Draft Standard for Local and Metropolitan Area Networks-
Emergency Services for Internet Protocol (IP) Based
Citizen-to-Authority Communications

Sponsor
LAN/MAN Committee
of the
IEEE Computer Society
Approved <XX MONTH 20XX>
IEEE-SA Standards Board

This is the initial public draft proposed for IEEE 802.23. It defines the additional elements generally needed to meet the regulatory requirements for interconnected VoIP calls originating on an IEEE 802 network when making a call to Emergency Services via a special access code for that purpose (e.g. 112/911). Draft D0.9 is prepared by the IEEE 802.23 for initial consideration and review before formal Working Group Ballot. This draft expires 6 months after the date of publication or when the next version is published, whichever comes first.

IEEE Standards Activities Department
445 Hoes Lane
Piscataway, NJ 08854, USA

<Editor's Note to be removed when action is complete: INSERT REMAINDER OF FRONT MATTER HERE>

Contents

<Editor's Note to be removed when action is complete: After draft body is complete, select this text and click Insert Special->Add (Table of) Contents>

Draft Standard for Local and Metropolitan Area Networks- Emergency Services for Internet Protocol (IP) Based Citizen-to-Authority Communications

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers.

These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

1. Overview

1.1 Scope

This standard defines a media independent framework within IEEE 802 to provide consistent access and data that facilitate compliance to applicable civil authority requirements for communications systems that include IEEE 802 networks. This includes a data link layer interface for a consistent view of IEEE 802 networks by IP (Internet Protocol) based Citizen-to-Authority emergency services capabilities from the Internet Engineering Task Force (IETF) Emergency Context Resolution with Internet Technologies (ECRIT). This standard specifies a Layer 2 entity and associated behaviors with a uniform structure of management information for transferring data required by an emergency services request.

1.2 Purpose

The purpose of this standard is to support compliance to civil authority requirements complementary to IETF ECRIT specifications for Citizen-to-Authority emergency services functionality. This standard intends to encompass voice, data and multi-media requests across IEEE 802 using a new Layer 2 entity and associated behaviors and provide a uniform Structure of Management Information (SMI) for transferring required data for emergency services requests.
(Editor's Note to be removed when action is complete: The purpose as stated here (i.e. on the PAR) will not be included in the standard. Working group to determine purpose text to be inserted in the draft.)

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

- NENA i3, Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3, Sept. 30, 2010.
- RFC 3693, GeoPriv Requirements
- draft-ietf-ecrit-phonebcp-13 ECRIT Req'ts
- (US) FCC 05-116
- IEEE 802.11u draft 13.0
- IEEE Std 802.16n – 200n
- ietf-draft-rosen-ecrit-additional-data
- ietf-draft-schulzrinne-ecrit-psap-callback
- ietf-draft-schulzrinne-ecrit-unauthenticated-access
- draft-ietf-geopriv-held-measurements

(Editor's note to be removed when action is complete: The list is not necessarily complete at this point in terms of items and each item has to be expanded to a full reference in line with the style guide.)

3. Definitions

For the purposes of this document, the following terms and definitions apply. The IEEE Standards Dictionary: Glossary of Terms & Definitions should be consulted for terms not defined in this clause.
Authorized service: The voice (or other ES applicable) service where the EUT has access to all network services (L1/L2, and higher level IP services) needed to support an ES call.

Emergency Services: Network communication services needed to support an emergency call between a EUT and a PSAP. These services may include, but are not be limited to, normal network services needed to support an ordinary VoIP call, location services, recognition and differentiation of an emergency call from an ordinary call.

End User Terminal: The host device to the IP application (e.g. VoIP) which places the ES call.

ESInet: An IP network/internetwork that is managed for the use of emergency services communications, and can be commonly shared by participating public safety agencies.

IEEE 802 network, 802 network: A local area (LAN) or other (e.g. MAN, WAN) packet switched network consisting of one or more interconnected subnetworks each using a MAC protocol specified in an IEEE 802 standard.

Internet Protocol: The principal communications protocol used for relaying datagrams (packets) across an internetwork (i.e. network of networks) using the Internet Protocol Suite. Responsible for routing packets across network boundaries (i.e. routers), it is the primary protocol that establishes the Internet. For the purposes of this standard, the term is limited to Internet Protocol version 4 (Ipv4, IETF RFC 791) and/or Internet Protocol version 6 (Ipv6, IETF RFC 2460)

Layer 1/Layer 2: Within Layer 1 and/or Layer 2 relative to the ISO 7 Layer model as adapted by IEEE Std 802.

Local Area Network: See IEEE 802 network.

Ordinary citizen: A user acting in his or her regular capacity, i.e. not acting as official or an agent of any governing authority.

Unauthorized service: Voice (or other ES applicable) service where the EUT does not have access to network services (L1/L2, and higher level IP services) needed to support an ES call. This may involve lack of security access to the L1/L2 network or lack of access for whatever reason (other than bandwidth) to an interconnected voice service at the higher layers.

4. Abbreviations and acronyms

ANI: Automatic Number Identification
ANQP: Access Network Query Protocol
ECRIT: Emergency Context Resolution with Internet Technologies
ES: Emergency Services
ESInet: Emergency Services IP Network
EUT: End User Terminal
GAS: Generic Advertisement Service
GEOPRIV: Geographic Location and Privacy
GPS: Global Positioning System
IETF: Internet Engineering Task Force
IP: Internet Protocol(s)
L1/L2: Layer 1/Layer 2
LAN: Local Area Network
LBS: Location Based Services
LLDP: Link Layer Discovery Protocol (Ref: IEEE Std 802.1AB)
LS: Location Server
MIB: Management Information Base
PSAP: Public Safety Answering Point
PSTN: Public Switched Telephone Network
RFC: Request For Comment (Ref: IETF)
SIP: Session Initiation Protocol
SMI: Structure of Management Information

STA: Station
VLAN: Virtual LAN
VOIP: Voice Over IP
WPAN: Wireless Personal Area Network (Ref: IEEE Std 802.15)

5. General description

Citizen-to-Authority emergency calls (e.g. "dialing" 112, 911 and most other country equivalents) are required to provide location information upon initiation. While other sources of location information may be available to the EUT (e.g. GPS), it is desirable to provide location from the adjacent network infrastructure (especially fixed infrastructure). This information is expected to be supplied via the management plane of the EUT. The EUT will transmit this data within an IP transaction across the IEEE 802 network to Layer 3 interfaces that providing IP services that are encountered away from the EUT. The data transaction exits the 802 scope and domain at the Layer 3 interface. In addition, an IP services Location Server (LS) attached to the IEEE 802 network needs to be able to provide location information for elements in the IEEE 802 network to the upper layers (security considerations).

For normal (i.e. non-emergency) call, a Voice over Internet Protocol (VoIP) system operates transparently and independently with respect to the Layer 1/Layer 2 (L1/L2) services. This transparency does not satisfy the requirements on originating VoIP calls imposed in the case of Citizen-to-Authority calls of an emergency nature (112/E911 calls). This standard is intended to provide L1/L2 information to upper layer implementations of VoIP and supporting services, including those as specified by the Internet Engineering Task Force (IETF). The primary interfaces for defining these requirements will be the Emergency Context Resolution with Internet Technologies (ECRIT) working group and Geographic Location and Privacy (GEOPRIV) working group.

The IEEE 802 family of standards may need to supply additional facilities and information to the upper layers in order to support ES requirements.
The mechanisms specified may be highly dependent on whether an EUT has a previously established relationship and/or connection with both the IEEE 802 network and any higher layer VoIP service. For the purposes of this standard the requirements will be divided into two major cases, those required to support “authorized service” (i.e. the EUT has an already established service relationship) and those required to support “unauthorized service”.

5.1   Overview of Emergency Services

For discussion and specification purposes, the overall scope of Emergency Services and Emergency Services standards are generally divided into four sub-areas. These are:

- Citizen-to-Authority calls
- Authority-to-Citizen alerts
- Authority-to-Authority communications
- Citizen-to-Citizen communications

The scope of this standard is limited to Citizen-to-Authority calls, that is calls or communications that a ordinary citizen makes to contact and communicate with the emergency services dispatch center that serves the present location of the citizen. Such a dispatch center is known as a PSAP (Public Safety Answering Point), a call processing and dispatch center that is responsible for answering calls to police, firefighting, ambulance and other appropriate services.

5.2 Citizen-to-Authority Emergency Services in the legacy PSTN environment.

A uniform system for Citizen-to-Authority emergency calls for the public switched telephone network (PSTN) for the USA started in the late 1960s in what was largely a single vendor environment for an entirely wireline network. It was based on a uniform number for accessing Emergency Services (i.e. 911 for North America) and informing the PSAP of the calling number (ANI, Automatic Number Identification). Location information was obtained by doing a reverse directory look-up of the calling phone number in the customer database owned by the local phone company. In general, at that time there was a fairly good match between the service area of a PSAP and each area of administration of the phone company. Similar systems were developed in many other countries.

The underlying design assumptions of the legacy system described above deteriorated badly over time, influenced by:

- Deregulation and breakup of telephone provider exclusive franchises
- The introduction and widespread deployment of cellular telephones
- The conversion of voice services from circuit switched to packet switched technology
- The rise of VoIP (Voice over Internet Protocol)
- The migration of voice from single purpose dedicated devices (i.e. telephones) to software based devices (e.g. PCs, laptops, smart-phones)
- The desire to add non-voice communications to the ES calling system (e.g. text and images)
- Broad area centralization/consolidation of PSAP service areas.

Deregulation and the rise of cellular telephony migrated from an environment of a single communications vendor environment with fixed customer locations to an environment that encompasses multiple vendors, a high percentage of mobile users and no correlation between phone number and location.

One core challenge of this transition was moving the source of and the responsibility for location information from a single database in the core of the PSTN to distributed information residing somewhere in the network close to the calling device. This major architectural change involves an addition to the capabilities of new networks, capabilities that are not inherent to their architecture and involves the addition of significant additional hardware and software.

5.3 Citizen-to-Authority Emergency Services in an 802/IP environment

In a multi-vendor packet switched (e.g. IEEE 802) environment there is no centralized registration of the location of the Physical Layer (L1) address nor are there any restrictions against the devices associated with L1 addresses being moved arbitrarily. While cellular networks tend to have a fairly high degree of vertical integration, that is not the general case for IEEE 802 and IP networks. For example, while the lowest level IP device in the core network may be well-known and located, there may be an attached pure L1/L2 802 network that is (at least partially) ad hoc in its configuration, heterogeneous in its nature and physically large (multiple kilometers) in diameter. Such a network may have multiple owners with equipment from many vendors. It is therefore essential that standards be in place to convey location information to the EUT as well as to support of any communication path tracing functions. Additionally, there may well be regulatory requirements to support unauthorized access to the L1/L2 network in an emergency call scenario. This standard supports an optional capability in support of this, should it be required.

5.3.1 End User Terminal (EUT) upper layers in an emergency call situation

The specific details of the EUT upper layers in an emergency call situation are beyond the scope of this standard.

5.3.1.1 EUT upper layer location function

It is the responsibility of the EUT upper layers to provide location information when initiating an emergency call (Ref: ECRIT [Editor's note: specify to a finer level, i.e. RFC, chapter and verse]). The source (e.g., GPS location information or via Layer 2 from the next node on the IEEE 802 network) the EUT upper layers choose as the source of the location information to satisfy this requirement is outside the scope of this standard. It is a conformance requirement of this standard for the attached network device to make relevant location information available to the EUT.

5.3.1.2 upper layer EUT unauthorized access function

An EUT that does not have a service relationship with the network provider may request authorization for limited use via the network’s authorization mechanism. The responsibility for limiting such use to ES is a policy decision of the 802 network operator(s). Such a policy may be accomplished by restricting the access to a L2 VLAN that is dedicated and restricted to ES use or it may be accomplished by upper layer policy restrictions that only grant limited use to the MAC address associated with the EUT.

5.3.2 EUT L1/L2 in an emergency call situation

In order for a EUT to retrieve location information from the IEEE 802 network per this standard, the EUT must support a Layer 2 protocol for this transfer. Details for each transfer mechanism are detailed below.

5.3.2.1 Location information transfer from IEEE 802.1 based devices.

IEEE Std 802.1AB specifies a generalized Layer 2 single hop protocol known as LLDP (Link Layer Discovery Protocol) that is suitable for conveying location information. Currently there does not exist a definition for the Location MIB (Management Information Base) or definitions for the TLVs needed to convey the specific location information.

LLDP is a powerful generalized protocol for this sort of information and is designed to operate in a manner that is independent of the particular access method used. It is to be used for EUTs attaching to the network via a link based on IEEE Std 802.3. Other IEEE 802 access methods should also use LLDP.

5.3.2.2 Location information transfer from IEEE 802.11 based devices.

IEEE Std 802.11-2007 Amendment 9 (802.11u) [Editor's note: Std 802.11REV is currently in Sponsor Ballot. This revision includes the roll-up of 802.11 amendments k, r, y, w, n, p, z, v, and u] has a separate protocol to provide location information to a EUT from an IEEE 802.11 access point in a pre-associated state within the 802.11 generic advertisement service (GAS) known as ANQP (Access Network Query Protocol) to provide hotspot and network information to a STA in a pre-associated state supports determining and conveying location information as either a Geospatial Location element or a Civic Location element.

5.3.2.3 Location information transfer from IEEE 802.15 based devices.
It is believed that the nature of currently standardized IEEE 802.15 WPAN products is such that they provide links to peripheral devices from an EUT rather than attachment of an EUT to an IP connected L2 network. Therefore, there is no special need for differentiated ES services on WPAN links. If such a need emerges for future IEEE 802.15 based products then LLDP should be used.

5.3.2.4 Location information transfer from IEEE 802.16 based devices.
IEEE Std 802.16 has support for both measuring and conveying location information within its Location Based Services (LBS) function.

5.3.3 IEEE 802 Backhaul infrastructure in an emergency call situation.
Each IEEE 802 network relay device (IEEE 802.3 Repeaters and IEEE 802.1 MAC Relay devices excepted) should carry standardized location information locally in their management information base (MIB) and support the IEEE 802.1 Linktrace protocol. A Location Server (LS)connected to the IEEE 802 Layer 2 network should thus be able to compute and maintain a network map of the IEEE 802 Layer 2 network. With the network map and the location information retrieved (SNMP presumed) from the MIB of each node, the location server is equipped to respond to queries as to the best estimate (i.e. nearest network node with a location MIB) of the calling location of any EUT that has not provided location information or has not provided credible location information. This facility provides the means for a successive de-approximation of the calling location. The LS mapping and trace services are accessible to the PSAP via upper layer services and protocols. Specification of those services and protocols is outside the scope of this standard.

5.3.4 IEEE 802 Backhaul interfaces to Layer 3 Services and gateway to the Internet.
It is the responsibility of the Layer 3 devices that provide upper layer network services and traffic gateway functions to enforce whatever service restrictions are placed on EUTs that have attached to the IEEE 802 network for emergency only service.

6 Detailed Specification

6.1 Location

This location requirement is specified in NENA i3 (858 et seq). Location in NG9-1-1 is represented by validated content in the PIDF-LO2 (RFC4119, updated by RFC5139 and RFC5491) with field use for the United States as documented in the NENA Civic Location Exchange Format [111]. Fields in the PIDF-LO must be used as defined; no local variation is permitted. A service (PIDFLOtoMSAG) is provided in this document for translating PIDF-LO to a NENA standard MSAG representation for backwards compatibility. All geodetic data in i3 uses WGS84 as the datum.

6.2 Unauthorized Access

For those instances where it is required to provide a restricted service path across an IEEE 802 L1/L2 network to provide L1/L2 access for a user that does not have authorized access to the L1/L2 network, this standard provides such a path. This path is designated as an ES VLAN. Its purpose is to provide a virtual LAN whose traffic may be limited to that which is required for ES. The ES VLAN may be functionally identical or may even be shared with other restricted access usage such as that by a user when seeking authorization for normal usage (i.e. Logon)

The ES VLAN provides connectivity between an unauthorized EUT and the Layer 3 services connected to the IEEE 802 network. Each Layer 3 device providing service is responsible for the enforcement of the the policies necessary to limit service to only ES. In the simplest conceptual model, a core services gateway port is the equivalent to an RJ-45 on that device that is the plug-in point for an emergency "red-phone". The ES VLAN acts as an "virtual extension cord" the the far edge of the network for that restricted port.

Mechanisms other than an ES VLAN or other L1/L2 restrictions may be used by upper layer services to limit access by unauthorized users.

For this standard, the designation of a particular VLAN for ES is a matter of network administration. Whether it is appropriate to make the provision of a specific VLAN, whether within the existing VLAN standards or by definition of a new standard for a dedicated ES VLAN is a matter for further study (ffs).

6.3 Priority Recommendations

Not all IEEE 802 access methods support priorities. Where priorities are supported, it is recommended that ES be allocated the highest priority beneath Network Management.

7. Security Issues

This specification assumes that ES VoIP communications have the same level of security protection as afforded to normal VOIP calls and that security is sufficient to meet ES requirements.

Location Management objects defined in the MIB module or in other data structures may be considered sensitive or vulnerable in some network environments. Appropriate network management security measures should be taken. Such measures should encompass the LS.

Informative Annex Information to be supplied at a later date.