MOTOTRBO™

IP Site Connect Interface Protocol Specification

Version 02.00

November 5, 2010

COPYRIGHTS

REVISION HISTORY

Version	Date	Feature	Section	Page	Lines	Description
02.00	10/29/2010	Capacity Plus Repeater Interface	1.1	8, 11, 12	3-4, 6-11, 14	Included Capacity Plus system
			2.0	11 - 12	52-64, 74-92,	Included Capacity Plus system overview
			2.1	13	101-103	Clarified the repeaters in Capacity Plus shall be in the same local area network
			2.3	14	139-141	Clarify router setting in Capacity Plus system
			3.6	19	263-265	Clarify Capacity Plus supported feature at different protocol versions
			5.2.2 – 5.2.13	24 – 43	404-405 436-437 456 479 507-508 533-534 570-571 588-589 613-614 625-626 654 669	Included Capacity Plus in the LE packet format tables

Version	Date	Feature	Section	Page	Lines	Description
			6.3.1.3	65	1036	Included Capacity Plus in the Common CSBK Response packet format table
			6.4.1.3	69	1086	Included Capacity Plus in the IPSC Call Header packet format table
			8.2.1.3	110	1595	Included Capacity Plus in the XCMP packet format tables
		Link Protocol Update	3.6 5.3.8	19, 50	252 800-808	Updated Link Protocol Version for R1.7
			5.3.7	46-50	740-785	Update Service Bit for R1.7 and Clarified service bit usage per system type and peer type
			6.4.1.33	69	1099 – 1100 1106-1108	Update Call Priority and clarify the channelNum usage in IPSC Call Header for Capacity Plus
		Call Monitoring	3.3	17	202	Updated opcode allocation table to include the call monitoring messages
			5.3.7	46 - 47	748	Updated service bit field for call monitoring service and Capacity Plus interface

Version	Date	Feature	Section	Page	Lines	Description
			7.0	98 - 106	1408-1515	Added Call Monitoring message defintions
		Unauthorized Access Control	9.1.8.5	118	1694	Added IP Console Inhibit / Uninhabit CSBK commands
		LE	5.2.5.3	30	479	Remove peerMode before the maplen in LE map notiifcation message (CCMPD01321201)
		HMAC	Appendix A	124	1759 - 1765	Clarify HMAC key input format (CCMPD01368155), (CCMPD01349839)

TABLE OF CONTENTS

1.0 Introduction

1.1 Overview

This document describes the MOTOTRBO IP Site Connect protocol definitions used in an IP Site Connect system or a Capacity Plus system for communication between peers. The IP Site Connect system links two or more MOTOTRBO repeaters over an IP network. It enables a wide area system access for voice and data service support. The Capacity Plus system links two or more MOTOTRBO repeaters at the same location over an IP network. It enables the trunking of channels from multiple repeaters, and reduces the waiting time to access the system. With the MOTOTRBO repeater IP Site Connect protocol, a third party application can send / receive messages to / from the MOTOTRBO repeater peers in an IP Site Connect system or Capacity Plus system. The IP Site Connect protocol is “language-independent.” Developers may implement this protocol in any programming language which supports bit stream manipulation.

1.2 Terminology

AMBE	Advanced Multi-Band Excitation
BSI	Base Station Identifier
CAI	Common Air Interface
CC	Color Code
CPS	Customer Programming Software
CSBK	Control Signal Block
CWID	Continuous Waveform Identifier
DMR	Digital Mobile Radio
ETSI	European Telecommunications and Standards Institute
FCC	Federal Communications Commission
HMAC	Hash Message Authentication Code
ID	Identity
IP	Internet Protocol
IPSC	IP Site Connect
LAN	Local Area Network
LE	Link Establishment
MFID	Manufacturer’s ID
OACSU	Off Air Call Setup
OTA	Over the Air
PDU	Protocol Data Uint
PC	Personal Computer
PTT	Push To Talk
RDAC	Repeater Diagnostics, Alarms and Controls
RDAC-IP APP	RDAC-IP Application
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTP	Real-time Transport Protocol

RX	Receive
SHA-1	Secure Hash Algorithm
TX	Transmit
XCMP	Extended Control and Management Protocol

1.3 Assumptions

It is assumed that the reader of this document has the following domain knowledge:

- Principle of two-way radio communications
- ETSI Digital Mobile Radio (DMR) Air Interface Protocol
- Real-time Transport Protocol (RTP)
- UDP/IP Protocol

The following domain knowledge is considered beneficial, but is not required:

- Digital two-way radio communications
- Time Division Multiplexing (TDM)
- Voice Encoding/Decoding

1.4 References

[1] RFC 3174 – US Secure Hash Algorithm (SHA-1), September 2001, D. Eastlake, 3rd, http://www.faqs.org/rfcs/rfc3174.html

[2] RFC 3550 RTP: A Transport Protocol for Real Time Application, H. Schulzrinne, July 2003 http://tools.ietf.org/html/rfc3550

[3] Electromagnetic compatibility and Radio spectrum Matters (ERM; Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface (AI) protocol, ETSI TS 102 361-1 V1.4.5 (2007 -12)

[4] Electromagnetic compatibility and Radio spectrum Matters (ERM; Digital Mobile Radio (DMR) Systems; Part 2: DMR voice and generic services and facilities, TS 102361-2 V1.2.6 (2007-12)

[5] MOTOTRBO™ XCMP RDAC Commands

[6] MOTOTRBO™ Repeater XCMP Development Guide

[7] MOTOTRBO™ IP Site Connect Guide ADK

[8] HMAC: http://en.wikipedia.org/wiki/HMAC

[9] MOTOTRBO™ System Planner

2.0 System Overview

An IP Site Connect system or a Capacity Plus system consists of two or more MOTOTRBO stations (repeaters and RDAC-IP applications) linked together over an IP network. The IP network configuration may be the public internet or a private LAN. The term 'Peer' means a MOTOTRBO repeater, a RDAC-IP application or a 3rd party application. Figure 1 shows an example IP Site Connect system. Figure 2 shows an example Capacity Plus system.

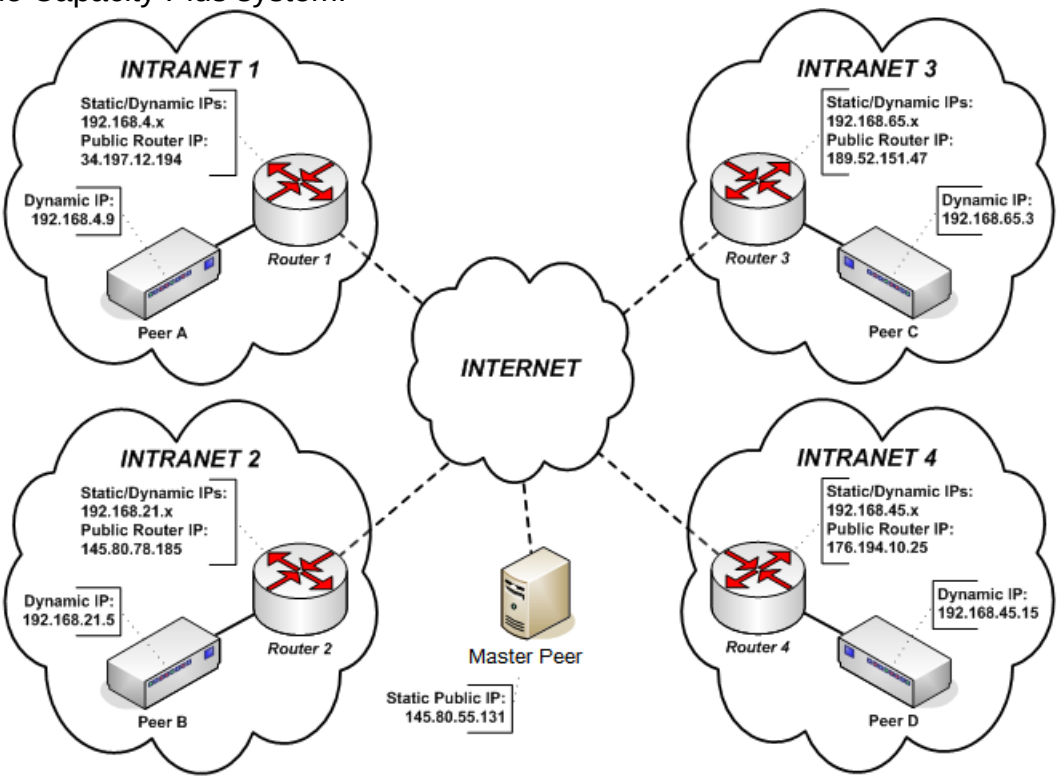


Figure 1 - IP Site Connect System Topology Configuration

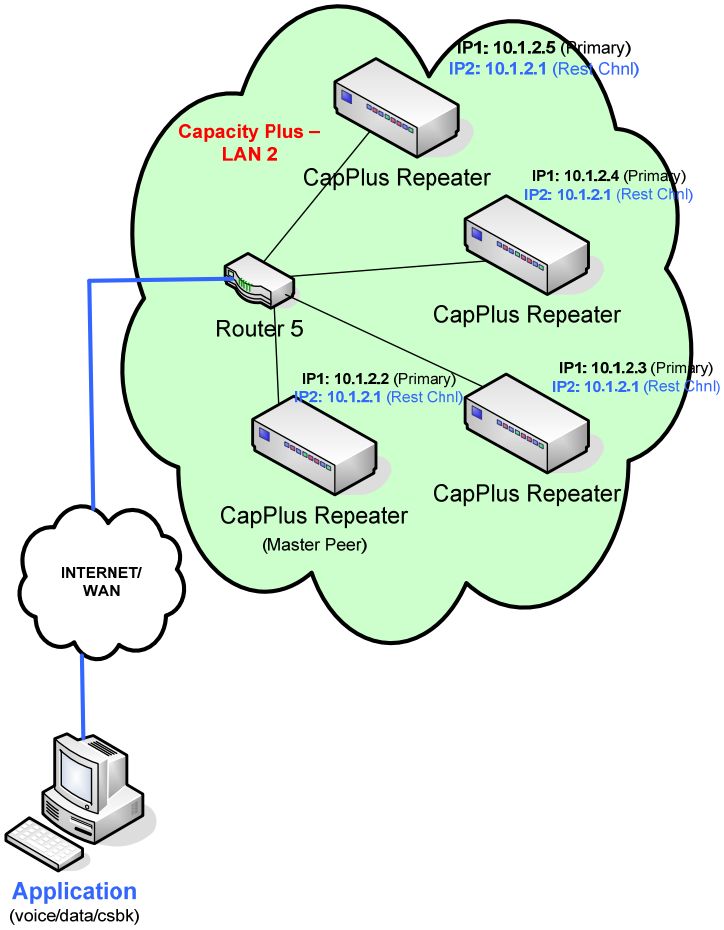


Figure 2 – Capacity Plus System Topology Configuration

In both the IP Site Connect system and the Capacity Plus system, there is a peer configured as the Master Peer. The Master Peer acts as the central point for a peer to find all other peers in the system. It has a static IP address and a UDP port number which are well known to all the peers in the system. When a peer powers up or intends to join the system, the peer begins the link establishment procedure by sending a registration request message to the Master Peer. The Master Peer maintains a map which is a registry of all the peers in the system. After establishing the link with the new joined peer, the Master Peer distributes the map to all peers currently linked in the system. Then all existing peers will create a link with the newly joined peer. Finally, each peer maintains a link with all other peers (including the Master Peer) in the system. This ensures that the system still works when there are any peers down, even the Master Peer.

In the IP Site Connect system, upon successful registration with the Master Peer, the repeater operates in IP Site Connect mode. When the repeater receives voice/data/control packets over the air on the IP Site Connect channel, it sends the packets through the IP Site Connect protocol to all the peers in the IP Site Connect system. Therefore, the voice, data and control packets can be exchanged across disperse locations.

Note: The term 'wide area' indicates coverage across geographically separate areas that may span cities, states or even countries. This however does not imply a 'blanket' coverage. A system instantiation may provide coverage in two different locations but no coverage in the area between the two locations.

In the Capacity Plus system, upon successful registration with the Master Peer, the repeater operates in Capacity Plus mode. When the repeater receives voice/data/control packets over the air on the rest channel, it finds the new rest channel, and notifies all MOTOTRBO repeater peers through the IP interface and informs all the radios over the air about the new rest channel. It sends the voice/data/control packets through the IP Site Connect protocol to all the third party application peers in the Capacity Plus system that registers the receiving service. To avoid the 3rd party application implementation on the rest channel scheduling, and to enable the third party interface at both WAN and LAN topology, the MOTOTRBO Capacity Plus repeater peer supports IP aliasing. A virtual peer with static IP address and static UDP port receives any message from third party application. Figure 2 shows each repeater peer has a two IP addresses: the repeater IP address and the virtual peer IP address for the rest channel. When a repeater peer owns the rest channel, it updates the router with the association of its MAC address and the virtual peer IP address through Address Resolution Protocol (ARP) protocol. When a third party application requests for the Rest Channel access over the Capacity Plus repeater IP interface, the application utilizes the Virtual Peer IP address. The router, connecting the Capacity Plus repeater peers to the external IP network, sends the data to the repeater peer which has the rest channel now based on its ARP cache.

2.1 System Model and Topology

Peers in the system form an overlay network on top of existing IP infrastructure. In other words, peers will not be connected directly (physically) to each other; instead they will use IP, as the connection fabric to communicate with each other.

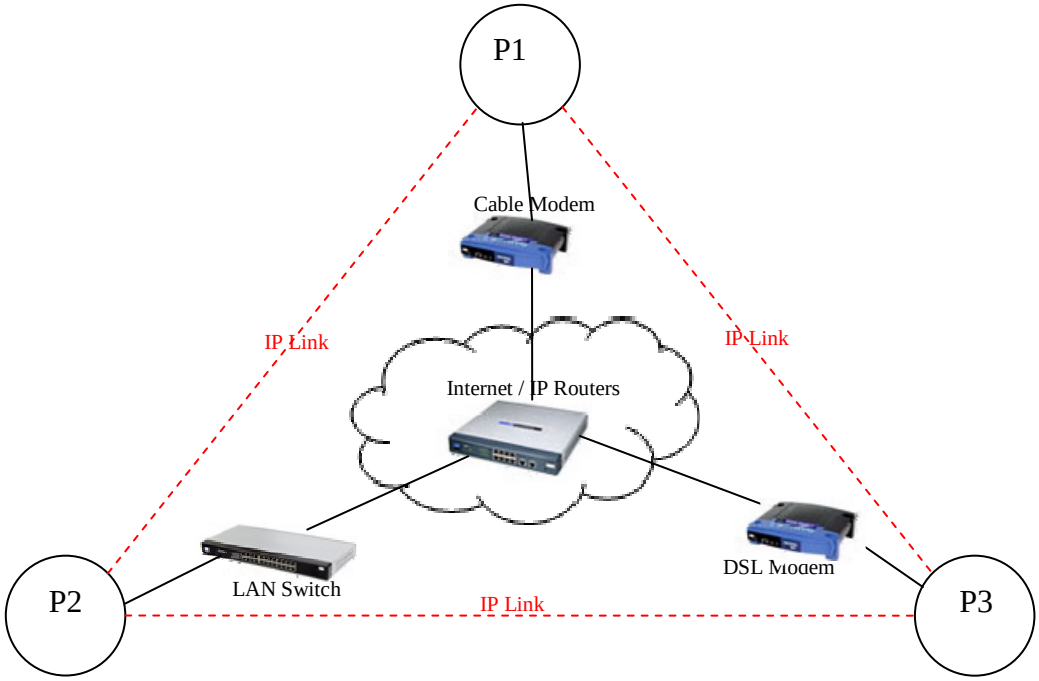


Figure 3 - IP Site Connect IP Network Topology Configuration

The IP Site Connect network will be a homogeneous network – capable of supporting mixed IP network configuration as depicted in Figure 3. All peers must support the IP Site Connect Protocol. In Capacity Plus system, all the repeater peers in one system have to be in the same local area network to avoid network delay impact on the rest channel movement.

The Master Peer has a well-known static IP address and source port number so that it is publicly visible to all other peers in the network topology. The Master Peer can be assigned an IP address through DHCP when located behind a network router. This router must be publicly visible to all other peers in the network topology. The router must have a well-known static IP address and leave open a well-known port number that it will use to forward traffic to the peer located behind the router. The IP Site UDP port of each peer in the system is utilized for exchanging all types of data between peers using the IP Site Connect Protocol.

2.2 System-wide Information

In keeping with the homogeneous network paradigm, the system as a whole ensures that all peers have a copy of the system-wide data that is required to support the expected features and services. The system-wide data includes each peer's ID, IP address and UDP port number. Every peer designates a UDP port on which it sends/receives the IP Site Connect traffic (both data and audio packets). This port number is determined by the peer at power-up and will not change as long as the peer remains powered up. This port number will be conveyed to other peers as part of the

link establishment procedure. When a peer sends a data or audio packet to another peer, it sends the packet to this UDP port number.

A peer stores the IP addresses and port numbers of other peers. Table 1 depicts a snapshot of the map table from the Master Peer perspective from Figure 1 – when all links are established through the discovery algorithm and are in active state.

Peer ID	IP Address	Port Number
1	192.168.4.9	5400
2	192.168.21.5	3500
3	192.168.65.3	5400
4	192.168.45.15	2400

Table 1 - Peer-IP Address Map

There are two fundamental kinds of services supported in the IP Site Connect system – group and individual. Group services are directed at multiple recipients, for example, a group voice call. Individual services are directed at only one recipient, for example, an individual voice call. In either case, the peer does not track the presence of subscribers and talk groups on other peers. The peer just sends a copy of the voice / data message to all the other peers.

2.3 Recommended Router

Although IP Site Connect will work through most off-the-shelf network devices, the following two router/NAT/firewalls have been validated and are therefore suggested for use:

- D-Link - EBR-2310
- CISCO - PIX 501

In the Capacity Plus system, to support the third party application interface, the router must support hair-pin; all the peers must use the Master Peer's static public IP address to communicate with the Master Peer.

IP Site Connect supports the ability to work through a Secure VPN (Virtual Private Network). It is important to note that VPN does add the need for additional bandwidth and may introduce additional delay. The following Secure VPN router has been validated and is therefore suggested for use:

- Linksys EtherFast Cable/DSL VPN Router with 4-port switch. Model: BEFVP41.

See Reference [8] for detailed information on network bandwidth consideration and planning.

3.0 Protocol Definitions

3.1 Protocol Stack

Figure 4 shows the protocol stack that is used for the IP Site Connect System. The UDP/IP is used as transport layer protocol and the protocol stack under UDP/IP is dependent on how these two devices are connected.

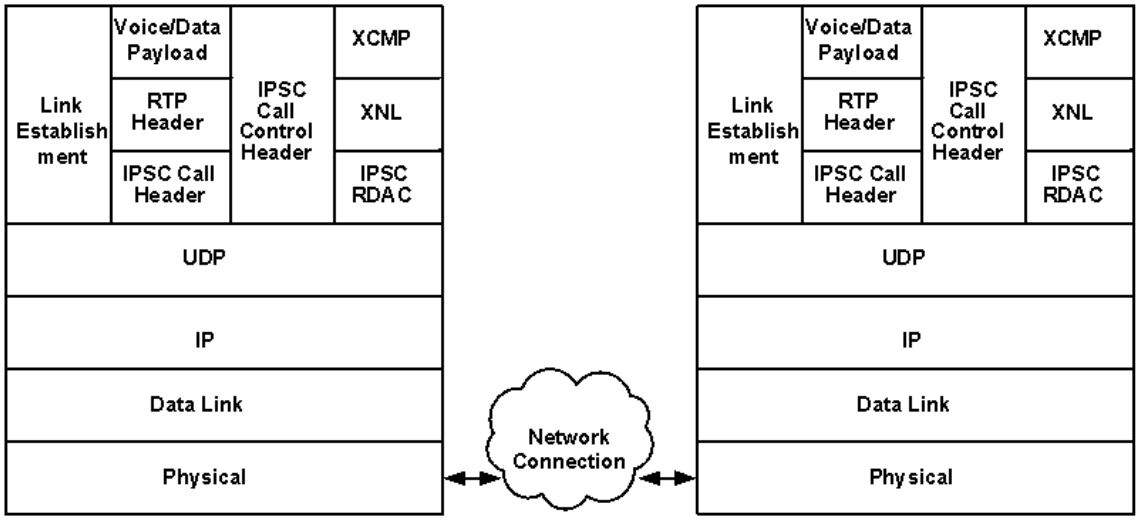


Figure 4 – IP Site Connect Protocol Stack

3.2 Optional Authentication Header

The IP Site Connect system has an optional configuration scheme to support protocol authentication based on SHA-1 for computing a condensed representation of a protocol message, refer to Reference [1] for more details. In cryptography, a keyed-Hash Message Authentication Code (HMAC), is a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-SHA-1 accordingly. The HMAC key is a programmable entity for each IP Site Connect peer configuration and requires them to be identical for link establishment. The authentication header will be a truncated 10 bytes (10 most significant bytes) field based on the SHA-1 and HMAC.

The authentication header is appended to the end of each IP Site Connect packet when authentication is enabled.

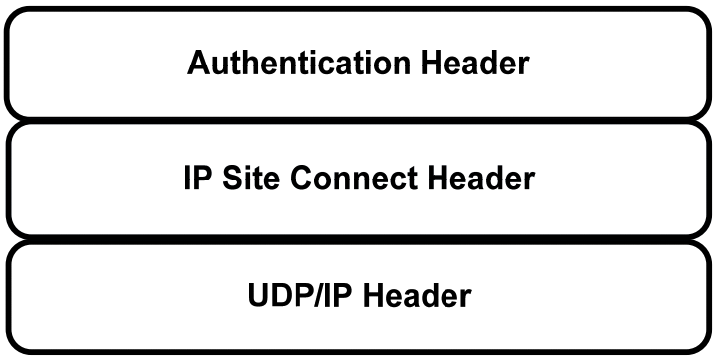


Figure 5 – Authentication Header

Note the releases of MOTOTRBO repeater R1.4, R1.5 and R1.5A use an alternative byte-ordering schema when calculating the HMAC-SHA1 hash, which makes the final computed hash value is different from the standard HMAC-SHA1 calculation. See Appendix A for the detailed MOTOTRBO byte-ordering schema.

Since Release 1.6, the MOTOTRBO repeater complies with the standard HMAC-SHA1 calculation by removing the alternative byte-ordering schema from its implementation.

3.3 Message Structure/Message Classes

Figure 6 shows the IP Site Connect packet format. The IP Site Connect packet contains no addressing information, message length, or frame check sequence. The IP Site Connect protocol depends on the UDP/IP transport layer to provide these services.

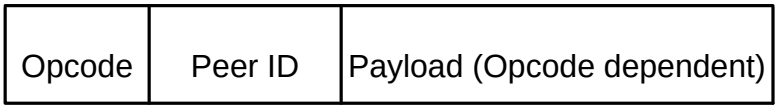


Figure 6 – IP Site Connect Message Format

All IP Site Connect messages have a one-byte opcode that specifies the type of the message, and a four-byte ID of the peer that is sending the message. The payload is entirely dependent on the opcode.

IP Site Connect Opcode:

Based on the purpose of the message, the IP Site Connect messages are divided into four categories:

- Link Establishment message
- Call Control message
- Voice/Data Call
- XCMP/XNL message

The Link Establishment messages establish and maintain the connection between two or more peers in an IP Site Connect network. The Call Control messages and the Voice/Data Call messages are used for voice, data and control call message transmission. The XCMP/XNL message sends XCMP/XNL message over the UDP/IP transport layer.

Table 2 shows all IP Site Connect Opcodes definition.

Opcode	Value	Class	Reference
IPSC_CALL_ALERT_RESP	0x04	Call Control	6.2.2
IPSC_COMMON_CSBK_RESP	0X05	Call Control	6.3.1
IPSC_PVT_CALL_RESP	0x06	Call Control	6.2.3
IPSC_EMRG_ALRM_RESP	0x08	Call Control	6.2.4
IPSC_RAD_MON_RESP	0x0A	Call Control	6.2.5
IPSC_CALL_TRANSMISSION_STATUS	0x61	Call Monitor	7.1.2
IPSC_CALL_CONTROL_NOTIFICATION	0x62	Call Monitor	7.1.3
IPSC_REPEATER_BLOCKED_INDICATION	0x63	Call Monitor	7.1.4
IPSC_XCMP_XNL_DATA	0x70	XCMP/XNL	8.2.1
IPSC_GRP_VOICE_CALL	0x80	Voice/Data Call	6.4.1
IPSC_PVT_VOICE_CALL	0x81	Voice/Data Call	6.4.1
IPSC_GRP_DATA_CALL	0x83	Voice/Data Call	6.4.1
IPSC_PVT_DATA_CALL	0x84	Voice/Data Call	6.4.1
IPSC_ALL_SITE_WAKEUP	0x85	Call Control	6.2.6
LE_MASTER_PEER_REGISTRATION_REQUEST	0x90	Link Establishment	5.2.2
LE_MASTER_PEER_REGISTRATION_RESPONSE	0x91	Link Establishment	5.2.4
LE_NOTIFICATION_MAP_REQUEST	0x92	Link Establishment	5.2.4
LE_NOTIFICATION_MAP_BROADCAST	0x93	Link Establishment	5.2.5
LE_PEER_REGISTRATION_REQUEST	0x94	Link Establishment	5.2.6
LE_PEER_REGISTRATION_RESPONSE	0x95	Link Establishment	5.2.7
LE_MASTER_KEEP_ALIVE_REQUEST	0x96	Link Establishment	5.2.8
LE_MASTER_KEEP_ALIVE_RESPONSE	0x97	Link Establishment	5.2.9
LE_PEER_KEEP_ALIVE_REQUEST	0x98	Link Establishment	5.2.10
LE_PEER_KEEP_ALIVE_RESPONSE	0x99	Link Establishment	5.2.11
LE_DEREGISTRATION_REQUEST	0x9A	Link Establishment	5.2.12
LE_DEREGISTRATION_RESPONSE	0x9B	Link Establishment	5.2.13

Table 2 – IP Site Connect Opcode

3.4 Byte Order

The protocol definitions formatted in this document are based on the most significant bit (as depict below).

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

As a general rule, all fields in an IP Site Connect message will use the integer data type (either signed or unsigned) and they will be transmitted in network byte order (big Endian).

3.5 Opcode Support

The IP Site Connect Protocol defines a set of opcodes to be used for the exchange of information between peers in the system topology. These opcodes are used for maintaining links, transmitting voice call streams, and for command and control related information. Regardless of the opcode type, if a peer receives a UDP packet with an opcode not defined by the IP Site Connect Protocol, then the peer shall drop the packet and take no further actions based on the receipt of the packet.

3.6 Link Protocol Version Support

Starting from R1.6, MOTOTRBO repeater utilizes the link protocol version in the LE protocol to support firmware backward compatibility and identify the system type that the peers join. The link protocol version provides a more robust software release migration for upcoming releases. The peers use the link protocol version automatically at the detection of multiple software release loads. During link establishment, all the peers exchange the link protocol version, and validate the interoperability support. For example, in a MOTOTRBO R1.5 IP Site Connect system, one of the repeaters upgrades to MOTOTRBO R1.6 version, the MOTOTRBO R1.6 repeater uses the R1.5 protocol information to communicate with the MOTOTRBO R1.5 repeater after exchanging link protocol version with the R1.5 repeaters.

Even though the MOTOTRBO repeater releases before R1.6 do not support the link protocol version, the R1.6 and later releases use the link protocol version information of zero to internally identify the peers with these early releases.

The MOTOTRBO repeater supports a maximum depth of current and its three previous major releases. The minor releases between the major releases are counted as part of their associated major release when considering backward compatibility. Beyond this maximum release depth, incompatibility and connectivity issues may happen. In such abnormal scenarios, the non-compatible repeaters have to upgrade to fit in the maximum software release depth. Slight service degradation occurs when multiple MOTOTRBO repeater firmware versions are running in the system.

When upgrading peers to the new software release, since the Master Peer is an autonomous centralized entity in the system, we highly recommend to upgrade the Master Peer first in order to minimize the system downtime, optimize IP link connectivity and improve system access time across the IP network. Otherwise, the peer link establishments can become very lengthy, e.g. 30 minutes (worse case) in a fully loaded IP Site Connect system.

Table 3 shows the link protocol version assignment for each MOTOTRBO system release and the supported versions in each system release. This table is updated at each major system release.

System Release Number	System	Protocol Version	Supported Versions
R1.4	IP Site Connect	0	0
R1.5	IP Site Connect	0	0
	Capacity Plus	0	0
R1.5A	IP Site Connect	0	0
	Capacity Plus	0	0
R1.6	IP Site Connect	1	0, 1
	Capacity Plus	1	0, 1
R1.7	IP Site Connect	2	0, 1, 2
	Capacity Plus	2	0, 1, 2
…	…		

Table 3: Link Protocol Version Supported in Each Release

Under the same major release, all the sub-releases share the same link protocol version. For example, the MOTOTRBO repeater R1.4.1 and R1.4.2 have the same link protocol version of zero.

R1.4, R1.5 and R1.5a repeater firmware have the same link protocol version of zero since the IP Site Connect protocol is the same across these releases. R1.6 firmware is backwards compatible with R1.4, R1.5 and R1.5a since its oldest supported link protocol version is zero.

The Capacity Plus repeater IP interface is available for Link Establishment and RDAC communication since R1.5. The repeater must have R1.7 or beyond firmware to communicate with third party application peer for voice /data / CSBK calls.

The link protocol version has two components: system type and protocol version. In the following message definition sections, a link protocol version table is added at the top of each packet format table. Refer to section 5.3.8 for the detailed definition on link protocol version.

4.0 Key to Message Specification

This section defines the IP Site Connect message specification template that is used to describe each command.

4.1 Message Dashboard

Class	Link Establishment	Type	Request
Opcode	0x90	Command	LE_MASTER_REGISTRATION_REQUEST
Description	Master Registration Request		

At the top of each specification is a dashboard depicting the key characteristics of the IP Site Connect message. The sections of the dashboard are described below:

- Class – Category of the messages that share common properties, operations. The major defined classes are Link Establishment, Voice/Data/Control, and XCMP/XNL.
- Type – Indicates whether the message is a Request, Reply, or Broadcast message type.
- Opcode – Static enumerated value assigned to the message; the size of this value is 1 byte.
- Command – Common alphabetic alias for the message.
- Description – Elaborated definition of the Command assigned to the message.

4.2 Message Field Types

Uint8 – A 8-bit unsigned integer.

Uint16 - A 16-bit unsigned integer.

Uint24 – A 24-bit unsigned integer.

Uint32 - A 32-bit unsigned integer.

String – A NULL terminated array of UCS-2 Unicode characters, unless otherwise specified in the message

4.3 Reserved Fields

Some IP Site Connect messages may have reserved fields identified in the message structure. These fields have been identified for future use and should not be utilized in any way. For any fields marked as “(Reserved)”, the value assigned to that field must be 0x00 up to the length / size of the reserved field. Failure to do so may result in unexpected operation or behavior.

4.4 Packet Format per Link Protocol Version

System	Version Introduced
IP Site Connect	1

At the top of each packet format table is a overhead table identifying its link protocol version.

As described in section 3.6, the message format can be different based on the link protocol version, which has two fields: system ID and protocol version. The MOTOTRBO repeater can only support the current link protocol version and the previous three versions. The third party application shall follow the same backward compatibility depth as the MOTOTRBO repeater peer.

- Version Introduced – The protocol version at which the packet format starts. The Version Introduced is the version protocol field in the link protocol version. If the packet format changes, a separate message format table shows the new format in the new protocol version.

  Note: For Release R1.4, R1.5 and R1.5A, the link protocol version does not exist in the protocol. Protocol version of zero is assigned to these releases, which is used by the R1.6 and later releases to internally identify the peers with these early releases.

- System – The system at which the packet format is supported. It is the system ID in the link protocol version.

5.0 Link Establishment Protocol and Definitions

The section is to define the Link Establishment Protocol Message that is used in the IP Site Connect peers.

The Link Establishment Protocol is supported by the MOTOTRBO repeaters based on MOTOTRBO 1.4 release and higher, regardless of which mode the repeater operates on, when it is configured as an IP Site Connect peer.

5.1 Link Establishment Protocol

The basic format of an IP Site Connect LE packet is shown below:

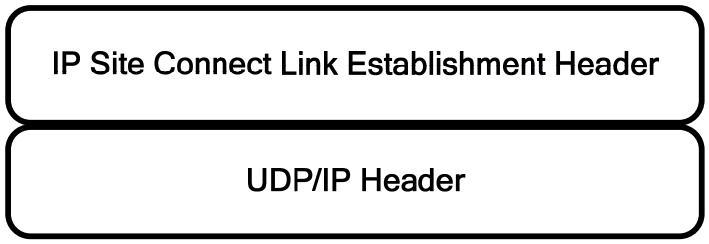


Figure 7 – Basic IP Site Link Establishment Packet Format

The enhanced format of an IP Site Connect LE packet is shown below (which includes configuration scheme when authentication is enabled):

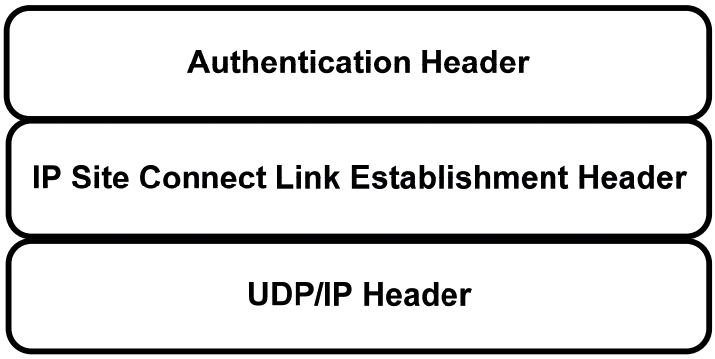


Figure 8– Enhanced IP Site Link Establishment Packet Format

5.1.1 Transaction Types/Message Types

The Link Establishment Protocol allows two transaction types:

- **Request/Response** – a peer makes a request to a Master Peer or another peer, which sends a corresponding response.
- **Broadcast –**sends a message to all linked peers by unicast.

5.1.2 Message Interleaving

The Link Establishment Protocol does not define constraints on when messages can be sent. This means that a peer including the Master Peer is not restricted on what it can send or receive while waiting on a reply to a request.

5.1.3 Message Timeout

Developer should employ timeout mechanisms for the condition in which a peer does not respond to a request message in a timely fashion. This would be considered an error condition in a peer. A timeout allows the device to minimize the time spent waiting before recovery procedures are attempted.

The recommended timer values in this section are based on the IP Site Connect network with the routers listed in section 2.3.

5.2 Link Establishment Message Definitions

5.2.1 Basic Message Format

The basic structure for a Link Establishment Message is shown below.

Field	Type	Description
opcode	Uint8	Specifies the type of the PDU
peerID	Uint32	The ID of the sending peer
Opcode Specific Field 1		
……..		
……..		
Opcode Specific Field N		

All Link Establishment Messages opcodes specify the type of the Message and the ID of the peer sending the Message.

5.2.2 0x90 – LE_MASTER_PEER_REGISTRATION_REQUEST

Class	Link Establishment	Type	Request
Opcode	0x90	Command	LE_MASTER_PEER_REGISTRATION_REQUEST
Description	Master Peer Registration Request		

5.2.2.1. Description

This message is used to register with the Master Peer.

A peer sends out an LE_MASTER_PEER_REGISTRATION_REQUEST in one of the following situations:

1) When the peer first powers up
2) When a peer stops receiving keep alive data from another peer
3) When a peer stops receiving keep alive data from the Master Peer
4) When the Master Peer fails to respond to a LE_MASTER_PEER_REGISTRATION_REQUEST

The LE_MASTER_PEER_REGISTRATION_REQUEST is only sent from a peer to the Master Peer. If a peer stops sending keep alive data, the other peers send a registration request to the Master Peer to re-register. After getting the updated information, the sending peer proceeds based on the number of peers currently in the system. The Master Peer subsequently sends a notification map broadcast containing the latest peer information.

After the peer sends LE_MASTER_PEER_REGISTRATION_REQUEST, it starts the MasterPeerRegister Timer. If the Master Peer fails to respond the LE_MASTER_PEER_REGISTRATION_REQUEST before timeout, the peer resends the LE_MASTER_PEER_REGISTRATION_REQUEST. If the peer's current link protocol version is higher than zero and the peer can support the link protocol version of zero, it shall resends the LE_MASTER_PEER_REGISTRATION_REQUEST with link protocol version of zero, which does not have the protocol version field. After the peer receives the LE_MASTER_PEER_REGISTRATION_RESPONSE with link protocol version of zero, it sends the LE_MASTER_PEER_REGISTRATION_REQUEST with the current link protocol version again. This process stops when one of the following conditions is met:

1) The peer receives three consecutive LE_MASTER_PEER_REGISTRATION_RESPONSE messages with link protocol version of zero. The peer uses the IPSC message with link protocol version of zero to communicate with the Master Peer.
2) The peer receives a LE_MASTER_PEER_REGISTRATION_RESPONSE message with link protocol version field. The peer uses the IPSC message with link protocol version of acceptedLinkProtocolVersion in the LE_MASTER_PEER_REGISTRATION_RESPONSE to communicate with the Master Peer.

There is no limit on the setting of the MasterPeerRegister Timer. The MOTOTRBO repeaters use 10 seconds for this timer.

401

402 #### 5.2.2.2. Cautions / Warnings

403 None

404 #### 5.2.2.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x90	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint16	The services supports of the sending peer.	5.3.7

405

System	Version Introduced
IP Site Connect	1
Capacity Plus	1

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x90	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint32	The services supports of the sending peer.	5.3.7
10	currentLinkProtocolVersion	Uint16	The field that represents the current working protocol version that the peer supports for messaging between peers.	5.3.8
12	oldestLinkProtocolVersion	Uint16	The field that represents the oldest working protocol version that the peer can support exchanging with another peer.	5.3.8

5.2.3 0x91 – LE_MASTER_PEER_REGISTRATION_RESPONSE

Class	Link Establishment	Type	Response
Opcode	0x91	Command	LE_MASTER_PEER_REGISTRATION_RESPONSE
Description	Master Peer Registration Response		

5.2.3.1. Description

This message is used to respond the register request of the sending peer.

The Master Peer sends out an LE_MASTER_PEER_REGISTRATION_RESPONSE in the following situation:

1) Upon receiving an LE_MASTER_PEER_REGISTRATION_REQUEST

The LE_MASTER_PEER_REGISTRATION_ RESPONSE is sent from the Master back to the requesting peer only. If the Master Peer is attempting to establish a link with another peer when it receives an LE_MASTER_PEER_REGISTRATION_REQUEST, it does not respond. After the Master Peer has finished establishing the link, it responds to the next LE_MASTER_PEER_REGISTRATION_REQUEST issued by the sending peer.

The LE_MASTER_PEER_REGISTRATION_RESPONSE contains the current operating modes and supported services of the Master Peer. The receiving peer shall use this information to update its local map with information about the Master Peer.

When receiving a LE_MASTER_PEER_REGISTRATION_REQUEST with link protocol version field, if the Master Peer can support at least one of the protocol versions from the LE_MASTER_PEER_REGISTRATION_REQUEST, it chooses the biggest common protocol version as the acceptedLinkProtocolVersion in the LE_MASTER_PEER_REGISTRATION_RESPONSE.

If the Master Peer does not support the message format of the LE_MASTER_PEER_REGISTRATION_REQUEST or the range of the link protocol version in the LE_MASTER_PEER_REGISTRATION_REQUEST, the Master Peer silently discards the LE_MASTER_PEER_REGISTRATION_REQUEST without sending LE_MASTER_PEER_REGISTRATION_RESPONSE.

The MOTOTRBO repeater can support the repeater peers with the current software release and three previous major releases. We recommend the third party application peers to use the current link protocol version and three previous link protocol versions as their version support range.

5.2.3.2. Cautions / Warnings

None.

436

5.2.3.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x91	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint16	Services supports of the sending peer	5.3.7
8	numPeers	Uint16	The number of peers that have established links with the Master Peer	5.3.2

437

System	Version Introduced
IP Site Connect	1
Capacity Plus	1

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x91	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint32	Services supports of the sending peer	5.3.7
10	numPeers	Uint16	The number of peers that have established links with the Master Peer	5.3.2
12	acceptedLinkProtocolVersion	uint16	The field that represents the common protocol version accepted for messaging between peers.	5.3.8
14	oldestLinkProtocolVersion	uint16	The field that represents the oldest working protocol version that the peer can support exchanging with another peer.	5.3.8

5.2.4 0x92 – LE_NOTIFICATION_MAP_REQUEST

Class	Link Establishment	Type	Request
Opcode	0x92	Command	LE_NOTIFICATION_MAP_REQUEST
Description	Master Peer Map Request		

5.2.4.1. Description

This message is used to request the IP Site Connect System Map information.

A peer sends out an LE_NOTIFICATION_MAP_REQUEST in the following situation:
1) When it receives an LE_MASTER_PEER_REGISTRATION_RESPONSE where the number of linked peers value is greater than zero.

The LE_NOTIFICATION_MAP_REQUEST is sent from a peer to the Master Peer. The request normally follows an LE_MASTER_PEER_REGISTRATION_ RESPONSE when there are one or more linked peers in the system. Otherwise, when the linking peer is the first peer in the system, then notification of the current peer map is not requested.

The peer map is only requested when updated information about the state of the linked peers is needed. For example, when a peer stops receiving keep alive data from another peer for a predetermined amount of time (typical 60s) it sends LE_MASTER_PEER_REGISTRATION_REQUEST and gets a new peer map to decide whether this peer has actually become disconnected from the network or simply changed its IP address or port number.

5.2.4.2. Cautions / Warnings

None.

5.2.4.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x92	
1	peerID	Uint32	The ID of the sending peer	5.3.1

5.2.5 0x93 – LE_NOTIFICATION_MAP_BROADCAST

Class	Link Establishment	Type	Broadcast
Opcode	0x93	Command	LE_NOTIFICATION_MAP_BROADCAST
Description	Master Peer Map Broadcast		

5.2.5.1. Description

This message is used to broadcast the IP Site Connect System Map information.

The Master Peer sends out an LE_NOTIFICATION_MAP_BROADCAST in one of the following situations:

1) Upon receiving an LE_NOTIFICATION_MAP_REQUEST
2) After sending an LE_MASTER_PEER_DEREGISTRATION_RESPONSE

The LE_NOTIFICATION_MAP_BROADCAST is always sent from the Master Peer to all linked peers in the system including the peer currently establishing a link to the Master Peer. The receiving peers then update their peer map and establish links to any newly identified peers. Or, they re-establish links with peers containing updated information (i.e. new IP address, different port).

When the Master Peer receives a Deregistration Request, it sends a Deregistration Response to the requesting peer followed by an updated peer map to all of the peers in the system with the requesting peer removed from the map. However, peers shall only remove peers from their local map when they receive a Deregistration Request or they fail to receive Peer Keep Alive Responses after a predetermined number of Peer Keep Alive Requests are sent.

Note the System Map in the LE_NOTIFICATION_MAP_BROADCAST does not contain an entry for the Master Peer.

5.2.5.2. Cautions / Warnings

None.

479 **5.2.5.3. Packet Format**

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x93	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	mapLength	Uint16	The number of bytes that will be contained in the following peer map	5.3.3
7	remotePeerID (1)	Uint32	The ID of the peer that established a link to the Master Peer	5.3.1
11	remoteIPAddr (1)	Uint32	The IP address of this peer as seen to the public internet (i.e. router address)	5.3.4
15	remotePort (1)	Uint16	The port address of this peer as seen to the public internet (i.e. router port)	5.3.5
17	peerMode(1)	Uint8	The field represents the current operating modes of the peer	5.3.6
	……..			
	……..			
(N-1) *11+7	remotePeerID (N)	Uint32	The ID of this peer that established a link to the Master Peer	5.3.1
(N-1) *11+11	remoteIPAddr (N)	Uint32	The IP address of this peer as seen to the public internet (i.e. router address)	5.3.4
(N-1) *11+15	remotePort (N)	Uint16	The port address of this peer as seen to the public internet (i.e. router port)	5.3.5
(N-1) *11+17	peerMode(N)	Uint8	The field represents the current operating modes of the peer	5.3.6

5.2.6 0x94 – LE_PEER_REGISTRATION_REQUEST

Class	Link Establishment	Type	Request
Opcode	0x94	Command	LE_PEER _REGISTRATION_REQUEST
Description	Peer Registration Request		

5.2.6.1. Description

This message is used to register with another peer.

A peer sends out an LE_PEER_REGISTRATION_REQUEST to another peer in the following situation:

1) Upon receiving an LE_NOTIFICATION_MAP_BROADCAST identifying new or updated peers

The LE_PEER_REGISTRATION_REQUEST is only sent from one peer to another peer, but not to the Master Peer. When a new peer map from the Master Peer identifies a newly linked peer or a peer with new IP address or port number, it shall attempt to establish a link based on the latest information.

After the peer sends LE_PEER_REGISTRATION_REQUEST, it starts the PeerRegister Timer. If another peer fails to respond the LE_PEER_REGISTRATION_REQUEST before timeout, the peer will resend the LE_PEER_REGISTRATION_REQUEST.

If the peer's current link protocol version is higher than zero and supports the link protocol version of zero, when it receives LE_PEER_REGISTRATION_REQUEST without link protocol version field, it shall take the following actions:

1) Send the LE_PEER_REGISTRATION_RESP without link protocol version field
2) Stop the current PeerRegister Timer for the LE_PEER_REGISTRATION_REQUEST with link protocol version field
3) Send the LE_PEER_REGISTRATION_REQUEST without link protocol version field.
4) Start the PeerRegister Timer

There is no limit on the setting of the PeerRegister Timer. The MOTOTRBO repeaters use 1 second for this timer.

5.2.6.2. Cautions / Warnings

None.

507

5.2.6.3. Packet Format

System		Version Introduced		
IP Site Connect		0		
Capacity Plus		0		
Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x94	
1	peerID	Uint32	The ID of the sending peer	5.3.1

508

System		Version Introduced		
IP Site Connect		1		
Capacity Plus		1		
Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x94	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	currentLinkProtocolVersion	uint16	The field that represents the current working protocol version that the peer supports for messaging between peers.	5.3.8
7	oldestLinkProtocolVersion	uint16	The field that represents the oldest working protocol version that the peer can support exchanging with another peer.	5.3.8

509

5.2.7 0x95 – LE_PEER_REGISTRATION_RESPONSE

Class	Link Establishment	Type	Response
Opcode	0x95	Command	LE_PEER_REGISTRATION_RESPONSE
Description	Peer Registration Response		

5.2.7.1. Description

This message is used to respond the register request of a peer.

A peer sends out an LE_PEER_REGISTRATION_RESPONSE in the following situation:

1) Upon receiving an LE_PEER_REGISTRATION_REQUEST

The LE_PEER_REGISTRATION_RESPONSE is only sent from a peer back to the requesting peer. When the requesting peer receives an LE_PEER_REGISTRATION_RESPONSE, it shall consider that a link has been established with the responding peer.

When receiving a LE_PEER_REGISTRATION_REQUEST with link protocol version field, if the receiving peer can support at least one of the protocol versions from the LE_PEER_REGISTRATION_REQUEST, it chooses the biggest common protocol version as the acceptedLinkProtocolVersion in the LE_PEER_REGISTRATION_RESPONSE.

If the receiving peer does not support the message format of the LE_PEER_REGISTRATION_REQUEST or the range of the link protocol version in the LE_PEER_REGISTRATION_REQUEST, the receiving peer silently discards the LE_PEER_REGISTRATION_REQUEST without sending LE_PEER_REGISTRATION_RESPONSE.

The MOTOTRBO repeater supports the repeater peers with the current software release and three previous major releases. We recommend the third party application peer to use the current link protocol version and three previous link protocol versions as their version support range.

5.2.7.2. Cautions / Warnings

None.

534 #### 5.2.7.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x95	
1	peerID	Uint32	The ID of the sending peer	5.3.1

535

System	Version Introduced
IP Site Connect	1
Capacity Plus	1

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x95	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	acceptedLinkProtocolVersion	Uint16	The field that represents the common protocol version accepted for messaging between peers.	5.3.8
7	oldestLinkProtocolVersion	Uint16	The field that represents the oldest working protocol version that the peer can support exchanging with another peer.	5.3.8

536

5.2.8 0x96 – LE_MASTER_PEER_KEEP_ALIVE_REQUEST

Class	Link Establishment	Type	Request
Opcode	0x96	Command	LE_MASTER_PEER_KEEP_ALIVE_REQUEST
Description	Master Peer Keep Alive Request		

5.2.8.1. Description

This message is used to request the keep alive with the Master Peer.

A peer sends out this message in one of the following situations:

1) Upon receiving an LE_NOTIFICATION_MAP_BROADCAST from the Master Peer
2) Upon receiving an LE_MASTER_PEER_REGISTRATION_RESPONSE from the Master Peer when the number of linked peers is less than one
3) Upon receiving an LE_MASTER_PEER_KEEP_ALIVE_RESPONSE from the Master Peer.
4) Upon the MasterPeer KeepAlive Timer times out.

The LE_MASTER_PEER_KEEP_ALIVE_REQUEST is only sent from a peer to the Master Peer. However, the LE_MASTER_PEER_KEEP_ALIVE_REQUEST is not immediately sent following the above messages. Instead, the peer waits a predetermined amount of time (typical 15s) before proceeding to send the Keep Alive Request.

The LE_MASTER_PEER_KEEP_ALIVE_REQUEST also contains the peer mode and peer services fields. The Master Peer uses this information to rebuild the peer map when it encounters a fault and resets. A peer can also use this information to re-register with the Master Peer after the fault occurs.

When a peer encounters a fault scenario and resets at the same time as the Master Peer, it shall attempt to re-register with the Master Peer after resetting. The same is true for the case when the peer changes its peer mode and/or peer service bits at the same time as the Master Peer encounters a fault scenario and resets.

After the peer joins the IP Site Connect system, it starts the MasterPeerKeepAlive Timer. When the MasterPeerKeepAlive Timer times out, the peer sends LE_MASTER_PEER_KEEP_ALIVE_REQUEST to the Master Peer. After the peer does not receive the LE_MASTER_PEER_KEEP_ALIVE_RESPONSE for 3 times continuously from the Master Peer, the peer considers the link is down and starts the registration process by sending the LE_MASTER_PEER_REGISTRATION_REQUEST to the Master Peer.

There is no limit on the setting of the MasterPeerKeepAlive Timer. The MOTOTRBO repeaters use 15 seconds for this timer.

5.2.8.2. Cautions / Warnings

None.

572 #### 5.2.8.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x96	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint16	Services supports of the sending peer	5.3.7

573

System	Version Introduced
IP Site Connect	1
Capacity Plus	1

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x96	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint32	Services supports of the sending peer	5.3.7
10	currentLinkProtocolVersion	Uint16	The field that represents the current working protocol version that the peer supports for messaging between peers.	5.3.8
12	oldestLinkProtocolVersion	Uint16	The field that represents the oldest working protocol version that the peer can support exchanging with another peer.	5.3.8

574

5.2.9 0x97 – LE_MASTER_PEER_KEEP_ALIVE_RESPONSE

Class	Link Establishment	Type	Response
Opcode	0x97	Command	LE_MASTER_PEER_KEEP_ALVIE _RESPONSE
Description	Master Peer Keep Alive Response		

5.2.9.1. Description

This message is used to respond the request of a peer.

The Master Peer sends out an LE_MASTER_PEER_KEEP_ALIVE_RESPONSE in the following situation:

1) Upon receiving an LE_MASTER_PEER_KEEP_ALIVE_REQUEST

The LE_MASTER_PEER_KEEP_ALIVE_RESPONSE is only to be sent from the Master Peer back to the requesting peer. When a peer receives the LE_MASTER_PEER_KEEP_ALIVE_RESPONSE from the Master Peer, it confirms that a link has been established with the Master Peer.

The LE_MASTER_PEER_KEEP_ALIVE_RESPONSE contains the current operating modes, and supporting services of the Master Peer. The receiving peer uses this information as necessary to update its local map with information about the Master Peer.

5.2.9.2. Cautions / Warnings

None.

591 #### 5.2.9.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x97	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint16	Services supports of the sending peer	5.3.7

592

System	Version Introduced
IP Site Connect	1
Capacity Plus	1

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x97	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint32	Services supports of the sending peer	5.3.7
10	acceptedLinkProtocolVersion	Uint16	The field that represents the common protocol version accepted for messaging between peers.	5.3.8
12	oldestLinkProtocolVersion	Uint16	The field that represents the oldest working protocol version that the peer can support exchanging with another peer.	5.3.8

593

5.2.10 0x98 – LE_PEER_KEEP_ALIVE_REQUEST

Class	Link Establishment	Type	Request
Opcode	0x98	Command	LE_PEER_KEEP_ALIVE_REQUEST
Description	Peer Keep Alive Request		

5.2.10.1. Description

This message is used to request the keep alive with the peer.

A peer sends out an LE_PEER_KEEP_ALIVE_REQUEST to another peer in the following situation:

1) Upon receiving an LE_PEER_REGISTRATION_RESPONSE from another peer

A peer sends a LE_PEER_KEEP_ALIVE_REQUEST to another peer after receiving the LE_PEER_REGISTRATION_RESPONSE from another peer. However, the LE_PEER_KEEP_ALIVE_REQUEST is not immediately sent following the receipt of any IP Site Connect Protocol messages. Instead, the peer waits a predetermined amount of time (typical 6s) before proceeding to send the next LE_PEER_KEEP_ALIVE_REQUEST.

After the peer joins the IP Site Connect system, it starts the PeerKeepAlive Timer for each non-Master peer in the system. When the PeerKeepAlive Timer times out, the peer sends LE_PEER_KEEP_ALIVE_REQUEST to another peer in the system. After the peer does not receive the LE_PEER_KEEP_ALIVE_RESPONSE for 10 times continuously from another peer, the peer considers the link is down and starts the registration process by sending the LE_MASTER_PEER_REGISTRATION_REQUEST to the Master Peer.

There is no limit on the setting of the PeerKeepAlive Timer. The MOTOTRBO repeaters use 6 seconds for this timer.

5.2.10.2. Cautions / Warnings

None.

5.2.10.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x98	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint16	Services supports of the sending peer	5.3.7

System	Version Introduced
IP Site Connect	1
Capacity Plus	1

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x98	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint32	Services supports of the sending peer	5.3.7

620 ## 5.2.11 0x99 – LE_PEER_KEEP_ALIVE_RESPONSE

Class	Link Establishment	Type	Response
Opcode	0x99	Command	LE_PEER_KEEP_ALVIE_RESPONSE
Description	Peer Keep Alive Response		

621 ### 5.2.11.1. Description

622 This message is used to respond the request of a peer.

623 A peer sends out an LE_PEER_KEEP_ALIVE_RESPONSE in the following situation:

624 1) Upon receiving an LE_PEER_KEEP_ALIVE_REQUEST

625 The LE_PEER_KEEP_ALIVE_RESPONSE is only sent from a peer back to the
626 requesting peer. A peer stops receiving a LE_PEER_KEEP_ALIVE_RESPONSE when
627 its link with another peer goes down.

628 ### 5.2.11.2. Cautions / Warnings

629 None.

630 ### 5.2.11.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x99	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint16	Services supports of the sending peer	5.3.7

631

System	Version Introduced
IP Site Connect	1
Capacity Plus	1

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x99	
1	peerID	Uint32	The ID of the sending peer	5.3.1
5	peerMode	Uint8	The current operating modes of the sending peer	5.3.6
6	peerServices	Uint32	Services supports of the sending peer	5.3.7

632

5.2.12 0x9A – LE_DEREGISTRATION_REQUEST

Class	Link Establishment	Type	Request
Opcode	0x9A	Command	LE_DEREGISTRATION_REQUEST
Description	Deregistration Request		

5.2.12.1. Description

This message is used to deregister with the Master Peer or other peer.

A peer sends out an LE_DEREGISTRATION_REQUEST in the following situation:

1) Whenever it desires to remove itself from the IP Site Connect system

The LE_DEREGISTRATION_REQUEST is sent from a peer to the Master Peer or other peers. A peer only sends a LE_DEREGISTRATION_REQUEST when it wants to be immediately removed from the system and to notify all peers to stop sending packets to it. This is normally only utilized by peers that are running on a PC environment. The MOTOTRBO repeater does not send the LE_DEREGISTRATION_REQUEST.

Without this message a peer is automatically removed from the peer maps in each linked peer after a predetermined inactivity timeout period (typical 60s) by the Master Peer or other peers. This is important to note that an updated peer map from the Master Peer with a peer removed does not cause the others peers to remove the peer from their map just because communications with the Master Peer failed and the peer was removed the Master Peer map. Instead, each peer shall independently decide whether a peer is to be removed from its peer map either by inactivity timeout or the use of the deregistration request.

It is recommended that this message shall be sent to the Master Peer first and then to all non-Master Peers. Otherwise, the Master Peer could send out a peer map with the to-be-removed peer to a peer that just updated its own peer map based on the deregistration message. When this happens, the receiving peer identifies the to-be-removed peer as a new peer in the system and attempts to re-establish a link with this peer even though it just removes the to-be-removed peer from its map table. Deregistration of the peer still occurs, but is less efficient.

5.2.12.2. Cautions / Warnings

None.

5.2.12.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x9A	
1	peerID	Uint32	The ID of the sending peer	5.3.1

5.2.13 0x9B – LE_DEREGISTRATION_RESPONSE

Class	Link Establishment	Type	Response
Opcode	0x9B	Command	LE_DEREGISTRATION_RESPONSE
Description	Deregistration Response		

5.2.13.1. Description

This message is used to respond the request of a peer.

The Master Peer or a peer will send out an LE_DEREGISTRATION_RESPONSE in the following situation:

1) Upon receiving an LE_DEREGISTRATION_REQUEST

The LE_DEREGISTRATION_RESPONSE is only sent from the Master Peer or a peer back to the requesting peer. Once the requesting peer receives LE_DEREGISTRATION_RESPONSE from every linked peer in the system, it can be safely removed from the system. It then proceeds with any other shutdown procedures. When the requesting peer fails to receive the LE_DEREGISTRATION_RESPONSE from all other peers, it may optionally retry or proceed with shutting down.

5.2.13.2. Cautions / Warnings

None.

5.2.13.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x9B	
1	peerID	Uint32	The ID of the sending peer	5.3.1

5.3 Information Fields

5.3.1 Unique Master or Peer Identifier (peerID and remotePeerID)

This field specifies the identity of a peer or the Master Peer. It is a 32-bit unsigned integer in network byte order.

Peer ID Value	Allocation
0x00000000	RESERVED
0x00000001 to 0xFFFFFFFE	Valid Range
0xFFFFFFFF	RESERVED

Table 4 - Peer ID Allocation

5.3.2 Number of Linked Peers (numPeers)

This field indicates the number of peers that have established a links with the Master Peer. Since the IPv4 Protocol limits the UDP data length to 65,507 bytes, the maximum number peers is limited to 5,037 (or 0x13AD). This value is calculated by taking the maximum UDP data length (65,507) and subtracting the LE Header size (5) and map length (4) and then dividing this value by the number of bytes per peer map entry (13).

Number of Peers Value	Allocation
0x0000 to 0x13AD	Valid Range
0x13AE to 0xFFFF	RESERVED

Table 5 - Number of Linked Peers Allocation

5.3.3 Peer Map Length (mapLength)

This field indicates the total length of the Peer Map sent from the Master Peer. Since the IPv4 Protocol limits the UDP data length to 65,507 bytes, the maximum peer map length is 65,481(or 0xFFC9).

Map Length Values	Allocation
0x0000 to 0xFFC9	Valid Range
0xFFCA to 0xFFFF	RESERVED

Table 6 - Map Length Allocation

5.3.4 Peer IP Address (remoteIPAddr)

This field identifies the IP Address of a peer in the system. The actual allocation for the IP address shall adhere to that defined by the IPv4 Protocol. The following is an example of how the common logical decimal representation compares to the physical packet representation in hexadecimal.

If the peer is behind a firewall, the Peer IP Address is router's IP Address.

Physical Representation	Logical Representation
0x0A029636	10.2.150.54

Table 7 - Peer IP Address Representation

5.3.5 Peer IP Port Address (remotePort)

This field represents UDP IPv4 Port Address/Number used by a peer or the Master Peer in the system. The IPv4 Protocol limits the port address range to be from 0 to 65,535. Port addresses 0 to 49,151 are already reserved for the Well Known Ports or the Registered Ports. So the Link Establishment protocol will use port addresses 49,152 to 65,535 (also used for temporary usage between clients and servers).

If the peer is behind a firewall, the peer IP Port Address is router's IP Port Address.

Map Length Values	Allocation
0x0000 to 0xBFFF	RESERVED
0xC000 to 0xFFFF	Valid Range

Table 8 - IP Port Address Allocation

5.3.6 Peer Mode Bit Field (peerMode)

This field specifies current operating mode information associated with this peer. There are four different modes specified in this field. Each mode indicator represents 2 bits.

Peer Mode Bit	Peer Mode Bit Name
0	Slot 2 Assignment[1]
1	Slot 2 Assignment[2]
2	Slot 1 Assignment[1]
3	Slot 1 Assignment[2]
4	Current Signaling Mode[1]
5	Current Signaling Mode[2]
6	Peer Status[1]
7	Peer Status[2]

Table 9 - Peer Mode Bit Allocation

The Slot Assignment fields are located near the least significant bit position, and the Peer Status fields are located near the most significant bit position.

5.3.6.1. Slot Assignment

This field will contain two bits to indicate the slot assignment information regarding use for IP Site Connect call support, local site call support only, or no call support on this peer (i.e. an RDAC peer).

Value	Allocation
0b00	No Call Support
0b01	Local Site Call Support Only
0b10	IP Site Connect Call Support
0b11	RESERVED

Table 10 - Slot Assignment Bit Allocation

5.3.6.2. Current Signaling Mode

This field will contain two bits to indicate the current RF signaling mode information pertaining to the Analog or Digital modes of operation. A peer can also indicate that it has no RF support.

Value	Allocation
0b00	No RF Support
0b01	Analog Mode
0b10	Digital Mode
0b11	RESERVED

Table 11 - Current Signaling Mode Bit Allocation

5.3.6.3. Peer Status

This field contains two bits to indicate whether a peer is currently disabled or enabled. When a peer is disabled, it only supports Link Establishment and some peer services (i.e. RDAC and other XCMP/XNL services). It does not support voice, data, or CSBK calls when disabled.

Value	Allocation
0b00	Disabled
0b01	Enabled
0b10	Knocked Down
0b11	Locked

Table 12 - Peer Status Bit Allocation

Enabled Status: Repeater is in the normal mode of transmitting, receiving and repeating. Repeater is capable of transmitting, receiving and repeating operations.

Knocked Down Status: Repeater does not repeat received signals, but is capable of receiving and transmitting through an external PTT.

Disabled Status: Repeater does not perform transmitting, receiving and repeating operations.

Locked Status: Repeater is in a failure mode, in which transmitting, receiving and/or repeating capabilities have failed.

5.3.7 Peer Services Bit Field (peerServices)

This field specifies the services supported by the associated peer. When a bit is enabled or set to 1, the associated service is supported by the peer. Otherwise, the service is not supported by the peer.

Each peer defines which services it supports during the registration process with other peers in the system. A peer can selectively decide which services it wants to support on a one-to-one basis. For example, Peer A registers with Peer B for receiving voice and data call messages; and registers with Peer C for only receiving voice call messages.

The Voice, Data and CSBK Call services require a peer that can handle digital services similar to an embedded peer that supports digital RF signaling. Bit 0 represents the least significant bit in the 4-byte field.

754

Peer Services Bit	Peer Service Name	Description
The following 16 bits are allocated or reserved for support by all releases		
0	Primary Master Peer	Indicates a peer acts as a Master Peer for the system.
1	RESERVED	
2	Voice Call	The peer supports receiving packets related to voice calls. To respond, this peer needs to support interpreting DMR control data and encoding and decoding AMBE voice data.
3	Data Call	The peer supports receiving packets related to data calls. To respond, this peer will need to support interpreting DMR control data and ARS for digital data calls.
4	Packet Authentication	This bit should indicate whether Authentication is enabled on the peer. If this bit does not match that of the Master Peer, then a peer should not be allowed to join the IP Site Connect Network.
5	XNL Slave Device	This bit indicates whether this peer is capable of being an XNL Slave device.
6	XNL Master Device	This bit indicates whether this peer is capable of being an XNL Master device. Only the repeater peer can be the XNL Master Device.
7	XNL Master Connection Status	This bit indicates whether this peer has established an XNL connection with the Master Peer.
8	Slot 1 Assignment in Capacity Plus	Only applicable for Capacity Plus repeater peer. This bit indicates whether this peer supports Capacity Plus channel in slot 1.
9		
10	Slot 2 Assignment in Capacity Plus	Only applicable for Capacity Plus repeater peer.,This bit indicates whether this peer supports Capacity Plus channel in slot 2
11		
12	RESERVED	
13	Remote 3rd Party Console Application	This bits indicates that the peer is a remote 3rd party application peer.
14	Repeater Call Monitoring	This bit indicates that the peer wants to receive the repeater call monitoring messages that can be used for billing or diagnostic purposes.
15	CSBK Call	The peer supports receiving packets related to digital CSBK calls. To respond, this peer will need to support interpreting DMR CSBK calls.
The following 16-bits are reserved for usage by releases post-R1.6		
16-17	RESERVED	
18	Virtual Peer	Only applicable for Capacity Plus repeater peer. This bit indicates whether this peer is a virtual peer or not
19-31	RESERVED	

755 **Table 13 - Peer Services Bit Allocation**

756 Before link protocol version 2, when a peer registers the Data Call service it receives
757 both data and CSBK call. Starting from link protocol version 2, the peer has to register
758 the CSBK Call service to receive the CSBK call.

759 The XNL Slave Device bit and the XNL Master Device bit indicate if the peer, which
760 sends the registration request, supports XNL message communication and the roles in

the XNL communication. A peer cannot be both an XNL Master Device and an XNL Slave Device at the same time. Therefore, the XNL Slave Device bit and the XNL Master Device bit shall not be set on the same peer. The MOTOTRBO repeater peer is always the XNL Master Device. The third party application can only be XNL Slave Device. The XNL Connection Status bit is set to 1 when a peer has established an XNL connection with a remote peer. After establishing the XNL connection, if the XNL is dropped due to peer reset or other reason, the XNL Connection Status bit is set to 0 in both the LE registration request and the keep alive messages until the XNL is re-established.

The Remote 3rd Party Console Application service bit must set to 1 in the Capacity Plus system. The MOTOTRBO Repeater peers will not send call traffic to the repeater peers. The MOTOTRBO Repeater peers use this bit to determine if a console peer exists or not and distinguish the console peer from other repeater peers. In both IPSC system and Capacity Plus system, the application peer has to register the Remote 3rd Party Console Application service to send out the IP Console Inhabit / Uninhabit commands.

Peer Service Name	MOTOTRBO Repeater Peer		RDAC Peer		Third Party Console Application	
	IP Site Connect	Capacity Plus	IP Site Connect	Capacity Plus	IP Site Connect	Capacity Plus
Primary Master Peer	Optional	Optional (one of the repeater has to be the master peer)	Optional	No	Optional	No
Voice Call	Yes	No	No	No	Optional	Optional
Data Call	Yes	No	No	No	Optional	Optional
Packet Authentication	Optional	Optional	Optional	Optional	Optional	Optional
XNL Slave Device	No	No	Yes	Yes	Optional	Optional
XNL Master Device	Yes	Yes	No	No	No	No
XNL Master Connection Status	Optional (Depend on the XNL connection status)	Optional (Depend on the XNL connection status)	Optional (Depend on the XNL connection status)	Optional (Depend on the XNL connection status)	Optional (Depend on the XNL connection status)	Optional (Depend on the XNL connection status)

Peer Service Name	MOTOTRBO Repeater Peer		RDAC Peer		Third Party Console Application	
	IP Site Connect	Capacity Plus	IP Site Connect	Capacity Plus	IP Site Connect	Capacity Plus
Primary Master Peer	Optional	Optional (one of the repeater has to be the master peer)	Optional	No	Optional	No
Slot 1 Assignment in Capacity Plus	No	Yes	No	No	No	No
Slot 2 Assignment in Capacity Plus	No	Yes	No	No	No	No
Remote 3rd Party Console Application	No	No	No	No	Optional	Yes
Repeater Call Monitoring	No	No	No	No	Optional	Optional
CSBK Call	Yes	No	No	No	Optional	Optional
Virtual Peer	No	Optional	No	No	No	No

Table 14: Service Bit Usage in the Peers

In Table 14, No means the bit must set to 0, Yes means the bit must set to 1, Optional means the bit can be set to either No or Yes.

For the Primary Master Peer bit, only one of the peers in the system can set this bit to Yes. For the Packet Authentication bit, all the peers in the system must have the same setting. For the Virtual Peer bit, it is set only when the repeater peer finds out there is no entry for the virtual peer in the Master's system map, and the repeater initiates the LE registration on behalf of the virtual peer.

The RDAC peer in Table 14 only provides the RDAC related functions. The third party console application in Table 14 only provides voice/data/CSBK related functions. It is possible to have a third party application to have both RDAC and voice/data/CSBK related functions. In this case, the following rules shall be used:

- No + No = No
- No + Optional = Optional

- No + Yes = Yes
- Yes + Optional = Yes
- Yes + Yes = Yes

For example, the XNL Slave Service bit must set to Yes, and the Voice Call bit can be Optional for the application with both RDAC and voice/data/CSBK functions.

5.3.8 Link Protocol Version Bit Field (Link Protocol Version)

This field is used to exchange link protocol version information for the accepted, current, and oldest supported versions. The link protocol version has two components: system ID and version information, which are used to determine the message structure and procedure in the multi-software-version system interactions. Each PDU is defined to support a specific system ID and protocol in section 5.2.

The overall field size is 16 bits that is broken into the 10-bit version information field and 6-bit system ID field as shown in Figure 9:

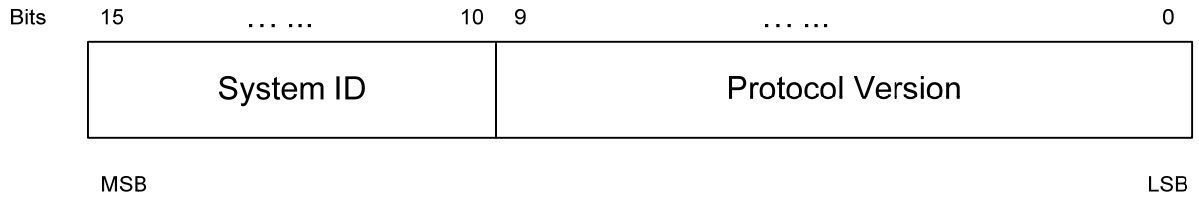


Figure 9: Link Protocol Version Bits

A bit mask of 0xFC00 can be used to derive the System ID from the Link Protocol Version field. A bit mask of 0x03FF can be used to derive the version information value from the Link Protocol Version field. The system ID field allows for the definition of up to 63 unique systems. The version information field allows for 1023 possible versions of the protocol for each system ID.

Link Protocol Version Bits	Link Protocol Version Name	Description
0-9	Protocol Version	0b00 0000 0000 = R1.4, R1.5, R1.5a 0b00 0000 0001 = R1.6
10-15	System ID	0b0000 00 = RESERVED 0b0000 01 = IP Site Connect 0b0000 10 = Capacity Plus

Table 15: Link Protocol Version Bit Allocation

A MOTOTRBO repeater peer can only exist in one system at one time. It can only have one System ID. A third party application can have multiple system IDs to support different types of system at the same time, e.g. a Capacity Plus system and an IP Site Connect system. It has to use the same system ID as the MOTOTRBO repeater peers to establish the connection. It has to use system ID of 1 to communicate with the peers

816 in the IP Site Connect system, and use system ID of 2 to communicate with the peers in
817 the Capacity Plus system.

6.0 Voice and Data Protocol and Definitions

This section describes the IP Site Connect voice and data protocol that will be used by peers to communicate with each other over an IP network.

6.1 Voice and Data Protocol

When a peer receives a voice call, data call or control call over the air, it sends the DMR bursts through IP Site Connect voice and data protocol to all other peers. The IP Site Connect protocol defines two types of message for voice, data and control burst transmission. One is IP Site Connect Call Control Header, and the other is IP Site Connect Call Header.

The IP Site Connect Call Header is used for voice call, data call and control call request transmission. When a peer receives a voice call (or data call / control call request) over the air, it encapsulates the DMR voice burst as the RTP payload, then encapsulates the RTP packet as the payload of the IP Site Connect Call Header message, and sends the IP Site Connect Call Header message over UDP/IP transport layer to all the peers in the system. For more detail message definition, refer to section 6.2.7 in this document.

The IP Site Connect Call Control Header is used for control call responses transmission. When a peer receives a control call response over the air, i.e. Emergency Alarm response, it converts the control call DMR burst to an IP Site Connect Call Control message, then wraps the IP Site Connect Call Control message in the UDP/IP message and sends it out to all the peers in the system. For more detail message definition, refer to section 0 in this document.

6.1.1 Transaction Types/Message Types

There is only one transaction type for the IP Site Connect voice and data protocol.

- Broadcast - A peer sends an IP Site Connect message to all other peers by unicast.

6.1.2 Message Interleaving

The IP Site Connect Voice and Data protocol does not define any procedure for ACKs or retries for peer-to-peer messaging. It is assumed that the underlying transport will provide these mechanisms.

The peer maintains no state information for the IP Site Connect CALL HEADER and CALL CONTROL HEADER messages to track if they were delivered or whether they should be retried or acknowledged. The peer in this case only acts as a relay. It is assumed that the subscriber (or third party application) has the appropriate mechanism in place to perform retries and acknowledgements.

To support all-site light up, only one call per slot will be granted the channel in the IP Site Connect system. So when a peer receives a call setup request from either a local subscriber or another peer, it will determine if the request can be granted the channel access using the floor control mechanism. If the channel access is granted, the peer will

continue to process the request, either send out the request over the air, or send the request to all other peers. Otherwise, the peer will drop the request. Each peer is required to use the same mechanism to implement the floor control. Please refer to the IP Site Connect Guide ADK for more detail on the floor control.

6.1.3 Message Timeout

The peer acts as a relay during the CALL CONTROL HEADER and CALL HEADER PDUs transmission. It does not track if the PDUs were delivered or whether they should be retried or acknowledged. So no timeout is defined for the message transmission.

6.2 IP Site Connect Call Control PDU Definition

The IP Site Connect Call Control Header is used for control call responses transmission. The basic format of an IP Site Connect control packet is shown below:

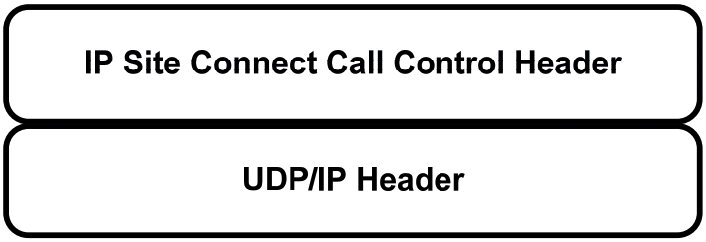


Figure 10 – Basic IP Site Connect Call Control Packet Format

The enhanced format of an IP Site Connect call control packet is shown below (when authentication is enabled):

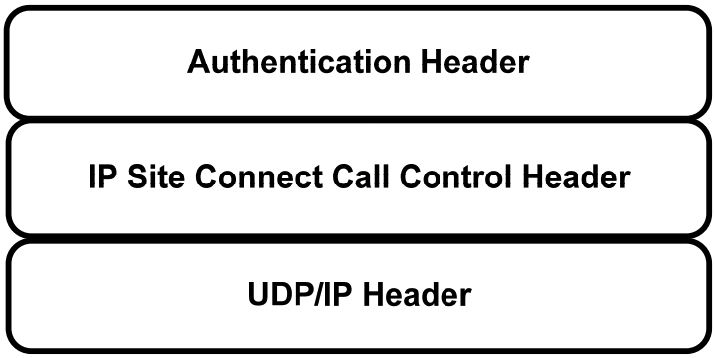


Figure 11 – Enhanced IP Site Connect Call Control Packet Format

6.2.1 Basic Call Control PDU Format

The basic structure of an IP Site Connect Call Control Header PDU is shown below.

Field	Type	Description
opcode	Uint8	Specifies the type of the PDU
peerID	Uint32	The ID of the peer that is sending this PDU
seqNumber	Uint32	The sequence number of this PDU
Opcode Specific Field 1		
……..		
……..		
Opcode Specific Field N		

Table 16 : Basic IP Site Connect Control PDU Format

All PDUs will have an opcode that specifies the type of the PDU, the ID of the peer that is sending the PDU and the sequence number of the PDU.

6.2.2 0x04 - IPSC_CALL_ALERT_RESP

Class	Call Control	Type	Broadcast
Opcode	0x04	Command	IPSC_CALL_ALERT_RESP
Description	Call Alert Response		

6.2.2.1. Description

This PDU is used to convey a call alert response.

Sending Peer Actions:

When a peer receives a call alert response from a local subscriber, that peer sends an IPSC_CALL_ALERT_RESP PDU to all other peers in the IP Site Connect network.

Receiving Peer Actions:

The peer sends the call alert response OTA but only if it can resolve any channel contention (floor control) issues.

6.2.2.2. Cautions / Warnings

Starting from R1.6, this message is replaced by the IP Site Connect Common CSBK Response. See section 6.3 for details.

6.2.2.3. Packet Format

System		Version Introduced		
IP Site Connect		0		
Offset	Field	Type	Description	Information Field
0	opcode	Uint8	Value = 0x04	
1	peerID	Uint32	The ID of the peer that is sending this PDU	6.2.7.6
5	pduSeqNumber	Uint32	The sequence number of this PDU	6.2.7.5
9	srcID	Uint24	The ID of the subscriber that sent the call alert response	6.2.7.8
13	tgtID	Uint24	The ID of the target subscriber	6.2.7.8
17	callAlertResp	Uint8	The response (ACK or NACK)	6.2.7.2
18	channelNum	Uint8	The channel (slot) number assignment for the PDU.	6.2.7.3

6.2.3 0x06 - IPSC_PVT_CALL_RESP

Class	Call Control	Type	Broadcast
Opcode	0x06	Command	IPSC_PVT_CALL_RESP
Description	Private Call Response		

6.2.3.1. Description

This PDU is used to convey an OACSU private call response.

Sending Peer Actions:

When a peer receives an OACSU private call response from a local subscriber, that peer sends an IPSC_PVT_CALL_RESP PDU to all other peers in the IP Site Connect network.

Receiving Peer Actions:

The peer sends the private call response over the air but only if it can resolve any channel contention (floor control) issues.

6.2.3.2. Cautions / Warnings

Starting from R1.6, this message is replaced by the IP Site Connect Common CSBK Response. See section 6.3 for details.

6.2.3.3. Packet Format

System		Version Introduced		
IP Site Connect		0		
Offset	Field	Type	Description	Information Field
0	opcode	Uint8	Value = 0x06	
1	peerID	Uint32	The ID of the peer that is sending this PDU	6.2.7.6
5	pduSeqNumber	Uint32	The sequence number of this PDU	6.2.7.5
9	srcID	Uint24	The ID of the subscriber that sent the private call response	6.2.7.8
13	tgtID	Uint24	The ID of the target subscriber	6.2.7.8
17	answerResp	Uint8	The response (Proceed or Deny)	6.2.7.1
18	channelNum	Uint8	The channel (slot) number assignment for the PDU.	6.2.7.3

6.2.4 0x08 - IPSC_EMRG_ALRM_RESP

Class	Call Control	Type	Broadcast
Opcode	0x08	Command	IPSC_EMRG_ALRM_RESP
Description	Emergency Alarm Response		

6.2.4.1. Description

This PDU will be used to convey an emergency alarm response.

Sending Peer Actions:

When a peer receives an emergency alarm response from a subscriber, that peer will send an IPSC_EMRG_ALRM_RESP PDU to all peers in the IP Site Connect network.

Receiving Peer Actions:

The peer sends the emergency alarm response OTA but only if it can resolve any channel contention (floor control) issues.

6.2.4.2. Cautions / Warnings

Starting from R1.6, this message is replaced by the IP Site Connect Common CSBK Response. See section 6.3 for details.

6.2.4.3. Packet Format

System		Version Introduced		
IP Site Connect		0		
Offset	Field	Type	Description	Information Field
0	opcode	Unit8	Value = 0x08	
1	peerID	Unit32	The ID of the peer that is sending this PDU	6.2.7.6
5	pduSeqNumber	Unit32	The sequence number of this PDU	6.2.7.5
9	srcID	Unit24	The ID of the subscriber that sent the emergency alarm response	6.2.7.8
13	tgtID	Unit24	The ID of the target subscriber	6.2.7.8
17	emrgAlrmResp	Unit8	The response (ACK or NACK)	6.2.7.4
18	channelNum	Unit8	The channel (slot) number assignment for the PDU.	6.2.7.3

6.2.5 0x0A - IPSC_RAD_MON_RESP

Class	Call Control	Type	Broadcast
Opcode	0x0A	Command	IPSC_RAD_MON_RESP
Description	Radio Remote Monitor Response		

6.2.5.1. Description

This PDU is used to convey a remote monitor response.

Sending Peer Actions:

When a peer receives a remote monitor response from a local subscriber, that peer sends an IPSC_RAD_MON_RESP PDU to all peers in the IP Site Connect network.

Receiving Peer Actions:

The peer sends the remote monitor response OTA but only if it can resolve any channel contention (floor control) issues.

6.2.5.2. Cautions / Warnings

Starting from R1.6, this message is replaced by the IP Site Connect Common CSBK Response. See section 6.3 for details.

6.2.5.3. Packet Format

System	Version Introduced			
IP Site Connect	0			
Offset	Field	Type	Description	Information Field
0	opcode	Uint8	Value = 0x0A	
1	peerID	Uint32	The ID of the peer that is sending this PDU	6.2.7.6
5	pduSeqNumber	Uint32	The sequence number of this PDU	6.2.7.5
9	srcID	Uint24	The ID of the subscriber that sent the remote monitor response	6.2.7.8
13	tgtID	Uint24	The ID of the target subscriber	6.2.7.8
17	radMonResp	Uint8	The response (ACK or NACK)	6.2.7.7
18	channelNum	Uint8	The channel (slot) number assignment for the PDU.	6.2.7.3

6.2.6 0x85 - IPSC_ALL_SITE_WAKEUP

Class	Call Control	Type	Broadcast
Opcode	0x85	Command	IPSC_ALL_SITE_WAKEUP
Description	IP Site Connect Wakeup Broadcast		

6.2.6.1. Description

This PDU is used to synchronize the keying up all peers in the system.

Sending Peer Actions:

A peer sends an IPSC_ALL_SITE_WAKEUP PDU:

1) Upon receiving a DMR over-the-air CSBK wakeup burst from a subscriber to all applicable peers in system, and qualifying the CSBK wakeup burst by checking the color code, MFID and valid CRC.
2) Upon scheduling beacons for auto-roaming feature support, with wakeupType set to wakeup beacon.
3) For a third party application peer, it should send out the wakeup message to all applicable peers before initiating a voice call or data call.

Receiving Peer Actions:

A peer receiving an IPSC_ALL_SITE_WAKEUP PDU handles it as described below:

1) If the MOTOTRBO repeater peer is in de-keyed conditions, it shall initiate a normal wake-up sequence.
2) If the MOTOTRBO repeater peer is already keyed up (transmitting IDLES), it prepares to receive a possible IP call.
3) Upon receiving beacon type wakeup PDU, it starts transmitting idles, if not already transmitting idles frames.

6.2.6.2. Cautions / Warnings

None.

6.2.6.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	opcode	Uint8	Value = 0x85	
1	peerID	Uint32	The ID of the peer that is sending this PDU	6.2.7.6
5	pduSeqNumber	Uint32	The sequence number of this PDU	6.2.7.5
9	channelNum	Uint8	The channel (slot) number assignment for the PDU.	6.2.7.3
10	wakeupType	Uint8	The wakeup type – beacon or CSBK wakeup type.	6.2.7.9

6.2.7 Information Fields

6.2.7.1. Answer Response

This field indicates the response to an OACSU private call request. It is an 8 bit unsigned integer.

secure Value	Allocation
0x00 to 0x1F	RESERVED
0x20	Proceed
0x21	Deny
0x22 to 0xFF	RESERVED

Table 17 - answerResponse Allocation

6.2.7.2. Call Alert Response

This field indicates a subscriber's response to a call alert request. It is an 8 bit unsigned integer. A zero value indicates an ACK. Non-zero values indicates a NACK along with a reason.

callAlertResp Value	Allocation
0x00	ACK
0x01	NACK – Service not supported
0x02 to 0xFF	Reserved

Table 18 - callAlertResp Allocation

6.2.7.3. Channel Number

This field conveys the channel number (or slot usage) associated with the PDU.

Channel Number Value	Allocation
0x00	Channel 1 (slot 1)
0x01	Channel 2 (slot 2)
0x02-FF	Reserved

Table 19 : Channel Number Allocation

6.2.7.4. Emergency Alarm Response

This field indicates a subscriber's response to an emergency alarm request. It is an 8 bit unsigned integer. A zero value indicates an ACK. Non-zero values indicates a NACK along with a reason.

emrgAlrmResp Value	Allocation
0x00	ACK
0x01	NACK – Service not supported
0x02 to 0xFF	Reserved

Table 20 : emrgAlrmResp Allocation

6.2.7.5. Packet Data Unit Sequence Number

This field specifies the sequence number of a PDU. It is a 32 bit unsigned integer in network byte order. The sequence number is generated by the peer that is sending the PDU and is incremented every time a PDU is sent. The number is reset to 0 when it crosses the maximum value of Uint32.

Sequence Number Value	Allocation
0x00000000 to 0xFFFFFFFF	Valid Range

Table 21 - pduSeqNumber Allocation

6.2.7.6. Peer Identifier

This field specifies the identity of a peer. It is a 32 bit unsigned integer in network byte order.

Peer ID Value	Allocation
0x00000000	RESERVED
0x00000001 to 0xFFFFFFFE	Valid Range
0xFFFFFFFF	RESERVED

Table 22 - peerID Allocation

6.2.7.7. Radio Monitor Response

This field indicates a subscriber's response to a remote monitor command. It is an 8 bit unsigned integer. A zero value indicates an ACK. Non-zero values indicates a NACK along with a reason.

radMonResp Value	Allocation
0x00	ACK
0x01	NACK – Service not supported
0x02 to 0xFF	Reserved

Table 23 : radMonResp Allocation

6.2.7.8. srcID and tgtID

This field specifies the identity of a subscriber. It is a 24 bit unsigned integer in network byte order.

Subscriber ID Value	Allocation
0x000000	RESERVED
0x000001 to 0xFFFCDF	Valid Range
0xFFFCE0 to 0xFFFFFF	RESERVED

Table 24 - srcID Allocation

6.2.7.9. Wakeup Type

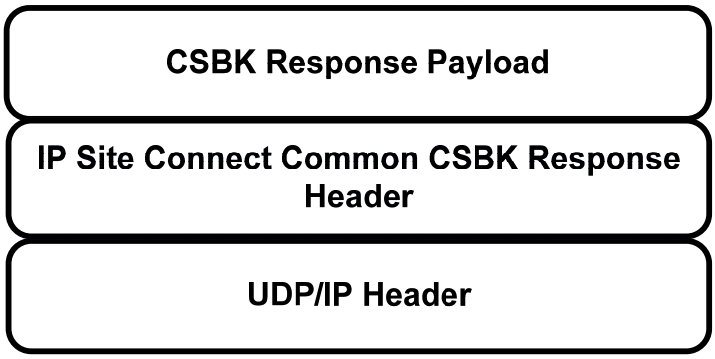
This field indicates the type of wake-up message PDU. It is an 8 bit unsigned integer.

wakeUp Value	Allocation
0x01	All-site wakeup
0x02	Beacon wakeup
0x03-0xFF	RESERVED

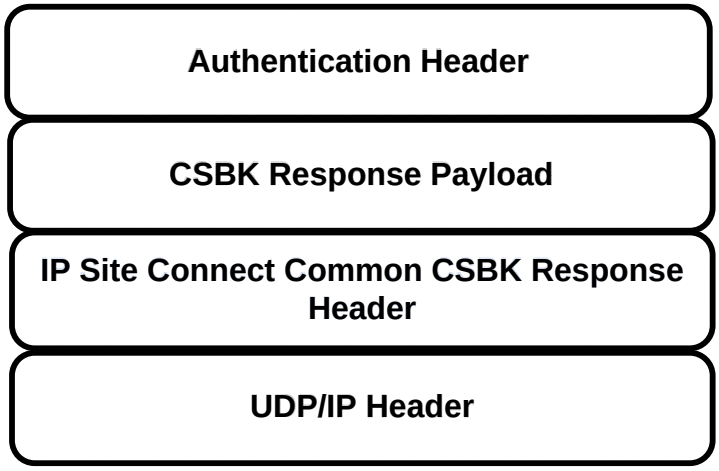
Table 25 - Wakeup Type Allocation

6.3 IP Site Connect Common CSBK Response Control PDU Definition

Starting from the MOTOTRBO repeater R1.6 release, the IP Site Connect Common CSBK Response Control PDU is introduced to replace all the IP Site Connect Call Control PDUs for the CSBK responses including IPSC_CALL_ALERT_RESP, IPSC_PVT_CALL_RESP, IPSC_EMRG_ALRM_RESP and IPSC_RAD_MON_RESP. The following is the basic format of an IPSC Common CSBK Response Control Header packet:



The following is the enhanced format of an IP Site Connect Common CSBK Response Control Header packet when authentication is enabled:



The CSBK Response Payload specification details are at section 9.1.2. Note the IP Site Connect Common CSBK Response Control PDU is not applicable for the Extended Function Type CSBKs (request and responses). The Extended Function Type CSBKs use the IP Site Connect Voice and Data Call PDU.

The MOTOTRBO repeater can directly use the CSBK Response Payload in the IP Site Connect Common CSBK Response PDU to generate the over-the-air CSBK acknowledgement bursts. This common CSBK response allows flexibility and clean interface in the future support.

6.3.1 IP Site Connect Common CSBK Response Header

Class	Call Control	Type	Broadcast
Opcode	0x05	Command	IPSITECONN_COMMON_CSBK_RESP
Description	IP Site Connect Common CSBK Response Header		

6.3.1.1. Description

This PDU is used to convey the CSBK response for the following CSBK message:

- Call Alert
- Remote Monitor
- Emergency Alarm
- OACSU Private Call

Sending Peer Actions:

When a peer receives a CSBK Response (i.e. Call Alert Response) over the air, it first encapsulates the CSBK Response bursts in the payload of the IP Site Connect Common CSBK Response message and sends IP Site Connect Common CSBK Response message over UDP/IP transport layer to all the peers in the system.

Receiving Peer Actions:

The peer sends the CSBK response in the payload of the IP Site Connect Common CSBK Response message OTA but only if it can resolve any channel contention (floor control) issues.

6.3.1.2. Cautions / Warnings

None.

1046 #### 6.3.1.3. Packet Format

System		Version Introduced		
IP Site Connect		1		
Capacity Plus		2		
Offset	Field	Type	Description	Information Field
0	opcode	Uint8	Value = 0x05	
1	peerID	Uint32	The ID of the peer where this packet originated	6.2.7.6
5	pduSeqNumber	Uint32	The sequence number of this PDU	6.2.7.5
9	commonCSBKRespType	Uint8	Specifies the CSBK Response type	6.3.2.2
10	srcID	Uint24	The ID of the subscriber that sends the CSBK response	6.2.7.8
13	tgtID	Uint24	The ID of the subscriber to which the response is targeted	6.2.7.8
16	commonCSBKInfoResp	Uint8	The response (ACK or NACK)	6.3.2.1
17	channelNum	Uint8	The channel (slot) number assignment for the PDU.	6.2.7.3

1047 **Table 26 - IP Site Connect Common CSBK Response Header Format**

6.3.2 Information Fields

6.3.2.1. Common CSBK Information Response

This field indicates a subscriber's response to a particular call CSBK request. It is an 8-bit unsigned integer.

commonCSBKInfoResp Value	Allocation
0x20	ACK
0x26	NACK

Table 27: Common CSBK Information Response Allocation

6.3.2.2. Common CSBK Response Type

This field indicates the type of CSBK response. It is an 8-bit unsigned integer. This field is the DMR CSBK Opcode value.

commonCSBKRespType Value	Allocation
0x00	UNKNOWN
0x05	OACSU Private Call Response
0x1F	Call Alert Response
0x27	Emergency Alarm Response
0x1D	Remote Monitor Response

Table 28: Common CSBK Response Type

6.4 IP Site Connect Voice and Data Calls PDU Definition

A stream of audio/data between two peers is carried over Real-time Transport Protocol (RTP). Every packet has a separate IP Site Connect header that specifies the call to which that packet belongs.

The basic format of an IP Site Connect call packet is shown below:

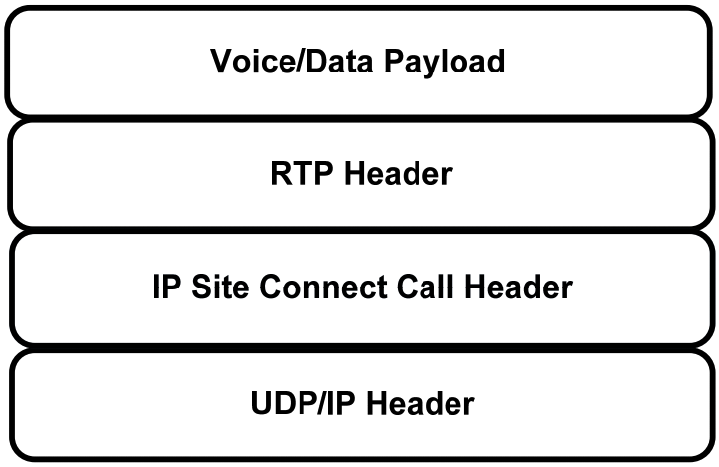


Figure 12 – Basic IP Site Connect Call Packet Format

Figure 10 also shows the protocol stack for the IP Site Connect voice and data call. For a voice / data call received over the air, the peer first encapsulates the DMR burst into the RTP package payload, and then adds the RTP package as the payload of the IP Site Connect Call message. Finally the peer sends the IP Site Connect Call message over UDP/IP transport layer to all the peers in the system. The following sub-sections provide detailed description for each protocol layer's packet format definition:

- IP Site Connect Call Header
- RTP Header
- Voice/Data Payload

The enhanced format of an IP Site Connect call packet is shown below (when authentication is enabled):

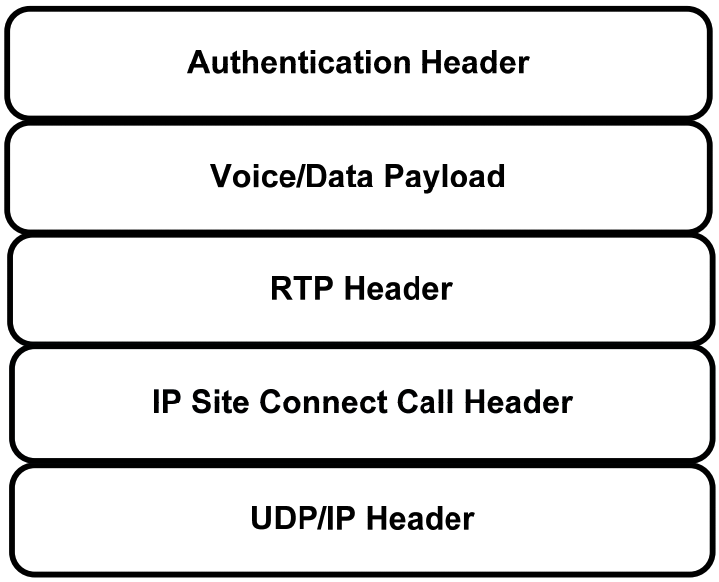


Figure 13 - Enhanced IP Site Connect Call Packet Format

6.4.1 IP Site Connect Call Header

Class	Voice/Data Call	Type	Broadcast
Opcode	0x80, 0x81, 0x83 and 0x84	Command	IPSC_CALL_HEADER
Description	IP Site Connect Call Header		

6.4.1.1. Description

This PDU is used to convey a voice/data message received over the air.

Sending Peer Actions:

When a peer receives a voice/data call over the air, it first encapsulates the DMR bursts as the RTP payload, and then adds the RTP package as the payload of the IP Site Connect Call message. Finally the peer sends the IP Site Connect Call message over UDP/IP transport layer to all the peers in the system.

Receiving Peer Actions:

The peer extracts the voice/data call message from the IP Site Connect Call message and sends the voice/data DMR burst over the air but only if it can resolve any channel contention (floor control) issues.

6.4.1.2. Cautions / Warnings

None.

6.4.1.3. Packet Format

The format of the IP Site Connect Call Header is described below:

System		Version Introduced		
IP Site Connect		0		
Capacity Plus		2		
Offset	Field	Type	Description	Information Field
0	opcode	Uint8	The type of call – group voice/data or private voice/data	6.4.1.3.1
1	peerID	Uint32	The ID of the peer where this packet originated	6.2.7.6
5	callSeqNumber	Uint8	The sequence number of this call	6.4.1.3.2
6	srcID	Uint24	The ID of the subscriber that initiated the call	6.2.7.8
9	tgtID	Uint24	The ID of the subscriber or talk-group to which the call is targeted	6.2.7.8
12	callPriority	Uint8	Specifies the priority of the call	6.4.1.3.3
13	flloorControlTag	Uint32	The tag that will be used to resolve floor contention	6.4.1.3.4
17	callControlInformation	Uint8	Specialized bits allocation that: Specifies if this is a secure call or not. Specifies if this is the last packet of voice/data for this call. Specifies channel (slot) number assignment for the PDU.	6.4.1.3.5

Table 29 - IP Site Connect Call Header Format

6.4.1.3.1 Opcode

This field indicates the type of the IP Site Connect Call message.

Opcode Value	Description
IPSC_GRP_VOICE_CALL	Group voice call
IPSC_PVT_VOICE_CALL	Private voice call
IPSC_GRP_DATA_CALL	Group data call
IPSC_PVT_DATA_CALL	Private data call

6.4.1.3.2 Call Sequence Number

This field specifies the sequence number of a Call. The sequence number is generated by the peer that sources the call and is incremented every time a new call originates. The number is set to zero when it crosses the maximum value of Uint8.

Note: Once a sequence number is assigned to a call, all the audio packets in that call will carry the same call sequence number. Please refer to Reference [7] for more information on how to set the Call Sequence Number.

Sequence Number Value	Allocation
0x00 to 0xFF	Valid Range

6.4.1.3.3 Call Priority

This field indicates the priority of a call.

Call Priority Value	Allocation
0x00	None
0x01	Data
0x02	Voice
0x03	Emergency
0x04 to 0xFF	RESERVED

Note: In a system that supports floor control / arbitration, such as the IP Site Connect system's wide area channel, floor Control shall allow emergency calls to interrupt and take over ongoing emergency calls. Data calls are not allowed to be taken over by any calls, including emergency. Impolite scenario shall only be allowed on the initiating peer, where RF contention rules would apply and use the same session, as ongoing calls. In the case of RF contention, the IP Site Connect Header shall be updated to reflect the new call type and link control information. Impolite scenarios on a remote peer where the ongoing call has not won the floor are call rejected. In a system that does not support floor control / arbitration, such as the Capacity Plus system, a call priority of zero (0x00) shall be used.

6.4.1.3.4 Floor Control Tag

This field specifies the floor control tag assigned to a call. It is a 32 bit unsigned integer in network byte order and randomly generated. It is used to resolve floor contentions.

Floor Control Tag Value	Allocation
0x00000000 to 0xFFFFFFFF	Valid Range

6.4.1.3.5 CallControlInformation

1123 This field identifies the call control information for the active call session. It uses
1124 Boolean values to optimize bandwidth.

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
secure	lastPacket	channelNumber	Reserved	Reserved	Reserved	Reserved	Reserved

1125

callControlInformation	Allocation	Description
0x0 – non-secure 0x1 - secure	Secure	This field indicates whether a call is a secure call or not. A zero value indicates a non-secure call and a non-zero value indicates a secure call. This field is to identify the call request/session between two or more peers as a secure call setup – supporting basic or enhance privacy requirements.
0x0 – normal packet 0x1 – last packet	lastPacket	This field indicates whether this packet is the last audio packet for this call or not. It is an 8 bit unsigned integer. A zero value indicates that this is a regular packet and a non-zero value indicates that this is the last packet.
0x0 – slot 1 0x1 – slot 2	channelNumber	This field conveys the channel number (or slot usage) associated with the PDU. This bit in the message from a third party application is ignored by the Capacity Plus repeater peer.

1126

6.4.2 RTP Header

The format of the RTP header with the field definitions is depicted below.

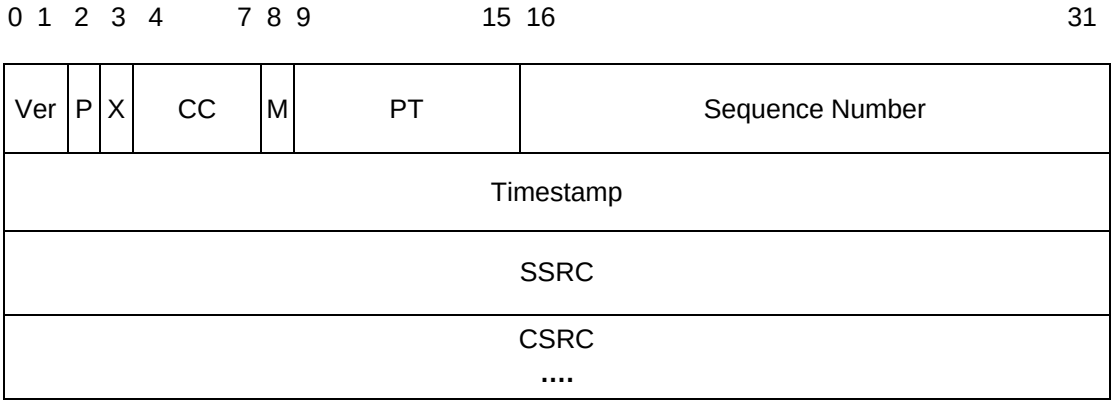


Figure 14 – RTP Header Format

Ver (Version): 2 bits. It is always set to 2.

P (Padding): 1 bit. When this bit is set, this packet contains one or more additional padding bytes at the end, which are not part of the payload. The last byte of the padding contains a count of how many padding bytes should be ignored. Padding may be needed by some encryption algorithms with fixed block sizes or for carrying several RTP packets in a lower-layer protocol data unit.

X (Extension): 1 bit. If it is set, the fixed header is followed by exactly one header extension.

CC (CSRC count): 4 bits. The number of CSRC identifiers that follow the fixed header. A CSRC is not used in the IP Site Connect system, so this count is set to zero.

M (Marker): 1 bit. The interpretation of the marker is defined by a profile. It is intended to allow significant events such as frame boundaries to be marked in the packet stream. A profile may define additional marker bits or specify that there is no marker bit by changing the number of bits in the payload type field. This Marker is not used in IP Site Connect system. The third party application peer should ignore the setting of this Marker.

PT (payload type): 7 bits. MOTOTRBO repeater defines two specific payload types for IP Site Connect RTP payload.

Payload Type Value	Description
0x5D	Indicates an ongoing voice/data call. Apply to all payloads except the last RTP frame.
0x5E	Indicates the RTP payload is the last RTP payload frame or a single CSBK.

Table 30 – Payload Type definition

Sequence Number: 16 bits. The sequence number increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss and to restore packet sequence. The initial value of the sequence number is random (unpredictable) to make known-plaintext attacks on encryption more difficult, even if the source itself does not encrypt, because the packets may flow through a translator that does.

Timestamp: 32 bits. It is incremented by 480 (60ms * 8000kHz).The timestamp reflects the sampling instant of the first octet in the RTP data packet. The sampling instant must be derived from a clock that increments monotonically and linearly in time to allow synchronization and jitter calculations. Note that MOTOTRBO repeater does not maintain a real time clock, so the timestamp is a relative time for a specific repeater. And this relative time is not synchronized with any network protocol such as Internet Time Protocol because the repeater may not have access time servers in a private network.

SSRC (Synchronization source): 32 bits. This field is not used in the IP Site Connect system and should be set to 0.

CSRC (Contributing source): Not used in the IP Site Connect System.

For more information on RTP, please refer to Reference [2].

6.4.3 Voice / Data Payload

The DMR voice and data bursts received over the air are encapsulated in the RTP payload. The following sections describe the packet format of each voice and data burst. The bit with the biggest index means the most significant bit. For example, d48 in Burst A's AMBE Voice Frame means the most significant bit in the field. As another example, the figure in section 6.4.3.2.3 shows how the DMR confirmed data header is encapsulated in the IPSC RTP data payload. The d79 bit in the 80-bit Data Header field represents the most significant bit in byte 1 of the confirmed data header, which is the G/I field. Refer to section 8.2.1.2 in Reference [3] for the DMR confirmed data header definition.

6.4.3.1. Voice Payload

As specified in Reference [3], each voice superframe contains six bursts: A, B, C, D, E and F. And each burst contains three 20ms vocoder compressed frames. The following sub-sections provided detail description on the RTP payload format for each voice burst. For more information on how to encapsulate a voice burst into a RTP data payload, please refer to Reference [7].

6.4.3.1.1 Burst A

The RTP payload format for Burst A is defined as below. All three voice frames in Burst A are sent in one RTP message.

7 0 Byte No.

Slot num	RepeaterBurstDataType (7 bits)							0
Length in bytes to follow								1
Embedded-LC Parity	Sync	NULL LC	72 Bit EMB LC	Ignore Sig Bits	EMB	Emb_LC Hard Bits	Bad Voice Burst	2
AMBE Voice Frame 1 (49 bits) d48 d47 d46 d45 d44 d43 d42 d41								3
AMBE Voice Frame 1 (49 bits) d40 d39 d38 d37 d36 d35 d34 d33								4
AMBE Voice Frame 1 (49 bits) d32 d31 d30 d29 d28 d27 d26 d25								5
AMBE Voice Frame 1 (49 bits) d24 d23 d22 d21 d20 d19 d18 d17								6
AMBE Voice Frame 1 (49 bits) d16 d15 d14 d13 d12 d11 d10 d9								7
AMBE Voice Frame 1 (49 bits) d8 d7 d6 d5 d4 d3 d2 d1								8
AMBE Frame1 (49 bits),	Bad Voice Bit	AMBE Voice Frame 2 (49 bits) d48 d47 d46 d45 d44 d43						9

d0			
AMBE Voice Frame 2 (49 bits) d42 d41 d40 d39 d38 d37 d36 d35			10
AMBE Voice Frame 2 (49 bits) d34 d33 d32 d31 d30 d29 d28 d27			11
AMBE Voice Frame 2 (49 bits) d26 d25 d24 d23 d22 d21 d20 d19			12
AMBE Voice Frame 2 (49 bits) d18 d17 d16 d15 d14 d13 d12 d11			13
AMBE Voice Frame 2 (49 bits) d10 d9 d8 d7 d6 d5 d4 d3			14
AMBE Voice Frame 2 (49 bits) d2 d1 d0	Bad Voice Bit	AMBE Voice Frame 3 (49 bits) d48 d47 d46 d45	15
AMBE Voice Frame 3 (49 bits) d44 d43 d42 d41 d40 d39 d38 d37			16
AMBE Voice Frame 3 (49 bits) d36 d35 d34 d33 d32 d31 d30 d29			17
AMBE Voice Frame 3 (49 bits) d28 d27 d26 d25 d24 d23 d22 d21			18
AMBE Voice Frame 3 (49 bits) d20 d19 d18 d17 d16 d15 d14 d13			19
AMBE Voice Frame 3 (49 bits) d12 d11 d10 d9 d8 d7 d6 d5			20
AMBE Voice Frame 3 (49 bits) d4 d3 d2 d1 d0		Reserved (bits 2 - 0)	21

6.4.3.1.2 Burst B, C, D

Voice Bursts B, C and D have the same RTP packet format. All three voice frames for each burst are sent in one RTP message with 7 bits decoded EMB and 32 bits of raw LC.

7 0 Byte No.

Slot num	RepeaterBurstDataType (7 bits)							0
Length in bytes to follow								1
Embedded-LC Parity	Sync	NULL LC	72 Bit EMB LC	Ignore Sig Bits	EMB	Emb_LC Hard Bits	Bad Voice Burst	2
AMBE Voice Frame 1 (49 bits) d48 d47 d46 d45 d44 d43 d42 d41								3
AMBE Voice Frame 1 (49 bits) d40 d39 d38 d37 d36 d35 d34 d33								4
AMBE Voice Frame 1 (49 bits) d32 d31 d30 d29 d28 d27 d26 d25								5
AMBE Voice Frame 1 (49 bits) d24 d23 d22 d21 d20 d19 d18 d17								6
AMBE Voice Frame 1 (49 bits) d16 d15 d14 d13 d12 d11 d10 d9								7
AMBE Voice Frame 1 (49 bits) d8 d7 d6 d5 d4 d3 d2 d1								8
Voice Frame1 (bit 48)	Bad Voice Bit	AMBE Voice Frame 2 (49 bits) d48 d47 d46 d45 d44 d43						9
AMBE Voice Frame 2 (49 bits) d42 d41 d40 d39 d38 d37 d36 d35								10
AMBE Voice Frame 2 (49 bits) d34 d33 d32 d31 d30 d29 d28 d27								11
AMBE Voice Frame 2 (49 bits) d26 d25 d24 d23 d22 d21 d20 d19								12
AMBE Voice Frame 2 (49 bits) d18 d17 d16 d15 d14 d13 d12 d11								13
AMBE Voice Frame 2 (49 bits) d10 d9 d8 d7 d6 d5 d4 d3								14
AMBE Voice Frame 2 (49 bits) d2 d1 d0			Bad Voice Bit	AMBE Voice Frame 3 (49 bits) d48 d47 d46 d45				15
AMBE Voice Frame 3 (49 bits) d44 d43 d42 d41 d40 d39 d38 d37								16

AMBE Voice Frame 3 (49 bits) d36 d35 d34 d33 d32 d31 d30 d29		17
AMBE Voice Frame 3 (49 bits) d28 d27 d26 d25 d24 d23 d22 d21		18
AMBE Voice Frame 3 (49 bits) d20 d19 d18 d17 d16 d15 d14 d13		19
AMBE Voice Frame 3 (49 bits) d12 d11 d10 d9 d8 d7 d6 d5		20
AMBE Voice Frame 3 (49 bits) d4 d3 d2 d1 d0	Reserved (Bits 2 - 0)	21
Emb LC Hard Bits(32 bits) d31 d30 d29 d28 d27 d26 d25 d24		22
Emb LC Hard Bits (32 bits) d23 d22 d21 d20 d19 d18 d17 d16		23
Emb LC Hard Bits (32 bits) d15 d14 d13 d12 d11 d10 d9 d8		24
Emb LCHardBits (32 bits) d7 d6 d5 d4 d3 d2 d1 d0		25
EMB (7 bits)	Not Used	26

6.4.3.1.3 Burst E

All three voice frames in Burst E are sent in one RTP message with 7 bits decoded EMB, 32 bits of raw LC and 72 bits of decoded LC. The payload length is 35 bytes.

7 0 Byte No.

Slot num	RepeaterBurstDataType (7 bits)							0
Length in bytes to follow								1
Embedded-LC Parity	Sync	NULL LC	72 Bit EMB LC	Ignore Sig Bits	EMB	Emb_LC Hard Bits	Bad Voice Burst	2
AMBE Voice Frame 1 (49 bits) d48 d47 d46 d45 d44 d43 d42 d41								3
AMBE Voice Frame 1 (49 bits) d40 d39 d38 d37 d36 d35 d34 d33								4
AMBE Voice Frame 1 (49 bits) d32 d31 d30 d29 d28 d27 d26 d25								5
AMBE Voice Frame 1 (49 bits) d24 d23 d22 d21 d20 d19 d18 d17								6
AMBE Voice Frame 1 (49 bits) d16 d15 d14 d13 d12 d11 d10 d9								7
AMBE Voice Frame 1 (49 bits) d8 d7 d6 d5 d4 d3 d2 d1								8
AMBE Voice Frame1 d0	Bad Voice Bit	AMBE Voice Frame 2 (49 bits) d48 d47 d46 d45 d44 d43						9
AMBE Voice Frame 2 (49 bits) d42 d41 d40 d39 d38 d37 d36 d35								10
AMBE Voice Frame 2 (49 bits) d34 d33 d32 d31 d30 d29 d28 d27								11
AMBE Voice Frame 2 (49 bits) d26 d25 d24 d23 d22 d21 d20 d19								12
AMBE Voice Frame 2 (49 bits) d18 d17 d16 d15 d14 d13 d12 d11								13
AMBE Voice Frame 2 (49 bits) d10 d9 d8 d7 d6 d5 d4 d3								14
AMBE Voice Frame 2 (49 bits) d2 d1 d0			Bad Voice Bit	AMBE Voice Frame 3 (49 bits) d48 d47 d46 d45				15
AMBE Voice Frame 3 (49 bits) d44 d43 d42 d41 d40 d39 d38 d37								16

AMBE Voice Frame 3 (49 bits) d36 d35 d34 d33 d32 d31 d30 d29		17
AMBE Voice Frame 3 (49 bits) d28 d27 d26 d25 d24 d23 d22 d21		18
AMBE Voice Frame 3 (49 bits) d20 d19 d18 d17 d16 d15 d14 d13		19
AMBE Voice Frame 3 (49 bits) d12 d11 d10 d9 d8 d7 d6 d5		20
AMBE Voice Frame 3 (49 bits) d4 d3 d2 d1 d0	Reserved (bits 2 - 0)	21
Emb LC Hard Bits(32 bits) d31 d30 d29 d28 d27 d26 d25 d24		22
Emb LC Hard Bits (32 bits) d23 d22 d21 d20 d19 d18 d17 d16		23
Emb LC Hard Bits (32 bits) d15 d14 d13 d12 d11 d10 d9 d8		24
Emb LCHardBits (32 bits) d7 d6 d5 d4 d3 d2 d1 d0		25
EMB_LC (72 bits) d72 d70 d69 d68 d67 d66 d65 d64		26
EMB_LC (72 bits) d63 d62 d61 d60 d59 d58 d57 d56		27
EMB_LC (72 bits) d55 d54 d53 d52 d51 d50 d49 d48		28
EMB_LC (72 bits) d47 d46 d45 d44 d43 d42 d41 d40		29
EMB_LC (72 bits) d39 d38 d37 d36 d35 d34 d33 d32		30
EMB_LC (72 bits) d31 d30 d29 d28 d27 d26 d25 d24		31
EMB_LC (72 bits) d23 d22 d21 d20 d19 d18 d17 d16		32
EMB_LC (72 bits) d15 d14 d13 d12 d11 d10 d9 d8		33
EMB_LC (72 bits) d7 d6 d5 d4 d3 d2 d1 d0		34
EMB (7 bits)	Not Used	35

6.4.3.1.4 Burst F

All three voice frames in Burst F are sent in one RTP message with 7 bits decoded EMB and 43 crypto parameter bits.

7							0	Byte No.
Slot num	Crypto Ready bit	RepeaterBurstDataType (6 bits)						0
Length in bytes to follow								1
Embedded-LC Parity	Sync	NULL LC	72 Bit EMB LC	Ignore Sig Bits	EMB	Emb_LC Hard Bits	Bad Voice Burst	2
AMBE Voice Frame 1 (49 bits) d48 d47 d46 d45 d44 d43 d42 d41								3
AMBE Voice Frame 1 (49 bits) d40 d39 d38 d37 d36 d35 d34 d33								4
AMBE Voice Frame 1 (49 bits) d32 d31 d30 d29 d28 d27 d26 d25								5
AMBE Voice Frame 1 (49 bits) d24 d23 d22 d21 d20 d19 d18 d17								6
AMBE Voice Frame 1 (49 bits) d16 d15 d14 d13 d12 d11 d10 d9								7
AMBE Voice Frame 1 (49 bits) d8 d7 d6 d5 d4 d3 d2 d1								8
AMBE Voice Frame1 d0	Bad Voice Bit	AMBE Voice Frame 2 (49 bits) d48 d47 d46 d45 d44 d43						9
AMBE Voice Frame 2 (49 bits) d42 d41 d40 d39 d38 d37 d36 d35								10
AMBE Voice Frame 2 (49 bits) d34 d33 d32 d31 d30 d29 d28 d27								11
AMBE Voice Frame 2 (49 bits) d26 d25 d24 d23 d22 d21 d20 d19								12
AMBE Voice Frame 2 (49 bits) d18 d17 d16 d15 d14 d13 d12 d11								13
AMBE Voice Frame 2 (49 bits) d10 d9 d8 d7 d6 d5 d4 d3								14
AMBE Voice Frame 2 (49 bits) d2 d1 d0		Bad Voice Bit	AMBE Voice Frame 3 (49 bits) d48 d47 d46 d45					15
AMBE Voice Frame 3 (49 bits) d44 d43 d42 d41 d40 d39 d38 d37								16

AMBE Voice Frame 3 (49 bits) d36 d35 d34 d33 d32 d31 d30 d29		17
AMBE Voice Frame 3 (49 bits) d28 d27 d26 d25 d24 d23 d22 d21		18
AMBE Voice Frame 3 (49 bits) d20 d19 d18 d17 d16 d15 d14 d13		19
AMBE Voice Frame 3 (49 bits) d12 d11 d10 d9 d8 d7 d6 d5		20
AMBE Voice Frame 3 (49 bits) d4 d3 d2 d1 d0	Reserved (bits 2 - 0)	21
Emb LC Hard Bits(32 bits) d31 d30 d29 d28 d27 d26 d25 d24		22
Emb LC Hard Bits (32 bits) d23 d22 d21 d20 d19 d18 d17 d16		23
Emb LC Hard Bits (32 bits) d15 d14 d13 d12 d11 d10 d9 d8		24
Emb LCHardBits (32 bits) d7 d6 d5 d4 d3 d2 d1 d0		25
EMB (7 bits)	Not Used	26
Crypto Parameters (43 bits) d43 d42 d41 d40 d39 d38 d37 d36		27
Crypto Parameters (43 bits) d35 d34 d33 d32 d31 d30 d29 d28		28
Crypto Parameters (43 bits) d27 d26 d25 d24 d23 d22 d21 d20		29
Crypto Parameters (43 bits) d19 d18 d17 d16 d15 d14 d13 d12		30
Crypto Parameters (43 bits) d11 d10 d9 d8 d7 d6 d5 d4 d3		31
Crypto Parameters (43 bits) d2 d1 d0	Reserved (Bits 4 - 0)	32

For a non-encrypted voice call, the RTP payload does not include the Crypto parameters field and the Crypto Ready bit is set to Not Present.

Note: AMBE+2 RTP voice frames contain 49 bits AMBE with 0 bits FEC (2450Hz). And EMB is repeated in the burst B, C, D and F.

6.4.3.1.5 Field Definitions

Note: All the fields are in Big Endian order.

6.4.3.1.5.1 Slot Num

This field specifies the slot number associated with the RTP message.

Slot number Value	Allocation
0x0	slot 1
0x1	slot 2

6.4.3.1.5.2 RepeaterBurstDataType

This field specifies the burst data type. Below is the enumeration of the RepeaterBurstDataType.

RepeaterBurstDataType	Value
DATA_TYPE_PI_HEADER	0x00
DATA_TYPE_VOICE_HEADER	0x01
DATA_TYPE_VOICE_TERMINATOR	0x02
DATA_TYPE_CSBK	0x03
DATA_TYPE_DATA_HEADER	0x06
DATA_TYPE_UNCONFIRM_DATA_CONT	0x07
DATA_TYPE_CONFIRM_DATA_CONT	0x08
DATA_TYPE_VOICE	0x0A
DATA_TYPE_SYNC_UNDETECT	0x13

6.4.3.1.5.3 Length

The length indicates the number of bytes of the entire message frame that follows this field. It does not include the length field itself. For example, for Burst A, the length is 20 bytes.

6.4.3.1.5.4 Control Fields for Voice

Bit 7 Bit 0

Embedded-LC Parity	Sync	NULL LC	72 Bit EMB LC	Ignore Sig Bits	EMB	Emb_LC Hard Bits	Bad Voice Burst

- Embedded-LC Parity

'0' indicates that the 72-bit embedded LC has been decoded without bit errors. The 72-bit embedded LC is present with Burst E. '1' means that the CRC parity has failed.

- Sync

This bit needs to be set to 1 for burst A, and set to ZERO for bursts B through F.

- NULL LC

Currently this option is not supported and shall always be set to 0

- 72 Bit EMB LC

'1' indicates that 72-bit decoded embedded LC is present. This bit is set only for Burst E.

- Ignore Sig Bit

‘1’ indicates that the repeater’s receiver has lost sync with the subscriber and is keeping the voice call active for 720 ms to enable a fading subscriber to rejoin a call. During this 720 ms, the ‘Ignore Sig bit’ is set to 1 to indicate that the EMB, Embedded LC, 72 Bit EMB LC, EMB LC Hard bits are likely to be in error.

- EMB

‘1’ indicates the 7-bit EMB field is present. This bit is not set for Burst A. Even when the EMB bit in the Control Field for Voice shall be set to 1, the 7-bit EMB field can be set to 0. The 7-bit EMB bit fields follow the DMR standard.

- EMB LC Hard Bits

‘1’ indicates that the 32-bit un-encoded LC bits are present in this burst. This bit is set to 1 for Burst B, C, D, E and F. An external non-repeater sending voice to the repeater needs to generate the EMB LC Hard bits. ‘0’ means that the 32-bit Emb Hard LC does not exist.

- Bad Voice Burst

‘1’ indicates that AMBE decoder could not correct all the bit errors in that 20 ms voice frame. ‘0’ means that AMBE decoder corrected all the bit errors if any or there were none.

6.4.3.1.5.5 EMB

The EMB bit fields follow DMR standard. EMB contains 4 bits CC, 1 bit Encryption and 2 bits LCSS. The bit definitions are represented as below.

Bit 6 5 4 3	2	1 Bit 0
CC	EEEI	LCSS

6.4.3.1.5.6 EMB LC

The 72-bit EMB_LC (only in burst E) is the same as 72-bit LC in the voice header and terminator as described in section 7.1 of DMR standard (referenced [4]).

6.4.3.1.5.7 Crypto Ready bit

‘1’ indicates that there are proprietary crypto parameters associated with the voice call.

6.4.3.1.5.8 Crypto Parameters

This field is present when Crypto Ready bit is set. There are 43 bits of decoded Crypto Parameters. The CryptoParameters bits are sent when the entire crypto parameters (11 bits keyed&AlgID and 32 bits IV) are decoded and IV CRC check passed. The packing format for CryptoParameters is as shown below:

```
xxxx xxxx xxxx xxxx    16 bits IV
xxxx xxxx xxxx xxxx    16 bits IV
xxxx xxxx xxx0 0000    8 bits KeyID + 3bits AlgID
```

The 43 bit crypto parameter is sent in the burst F in the following way:
The IV is sent by stealing the audio bit in the bursts, the key ID and algorithm ID is sent in the embedded signal field.

6.4.3.2. Data Payload

Besides the voice bursts, the following data bursts will be received during a voice call / data call / control call:

- Voice Header
- Voice Terminator
- CSBK Data
- Confirmed Data – Contains three types of data burst
  - Confirmed Data Header
  - Confirmed Non-Last Data block
  - Confirmed Last Data block
- Unconfirmed Data – Contains three types of data burst
  - Unconfirmed Data Header
  - Unconfirmed Non-Last Data block
  - Unonfirmed Last Data block
- Confirmed Data Response Header
- Confirmed Data Response Data Block
- Privacy Indicator Header

The following sections provide detailed description on the RTP payload format for each data burst. For more information on how to encapsulate a data burst into a RTP data payload, please refer to Reference [7].

6.4.3.2.1 Voice Header and Voice Terminator

The Voice Header is used to initiate a voice call. And the Voice Terminator is used to terminate a voice call. Both the Voice Header and Voice Terminator are transmitted as a data burst and have the same RTP payload format shown as below. The field of RepeaterBurstDataType in the RTP packet differentiates the Voice Header and the Voice Terminator.

15 — 8	7 — 0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus	0
Length in Words to follow		1
RepeaterBurstEmbSigBits		2
RepeaterBurstDataSize (in bits, 96 bits)		3
LC (72 bits) d71 d70 d69 d68 d67 d66 d65 d64 d63 d62 d61 d60 d59 d58 d57 d56		4
LC (72 bits) d55 d54 d53 d52 d51 d50 d49 d48 d47 d46 d45 d44 d43 d42 d41 d40		5
LC (72 bits) d39 d38 d37 d36 d35 d34 d33 d32 d31 d30 d29 d28 d27 d26 d25 d24		6
LC (72 bits) d23 d22 d21 d20 d19 d18 d17 d16 d15 d14 d13 d12 d11 d10 d9 d8		7
LC (72 bits) d7 d6 d5 d4 d3 d2 d1 d0	CRC (24 bits)d23 d22 d21 d20 d19 d18 d17 d16	8
CRC (24 bits) d15 d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0		9
Reserved (ZERO)	Slot type	10

6.4.3.2.2 CSBK RTP Payload Format

As specified in Reference [3], CSBK is a single data burst which is used to initiate a radio feature, such as Call Alert, Emergency Alarm and Remote monitor etc. The DMR CSBK packet is encapsulated in the RTP payload when transmitting in the IP Site Connect network. The RTP payload format for CSBK is shown as below.

15 8	0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus	0
Length in Words to follow		1
RepeaterBurstEmbSigBits		2
RepeaterBurstDataSize (in bits, 96 bits)		3
CSBK (80 bits) d79 d78 d77 d76 d75 d74 d73 d72 d71 d70 d69 d68 d67 d66 d65 d64		4
CSBK (80 bits) d63 d62 d61 d60 d59 d58 d57 d56 d55 d54 d53 d52 d51 d50 d49 d48		5
CSBK (80 bits) d47 d46 d45 d44 d43 d42 d41 d40 d39 d38 d37 d36 d35 d34 d33 d32		6
CSBK (80 bits) d31 d30 d29 d28 d27 d26 d25 d24 d23 d22 d21 d20 d19 d18 d17 d16		7
CSBK (80 bits) d15 d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0		8
CRC		9
Reserved (ZERO)	Slot type	10

Besides the standard CSBK commands defined in Reference [4], there are some Motorola proprietary CSBK messages used in MOTOTRBO. When a third party application peer initiates a Motorola proprietary CSBK message, it must follow the Motorola proprietary CSBK's definition. Please refer to Section 9.1 in this document for more information on Motorola proprietary CSBK definitions.

6.4.3.2.3 Data Header

As specified in Reference [3], the data transmission is initiated with one or two data headers that contain addressing as well as information about the payload. There are four types data header: Confirmed Data Header, Confirmed Data Response Header, UnConfirmed Data Header, and Data Privacy Header. Data Privacy Header is a Motorola Proprietary header, please refer to section 9.2.2 for the packet definition. All these data headers have the same RTP payload format shown as below. The field of RepeaterBurstDataType in the RTP packet is set to DATA_TYPE_DATA_HEADER for all these four types of header.

15 8	0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus	0
Length in Words to follow		1
RepeaterBurstEmbSigBits		2
RepeaterBurstDataSize (in bits, 96 bits)		3
Data Header (80 bits) d79 d78 d77 d76 d75 d74 d73 d72 d71 d70 d69 d68 d67 d66 d65 d64		4
Data Header (80 bits) d63 d62 d61 d60 d59 d58 d57 d56 d55 d54 d53 d52 d51 d50 d49 d48		5
Data Header (80 bits) d47 d46 d45 d44 d43 d42 d41 d40 d39 d38 d37 d36 d35 d34 d33 d32		6
Data Header (80 bits) d31 d30 d29 d28 d27 d26 d25 d24 d23 d22 d21 d20 d19 d18 d17 d16		7
Data Header (80 bits) d15 d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0		8
Data Header CRC		9
Reserved (ZERO)	Slot type	10

6.4.3.2.4 Confirmed Data Continuation

For a confirmed data transmission, one or more data block follows the confirmed data header. The last block in the transmission indicates the end of the entire data message. As specified in Reference [3], there are three types of confirmed data continuation data block: Non-last Confirmed Data block, Last Confirmed Data block and Confirmed Data Response Data block. The field of RepeaterBurstDataType in the RTP packet is set to DATA_TYPE_CONFIRMED_DATA_CONT for all these three types of confirmed data block.

For a non-last confirmed data burst, the RTP payload format definition is shown as below.

15 — 8	7 — 0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus	0
Length in Words to follow		1
RepeaterBurstEmbSigBits		2
RepeaterBurstDataSize (in bits, 144 bits)		3
Data		4
Data		5
Data		6
Data		7
Data		8
Data		9
Data		10
Data		11
Serial Number (7 bits)	CRC Bits (9 bits)	12
Reserved (ZERO)	Slot type (8 bits)	13

For the last confirmed data burst, the RTP packet format is shown as below.

15	8	0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus		0
Length in Words to follow			1
RepeaterBurstEmbSigBits			2
RepeaterBurstDataSize (in bits, 144 bits)			3
Data			4
Data			5
Data			6
Data			7
Data			8
Data			9
Fragment CRC (32 bits) d31 d30 d29 d28 d27 d26 d25 d24 d23 d22 d21 d20 d19 d18 d17 d16			10
Fragment CRC (32 bits) d15 d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0			11
Serial Number (7 bits)	CRC Bits (9 bits)		12
Reserved (ZERO)	Slot type (8 bits)		13

For a Confirmed Data Response Data Block, the RTP packet format is shown as below.

15 — 8	0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus	0
Length in Words to follow		1
RepeaterBurstEmbSigBits		2
RepeaterBurstDataSize (in bits, 96 bits)		3
Data		4
Data		5
Data		6
Data		7
CRC (32 bits) d31 d30 d29 d28 d27 d26 d25 d24 d23 d22 d21 d20 d19 d18 d17 d16		8
CRC (32 bits) d15 d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0		9
Reserved (ZERO)	Slot type (8 bits)	10

6.4.3.2.5 UnConfirmed Data Continuation

Similar as the confirmed data transmission, one or more data block follows the unconfirmed data header in an unconfirmed data transmission. For a non-last UnConfirmed data burst, the packet definition is shown as below. The RepeaterBurstDataType is set to DATA_TYPE_UNCONFIRMED_DATA_CONT for both non-last and last unconfirmed data block.

15	8	0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus		0
Length in Words to follow			1
RepeaterBurstEmbSigBits			2
RepeaterBurstDataSize (in bits, 96 bits)			3
Data			4
Data			5
Data			6
Data			7
Data			8
Data			9
Reserved (ZERO)	Slot type (8 bits)		10

For the last UnConfirmed data burst, the packet definition is shown as below.

15	8	0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus		0
Length in Words to follow			1
RepeaterBurstEmbSigBits			2
RepeaterBurstDataSize (in bits, 96 bits)			3
Data			4
Data			5
Data			6
Data			7
Fragment CRC (32 bits) d31 d30 d29 d28 d27 d26 d25 d24 d23 d22 d21 d20 d19 d18 d17 d16			8
Fragment CRC (32 bits) d15 d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0			9
Reserved (ZERO)	Slot type (8 bits)		10

6.4.3.2.6 Privacy Indicator (PI) Header

The PI header is used in the voice /data privacy transmission. It is transported through RTP payload in the IP Site Connect system. The RTP payload format for PI header is shown as below. The RepeaterBurstDataType is set to DATA_TYPE_PI_HEADER.

15 8	0	Word Num
RepeaterBurstDataType	RepeaterBurstDataStatus	0
Length in Words to follow		1
RepeaterBurstEmbSigBits		2
RepeaterBurstDataSize (in bits, 96 bits)		3
PI Header (80 bits) d79 d78 d77 d76 d75 d74 d73 d72 d71 d70 d69 d68 d67 d66 d65 d64		4
PI Header (80 bits) d63 d62 d61 d60 d59 d58 d57 d56 d55 d54 d53 d52 d51 d50 d49 d48		5
PI Header (80 bits) d47 d46 d45 d44 d43 d42 d41 d40 d39 d38 d37 d36 d35 d34 d33 d32		6
PI Header (80 bits) d31 d30 d29 d28 d27 d26 d25 d24 d23 d22 d21 d20 d19 d18 d17 d16		7
PI Header (80 bits) d15 d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0		8
PI Header CRC		9
Reserved (ZERO)	Slot type	10

The PI header is a Motorola proprietary message. Please refer to Section 9.1 in this document for more detail on the message definition.

6.4.3.2.7 Sync Undetect

The sync undetect message is not a DMR data burst. It is generated by the repeater peer when the repeater lost sync pattern. The sync undetect message is used to inform other peers to terminate the ongoing call. The RepeaterBurstDataType is set to DATA_TYPE_SYNC_UNDETECT.

15 8	0	Word Num
RepeaterBurstDataType	Reserved	0

6.4.3.2.8 Field Definitions

6.4.3.2.8.1 RepeaterBurstDataType

Refer to section 6.4.3.1.5.2 for more information.

6.4.3.2.8.2 RepeaterBurstDataStatus

It represents the status of the current RepeaterBurstData. The status is mainly in terms of whether the CRC has passed (matched) or failed (not matched). The bit definitions for this field are shown below. Non-applicable bits should be set to Zero.

Bit 7	6	5	4	3	2	1	Bit 0
Slot number	RSSI Status	0	0	0	RS Parity	CRC Parity	Embedded LC Parity

Slot number: ‘0’ means slot number 1 and ‘1’ means slot number 2.

RSSI Status: ‘1’ indicates that the RSSI value is below the threshold value and ‘0’ indicates that the RSSI value is above the threshold value.

Other status bits : ‘0’ means that the particular field has passed/matched. ‘1’ means failed (not matched).

Embedded LC Parity: Applies to 72-bit Embedded LC portion.
CRC Parity : Applies to DATA_HEADER, CONFIRM_DATA, and CSBK.
RS Parity : Applies to VOICE_HEADER and VOICE_TERMINATOR.

6.4.3.2.8.3 Length

The length indicates the number of 16-bit words of the entire message frame that follows this field. It does not include the RepeaterBurstDataType field, the RepeaterBurstDataStatus field and the length field itself.

6.4.3.2.8.4 RepeaterBurstEmbSigBits

The bit definitions for this field are shown as below.

Bit 15	14	13	12	11	10	9	Bit 8
RSSI Status	Reserved	Reserved	Burst Source	Reserved	Reserved	Reserved	Reserved

Bit 7	6	5	4	3	2	1	Bit 0
Reserved	Sync Hard Bits Present	Reserved	Reserved	Slot Type	Reserved	Sync	Sync

RSSI Status: ‘1’ indicates that the 2-byte RSSI value is present at the end of the data/voice burst and ‘0’ indicates that the RSSI value is not present.

Burst Source: ‘1’ indicates that the voice header is generated by the repeater based on the voice frames in case the repeater does not receive the voice header or the voice header is corrupted. ‘0’ means the burst is generated by the subscriber or non-repeater peer. If the non-repeater peer generates the burst, CRC must be generated by the non-repeater peer itself.

Sync Hard Bits Present: This bit is set to 1 by the repeater’s receiver if the receiver cannot correct all the bit errors. An external non-repeater peer may receive the burst with this bit set to 1. However when the non-repeater peer generates the CSBK data there cannot be any error and hence this bit should be set to 0.

Slot Type: ‘1’ means the slot type is present in this packet. ‘0’ means the slot type is not present. The slot type definition and bit fields follow DMR. Slot Type bit should be set to ‘1’ for all data types defined in section 6.2 of reference [4].

Sync: ‘00’ means Sync is not detected. ‘01’ means voice sync is detected. ‘10’ means data sync is detected.

Reserved: Reserved for future use and must be set to ZERO.

6.4.3.2.8.5 RepeaterBurstDataSize

This field represents the number of bits in the burst data. The burst data includes any data burst defined in DMR and any associated CRC with it.

Example : The RepeaterBurstDataSize is set to 96 for Voice Header and Voice Terminator includes 72-bit LC and 24-bit CRC.

6.4.3.2.8.6 Slot Type

Slot Type contains 4-bit color code and 4-bit data type. The bit definitions are shown as below. The slot type definition and bit fields follow DMR.

Bit 7	6	5	4	3	2	1	Bit 0
Color code (4 bits)				Data Type (4 bits)			

Data Type enumeration:

Data Type	Allocation
%0000	PI Header
%0001	Voice Header
%0010	Terminator
%0011	CSBK
%0100	Reserved
%0101	Reserved
%0110	Data Header

%0111	Rate ½ Data Continuation
%1000	Rate ¾ Data Continuation

Note that MOTOTRBO system use Rate ¾ Data for confirmed data, Rate ½ Data for confirmed data response and unconfirmed data block.

7.0 Repeater Call Monitoring Protocol Definitions

The Repeater Call Monitoring (RCM) messages are introduced since the MOTOTRBO repeater R1.7 release. The RCM messages improve the bandwidth efficience by only sending the call information instead of the whole voice/data raw traffic for a billing application. The RCM messages also indicate the repeater peer's state change, and call failure reasons so that the third party application can better interoperate with the repeater peers.

The RCM messages are sent from the Repeater peer to the third party console application peer after the application sets the Repeater Call Monitoring bit in the Peer Service field of the LE_MASTER_PEER_REGISTRATION_REQUEST or LE_PEER_REGISTRATION_REQUEST.

The RCM messages can be used in Capacity Plus system and IP Site Connect system. Some fields in the RCM messages are only applicable to either Capacity Plus system or IP Site Connect system.

7.1 Repeater Call Monitoring Protocol

The following is the basic format of an IP Site Connect RCM packet:

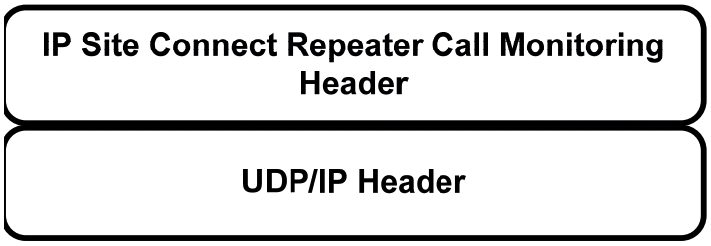


Figure 15 - Basic IP Site Connect Repeater Call Monitoring Packet Format

The following is the enhanced format of an IP Site Connect IP Site Connect RCM Header packet when authentication is enabled:

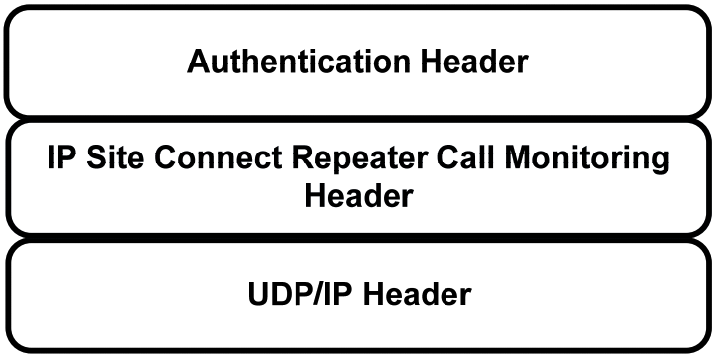


Figure 16 - Enhanced IP Site Repeater Call Monitoring Packet Format

7.1.1 Basic Message Format

The basic structure for a RCM Message is shown below.

Field	Type	Description
opcode	Uint8	Specifies the type of the PDU
peerID	Uint32	The ID of the sending peer
Opcode Specific Field 1		
……..		
……..		
Opcode Specific Field N		

All RCM Messages opcodes specify the type of the Message and the ID of the peer sending the Message.

7.1.2 0x61 – RCM_CALL_TRANSMISSION_STATUS

Class	Call Monitoring	Type	Broadcast
Opcode	0x61	Command	RCM_CALL_TRANSMISSION_STATUS
Description	Call Transmission Status		

7.1.2.1. Description

This message is sent from the repeater peer to the remote console application peers to indicate a call status, e.g. start, end, successful or failure.

A repeater peer sends out an RCM Call Transmission Status after determining whether the received call can be repeated over-the-air in one of the following situations:

1) When receiving a DMR voice or data call burst over-the-air from a local subscriber
2) When receiving a DMR voice or data call burst over IP interface from a remote subscriber.
3) When receiving a DMR voice or data call burst over IP from a remote console application peer.

A peer that receives an RCM_CALL_TRANSMISSION_STATUS PDU can parse the information in the packet and relay that information to the user in some way, e.g. indicating call status. This information can be used for billing purpose based on the time duration between call start and call end.

When the call status field has a failure type, depending on the failure type, the fields that come after the call status field may be set to zero out.

7.1.2.2. Cautions / Warnings

None

1464 #### 7.1.2.3. Packet Format

System	Version Introduced
IP Site Connect	2
Capacity Plus	2

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x61	
1	peerID	Uint32	The ID of the sending peer	6.2.7.6
5	srcPeerID	Uint32	The ID of the peer where the call originated	6.2.7.6
9	callSeqNumber	Uint32	The sequence number of this call	6.4.1.3.2
13	channelNum	Uint8	The source channel number (or slot number) assignment for the call.	6.2.7.3
14	callStatus	Uint16	The status of the call (Started Successfully, Ended Successfully, Failure, etc.)	7.2.4
16	srcID	Uint24	The ID of the subscriber that initiated the call	6.2.7.8
19	tgtID	Uint24	The ID of the subscriber or talk-group to which the call is targeted	6.2.7.8
22	callType	Uint8	Call Type (private, group, all call, etc)	7.2.1
23	callPriority	Uint8	The priority of the call	6.4.1.3.3
24	callSecurityType	Uint8	The privacy used in the call (Enhanced, Basic, or Clear)	7.2.2
25	manufacturerID (MFID)	Uint8	The DMR Feature Set ID / Manufacturer's ID	7.2.3

7.1.3 0x62 – RCM_CALL_CONTROL_NOTIFICATION

Class	Call Monitoring	Type	Broadcast
Opcode	0x62	Command	RCM_CALL_CONTROL_NOTIFICATION
Description	Call Control Notification		

7.1.3.1. Description

This message is sent from the repeater peer to the remote console application peers to indicate state update at each repeater's slot: idle or busy, enabled or disabled.

A repeater peer sends out a RCM Call Control Notification in one of the following situations:

1) When the repeater slot state changes due to call activities on one or both of the slots
2) When the repeater slot state changes due to XCMP message for enabling/disabling the slot.

A peer that receives an RCM_CALL_CONTROL_NOTIFICATION PDU can parse the information in the packet and relay that information to the user in some way, e.g. indicating repeater slot state.

7.1.3.2. Cautions / Warnings

When the repeater peer is in disabled state, it does not generate Call Transmission Status message. It can still send IPSC voice / data /control messages at the IP interface when receiving call over the air.

7.1.3.3. Packet Format

System	Version Introduced
IP Site Connect	2
Capacity Plus	2

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x62	
1	peerID	Uint32	The ID of the sending peer	6.2.7.6
5	rptCallState1	Uint8	The state of repeat slot 1 (Active, Idle, Disabled)	7.2.5
6	rptCallState2	Uint8	The state of repeat slot 2 (Active, Idle, Disabled)	7.2.5

7.1.4 0x63 – RCM_REPEAT_BLOCKED_INDICATION (RCM Repeat Blocked Indication)

Class	Call Monitoring	Type	Broadcast
Opcode	0x63	Command	RCM_REPEAT_BLOCKED_INDICATION
Description	Repeat Blocked Indication		

7.1.4.1. Description

This message is sent from the repeater peer to the remote console application peers to indicate if the repeater is currently blocked from repeating on both slots due to signal interference or the repeat of CWID/BSI.

A repeater peer sends out a RCM Repeat Block Indication in one of the following situations:

1) When the signal interference is strong enough and begins blocking repeat.
2) When the signal interference is weak enough and repeater resumes over the air repeat.
3) When the repeater has to transmit CWID/BSI and begins blocking repeat
4) When the repeater finishes CWID/BSI transmission and resumes over-the-air-repeat.

A peer that receives an RCM_REPEAT_BLOCKED_INDICATION PDU can parse the information in the packet and relay that information to the user in some way, e.g., indicating of repeater block state.

7.1.4.2. Cautions / Warnings

None

7.1.4.3. Packet Format

System	Version Introduced
IP Site Connect	2
Capacity Plus	2

Offset	Field	Type	Description	Information Field
0	Opcode	Uint8	Value = 0x63	
1	peerID	Uint32	The ID of the sending peer	6.2.7.6
5	rptBlockStatus	Uint8	Specifies the repeat block status (Signal Interference Started/Ended, CWID/BSI Started/Ended)	7.2.6

7.2 Information Field Details

7.2.1 Call Type

This field conveys the call type in the Call Transmission Status PDU.

Call Type Value	Allocation
0x00-0x2F	RESERVED
0x30	Preamble Private Data Call
0x31	Preamble Group Data Call
0x32	Preamble Private CSBK Call
0x33	Preamble Group CSBK Call
0x34	Preamble Emergency Call
0x35-0x3F	RESERVED
0x40	Emergency CSBK Alarm Request
0x41	Emergency CSBK Alarm Response
0x42	Emergency Voice Call
0x43	Private Call Request
0x44	Private Call Response
0x45	Call Alert Request
0x46	Call Alert Response
0x47	Radio Check Request (Extended Function Command)
0x48	Radio Check Response (Extended Function Response)
0x49	Radio Disable Request (Extended Function Command)
0x4A	Radio Disable Response (Extended Function Response)
0x4B	Radio Enable Request (Extended Function Command)
0x4C	Radio Enable Response (Extended Function Response)
0x4D	Radio Monitor Request
0x4E	Radio Monitor Response
0x4F	Group Voice Call
0x50	Private Voice Call
0x51	Group Data Call
0x52	Private Data Call
0x53	All Call
0x54	Confirmed Data Response (confirmed)
0x55	Other Calls
0x56	IP Console Radio Un-Inhibit Request (Extended Function Command)
0x57	IP Console Radio Inhibit Request (Extended Function Command)
0x58	IP Console Radio Un-Inhibit Response (Extended Function Response)
0x59	IP Console Radio Inhibit Response (Extended Function Response)
0x5A-0xFF	RESERVED

Table 31: Call Type Allocation

7.2.2 Security Type

This field conveys the security type in the Call Transmission Status PDU.

Security Type Value	Allocation
0x00	Clear
0x01	Basic Privacy
0x02	Enhanced Privacy
0x03-FF	Reserved

Table 32: Security Type Allocation

7.2.3 Manufacturer's ID (MFID)

This field conveys the DMR Feature ID / Manufacturer's ID in the Call Transmission Status PDU.

Maufacturer's ID Value	Allocation
0x00	Standard Feature
0x01	Reserved
0x10	Motorola Proprietary Feature
0x03-FF	Reserved

Table 33: Manufacturer's ID Allocation

7.2.4 Call Status

This field conveys success and failure call status values in the Call Transmission Status PDU. The Valid Mode field specifies which system the value is applicable. IPSC mode includes both IPSC wide area slot interface and IPSC local area slot interface. For example, value 0x05 is applicable for IPSC system only; value 0x06 is applicable for Capacity Plus system only.

Call Status Value	Allocation	Valid Mode
0x00	Reserved	
0x01	Call Started Successfully	IPSC, Cap Plus
0x02	Call Ended Successfully	IPSC, Cap Plus
0x03	Race Condition Failure	IPSC, Cap Plus
0x04	Invalid/Prohibited Call Failure	IPSC, Cap Plus
0x05	Destination Slot Busy Failure	IPSC
0x06	Subscriber Destination Busy Failure	Cap Plus
0x07	All Channels Busy Failure	Cap Plus
0x08	OTA Repeat Disabled Failure	IPSC, Cap Plus
0x09	Signal Interference Failure	IPSC, Cap Plus
0x0A	CWID In Progress Failure	IPSC, Cap Plus
0x0B	TOT Expiry Premature Call End Failure	IPSC, Cap Plus
0x0C	Transmit Interrupted Call Failure	IPSC, Cap Plus
0x0D	Higher Priority Call Takeover Failure	IPSC
0x0E	Other Unknown Call Failure	IPSC, Cap Plus
0x0C-FF	Reserved	

Table 34: Call Status Allocation

7.2.5 Repeater Call State

This field conveys the repeater call state relating to slot 1 or slot 2 in the Call Control Notification PDU.

Repeater Call State Value	Allocation
0x00	Reserved
0x01	Active Repeat Repeater is either repeating the call or in call hang state.
0x02	Idle. Rpeater is in Channel Hang state, Reactivation state, or Hibernating state
0x03	Slot Disabled
0x04	Slot Re-Enabled
0x05-FF	Reserved

Table 35: Repeater Call State Allocation

7.2.6 Repeat Block Status

This field conveys the repeat block status in the Repeat Blocked Indication PDU.

Repeater Block Value	Allocation
0x00	Reserved
0x01	Start of Signal Interference (FCC Type I)
0x02	End of Signal Interference (FCC Type I)
0x03	Start of Signal Interference (FCC Type II)
0x04	End of Signal Interference (FCC Type II)
0x05	Start of CWID/BSI Repeat
0x04	End of CWID/BSI Repeat
0x05-FF	Reserved

Table 36: Repeater Block State Allocation

8.0 IPSC-XCMP Protocol Definitions

This section describes the RDAC-IP IP Site Connect protocol definition.

8.1 IPSC-XCMP Protocol

The RDAC over IP network solution utilizes the IPSC-XCMP protocol to support IP Site Connect peer to peer networking, transporting and routing.

The RDAC peer connects into the IP Site Connect network and sends XCMP/XNL commands over IPSC/UDP/IP transport layer to control and manage a remote MOTOTRBO repeater peer. An XNL connection session is required for peer to peer XCMP/XNL message communication. If the connected RDAC peer is removed from the IP Site Connect networking, the XNL session to the removed peer will be terminated.

Also, RDAC over IP inherits the IP Site Connect networking securities. Thus, no extra IP networking security is required for RDAC over IP. The RDAC application level securities are required and are handled at the XNL layer.

8.1.1 RDAC-IP Network Link Establishment

There are two types of connections from the RDAC server to the repeater:

- Local IP Connection: RDAC server connects directly to the repeater's USB port.
- IP Site Connect Network Connection: RDAC server joins the IP Site Connect network as a peer.

In the local IP connection, the repeater, acting as a DHCP server, assigns an IP address (Accessory IP) to the RDAC server, and has a dedicated UDP port (8002) to send/receive RDAC XCMP/XNL message to/from the RADC server.

RDAC over WAN IP Network is different from the local connection. The repeater peer can be connected to an ISP router with NAT/Firewall. The IP address of the ISP router is not static. It is not possible for the repeater peer to run a RDAC server application over a well known port with an un-established IP address. Thus, the RDAC peer has to finish the IP Site Connect Link Establishment process before supporting RDAC over IP network. Once a RDAC Peer powers up and connects to the network, it must determine which other peers in the network are currently available. It also must let all peers know that it is available for RDAC service.

The RDAC peer implements the IP Site Connect protocol for link establishment procedure. After the RDAC peer is successfully registered/authenticated to the network, all RDAC data packets, from/to all peers, should be sent through the IP Site Connect established socket (peerPort & peerAddress).

8.1.2 RDAC-IP Network Securities

Since the IP Site Connect protocol is used for RDAC, it inherits the IP Site Connect encryption/authentication security scheme. Thus, the IP network security for the RDAC is same as the IP Site Connect. Since the IP Site Connect MAC key security scheme is designed for networking, RDAC command services should not just rely on it for command level accessing. An application level of security is required. Since XCMP is

the protocol choice for supporting RDAC services, the XNL layer should be used for command level authentication.

8.1.3 RDAC-IP XNL Link Establishment & Data Transmission

After the RDAC peer has registered to the IP network, it will know all available peer repeaters within the network. If the RDAC peer needs to monitor or send XCMP command to the peer repeater, it must start the XNL authentication procedure to establish an XNL connection to the repeater peer. The RDAC peer encapsulates the XCMP/XNL command in the IPSC-XCMP PDU and sends to the target peer repeater over the UDP/IP transport layer.

At the XCMP/XNL layer, the peer repeater must act as the Master device and the RDAC peer acts as the Slave device. The RDAC peer can establish multiple XNL connections to different peer repeaters. But each XNL connection is independent to each other.

The basic format of an IP Site Connect XCMP/XNL Message packet is shown below:

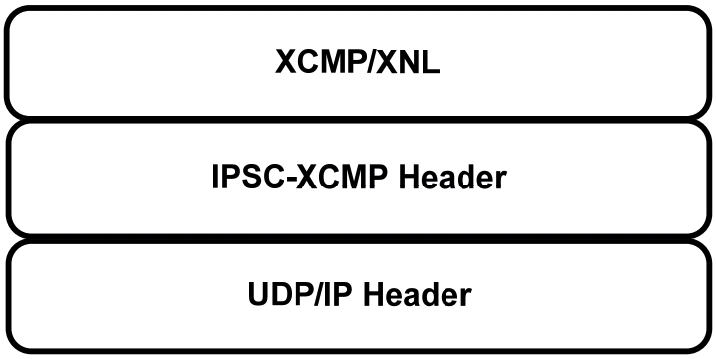


Figure 17 – Basic IP Site Connect RDAC Packet Format

The enhanced format of an IP Site Connect XCMP/XNL Message packet (with authentication enabled) is shown below:

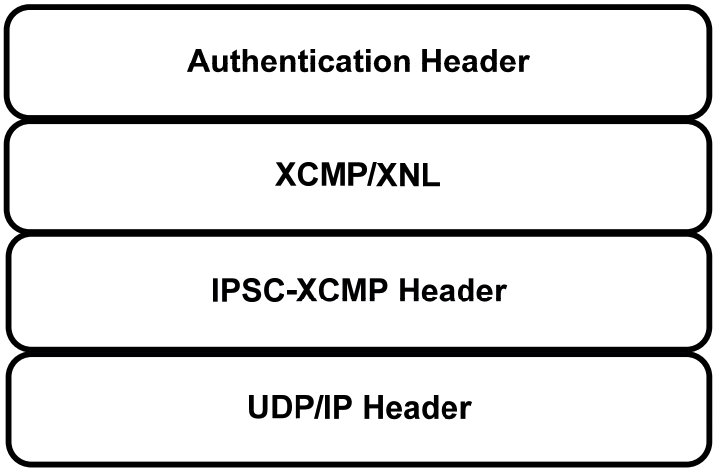


Figure 18 - Enhanced IP Site Connect RDAC Packet Format

8.2 IPSC-XCMP PDU Definitions

8.2.1 0x70 - IPSC_XCMP_XNL_DATA

Class	XCMP/XNL	Type	Request
Opcode	0x70	Command	IPSC_XCMP_XNL_DATA
Description	IP Site Connect XCMP/XNL Data Message		

8.2.1.1. Description

This PDU is used to convey a XCMP/XNL message send/receive on both a repeater peer and a RDAC Peer. This message is not acknowledged at the IP Site Connect layer. The XCMP/XNL layer should handle the message acknowledgement at the repeater peer and RDAC peer.

Sending Peer Actions:

A peer will send an IPSC_XCMP_XNL_DATA to create an XNL connection, or to send an XCMP command to a remote peer.

Receiving Peer Actions:

The peer extracts the XCMP/XNL message from this RDAC PDU. If the XCMP/XNL message is an XNL control message, the peer sends back a corresponding XNL control response to the sending peer. If the message is an XCMP command, the peer first sends back an XNL ACK to the sending peer and then processes this XCMP command according to the XCMP protocol definition. For more information on the XCMP/XNL command processing, please refer to the Reference [5] and [6].

8.2.1.2. Cautions / Warnings

None.

8.2.1.3. Packet Format

System	Version Introduced
IP Site Connect	0
Capacity Plus	0

Offset	Field	Type	Description	Information Field
0	opcode	Uint8	Value = 0x70	
1	peerID	Uint32	The ID of the peer that is sending this PDU	6.2.7.6
5	length	uint16	The length of the payload in byte	
7	payload	Array	XCMP/XNL packets, see reference [5] and [6] for details.	

9.0 Motorola Proprietary Message Definitions

9.1 DMR CSBK Messages

9.1.1 Single Block Packet Description

The CSBK message contains a 96-bit information field. The general structure of the CSBK message is shown inFigure 19.

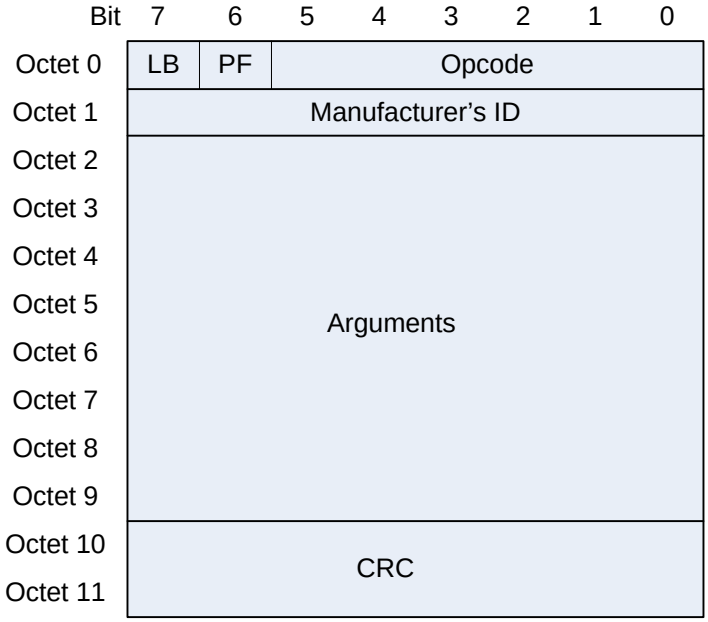


Figure 19 - CSBK message structure

- Last block flag (LB):

This flag indicates whether more CSBKs should be expected in this packet.
0: other CSBKs to follow for this packet
1: last (only) CSBK for this packet
It is always set to 1 for MOTOTRBO.

- Protected flag (PF):

This flag designates the protection mode for this CSBK.
0: non-protected mode
1: protected mode
It is always set to 0 for MOTOTRBO.

- Opcode:

It specifies the type of the message. The Data field is entirely dependent on the opcode. Motorola proprietary CSBK messages are shown as below.

Opcode	Value
ACK_RSP_U	%100000
CALL_ALERT_REQ	%011111
EMRG_ALRM_REQ	%100111
RAD_MON_COM	%011101
EXT_FNCT_CMD	%100100
EXT_FNCT_RSP	%100100

Table 37 – CSBK Opcode Definitions

For ETSI DMR standard CSBK messages:

- Preamble CSBK
- Negative Acknowledgement Response (NACK_RSP_U)
- Unit to Unit Voice Service Request (UU_V_REQ)
- Unit to Unit Voice Service Answer Response (UU_ANS_RSP)

Please refer to Reference [4] and [5] for more information.

- Manufacturer's ID (MFID):

It identifies the manufacturer for non-standard control channel messaging. For the Motorola proprietary CSBK, the MFID is 0x10. And for the ETSI DMR standard CSBK, the MFID is 0x00.

MFID Value	Allocation
0x00	Standard
0x10	Motorola Proprietary

For Motorola proprietary CSBK messages, their message definition is described in the following sections.

- CRC

This is the CRC parity check. It provides error detection for the information of this CSBK (Octets 0-9). For the CRC calculation, please refer to Reference [3], section B.3.8, for more information.

9.1.2 Acknowledge Response - Unit (ACK_RSP_U)

This is the generic response to acknowledge an action when there is no other expected response.

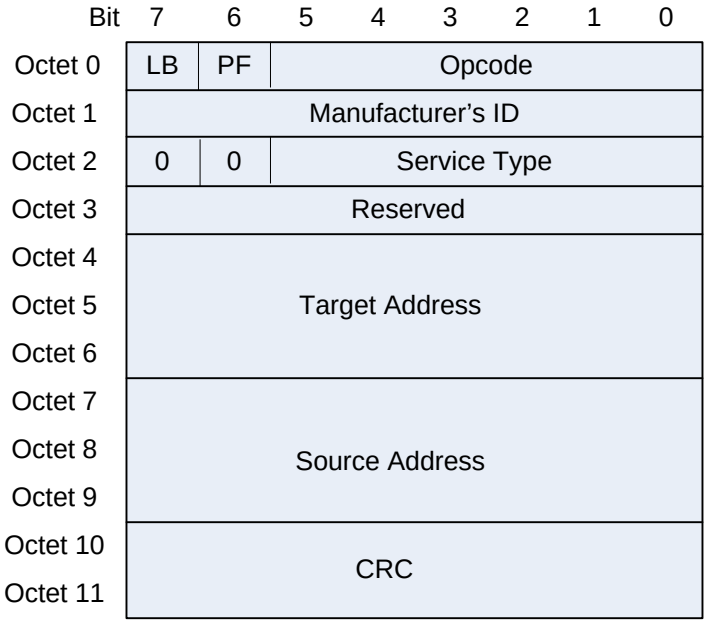


Figure 20 - Acknowledge Response - Unit

9.1.3 Call Alert Request (CALL_ALERT_REQ)

This message is used to command a radio to execute a Call Alert request operation.

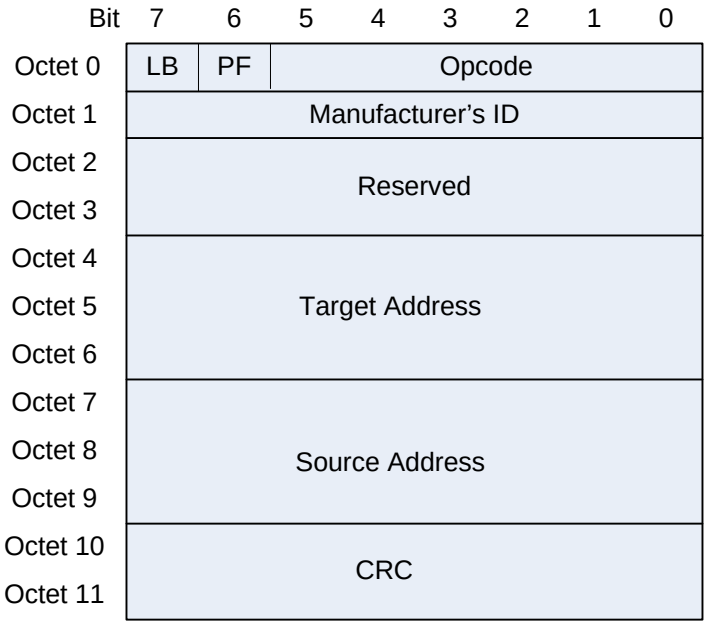


Figure 21 – Call Alert Request

9.1.4 Emergency Alarm Request (EMRG_ALRM_REQ)

This is a special status indication typically reserved for the "life threatening" situation.

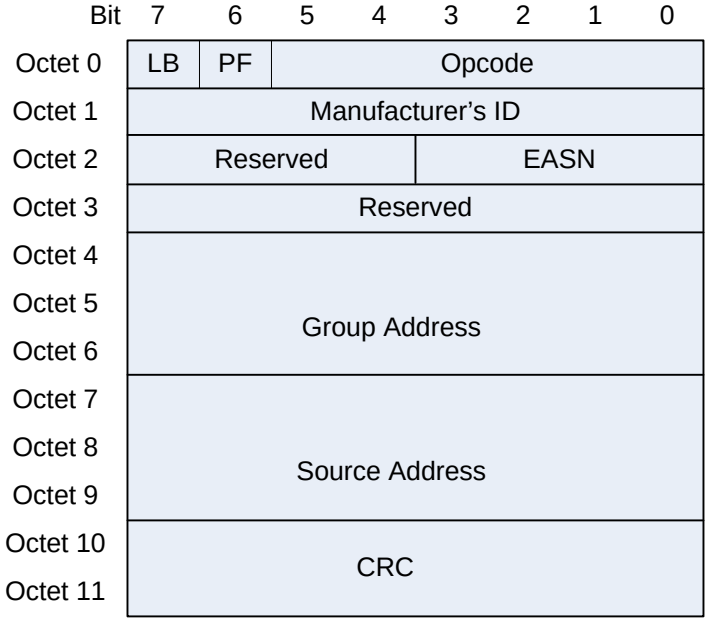


Figure 22 – Emergency Alarm Request

9.1.5 Radio Remote Monitor command (RAD_MON_CMD):

This message is used to command a radio to execute a Radio Unit Remote Monitor operation.

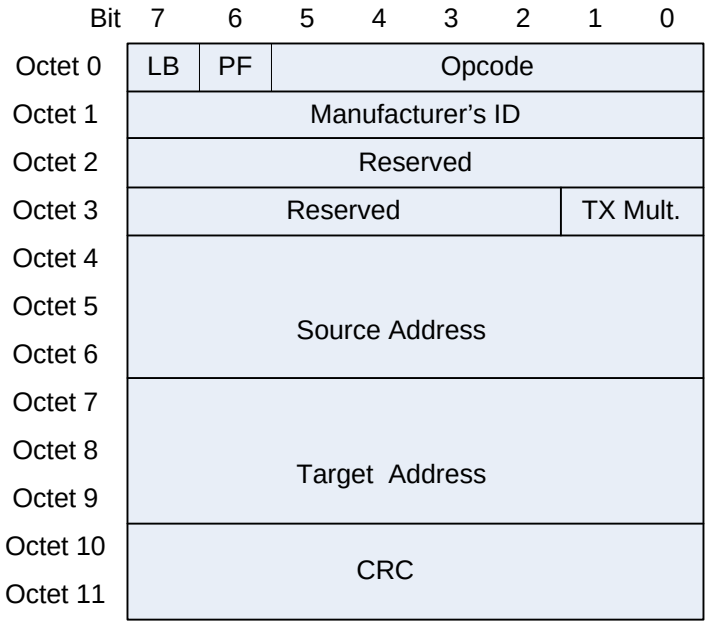
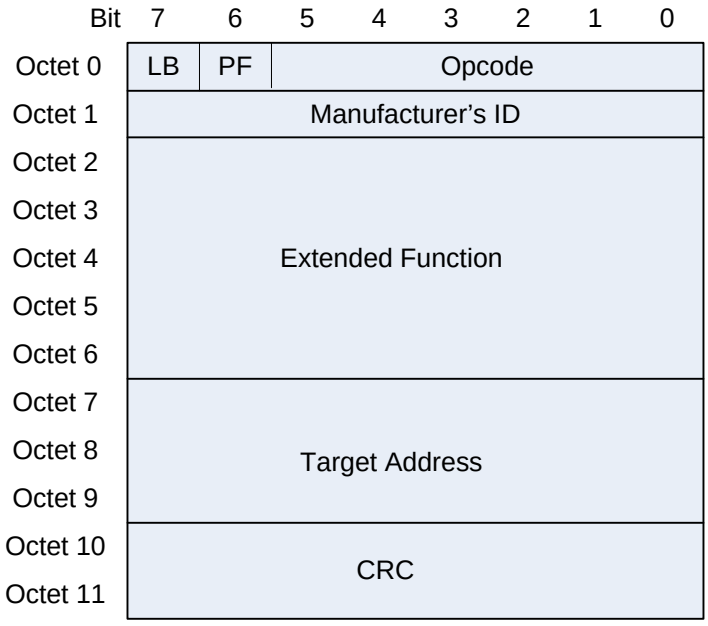


Figure 23 – Radio Remote Monitor Command

1666 The TX Multiplier is a 2-bit value ranging from 0 to 3. It multiplies a stored value
1667 programmed in the target radio to represent the requested time to key the transmitter
1668 during the monitor function. The zero value does not cause the radio to key.

1669 9.1.6 Extended Function Command (EXT_FNCT_CMD)

1670 This is the transaction addressed to an SU for an extended function.



1671

1672 **Figure 24 – Extended Function Command**

9.1.7 Extended Function Response (EXT_FNCT_RSP)

This transaction is the response to an Extended Function command.

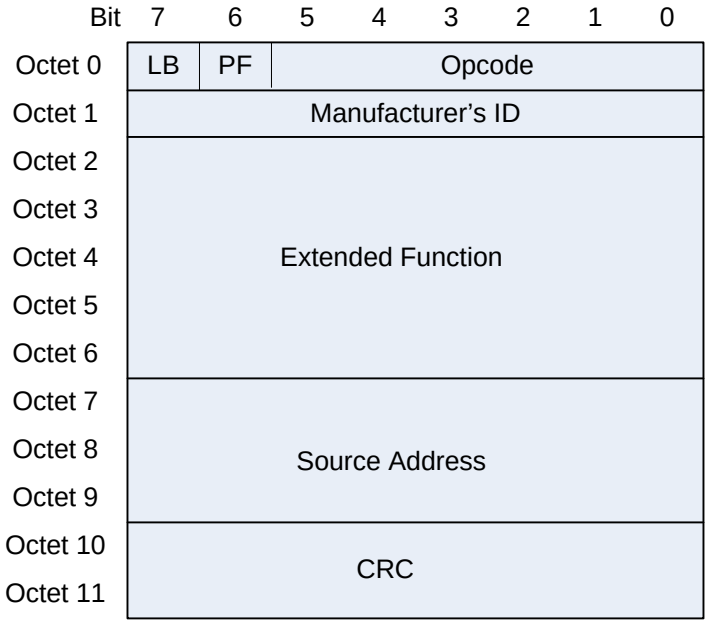


Figure 25 – Extended Function Response

9.1.8 Field Definitions

9.1.8.1. Service Type

The Service Type field indicates the service which is being identified. This is set equal to the appropriate CSBK Opcode value (defined in Table 37) for the identified service.

9.1.8.2. Emergency Alarm Sequence Number (EASN)

The Emergency Alarm Sequence Number field is a 4-bit value ranges from 0 to 15. This field shall only increment when an emergency is first initiated. Multiple attempts of the same emergency alarm message shall have the same Emergency Alarm Sequence Number. Default value shall be 0.

9.1.8.3. Target Address

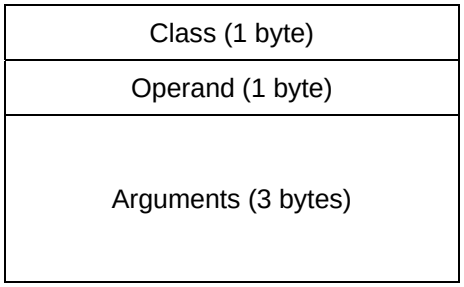
This field identifies the individual subscriber unit which is the destination of the CSBK. This is a 24-bit vector which uniquely identifies the subscriber unit within the System. It shall utilize the Subscriber Unit address definitions.

9.1.8.4. Source Address

This field identifies the individual subscriber unit which originates the CSBK. This is a 24-bit vector which uniquely identifies the subscriber unit within the System. It shall utilize the Subscriber Unit address definitions.

9.1.8.5. Extended Function

The Extended Function is a collection of related functions and operations. The Extended Function field is composed of the following subfields:



Class will determine the type of extended function to be considered.

Operand will determine the actual function being addressed based upon the Class designation.

Arguments will supply additional processing information. This may not be required for all extended functions, and will be set to "null" (0) if not required.

1705

Class	Operand	Arguments	Description
0x00	0x00	Source Address	Radio Check
0x00	0x01 – 0x7C	Reserved	Reserved
0x00	0x7D	Source Address	Reserved
0x00	0x7E	Source Address	Radio Uninhibit
0x00	0x7F	Source Address	Radio Inhibit
0x00	0x80	Target Address	Radio Check ACK
0x00	0x81	Source Address	IP Console Radio Un-inhibit
0x00	0x82	Source Address	IP Console Radio Inhibit
0x00	0x83	Target Address	IP Console Radio Un-inhibit Acknowledgement
0x00	0x84	Target Address	IP Console Radio Inhibit Acknowledgement
0x00	0x85 – 0xFC	Reserved	Reserved
0x00	0xFD	Source Address	Reserved
0x00	0xFE	Target Address	Radio Uninhibit ACK
0x00	0xFF	Target Address	Radio Inhibit ACK

1706 **Table 38 – Extended Function Values**

1707

9.2 DMR Data Messages

9.2.1 PI Header

The PI header is only sent in enhanced privacy transmission for a voice call. The basic privacy does not use the PI header. The packet format is shown as below. Please refer to Reference [7] for more detail on Voice Privacy.

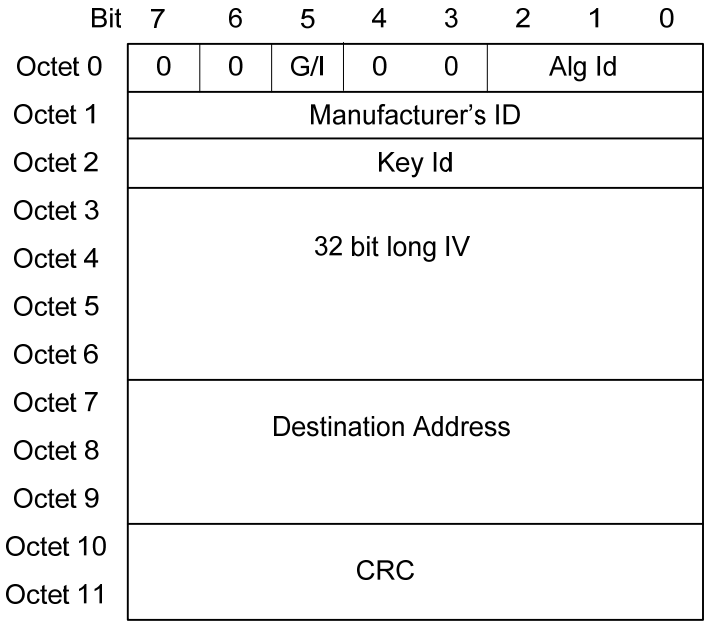


Figure 26 – PI Header Format for Voice Privacy

G/I: Indicates whether the destination is for a group or not. If the bit is set, it means the destination is for a group. Otherwise, it is for an individual.

Alg Id: 3 bit Algorithm Id; it is used in voice decryption by the receiver.

Manufacturer's ID (MFID): the Enhanced Privacy is a Motorola proprietary feature, so the MFID is set to 0x10.

Key Id: 8 bit Key Id; it is used in voice decryption by the receiver.

IV: 32 bit Initialization Vector; it is used in voice decryption by the receiver.

Destination Address: Depending on the G/I setting, it is a group id or individual Subscriber id.

CRC: For the CRC calculation, please refer to Reference [3], section B.3.8, for more information.

9.2.2 Data Privacy Header

The Data Privacy header is sent in both Basic Privacy and Enhanced Privacy transmission for a data call. But the setting of Data Privacy header is different in these two types of privacy. Please refer to Reference [7] for more detail on data privacy.

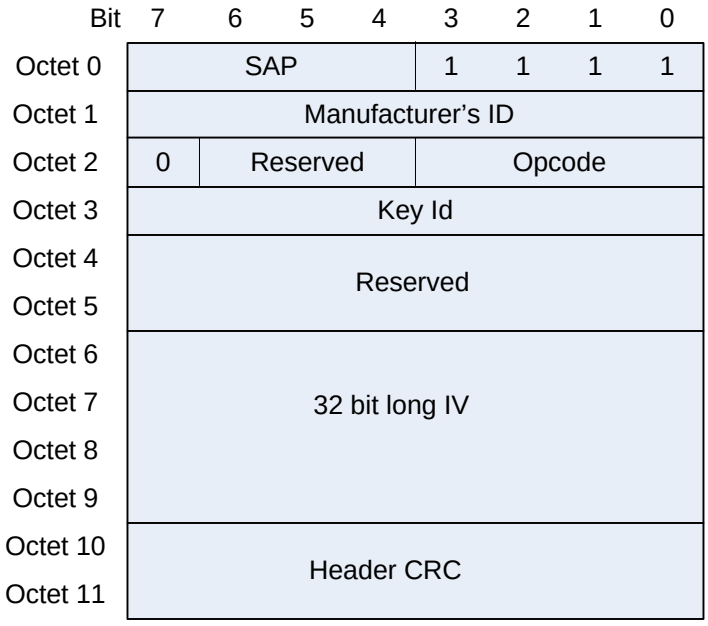


Figure 27 – PI Header Format for Data Privacy

SAP: Service Access Point, it is set to 4 for data privacy.

Manufacturer's ID (MFID): the MFID is set to 0x10 since data privacy is a Motorola proprietary feature.

Reserved: All reserved fields are set to 0.

Opcode: It is set to 1 for data privacy.

Key Id: 8 bit Key Id. For basic data privacy, the key id is set to 0 because it is not used in basic privacy. For enhanced data privacy, it is used in data decryption by the receiver.

IV: 32 bit Initialization Vector. For basic data privacy, the IV is set to 0 because it is not used in basic privacy. For enhanced data privacy, it is used in data decryption by the receiver.

CRC: For the CRC calculation, please refer to Reference [3], section B.3.8, for more information.

Appendix A: MOTOTRBO Byte-Ordering Schema Variation in HMAC-SHA1 Hash Calculation

The MOTOTRBO R1.4, R1.5 and R1.5A releases use an alternative byte-order schema in the HMAC-SHA1 hash calculation, which makes the final hash output value from the standard HMAC-SHA1 calculation.

As described in Reference [8], there are two-stage hash calculations in the HMAC-SHA1:

- Stage-One Hash = H ((k ⊕ ipad) || m)
- Stage-Two Hash = H ((k ⊕ opad) || Stage-one hash)

The MOTOTRBO R1.4, R1.5 and R1.5A releases apply the special byte-order schema in the output of stage-one hash before using it in the Stage-Two hash calculation. As shown in Figure 28, the 20-byte Stage-One output is divided into 5 4-byte units. Within each 4-byte unit, the lower 2-byte is swapped with the higher 2-byte. And the two bytes are swapped in each 2-byte unit.

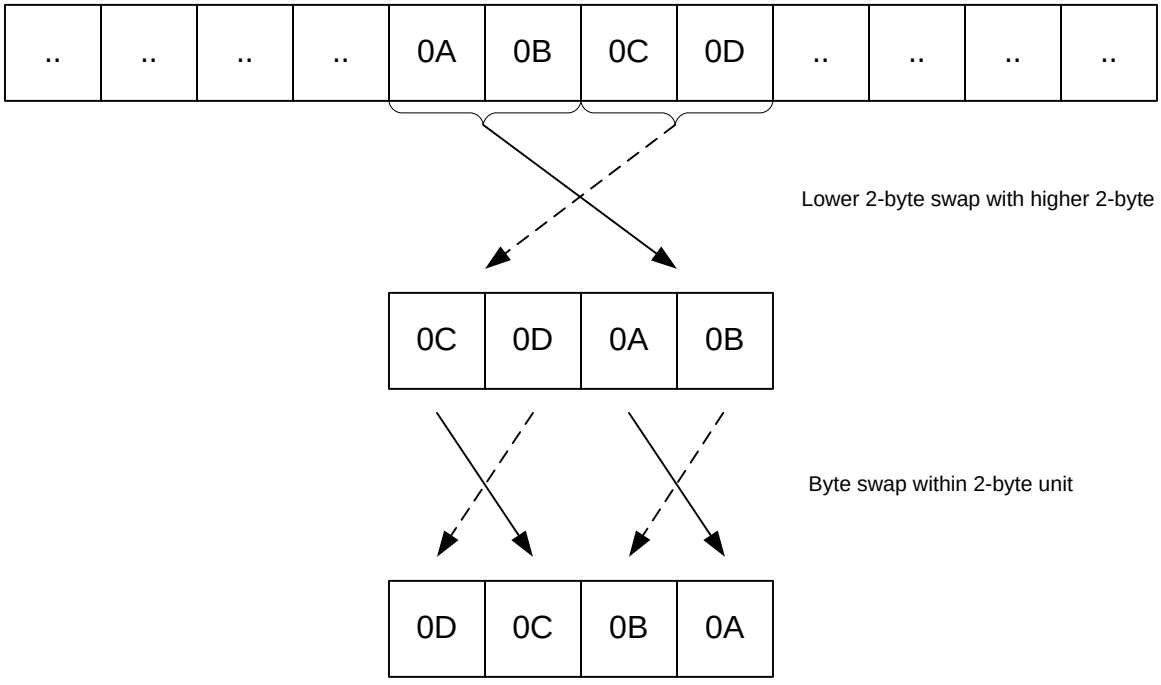


Figure 28: Motorola HMAC Byte Ordering

Below is a working example for the byte-order schema used in MOTOTRBO R1.4, R1.5 and R1.5A releases.

Assume the input message is a LE_MASTER_PEER_REGISTRATION_REQUEST in hex:

90 00 00 00 19 40 00 10.

If the authentication key is configured in CPS as

1111111111111111111111111111111111111111, the radio uses it as a hex string of 0x1111111111111111111111111111111111111111 in the hash calculation..

	Standard HMAC Calculation	HMAC Calculation with Motorola byte-ordering
Stage-One Hash Value	05 95 8a c3 08 89 c7 33 62 b3 93 35 36 7b 8e c5 c8 97 85 b7	c3 8a 95 05 33 c7 89 08 35 93 b3 62 c5 8e 7b 36 b7 85 97 c8
Stage-Two Hash Value	91 03 d8 ae 2e 01 65 74 55 ae b0 e1 3f c7 42 23 1a ba 13 38	9f a1 39 40 ac 52 f5 d2 d0 9f b2 29 dc 52 2e 5e e4 46 2e 69
Message with Authentication Header (10-byte HMAC output)	90 00 00 00 19 40 00 10 91 03 d8 ae 2e 01 65 74 55 ae	90 00 00 00 19 40 00 10 9F A1 39 40 AC 52 F5 D2 D0 9F

Note: If the authentication key configured in the CPS is less than 40 characters, CPS pads the authentication key to full 40 characters with zeros before the HEX conversation. For example, if configured as ABCDE in CPS, the authentication key value is HEX 0x0000000000000000000000000000000000ABCDE.

RA-SW-1750

RA-SW-1750