Forward Link Only Transport Specification

ARIB STANDARD

ARIB STD-B48 Version 1.1

Version 1.0 November 5, 2010
Version 1.1 July 3, 2012

Association of Radio Industries and Businesses

Foreword

1. Introduction

With participation of radio equipment manufacturers, telecommunications operators, broadcasting equipment manufacturers, broadcasters and general users, Association of Radio Industries and Businesses (ARIB) defines basic technical requirements for standard specifications of radio equipment, etc. as an "ARIB STANDARD" in the field of various radio systems.

In conjunction with national technical standards which are intended for effective spectrum utilization and avoidance of interference with other spectrum users, an ARIB STANDARD is intended as a standard for use by a private sector compiling various voluntary standards regarding the adequate quality of radio and broadcasting service, compatibility issues, etc., and aims to enhance conveniences for radio equipment manufacturers, telecommunications operators, broadcasting equipment manufacturers, broadcasters and general users.

An ARIB STANDARD herein is published as "Forward Link Only Transport Specification." In order to ensure fairness and transparency in the defining stage, the standard was set by consensus of the standard council with participation of interested parties including radio equipment manufacturers, telecommunications operators, broadcasting equipment manufacturers, broadcasters, general users, etc. with impartiality.

It is our sincere hope that the standard would be widely used by radio equipment manufacturers, telecommunications operators, broadcasting equipment manufacturers, broadcasters, general users, etc.

2. Scope

This standard applies to the multimedia broadcasting defined in Section 2 of Chapter 4, Ordinance No.87 of the Ministry of Internal Affairs and Communications, 2011.

3. Standard References for Forward Link Only

The following list identifies the current version of the standards in the FLO family of standards.

Standard#	Title
STD-B47	Forward Link Only Air Interface Specification for Terrestrial Mobile Multimedia Multicast
STD-B48	Forward Link Only Transport Specification
STD-B49	Forward Link Only Media Adaptation Layer Specification
STD-B50	Forward Link Only Open Conditional Access (OpenCA) Specification
STD-B51	Forward Link Only System Information Specification
STD-B52	Forward Link Only Messaging Transport Specification
STD-B32	Video Coding, Audio Coding and Multiplexing Specifications for Digital Broadcasting*

*NOTE: The original document of this standard is Japanese version. Part 3 of this standard is not applicable to Forward Link Only system.

4. Industrial Property Rights

This standard does not describe industrial property rights mandatory to this standard. However, the right proprietor of the industrial property rights has expressed that "Industrial property rights related to this standard, listed in the annexed table below, are possessed by the applicator shown in the list. However, execution of the right listed in the annexed table below is permitted indiscriminately, without exclusion, under appropriate condition, to the user of this standard. In the case when the user of this standard possesses the mandatory industrial property rights for all or part of the contents specified in this standard, and when he asserts his rights, it is not applied."

Annexed Table (Selection of Option 2)

Patent Applicant/Holder	Name of Patent	Registration No./ Application No.	Remarks
QUALCOMM Incorporated (*1)	A comprehensive confirmation form has been submitted with regard to ARIB STD-B48 Ver.1.0.		
JVC KENWOOD Holdings, Inc. (*1)	A comprehensive confirmation form has been submitted with regard to ARIB STD-B48 Ver.1.0.		

(*1) These patents are applied to the part defined by ARIB STD-B48 Ver. 1.0. (Received on October 28, 2010)

Table of Contents

FOREWORD

(This foreword is not part of this Standard.)

This draft Standard is intended for use in TM3 networks using ARIB STD-B47 [4]. This draft Standard makes use of certain standards and recommendations defined by TIA and other bodies as listed in subclause 2.5.

1 INTRODUCTION AND SCOPE

This Standard specifies the Transport Layer for TM3 systems using ARIB STD-B47 [4]. The Standard specifies the framing formats and procedures for delivering application service packets securely over the air interface specified in ARIB STD-B47.

This Standard is organized into the following clauses:

Clause 1: An informative clause describing the scope and the organization of the Standard.

Clause 2: A normative clause defining compliance terminology, acronyms, definitions of terms, conventions for specifying data types, and references.

Clause 3: An informative clause providing an overview of the services provided by the Transport Layer, the reference model assumed by the Transport Layer, and an overview of the protocol hierarchy specified in this Standard.

Clause 4: A normative clause defining the encryption procedures optionally associated with Streams specified in ARIB STD-B47 .

Clause 5: A normative clause defining the framing and CRC procedures for transport of application service packets over Streams in Multicast Logical Channels specified in ARIB STD-B47.

Clause 6: A normative clause defining the transport and message structures of control messages transported in Stream 0 of Multicast Logical Channels.

2 APPARATUS

2.1 Compliance Terminology

The key words “shall”, “shall not”, “should”, “should not”, “may”, “need not”, “can” and “cannot”, when used in this Standard, are to be interpreted as specified in Annex C of the TIA Style Manual [3].

2.2 Symbols and Abbreviations

The following symbols and abbreviations are used in this Standard:

AES: Advanced Encryption Standard

ANSI: American National Standard Institute

CAS: Conditional Access System

CRC: Cyclic Redundancy Check

CTR: CounTeR

ECM: Entitlement Control Message

FASB: Fragmentation Across Superframe Boundaries

FH: Fragment Header

FIPS: Federal Information Processing Standard

LSB: Least Significant Bit

MAC: Media Access Control

MLC: Multicast Logical Channel

MSB: Most Significant Bit

TIA: Telecommunications Industry Association

TM3: Terrestrial Mobile Multicast Multimedia

UINT: Unsigned INTeger

2.3 Message Description Rules

The formats of messages transported in Stream 0 are specified as binary structures. The conventions for specifying binary structures are specified in subclause 2.3.1.

2.3.1 Binary Message Specifications

This subclause specifies the atomic data types used in this Standard and describes the general message guidelines and ordering rules.

2.3.1.1 Message Specification Tables

A message is an ordered collection of fields. Messages are specified in tables. An example is shown in Table 1.

Table 1: Example Message Specification

Field Name	Field Type	Field Presence	Subclause Reference
FIELD_A	UINT(8)	MANDATORY	[Field A subclause]
FIELD_B	BIT(1)	MANDATORY	[Field B subclause]
FIELD_C	FIELD_C_TYPE	CONDITIONAL	[Field C subclause]

In the above example, the message has three fields, FIELD_A, FIELD_B and FIELD_C. The second column in the table defines the type of the field. For example, FIELD_A is an unsigned 8-bit integer (UINT(8)) and FIELD_B is a bit field of size 1 bit. UINT(8) and BIT(N) are basic types. The list of basic types is defined in subclause 2.3.1.3.

FIELD_C is of type FIELD_C_TYPE. FIELD_C_TYPE is a composite data type which is defined elsewhere by a similar table specifying its sub-fields.

The third column of the table specifies the rules for the presence of a field. Fields can be MANDATORY, CONDITIONAL or OPTIONAL.

The fourth column of the table identifies the subclause of this Standard where the field is specified.

2.3.1.2 Field Presence Classes

The possible Field Presence classes are specified in the following subclauses.

2.3.1.2.1 MANDATORY field

A MANDATORY field shall occur in every instance of the message.

2.3.1.2.2 CONDITIONAL field

The presence of a CONDITIONAL field is conditioned on the value of another field. The conditions under which the field is present are specified in the subclause where the field is described.

2.3.1.2.3 OPTIONAL field

An OPTIONAL field may occur in an instance of the message, according to the requirements of the message source.

2.3.1.3 Basic Data Types

The following basic data types are used in this Standard.

2.3.1.3.1 UINT(n)

This is an n-bit unsigned integer. The possible range of values is 0 to $2^n - 1$. A field of this type may be restricted to a subset of these values.

2.3.1.3.2 BIT(n)

This is an n-bit pattern type.

2.3.1.3.3 INT(n)

This is an n-bit signed integer. Twos complement representation is used. The possible range of values is $-2^{(n-1)}$ to $2^{(n-1)} - 1$. A field of this type may be further restricted to a subset of this range.

2.3.1.4 Ordering Rules

In general, message fields are arranged in “little endian” order. Bits are numbered from 1 to 8 in a byte, where bit 1 is the least significant bit. Bytes are numbered from 1 to N, where byte 1 is the least significant byte of an N-byte quantity.

For example, the ordering of the bits and bytes of a field of type UINT(32) is shown in Table 2. The least significant bit of the field is bit 1 of byte 1. The most significant bit is bit 8 of byte 4.

Table 2: Bit and Byte Order of UINT(32) Values

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
							LSB	**1**
								2, 3
MSB								**4**

A more complex field type with two sub-fields is shown in Table 3.

Table 3: Example Complex Field Type

Field Name	**Field Type**	**Field Presence**
VALUE	**UINT(5)**	**MANDATORY**
INDEX	**UINT(5)**	**MANDATORY**

In this example, the bits are arranged as shown in Table 4. The VALUE field is listed in the table before the INDEX field. The bits of the VALUE field appear in the least significant bits of byte 1. The least significant bit of INDEX appears at bit 6 of byte 1 and the most significant bit appears in bit 2 of byte 2.

Table 4: Bit and Byte Order of Complex Field Type Example

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
		LSB of INDEX	**MSB of VALUE**				**LSB of VALUE**	**1**
OTHER BITS…						**MSB of INDEX**		**2**

2.3.1.5 Byte Alignment

All messages shall contain an integer number of bytes. Padding bits shall be added to the last byte at the most significant end, if necessary.

Byte alignment of individual fields, if required, is specified on a case-by-case basis.

2.4 Definitions

For the purposes of this Standard, the following definitions apply:

Term	Definition
Base Modulation Component	A set of modulation symbols reserved to transmit Stream Packets for any Flow in a waveform conformant to **ARIB STD-B47** [4].
Block Mode	A mode for transmitting a Stream Packet defined in **ARIB STD-B47** [4].
Conditional Access	Any technical measure and/or arrangement whereby access to the signals transmitted by a protected service in intelligible form is made conditional upon subscription or other forms of prior individual authorization.
Conditional Access System	A subsystem of the Network providing Conditional Access capabilities.
Control Word	A secret key used by the Device to decrypt Stream Packets delivered on a specified Flow in a specified Superframe.
Crypto Period	A period of time in which a specific Control Word is valid.
Device	Customer Equipment that can be activated to access Service in a Network.
Enhancement Modulation Component	A set of modulation symbols reserved to transmit Stream Packets for certain Flows in a waveform conformant to **ARIB STD-B47** [4] in addition to the Base Modulation Component.
Flow	A logical stream within a Multiplex.
Flow Cipher	The algorithm used in conjunction with a Control Word to decrypt a Stream Packet
Fragment	A portion of a Service Packet encapsulated in a Frame.
Fragment Header	A header delimiting Fragment and Service Packet boundaries within a Frame.
Frame	The protocol data unit of the Transport Layer
Framing Layer	The sublayer of the Transport Layer responsible for encapsulating Service Packets into Frames and Stream Packets, and for extracting Frames from Stream Packets and Service Packets from Frames
Increment	Addition of 1.
Multicast Logical Channel	An addressable logical channel which is the smallest content-bearing component of the Network transmission that can be received by the Device. The Multicast Logical Channel is comprised of a set of Streams.
Multiplex	A set of Flows available in a given signal conformant to **ARIB STD-B47** [4]. The signal may contain more than one Multiplex.
Network	A wireless multicast network using **ARIB STD-B47** [4].
Octet Mode	A mode for transmitting a Stream Packet defined in **ARIB STD-B47** [4].
Padding Byte	A byte with a standard value of zero (0) used solely for the purpose of completing a Frame.
Service Layer	The entity using the services of the Transport Layer.
Service Packet	The unit of data provided to the Transport Layer by the Service Layer.

Term	Definition
Stream	A logical subchannel of an MLC transporting Stream Packets, containing the content of a single Flow, except for Stream 0.
Stream 0	The Stream in an MLC which transports control data related to the Flows carried by other Streams in the MLC needed for rapid acquisition.
Stream Encryption/Decryption Layer	The sublayer of the Transport Layer responsible for encrypting and decrypting Stream Packets
Stream Layer	The protocol layer responsible for multiplexing Flows into MLCs. It is the highest layer of air interface specified in **ARIB STD-B47** [4]
Stream Packet	The unit of data carried in a Stream, which is processed in a specific Superframe.
Superframe	The portion of a signal conformant to **ARIB STD-B47** [4] for a specific second.
Transport Layer	The protocol layers responsible for transporting Service Packets from Network to the Device using the services of the Stream Layer, as specified in this Standard.

2.5 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards 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 standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

[1] FIPS[1)] PUB 197. *Specification for the advanced encryption standard (AES)*, 2001.

[2] NIST SP[1)] 800-38A. Dworkin, Morris. *Recommendation for block cipher modes of operations: methods and techniques*, 2001.

[3] TIA[2)] Engineering Committee Recommendation. *TIA style manual (Internet Version),* 1992.

[4] ARIB STD-B47 , *Forward Link Only Air Interface Specification for Terrestrial Mobile Multimedia Multicast*.

[5] Ordinance No.87 of the Ministry of Internal Affairs and Communications, 2011.

[6] Notification No.299 of the Ministry of Internal Affairs and Communications, 2011.

[1)] FIPS and NIST SP publications are issued by the National Institute of Standards and Technology (NIST). The address of NIST is: Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900 USA.

[2)] TIA Standards and recommendations are issued by the Telecommunications Industry Association (TIA). The address of the TIA is: Telecommunications Industry Association, 2500 Wilson Blvd., Suite 300, Arlington, VA 22201 USA

3 TRANSPORT LAYER OVERVIEW

3.1 Introduction

TM3 Networks efficiently distribute broadband multimedia content over multicast wireless networks to mobile devices supporting large numbers of subscribers. ARIB STD-B47 [4] specifies physical, MAC and control/stream layers appropriate for a TM3 Network. This Standard specifies the Transport Layer for TM3 Networks conformant to ARIB STD-B48 . It consists of the stream encryption/decryption and framing protocols used to transport application service packets securely over Streams in the Network.

3.2 Reference Model

The reference model for the Transport Layer is shown in Figure 1. The Network delivers content to the Devices as a sequence of application service packets over the Transport Layer, using the services of ARIB STD-B47 [4].

Figure 1: Transport Layer Reference Architecture

The Transport Layer defines protocols for unidirectional communication between two components of a TM3 system over the air interface specified in ARIB STD-B47 [4]:

- The Device
- The Network

3.2.1 The Device

The Device is any device capable of receiving and interpreting Services delivered over the Network using an air interface conformant to ARIB STD-B47 [4]. Typically, it has an integrated receiver that allows it to detect and acquire the waveform, and to process the content transmitted over it to deliver it in a form intelligible to the user (e.g. as video or audio).

3.2.2 The Network

The Network transmits content to the Devices.

The tasks performed by the Network in support of the Transport Layer include:

- Fragmenting application service packets and concatenating the fragments into frames
- Delivery of content to the Stream Layer of the air interface.
- Encryption of Stream Layer packets to support Conditional Access.
- Formation and transmission of a waveform conformant to ARIB STD-B47 [4] for reception by the Device.

3.3 Transport Layer Protocol Architecture

The Transport Layer forms a sequence of application service packets for a specific flow into one or two Stream Layer packets every second for delivery over the Stream Layer. The Stream Layer packets may be encrypted. The Transport Layer makes use of the services provided by the Stream Layer specified in clause 3 of ARIB STD-B47 [4] to deliver a set of Flows containing the application service packets.

The layering architecture of the Transport Layer is shown in Figure 2.

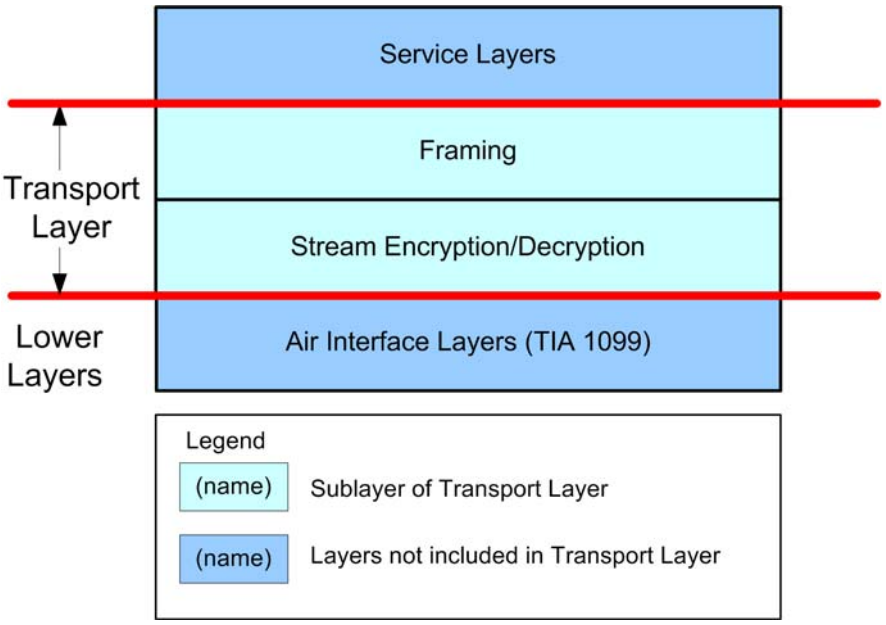

Figure 2: Transport Layer Protocol Architecture

The Transport Layer provides services which are used by all higher layer protocols in Networks. From the perspective of the Transport Layer, the layer using the services of the Transport Layer is considered to be the Service Layer. The Service Layer protocol provides support for a specific application class, and may be different depending on the class of service. These differences are transparent to the Transport Layer.

The Transport Layer consists of two sublayers: the Stream Encryption/Decryption Layer and the Framing Layer. The Framing Layer in the Network accepts a sequence of application service from the Service Layer and embeds them in one or two sequences of frames, depending on whether the application service requires use of the Enhancement Modulation Component in addition to the Base Modulation Component [4]. The Framing Layer in the Device extracts a sequence of application service packets from the sequence(s) of received frames and delivers them to the Service Layer. The set of frames delivered in a particular second for a particular modulation component and a particular Flow, forming a Stream Layer packet in the Superframe, may be encrypted and decrypted in the Stream Encryption/Decryption Layer.

3.3.1 Services Provided to Transport Layer

The Transport Layer assumes the services supplied by the Stream Layer specified in clause 3 of ARIB STD-B47 [4]. ARIB STD-B47 provides the Devices with access to a set of Multicast Logical Channels (MLCs) made up of several independent data Streams. Each Flow is mapped to a specific Stream. The Flow data is delivered to the Devices in Stream Packets, which comprise the Flow data for a specific Superframe. In addition, Stream 0 in each MLC is designed to carry small amounts of data, i.e. signaling information associated with the other Streams in the MLC. Stream 0 is not considered to be transporting a separate Flow.

In the Network, the Transport Layer accepts Service Layer application packets for the set of Flows to be delivered. The Network maps each Flow onto a Stream and then combines Streams into MLCs. In the example shown in Figure 3, two Flows (x and y) are mapped to Streams 1 and 2 of MLC n respectively.

The MLC in the waveform may be transmitted as a Base Modulation Component only, or as a Base Modulation Component and an Enhancement Modulation Component. If the MLC is

transmitted as a Base Modulation Component only, all Streams in the MLC are restricted to the Base Modulation Component. If the MLC is transmitted as a Base Modulation Component and an Enhancement Modulation Component, each Stream in the MLC may be configured for transmission in both components, or in the Base Modulation Component only, independently of the other Streams.

Stream 0 of the MLC is used to carry signaling messages associated with Flows x and y, such as Entitlement Control Messages (ECMs) delivering Conditional Access data needed to determine the keys necessary to decrypt these Streams. The general structure of messages transported in Stream 0 is specified in clause 6.

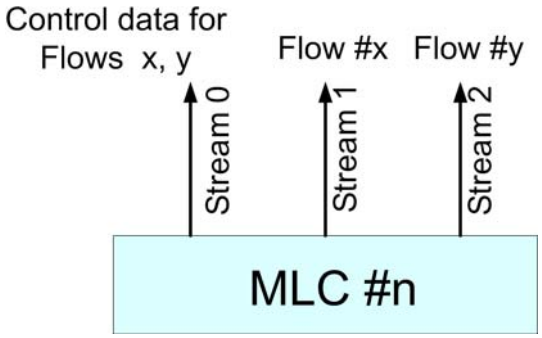

Figure 3: Mapping of Flows to MLC and Streams

3.3.2 Stream Encryption/Decryption Layer

The lowest sublayer of the Transport Layer is the Stream Encryption/Decryption Layer. This sublayer encrypts and decrypts the content of those Streams transporting Flows which are subject to Conditional Access at this layer. Streams not subject to Conditional Access at this layer are not encrypted.

Conditional Access is controlled through a Conditional Access System (CAS). There may be more than one CAS controlling access to an encrypted Stream. The CAS provides the data necessary for an authorized Device to determine the Control Word necessary to decrypt the encrypted Stream. The same value of the Control Word shall be used by all CASs controlling access to a given Stream. The protocols necessary to support the CAS are outside the scope of this Standard.

Clause 4 specifies the Stream Encryption/Decryption Layer protocols.

3.3.3 Framing Layer

The core function of the Framing Layer is to deliver variable-sized service packets over the Stream Layer specified in clause 3 of ARIB STD-B47 [4] as a set of Frames. The service layers deliver a sequence of packets to the Framing Layer which are concatenated and then fragmented and recombined into a sequence of Frames. The Frames are delivered to the Stream Encryption/Decryption Layer and then to the Stream Layer specified in clause 3 of ARIB STD-B47 [4]. The Framing Layer in the Device extracts the Frames from the decrypted Stream Packets, recovers the packet fragments from the Frames and recombines them to restore the original packets for delivery (with possible errors) to the higher layers in the Device. In addition, the Framing Layer provides an optional CRC to verify data integrity. Clause 5 specifies the Framing Layer protocols and messages.

3.3.4 Service Layer

The Service Layer is an abstract label for the layer using the services of the Transport Layer. In general, Service Layer protocols supply adaptations that are specific to the class of content being transported, such as realtime and non-realtime services. Service Layer protocols are outside the scope of this Standard.

4 STREAM ENCRYPTION/DECRYPTION LAYER

4.1 Introduction

This clause specifies the Stream Encryption/Decryption Layer. All Networks based on ARIB STD-B47 [4] shall implement the protocols specified in this clause.

The Stream Layer specified in clause 3 of ARIB STD-B47 [4] supplies a sequence of Stream Packets. Each Stream Packet supplies Flow Data for a specific Superframe. Each Superframe may contain one or two Stream Packets for a given active Flow. If the Flow has only a Base Modulation Component, there is one Stream Packet per Superframe. If the Flow has both a Base and an Enhancement Modulation Component, there are two Stream Packets per Superframe. The structure of the Superframe is defined in detail in subclause 3.2.4 of ARIB STD-B47 [4].

The Stream Encryption/Decryption layer performs the following functions for Services that require protection across the air interface specified in ARIB STD-B47 [4]:

- Encryption of Stream Packets by the Network
- Decryption of Stream Packets by the Device

These functions are described in the following subclauses.

4.2 Stream Encryption and Decryption

For each Stream that requires encryption for transmission across the Air interface, the Network generates a Control Word. A Control Word is valid during a Crypto Period. The duration of the Crypto Period is typically a few seconds, minutes or hours. The value of the Control Word and the length of the Crypto Period are determined by the Device using means which are outside the scope of this specification.

The Control Word is used to encrypt Stream Packets before they are transmitted according to a specified encryption algorithm, the Flow Cipher. The Stream encryption process shall be reinitialized in each Superframe. It preserves the length of the data, and each Stream Packet is separately encrypted.

The Flow Cipher for which support is specified in this Standard is AES in CTR mode with 128-bit keys [2]. A Device shall support AES in CTR mode with 128-bit keys unless prohibited by regulatory requirements. Support for alternate Flow Ciphers may be provided in future versions of this Standard. A Network may use any Flow Cipher algorithm for which support is defined. A CAS which is intended for use in Networks supporting different Flow Ciphers should specify a method to signal the Device which Flow Cipher is in use.

4.3 Initial Counter Value in AES CTR Flow Cipher

The counter value for the Flow Cipher shall be reinitialized in each Superframe to the 128-bit quantity constructed as shown in Table 5, and Incremented for each keystream block required to encrypt the stream packet.

Table 5: Initial Counter Value for AES CTR Flow Cipher

Bits	Value
0-74	**0**
75	**Layer**
76-107	**System Time**
108-127	**Flow ID**

The value of the Layer bit shall be set to zero if the Stream Packet is transmitted in the Base Modulation Component. It shall be set to one if the Stream Packet is transmitted in the Enhancement Modulation Component.

The value of the System Time shall be the System Time of the Superframe as defined in subclause 4.2.5.1 of ARIB STD-B47 [4].

The value of the Flow ID shall be the ID of the Flow carried in the encrypted stream.

5 FRAMING LAYER

5.1 Introduction

All Networks based on ARIB STD-B47 [4] shall implement the protocols specified in this clause.

The Framing layer adapts Service Packets in a Flow for transport over a Stream, which is then multiplexed into an MLC. Operation of the Framing Layer in conjunction with a Stream Layer configured to operate in Block Mode is shown in Figure 4. The Framing Layer may be used in conjunction with a Stream Layer configured to operate in either Block Mode or Octet Mode [4].

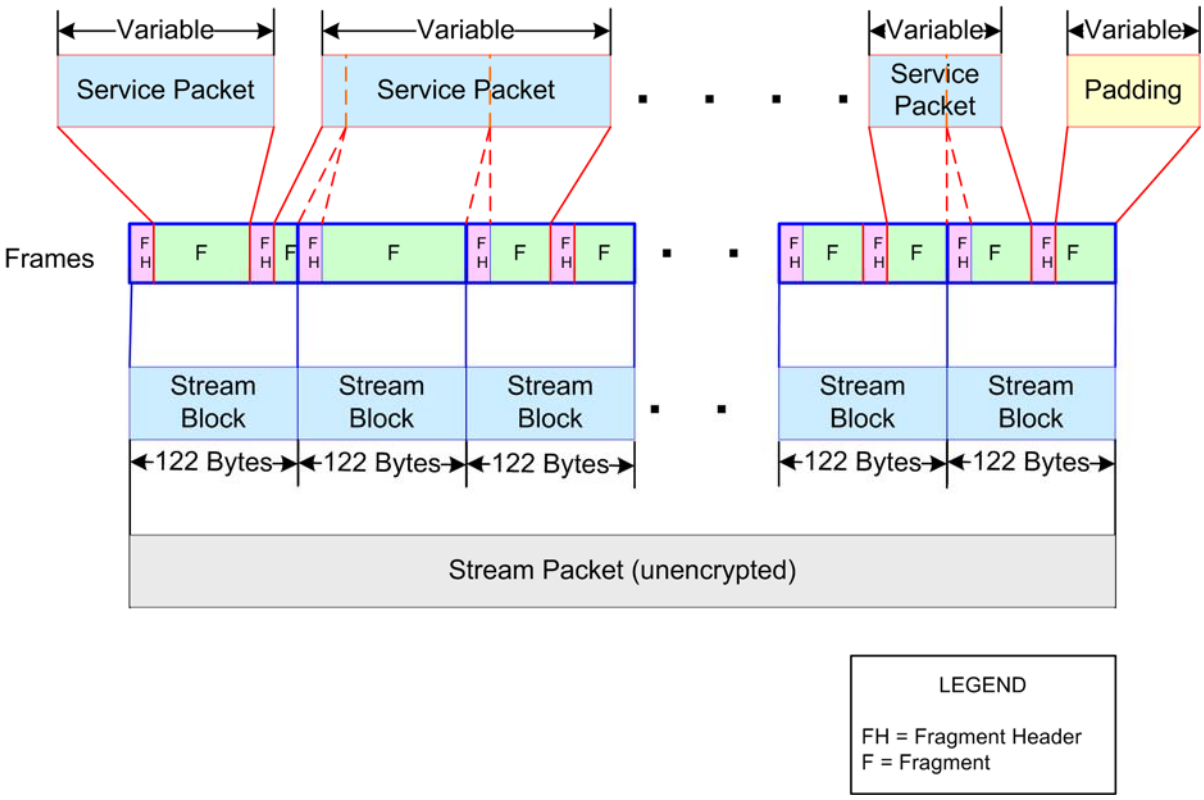

Figure 4: Working of the Framing Layer

On the Network side, the Service layer delivers a sequence of Service Packets belonging to a Flow to the Framing Layer. The Framing Layer may append a CRC to each of the Service Packets (not shown in Figure 4). The Framing Layer then buffers the Service Packets intended to be sent in a specific Superframe in sequence. It fragments the buffered Service Packets such that the Fragments may be combined with 1-byte Fragment Headers and then concatenated into fixed size protocol data units called Frames (122 bytes). The final Frame of a Superframe transported in conjunction with a Stream Layer configured to operate in Octet Mode may be less than 122 bytes if the final Fragment of the final Service Packet in the Superframe is less than 121 bytes long.

If necessary, the final Fragment of a Service Packet is followed by one or more Fragments of Padding Bytes, so that the total number of bytes to be transmitted is an integer multiple of 122. The Framing Layer may also be configured such that a Service Packet is permitted to cross Superframe boundaries.

The 122-byte Blocks so formed are the sequence of 122-byte Stream Blocks which form the unencrypted Stream Packet for the Superframe. The resultant unencrypted Stream Packet is then passed to the Stream Encryption/Decryption Layer for encryption as required.

If the Flow is only available in the Base Modulation Component then one Stream Packet per Superframe is formed using the above procedure. If the Flow is available in both the Base and Enhancement Modulation Components, then two Stream Packets per Superframe are formed using the above procedure, one for each modulation component. In this case, the two Stream Packets shall be of equal size. The Framing Layer shall insert sufficient Padding Bytes in both Stream Packets to fulfill this requirement.

The Device reverses this procedure to extract the sequence of Service Packets from a received and decrypted Stream Packet, processing and removing the CRCs if present, and delivering the resultant sequence of Service Packets to the Service Layer. If errors were detected in the decoding process, the Framing Layer in the Device may signal the presence to errors to the Service Layer.

5.2 Framing Protocol

The functions of the Framing Protocol are:

- Providing a “packet” interface to the Service Layer.
- Detecting and signaling data errors at the Device.
- Providing an interface to the Stream Encryption/Decryption and Stream Layers.

5.2.1 Framing Layer Service Interface

In the Network, the Service layer commands the Framing layer to send data over a particular Flow. The command shall contain the following parameters:

- The Flow ID on which the data is to be sent
- The number of Service Packets to be sent
- The length and contents of each Service Packet

If the Flow is transported in a Stream which is transmitted in both Base and Enhancement Modulation Components, the Service Layer in the Network shall also indicate to the Framing Layer whether the Service Packet is intended for transmission in the Base or Enhancement component. Otherwise, all Service Packets in the Flow shall be transmitted in the Base Modulation Component.

The Framing Layer in the Device shall recover the sequence of Service Packets and deliver them to the Service Layer in the order received, with error indications if an error is detected, and indicating which modulation component was used to deliver the Service Packet.

5.2.2 Stream Layer Service Interface

In each Superframe, the MAC Layer in the Network determines the maximum number of MAC Layer Packets that can be sent for each MLC in the System. Each MAC Layer Packet corresponds to a sequence of 122 bytes, which represents a Stream Block if the Stream is configured in Block Mode. If the Stream is configured to operate in Octet Mode, the sequence of 122 bytes is a sequence of octets. The Stream Layer uses this information to determine the maximum number of Stream Blocks or octets that can be sent for each Stream of an MLC. The Stream Layer notifies the Framing Layer of the maximum number of Blocks or octets that may be sent in that Superframe for each Stream.

5.2.3 Service Packet Checksum Option

If the Flow is configured to support the Service Packet Checksum Option, the Network adds a 16-bit CRC to each Service Packet before commencing fragmentation processing. The CRC is a 16-

bit field that contains the value of the Checksum Sequence for the service packet. The CRC is calculated according to the procedure specified in subclause 5.1.4 of ARIB STD-B47 [4].

If the Checksum option has been selected, the last 2 bytes of a reconstructed Service Packet shall be considered as the 16 CRC bits by the Device. The CRC is computed over the entire Service Packet (excluding the two CRC bytes) and compared with the received CRC bits. If there is a mismatch, the packet is marked as being in error. The Framing Layer then removes the two CRC bytes, and delivers the packet, its length and any error indications to the Service Layer.

5.2.4 Service Packet Fragmentation

The Framing Layer entity fragments one or more Service Packets addressed to a Flow, with or without CRC as appropriate, up to the limit of the number of Stream Blocks or octets available for transmission in the Superframe for that Flow, and sends them over the Stream corresponding to the requested Flow.

Each Fragment consists of a Fragment Header (FH) followed by zero or more bytes of a Fragment Body. The Fragments of a Service Packet are transmitted in the order in which the bytes of the Fragment Body appear in the Packet. The Fragment Header indicates the number of bytes in the Fragment Body, and whether the Fragment is the last Fragment of a Service Packet. Additionally, the Fragment Header may indicate that the following bytes in the Frame are padding.

The size of each Fragment Body shall be the minimum of:

- The residual number of bytes in the Frame currently being created, excluding the Fragment Header
- The residual number of bytes in the Service Packet currently being fragmented
- 121 bytes

If the fragmentation of a Service Packet results in the creation of a Frame with one unused byte, the Framing Layer in the Network shall complete the Frame by inserting a Fragment Header for a notional zero-length Service Packet in that residual byte. The Framing Layer in the Device shall recover and discard this notional Service Packet without delivering it to the Service Layer.

Fragments of different Packets are not interleaved, i.e. the last Fragment of a Packet is followed by the first Fragment of the next Packet.

5.2.5 Fragmentation Mode

In Streams other than Stream 0, the Framing Protocol may be configured to operate in one of two modes with respect to Superframe boundaries, according to the requirements of the Service Layer. In Stream 0, fragmentation shall not be permitted across Superframe boundaries.

5.2.5.1 Fragmentation Across Superframe Boundaries Allowed

In this mode, the Network allows Fragments of a Packet to be transmitted on either side of a Superframe boundary.

5.2.5.2 Fragmentation Across Superframe Boundaries Not Allowed

In this mode, the Network does not allow Fragments of a Packet to be transmitted on either side of a Superframe boundary.

5.2.5.3 Effect of Fragmentation Mode

In Block Mode, the last Fragment of the last Packet transmitted in the Superframe shall be followed by Padding Bytes for the remainder of the Blocks allocated to the Stream in the

Superframe, unless fragmentation is permitted across Superframe boundaries for this Flow, and there are sufficient Service Packets available for a partial Service Packet to be included in the current Superframe. In this instance, the Network may fragment a Service Packet and transmit the Fragments in consecutive Superframes. The Device shall combine the first Fragments of the Service Packet, received at the end of a Superframe, with the remaining Fragments of the Service Packet, received at the beginning of the next Superframe containing data for the Flow, in order to recover the Service Packet.

In Octet Mode provision of Padding Bytes is optional.

5.2.5.4 Fragment Format

Each Fragment consists of a Fragment Header followed by a Fragment Body. The Fragment Header is 1 byte long. The format of the Fragment Header is shown in Table 6

Table 6: Fragment Header Format

Field Name	Field Type	Field Presence	Subclause Reference
LENGTH	**UINT(7)**	**MANDATORY**	**5.2.5.4.1**
LAST	**BIT(1)**	**MANDATORY**	**5.2.5.4.2**

5.2.5.4.1 LENGTH

This field indicates the number of bytes of the Service Packet present in a Fragment. Values in the range 0-121 (inclusive) indicate that the Fragment Header is followed by a Fragment Body of the specified size. A value of 127 indicates that the remainder of the Frame consists of Padding Bytes.

The values 122-126 for the LENGTH field are reserved.

5.2.5.4.2 LAST

The LAST bit indicates whether the current Fragment is the last Fragment of a Service Packet.

The LAST bit shall be set to 0 to indicate that the current Fragment is not the last Fragment of a Service Packet.

The LAST bit shall be set to 1 to indicate that the current Fragment is the last Fragment of a Service Packet. Additionally, the LAST bit shall be set to 1 if the Fragment Header is introducing a sequence of Padding Bytes.

5.2.5.5 Padding Bytes

Each Padding Byte in a Frame shall have the value of zero.

5.3 Flow Configuration Options

There are several configurable options associated with the Framing and Stream Encryption/Decryption Layers supporting each Flow:

- Fragmentation Across Superframe Boundaries (FASB) allowed or not
- Checksum Protocol in use or not
- Stream Encryption in use or not

5.3.1 Signaling Flow Configuration Options

The set of Flow Configuration options selected for a given flow is communicated to the device over the Control Channel in the FlowBLOB field in the Flow Description Message for that Flow, as

specified in subclause 2.2.5.2.2.1 of ARIB STD-B47 [4]. There is no FlowBLOB field corresponding to Stream 0. The assignment of FlowBLOB bits to Flow Configuration Options is defined in Table 7.

Table 7: Assignment of FlowBLOB Bits for Flow Configuration Options

Bit Name	FlowBLOB Bit Number	Subclause Reference
FASB_ALLOWED	**0**	**5.3.1.1**
CHECKSUM_ACTIVE	**1**	**5.3.1.2**
STREAM_ENCRYPTION_ACTIVE	**2**	**5.3.1.3**

The FlowBlobLength field of the Flow Description Message shall be set to a value greater than or equal to 3. The remaining FlowBLOB bits, if any, are reserved and shall be set to 0.

An option shall be considered as selected if the corresponding bit in the FlowBLOB field is set to 1. An option shall be considered as not selected if the corresponding bit in the FlowBLOB field is set to 0.

The options are defined in the following subclauses.

5.3.1.1 FASB_ALLOWED

The FASB_ALLOWED option shall be selected for the Flow if and only if fragments of Service Packets are permitted to cross Superframe boundaries.

5.3.1.2 CHECKSUM_ACTIVE

The CHECKSUM_ACTIVE option shall be selected if and only if the CRC is applied to Service Packets in the Flow.

5.3.1.3 STREAM_ENCRYPTION_ACTIVE

The STREAM_ENCRYPTION_ACTIVE option shall be selected if and only if the Stream transporting the Flow is encrypted, as specified in clause 4.

5.3.2 Flow Configuration Profiles

The permitted combinations of Flow Configuration options may be fixed according to the content of the Flow.

6 STREAM 0 MESSAGES

All Networks based on ARIB STD-B47 [4] shall implement the protocols specified in this clause.

Stream 0 is reserved for transporting control messages related to the Flows carried on the other Streams of an MLC. Stream 0 messages are tightly synchronized to the Superframe. Stream 0 messages do not constitute an identified Flow.

Messages transported in Stream 0 shall be subject to Framing as specified in subclause 5.2. Stream 0 messages shall not be subject to CRC protection, shall not be subject to the stream encryption process defined in clause 4, and shall not be fragmented across Superframe boundaries. Stream 0 messages shall only be transmitted in the Base Modulation Component. The total bandwidth allocated to Stream 0 messages cannot exceed 4 kbps if there are two other streams present in the MLC, and cannot exceed 255 kbps if there is only one other stream present in the MLC [4].

Each Message on Stream 0 shall begin with a header consisting of a one-byte MESSAGE_ID field. The general format of the Stream 0 Message is shown in Table 8.

Table 8: Format of Stream 0 Messages

Field Name	Field Type	Field Presence
MESSAGE_ID	**UINT(8)**	**MANDATORY**
MESSAGE_BODY	**Variable**	**CONDITIONAL**

The MESSAGE_ID field indicates the type of the Message being transported in Stream 0. The specification of the individual messages transported in Stream 0 is outside the scope of this specification.

Change History List of Standard Ver.1.1

No.	Item No.	Description	Page	Reason
1	Scope	This standard applies to the multimedia broadcasting defined in Section 2 of Chapter ~~3~~ 24, Ordinance No.~~26~~87 of the Ministry of Internal Affairs and Communications, ~~2003~~2011.		Modifications in line with the amendment of Ordinance and Notification.
2	Normative References	[5] Ordinance No.~~26~~87 of the Ministry of Internal Affairs and Communications, ~~2003~~2011. [6] Notification No.~~88~~299 of the Ministry of Internal Affairs and Communications, ~~2009~~2011.	6	Modifications in line with the amendment of Ordinance and Notification.

Forward Link Only Transport Specification

ARIB STANDARD

ARIB STD-B48 Version 1.1

Version 1.0 November 5, 2010
Version 1.1 July 3, 2012

Published by

Association of Radio Industries and Businesses

11F, Nittochi Building,
1-4-1 Kasumigaseki, Chiyoda-ku, Tokyo 100-0013,Japan

TEL 03-5510-8590
FAX 03-3592-1103

Printed in Japan