SCTE | STANDARDS

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 173-2 2017 (R2021)

Framework for Implementing Preferential Telecommunications in IPCablecom and IPCablecom2 Networks

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interoperability, interchangeability, best practices, and the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

NOTE: The user's attention is called to the possibility that compliance with this document may require the use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at https://scte.org.

140 Philips Road
Exton, PA 19341

Document Types and Tags

Document Type: Specification

Document Tags:

☐ Test or Measurement	☐ Checklist	☐ Facility
X Architecture or Framework	☐ Metric	X Access Network
☐ Procedure, Process or Method	☐ Cloud	☐ Customer Premises

Document Release History

Release	Date
SCTE 173-2 2010	*12/20/2010*
SCTE 173-2 2017	*2/27/2017*

Note: This document is a reaffirmation of SCTE 173-2 2017. No substantive changes have been made to this document. Information components may have been updated such as the title page, NOTICE text, headers, and footers.

SUMMARY

NOTE: This document is identical to SCTE 173-2 2010 except for informative components which may have been updated such as the title page, NOTICE text, headers and footers. No normative changes have been made to this document.

This standard provides a framework for implementing preferential capabilities in IPCablecom and IPCablecom2 networks. The approach of this standard is to define a framework for capabilities that can be utilized to meet the requirements in ANSI/SCTE 173-1 2010 and forms the basis for detailed IPCablecom and IPCablecom2 standards in support of preferential telecommunications.

INTRODUCTION

Emergency/disaster telecommunications for authorized users plays a vital role in the health, safety and welfare of people in all countries. The common thread to facilitate emergency/disaster operations is the utility of assured capabilities for user-friendly preferential telecommunication services that may be realized by technical solutions and/or administrative policy. The capabilities of IPCablecom and IPCablecom2 cable infrastructures offer an important resource for assured preferential telecommunication services.

The essential aspects of preferential telecommunication over cable networks that this framework standard addresses are grouped into two prime areas: authentication and priority. These two areas are the vital network features needed to obtain the resources of cable networks when preferential treatment is required. Other areas such as policy, traffic engineering, alternate routing, provisioning for restorability, etc., are either out of scope or not addressed in this version.

The evolving nature of telecommunication networks in general, and of cable networks in particular, lends itself to a phased approach for the support of preferential treatment. A phased approach needs to consider the evolution of IPCablecom standards: the initial suite of IPCablecom standards, the IPCablecom standards as revised in 2005, and the IPCablecom2 suite of standards.

TABLE OF CONTENTS

		Page
1	Scope	1
2	References	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined here	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Common framework for priority	3
7	Common framework for authentication	5
	7.1 User credentials-based authentication	5
	7.2 Equipment-based authentication	5
	7.3 Basic authentication mechanisms	5
	7.4 Credentials management mechanisms	6
8	Authentication and priority in IPCablecom networks	7
	8.1 Authentication in IPCablecom networks	7
	8.2 Priority in IPCablecom networks	7
9	Authentication and priority in IPCablecom2 networks	7
	9.1 Authentication in IPCablecom2 networks	7
	9.2 Priority in IPCablecom2 networks	8
Bibliography		10

Framework for implementing Preferential Telecommunications in IPCablecom and IPCablecom2 Networks

1.0 Scope

The objective of this Standard is to provide a framework for the implementation of preferential telecommunications services within cable networks as described in [ANSI/SCTE 24-1] and [ITU-T J.360]. This framework is one of the series of Standards addressing these services.

The key aspects of preferential telecommunications services addressed in this framework are priority and authentication. The architectural differences in the two key aspects are addressed in terms of the logical functional entities defined in [ANSI/SCTE 24-1] and [ITU-T J.360], respectively.

Although this version of the framework addresses the two key aspects, namely, priority and authentication, necessary to support preferential treatment in telecommunications services, other aspects such as policy, traffic engineering, alternate routing, provisioning, etc., are either out of scope or left for future study. As an example, future versions are expected to address provisioning of preferential services for specific users and/or devices (media terminal adapters) at specific locations.

2.0 Normative References

The following ITU-T Recommendations and other 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 Recommendations and other references are subject to revision; users of this Standard are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Standard does not give it, as a stand-alone document, the status of a Recommendation.

[ANSI/SCTE 24-1]	*Architectural framework for the delivery of time-critical services over cable television networks using cable modems*
[ANSI/SCTE 24-4]	*Dynamic quality of service for the provision of real-time services over cable television networks using cable modems*
[ANSI/SCTE 24-10]	*IPCablecom security specification*
[ANSI/SCTE 159-1]	*IPCablecom Multimedia Part 1: Multimedia Applications and Service*
[ANSI/SCTE 173-1]	*Requirements for preferential telecommunications over IPCablecom networks*
[ITU-T J.360]	Recommendation ITU-T J.360 (2006), *IPCablecom2 architecture framework*
[ITU-T J.368]	Recommendation ITU-T J.368 (2008), *IPCablecom2 quality of service specification*
[IETF RFC 3261]	IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*
[IETF RFC 4412]	IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP)*

3.0 Terms and Definitions

3.1 Terms defined elsewhere

This standard uses the following terms defined elsewhere:

3.1.1 assured capabilities [ANSI/SCTE 173-1]: Capabilities providing high confidence or certainty that critical telecommunications are available and perform reliably.

3.1.2 authentication [ANSI/SCTE 173-1]: The act or method used to verify a claimed identity.

3.1.3 authorization [ANSI/SCTE 173-1]: The act of determining if a particular privilege, such as access to telecommunications resources, can be granted to the presenter of a particular credential.

3.1.4 cable modem [ANSI/SCTE 24-1]: A cable modem is a layer two termination device that terminates the customer end of the DOCSIS connection.

3.1.5 emergency situation [ANSI/SCTE 173-1]: A situation, of serious nature, that develops suddenly and unexpectedly. Extensive immediate important efforts, facilitated by telecommunications, may be required to restore a state of normality to avoid further risk to people or property. If this situation escalates, it may become a crisis and/or disaster.

3.1.6 international emergency situation [ANSI/SCTE 173-1]: An emergency situation, across international boundaries, that affects more than one country.

3.1.7 IPCablecom [ANSI/SCTE 24-1]: An ITU-T project that includes an architecture and a series of Recommendations that enable the delivery of real-time services over the cable television networks using cable modems.

3.1.8 label [ANSI/SCTE 173-1]: An identifier occurring within or attached to data elements. In the context of preferential telecommunications it is an indication of priority. This identifier can be used as a mapping mechanism between different network priority levels.

3.1.9 managed IP network [ANSI/SCTE 24-1]: An IP network, managed by a single entity for the purpose of transporting IPCablecom signalling and media packets.

3.1.10 preferential [ITU-T J.260]: A capability offering advantage over regular capabilities.

3.1.11 priority treatment capabilities [ANSI/SCTE 173-1]: Capabilities that provide premium access to, and/or use of telecommunications network resources.

3.1.12 subscriber [ITU-T J.360]: An entity (comprising one or more users) that is engaged in a subscription with a service provider.

3.1.13 user agent (UA) [ITU-T J.360]: A SIP user agent as defined by [IETF RFC 3261].

3.2 Terms defined in this Standard

This Standard defines the following term:

3.2.1 user equipment: Any device used directly by an end user to communicate.

4 Abbreviations and Acronyms

This Standard uses the following abbreviations and acronyms:

AKA Authentication and Key Agreement

ATM Automatic Teller Machine

AVP Attribute Value Pair

CM Cable Modem

CMS Call Management Server

CMTS	Cable Modem Termination System
DQoS	Dynamic Quality of Service
E-DVA	Embedded Digital Voice Adapter
E-MTA	Embedded Media Terminal Adapter
IPSec	Internet Protocol Security
KDC	Key Distribution Centre
MGC	Media Gateway Controller
MTA	Media Terminal Adapter
P-CSCF	Proxy Call Session Control Function
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKINIT	Public Key Cryptography for Initial Authentication
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
UE	User Equipment

5 Conventions

None.

6 Common framework for priority

[ANSI/SCTE 173-1] lists a number of requirements to assure priority treatment in IPCablecom and IPCablecom2 networks. Even though architectural differences exist between IPCablecom described in [ANSI/SCTE 24-1] and IPCablecom2 in [ITU-T J.360], this clause discusses the framework that is applicable for both networks. There are three aspects to consider when addressing priority treatment for preferential telecommunications services. These are classification or labelling of the session or call as requiring priority treatment, signalling for priority and the mechanisms to support the requested priority. The selection of mechanisms and policies, along with their respective implementations, are outside the scope of this Standard.

Table 1 categorizes the requirements according to these three aspects: classification, signalling and mechanisms. Some of the requirements are categorized to have more than one aspect because the priority classification of the call is to be maintained and the actual mechanisms to preserve the classification may vary.

Table 1 – Mapping requirements to priority aspects

[ANSI/SCTE 173-1] requirement	Category
Priority access to the IPCablecom and IPCablecom2 networks (1a)	Classification
Call activation and call features (1b)	Signalling
Allocating network resources (1c)	Mechanisms
Priority given to labelled calls at gateways (1d)	Signalling and mechanisms
Assigning labels at call origination (2)	Classification
Priority given to labelled calls within IPCablecom and IPCablecom2 networks (3)	Mechanisms
Map the labels used from/to the cable network to/from the connecting network gateway device (4 and 5)	Mechanisms
Preserve the priority label across the cable network (6)	Signalling and mechanisms
Priority call in transit through cable network is treated according to cable network capabilities (7)	Classification and mechanisms
Number of levels for priority: minimum 1 and additional levels based on national options (8)	Classification
Priority treatment given by cable network to calls with priority label from a trusted network (9)	Mechanisms

Prioritization means obtaining a higher probability for completing a call/session. In other words, once the traffic is identified to be for a preferential telecommunications service, the policies need to provide a higher probability of success relative to call admission, routing and delivery of traffic. This capability should exist on the access link and should also be propagated throughout all relevant network entities such as call management servers (CMSs) and media gateway controllers (MGCs) or the entities in the session initiation protocol (SIP) infrastructure.

Even though priority enabling mechanisms and assignment of QoS are not the same, in IPCablecom, DQoS session classes can be used to assign priority treatment to a session. One of the requirements to allocate resources that can be supported in IPCablecom networks is the concept of multimedia gates described in [ANSI/SCTE 24-4] and [ANSI/SCTE 159-1]. [ANSI/SCTE 24-4] is specific to IPCablecom and is addressed below. The gates are used to control access by an IP flow to enhanced QoS from the DOCSIS network. Gates are installed in the cable modem termination system (CMTS) to allow the creation of service flows with a guaranteed QoS by reserving the required resources. Admission control at the CMTS is used to ensure available resources are greater than committed and reserved resources. In the case of IPCablecom using [ANSI/SCTE 24-4], a client such as embedded media terminal adapter (E-MTA) initiates resource reservation and activation, whereas [ANSI/SCTE 159-1] supporting multimedia allows a proxy to perform these steps on behalf of the endpoint client.

Priority signalling is addressed separately for IPCablecom and IPCablecom2 because of the differences in approaches used by an E-MTA or UE to connect to the access network.

IPCablecom and IPcablecom2 use real-time transport protocol (RTP) as media transport protocol for audio and video packets. As discussed in [b-IETF RFC 4190], RTP does not include markings to indicate the priority of the packet with a label. Different methods are discussed which include defining a new per-hop behaviour for preferential traffic, new shim layer protocol over IP or marking an application layer packet.

7 Common framework for authentication

Authentication in IPCablecom and IPCablecom2 networks requires the provision of credentials, in some form, that are used by the system to verify the integrity of an identifier presented by an intended system user. The management of these credentials has considerable importance when considering the type of authentication mechanism(s) used in any cable network. One needs also to consider existing deployed authentication mechanisms (e.g., for subscribers), as well as the acceptability and usability of any existing deployed authentication mechanisms in use for preferential telecommunications in other networks. The two forms of authentication available are:

- user credentials-based where the preferential user has to enter or provide information to the device (e.g., E-MTA); and
- equipment-based where authentication is based upon the recognition of the preferential user's equipment by the cable network system.

7.1 User credentials-based authentication

User credentials-based authentication relies on functionality built into the device or the network that accepts input of some form by which the preferential user can authenticate their identifier. The device interacts with an authentication server within the infrastructure to validate the identifier to enable the preferential service. User credentials-based authentication can be accomplished by the user by calling a special number and entering a personal identification number (PIN). This method allows any IPCablecom and IPCablecom2 user equipment with a standard 12-button numeric key pad to be used. The PIN method is useful because of simplicity and backward compatibility with preferential service capabilities in deployed networks.

7.2 Equipment-based authentication

Equipment-based authentication is based upon the recognition of the preferential telecommunications user's equipment by the IPCablecom or IPCablecom2 system. This method uses the equipment identity (e.g., a device's digital certificate) as all or part of the preferential telecommunications user's identification. This authentication will only be available on particular pieces of equipment (e.g., telephones, E-MTAs) and may additionally require further mechanisms (e.g., smartcards, tokens, and/or a PIN) beyond basic physical security of the equipment.

7.3 Basic authentication mechanisms

Although PIN mechanisms are the simplest and most accessible methods possible in current IPCablecom networks, more secure methods may be needed in the future for some applications. These methods are discussed in this clause.

Authentication can be accomplished by the user by calling a special number and entering a PIN. This method allows any IPCablecom user equipment with a standard 12-button numeric key pad to be used. The PIN method is useful because of simplicity and backward compatibility with preferential service capabilities in deployed networks. However, relying on a PIN means to rely on a single factor (something the individual knows), rather than a combination of factors (such as "something the individual possesses" or "something unique to the individual"). With the increased dependence on packet-based communications, the generally accepted baseline is to use two factors, such as:

- Knowledge of a PIN in conjunction with possession of a magnetic stripe card (e.g., as used for bank ATM access).
- Knowledge of a password in conjunction with possession of a time-constrained token device (e.g., as used for banking and financial on-line activities).

However, most of these alternative methods are usable only if the device has input/output capabilities beyond the standard 12-button numeric key pad.

There are few authentication mechanisms (or combinations of mechanisms) possible for use in cable networks other than PIN functionalities, e.g., pass-phrases could be used as an alternative (assuming voice recognition capabilities that achieve sufficiently low 'false positive' and 'false negative' rates). While numerous other authentication mechanisms exist (e.g. passwords, smartcards, biometric readers, etc.), given the cable network architectures, these are not easily supported (e.g., E-MTAs do not have smartcard readers).

For multimedia services that require QoS, IPCablecom defines interfaces where RADIUS- and Diameter-based authentication is used: RADIUS between call management server and record-keeping system and diameter between P-CSCF and charging data function. The following are possible mechanisms not defined in IPCablecom Standards that could be considered to authenticate the user of the preferential treatment services:

- passwords coupled with a RADIUS-based authentication infrastructure;
- passwords coupled with a Diameter-based authentication infrastructure;
- passwords coupled with a key distribution centre (KDC) such as Kerberos;
- pass-phrases coupled with smartcard; and
- pass-phrases coupled with smartcard and public key infrastructure (PKI).

Each of these types of mechanism differs as to the degree of assurance each provides that an asserted identity is valid and being presented by a valid system user. These mechanisms also differ in their magnitude of deployment, operational capabilities and complexity. The above-listed methods are to be further considered in terms of their relative authentication capabilities, degree of scalability, performance, cross-domain interoperability and interoperability with legacy/existing authentication mechanisms.

For authenticating preferential treatment of certain calls/sessions in IPCablecom networks, the level of security must be high. However, the ease with which a user obtains authentication must be high as well because, in some cases, the user will be in an emergency situation. Therefore, a combination of mechanisms that will both provide ease of use and a high level of security should be chosen whenever possible.

7.4 Credentials management mechanisms

Management of credentials is important to ensure that the system is using up-to-date and accurate credentials for user authentication. Management of credentials usually entails the following: credential updates, credential revocation, and the exchange of credentials across service provider domains.

Management of credentials is dependent on the credential itself, such as password databases, RADIUS/Diameter servers, KDC servers, smartcards and PKI root, etc. Each of these types of mechanism differs with respect to the degree of data integrity and confidentiality protection provided to the credentials. These mechanisms also differ in the magnitude of deployment, operational capabilities and complexity.

8 Authentication and priority in IPCablecom networks

8.1 Authentication in IPCablecom networks

[ANSI/SCTE 24-1] and [ANSI/SCTE 24-10] describe the mechanisms used to authenticate the client requesting the service. The protocol used to authenticate the client is Kerberos with public key cryptography for initial authentication (PKINIT) extension. Kerberized Internet protocol Security (IPSec) is used to create a secure association between the CMS and the MTA (client). Three phases are described. In the first phase, the client interacts with the key distribution centre (KDC) by providing its device certificate to obtain a ticket granting ticket (TGT) to obtain a ticket from the KDC for a specific server such as the CMS. A client may bypass the first phase and provide the KDC with its device certificate to directly obtain a ticket for a specific server. In the third phase, a pair of security parameters is established with the application server for sending and receiving secure data over IPSec.

8.2 Priority in IPCablecom networks

Preferential users will receive priority treatment. This priority treatment is supported using the method defined in [ANSI/SCTE 24-4].

In IPCablecom, resource reservation is performed using two components. The first is at the data link layer and involves making DOCSIS service flows more promptly available for gates of a certain session class. The second is at the session layer and involves describing the priority status of a call so that the information can be propagated to all relevant entities in the network.

On the cable access link, prioritization can be enabled by first associating dynamic quality of service (DQoS) gates with a particular session class reserved specifically for this purpose and then, as a result, requiring the CMTS to take a specific action. Depending on the value of the session class, different admission control is applied to the resulting resource request. For instance, a session class for normal voice communications and an overlapping session class for preferential telecommunications calls could be defined to allow the allocation of up to, respectively, 50% and 70% of the total upstream resources, and leaving the remaining 30-50% of the total upstream bandwidth available to other, possibly lower priority, services.

[b-ITU-T J.162] describes network-based call signalling used in IPCablecom between the E-MTA and call agent for creating and deleting connections. While the call agent provides the GateID to the MTA during call establishment, a mechanism not currently available to communicate the desired DOCSIS traffic priority to the MTA should be used for the session. The DOCSIS traffic priority is used by the CMTS to prioritize traffic during periods of congestion. Further study is needed in this area in the context of preferential telecommunications.

9 Authentication and priority in IPCablecom2 networks

9.1 Authentication in IPCablecom2 networks

IPCablecom2 supports both embedded and standalone UEs. The UEs are software based and may have the capabilities to connect to a secure hardware store such as a smartcard. Authentication mechanisms available on IPCablecom2 networks are expected to be more versatile and the achievement of adequate authentication on IPCablecom2 networks will be readily available.

Appendix III of [ITU-T J.360], describes three authentication mechanisms supported by the IPCablecom2 architecture: IMS authentication and key agreement (AKA), SIP digest authentication and certificate-based authentication. Depending on the mechanism used for authentication, requirements are specified for the various components of the IPCablecom2 networks. As an example, to support digest authentication, it is necessary to store securely user names and passwords.

The signalling between the UE and the P-CSCF is secured by using either IPSec or TLS. [ITU-T J.360] requires an UE to support negotiating the use of TLS. Two models are defined for securing over TLS: mutually authenticated whereby both the UE and the server (P-CSCF for example) validate each other's certificate and server-side authentication where only the server side provides a certificate to establish signalling security. The former offers a higher level of security; IPCablecom2 requires the support of server-side authentication. It may be desirable to consider mutual authentication for UEs that are used to originate preferential treatment services.

An IPcablecom2 network requires that the identity assertion of the subscriber is performed by P-CSCF to convey the authenticity of the user to the other network elements in a trusted network and to remove the identity when communicating with network elements in non-trusted networks. The identity assertion and removal ensures that preferential telecommunications services are originated by an authorized user.

[b-ANSI/SCTE xx] defines the requirements.

9.2 Priority in IPCablecom2 networks

The IPCablecom2 architecture, as described in [ITU-T J.360], is based on the 3GPP IMS infrastructure. Priority occurs in three places: the IMS signalling, the enabling mechanism and using packet labelling.

9.2.1 Priority signalling

At the IMS signalling level, new Resource-Priority (R-P) and Accept-Resource-Priority SIP headers defined in [IETF RFC 4412] are used. The addition of these headers in request and response messages, respectively, allows the SIP proxies and UAs to give priority treatment to requests.

[IETF RFC 4412] defines new headers, referred to as Resource-Priority (R-P) in SIP request messages to request prioritized access to resources. Accept-Resource-Priority is included in the response indicating the R-P values that a SIP user agent is willing to support. The R-P values are registered with IANA and the header is an optional field. Five name spaces are registered by IANA and included in the RFC. This Standard does not propose a specific name space to be used, and additional name spaces as required for preferential telecommunications services may be registered following the procedures defined in [IETF RFC 4412]. The use of R-P headers supports priority signalling.

It should be noted that these headers do not directly influence the forwarding behaviour of IP routers. Such functionality, that is, at the network layer or layer 3, is under study. [b-IETF RFC 3690] defines general system requirements for supporting preferential services in the general area of IP telephony as an end-to-end service. It is useful to consider these requirements in the context of IPCablecom2 to support preferential treatment.

9.2.2 Enabling mechanism

At the access network level, the Reservation-Priority attribute value pair (AVP) can be used to indicate priority in requesting access network resources. In order to define the GateSpec for reservation of resources, the P-CSCF interacts with the IPCablecom2 application manager using the Rx interface defined in 3GPP IMS. This interface uses the Diameter protocol with a number of new AVPs defined in [ITU-T J.368] QoS specification.

The GateSpec messages used to request and activate access network resources include a session class ID that defines the priority level of the request. While the call agent provides the GateID to the embedded digital voice adapter (E-DVA) during call establishment, a mechanism not currently available to communicate the desired DOCSIS traffic priority, the E-DVA should be used for the session. The DOCSIS traffic priority is used by the CMTS to prioritize traffic during periods of congestion. Further study is needed in this area.

Within the DOCSIS access network, a traffic priority can be assigned to give priority treatment within the various service flow types.

The definition of specific values to be used to specify priority levels for preferential telecommunications services is outside the scope of this Standard.

Mechanisms exist to support priority routing in the core network of IP packets, including the SIP signalling and the RTP bearer packets, but their definitions are not covered in this Standard.

9.2.3 Labelling

Currently, RTP does not support priority labelling, which is the media transfer protocol used in IPCablecom2.

[b-ANSI/SCTE 173-4] defines the detailed requirements.

Bibliography

[b-ITU-T E.106] Recommendation ITU-T E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*

[b-ITU-T J.162] Recommendation ITU-T J.162 (2007), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*

[b-ANSI/SCTE 173-3] *Specifications for authentication in preferential telecommunications over IPCablecom2 networks*

[b-ANSI/SCTE 173-4] *Specification for priority in preferential telecommunications over IPCablecom2 networks*

[b-ITU-T Q-Sup.57] ITU-T Q-series Recommendation Supplement 57 (2008), *Signalling requirements to support the emergency telecommunications service (ETS) in IP networks*

[b-ITU-T Y.1271] Recommendation ITU-T Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packet-switched networks*

[b-ITU-T Y.2205] Recommendation ITU-T Y.2205 (2008), *Next Generation Networks – Emergency telecommunications – Technical considerations*

[b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*

[b-IETF RFC 3689] IETF RFC 3689 (2004), *General Requirements for Emergency Telecommunication Service (ETS)*

[b-IETF RFC 3690] IETF RFC 3690 (2004), *IP Telephony Requirements for Emergency Telecommunication Service (ETS)*

[b-IETF RFC 4190] IETF RFC 4190 (2005), Framework for Supporting Emergency Telecommunication Services (ETS) in IP Telephony

