



ANSI/TIA-102.AABB-B 2011
APPROVED: APRIL 22, 2011

# TIA STANDARD

# Trunking Control Channel Formats

**TIA-102.AABB-B**
**(Revision of TIA-102.AABB-A)**

**July 2011**

TELECOMMUNICATIONS
INDUSTRY ASSOCIATION

tiaonline.org

## NOTICE

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

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

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

(From Project No. 3-4623-RV2, formulated under the cognizance of the TIA TR-8 Mobile and Personal Private Radio Standards, TR-8.10 Subcommittee on Trunking and Conventional Control.

.

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

**PRICE: Please refer to current Catalog of**
**TIA TELECOMMUNICATIONS INDUSTRY ASSOCIATION STANDARDS**
**AND ENGINEERING PUBLICATIONS**
**or call IHS, USA and Canada**
**(1-877-413-5187) International (303-397-2896)**
**or search online at http://www.tiaonline.org/standards/catalog/**

# NOTICE OF COPYRIGHT

## This document is copyrighted by the TIA.

## NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

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

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

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

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

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

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

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

TIA SHALL NOT BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

# Foreword

(This foreword is not part of the standard.)

This document will be submitted to APCO/NASTD/FED by the Telecommunications Industry Association (TIA), as provided for in a Memorandum of Understanding (MoU) dated December 1993. That MoU provides that APCO/NASTD/FED will devise a Common System Standard for digital public safety communications (the Standard), and that TIA shall provide technical assistance in the development of documentation for the Standard.

This document has been developed with inputs from the TIA/APCO Project 25 Interface Committee (APIC), the TR-8.10 Trunking and Conventional Control Subcommittee, and TIA Industry members.

This document is being published because it is felt that there is an urgent need for technical information for the emerging digital systems for Land Mobile Radio Service.

This document describes the general descriptions, packet structures, information block structures for both single and multiple block formats for trunked radios meeting the Project 25 requirements. These definitions are necessary to ensure interoperability of trunked radio units.

This Standard presents a design for control channel bit structures which was recommended by TIA to APCO/NASTD/FED as being suitable for use as part of their standard for a digital public safety radio system (Project 25). TIA expects that APCO/NASTD/FED will establish and publish additional standards for trunking operation which will then provide the basis for additional TIA standards planned for the Project 25 system.

There is one annex in this Standard. Annex A is informative and is not considered part of this Standard.

# Contents



## Figures

## Tables

# Patent Identification

The reader's attention is called to the possibility that compliance with this document may require the use of one or more inventions covered by patent rights.

By publication of this document no position is taken with respect to the validity of those claims or any patent rights in connection therewith. The patent holders so far identified have, we believe, filed with APCO/NASTD/FED statements of willingness to grant licenses under those rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such licenses. Details may be obtained from APCO/NASTD/FED.

The following patent holders and patents have been identified in accordance with the TIA intellectual property rights policy:

*TIA shall not be responsible for identifying patents for which licenses may be required by this document or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention*.

Ericsson Inc. -- Patent Nos. US 5,574,788

# 1 Introduction

## 1.1 Scope

The intent of this document is to define the general control channel structures to be employed on the Project 25 trunking control channel.

The 9600 b/s control channel scheme is designed to be compatible per **[BAAA]**.

## 1.2 Revision history

July, 2005 Revision A approved for TIA publication.

April, 2011 Revision B approved for TIA publication.

## 1.3 References

The following documents contain provisions, which, through reference herein, 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 maintained by them.

### 1.3.1 Normative References

1. **[BAAA]** "*Project 25 FDMA Common Air Interface",* ANSI/TIA 102.BAAA-A, September 2003 - This document describes the basic over the air formats used on the Trunking control channel.
2. **[AABC]** "*Project 25 Trunking Control Channel Messages"*, ANSI/TIA-102.AABC-C, November 2009 - This is a separate companion document that describes the specific use of the general Trunking control channel structures.
3. **[AABD]** "*Trunking Procedures"*, TIA-102.AABD-A, December 2008
4. **[BAAC]** "*Project 25 - Common Air Interface - Reserved Values"* , TIA-102.BAAC-A, December 2003

### 1.3.2 Informative References

5. Project 25 Guidelines to Assign Wide Area Communication Network and System Identities, April 2001 – This document provides guidelines which explain how to assign the WACN ID and System ID in a uniform manner (with and without an FCC Call Sign correlation) so that interoperability across diverse Project 25 systems is possible.

## 1.4 Number Nomenclature

There are references to bit patterns in this document. In general the following applies:

If a number is preceded by a "**%**" the number is to be interpreted as a binary representation with the appropriate number of symbols (e.g. %1010 is 4 symbol binary for 10)

If a number is preceded by a "**$**" the number is to be interpreted as a hexadecimal representation with the appropriate number of symbols. (e.g., $0A is 2 symbol hexadecimal for 10)

If a number is presented with neither a "**%**" or "**$**" preceding it, the number is to be considered as a decimal representation with the appropriate number of symbols. (e.g., 15 is decimal 15)

# 2 Overview

The trunking control channel packet structure is based upon the data packet structure of the Common Air Interface (CAI). This allows the control channel transactions to both be usable on system channel resources supporting only control channel packets or system channel resources which support both control channel packets and other system packets (e.g. voice or data packets).

The trunking control channel shall be considered to consist of two (2) separate communication paths, the inbound control channel path and the outbound control channel path. The inbound path is used for transmissions from the subscriber units to be received by the RFSS. The outbound path is used for transmissions from the RFSS to be received by the subscriber units.

## 2.1 Control Channel Packets

A control channel packet sent from the RFSS to the subscriber unit shall be termed the Outbound Signaling Packet (OSP) using the outbound control channel. A control channel packet sent from the subscriber unit to the RFSS shall be termed the Inbound Signaling Packet (ISP) using the inbound control channel.

Control channel packets are identified as single block and multiple block formats. The majority of operations of the trunking control channel are accomplished with the single block packet format to afford the greatest throughput potential. The multiple block format is reserved for the transactions which have need of greater information transfer than provided in the preferred single block format.

The single block control channel format is not an unconfirmed data packet as defined by the CAI. The single block control channel format has a unique preamble to indicate it is a special trunking signaling block. With this special "trunking signaling block" consideration, an associated Trunking Service Access Point (SAP) is implied, thereby removing the need to explicitly cite SAP information.

Two different multiple block formats are defined. One multiple block format uses the normal Unconfirmed Data Packet format, with inclusion of an explicit header block. There is a unique SAP identified in this header block to indicate that this is to be processed as a multiple block trunking format. See **[AABC]** for more details.

Another multiple block format is similar to the normal Unconfirmed Data Packet format. There is a unique SAP identified in this header block to indicate that this is to be processed as a multiple block trunking format. This multiple block format differs from the previously mentioned multiple block format in definition of the header block, which is defined in clause 6. One multi-block format is distinguished from the other by a unique format value.

The Unconfirmed Data Packet type is to be applied to each instance in this document, unless otherwise stated.

## 2.2 Protected Control Channel Transactions

Control channel transactions may be protected, with only the intended audience faithfully recovering the information transferred. This is accomplished with the use of common encryption schemes shared between the RFSS and the subscriber units of the RFSS. Both the RFSS and the subscriber unit shall utilize the same encryption scheme and associated operational encryption parameters (e.g. encryption algorithm, encryption key, and encryption synchronization) to provide valid communications. Both the inbound and the outbound transactions may be appropriately protected on the control channel.

Extended protected transactions may be processed directly on the primary control channel. These protected transactions are requested on the trunking control channel, but may be directed to a separate working channel which may be allocated for this protected operation.

The use of protected control channel packets and nonprotected control channel packets are allowed upon the same control channel. The subscriber units not capable of processing the protected information of the protected packets are not able to discern the information content of these packets, but are able to verify proper control channel operation by verifying TSBK CRCs (Cyclic Redundancy Check) which are not encrypted. Likewise the protected subscriber units are capable of processing both unprotected and protected packets on the control channel.

In general the encryption scheme and/or encryption parameters utilized on the trunking control channel are different from the encryption scheme and/or encryption parameters utilized on protected working channels.

# 3 General descriptions

## 3.1 Control channel designation

There shall be at least one 9600 b/s control channel for each trunked RF Sub-system (RFSS). The transactions for each of the control channels are under the direction of the RFSS. It is not necessary that each control channel present exactly the same information as the other control channels. The control channel message contents are representative of the activity of the traffic channel(s) local to this control channel.

If protected information is to be shared between multiple control channels, this information is always presented in a protected format.

The control channel repeater is composed of a radio frequency pair, an inbound receive channel and an outbound transmit channel. A message received on the inbound channel to the control channel repeater is designated as an Inbound Signaling Packet (ISP). A message transmitted on the outbound channel of a control channel repeater is designated as an Outbound Signaling Packet (OSP). The control channel repeater is full duplex in operation, allowing transmission of OSPs while there are ISPs being received.

## 3.2 Modes of control channel

A control channel may be either of a dedicated or composite control channel mode:

The dedicated control channel mode has the channel function as a conduit for system information and service requests among the communication unit population.

The composite control channel mode has a channel function both as a control channel and as a bearer channel. This may be a mutually exclusive use of the channel, such that the channel is used as a control channel until a service request requires this channel resource as a bearer channel to satisfy the service request. While the channel is being used as a bearer channel it may not be used to transact control channel operations. While the channel is functioning as a control channel, it operates as a dedicated control channel. The composite control channel may function as the dedicated control channel between the traffic channel signaling. *NOTE: In this mode, there are periods of time in which a control channel is "not" available to the subscriber units (since the channel is supporting traffic channel signaling during those times),*

*and thus any services that require dedicated control channel transactions are not normally processed.*

One of the control channels is designated as the primary control channel for this portion (e.g. site) of the RFSS. Other control channels, whether dedicated or composite, are designated as secondary control channel(s) for this portion of the RFSS. The primary control channel is used for normal system transactions.

Both the primary and the secondary control channels may support protected packet formats for the control channel transactions. The same information is presented on different control channels in the same mode, e.g., all protected or all nonprotected.

The protection mode of the control channel shall be made aware to the receiving subscriber units via a broadcast update message on the control channel.

## 3.3 Inbound Control Channel Access

Access to the inbound control channel is accomplished via a Slotted ALOHA scheme. In Slotted ALOHA all transmissions are required to commence on any occurrence of a regular spaced slot boundary. In this system, a slot boundary is marked at every uniform number of microslots. The outbound signaling stream supplies synchronization information to be used by the receiving subscriber units to define the inbound slot times. The inbound slot boundaries can be redefined by the outbound signaling bit stream, but should be a multiple of the 7.5 ms microslot times that exceeds the expected inbound packet size to optimize throughput. See **[AABD]** for more detail regarding the use of slotted ALOHA.

# 4 Packet structure

Each control channel message is considered a packet. Each packet is composed of one or more information blocks. Each block is protected by a rate 1/2 trellis code, and the sequence of blocks is transferred over the common air interface as a single packet. Part of the packet is a checksum to be used to verify the accuracy of the error correction in the receiver. If the packet is corrupted, then appropriate error correction mechanisms are employed to correct the error at the receiver.

The general packet structure for data packets in the CAI is employed for the control channel packets. There is a preamble to preface the information block(s) of the packet. The preamble contains Frame Synchronization (FS) and Network Identifier (NID) fields. The FS bit sequence indicates the location of the first bit of the packet. The NID is used to address this packet to specific receiving components of the system, and to indicate the type of packet so that the proper error correction scheme may be performed. The information block(s) for the packet follow the preamble.

The packet is integral multiples of 70 bit micro-slots. There is one Status Symbol (SS) consisting of two (2) bits inserted after every micro-slot (every 70 bits) in a packet.

## 4.1 Frame Sync Word

The Frame Synchronization bit pattern is the same as is used for the data packets as detailed in **[BAAA]** subclause 8.3 and is not repeated here.

## 4.2 Network Identifier

The Network Identifier is defined in **[BAAA]** subclause 8.5 and is not repeated here.

The 4-bit Data Unit ID portion of the 16-bit Network Identifier (NID) indicates the format of the control channel packet as either:

$7 indicating the single block format (TSBK)
$C indicating the multiple block format (PDU)

This shall be used for both the OSP and ISP signaling. ($ = hex)

When a SU first acquires a control channel, it decodes the NAC from the received NID. The SU shall use this acquired NAC in all transmissions to the RFSS. See **[AABD]** for more detail.

## 4.3 Status Symbols

Status Symbol codes presented in the OSP are given in the table below.

Table 4.3-1 OSP Status Symbol Codes

| Status Symbol | Meaning |
|---|---|
| 00 | Unknown, not used for OSPs |
| 01 | Busy - inbound control channel is currently not available |
| 10 | Unknown, used to space out microslots to a slot boundary |
| 11 | Indicates start of Inbound slot |

The Status Symbol codes for the ISP are given in the table below:

Table 4.3-2 ISP Status Symbol Codes

| Status Symbol | Meaning |
|---|---|
| 00 | Unknown, not used for ISPs |
| 01 | Busy - not used for ISPs |
| 10 | Unknown, used for ISPs |
| 11 | Idle - not used for ISPs |

The Status Symbols are always presented in nonprotected form, whether the transaction is presented in protected mode or nonprotected mode.

## 4.4 Data Error Correction

This applies across the information blocks of the packet whether in the Single or Multiple Block format.

The information blocks use a rate 1/2 trellis code. The encoding process of the rate 1/2 code is detailed in **[BAAA]** clause 7 and is not repeated here.

## 5 Information Block Structure - Single Block Packet

To provide a consistent response time potential, a special abbreviated packet format is provided in the form of a single block of information for the trunking control channel packet, a special header block. A Trunking control channel message may be as short as a single block. This is denoted as the Trunking Signaling Block (TSBK). This packet structure is typically used for the control channel transactions which are of a very time critical nature, or account for a large portion of the normal trunking control channel transactions. Examples of these would be call requests and call grants requiring immediate response, talkgroup affiliation updates, etc.

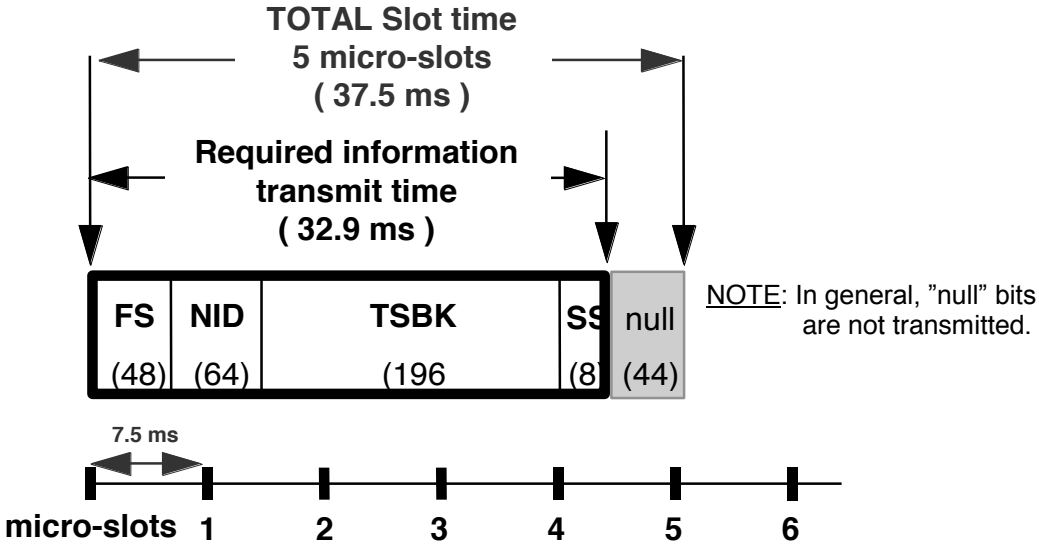


Figure 5-1 Single Block ISP Format

Figure 5-1 depicts the single block ISP format under the condition that a slot is defined as 5 microslots. As another example, a slot would be 45 ms were it to be defined as 6 microslots. The ISP has a preamble of Frame Sync and Network Identifier preceding the TSBK to afford proper inbound packet framing. A single block of trunking information is all that is allowed for this ISP. Note: The inbound slot time is larger than the required information transmit time, where the information transmit time refers to the necessary time to transmit the information and status symbols of the ISP.

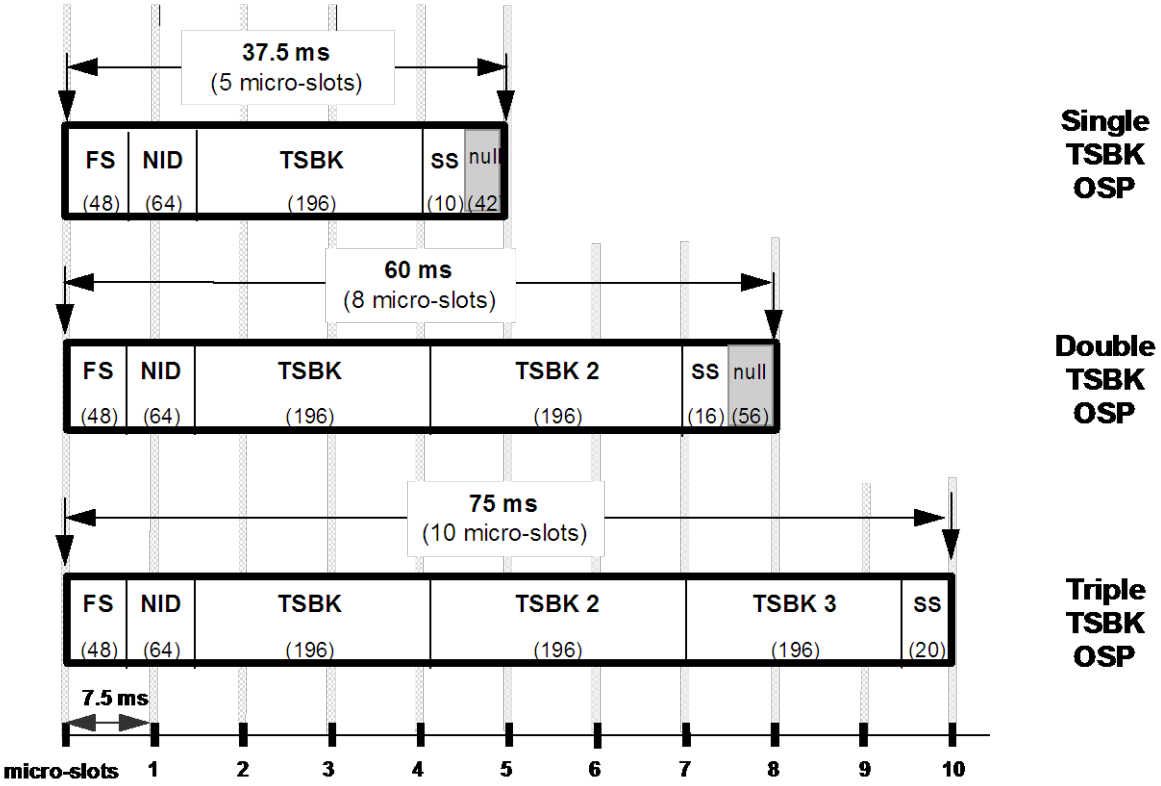


Figure 5-2 Single Block OSP Formats

Figure 5-2 depicts all three single block OSP formats on a common scale reference of microslot durations. A dedicated control channel would normally transmit OSPs continually with one immediately following another.

Figure 5-2 depicts the single block OSP formats. The OSP has a preamble of Frame Sync and Network Identifier preceding the TSBK also, but allows for up to two (2) additional TSBKs to follow without an additional preamble. No CRC across all of these TSBKs is required, since each of the TSBKs maintains a CRC across its own information block.

The subscriber unit is aware of the current format (single, double, or triple TSBK) for the outbound control channel using the DUID and LB field in the TSBK, and thereby can determine when to expect the preamble and when to expect the TSBK(s) of the OSP.

Additionally the subscriber unit needs to remain aware of Frame Sync reception and use this condition as an indication of the start of an OSP.

Each of the TSBKs can be independently designated as protected or nonprotected.

The three TSBK packet option is the most control channel efficient of the three offered outbound modes (single TSBK, double TSBK, or triple TSBK), with regard to airtime resource usage. The number of TSBKs in the OSP is variable and controlled by the FNE to maximize the control channel resource. This is evaluated with regard to the Multiple Block Packets awaiting transmission as well as the current control channel demands of unit ISPs.

The actual channel transmit time is indicated for each allowed transaction by the wide black box outline in Figures 5-1 and 5-2. Null bits pad the packet to the end of a micro-slot. This padding is necessary because the Status Symbol (SS) is the last two bits in each micro-slot. However, if no more data units are to follow on the channel, (e.g., a single ISP on a control channel), then the transmitter simply turns off after the required bits are sent and the nulls are not physically modulated. Of course, the receivers ignore any nulls that are transmitted. The null bits are always set to zero. Null bits are discussed further in **[BAAA]** § 5.1.2.

The periodic insertion of Status Symbols both in the OSP and ISP are not explicitly shown, though the total number of Status Symbol bits required is indicated. This occurs after every 70 bits have been transmitted for the packet.

## 5.1 Trunking Signaling Block Format

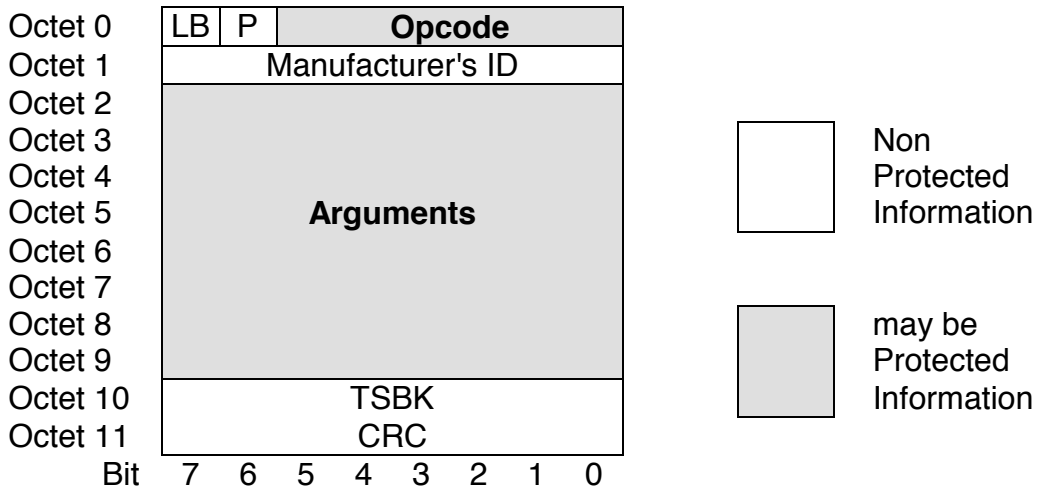


Figure 5.1-1 Single Block Packet Transactions

The Trunking Signaling block contains 10 octets of address and control information, followed by 2 octets of CRC.

Following is the general description of the fields of this TSBK:

Last Block flag (LB) - (octet 0, bit 7)

- this indicates if more TSBKs are to follow in this packet
  - = 0 at least one more TSBK to follow in this packet
  - = 1 last TSBK in this packet

Protected trunking block flag (P)- (octet 0, bit 6)

- this designates the protection mode for this packet
  - = 0 - nonprotected packet mode
  - = 1 - protected packet mode

Opcode - (octet 0, bit5-0)

- this field specifies the basic message type for this packet. (e.g. This specifies Unit to unit call service, group call service, USER status, etc.) This defines how the Argument 1, Argument 2, and Logical Link ID fields are parsed and what information these fields contain pertaining to this control channel message. (The opcodes, under the standard manufacturer's ID, are meant to be system independent definitions, with the same opcodes depicting the same information in any system. See the **[AABC]** for explicit definition of the bits for each message.)

Manufacturer's ID - (octet 1)

- identifies the manufacturer for nonstandard control channel messaging. The values for the Manufacturer ID's are given in **[BAAC]**. As of 2004/6/10, an MFID of $00 or $01 (the standard values) indicates a Standard Project 25 message.

Arguments - (octets 2-9)

- this contains the necessary identification of the destination and/or source for this packet. This may also convey additional processing information such as options to be applied to the service addressed by this packet.

Logical Link ID - (octets 7-9)

- this identifies the subscriber unit (SU) to which the OSP is being sent, or the SU which is sending the ISP. This is intended to be system-specific information.

TSBK CRC - (octets 10-11)

- this is the CRC parity check as described in **[BAAA]** subclause 6.2.

## 5.2 Protected TSBK description

The intent is that all the sensitive information of the TSBK shall be presented in a protected mode. To this end the sensitive information of the TSBK shall be encrypted according to a pre-arranged encryption scheme and set of encryption parameters.

To facilitate proper control channel operations of subscriber units not capable of encryption techniques, some of the TSBK information is presented in nonprotected mode. This limited TSBK information is presented in nonprotected mode to allow these subscriber units to discern this as a valid, though unknown, block of a trunking control channel packet. Following is the list of the information that shall be presented in non-protected mode.

Octet 0, bits 7-6 provides the information that this is the last (only) block of this packet (b7=1) and that this is a protected format (b6=1). Subscriber units not capable of protected operations still detect this as a potential TSBK and are able to validate the proper reception of the symbols for this block.

Octet 1 indicates the Manufacturer's ID to allow the proper set of encryption parameters and block parsing to be applied.

Octets 10-11 provide the block error check. This is applied to the contents of the block after the appropriate areas have undergone the encryption process. This is used by the recipient to indicate that the received symbols are proper prior to the decrypting of any information in the block. The subscriber unit which is not capable of protected operations is able to identify this as a proper single block packet, but is not able to utilize any of the protected information fields.

## 5.3 Example of protected TSBKs - Unit to Unit call

This example shows how the protected TSBK would be populated for a unit requesting a Unit to Unit voice call, and the response OSP granting a channel resource to this requested service.

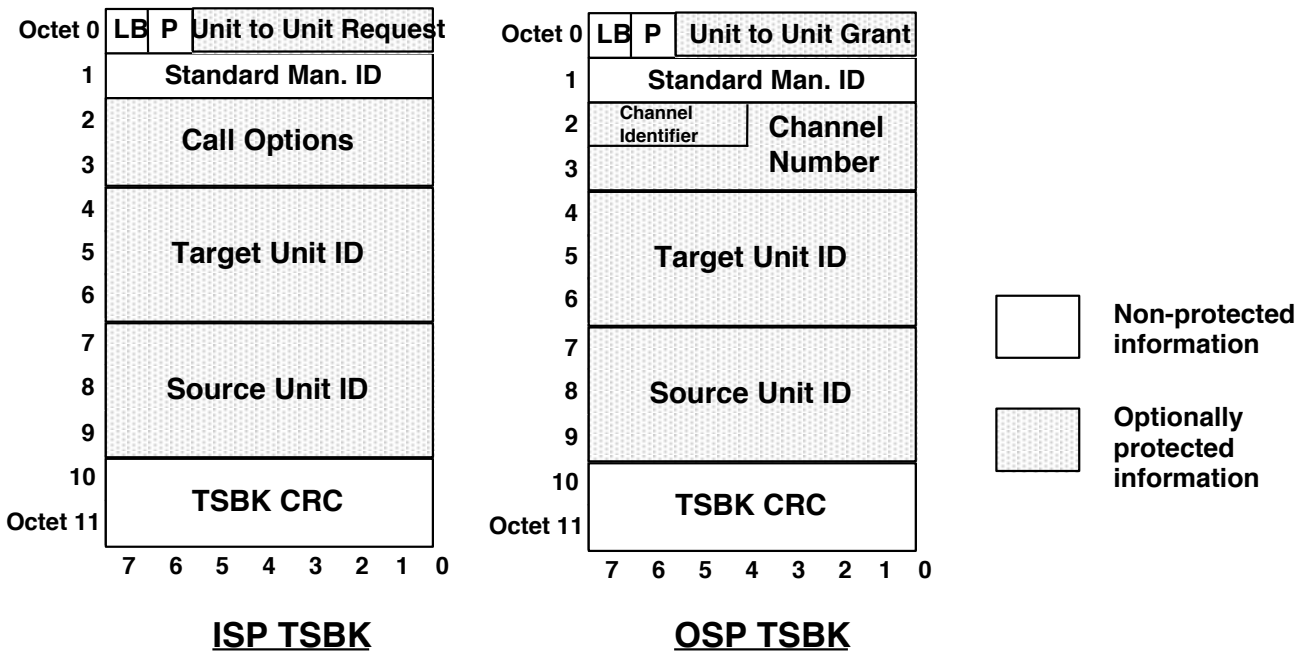


Figure 5.3-1 ISP/OSP TSBKs for Unit to Unit call example

### 5.3.1 Service Request Packet

Referring to Figure 5.3-1, ISP TSBK, this is the request for Unit to Unit call service from the requesting SU.

The LB bit (octet 0, bit 7) has been set to indicate this is the last TSBK in this packet. *This is transmitted in nonprotected mode.*

The P bit (octet 0, bit 6) has been set for protected mode making this a protected ISP. *This is transmitted in nonprotected (e.g. nonencrypted) mode.*

The Opcode field (octet 0, bit 5-0) indicates a request for unit to unit operation. *This is transmitted in protected (e.g. encrypted) mode.*

The Argument field (octets 2-3) has additional information concerning the processing of this call request. In this case it indicates that this request is to be applied to a channel resource immediately. *This is transmitted in protected (e.g. encrypted) mode.*

The Argument field (octets 4-6) indicates the desired target unit identity. *This is transmitted in protected (e.g. encrypted) mode.*

The Logical Link ID field (octets 7-9) indicates the identity of the requesting unit. *This is transmitted in protected (e.g. encrypted) mode.*

The TSBK CRC (octets 10-11) is computed upon the 10 preceding octets. This is *transmitted in nonprotected (e.g. nonencrypted) mode.*

### 5.3.2 Service Response Packet

Referring to Figure 5.3-1, this is the response for Unit to Unit call service from the Trunking Controller to the SUs involved in the Unit to Unit call.

The LB bit (octet 0, bit 7) has been set to indicate this is the last TSBK in this packet. *This is transmitted in nonprotected mode.*

The P bit (octet 0, bit 6) has been set for protected mode making this a protected ISP. *This is transmitted in nonprotected (e.g. nonencrypted) mode.*

The Opcode field (octet 0, bit 5-0) indicates a channel grant for unit to unit operation. *This is transmitted in protected (e.g. encrypted) mode.*

The Argument field (octets 2-3) has additional information concerning the processing of this call response. In this case it indicates the channel assigned for this call service. This is provided with a channel identifier field to specify the channel characteristics (e.g. frequency band), and a channel number that represents one of the channels in this frequency band. *This is transmitted in protected (e.g. encrypted) mode.*

The Argument field (octets 4-6) indicates the target unit identity. *This is transmitted in protected (e.g. encrypted) mode.*

The Logical Link ID field (octets 7-9) indicates the identity of the requesting unit. *This is transmitted in protected (e.g. encrypted) mode.*

The TSBK CRC (octets 10-11) is computed upon the 10 preceding octets. *This is transmitted in nonprotected (e.g. nonencrypted) mode.*

## 5.4 ISP timing

Access to the inbound control channel is accomplished via a Slotted ALOHA scheme. The inbound slots are determined to be a multiple of the micro-slots of the outbound signaling to accommodate the inbound packet size, signaling characteristics of the subscriber unit (i.e. Transmitter turn on time (TONT), Transmitter turn off time (TOFFT), etc.), and RF propagation delay time (PD). The slot boundaries are demarcated by the Status Symbols assuming the "IDLE" status value (%11). Other Status Symbols occurring intraslot are assigned the non-IDLE status of "unknown" (%10).

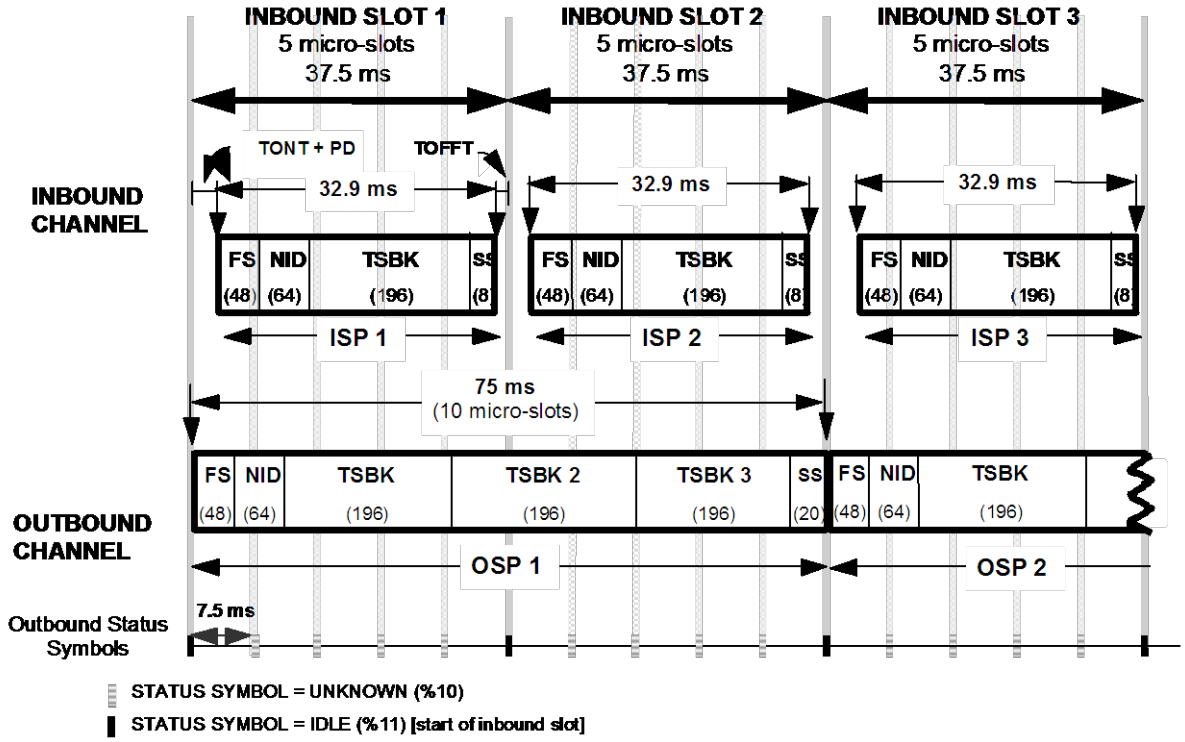


Figure 5.4-1 ISP Timing Relationships

A unit desiring to transmit on the inbound control channel needs to wait for a slot boundary after the assertion of PTT, indicating the beginning of the inbound slot. Assuming all is proper, the unit starts transmitting the ISP within the indicated slot boundaries on the inbound control channel.

In general the start of an ISP does not need to correspond to the start of an OSP, but the ISP is still synchronized to the OSP signaling stream with respect to the micro-slotting.

For an ISP of 37.5 ms. (including "null" bit times), the inbound slot length is also chosen as 37.5 ms, or 5 micro-slots. This allows 44 bit times for the combined effects of TONT, TOFFT, and PD (360 - 196 - 64 - 48 - 8 = 44).

# 6 Information Block Structure – Multiple Block Trunking Packet Format

Trunking control channel messages which require more information transfer than can be accommodated by the single block TSBK capacity, make use of the Unconfirmed data packet format **[BAAA]**, subclause 6.6), utilizing the Unconfirmed header block format and blocks of user defined trunking message information. This packet structure would be used for the control channel transactions which were not of a time critical nature, and exceed the information capability of the single block TSBK format. Examples of these would be unit registration transactions, talkgroup registration, system status updates, adjacent system status updates, etc.

Specifically the multiple block trunking packet header block does not employ octets 7, 8, and 9 of the standard unconfirmed data packet header format (Pad Octet Count, Reserved Octet, and Data Header Offset respectively). A different FORMAT value in Octet 0 than defined for standard unconfirmed data packet format is used to distinguish Multiple Block Trunking Packet header blocks. This permits octets 7, 8, and 9 of the alternative form header, as defined later, to contain specific Trunking Message data defined in **[AABC]**.

The maximum length of a packet on the control channel is specified to control channel access time. The packets of a trunking control channel message are no longer than 44 octets. (This provides an outbound latency of about 135 ms.) The packet is split into blocks with each block containing exactly 12 octets. The first block of each of these packets is a special block, called a header block. The last block of the packet contains the CRC for the packet along with any message information. The maximum number of blocks in a packet, including the header block, is 4.

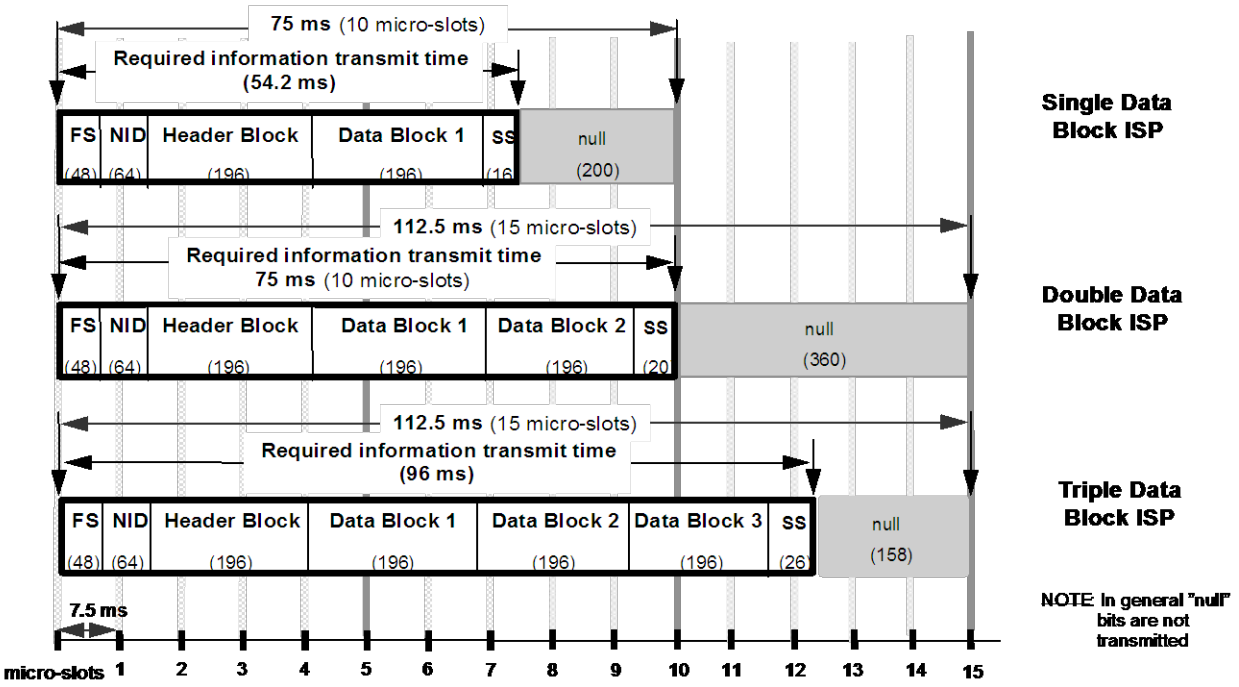


Figure 6-1 Multiple Block ISP Formats

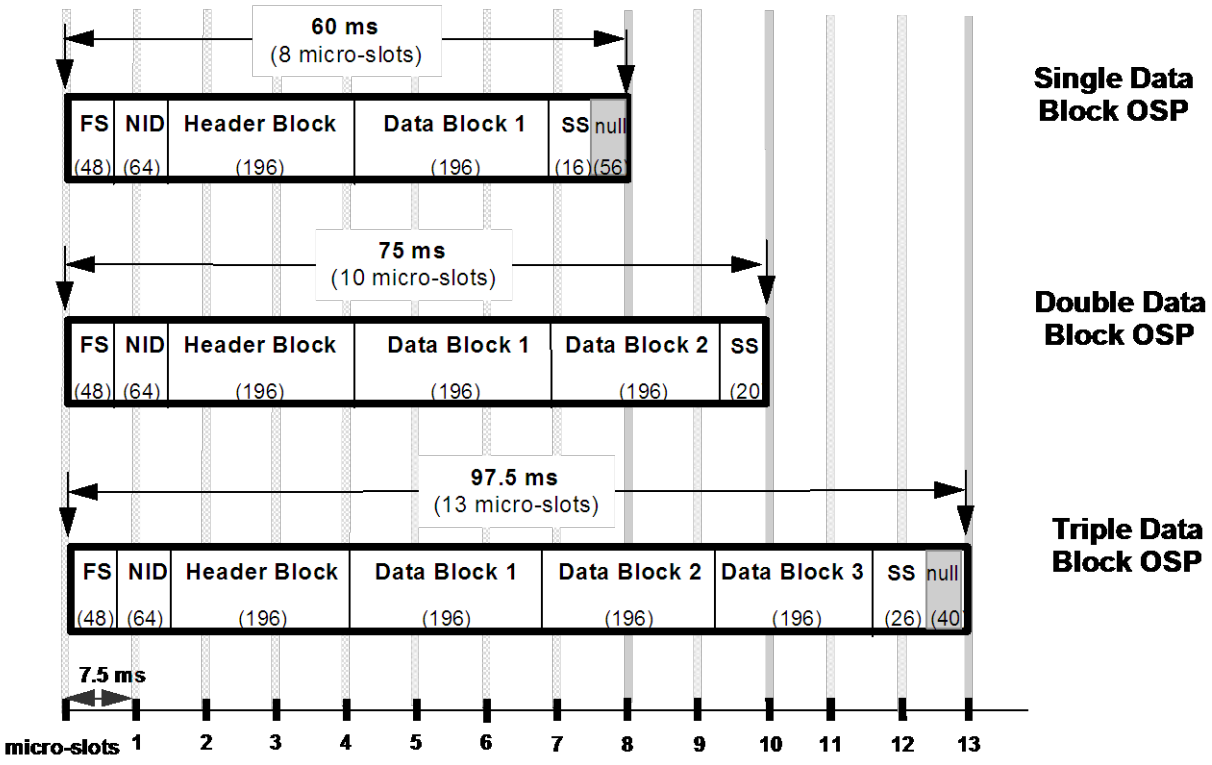


Figure 6-2 Multiple Block OSP Formats

Figure 6-1 depicts the multiple block ISP formats, and Figure 6-2 depicts the multiple block OSP formats. The maximum number of blocks allowed is 4 in either the ISP or the OSP. Both the OSP and the ISP have a preamble of Frame Sync and Network Identifier preceding the information blocks. The actual channel transmit time is indicated for each allowed packet size by the wide black box outline in Figures 6-1 and 6-2.

The last information block of the packet contains a 4 octet CRC across all the information blocks after the Header Block. This CRC is as detailed in **[BAAA]** subclause 6.3.

Not explicitly shown, but accounted for in the air time values, is the periodic insertion of Status Symbols both in the OSP and ISP. This occurs after every 70 bits have been transmitted for the packet.

## 6.1 Trunking Control Packet Header Format

One format for the Trunking Control Packet Header block is of the same form as the Unconfirmed Data Packet Header defined in **[BAAA]** subclause 6.6. Extensions to this format are noted below.

The Trunking Control packet header block is shown in Figure 6.1-1. Unused bits in the block are set to 0.

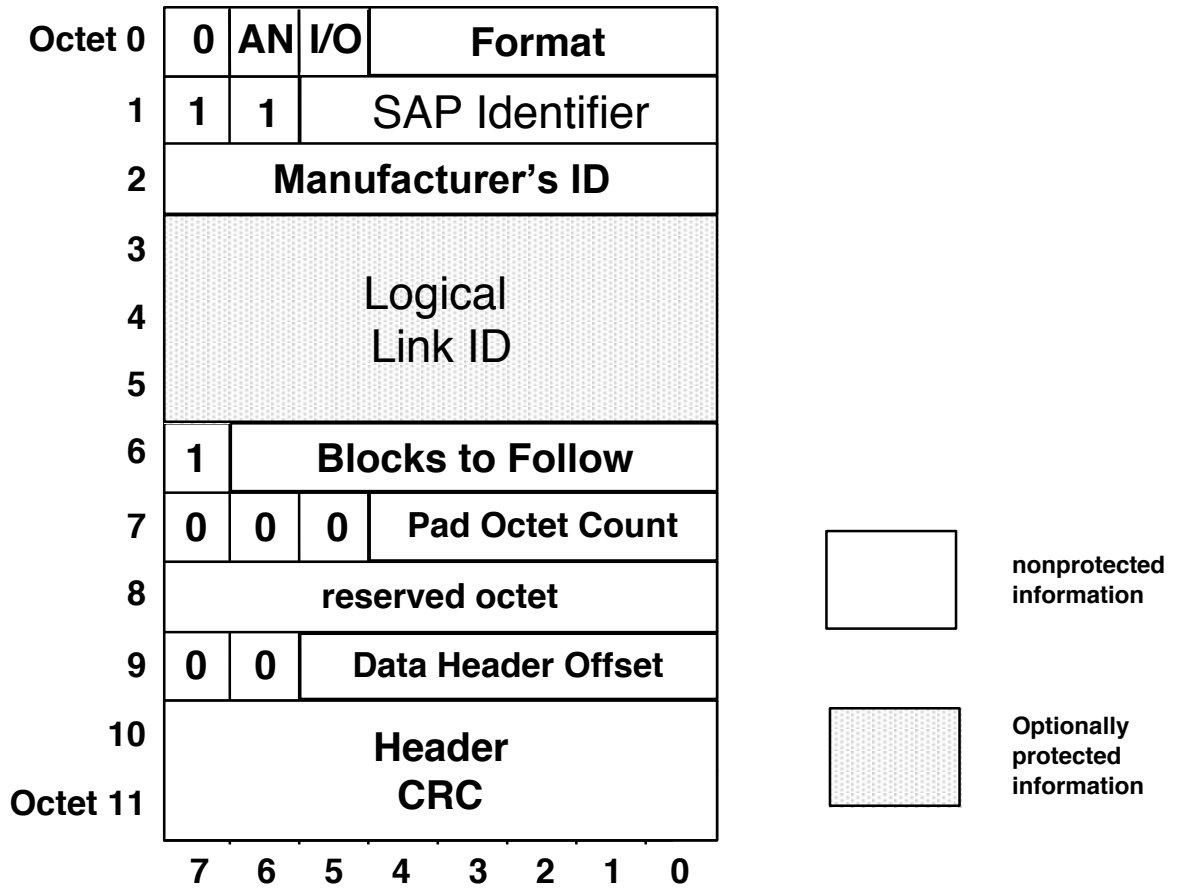


Figure 6.1-1 Trunking Control Packet Header Block

The alternative form for the Trunking Control Packet Header format is of a similar form as the Unconfirmed Data Packet Header defined in **[BAAA]** subclause 6.6. The alternative format is distinguished from the previous format by a different value of Format field in Octet 0. In layout, it differs in that octets 7, 8, and 9 contain information on the trunking message defined by **[AABC]**. Specifically, Octet 7

contains the message opcode, and octets 8 and 9 contain information defined by **[AABC]**.

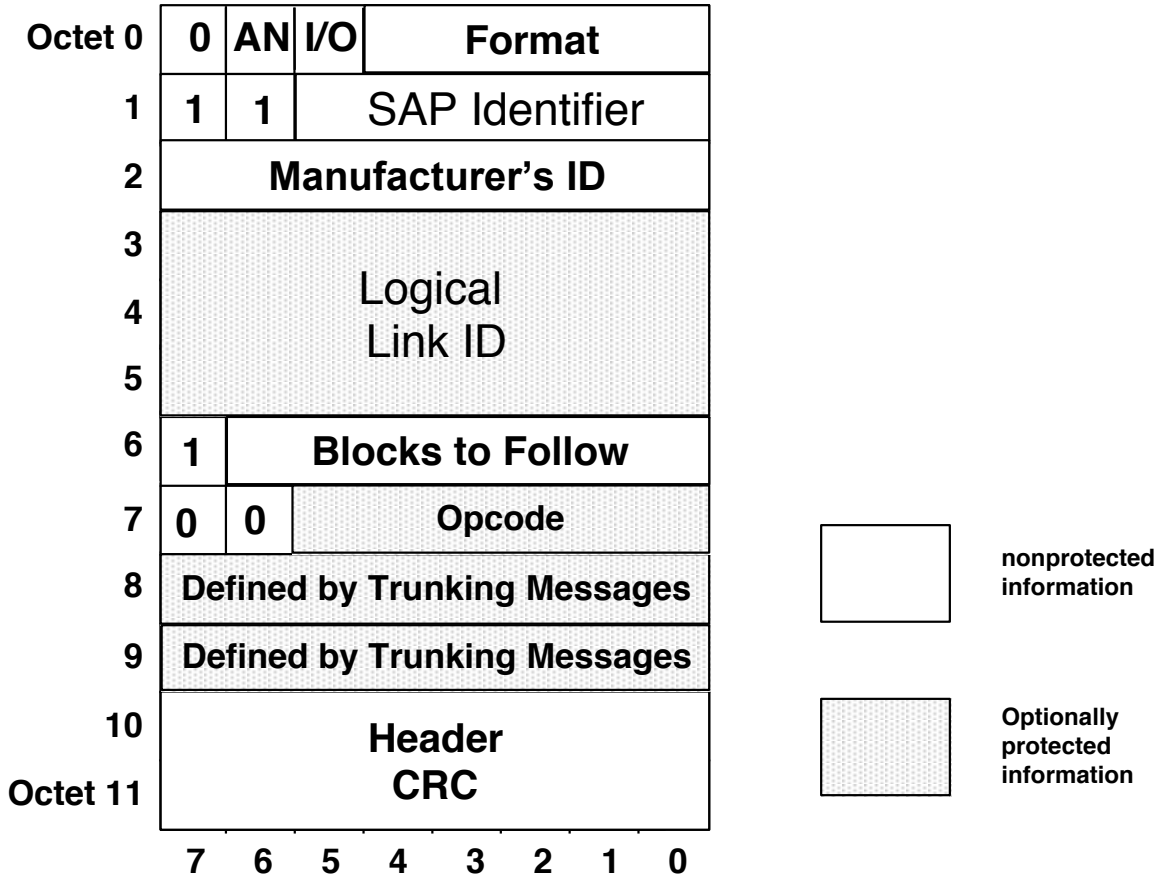


Figure 6.1-2 Alternative Trunking Control Packet Header Block

This is the Unconfirmed Data Packet Header as detailed in **[BAAA]** with the following field modifications:

Format

%10101 - Unconfirmed multiblock trunking control
%10111 - Alternative multiblock trunking control

SAP Identifier

61 - Trunked Control SAP (Multi-block)
63 - Protected Trunked Control SAP (Multi-block)

Logical Link ID identifies the Subscriber unit (SU) that sent the ISP, or the SU to which the OSP is directed.

## 6.2 Data Block Structure

The Data Block structure is that as detailed in **[BAAA]** Subclause 6.6 for Unconfirmed Data Packet and is not repeated here.

## 6.3 Protected Multiple Block Trunking packet description

All of the sensitive information of the Multiple Block packet shall be presented in a protected mode. To this end the sensitive information of this Multiple Block packet shall be protected according to a pre-arranged protection scheme and set of protection parameters.

All the fields of the Header block of this Multiple Block Trunking packet shall be presented in a nonprotected manner with the exception of the Logical Link ID field (octets 3-5) for both formats and the opcode and octets 8 and 9 for only the alternative form. This excepted information shall be presented in a protected form as per the protection scheme and protection parameters active for this control channel. The CRC for the Header Block shall be determined after the Logical Link ID field has been properly protected. Both protected and nonprotected capable subscriber units are able to recover the block structure of the Header block, but only the properly equipped protected units are able to discern useful information from the Logical Link ID field. All subscriber units are able to discern the size of this Multiple Block packet from the header block information.

All the fields of the following Data blocks of this Multiple Block Trunking packet shall be presented in a protected manner as per the protection scheme and protection parameters active for this control channel, with the exception of the last four (4) octets of the last Data block which shall contain the CRC across all preceding Data block contents. The CRC for the Data Block(s) shall be determined after the Data Block fields have been properly protected. Both protected and nonprotected capable subscriber units are able to recover the packet structure as indicated in the Header block, but only the properly equipped protected units are able to discern useful information from the fields of the Data blocks of this protected control channel packet.

## Annex A (Informative): Glossary of Terms

| | |
|---|---|
| b/s | bits per second |
| CAI | Common Air Interface |
| CRC | Cyclic Redundancy Checksum, for error detection |
| DUID | Data Unit Identifier |
| FNE | Fixed Network Equipment, the fixed end infrastructure |
| FS | Frame Synchronization, to mark the first information bit |
| ISP | Inbound Signaling Packet, control channel message sent by SU |
| LB | Last Block |
| NID | Network Identifier, code word following the FS |
| Nonprotected | Information presented without an attempt to guard its recovery from unintended recipients. |
| OSP | Outbound Signaling Packet, control channel message sent to SU |
| PD | Propagation delay, delay to account for the physics of radio transmission |
| PDU | Packet Data Unit |
| Protected | Information presented with some scheme to guard the recovery of the raw information from unintended recipients. |
| PTT | Push to Talk, initiation of transmit action |
| RFSS | RF Sub-System |
| SAP | Service Access Point, where the network provides a service |
| Slotted ALOHA | A channel access scheme providing discrete time slots in which users may transmit their packets |
| SS | Status Symbol, channel access control signaling |
| SU | Subscriber unit |
| TOFFT | Transmitter Turn-Off Time, time required for a radio to cease transmitting after the last bit has been transmitted |

| | |
|---|---|
| TONT | Transmitter Turn-On Time, time required for a radio to begin transmitting the first bit after the transmitter trigger signal is asserted |
| TSBK | Trunked Signaling Block, single block control channel message |

## THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TIA represents the global information and communications technology (ICT) industry through standards development, advocacy, tradeshows, business opportunities, market intelligence and world-wide environmental regulatory analysis. With roots dating back to 1924, TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications.

TIA members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment and entertainment. TIA co-owns the SUPERCOMM® tradeshow and is accredited by the American National Standards Institute (ANSI).

ADVANCING GLOBAL COMMUNICATIONS

HEADQUARTERS
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834
+1.703.907.7700
+1.703.907.7727 (fax)

tiaonline.org