enforce, the PSE device shall not change the Power Priority value it is advertising to match that of the PD Power Priority value.

NOTE 1 – The above statements are with respect to LLDP-MED protocol operation only, and do not set requirements on the application layer. The application(s) sitting on top of LLDP-MED may make use of information provided through the corresponding MIB objects, for example to adjust power policy (and hence PD Priority advertised) in the Network Connectivity Device side, or either end may be changed due to administration.

NOTE 2 – The use of this field allows network operators to quickly detect a configuration mismatch, between endpoints and network connectivity devices. As an example, if a high priority endpoint is attached to a low priority port, then network operators would be capable of quickly diagnosing the mismatch.

10.2.5.4 Power Value

The Power Value field shall contain a numerical value that indicates the total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The Power Value field is two octets wide of which 10 bits are used to indicate the power required by a PD device or power available by a PSE type device.

The Power Value field is divided into 4096 increments, with each increment representing 0.1 Watts of power. As an example, if the Power Value field contained a value of 96 decimal and the TLV was being transmitted by a PSE type device, then PD type receiving device would interpret that the PD available power on a maximum length cable as 9.6 Watts. The Power Value field format is represented in Table 18, below.

Table 18 – Power Value Field Format

Integer Value	Power Value
0 – 1023	0 – 102.3 Watts
1024 – 65536	Reserved

NOTE – IEEE 802.3af compliant PSE devices can currently provide a maximum of 12.95 Watts over a maximum length cable (field value of 129). The Power Value field supports a maximum power required or available value of 102.3 Watts (field value of 1023) to allow for future expansion.

If a PSE Network Connectivity Device is incapable of determining the exact power it can provide to a PD Endpoint Device, then it shall transmit a Power Value associated with the 802.3af class the port supports. If a PD Endpoint Device is incapable of determining the exact power it requires, then it shall transmit a Power Value of the 802.3af power class it belongs to. Table 19, below, provides a reference of IEEE 802.3af power classes and their associated Power Values.

Table 19 – Mapping of IEEE 802.3af Power Class to Power Value

IEEE 802.3 AF Power Class	Minimum Power Level Output at the PSE	Maximum Power Levels at the PD	Power Value
0	15.4W	0.44 to 12.95W	130
1	4.0W	0.44 to 3.84W	38
2	7.0W	3.84 to 6.49W	65
3	15.4W	6.49 to 12.95W	130

The Power Value field shall represent the maximum power consumption of an Endpoint Device or the minimum power available from a PSE port of a Network Connectivity Device when the LLDPDU is transmitted. It shall not be used to indicate instantaneous variations of power required or offered at the time of transmission of the LLDPDU.

Specifically, a PD Endpoint Device shall advertise the maximum power it can consume during normal operation in its current configuration (e.g. power required during an active call using its most power-consuming transducers, display backlight on, etc), even if its actual power draw at that instant of time is less than the advertised power draw. If a PD Endpoint Device is capable of determining that it is currently receiving power from a local power source, it shall advertise the maximum power that it would consume during normal PD operation if that external power were to be removed or fail.

A PD Endpoint Device may advertise a power value lower than a previously advertised value if, due to a hardware reconfiguration, it will consume less power than it previously did (e.g. if an auxiliary module is removed, a docked PDA is removed, etc).

A PD Endpoint Device shall not advertise a higher power value than the IEEE 803.3af power class to which it belongs.

A PD Endpoint Device that requires more power than previously advertised, due to a hardware reconfiguration, shall not advertise a higher power value than is currently advertised by the PSE Network Connectivity Device it is connected to on that port.

If the PD Endpoint Device requires power greater than either the power value currently advertised by the PSE Network Connectivity Device or the upper power limit of the corresponding IEEE 802.3af power class, then it must renegotiate this new power limit by resetting the port (i.e. by triggering renegotiation of power at the IEEE 802.3af level).

It is expected that Endpoint Devices supporting advanced power management features would potentially be capable of operating in a power conservation mode when they detect that the PSE Network Connectivity Device is operating on backup power. If an Endpoint Device supports a power conservation mode where it may operate with reduced maximum power consumption, it shall continue to advertise the maximum power value it would consume during normal PD operation.

A PSE Network Connectivity Device shall advertise the minimum power it is capable of delivering on its ports. If reduced power is available due to the Network Connectivity Device operating on backup power, this reduced power capability shall be advertised while the condition persists.

10.2.5.5 Extended Power-Via-MDI TLV usage rules

LLDP-MED Endpoint Devices and Network Connectivity Devices shall advertise at most one Extended Power-Via-MDI TLV per LLDPDU.

Usage of the data supplied by the Extended Power-Via-MDI TLV from LLDP-MED Endpoint Devices to Network Connectivity Devices is not binding on the power management behavior of the Network Connectivity Devices. Specifically, the power policy executed by the Network Connectivity Devices is not assumed to be dictated by the supplied data (although it is permissible for this policy to be modified by the data supplied). Behavior with respect to changes to the advertised power priority expected by PD Endpoint Devices or being supplied by PSE Network Connectivity Devices shall be in accordance with the rules for manipulation of the Power Priority field as defined in section 10.2.5.3, above. Behavior with respect to changes to the advertised maximum power required by PD Endpoint Devices or capable of being supplied by PSE Network Connectivity Devices shall be in accordance with the rules for manipulation of the Power Value field as defined in section 10.2.5.4, above.

10.2.6 Inventory Management TLV Set

Inventory information is important in a managed VoIP network. The administrative tasks of managers of such networks is made more difficult in this respect by the lack of standard interfaces for assets or inventory management in VoIP entities, and the lack support of management protocols such as SNMP in the majority of IP Phone implementations.

The standard SNMP MIB module that provides basic inventory management information is the IETF Entity MIB, RFC 2737 [20]. The relevant objects within that MIB module are part of the entPhysicalTable. Table 20, below, shows the mapping between the LLDP-MED Inventory TLVs and the entPhysicalTable objects.

Table 20 – Inventory TLV to Entity MIB Mapping

LLDP-MED Inventory TLV	EntPhysicalTable Object
Hardware Revision	entPhysicalHardwareRev
Firmware Revision	entPhysicalFirmwareRev
Software Revision	entPhysicalSoftwareRev
Serial Number	entPhysicalSerialNum
Manufacturer Name	entPhysicalMfgName
Model Name	entPhysicalModelName
Asset ID	entPhysicalAssetID

The Inventory Management TLV set is optional to implement for all LLDP-MED Devices. If support for any of the TLVs in the Inventory Management set is implemented, then support for all Inventory Management TLVs shall be implemented.

In the case that SNMP and the Entity MIB are supported in the LLDP-MED Endpoint Device, implementation of the Inventory TLVs is not recommended, since a management application can retrieve this information directly from the Endpoint Devices. Otherwise, if SNMP is not supported or the Entity MIB is not supported, then support of the Inventory Management TLV Set is recommended.

NOTE – Some more complex IP Phones may include sub-systems, sometimes from different vendors. The Entity MIB provides an answer to such issues by defining containment relationships between entities. In such cases the IP Phone should transfer through LLDP-MED the inventory information specific to the highest level contained (typically 'chassis' level) in the Entity MIB.

10.2.6.1 Hardware Revision TLV

The LLDP-MED hardware Revision TLV allows the endpoint to advertise its hardware revision. The format of this TLV is shown in Figure 13, below.

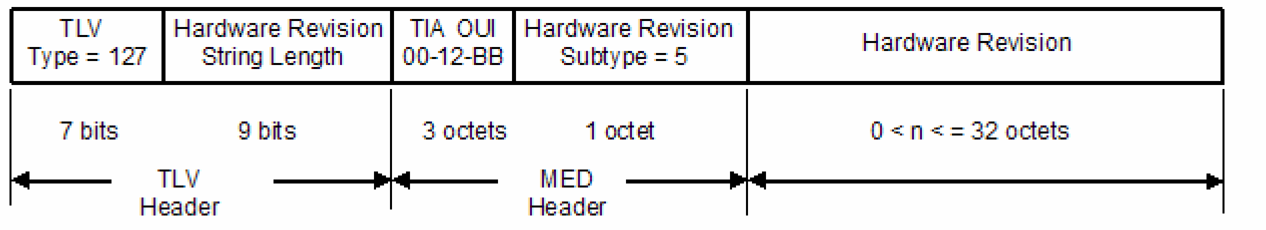

Figure 13 – Hardware Revision TLV Format

10.2.6.1.1 Hardware Revision string length

This field shall contain the exact length, in octets of the hardware revision field plus 4.

10.2.6.1.2 Hardware revision

This field shall contain an alphanumerical string that contains the hardware revision of the endpoint. The preferred value is the hardware revision value printed on the device itself (if available). If the revision information is stored internally in a non-printable (e.g., binary) format, then the Endpoint software shall convert such information to a printable format, in a manner that is implementation-specific. If the implementation supports IETF RFC 2737, the use of the entPhysicalHardwareRev object is recommended for this field.

10.2.6.1.3 Hardware revision TLV usage rules

An LLDPDU shall not contain more than one hardware revision TLV.

10.2.6.2 Firmware Revision TLV

The LLDP-MED firmware Revision TLV allows the endpoint to advertise its firmware revision. The format of this TLV is shown in Figure 14, below.

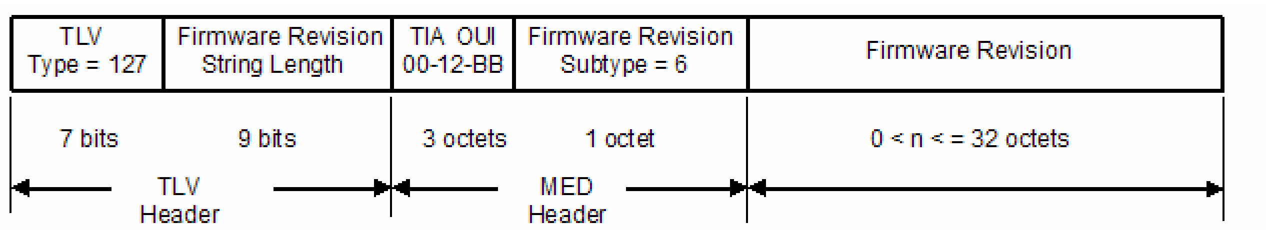

Figure 14 – Firmware Revision TLV Format

10.2.6.2.1 Firmware Revision string length

This field shall contain the exact length, in octets, of the firmware revision field plus 4.

10.2.6.2.2 Firmware revision

This field shall contain an alphanumerical string that contains the hardware revision of the endpoint. If the revision information is stored internally in a non-printable (e.g., binary) format, then the endpoint software shall convert such information to a printable format, in a manner that is implementation-specific. If implementations support IETF RFC 2737, the use of the entPhysicalFirmwareRev object is recommended for this field.

10.2.6.2.3 Firmware revision TLV usage rules

An LLDPDU shall not contain more than one firmware revision TLV.

10.2.6.3 Software Revision TLV

The LLDP-MED Software Revision TLV allows the endpoint to advertise its hardware revision. The format of this TLV is shown in Figure 15, below.

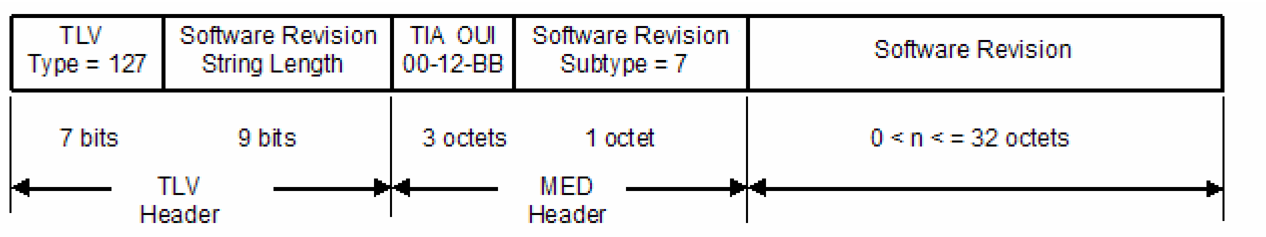

Figure 15 – Software Revision TLV Format

10.2.6.3.1 Software Revision string length

This field shall contain the exact length, in octets, of the software revision field plus 4.

10.2.6.3.2 Software revision

This field shall contain an alphanumerical string that contains the software revision of the endpoint. If the revision information is stored internally in a non-printable (e.g., binary) format, then the endpoint software shall convert such information to a printable format, in a manner that is implementation-specific. If implementations support IETF RFC 2737, the use of the entPhysicalSoftwareRev object is recommended for this field.

10.2.6.3.3 Software revision TLV usage rules

An LLDPDU shall not contain more than one software revision TLV.

10.2.6.4 Serial Number TLV

The LLDP-MED hardware Revision TLV allows the endpoint to advertise its serial number. The format of this TLV is shown in Figure 16, below.

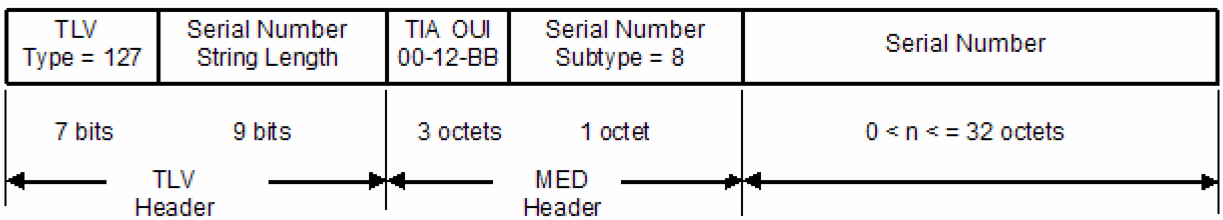

Figure 16 – Serial Number TLV Format

10.2.6.4.1 Serial Number string length

This field shall contain the exact length, in octets, of the serial number field plus 4.

10.2.6.4.2 Serial number

This field shall contain an alphanumerical string that contains the serial number of the endpoint. The preferred value is the serial number value printed on the device itself (if available). If the serial number information is stored internally in a non-printable (e.g., binary) format, then the endpoint software shall convert such information to a printable format, in a manner that is implementation-specific. If implementations support IETF RFC 2737, the use of the entPhysicalSerialNum object is recommended for this field.

10.2.6.4.3 Serial number TLV usage rules

An LLDPDU shall not contain more than one serial number TLV.

10.2.6.5 Manufacturer Name TLV

The LLDP-MED Manufacturer Name TLV allows the endpoint to advertise the name of its manufacturer. The format of this TLV is shown in Figure 17, below.

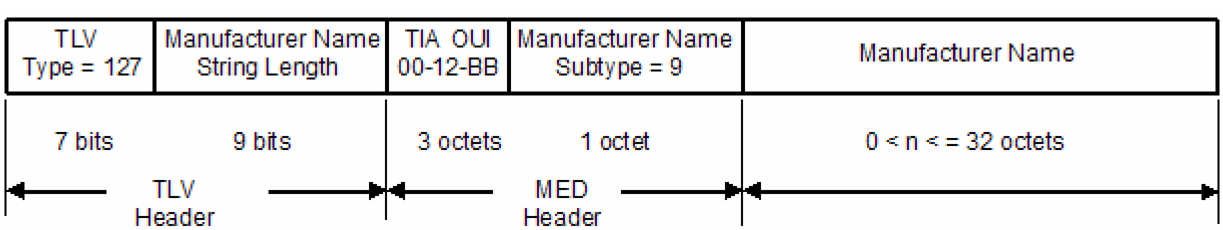

Figure 17 – Manufacturer Name TLV Format

10.2.6.5.1 Manufacturer Name string length

This field shall contain the exact length, in octets, of the manufacturer name field plus 4.

10.2.6.5.2 Manufacturer name

This field shall contain an alphanumerical string that contains the name of the manufacturer of the endpoint. The preferred value is the name of the manufacturer as printed on the device itself (if available). If implementations support IETF RFC 2737, the use of the entPhysicalMfgName object is recommended for this field.

10.2.6.5.3 Manufacturer name TLV usage rules

An LLDPDU shall not contain more than one Manufacturer Name TLV.

10.2.6.6 Model Name TLV

The LLDP-MED Model Name TLV allows the endpoint to advertise its model name. The format of this TLV is shown in Figure 18, below.

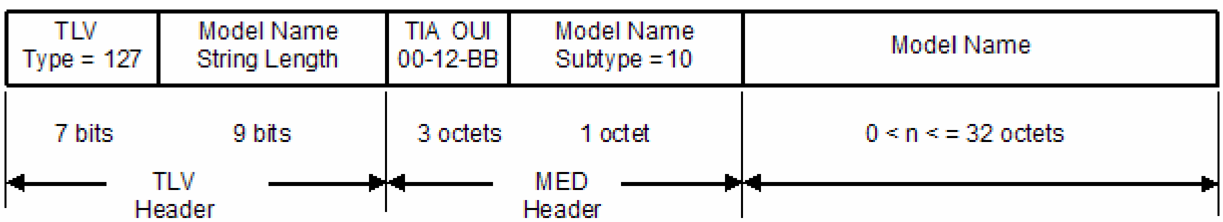

Figure 18 – Model Name TLV Format

10.2.6.6.1 Model Name string length

This field shall contain the exact length, in octets, of the model name field plus 4.

10.2.6.6.2 Model Name

This field shall contain an alphanumerical string that contains the model name of the endpoint. The preferred value is the model name printed on the device itself (if available). If implementations support IETF RFC 2737, the use of the entPhysicalModelName object is recommended for this field.

10.2.6.6.3 Model name TLV usage rules

An LLDPDU shall not contain more than one model name TLV.

10.2.6.7 Asset ID TLV

The LLDP-MED Asset ID TLV allows the endpoint to advertise its asset ID. The format of this TLV is shown in Figure 19, below.

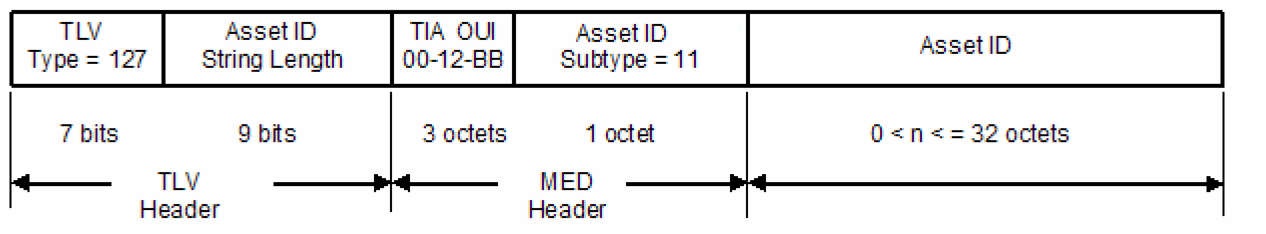

Figure 19 – Asset ID TLV Format

10.2.6.7.1 Asset ID string length

This field shall contain the exact length, in octets, of the Asset ID field plus 4.

10.2.6.7.2 Asset ID

This field shall contain an alphanumerical string that contains the asset identifier of the endpoint. Endpoints are typically assigned asset identifiers by users for the purpose of inventory management and assets tracking. If implementations support IETF RFC 2737, the use of the entPhysicalAssetID object is recommended for this field.

10.2.6.7.3 Asset ID TLV usage rules

An LLDPDU should not contain more than one Asset ID TLV.

11 LLDP-MED Protocol Interactions (Normative)

This section describes the specific requirements pertaining to the LLDP-MED protocol interactions with the local LLDP agent, for a single port, as it applies to both Endpoints and Network Connectivity Devices. It covers the LLDP-MED Fast Start interaction, new LLDP-MED global variables required, protocol initialization, and the specific inter-state-machine interactions between LLDP and LLDP-MED. Implications of interaction with IEEE 802.1X authentication are also briefly discussed.

The operation of the base LLDP protocol can be represented with two simple state machines (transmit and receive), along with the associated timing counters and global variables to indicate when the local system managed object values need to be transmitted and when object values in the local LLDP agent's remote systems MIB will become invalid. See the IEEE 802.1AB specification [1] for definitive details.

Since LLDP-MED has different protocol interaction requirements for Endpoint Devices and Network Connectivity Devices, they are described separately in subsections below.

11.1 Conservation of LLDPDU Space

All TLVs transmitted by IEEE 802.1AB and all extensions to 802.1AB, must fit inside of one LLDPDU. This is a significant limitation for IEEE 802.3 networks, where the maximum LLDPDU length is 1500 octets for a basic, untagged MAC frame.

Since LLDP-MED has defined several TLVs sets that are only applicable and relevant to LLDP-MED Endpoints, Network Connectivity Devices should conserve the LLDPDU space by only transmitting LLDP-MED specific TLV sets on a port after an LLDP-MED Device has been detected on that port, as specified in the following sections.

The selection of optional LLDP-MED TLVs in an LLDPDU should be performed by network management using the LLDP-MED local system MIB, if implemented.

11.2 Network Connectivity Device Protocol Interactions

This section defines the LLDP-MED specific protocol interactions for Network Connectivity Devices.

All Network Connectivity Devices claiming support of this Standard shall support all of the following Network Connectivity Device specific protocol interactions.

11.2.1 Protocol Initialization

A Network Connectivity Device claiming support of this specification shall implement both LLDP transmit and receive. The default value of the 'adminStatus' variable (defined in the LLDP base protocol) shall be set to 'enabledRxTx'. If 'adminStatus' is set to any value other than 'enabledRxTx', then the protocol initialization for LLDP-MED shall be halted.

The following new per-port global variables are defined for Network Connectivity Devices:

a) **‘medTransmitEnabled’**: indicates that LLDP-MED TLVs should be transmitted for this port. This variable is set to TRUE whenever an LLDPDU has been received containing an LLDP-MED Capabilities TLV on a port (see section 10.2.2).

b) ‘**medFastStart’**: a timer indicating that the LLDP-MED Fast Start mechanism is active. This timer is activated whenever an LLDPDU has been received containing an LLDP-MED Capabilities TLV not already associated with a remote MSAP identifier. This timer activation is performed by the receive state machine by setting it based on the ‘medFastStartRepeatCount’ parameter (see section 12.1, LLDP-MED Global Variables, below).

During LLDP-MED initialization and after loss of link, the local LLDP agent on a Network Connectivity Device shall perform the following tasks:

c) Perform the base LLDP protocol initialization

d) Set the ‘medTransmitEnabled’ variable to FALSE

e) Set the ‘medFastStart’ timer to 0

11.2.2 Frame Transmission

A Network Connectivity Device should conserve LLDPDU space by only transmitting LLDP TLVs in LLDPDUs until a device with LLDP-MED Capabilities is detected in the remote system MIB on the port. This selection is performed by the application layer, which should only include LLDP-MED TLVs within outgoing LLDPDUs after an LLDP-MED capable device has been detected on a port, by setting the ‘medTransmitEnabled’ variable to TRUE for that port (see section 11.2.4).

NOTE – Because the selection of which specific TLVs to include in an LLDPDU is an LLDP MIB management function, this TLV selection is not shown as a separate procedure in the transmit state machine diagram.

A Network Connectivity Device shall use the Fast Start mechanism to transmit an LLDP-MED frame whenever the ‘medFastStart’ timer has a non-zero value. This timer will typically span multiple LLDP-MED frame transmissions, with the duration based on the ‘medFastStartRepeatCount’ parameter (see section 12.1, LLDP-MED Global Variables, below).

Successive LLDP-MED frame transmissions are limited to once per second, the minimum interval allowed by the LLDP base protocol, by setting the ‘txDelayWhile’ timer (defined in the base LLDP specification) to 1 while the Fast Start mechanism is active.

11.2.3 Transmit State Machine Diagram

LLDP-MED defines a slightly enhanced transmit state machine for Network Connectivity Devices relative to the LLDP base protocol. The updated transmit state machine for an individual port is shown in Figure 20, below, highlighting the differences.

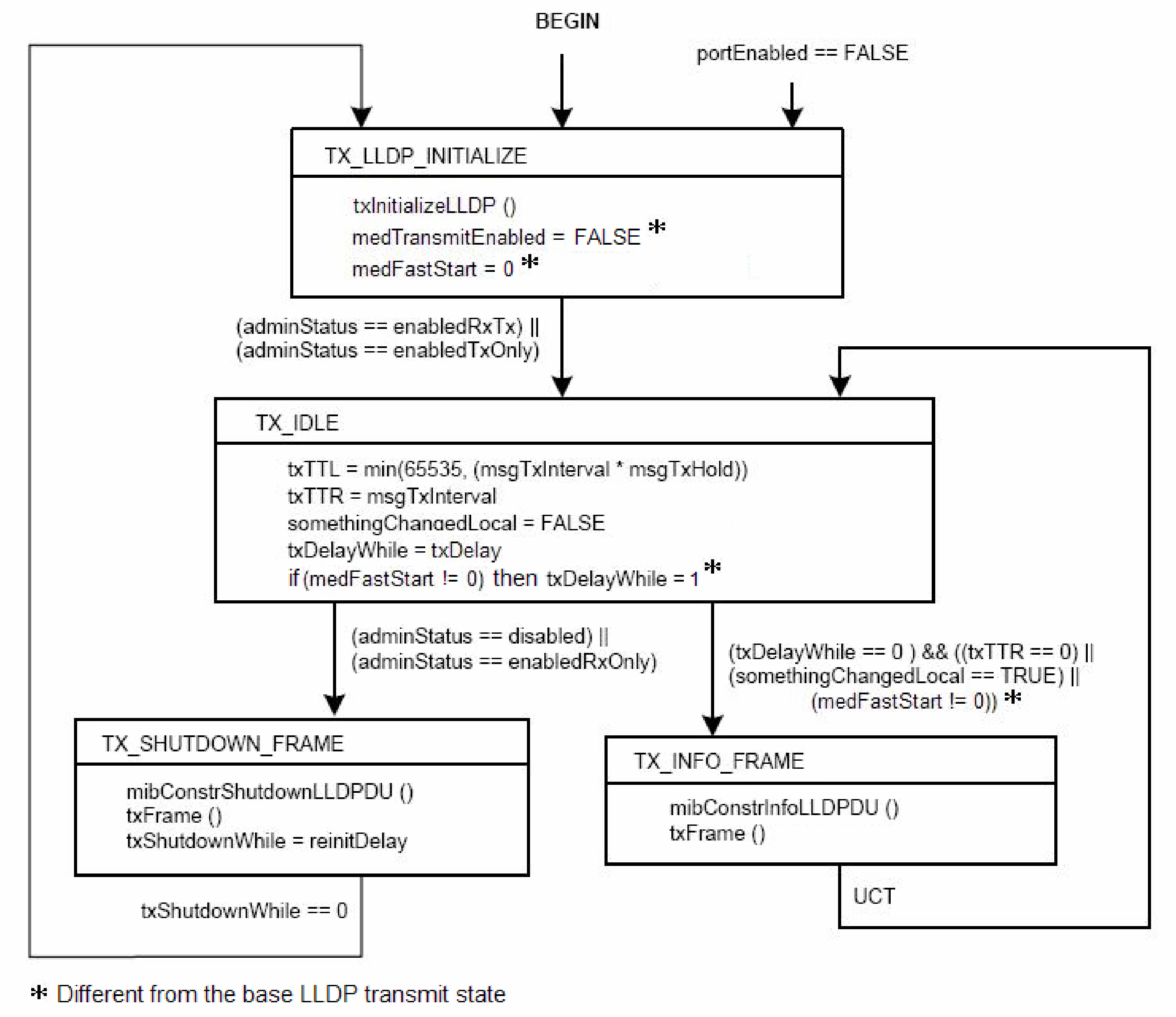

Figure 20 – Network Connectivity Device Transmit State Machine

11.2.4 Frame Reception

When an LLDP-MED Capabilities TLV is detected for an MSAP identifier not associated with an existing LLDP remote system MIB, then the application layer shall set the ‘medTransmitEnabled’ variable to TRUE and shall set the ‘medFastStart’ timer to ‘medFastStartRepeatCount’ times 1 (the minimum LLDP interval).

11.2.5 Remote systems MIB TTL expiration

When the last MSAP identifier, with associated LLDP-MED Capability TLV, has aged out in the remote system MIB for a given port, then the Network Connectivity Device should stop advertising all LLDP-MED specific data for that port by setting the variable ‘medTransmitEnabled’ to FALSE and by setting the ‘medFastStart’ timer to 0.

This processing is performed by the mibDeleteObjects () procedure, shown in the LLDP receive state machine diagram (refer to Figure 10-2 of the IEEE 802.1AB specification [1]).

NOTE – Because updating and deleting of the MIB objects is an LLDP MIB management function, the LLDP-MED specific changes do not impact the receive state machine diagram. No modifications to the base LLDP receive state machine diagram are required.

11.3 Endpoint Device Protocol Interactions

This section defines the LLDP-MED specific protocol interactions for Endpoint Devices.

All Endpoints Devices claiming support of this Standard shall support all the following Endpoint Device specific protocol interactions.

11.3.1 Protocol Initialization

An Endpoint Device claiming support of this specification shall implement both LLDP transmit and receive. The default value of the ‘adminStatus’ variable (defined in the LLDP base protocol) shall be set to ‘enabledRxTx’. If ‘adminStatus’ is set to any value other than ‘enabledRxTx’, then the protocol initialization for LLDP-MED shall be halted.

The following new per-port global variables are defined for Endpoint Devices:

a) **‘medTransmitEnabled’**: This variable is always TRUE for an endpoint device.

b) **‘medFastStart’**: a timer indicating that the LLDP-MED Fast Start mechanism is active.

During LLDP-MED initialization and after loss of link, the local LLDP agent on an endpoint device shall perform the following tasks:

c) Perform the base LLDP protocol initialization,

d) Set the ‘medTransmitEnabled’ variable to TRUE,

e) Set the ‘medFastStart’ timer to ‘medFastStartRepeatCount’ times 1 (the minimum LLDP interval).

11.3.2 Frame Transmission

An Endpoint Device shall always transmit all applicable LLDP-MED specific TLVs, based on its Endpoint Device Class.

An Endpoint Device shall use the Fast Start mechanism to transmit an LLDP-MED frame whenever the ‘medFastStart’ timer has a non-zero value. This timer will typically span multiple LLDP-MED frame transmissions, with the duration based on the ‘medFastStartRepeatCount’ parameter.

Successive LLDP-MED frame transmissions are limited to once per second, the minimum interval allowed by LLDP, by setting the ‘txDelayWhile’ timer (defined in the base LLDP specification) to 1 while the Fast Start mechanism is active.

Since Endpoint Devices enable the ‘medFastStart’ timer as part of the LLDP initialization, this results in the activation of the Fast Start mechanism starting from the first LLDP frame transmission, for a duration of ‘medFastStartRepeatCount’ seconds.

11.3.3 Transmit State Machine Diagram

LLDP-MED defines a slightly enhanced transmit state machine for Endpoint Devices relative to the LLDP base protocol. The updated transmit state machine for an individual port is shown in Figure 21, below, highlighting the differences.

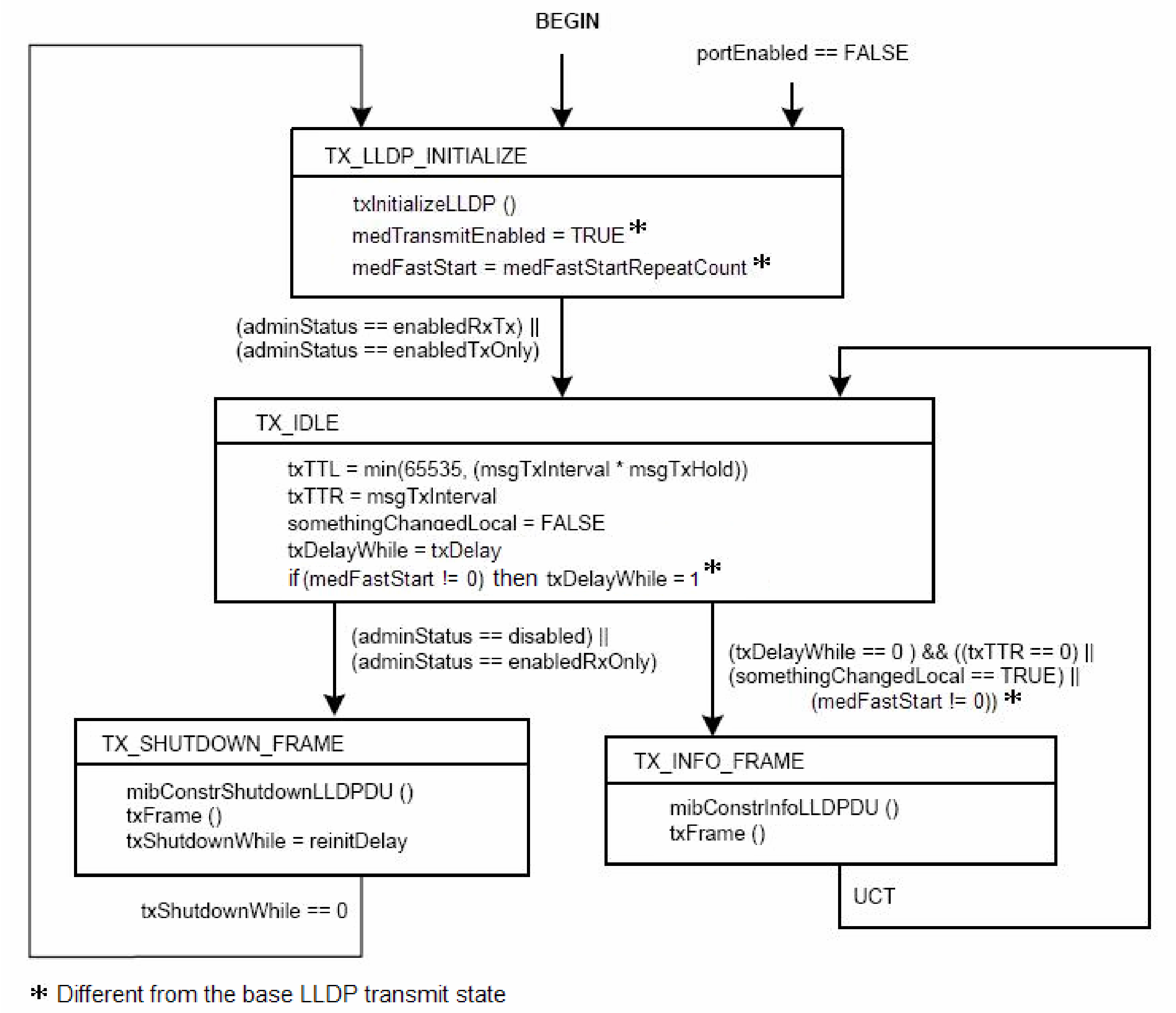

Figure 21 – Endpoint Device Transmit State Machine

11.3.4 Frame Reception

No modifications to the LLDP receive state machine are required for an Endpoint Device (refer to Figure 10-2 of the IEEE 802.1AB specification [1]).

11.4 Frame Validation

The receive module shall process each incoming LLDPDU as it is received. The LLDPDU shall be checked to verify the following LLDP-MED Organizationally Specific TLV requirements:

a) Any LLDP-MED TLV prior to the LLDP-MED Capabilities TLV shall be discarded and the ‘statsFramesInErrorsTotal’ and ‘statsTLVsDiscardedTotal’ counters (defined in the base LLDP specification) shall be incremented.

b) Each of the remaining LLDP-MED TLV shall be decoded in succession as required by their particular TLV format definitions.

11.5 LLDP-MED Interaction with IEEE 802.1X™ (Informative)

Implementers of LLDP-MED should be aware of potential issues that relate to the operation of LLDP in networks where IEEE 802.1X [24] port based access control protocol is operating. The use of IEEE 802.1X on the network connectivity devices through which endpoints connect will prevent the operation of LLDP-MED if these endpoints fail the 802.1X authentication process. Network connectivity devices that have 802.1X enabled will not be able to transmit 802.1AB LLDPDUs until the client system has successfully authenticated itself and has been authorized to access the network.

It is beyond the scope of this Standard to require that developers of LLDP-MED Endpoints or Network Connectivity Devices implement support for the 802.1X, although it is recommended as it would enhance the general security of the network.

12 LLDP-MED Management (Normative)

This section defines the set of managed objects and their functionality that allow administrative configuration and monitoring of LLDP-MED operation.

If an LLDP-MED device supports SNMP, then the system shall implement the basic LLDP-MED MIB as defined in section 13, LLDP-MED MIB Module (Normative).

12.1 LLDP-MED Global Variables

This section lists the new per-port global state machine variables required for Endpoint and Network Connectivity Devices.

Global variables are available for use by more than one state machine, and are used to perform inter-state machine communication.

a) **'medTransmitEnabled'**: an indication that LLDP-MED TLVs should be transmitted for this port (see section 11.2.1, Protocol Initialization).

b) '**medFastStart'**: a timer indicating that the LLDP-MED Fast Start mechanism is active for this port (see section 11.2.1, Protocol Initialization).

c) **'medFastStartRepeatCount'**: a parameter which indicates the number of successive LLDP frame transmissions for one complete Fast Start interval. The recommended default value for medFastStartRepeatCount is 4.

12.2 Relationship Between LLDP-MED Variables and Managed Objects

Table 21, below, lists the relationship both between LLDP operational control variables and their corresponding LLDP CONFIG objects.

Table 21 – LLDP-MED variable / MIB object cross-references

MIB Object Category	LLDP-MED Variable	LLDP-MED MIB Object
LLDP-MED Config	medFastStartRepeatCount	lldpXMedFastStartRepeatCount

Table 22, below, lists the relationship between the TLV variables and their corresponding LLDP-MED local system MIB objects defined in section 13, LLDP-MED MIB Module (Normative).

Table 22 – TLV variable / local-system MIB object cross-references

TLV Name	TLV Variable	LLDP-MED System MIB Object
LLDP-MED Capabilities	LLDP-MED Capabilities	lldpXMedPortCapSupported, lldpXMedPortConfigTLVsTxEnable
	LLDP-MED Class Type	lldpXMedLocDeviceClass
Network Policy	Application Type	lldpXMedLocMediaPolicyAppType
	Unknown Policy Flag	lldpXMedLocMediaPolicyUnknown
	Tagged Flag	lldpXMedLocMediaPolicyTagged
	VLAN ID	lldpXMedLocMediaPolicyVlanID
	L2 Priority	lldpXMedLocMediaPolicyPriority
	DSCP Value	lldpXMedLocMediaPolicyDscp
Location Identifier	Location Data Format	lldpXMedLocLocationSubtype
	Location ID Data	lldpXMedLocLocationInfo
Extended Power-via-MDI	Power Device Type	lldpXMedLocXPoEDeviceType
	Power Source	lldpXMedLocXPoEPSEPowerSource lldpXMedLocXPoEPDPowerSource
	Power Priority	lldpXMedLocXPoEPDPowerPriority lldpXMedLocXPoEPSEPortPDPriority
	Power Value	lldpXMedLocXPoEPSEPortPowerAv lldpXMedLocXPoEPDPowerReq
Inventory	Hardware Revision	lldpXMedLocHardwareRev
	Firmware Revision	lldpXMedLocFirmwareRev
	Software Revision	lldpXMedLocSoftwareRev
	Serial Number	lldpXMedLocSerialNum
	Manufacturer name	lldpXMedLocMfgName
	Model Name	lldpXMedLocModelName
	Asset ID	lldpXMedLocAssetID

Table 23, below, lists the relationship between the TLV variables and their corresponding LLDP-MED remote system MIB objects.

Table 23 – TLV variable / remote-system MIB object cross-references

TLV Name	TLV Variable	LLDP-MED System MIB Object
LLDP-MED Capabilities	LLDP-MED Capabilities	lldpXMedRemCapSupported, lldpXMedRemConfigTLVsTxEnable
	LLDP-MED Class Type	lldpXMedRemDeviceClass
Network Policy	Application Type	lldpXMedRemMediaPolicyAppType
	Unknown Policy Flag	lldpXMedLocMediaPolicyUnknown
	Tagged Flag	lldpXMedLocMediaPolicyTagged
	VLAN ID	lldpXMedRemMediaPolicyVlanID
	L2 Priority	lldpXMedRemMediaPolicyPriority
	DSCP Value	lldpXMedRemMediaPolicyDscp
Location Identifier	Location Data Format	lldpXMedRemLocationSubtype
	Location ID Data	lldpXMedRemLocationInfo
Extended Power-via-MDI	Power Device Type	lldpXMedRemXPoEDeviceType
	Power Source	lldpXMedRemXPoEPSEPowerSource lldpXMedRemXPoEPDPowerSource
	Power Priority	lldpXMedRemXPoEPSEPowerPriority lldpXMedRemXPoEPDPowerPriority
	Power Value	lldpXMedRemXPoEPSEPowerAv lldpXMedRemXPoEPDPowerReq
Inventory	Hardware Revision	lldpXMedRemHardwareRev
	Firmware Revision	lldpXMedRemFirmwareRev
	Software Revision	lldpXMedRemSoftwareRev
	Serial Number	lldpXMedRemSerialNum
	Manufacturer name	lldpXMedRemMfgName
	Model Name	lldpXMedRemModelName
	Asset ID	lldpXMedRemAssetID

12.3 Topology Change Notification

Topology Change Notification allows for significantly reduced overhead in device move tracking by providing VoIP device specific information only to the VoIP management application, and by providing key information in the notification itself.

LLDP-MED defines a notification, `lldpXMedTopologyChangeDetected`, which allows for a Device to transfer information related to topology changes to management applications in an asynchronous manner. Specifically, this enables notification of the fact that a new remote device was connected to the local port of an LLDP-MED Network Connectivity Device, or that a remote device was removed from the local port. The purpose of this notification is near-real-time transmission of information regarding moves and changes to the management applications in an efficient manner. Information carried by the list of objects (varbind) contained in the notification allows the receiving management application to uniquely identify the local port where the topology change occurred, as well as the device capability of the remote Endpoint Device that was attached to or removed from the port.

Generation of Topology Change Notification is triggered when the local port ID changes for an LLDP-MED Endpoint Device associated with a remote MSAP identifier.

In some deployments, customers may be concerned by the number of notifications, may not be interested in receiving the topology change information, or may need to temporarily disable these notifications for trouble-shooting purposes. In order to allow the topology change notifications to be enabled and disabled, the LLDP-MED MIB includes a read-write object, lldpXMedPortConfigNotifEnable. The default value of this object is 'false', i.e. notification is disabled by default.

NOTE 1 – Transmission of LLDP-MED Topology Change Notification is throttled by the lldpNotificationInterval object in the LLDP MIB.

NOTE 2 – Typically, SNMP would be the delivery mechanism for these notifications, although SNMP is not explicitly mandated by this Standard. Although the usage of SNMP notifications allows for a quick transfer of information as it happens, implementers are cautioned to take into account that SNMP typically runs over UDP, which does not guarantee delivery of datagrams from sender to receiver. As a result, it is recommended that management applications periodically poll the relevant tables in the LLDP and LLDP-MED Devices to ensure that no information was lost due to loss of notifications. It is not recommended that applications critical to the functionality of the network or accounting applications be based upon topology change notifications only.

13 LLDP-MED MIB Module (Normative)

This section defines the LLDP-MED MIB module (in subsection 13.3) as well as background information on the Internet Standard Management Framework on which it is based (subsection 13.1) and related security considerations (subsection 13.2).

13.1 The Internet-Standard Management Framework

This section includes the definition of a Management Information Base (MIB) module that is part of the Internet-Standard Management Framework. For a detailed overview of the documents that describe the current Internet-Standard Management Framework, refer to section 7 of IETF RFC 3410 [31].

Managed objects are accessed via a virtual information store, termed the Management Information Base, or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP) [9], [10], [11]. Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This Standard specifies a MIB module for LLDP-MED that is compliant to the SMIv2, which is described in IETF STD 58 (RFC 2578 - 2580) [12], [18], [19].

NOTE – This Standard does not specifically require implementation of SNMP for LLDP-MED Endpoint or Network Connectivity Devices. However SNMP support is recommended for Network Connectivity Devices.

13.2 Security Considerations for SNMP in LLDP-MED

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. The following are the tables and objects and their sensitivity/vulnerability:

- lldpXMedPortConfigTLVsTxEnable - incorrect setting of this object would result in the device sending information that is not relevant or not accurate, or not sending relevant topology information. Applications that are based upon the presence and accuracy of the information carried by LLDP-MED may be affected.

- lldpXMedLocLocationInfo - incorrect setting of this object may result in the device location information carried by the LLDP-MED Location TLV be inaccurate, and applications based on this mechanism being affected.

- lldpXMedFastStartRepeatCount - mis-configuration in setting the value of this object may result in the fast start mechanism not acting appropriately, and applications based on this mechanism being affected.

- lldpXMedPortConfigNotifEnable - incorrect setting of this object may result in the move detection notification not acting appropriately, and applications based on this mechanism being affected.

All readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. These objects include network topology information that may be considered sensitive in certain user administration domains, according to the policies of the respective user organizations. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to encrypt the values of these objects when sending them over the network via SNMP.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is recommended that implementers consider the security features as provided by the SNMPv3 framework (see RFC3410 [31], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is not recommended. Instead, it is recommended to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

13.3 LLDP-MED MIB Definition

In the following MIB module, should any discrepancy between the MIB DESCRIPTON text and the corresponding definition in clauses 10 through 12 occur, the definition in clauses 10 through 12 shall take precedence.

```
LLDP-EXT-MED-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, Integer32, Gauge32, Unsigned32,
    NOTIFICATION-TYPE
        FROM SNMPv2-SMI
    TEXTUAL-CONVENTION, TruthValue
        FROM SNMPv2-TC
    MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
        FROM SNMPv2-CONF
    lldpExtensions, lldpLocPortNum,
    lldpRemTimeMark, lldpRemLocalPortNum, lldpRemIndex,
    lldpPortConfigEntry, lldpRemChassisIdSubtype, lldpRemChassisId
        FROM LLDP-MIB
    Dscp
        FROM DIFFSERV-DSCP-TC
    SnmpAdminString
        FROM SNMP-FRAMEWORK-MIB;

lldpXMedMIB MODULE-IDENTITY
    LAST-UPDATED "200507280000Z" -- July 28th, 2005
    ORGANIZATION "TIA TR41.4 Working Group"
    CONTACT-INFO
"   WG-URL: http://www.tiaonline.org/standards/sfg/scope.cfm#TR-41.4
             WG-EMail: tr41@tiacomm.org
```

```
               Contact: Chair, TIA TR-41
                Postal: Telecommunications Industry Association
                        2500 Wilson Blvd., Suite 300
                        Arlington, VA 22201 USA
                   Tel: (703) 907-7700
                E-mail: tr41@tiacomm.org"
    DESCRIPTION
            "The LLDP Management Information Base extension module for
            TIA-TR41.4 Media Endpoint Discovery information.

            In order to assure the uniqueness of the LLDP-MIB,
            lldpXMedMIB is branched from lldpExtensions using the TIA OUI
            value as the node.  An OUI/'company_id' is a 24 bit globally
            unique assigned number referenced by various standards.

            Copyright (C) TIA (2005).  This version of this MIB module
            is published as Section 13.3 of ANSI/TIA-1057.

            See the standard itself for full legal notices."
    REVISION        "200507280000Z" -- July 28th, 2005
    DESCRIPTION
            "Published as part of ANSI/TIA-1057."
-- OUI for TIA TR-41 is 4795 (00-12-BB)
   ::= { lldpExtensions 4795 }

------------------------------------------------------------------------------
------------------------------------------------------------------------------
--
-- LLDP-MED Information
--
------------------------------------------------------------------------------
------------------------------------------------------------------------------

lldpXMedNotifications    OBJECT IDENTIFIER ::= { lldpXMedMIB 0 }
lldpXMedObjects          OBJECT IDENTIFIER ::= { lldpXMedMIB 1 }

-- LLDP MED Extension Notifications
-- Transmission of LLDP MED Extension Notification is controlled by the
-- lldpNotificationInterval object in the LLDP MIB defined in
-- IEEE 802.1AB-2005

lldpXMedTopologyChangeDetected NOTIFICATION-TYPE
     OBJECTS { lldpRemChassisIdSubtype,
               lldpRemChassisId,
               lldpXMedRemDeviceClass
               }
           STATUS current
DESCRIPTION
               "A notification generated by the local device sensing
                a change in the topology that indicates that a new remote
                device attached to a local port, or a remote device disconnected
                or moved from one port to another."
           ::= { lldpXMedNotifications 1 }


-- LLDP MED extension MIB groups
```

```
lldpXMedConfig     OBJECT IDENTIFIER ::= { lldpXMedObjects 1 }
lldpXMedLocalData  OBJECT IDENTIFIER ::= { lldpXMedObjects 2 }
lldpXMedRemoteData OBJECT IDENTIFIER ::= { lldpXMedObjects 3 }

-- textual conventions

LldpXMedDeviceClass  ::= TEXTUAL-CONVENTION
    STATUS     current
    DESCRIPTION
            "Device Class to which the device is a member.

            A value of notDefined(0) indicates that the device
            has capabilities not covered by any of the LLDP-MED classes.

            A value of endpointClass1(1) indicates that the device
            has endpoint class 1 capabilities.

            A value of endpointClass2(2) indicates that the device
            has endpoint class 2 capabilities.

            A value of endpointClass3(3) indicates that the device
            has endpoint class 3 capabilities.

            A value of networkConnectivity(4) indicates that the device
            has network connectivity device capabilities.
            "

    SYNTAX      INTEGER {
            notDefined(0),
            endpointClass1(1),
            endpointClass2(2),
            endpointClass3(3),
            networkConnectivity(4)
    }

-- LLDP-MED Capabilities TC

LldpXMedCapabilities  ::= TEXTUAL-CONVENTION
    STATUS     current
    DESCRIPTION
            "Bitmap that includes the MED organizationally defined set of LLDP
            TLVs the device is capable of and whose transmission is allowed on
            the local LLDP agent by network management.

            Each bit in the bitmap corresponds to an LLDP-MED subtype associated
            with a specific TIA TR41.4 MED TLV.

            Having the bit 'capabilities(0)' set indicates that the LLDP
            agent refers to the Capabilities TLVs.

            Having the bit 'networkPolicy(1)' set indicates that the LLDP
            agent refers to the Network Policy TLVs.

            Having the bit 'location(2)' set indicates that
            the LLDP agent refers to the Emergency Communications
            System Location TLVs.
```

```
            Having the bit 'extendedPSE(3)' set indicates that
            the LLDP agent refers to the Extended PoE TLVs with PSE
            capabilities.

            Having the bit 'extendedPD(4)' set indicates that
            the LLDP agent refers to the Extended PoE TLVs with PD
            capabilities.

            Having the bit 'inventory(5)' set indicates that
            the LLDP agent refers to the Hardware Revision, Firmware
            Revision, Software Revision, Serial Number, Manufacturer Name,
            Model Name, and Asset ID TLVs."

    SYNTAX      BITS {
            capabilities(0),
            networkPolicy(1),
            location(2),
            extendedPSE(3),
            extendedPD(4),
            inventory(5)
    }


--  Location Subtype Textual Convention

LocationSubtype ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "The location subtype advertised by the remote endpoint.

             A value coordinateBased(2) indicates that the location subtype
             advertised by the endpoint is defined to use the relevant sub-
             fields of the DHCP option for Coordinate LCI as specified in
             ANSI/TIA-1057, Section 10.2.4.3.1.

             A value civicAddress(3) indicates that the location subtype
             advertised by the endpoint is defined to use the relevant sub-
             fields of the DHCP option for Civic Address as specified in
             ANSI/TIA-1057, Section 10.2.4.3.2.

             A value elin(4) indicates that the location subtype
             advertised by the endpoint is defined to use the Emergency
             Location Information Number (ELIN) as specified in
             ANSI/TIA-1057, Section 10.2.4.3.3."
    SYNTAX      INTEGER  {
                    unknown(1),
                    coordinateBased(2),
                    civicAddress(3),
                    elin(4)
                }

-- Policy Application Type Textual Convention

PolicyAppType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "The media type that defines the primary function of the
```

```
            application for the policy advertised by an endpoint.

            Having the bit voice(1) set indicates that the media type defining
            a primary function of the application for the policy advertised on
            the local port is voice.

            Having the bit voiceSignaling(3) set indicates that the media type
            defining a primary function of the application for the policy
            advertised on the local port is voice signaling.

            Having the bit guestVoice(4) set indicates that the media type
            Defining a primary function of the application for the policy
            advertised on the local port is guest voice.

            Having the bit guestVoiceSignaling(5) set indicates that the media
            type defining a primary function of the application for the policy
            advertised on the local port is guest voice signaling.

            Having the bit softPhoneVoice(6) set indicates that the media type
            Defining a primary function of the application for the policy
            advertised on the local port is softphone voice.

            Having the bit videoConferencing(7) set indicates that the media
            type defining a primary function of the application for the policy
            advertised on the local port is voice.

            Having the bit streamingVideo(8) set indicates that the media type
            defining a primary function of the application for the policy
            advertised on  the local port is streaming video.

            Having the bit videoSignaling(2) set indicates that the media type
            defining a primary function of the application for the policy
            advertised on the local port is video signaling."
    SYNTAX      BITS  {
                    unknown(0),
                    voice(1),
                    voiceSignaling(2),
                    guestVoice(3),
                    guestVoiceSignaling(4),
                    softPhoneVoice(5),
                    videoconferencing(6),
                    streamingVideo(7),
                    videoSignaling(8)
                }


------------------------------------------------------------------------------
-- MED - Configuration
------------------------------------------------------------------------------

lldpXMedLocDeviceClass    OBJECT-TYPE
    SYNTAX      LldpXMedDeviceClass
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Local Device Class."
    REFERENCE
```

```
            " ANSI/TIA-1057, Section 10.2.2.2"
    ::= { lldpXMedConfig 1 }


lldpXMedPortConfigTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedPortConfigEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "A table that controls selection of LLDP TLVs to be transmitted
            on individual ports."
    ::= { lldpXMedConfig 2 }

lldpXMedPortConfigEntry  OBJECT-TYPE
    SYNTAX      LldpXMedPortConfigEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "LLDP configuration information that controls the
            transmission of the MED organizationally defined TLVs on
            LLDP transmission capable ports.

            This configuration object augments the lldpPortConfigEntry of
            the LLDP-MIB, therefore it is only present along with the port
            configuration defined by the associated lldpPortConfigEntry
            entry.

            Each active lldpXMedPortConfigEntry must be stored and
            retrieved from non-volatile storage (along with the
            corresponding lldpPortConfigEntry) after a re-initialization
            of the management system."
    AUGMENTS { lldpPortConfigEntry }
    ::= { lldpXMedPortConfigTable 1 }

LldpXMedPortConfigEntry ::= SEQUENCE {
    lldpXMedPortCapSupported        LldpXMedCapabilities,
    lldpXMedPortConfigTLVsTxEnable  LldpXMedCapabilities,
    lldpXMedPortConfigNotifEnable   TruthValue
}

lldpXMedPortCapSupported  OBJECT-TYPE
    SYNTAX      LldpXMedCapabilities
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The bitmap includes the MED organizationally defined set of LLDP
            TLVs whose transmission is possible for the respective port
            on the LLDP agent of the device. Each bit in the bitmap corresponds
            to an LLDP-MED subtype associated with a specific TIA TR41.4 MED
            optional TLV. If the bit is set, the agent supports the
            corresponding TLV."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.2.3"
    ::= { lldpXMedPortConfigEntry  1 }

lldpXMedPortConfigTLVsTxEnable  OBJECT-TYPE
    SYNTAX      LldpXMedCapabilities
```

```
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The lldpXMedPortConfigTLVsTxEnable, defined as a bitmap,
            includes the MED organizationally defined set of LLDP
            TLVs whose transmission is allowed on the local LLDP agent by
            the network management.  Each bit in the bitmap corresponds
            to an LLDP-MED subtype associated with a specific TIA TR41.4 MED
            optional TLV. If the bit is set, the agent will send the
            corresponding TLV if the respective capability is supported per
            port.

            Setting a bit with in this object for a non-supported capability
            shall have no functional effect and will result in an inconsistent
            value error returned to the management application.

            There are other rules and restrictions that prevent arbitrary
            combinations of TLVs to be enabled on LLDP-MED devices according to
            the device classes. These rules are defined in Section 10.2.1,
            Tables 5 - 9 of ANSI/TIA-1057. In case a management application
            attempts to set this object to a value that does not follow the rules,
            the set operation shall have and will result in an inconsistent
            value error returned to the management application.

            Setting this object to an empty set is valid and effectively
            disables LLDP-MED on a per-port basis by disabling transmission of
            all MED organizational TLVs. In this case the remote tables objects
            in the LLDP-MED MIB corresponding to the respective port will not
            be populated.

            The default value for lldpXMedPortConfigTLVsTxEnable object
            is an empty set, which means no enumerated values are set.

            The value of this object must be restored from non-volatile
            storage after a re-initialization of the management system."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.2.3"
    DEFVAL  { { } }
    ::= { lldpXMedPortConfigEntry  2 }

lldpXMedPortConfigNotifEnable    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "A value of 'true(1)' enables sending the topology change
             traps on this port.
             A value of 'false(2)' disables sending the topology change
             traps on this port."
    REFERENCE
            " ANSI/TIA-1057, Section 12.3"
    DEFVAL   { false }
    ::= { lldpXMedPortConfigEntry 3 }


lldpXMedFastStartRepeatCount    OBJECT-TYPE
```

```
    SYNTAX      Unsigned32 (1..10)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of times the fast start LLDPDU are being sent during the
             activation of the fast start mechanism defined by LLDP-MED."
    REFERENCE
            " ANSI/TIA-1057, Section 11.2.1"
    DEFVAL   { 3 }
    ::= { lldpXMedConfig 3 }




------------------------------------------------------------------------------
-- LLDP-MED - Local Device Information
------------------------------------------------------------------------------
---
--- lldpXMedLocMediaPolicyTable: Local Media Policy
---                        Information Table
---
---
lldpXMedLocMediaPolicyTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedLocMediaPolicyEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains one row per policy type per port
             of media policy information (as a part of the MED
             organizational extension) on the local system known
             to this agent."
    ::= { lldpXMedLocalData 1 }

lldpXMedLocMediaPolicyEntry OBJECT-TYPE
    SYNTAX      LldpXMedLocMediaPolicyEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about a particular policy on a specific
             port component."
    INDEX   { lldpLocPortNum, lldpXMedLocMediaPolicyAppType }
    ::= { lldpXMedLocMediaPolicyTable 1 }

LldpXMedLocMediaPolicyEntry ::= SEQUENCE {
              lldpXMedLocMediaPolicyAppType        PolicyAppType,
              lldpXMedLocMediaPolicyVlanID         Integer32,
              lldpXMedLocMediaPolicyPriority       Integer32,
              lldpXMedLocMediaPolicyDscp           Dscp,
              lldpXMedLocMediaPolicyUnknown        TruthValue,
              lldpXMedLocMediaPolicyTagged         TruthValue
}

lldpXMedLocMediaPolicyAppType OBJECT-TYPE
    SYNTAX      PolicyAppType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
            "The media type that defines the primary function of the
             application for the policy advertised by an endpoint."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.3.1"
    ::= { lldpXMedLocMediaPolicyEntry 1 }

lldpXMedLocMediaPolicyVlanID  OBJECT-TYPE
    SYNTAX      Integer32 (0|1..4094|4095)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "An extension of the VLAN Identifier for the port,
             as defined in IEEE 802.1P-1998.

             A value of 1 through 4094 is used to define a valid PVID.

             A value of 0 shall be used if the device is using priority tagged
             frames, meaning that only the 802.1p priority level is significant
             and the default VID of the ingress port is being used instead.

             A value of 4095 is reserved for implementation use."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.5"
    ::= { lldpXMedLocMediaPolicyEntry 2 }

lldpXMedLocMediaPolicyPriority  OBJECT-TYPE
    SYNTAX      Integer32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the 802.1p priority
            which is associated with the given port on the
            local system."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.6 "
    ::= { lldpXMedLocMediaPolicyEntry 3 }

lldpXMedLocMediaPolicyDscp  OBJECT-TYPE
    SYNTAX      Dscp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the Differentiated Service
            Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475
            which is associated with the given port on the local system."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.7"
    ::= { lldpXMedLocMediaPolicyEntry 4 }

lldpXMedLocMediaPolicyUnknown  OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A value of 'true' indicates that the
             network policy for the specified application type is
             currently unknown.  In this case, the VLAN ID, the
```

```
             layer 2 priority and the DSCP value fields are ignored.
             A value of 'false' indicates that this network policy
             is defined  "
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.2"
    ::= { lldpXMedLocMediaPolicyEntry 5 }

lldpXMedLocMediaPolicyTagged  OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A value of 'true' indicates that the application is using a
             tagged VLAN.
             A value of 'false' indicates that for the specific application
             the device either is using an untagged VLAN or does not
             support port based VLAN operation.  In this case, both the
             VLAN ID and the Layer 2 priority fields are ignored and
             only the DSCP value has relevance "
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.3"
    ::= { lldpXMedLocMediaPolicyEntry 6 }



--- Inventory Information
--- Local Inventory Information transmitted by an endpoint

lldpXMedLocHardwareRev    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific hardware revision string
            as advertised by the endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.1"
    ::= { lldpXMedLocalData 2 }

lldpXMedLocFirmwareRev    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific firmware revision string
            as advertised by the endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.2"
    ::= { lldpXMedLocalData 3 }

lldpXMedLocSoftwareRev    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific software revision string
            as advertised by the endpoint."
```

```
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.3"
    ::= { lldpXMedLocalData 4 }

lldpXMedLocSerialNum    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific serial number
            as advertised by the endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.4"
    ::= { lldpXMedLocalData 5 }

lldpXMedLocMfgName    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific manufacturer name
            as advertised by the endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.5"
    ::= { lldpXMedLocalData 6 }

lldpXMedLocModelName    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific model name
            as advertised by the endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.6"
    ::= { lldpXMedLocalData 7 }

lldpXMedLocAssetID    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific asset tracking identifier
            as advertised by the endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.7"
    ::= { lldpXMedLocalData 8 }



--- Location Information
--- Local Location Information transmitted by an endpoint
--- lldpXMedLocLocationTable - Location Information
---

lldpXMedLocLocationTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedLocLocationEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains Location information as advertised
            by the local system.

            The information may be configured per port by a Location
            Information Server (LIS) or other management application.

            Multiple Location TLVs of different subtypes may be transmitted
            in the same PDU.

            The information in this table MUST be stored in non-volatile-memory
            and persist over restart/reboot sequences."
    ::= { lldpXMedLocalData 9 }

lldpXMedLocLocationEntry OBJECT-TYPE
    SYNTAX      LldpXMedLocLocationEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about Location information for the local device."
    INDEX   { lldpLocPortNum, lldpXMedLocLocationSubtype}
    ::= { lldpXMedLocLocationTable 1 }

LldpXMedLocLocationEntry ::= SEQUENCE {
              lldpXMedLocLocationSubtype    LocationSubtype,
              lldpXMedLocLocationInfo       OCTET STRING
              }



lldpXMedLocLocationSubtype OBJECT-TYPE
    SYNTAX      LocationSubtype
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The location subtype advertised by the local device."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.4.2"
    ::= { lldpXMedLocLocationEntry 1 }


lldpXMedLocLocationInfo OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..256))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The location information. Parsing of this information is
             dependent upon the location subtype, as defined by the value of the
             lldpXMedLocLocationSubtype object. "
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.4.3"
    DEFVAL { "" }
    ::= { lldpXMedLocLocationEntry 2 }

--- Extended Power over Ethernet objects
```

```
---

lldpXMedLocXPoEDeviceType OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    pseDevice(2),
                    pdDevice(3),
                    none(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Defines the type of Power-via-MDI (Power over Ethernet) advertised
             by the local device.

             A value pseDevice(2) indicates that the device is advertised as a
             Power Sourcing Entity (PSE).

             A value pdDevice(3) indicates that the device is advertised as a
             Powered Device (PD).

             A value of none(4) indicates that the device does not support PoE."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.1"
    ::= { lldpXMedLocalData 10 }

--- Extended PoE - PSE objects



--- PSE Port Table

lldpXMedLocXPoEPSEPortTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedLocXPoEPSEPortEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains one row per port of PSE PoE
            information on the local system known to this agent."
    ::= { lldpXMedLocalData 11 }

lldpXMedLocXPoEPSEPortEntry OBJECT-TYPE
    SYNTAX      LldpXMedLocXPoEPSEPortEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about a particular port PoE information."
    INDEX   { lldpLocPortNum }
    ::= { lldpXMedLocXPoEPSEPortTable 1 }

LldpXMedLocXPoEPSEPortEntry ::= SEQUENCE {
              lldpXMedLocXPoEPSEPortPowerAv           Gauge32,
              lldpXMedLocXPoEPSEPortPDPriority        INTEGER
}

lldpXMedLocXPoEPSEPortPowerAv  OBJECT-TYPE
    SYNTAX      Gauge32 (0..1023)
```

```
    UNITS      "tenth of watt"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the power available from the
            PSE via this port expressed in units of 0.1 watts."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.5.4 "
    ::= { lldpXMedLocXPoEPSEPortEntry 1 }

lldpXMedLocXPoEPSEPortPDPriority OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    critical(2),
                    high(3),
                    low(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Reflects the PD power priority that is being advertised on this
             PSE port.

             If both locally configure priority and
             ldpXMedRemXPoEPDPowerPriority are available on this port, it is
             a matter of local policy which one takes precedence. This object
             reflects the active value on this port.

             If the priority is not configured or known by the PD, the value
             unknown(1) will be returned.

             A value critical(2) indicates that the device advertises its power
             Priority as critical, as per RFC 3621.

             A value high(3) indicates that the device advertises its power
             Priority as high, as per RFC 3621.

             A value low(4) indicates that the device advertises its power
             Priority as low, as per RFC 3621."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.3"
    ::= { lldpXMedLocXPoEPSEPortEntry 2 }



lldpXMedLocXPoEPSEPowerSource OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    primary(2),
                    backup(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Defines the type of PSE Power Source advertised
             by the local device.
```

```
             A value primary(2) indicates that the device advertises its power
             source as primary.

             A value backup(3) indicates that the device advertises its power
             Source as backup."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.2"
    ::= { lldpXMedLocalData 12 }


--- Extended PoE - PD objects

lldpXMedLocXPoEPDPowerReq  OBJECT-TYPE
    SYNTAX      Gauge32 (0..1023)
    UNITS      "tenth of watt"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the power required by a
            PD expressed in units of 0.1 watts."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.4.3 "
    ::= { lldpXMedLocalData 13 }

lldpXMedLocXPoEPDPowerSource OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    fromPSE(2),
                    local(3),
                    localAndPSE(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Defines the type of Power Source advertised as being used
             by the local device.

             A value fromPSE(2) indicates that the device advertises its power
             source as received from a PSE.

             A value local(3) indicates that the device advertises its power
             source as local.

             A value localAndPSE(4) indicates that the device advertises its
             power source as using both local and PSE power."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.2"
    ::= { lldpXMedLocalData 14 }

lldpXMedLocXPoEPDPowerPriority OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    critical(2),
                    high(3),
                    low(4)
                }
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
            "Defines the priority advertised as being required by this PD.

             A value critical(2) indicates that the device advertises its power
             Priority as critical, as per RFC 3621.

             A value high(3) indicates that the device advertises its power
             Priority as high, as per RFC 3621.

             A value low(4) indicates that the device advertises its power
             Priority as low, as per RFC 3621."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.3"
    ::= { lldpXMedLocalData 15 }



------------------------------------------------------------------------------
-- LLDP-MED  - Remote Devices Information
------------------------------------------------------------------------------



-- LLdpXMedRemCapabilitiesTable
-- this table is read by a manager to determine what capabilities
-- exists and are enabled on the remote system connected to the port

-- The information in this table is based upon the information advertised
-- by the remote device and received on each port in the capabilities TLV

lldpXMedRemCapabilitiesTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedRemCapabilitiesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "A table that displays LLDP-MED capabilities of remote devices
            connected to individual ports."
    ::= { lldpXMedRemoteData 1 }

lldpXMedRemCapabilitiesEntry  OBJECT-TYPE
    SYNTAX      LldpXMedRemCapabilitiesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "LLDP-MED capabilities of remote devices connected to the device
            ports and communicating via LLDP-MED.

            The remote tables in the LLDP-MED MIB excepting this table may be
            sparsely populate. An entry in one of these table is meaningful
            and shall be populated by the agent only if the corresponding bits
            for the respective function are set in the objects in this table. "
    INDEX   { lldpRemTimeMark,
              lldpRemLocalPortNum,
              lldpRemIndex }
    ::= { lldpXMedRemCapabilitiesTable 1 }
```

```
LldpXMedRemCapabilitiesEntry ::= SEQUENCE {
      lldpXMedRemCapSupported  LldpXMedCapabilities,
      lldpXMedRemCapCurrent    LldpXMedCapabilities,
      lldpXMedRemDeviceClass   LldpXMedDeviceClass
}

lldpXMedRemCapSupported  OBJECT-TYPE
    SYNTAX      LldpXMedCapabilities
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The bitmap includes the MED organizationally defined set of LLDP
            TLVs whose transmission is possible on the LLDP agent of the remote
            device connected to this port. Each bit in the bitmap corresponds
            to an LLDP-MED subtype associated with a specific TIA TR41.4 MED
            optional TLV. If the bit is set, the agent has the capability
            to support the corresponding TLV."
    REFERENCE
            "ANSI/TIA-1057, Sections 10.2.2.1"
    ::= { lldpXMedRemCapabilitiesEntry  1 }

lldpXMedRemCapCurrent  OBJECT-TYPE
    SYNTAX      LldpXMedCapabilities
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The bitmap includes the MED organizationally defined set of LLDP
            TLVs whose transmission is possible on the LLDP agent of the remote
            device connected to this port. Each bit in the bitmap corresponds
            to an LLDP-MED subtype associated with a specific TIA TR41.4 MED
            optional TLV. If the bit is set, the agent currently supports the
            corresponding TLV."
    REFERENCE
            "ANSI/TIA-1057, Sections 10.2.2.1"
    ::= { lldpXMedRemCapabilitiesEntry  2 }

lldpXMedRemDeviceClass    OBJECT-TYPE
    SYNTAX      LldpXMedDeviceClass
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Device Class as advertised by the device remotely connected to the
             port."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.2.2"
    ::= { lldpXMedRemCapabilitiesEntry 3 }




---
---
--- lldpXMedRemMediaPolicyTable: Media Policy Table
---
---
lldpXMedRemMediaPolicyTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedRemMediaPolicyEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains media policy information as advertised
            by the remote system.

            This table may be sparsely populated. Entries in this table are
            relevant only if the networkPolicy(0) bits in the
            lldpXMedRemCapSupported and lldpXMedRemCapCurrent objects of the
            corresponding ports are set."
    ::= { lldpXMedRemoteData 2 }

lldpXMedRemMediaPolicyEntry OBJECT-TYPE
    SYNTAX      LldpXMedRemMediaPolicyEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about the per port per policy type policy
             information for a particular physical network connection."
    INDEX   { lldpRemTimeMark,
              lldpRemLocalPortNum,
              lldpRemIndex,
              lldpXMedRemMediaPolicyAppType }
    ::= { lldpXMedRemMediaPolicyTable 1 }


LldpXMedRemMediaPolicyEntry ::= SEQUENCE {
              lldpXMedRemMediaPolicyAppType        PolicyAppType,
              lldpXMedRemMediaPolicyVlanID         Integer32,
              lldpXMedRemMediaPolicyPriority       Integer32,
              lldpXMedRemMediaPolicyDscp           Dscp,
              lldpXMedRemMediaPolicyUnknown        TruthValue,
              lldpXMedRemMediaPolicyTagged         TruthValue
}

lldpXMedRemMediaPolicyAppType OBJECT-TYPE
    SYNTAX      PolicyAppType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The media type that defines the primary function of the
             application for the policy advertised by the endpoint connected
             remotely to this port."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.3.1"
    ::= { lldpXMedRemMediaPolicyEntry 1 }

lldpXMedRemMediaPolicyVlanID  OBJECT-TYPE
    SYNTAX      Integer32 (0|1..4094|4095)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "An extension of the VLAN Identifier for the remote system
             connected to this port, as defined in IEEE 802.1P-1998.

             A value of 1 through 4094 is used to define a valid PVID.
```

```
             A value of 0 shall be used if the device is using priority tagged
             frames, meaning that only the 802.1p priority level is significant
             and the default VID of the ingress port is being used instead.

             A value of 4095 is reserved for implementation use."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.5"
    ::= { lldpXMedRemMediaPolicyEntry 2 }

lldpXMedRemMediaPolicyPriority  OBJECT-TYPE
    SYNTAX      Integer32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the 802.1p priority
            which is associated with the remote system connected at
            given port."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.6"
    ::= { lldpXMedRemMediaPolicyEntry 3 }

lldpXMedRemMediaPolicyDscp  OBJECT-TYPE
    SYNTAX      Dscp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the Differentiated Service
            Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475
            which is associated with remote system connected at the port."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.7"
    ::= { lldpXMedRemMediaPolicyEntry 4 }

lldpXMedRemMediaPolicyUnknown  OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A value of 'true' indicates that the
             network policy for the specified application type is
             currently unknown.  In this case, the VLAN ID, the
             layer 2 priority and the DSCP value fields are ignored.
             A value of 'false' indicates that this network policy
             is defined."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.2"
    ::= { lldpXMedRemMediaPolicyEntry 5 }

lldpXMedRemMediaPolicyTagged  OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A value of 'true' indicates that the application is using a
             tagged VLAN.
             A value of 'false' indicates that for the specific application
             the device either is using an untagged VLAN or does not
```

```
             support port based VLAN operation.  In this case, both the
             VLAN ID and the Layer 2 priority fields are ignored and
             only the DSCP value has relevance "
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.3.3"
    ::= { lldpXMedRemMediaPolicyEntry 6 }



--- lldpXMedRemInventoryTable - Remote Inventory Information
---

lldpXMedRemInventoryTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedRemInventoryEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains inventory information as advertised
            by the remote system.

            This table may be sparsely populated. Entries in this table are
            relevant only if the inventory(2) bits in the
            lldpXMedRemCapSupported and lldpXMedRemCapCurrent objects of the
            corresponding ports are set "
    ::= { lldpXMedRemoteData 3 }

lldpXMedRemInventoryEntry OBJECT-TYPE
    SYNTAX      LldpXMedRemInventoryEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about inventory information for the remote devices
             connected to the ports."
    INDEX   { lldpRemTimeMark,
              lldpRemLocalPortNum,
              lldpRemIndex }
    ::= { lldpXMedRemInventoryTable 1 }

LldpXMedRemInventoryEntry ::= SEQUENCE {
              lldpXMedRemHardwareRev           SnmpAdminString,
              lldpXMedRemFirmwareRev           SnmpAdminString,
              lldpXMedRemSoftwareRev           SnmpAdminString,
              lldpXMedRemSerialNum             SnmpAdminString,
              lldpXMedRemMfgName               SnmpAdminString,
              lldpXMedRemModelName             SnmpAdminString,
              lldpXMedRemAssetID               SnmpAdminString
              }

lldpXMedRemHardwareRev    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific hardware revision string
            as advertised by the remote endpoint."
    REFERENCE
```

```
        " ANSI/TIA-1057, Section 10.2.6.1"
    ::= { lldpXMedRemInventoryEntry 1 }

lldpXMedRemFirmwareRev    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific firmware revision string
            as advertised by the remote endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.2"
    ::= { lldpXMedRemInventoryEntry 2 }

lldpXMedRemSoftwareRev    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific software revision string
            as advertised by the remote endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.3"
    ::= { lldpXMedRemInventoryEntry 3 }

lldpXMedRemSerialNum    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific serial number
            as advertised by the remote endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.4"
    ::= { lldpXMedRemInventoryEntry 4 }

lldpXMedRemMfgName    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific manufacturer name
            as advertised by the remote endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.5"
    ::= { lldpXMedRemInventoryEntry 5 }

lldpXMedRemModelName    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific model name
            as advertised by the remote endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.6"
    ::= { lldpXMedRemInventoryEntry 6 }
```

```
lldpXMedRemAssetID    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The vendor-specific asset tracking identifier
            as advertised by the remote endpoint."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.6.7"
    ::= { lldpXMedRemInventoryEntry 7 }


--- lldpXMedRemLocationTable - Remote Location Information
---

lldpXMedRemLocationTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedRemLocationEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains Location information as advertised
            by the remote system.

            This table may be sparsely populated. Entries in this table are
            relevant only if the Location(3) bits in the
            lldpXMedRemCapSupported and lldpXMedRemCapCurrent objects of the
            corresponding ports are set "
    ::= { lldpXMedRemoteData 4 }

lldpXMedRemLocationEntry OBJECT-TYPE
    SYNTAX      LldpXMedRemLocationEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about Location information for the remote devices
             connected to the ports."
    INDEX   { lldpRemTimeMark,
              lldpRemLocalPortNum,
              lldpRemIndex,
              lldpXMedRemLocationSubtype}
    ::= { lldpXMedRemLocationTable 1 }

LldpXMedRemLocationEntry ::= SEQUENCE {
              lldpXMedRemLocationSubtype    LocationSubtype,
              lldpXMedRemLocationInfo       OCTET STRING
              }


lldpXMedRemLocationSubtype OBJECT-TYPE
    SYNTAX      LocationSubtype
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The location subtype advertised by the remote endpoint."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.4.2 "
```

```
    ::= { lldpXMedRemLocationEntry 1 }


lldpXMedRemLocationInfo OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..256))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The location information advertised by the remote endpoint.
             Parsing of this information is dependent upon the location
             subtype, as defined by the value of the corresponding
             lldpXMedRemLocationSubType object. "
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.4.3 "
    ::= { lldpXMedRemLocationEntry 2 }


--- lldpXMedRemXPoETable - Information about Remote PoE Device Type
---

lldpXMedRemXPoETable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedRemXPoEEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains information about the PoE device type
            as advertised by the remote system.

            This table is densely populated."
    ::= { lldpXMedRemoteData 5 }

lldpXMedRemXPoEEntry OBJECT-TYPE
    SYNTAX      LldpXMedRemXPoEEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about PoE type of the remote devices
             connected to the ports."
    INDEX   { lldpRemTimeMark,
              lldpRemLocalPortNum,
              lldpRemIndex }
    ::= { lldpXMedRemXPoETable 1 }

LldpXMedRemXPoEEntry ::= SEQUENCE {
              lldpXMedRemXPoEDeviceType    INTEGER
              }


lldpXMedRemXPoEDeviceType OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    pseDevice(2),
                    pdDevice(3),
                    none(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "Defines the type of Power-via-MDI (Power over Ethernet) advertised
             by the remote device.

             A value pseDevice(2) indicates that the device is advertised as a
             Power Sourcing Entity (PSE).

             A value pdDevice(3) indicates that the device is advertised as a
             Powered Device (PD).

             A value none(4) indicates that the device does not support PoE."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.1"
    ::= { lldpXMedRemXPoEEntry 1 }


--- lldpXMedRemXPoEPDTable - Extended PoE PSE Information from the remote device
---

lldpXMedRemXPoEPSETable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedRemXPoEPSEEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains extended PoE information as advertised
            by the remote devices of PSE type.

            This table may be sparsely populated. Entries in this table are
            relevant only if the extendedPSE(4) bits in the
            lldpXMedRemCapSupported and lldpXMedRemCapCurrent objects of the
            corresponding ports are set "
    ::= { lldpXMedRemoteData 6 }

lldpXMedRemXPoEPSEEntry OBJECT-TYPE
    SYNTAX      LldpXMedRemXPoEPSEEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about Extended PoE PSE information for
            the remote devices connected to the ports."
    INDEX   { lldpRemTimeMark,
              lldpRemLocalPortNum,
              lldpRemIndex }
    ::= { lldpXMedRemXPoEPSETable 1 }

LldpXMedRemXPoEPSEEntry ::= SEQUENCE {
              lldpXMedRemXPoEPSEPowerAv    Gauge32,
              lldpXMedRemXPoEPSEPowerSource INTEGER,
              lldpXMedRemXPoEPSEPowerPriority INTEGER
              }


lldpXMedRemXPoEPSEPowerAv  OBJECT-TYPE
    SYNTAX      Gauge32 (0..1023)
    UNITS      "tenth of watt"
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "This object contains the value of the power available from the
            PSE via this port expressed in units of 0.1 watts on the remote
            device."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.5.4"
    ::= { lldpXMedRemXPoEPSEEntry 1 }

lldpXMedRemXPoEPSEPowerSource OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    primary(2),
                    backup(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Defines the type of PSE Power Source advertised
             by the remote device.

             A value primary(2) indicates that the device advertises its power
             source as primary.

             A value backup(3) indicates that the device advertises its power
             Source as backup."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.2"
    ::= { lldpXMedRemXPoEPSEEntry 2 }

lldpXMedRemXPoEPSEPowerPriority OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    critical(2),
                    high(3),
                    low(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the PSE power priority
            advertised by the remote device.

            A value critical(2) indicates that the device advertises its power
            priority as critical, as per RFC 3621.

            A value high(3) indicates that the device advertises its power
            priority as high, as per RFC 3621.

            A value low(4) indicates that the device advertises its power
            priority as low, as per RFC 3621."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.3"
    ::= { lldpXMedRemXPoEPSEEntry 3 }
```

```
--- lldpXMedRemXPoEPDTable - Extended PoE PD Information from the remote device
---

lldpXMedRemXPoEPDTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF LldpXMedRemXPoEPDEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains extended PoE information as advertised
            by the remote devices of PD type.

            This table may be sparsely populated. Entries in this table are
            relevant only if the extendedPD(5) bits in the
            lldpXMedRemCapSupported and lldpXMedRemCapCurrent objects of the
            corresponding ports are set "
    ::= { lldpXMedRemoteData 7 }

lldpXMedRemXPoEPDEntry OBJECT-TYPE
    SYNTAX      LldpXMedRemXPoEPDEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information about XPoEPD information for the remote devices
             connected to the ports."
    INDEX   { lldpRemTimeMark,
              lldpRemLocalPortNum,
              lldpRemIndex }
    ::= { lldpXMedRemXPoEPDTable 1 }

LldpXMedRemXPoEPDEntry ::= SEQUENCE {
              lldpXMedRemXPoEPDPowerReq       Gauge32,
              lldpXMedRemXPoEPDPowerSource    INTEGER,
              lldpXMedRemXPoEPDPowerPriority  INTEGER
              }


lldpXMedRemXPoEPDPowerReq  OBJECT-TYPE
    SYNTAX      Gauge32 (0..1023)
    UNITS      "tenth of watt"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object contains the value of the power required by a
            PD connected remotely to the port
            expressed in units of 0.1 watts."
    REFERENCE
            " ANSI/TIA-1057, Section 10.2.5.4 "
    ::= { lldpXMedRemXPoEPDEntry 1 }

lldpXMedRemXPoEPDPowerSource OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    fromPSE(2),
                    local(3),
                    localAndPSE(4)
                }
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
            "Defines the type of Power Source advertised as being used
             by the device connected remotely to the port.

             A value fromPSE(2) indicates that the device advertises its power
             source as received from a PSE.

             A value local(3) indicates that the device advertises its power
             source as local.

             A value localAndPSE(4) indicates that the device advertises its
             power source as using both local and PSE power."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.2"
    ::= { lldpXMedRemXPoEPDEntry 2 }

lldpXMedRemXPoEPDPowerPriority OBJECT-TYPE
    SYNTAX      INTEGER  {
                    unknown(1),
                    critical(2),
                    high(3),
                    low(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Defines the priority advertised as being required by the PD
             connected remotely to the port.

             A value critical(2) indicates that the device advertises its power
             Priority as critical, as per RFC 3621.

             A value high(3) indicates that the device advertises its power
             Priority as high, as per RFC 3621.

             A value low(4) indicates that the device advertises its power
             Priority as low, as per RFC 3621."
    REFERENCE
            "ANSI/TIA-1057, Section 10.2.5.3"
    ::= { lldpXMedRemXPoEPDEntry 3 }







---


-- conformance information

lldpXMedConformance OBJECT IDENTIFIER ::= { lldpXMedMIB 2 }
lldpXMedCompliances OBJECT IDENTIFIER ::= { lldpXMedConformance 1 }
lldpXMedGroups      OBJECT IDENTIFIER ::= { lldpXMedConformance 2 }
```

```
-- compliance statements

lldpXMedCompliance MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
            "The compliance statement for SNMP entities which implement
            the LLDP MED extension MIB."

    MODULE  -- this module
        MANDATORY-GROUPS { lldpXMedConfigGroup,
                           lldpXMedRemSysGroup,
                           lldpXMedNotificationsGroup
        }
        GROUP lldpXMedOptMediaPolicyGroup
            DESCRIPTION
                "This group represents the information associated with
                the LLDP-MED optional Media Policy TLVs,
                therefore the agent may not implement them."
        GROUP lldpXMedOptInventoryGroup
            DESCRIPTION
                "This group represents the information associated with
                the LLDP-MED optional inventory TLVs,
                therefore the agent may not implement them."
        GROUP lldpXMedOptLocationGroup
            DESCRIPTION
                "This group represents the information associated with
                the LLDP-MED optional Location TLVs,
                therefore the agent may not implement them."
        GROUP lldpXMedOptPoEPSEGroup
            DESCRIPTION
                "This group represents the information associated with
                the LLDP-MED optional extended PoE PolicyTLVs, carrying
                PSE information, therefore the agent may
                not implement them."
       GROUP lldpXMedOptPoEPDGroup
            DESCRIPTION
                " This group represents the information associated with
                the LLDP-MED optional extended PoE Policy TLVs, carrying
                PD information, therefore the agent may
                not implement them."
    ::= { lldpXMedCompliances 1 }

-- MIB groupings

lldpXMedConfigGroup    OBJECT-GROUP
    OBJECTS {
        lldpXMedPortCapSupported,
        lldpXMedPortConfigTLVsTxEnable,
        lldpXMedPortConfigNotifEnable,
        lldpXMedFastStartRepeatCount,
        lldpXMedLocXPoEDeviceType,
        lldpXMedLocDeviceClass
    }
    STATUS  current
    DESCRIPTION
            "The collection of objects which are used to configure or
            describe the configuration or behavior of the LLDP-MED
```

```
            organizational extension implementation."
    ::= { lldpXMedGroups 1 }

lldpXMedOptMediaPolicyGroup  OBJECT-GROUP
    OBJECTS {
        lldpXMedLocMediaPolicyVlanID,
        lldpXMedLocMediaPolicyPriority,
        lldpXMedLocMediaPolicyDscp,
        lldpXMedLocMediaPolicyUnknown,
        lldpXMedLocMediaPolicyTagged
        }
    STATUS  current
    DESCRIPTION
            "The collection of objects which are used to represent LLDP
            MED organizational extensions for Media Policy Information."
    ::= { lldpXMedGroups 2 }



lldpXMedOptInventoryGroup  OBJECT-GROUP
    OBJECTS {
        lldpXMedLocHardwareRev,
        lldpXMedLocFirmwareRev,
        lldpXMedLocSoftwareRev,
        lldpXMedLocSerialNum,
        lldpXMedLocMfgName,
        lldpXMedLocModelName,
        lldpXMedLocAssetID
        }
    STATUS  current
    DESCRIPTION
            "The collection of objects which are used to represent LLDP
            MED organizational extension for inventory Information."
    ::= { lldpXMedGroups 3 }
lldpXMedOptLocationGroup  OBJECT-GROUP
    OBJECTS {
        lldpXMedLocLocationInfo
        }
    STATUS  current
    DESCRIPTION
            "The collection of objects which are used to represent LLDP
            MED organizational extension for Location Information."
    ::= { lldpXMedGroups 4 }


lldpXMedOptPoEPSEGroup  OBJECT-GROUP
    OBJECTS {
        lldpXMedLocXPoEPSEPortPowerAv,
        lldpXMedLocXPoEPSEPortPDPriority,
        lldpXMedLocXPoEPSEPowerSource
        }
    STATUS  current
    DESCRIPTION
            "The collection of objects which are used to represent LLDP
            MED organizational extensions for PoE PSE Information."
    ::= { lldpXMedGroups 5 }
```

```
lldpXMedOptPoEPDGroup  OBJECT-GROUP
    OBJECTS {
        lldpXMedLocXPoEPDPowerReq,
        lldpXMedLocXPoEPDPowerSource,
        lldpXMedLocXPoEPDPowerPriority
        }
    STATUS  current
    DESCRIPTION
            "The collection of objects which are used to represent LLDP
            MED organizational extensions for PoE PD Information."
    ::= { lldpXMedGroups 6 }

lldpXMedRemSysGroup  OBJECT-GROUP
    OBJECTS {
        lldpXMedRemCapSupported,
        lldpXMedRemCapCurrent,
        lldpXMedRemDeviceClass,
        lldpXMedRemMediaPolicyVlanID,
        lldpXMedRemMediaPolicyPriority,
        lldpXMedRemMediaPolicyDscp,
        lldpXMedRemMediaPolicyUnknown,
        lldpXMedRemMediaPolicyTagged,
        lldpXMedRemHardwareRev,
        lldpXMedRemFirmwareRev,
        lldpXMedRemSoftwareRev,
        lldpXMedRemSerialNum,
        lldpXMedRemMfgName,
        lldpXMedRemModelName,
        lldpXMedRemAssetID,
        lldpXMedRemLocationInfo,
        lldpXMedRemXPoEDeviceType,
        lldpXMedRemXPoEPSEPowerAv,
        lldpXMedRemXPoEPSEPowerSource,
        lldpXMedRemXPoEPSEPowerPriority,
        lldpXMedRemXPoEPDPowerReq,
        lldpXMedRemXPoEPDPowerSource,
        lldpXMedRemXPoEPDPowerPriority
    }
     STATUS  current
    DESCRIPTION
            "The collection of objects which are used to represent LLDP-
            MED organizational extension Remote Device Information."
    ::= { lldpXMedGroups 7 }

lldpXMedNotificationsGroup NOTIFICATION-GROUP
     NOTIFICATIONS { lldpXMedTopologyChangeDetected }
     STATUS current
     DESCRIPTION
           "Notifications sent by an LLDP-MED agent."
           ::= { lldpXMedGroups 8 }



END
```

ANNEX A: PICS Proforma for LLDP-MED (Normative)

The supplier of a protocol implementation that is claimed to conform to this Standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma. A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented.

Detailed instructions for completing a PICS Proforma can be found in Annex B, of the IEEE 802.1AB specification [2].

A.1 Status Symbols

M	Mandatory
O	Optional
O.n	Optional, but at least one group of options labeled by the same numeral n is required
X	Prohibited

A.2 Implementation Identification

Supplier	
Contact point for queries about the PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification—e.g., name(s) and version(s) of machines and/or operating system names	
NOTES 1—Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification. 2—The terms Name and Version should be interpreted appropriately to correspond with a supplier's terminology (e.g., Type, Series, Model).	

A.3 Protocol Summary

Identification of protocol specification	TIA-1057, LLDP Media Endpoint Discovery
Identification of amendments and corrigenda to the PICS proforma that have been completed as part of the PICS	Amd. : Corr. : Amd. : Corr. :
Have any Exception items been required? (The answer Yes means that the implementation does not conform to LLDP-MED.)	No [ ] Yes [ ]

Date of Statement	

A.4 Major Capabilities and Options

Item	Feature	Status	References	Support
lldptlv	Is the LLDP-MED LLDPDU usage of each of the following IEEE 802.1AB TLVs in conformance with the defined requirements			
	System Capabilities TLV	M	9.2.1	Yes [ ]
	MAC/PHY configuration/status TLV	M	9.2.2	Yes [ ]
	Chassis ID TLV	M	9.2.3	Yes [ ]
	Port ID TLV	M	9.2.3	Yes [ ]
	Power via MDI TLV	M	9.2.4	Yes [ ]

medxset	Which mandatory LLDP-MED Organizationally Specific TLV set is implemented (one is mandatory, only one allowed)	M	10.2.1	Yes [ ]
	Network Connectivity (if yes, answer item **nettlv** and skip **class1tlv, class2tlv, class3tlv**)	O.1	10.2.1.1	Yes [ ] No [ ]
	Endpoint Class I (if yes, answer item **class1tlv** and skip **nettlv, class2tlv, class3tlv**)	O.1	10.2.1.2	Yes [ ] No [ ]
	Endpoint Class II (if yes, answer item **class2tlv** and skip **nettlv, class1tlv, class3tlv**)	O.1	10.2.1.3	Yes [ ] No [ ]
	Endpoint Class III (if yes, answer item **class3tlv** and skip **nettlv, class1tlv, class2tlv**)	O.1	10.2.1.4	Yes [ ] No [ ]
nettlv	If the Network Connectivity TLV set is implemented, is each TLV in the set implemented and in conformance with the usage indicated in Table 5.			
	LLDP-MED Capabilities Network Policy Location Identification Extended Power-via-MDI	nettlv:M nettlv:M nettlv:M nettlv:M	10.2.2 10.2.3 10.2.4 10.2.5	Yes [ ] Yes [ ] Yes [ ] Yes [ ]
class1tlv	If the Endpoint Class I TLV set is implemented, is each TLV in the set implemented and in conformance with the usage indicated in Table 6.			
	LLDP-MED Capabilities Network Policy Extended Power-via-MDI	class1tlv:M class1tlv:M class1tlv:M	10.2.2 10.2.3 10.2.5	Yes [ ] Yes [ ] Yes [ ]
class2tlv	If the Endpoint Class II TLV set is implemented, is each TLV in the set implemented and in conformance with the usage indicated in Table 7.			
	LLDP-MED Capabilities Network Policy Extended Power-via-MDI	class2tlv:M class2tlv:M class2tlv:M	10.2.2 10.2.3 10.2.5	Yes [ ] Yes [ ] Yes [ ]

class3tlv	If the Endpoint Class II TLV set is implemented, is each TLV in the set implemented and in conformance with the usage indicated in Table 8. LLDP-MED Capabilities Network Policy Location Identification Extended Power-via-MDI	 class3tlv:M class3tlv:M class3tlv:M class3tlv:M	 10.2.2 10.2.3 10.2.4 10.2.5	 Yes [ ] Yes [ ] Yes [ ] Yes [ ]
invset	Is the optional LLDP-MED Inventory Management TLV set implemented (if yes, answer **invtlv**) (if no, skip **invtlv**)	O	10.2.1.5	Yes [ ] No [ ]
invtlv	If the Inventory Management TLV set is implemented, is each TLV in the set implemented Inventory - Hardware Revision Inventory - Firmware Revision Inventory - Software Revision Inventory - Serial Number Inventory - Manufacturer Name Inventory - Model Name Inventory - Asset ID	 invtlv:M invtlv:M invtlv:M invtlv:M invtlv:M invtlv:M invtlv:M	 10.2.6.1 10.2.6.2 10.2.6.3 10.2.6.4 10.2.6.5 10.2.6.6 10.2.6.7	 Yes [ ] Yes [ ] Yes [ ] Yes [ ] Yes [ ] Yes [ ] Yes [ ]
medprot	Are the LLDP-MED Protocol Interactions in conformance with the defined requirements	M	11	Yes [ ]
lldpmib	Which type of MIB is implemented (one is mandatory) SNMP is supported (if yes, answer item **snmpmib** and skip **equivstor**) SNMP is not supported (if yes, answer **equivstor** and skip **snmpmib**)	 O.2 O.2	 13 13	 Yes [ ] No [ ] Yes [ ] No [ ]
snmpmib	If the SNMP MIB is implemented, is the MIB module in conformance with the defined requirements	M	13	Yes [ ]

equivstor	If the SNMP is not supported, is the provided storage and retrieval capability functionally equivalent with the indicated specifications of this clause for the operating mode being implemented	M	10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 12.3	Yes [ ]

ANNEX B: Content of Civic Address LCI data format (Normative)

IMPORTANT INFORMATIVE NOTE

At time of publication of this Standard, the specific content of the Civic Address LCI subtype of the Location Identification TLV (see section 10.2.4.3.2, Civic Address LCI data format) is in draft form in IETF. The current version of this work in progress is draft-ietf-geopriv-dhcp-civil-07.txt.

In order to provide full information content in this Standard, the relevant sections of draft-ietf-geopriv-dhcp-civil-07 are reproduced below with permission of IETF and Henning Schulzrinne (author). Non-relevant sections are not provided here. For clarity, the original content of draft-ietf-geopriv-dhcp-civil-07 is provided in `plain text`, and additional notes to the reader are given in ***bold italics***.

The intention of this Standard is to directly reference this work when it becomes an IETF RFC, and to remove this Annex at that time. The reader is encouraged to check the status of this work in IETF.

```
3.  Format of the DHCP Civic Location Option

3.1  Overall Format for DHCPv4

   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | GEOCONF_CIVIC |       N       |      what     |    country    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    code       |        civic address elements                ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

NOTE – The Civic Address LCI data format, as used in the Location Identification TLV defined in this Standard, does NOT include the GEOCONF_CIVIC field (since it is the DHCP option number). Refer to section 10.2.4.3.2, Figure 10 – Civic Address LCI data format, for details of the format as used in this Standard.

```
   Code GEOCONF_CIVIC: The code for this DHCP option is TBD by IANA.

   N: The length of this option is variable.  The minimum length is 3.
```

NOTE – The 'N' field is renamed 'LCI Length' as used in this Standard, for clarity. As used in this Standard, the minimum value of this field is 5, since at least one civic address element must be provided. Refer to section 10.2.4.3.2, Figure 10 – Civic Address LCI data format.

```
   what: The 'what' element describes which location the DHCP entry
      refers to.  Currently, three options are defined:  the location of
      the DHCP server (a value of 0), the location of the network
      element believed to be closest to the client (a value of 1) or the
      location of the client (a value of 2).  Option (2) SHOULD be used,
      but may not be known.  Options (0) and (1) SHOULD NOT be used
      unless it is known that the DHCP client is in close physical
      proximity to the server or network element.

   country code: The two-letter ISO 3166 country code in capital ASCII
      letters, e.g., DE or US.  (Civic addresses always contain country
```

designations, suggesting the use of a fixed-format field to save space.)

civic address elements: Zero or more elements comprising the civic and/or postal address, with the format described below (Section 3.3).

3.3 Element Format

For both DHCPv4 and DHCPv6, each civic address element has the following format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   CAtype      |   CAlength    |      CAvalue                 ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

CAtype: A one-octet descriptor of the data civic address value.

CAlength: The length, in octets, of the CAvalue, not including the CAlength field itself.

CAvalue: The civic address value, as described in detail below.

3.4 Civic Address Components

Since each country has different administrative hierarchies, with often the same (English) names, this specification adopts a simple hierarchical notation that is then instantiated for each country. We assume that five levels are sufficient for sub-national divisions above the street level.

All elements are OPTIONAL and can appear in any order.

Component values MUST be encoded as UTF-8 [6]. They SHOULD be written in mixed case, following the customary spelling. The script indication (CAtype=128) MUST be written in mixed-case, with the first letter a capital letter.

Abbreviations MUST NOT be used unless indicated for each element. Abbreviations do not need a trailing period.

It is RECOMMENDED that all elements in a particular script (CAtype 128) and language (CAtype 0) be grouped together as that reduces the number of script and language identifiers needed.

For each script and language, elements SHOULD be included in numeric order from lowest to highest of their CAtype. In general, an element is labeled in its language and script by the most recent 'language tag' (CAtype = 0) element preceding it. Since not all elements depend on the script and language, a client accumulates the elements by CAtype and then selects the most desirable language and script rendition if there are multiple elements for the same CAtype.

CAtype	label	description
1	A1	national subdivisions (state, canton, region, province, prefecture)
2	A2	county, parish, gun (JP), district (IN)
3	A3	city, township, shi (JP)
4	A4	city division, borough, city district, ward, chou (JP)
5	A5	neighborhood, block
6	A6	street

Table 1

For specific countries, the administrative sub-divisions are described below.

CA (Canada): The mapping to NENA designations is shown in parentheses. A1=province (STA); A2=county (CNA); A3=city or town (MCN); A6=street (STN).

DE (Germany): A1=state (Bundesstaat); A2=county (Regierungsbezirk); A3=city (Stadt, Gemeinde); A4=district (Bezirk); A6=street (Strasse). Street suffixes (STS) are used only for designations that are a separate word (e.g., Marienthaler Strasse).

JP (Japan): A1=metropolis (To, Fu) or prefecture (Ken, Do); A2=city (Shi) or rural area (Gun); A3=ward (Ku) or village (Mura); A4=town (Chou or Machi); A5=city district (Choume); A6=block (Banchi or Ban).

KR (Korea): A1=province (Do); A2=county (gun); A3=city or village (ri); A4=urban district (gu); A5=neighborhood (dong); A6=street (no, ro, ga or gil).

US (United States): The mapping to NENA designations is shown in parentheses. A1=state (STA), using the the two-letter state and possession abbreviations recommended by the United States Postal Service Publication 28 [18], Appendix B; A2=county (CNA); A3=civic community name (city or town) (MCN); A6=street (STN). A4 and A5 are not used. The civic community name (MCN) reflects the political boundaries. These may differ from postal delivery assignments for historical or practical reasons.

Additional CA types appear in many countries and are simply omitted where they are not needed or known:

CAtype	NENA	PIDF	Description	Examples
0			language	i-default [3]
16	PRD	PRD	leading street direction	N
17	POD	POD	trailing street suffix	SW
18	STS	STS	street suffix	Ave, Platz
19	HNO	HNO	house number	123
20	HNS	HNS	house number suffix	A, 1/2
21	LMK	LMK	landmark or vanity address	Columbia University
22	LOC	LOC	additional location information	South Wing
23	NAM	NAM	name (residence and office occupant)	Joe's Barbershop
24	ZIP	PC	postal/zip code	10027-1234
25			building (structure)	Low Library
26			unit (apartment, suite)	Apt 42
27		FLR	floor	4
28			room number	450F
29			placetype	office
30	PCN		postal	Leonia

			community name	
31			post office box (P.O. Box)	12345
32			additional code	13203000003
128			script	Latn
255			reserved	

The CA types labeled in the second column correspond to items from the NENA "Recommended Formats & Protocols For ALI Data Exchange, ALI Response & GIS Mapping" [19], but are applicable to most countries. The "NENA" column refers to the data dictionary name in Exhibit 18 of [19].

The column labeled PIDF indicates the element name from [17]. (Some elements were added to this document after the PIDF location object definition had been completed. These elements currently do not have a PIDF-LO equivalent.)

Language: The "language" item (CAtype 0) optionally identifies the language used for presenting the address information, drawing from the tags for identifying languages in [7]. If omitted, the default value for this tag is "i-default" [3].

Script: The "script" item (CAtype 128) optionally identifies the script used for presenting the address information, drawing from the tags for identifying scripts in ISO 15924 [14]. If omitted, the default value for this tag is "Latn".

POD, PRD: The abbreviations N, E, S, W, and NE, NW, SE, SW SHOULD be used for POD (trailing street suffix) and PRD (leading street direction) in English-speaking countries.

STS: STS designates a street suffix. In the United States (US), the abbreviations recommended by the United States Postal Service Publication 28 [18], Appendix C, SHOULD be used.

HNS: HNS ("house number") is a modifier to a street address; it does not identify parts of a street address.

LMK: LMK ("landmark", CAtype 21) is a string name for a location. It conveys the same information as the street address, but reflects common local designation of a structure, a group of buildings or a place that helps recipients locate the place. For example, an industrial park may have a widely-recognized name that is more readily found than a single street address. Some places, such as parks, may not have street names or house numbers and SHOULD be identified by a LMK string. In addition, this component can be used to indicate where postal delivery locations differ from the jurisdictional one.

LOC: LOC ("location", CAtype 22) is an unstructured string specifying additional information about the location, such as the part of a building.

PCN: The postal community name (CAtype 30) and the post office box (CAtype 31) allow the recipient to construct a postal address. The post office box field should contain the words "P.O. Box" or other locally appropriate postal designation.

NAM: The NAM object is used to aid user location ("Joe Miller" "Alice's Dry Cleaning"). It does not identify the person using a communications device, but rather the person or organization associated with the address.

LMK: While a landmark (LMK, CAtype 21) can indicate a complex of buildings, 'building' (CAtype 25) conveys the name of a single building if the street address includes more than one building or the building name is helpful in identifying the location. (For example, on university campuses, the house number is often not displayed on buildings, while the building name is prominently shown.)

Unit: The 'unit' object (CAtype 26) contains the name or number of a part of a structure where there are separate administrative units, owners or tenants, such as separate companies or families who occupy that structure. Common examples include suite or apartment designations.

Room: A 'room' (CAtype 28) is the smallest identifiable subdivision of a structure.

The "type of place" item (CAtype 29) describes the type of place described by the civic coordinates. For example, it describes whether it is a home, office, street or other public space. The values are drawn from the items in the location types registry [13]. This information makes it easy, for example, for the DHCP client to then populate the presence information. Since this is an IANA-registered token, the language and script designations do not apply for this element.

The "additional code" item (CAtype 32) provides an additional, country-specific code identifying the location. For example, for Japan, it contains the Japan Industry Standard (JIS) address code. The JIS address code provides a unique address inside of Japan, down to the level of indicating the floor of the building.

4. Postal Addresses

In general, a recipient can construct a postal address by using all language-appropriate elements, including the postal code (ZIP, CAtype 24). However, certain elements override the civic address components to create a postal address. If the elments include a post office box (CAtype 31), the street address components (A6, PRD, POD, STS, HNO, HNS) are replaced with the post office box element. If a postal community name is specified, the civic community name (typically, A3) is replaced by the postal community name (PCN, CAtype 30). Country-specific knowledge is required to create a valid postal address. The formating of such addresses is beyond the scope of this document.

5. Example

Rather than showing the precise byte layout of a DHCP option, we show a symbolic example below, representing the civic address of the Munich city hall in Bavaria, Germany. The city and state name are also conveyed in English and Italian in addition to German; the other items are assumed to be common across all languages. All languages use the latin script.

CAtype	CAvalue
0	de
128	Latn
1	Bayern
2	Oberbayern
3	M=U+00FCnchen
6	Marienplatz
19	8
21	Rathaus
24	80331
29	government-building
31	Postfach 1000
0	en
1	Bavaria
3	Munich
0	it
1	Baviera
3	Monaco

NOTE – The references below are included in the reproduced sections of draft-ietf-geopriv-dhcp-civil-07 above. Other references are not included here.

8.1 Normative References

[3] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[6] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[7] Alvestrand, H., "Tags for the Identification of Languages", BCP 47, RFC 3066, January 2001.

[13] Schulzrinne, H. and H. Tschofenig, "Location Types Registry", draft-ietf-geopriv-location-types-registry-03 (work in progress), August 2005.

[14] International Organization for Standardization, ISO., "Information and documentation - Codes for the representation of names of scripts", February 2004.

8.2 Informative References

[17] Peterson, J., "A Presence-based GEOPRIV Location Object Format", draft-ietf-geopriv-pidf-lo-03 (work in progress), September 2004.

[18] United States Postal Service, "Postal Addressing Standards", November 2000.

[19] National Emergency Number Assocation, "NENA Recommended Formats and Protocols For ALI Data Exchange, ALI Response and GIS Mapping", NENA NENA-02-010, January 2002.

ANNEX C: LLDP-MED Support for Voice over Wireless LAN (Informative)

(This Annex is informative only, and is not part of this Standard.)

This section describes, at a high level, how the various LLDP-MED attributes apply to Voice over Wireless LAN (VoWLAN) environments.

While there are remaining VoWLAN concerns at time of writing of this Standard, notably related to device location, there do not appear to be open standards solutions to these issues available in the near future. Since many IEEE 802.11 standardization efforts are still in flux in related areas, VoWLAN-specific TLVs or other extensions are deferred for a future release of LLDP-MED, when the appropriate external standards efforts are better defined.

C.1 Standard AP Topology

Figure 22, below, shows a VoWLAN reference topology as applicable to LLDP-MED using a standard Access Point (AP) deployment.

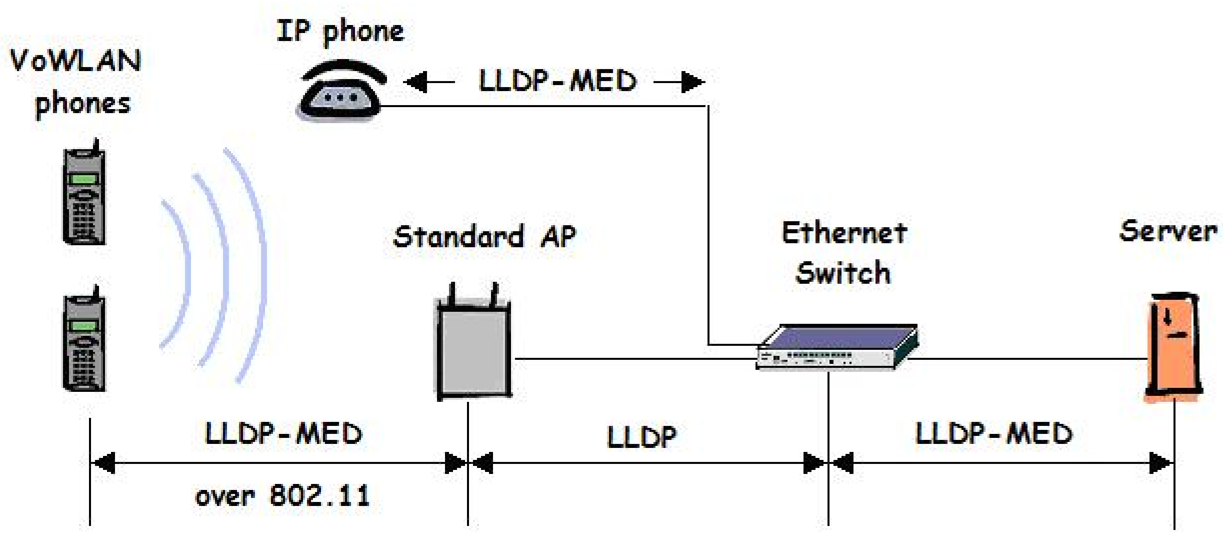

Figure 22 – VoWLAN Reference Topology for Standard APs

The reference topology illustrates the applicability of IEEE 802.1AB LLDP [1] and LLDP-MED across the different IEEE 802 LAN segments and media types. LLDP operates by transmitting and receiving LLDPDUs over LAN segments that are bounded by Media Access Control (MAC) Entities that operate within each LAN station connected to that segment. Multiple MAC entities may operate over a single LAN segment. LLDP operates above the MAC service layer defined in IEEE 802 and as such can be implemented in any networking device that implements a MAC service, which is required for the operation of the specific medium.

Since IEEE 802.11 wireless networks are based on a shared media, multiple devices may share the same Service Set Identifier (SSID) on a given AP. When used in conjunction with 802.11i encryption [26], an AP will create a separate virtual link between the AP and every station for unicast traffic. However, all stations still share a single logical channel for broadcast or multicast packets. Because LLDP is a multicast protocol, all stations in a given SSID will receive the same LLDPDU. This, in effect, limits the advertisement to TLV attributes common to all stations in the same SSID.

It should be noted that the LLDP multicast address is within a range reserved by IEEE 802.1D-2004 [3] for protocols constrained to an individual LAN. This ensures that an LLDPDU will not be forwarded between interfaces by MAC Bridges that conform to IEEE 802.1D-2004 [3].

The mechanism to send multicast packets, in an 802.11 distribution system, is for a station to unicast the packet to the AP; at which point the AP will re-distribute the packet as a multicast to all associated stations. This is because the access point may be the only device able to receive from all other stations. Based on this behaviour, it is strongly recommended that access points supporting LLDP-MED do not re-distribute or forward (i.e. relay between endpoints) any LLDP frames on the wireless link, in order to conserve RF resources and reduce associated security considerations.

C.2 WLAN Switch Architectures

There is a currently a great deal of standardization and development activity ongoing in the area of coordinated AP functions based on a variety of WLAN switch architectures. In these types of WLAN deployments, the IEEE 802.11 AP functions may be implemented across multiple physical devices through the use of an encapsulation and control protocol such as being defined by the IETF CAPWAP Working Group [32]. These types of split AP implementations are currently vendor dependent. In some, the wireless MAC service entities operate as part of a central WLAN switch to provide for wireless media access distributed across multiple different physical APs.

In this type of AP model, the LLDP protocol entity for the wireless link would operate wherever the specific AP MAC protocol entity resides. The central WLAN switch is required to operate a specific MAC entity along with the LLDP Protocol Entity for every AP associated with it. This differs from the traditional AP model; where the MAC service and LLDP Protocol Entity for the wireless LAN operates within the physical AP itself.

C.3 Applicable TLVs for VoWLAN

Given considerations described in the previous subsections, both LLDP and LLDP-MED are largely applicable to WLAN and VoWLAN environments, with some exceptions and restrictions.

Table 24, below, lists the applicability of LLDP core specification TLVs, as used in this Standard, in VoWLAN environments.

Table 24 – Applicability of LLDP TLVs for VoWLAN

Base LLDP TLVs	Applicable to VoWLAN	Restrictions
System Capabilities	Yes	None
MAC/PHY configuration	No	Not applicable to WLAN (IEEE 802.3-specific)
Chassis ID	Limited	Can only provide physical location of AP[1]
Port ID	Limited	Can only provide physical location of AP[1]
Power via MDI	No	Not applicable to WLAN

Note 1: Since LLDP is a multicast protocol, only one location ID can be advertised per SSID.

Table 25, below, lists the applicability of LLDP-MED extended TLVs, as defined in this Standard, in VoWLAN environments.

Table 25 – Applicability of LLDP-MED Extended TLVs for VoWLAN

LLDP-MED TLV Extensions	Applicable to VoWLAN	Restrictions
LLDP-MED Capabilities	Yes	None
Network Policy	Yes	VLAN ID does not typically apply
Location Identification	Limited	Can only provide physical location of AP[1]
Extended Power-via-MDI	No	Not applicable to WLAN
Inventory TLVs	Yes	None

Note 1: Since LLDP is a multicast protocol, only one location ID can be advertised per SSID.

C.4 Issues for VoWLAN Support

The following issues are known to exist at time of writing of this release of this Standard:

- There is currently no standardized method of endpoint device location to support ECS applications in enterprise 802.11 deployments. The most likely solutions would involve RSSI triangulation between several Access Points or Time Difference of Arrival (TDOA), however the specific methods and APIs are not standardized, nor do such standards appear to be close at hand.

- Based on the relatively dynamic nature of VoWLAN device location and that LLDP is designed as a slow multicast protocol; raises the question that LLDP may not be the appropriate protocol to distribute endpoint device location over 802.11.

Addressing these issues in the LLDP-MED context is left for future consideration.

ANNEX D: Informative References

(This Annex is informative only, and is not part of this Standard.)

The following documents contain useful information for understanding the basis for requirements contained in this Standard.

At the time of publication, the editions indicated were valid. All documents are subject to revision and parties are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below.

[22] TIA-811-A, Performance and Interoperability Requirements for Voice-over-IP (VoIP) Feature Telephones, March 2006.

[23] TIA-TSB-146, IP Telephony Support for Emergency Calling Service, March 2003.

[24] IEEE Std 802.1X™-2004, Standard for Local and Metropolitan Networks – Port-Based Network Access Control.[4]

[25] IEEE Std 802.11™, 1999 Edition, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[26] IEEE Std 802.11i™-2004, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements.

[27] IETF RFC 2475, An Architecture for Differentiated Services, Blake et al, December 1998 (see also RFC3260 [28]).

[28] IETF RFC 3260, New Terminology and Clarifications for Diffserv, Grossman, April 2002.

[29] IETF RFC 2131, Dynamic Host Configuration Protocol, Droms, March 1997.

[30] IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, Alexander et al, March 1997.

[31] IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, Case et al, December 2002.

[32] IETF Working Group - Control and Provisioning of Wireless Access Points (CAPWAP), refer to http://ietf.org/html.charters/capwap-charter.html (see also IETF RFC 3990, Configuration and Provisioning for Wireless Access Points (CAPWAP) Problem Statement, O'Hara et al, February 2005).

[33] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), Rigney et al, June 2000.

[4] The IEEE standards referred to in this Standard are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[34] ITU-T Recommendation E.164, The International Public Telecommunication Numbering Plan, May 1997.

TIA