STANDARD

HART®

COMMUNICATION PROTOCOL

Wireless Command Specification

HCF_SPEC-155, Revision 2.0

Release Date: 12 June 2012

Release Date: 12 June 2012

Document Distribution / Maintenance Control / Document Approval
To obtain information concerning document distribution control, maintenance control, and document approval please contact the HART Communication Foundation at the address shown below.

Trademark Information
HART® and WirelessHART® are registered trademarks of the HART Communication Foundation, Austin, Texas, USA. Any use of the term HART or WirelessHART hereafter in this document, or in any document referenced by this document, implies the registered trademark. All other trademarks used in this or referenced documents are trademarks of their respective companies. For more information contact the HCF Staff at the address below.

Attention: Foundation Director
HART Communication Foundation
9390 Research Boulevard
Suite I-350
Austin, TX 78759, USA
Voice: (512) 794-0369
FAX: (512) 794-3904

http://www.hartcomm.org

Use of imperatives in HART Specifications
The key words (imperatives) "must", "required", "shall", "should", "recommended", "may", and "optional" when used in this document are to be interpreted as follows:

Must	**Must**, **Shall**, or **Required** denotes an absolute mandatory requirement. For example, "All HART Field Devices must implement all Universal Commands"
Should	**Should** or **Recommended** indicates a requirement that, given good cause/reason, can be ignored. However, the consequences of ignoring the requirement must be fully understood and well justified before doing so.
May	**May** or **Optional** identifies a requirement that is completely optional and can be supported at the discretion of the implementation. May can be used to identify optional Host Application or Master functionality and, when this is the case, does not imply the function is optional in Field Devices.

Intellectual Property Rights
The HCF does not knowingly use or incorporate any information or data into the HART Specifications which the HCF does not own or have lawful rights to use. Should the HCF receive any notification regarding the existence of any conflicting Private IPR, the HCF will review the disclosure and either (a) determine there is no conflict; (b) resolve the conflict with the IPR owner; or (c) modify this specification to remove the conflicting requirement. In no case does the HCF encourage implementors to infringe on any individual's or organization's IPR.

Table of Contents

Preface

Revision 2.0 of the *Wireless Command Specification* both incorporates clarifications and corrections to the Specification and adds a number of useful enhancements. The enhancements fall into two broad categories:

- Improved Key Performance Indicators (KPIs); and
- Security Enhancements

Key Performance Indicators

Field experience and positive feedback from NAMUR (and several large end users) have led to enhancements to the performance statistics mandated in this Specification. In particular, improvements have been made to support NAMUR requirements for Key Performance Indicators (KPIs). These improvements, in many cases, result in expansion and standardization of statistics provides by Gateways. For example Command 840 was expanded and Command 846 was added to provide a summary of network performance.

In addition, "Stale Data" detection was added (see Commands 852-854). These standardize Gateway reporting should process data or events fail to arrive at the Gateway in a timely fashion. For example, Host Applications will receive the "Update Failure" Response Code should the process data in the command response be stale.

Security

WirelessHART has always supported Access Control Lists and the quarantining of devices pending their acceptance into the network. Improved standardization has been added in this Specification to promote interoperable application of these capabilities. This includes enhancements to Common Tables 55 and 56 (see the *Common Tables Specification*). In addition, Command 847 was added to simplify the population of the whitelist.

Simple key management interface is standardized and supplied in this Specification. Commands 848-850 allow the allocation of join keys and their synchronization between the Network Manager and the new (about to join) Field Device. These commands allow join keys to be allocated and managed without their disclosure to humans.

In addition, Command 851 allows key changes to be triggered (e.g., key changes can be triggered per plant security policy).

Summary

In total, 20 new commands have been developed, reviewed by HCF Working Groups and specified in this revision of the *Wireless Command Specification*.

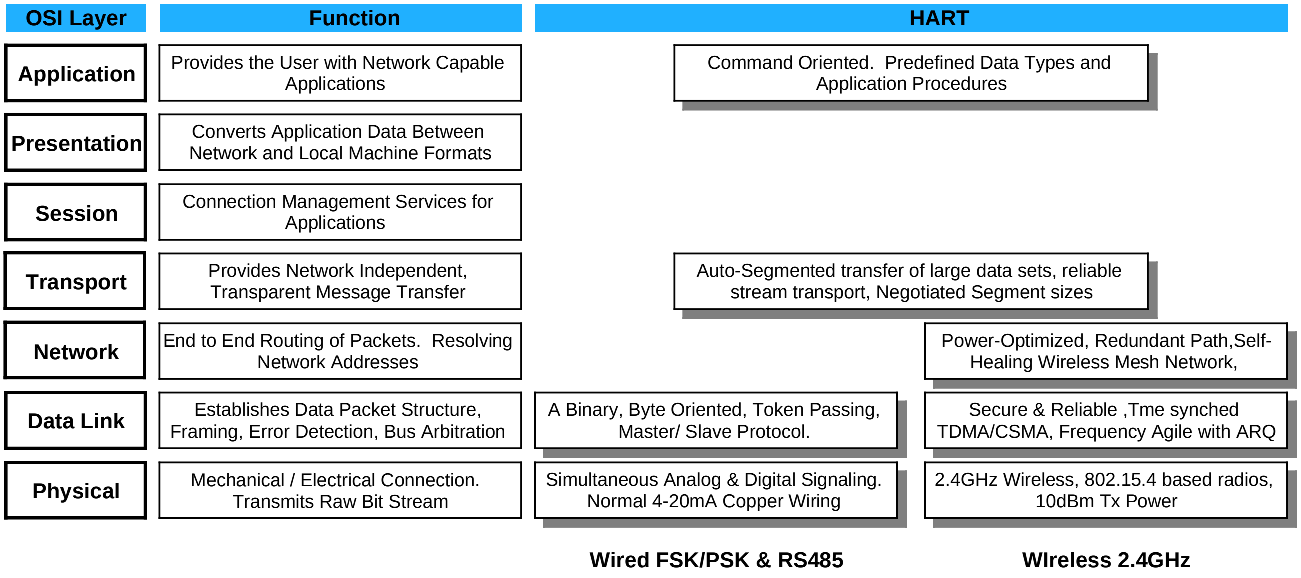
Section 6 of the Specification has been completely rewritten. Previously Section 6 did little more then list commands. In this release the commands are logically allocated to subsections. Then, within each subsection, detailed information and requirements on command operation are provided. The new and improved Section 6 enables more rapid assimilation of command operation and better insight into how the wireless commands work together.

In addition, a large number of clarifications and corrections have been made to the specification based on HCF Member feedback, suggestions from HCF Working Groups and experience gained in testing and registering many WirelessHART Field Devices.

Introduction

The *Wireless Command Specification* is a key document in the WirelessHART Specifications as it establishes the minimum Application/Network layer support required of all WirelessHART devices.

The Application Layer in HART defines the commands, responses, data types and status reporting supported by the Protocol. In addition, there are certain conventions in HART (for example how to trim the loop current) that are also considered part of the Application Layer. While the Command Summary, Common Tables and Command Response Code Specifications all establish mandatory Application Layer practices (e.g. data types, common definitions of data items and procedures), the WirelessHART Commands specify the minimum Application/Network Layer content for all WirelessHART compatible devices.



OSI Layer	Function	HART	
Application	Provides the User with Network Capable Applications	Command Oriented. Predefined Data Types and Application Procedures	
Presentation	Converts Application Data Between Network and Local Machine Formats		
Session	Connection Management Services for Applications		
Transport	Provides Network Independent, Transparent Message Transfer	Auto-Segmented transfer of large data sets, reliable stream transport, Negotiated Segment sizes	
Network	End to End Routing of Packets. Resolving Network Addresses		Power-Optimized, Redundant Path,Self-Healing Wireless Mesh Network,
Data Link	Establishes Data Packet Structure, Framing, Error Detection, Bus Arbitration	A Binary, Byte Oriented, Token Passing, Master/ Slave Protocol.	Secure & Reliable ,Tme synched TDMA/CSMA, Frequency Agile with ARQ
Physical	Mechanical / Electrical Connection. Transmits Raw Bit Stream	Simultaneous Analog & Digital Signaling. Normal 4-20mA Copper Wiring	2.4GHz Wireless, 802.15.4 based radios, 10dBm Tx Power
		Wired FSK/PSK & RS485	**WIreless 2.4GHz**

Figure 1. OSI 7-Layer Model

This document provides application layer command information for WirelessHART Network Manager, Gateway and device developers. Many of these application layer commands are used to control other layers within the protocol stack such as the physical layer, data link layer and the network layer.

1. SCOPE

The *Wireless Command Specification* is an Application Layer specification and accordingly builds on the Application Layer Requirements found in the *Command Summary Specification*. Conformance to all requirements of the Command Summary Specification is a prerequisite to conforming to this specification.

This specification contains both the definitions and the recommended usage of Wireless Commands. Wireless Commands, if used, must be implemented exactly as specified. Many Wireless Commands refer to tables from the Common Tables Specification. When Common Tables are referenced, the tables must be used exactly as specified.

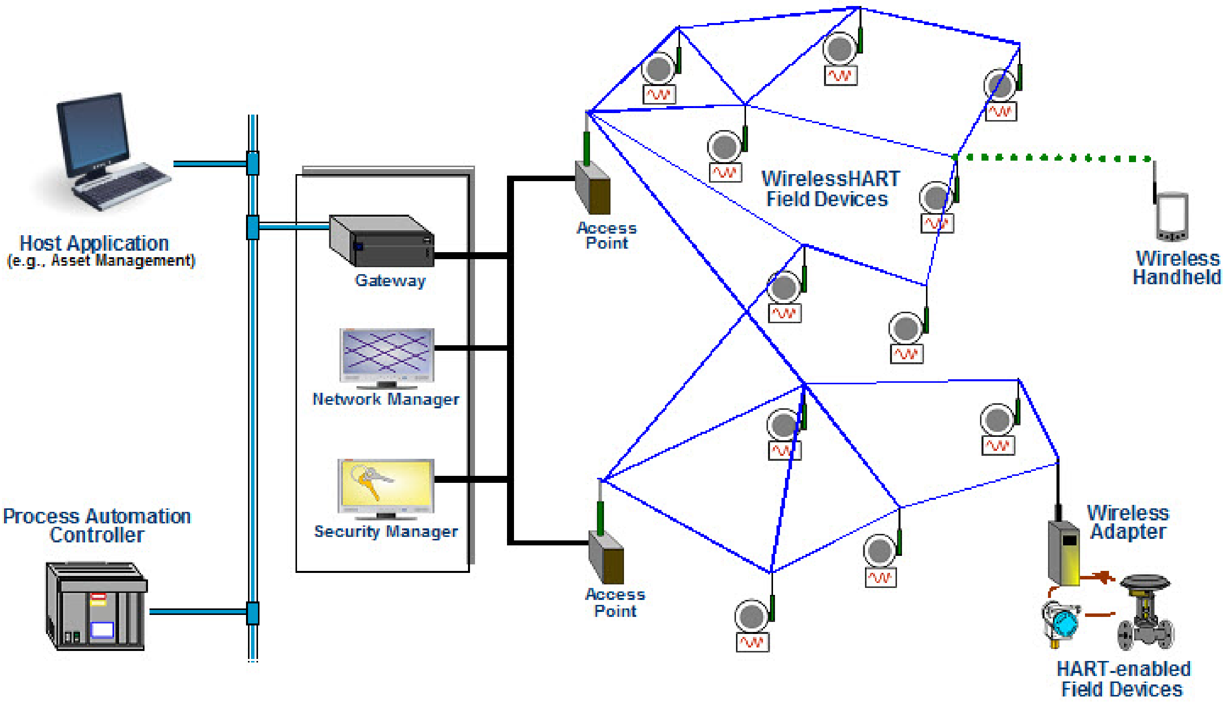


Figure 2 Elements of a WirelessHART Network

This specification contains commands that must be implemented by a Network Manager and Gateway as depicted in Figure 2 above. It also provides standard commands that must be implemented for the configuration of each device's Physical Layer, Data Link Layer as well as Network Layer.

2. REFERENCES

2.1 HART Field Communications Protocol Specifications

These documents published by the HART Communication Foundation are referenced throughout this specification:

HART Field Communications Protocol Specification. HCF_SPEC-13

TDMA Data Link Layer Specification. HCF_SPEC-075

Network Management Specification. HCF_SPEC-085

Command Summary Specification. HCF_SPEC-99

Common Tables Specification. HCF_SPEC-183

WirelessHART Device Specification. HCF_SPEC-290

Command Response Code Specification. HCF_SPEC-307

2.2 Related Documents

The following reference provides additional information about and algorithms used in conjunction with AES-128 cipher for security.

National Institute of Standards and Technology, U.S. Department of Commerce, "Specification for the Advanced Encryption Standard", Federal Information Processing Standards Publication 197 (FIPS-197), November 2001.

B. Gladman’s AES related home page http://fp.gladman.plus.com/cryptography_technology/.

3. DEFINITIONS

The HART Protocol Specifications must use a common and consistent vocabulary both within a specification and across all specifications. This section incorporates (by reference) definitions from the HART Field Protocol Specification (HCF_SPEC-12) and defines the terms unique to this specification. Vocabulary or phrases used in more then one specification must be defined in the HART Field Protocol Specification. Sometimes key definitions found in there are repeated and amplified in this section (rather then simply incorporating by reference).

Definitions for terms can be found in *HART Field Communications Protocol Specification.* Terms used throughout the *Wireless Command Specification* include: Superframe, neighbor, key, nonce, MAC, session, route, graph, RSL, ASN.

Some other terms used only within the context of the *Wireless Command Specification* are:

Availability Availability is the percentage of packets that arrive at the Gateway within the burst period of the device.

Coexistence Coexistence is the ability of one system to perform a task in a given shared environment in which other systems have an ability to perform their tasks and may or may not be using the same set of rules (IEEE).

Connected (to the network) The device has issued a Join Request.

Graph ID An identifier used to indicate a specific graph entry

Joined (to the network) The device is in communication with the Network Manager and has received at least: the Network Key, its Nickname, the Unicast Network Manager Session, a Superframe and links from the Network Manager, Graph Edges [1], a Time-source Neighbor, and a Route to the Network Manager.

Latency The time it takes for a packet to cross a network connection, from sender to receiver.

Packet Error Rate Packet Error Rate (PER) is the percentage of failed transmits to a device. The PER is given on a neighbor-by-neighbor basis.

Packet Loss Rate Packet Loss Rate is the percentages of packets lost by the WirelessHART network. This is derived from the Packet Loss Counter.

Parameterization Configuring a field device for proper operation in a given plant installation.

Portal The combination of Gateway, Network Manager, and Access Point(s)

Provisioning Configuring a field device for integration into the HART network.

Route ID An identifier used to indicate a specific route

Session ID An identifier used to indicate a specific session entry

Superframe ID An Identifier used to indicate a specific superframe entry

Throughput Average number of packets per second transmitted or received by the Network Manager and Gateway.

Transmission Time The time for a packet to traverse the network from the source to the destination.

Utilization Percentage of recommended capacity currently consumed.
(i.e., Throughput divided by (20 times Number of Access Points).

[1] If Superframe routing is specified then graph edges are inferred from Tx Links (see *Network Manager Specification*)

4. SYMBOLS/ABBREVIATIONS

DR **D**elayed **R**esponse.

LSB **L**east **S**ignificant **B**yte. The LSB is always the last byte transmitted over a HART data link.

MSB **M**ost **S**ignificant **B**yte. The MSB is always the first byte transmitted over a HART data link.

KPI **K**ey **P**erformance **I**ndicators

5. DATA FORMAT

In command specifications, the following key words are used to refer to the data formats. For more information about these formats, see the *Command Summary Specification*.

Bits Each individual bit in the byte has a specific meaning. Only values specified by the command may be used. Bit 0 is the least significant bit.

Enum An enumerated value. Only values specified in the *Common Tables Specification* may be used.

Date The Date consists of three 8-bit binary unsigned integers representing, respectively, the day, month, and year minus 1900. Date is transmitted day first followed by the month and year bytes.

Time The Time consists of a unsigned 32-bit binary integer with the least significant bit representing 1/32 of a millisecond (i.e., 0.03125 milliseconds).

Packed A string consisting of 6-bit alpha-numeric characters that are a subset of the ASCII character set. This allows four characters to be packed into three bytes. Packed ASCII strings are padded out with space (0x20) characters.

Unsigned-*nn* An unsigned integer where *nn* indicates the number of bits in this integer. Multi-byte integers are transmitted MSB - LSB.

Signed-*nn* A twos complement signed integer where *nn* indicates the number of bits in this integer. Multi-byte integers are transmitted MSB - LSB.

6. APPLICATION OF WIRELESSHART COMMANDS

6.1 Provisioning

Fundamentally, a WirelessHART Field Device only requires a valid Join Key and the correct Network ID in order to join the WirelessHART Network. These two data items may be written to the Field Device, for example, during the manufacture of the Field Device; while connected via the maintenance port to the Gateway; or by the instrument technician during the commissioning of the Field Device. That being said, the Protocol provides several additional commands to further support and customize the initial connection to the network including:

- Command 768 Write Join Key allows the 128-bit security key to be written to the Field Device[2].
- Command 773 Write Network ID and Command 774 Read Network ID identifies the network the device is to join.
- Command 769 Read Join Status allows the Field Device's progress toward joining the network.
- Command 770 Request Active Advertising can be used to improve the Field Device's chances of finding and joining the network quickly.
- While fine-tuning is generally not necessary, Command 771 Force Join Mode and Command 772 Read Join Mode Configuration can be used to control or fine tune join parameters.
- Command 797 Write Radio Transmit Power and Command 798 Read Radio Transmit Power can be used to specify the Transmit Power.

The two subsections describe the basic and optional provisioning procedures

6.1.1 Basic Provisioning

This subsection summarizes the basic steps for connecting a Field Device to a WirelessHART network. First the device must be provisioned:

- Using Command 768, write the Join Key to the Field Device. The join key must match the value provided in the Gateway. If the value is not correct join attempts will fail.
- Write the Network ID the Field Device (Command 773). The Network ID must match the ID of the network the device is to join.
- Perform optional provisioning (as needed).

The configuration for a join can be read using Command 774 to read the Network ID and Command 772 to read the join mode configuration. The join key can never be read from the device to avoid someone stealing the join key to introduce rogue devices or other attacks against a WirelessHART network.

[2] To further enhance security, Network Managers should change the join key after the Field Device joins.

6.1.2 Joining

The Field Device is now ready to join this network. Initial introduction of the Field Device to the network can be performed as follows:

- When the device has been installed and is ready to join the network, “Join now” is written using Command 771. The device will then scan the frequencies for advertisements and network traffic from the specified network. The parameters Active Search Time and Number of Join Retries determine how long the device will listen for the network and how often a join is attempted.

- The device's progress toward joining the network can be monitored using Command 769. Polling Command 769 provides the Join Status, the progress of a join attempt, number of detected neighbors and acquired advertisements. It also includes the active search time remaining.

- The device is joined once the Network Manager answers the Join Request (see the *Network Management Specification*) and writes the security keys and normal communication parameters (Network Manager route, Superframe, links, time source neighbor.)

6.1.3 Enabling Faster Network Detection and Joining

Advertisements are sent periodically on random frequencies and joining device must be on the right frequency at the right time to hear the advertisements. Consequently, joining can take some time as the joining device listens for advertisements. Using Command 770, the probability of network detection (and thus the joint time) may be improved by increasing the frequency of advertisement transmissions.

Increasing the advertisement rate consists of:

- Issuing Command 770 to the Gateway or via the maintenance port to a Field Device already in the network. In either case the recipient (Gateway or Field Device) must forward the command to the Network Manager.

- The Network Manager replies to Command 770 and increases the advertisement rate[3] for the interval indicated by "Active Advertising Shed Time".

- The new Field Device receives advertisements quickly and joins the network.

- Command 770 is issued once again (with Active Advertising Shed Time = 0) and the Network Manager advertisement rate is reduced for normal network operation.

6.1.4 Adjusting Transmit Power

Optionally, prior to joining the network, Command 797 may be used to configure the Field Device's transmit power. For more information see Subsection 6.7.3 Coexistence.

[3] Higher advertisement rates can increase the power consumption of the network.

6.2 Managing Superframes and Links

WirelessHART is a channel hopping, redundant mesh network. Superframes (and the Links they contain) specify the actual communication connections between devices within the mesh. Superframes and Links are Data-Link Layer functions with Links specifying communication opportunities and the Superframe (container) they reside in determine the frequency at which the communication opportunity arises. Three commands are used to create and manage a Superframe:

- Command 783 Read Superframe
- Command 965 Write/Modify Superframe
- Command 966 Delete Superframe

Superframes can be enabled and disabled by the Network Manager as needed. While disabled modifications can be performed to the Superframe and all of the Links for the Superframe can be created. Then the Superframe can be quickly enabled and disabled when bandwidth demand changes. For example, a preconfigured (but disabled) Superframe can be enabled by one command being broadcast along a graph to provide extra bandwidth for a surge in request/response traffic to a device in the network.

Superframe contains the specified number of slots and. once enabled, the Superframe shall continuously repeat. As the slot time occurs all Links assigned to that slot in the Superframe must be evaluated (see *TDMA Data-Link Layer Specification*).

Links are contained within a Superframe and are assigned to a slot. All devices must all multiple Links to be assigned to a single slot. The Link specifies a communication opportunity within a Superframe. Three commands are used to manage Links:

- Command 784 Read Link
- Command 967 Add Link
- Command 968 Delete Link

Links are identified by the unique combination (e.g., concatenation) of the Superframe ID, Slot Number, Neighbor Nickname[4] associated with a Link. The Network Manager may Add or Delete a Link (modification of an existing Link is not allowed).

If the Network Manager Adds a link with a hereto-unknown Neighbor the device must add Link and it must add the specified Neighbor to its Neighbor Table (see *TDMA Data-Link Layer Specification*). Deleting a the last link to a neighbor deletes the neighbor from the Neighbor Table.

If the Network Manager deletes a Superframe the device must also delete all links contained in the (deleted) Superframe.

[4] The Neighbor Nickname must be ignored when receiving a packet (i.e., only DLPDU Destination Address is relevant when receiving a packet).

6.3 WirelessHART Handheld Support

Universal support for HART-enabled Handhelds (wired and wireless) is a critical end-user requirement and support for Handhelds in HART-enabled products is essential. Network Managers, Gateways, Field Devices and other Wireless Devices must support and interoperate with WirelessHART Handhelds.

A Network Manager must create the Handheld Superframe (see Common Table 47 Superframe Mode Flags) in all devices (e.g., Field Device and Adapters). The Handheld and device must communicate directly with each other using the Handheld Superframe[5]. Two commands are used by the Handheld to initiate communications with the device to be serviced:

- Command 806 Read Handheld Superframe read the status of the Handheld Superframe.
- Command 807 Request Handheld Superframe Mode is used to activate (and deactivate) the Handheld Superframe as needed.

To enable Handheld use in a WirelessHART installation:

- Network Manager (using guidance and keys from the Security Manager) must establish a session in the device and Handheld to enable secure communications between them (see Command 823 Request Session).
- Network Manager must create a matching "Handheld Superframe" (with Links) in the device and Handheld.
- Once on site, Handheld must monitor and synchronize itself to network communications[6].
- The Handheld must identify the Handheld Superframe in the device and activate it in the device to be serviced. The Handheld must also activate its corresponding Superframe.
- Upon request devices (e.g., Field Device and Adapters) must immediately enable the Handheld Superframe.
- The Handheld and device must communicate directly with each other using the Handheld Superframe[7].

Terminating communications between the Handheld and device:

- Upon detecting a path down to the Handheld the device must assume the Handheld is no longer available. When this happens the device must: (a) deactivate the Handheld Superframe; and (b) forward the Path Down Alarm to the Network Manager.

More information about Handhelds can be found in the *Wireless Devices Specification*.

[5] Devices must not forward to the network any packets received from the Handheld. Any packet from the Handheld with a Network Layer destination other then the device must be discarded.

[6] Initial communications between Handheld and the device shall be via an advertised Superframe (of Handheld choosing). The Superframe ID selected by the Handheld shall be the Graph ID in the NPDU.

[7] Graph ID in NPDU must be Superframe ID.

6.4 Specifying and Managing Routes

Routes and Graphs are Network Layer functionality and the routing of network packets is a fundamental Network Manager responsibility. In WirelessHART, Graph Routing is the fundamental methodology used for routing of communications. The following three commands are used to establish and manage the routes that must be used by a Field Device when it creates a network packet:

- Command 802 Read Route
- Command 974 Write/Modify Route
- Command 975 Delete Route

The Field Device must use the Route specification corresponding to the destination device when creating a new network packet. The Route information is embedded in the network packet allowing it to be transferred over multiple hops to the desired destination (e.g., another Field Device). Only the Network Manager is allowed to create, modify or delete a Route.

A Graph Route is a redundant, multi-path, unidirectional route from the source device to the destination device. The Graph consists of nodes and edges. The nodes are Field Devices. The Network Manager constructs the Graph Route specifying the graph edges at each Field Device (node) along the route. In other words the edges identify neighbors to whom a Field Device must use when forwarding a network packet along a Graph. Remember that

- A Route is used when a device creates a network packet and
- Graphs are used to route network packets (both generated by the device and those forwarded by the device on behalf of another).

Consequently, the Network Manager will write graph edges to a Field Device that are not specified in any of the Routes used when the device creates a network packet. Three commands are used by the Network Manager to manage Graph Routes:

- Command 785 Read Graph List
- Command 969 Add Graph Edge
- Command 970 Delete Graph Edge

Only graph edges for outbound network packets are written to the Field Device. Graph edges must be used (by the device) to identify the set of neighbors to which a network packet maybe forwarded. Superframes and Links determine when the network packet may actually be transmitted.

Routes may also be specified using Source Routing. Source Routing specifies each hop that the network packet must take to reach its final destination. Since it does not provide redundant paths, Source Routing is not reliable and should not be used for recurring communications (e.g., routine request/response or burst-mode traffic). Source Routing is useful for ad-hoc routes that are only used for less than 60 minutes or for probing communication paths. The following three commands are used to manage Source Routes:

- Command 803 Read Source-Route (Optional)
- Command 976 Write/Modify Source-Route (Optional)
- Command 977 Delete Source-Route (Optional)

The implementation of Source Routes in Field Devices is optional.

6.5 Security

Security is fundamental to WirelessHART and essential to prevent malicious attacks on WirelessHART network. WirelessHART uses industry standard[8] AES-128 symmetric-key encryption. WirelessHART includes:

- Encryption of all Network Layer PDUs (NPDU) to ensure end-end communication confidentiality;
- Join keys used to encrypt all join requests/responses;
- Session keys used to encrypt end-end communication; and
- Data-Link level "Network (Data-Link) Keys" used to ensure the integrity of communications on a hop-by-hop basis.

Commands in this subsection facilitate the management of keys and sessions and enables controlled access to the network. In addition two commands allow for future enhancements to WirelessHART security:

- Command 979 Write Security Level Supported; and
- Command 857 Read Security Level Advertised

These two commands allow the security level supported by the Network Manager to be disclosed to devices joining the network. While today only "Joined-Keyed" (see Common Tables 53) is supported security best practices may evolve over time. These commands allow for potential evolution.

6.5.1 TDMA Data-Link Key Management

An AES-128 Network (Data-Link) Key is used to authenticate (but not encipher) the DLPDU. The following command allows the key to be written/changed.

- Command 961 Write Network (Data-Link) Key

All devices in the WirelessHART network must use the same Network (Data-Link) Key.

6.5.2 Session Key Management

There are 5 commands used to manage sessions.

For security, WirelessHART is session oriented thus enabling private and secure communication between a pair of network addresses. Three commands are used by the Network Manager to manage session in devices:

- Command 782 Read Session allows the sessions is a device to be read;
- Command 963 Write/Modify Session allows the session creation or modification (e.g. changing the session key); and
- Command 964 Delete Session that removes a session.

In addition there are two additional session management-related commands:

- Command 823 Request Session is used by (for example) Handheld to request a session with a device. Typically a Handheld is provisioned (e.g., based on service/work orders) to allow one or more devices be serviced. This command allows the session for the device to be provided to the Handheld. When this command is used the Network Manager must also configure the session in the device to be serviced to enable communication with the Handheld.
- Sessions correspond to end-end connections supported by a device. Command 855 Read Session (Extended) allows the end-end connections in a device to be read via the Gateway.

[8] e.g., FIPS PUB 197 (FIPS 197) by the US National Institute of Standards and Technology (NIST)

6.5.3 Access Control

The following four commands control criteria Gateways use for allowing devices to join the network. Devices that are part of the network can cause more damage then those that are not in the network. Consequently, it is very important to only allow trusted devices into the network. These commands control the level of trust required for admission to the network.

- Command 821 Write Network Access Mode
- Command 822 Read Network Access Mode
- Command 860 Read Join Key Mode
- Command 861 Write Join Key Mode

Gateways may contain access control lists. Commands 821 and 822 allow the use of black lists, white lists to be specified. These commands even allow the network to be locked down so no new devices may join the network. Depending on the Network Access Mode (see Common Table 56) authentication beyond confirming the Join key can be specified. For example:

- Only devices on the Whitelist can be allowed to Join[9];
- Those on the Blacklist[10] are not allowed to join; or
- Only devices on the Network List (see Common Table 55) are allowed to join.

Once joined, the device is added to the Active List (i.e., allowed to be used by Host Applications and for plant operation) and the Network List.

Often a network does not have access control enabled when it is first being commissioned. When the network deployment is complete and access control is to be asserted, Command 847 Transfer Network List to White List is used to create or update the Whitelist[11].

The Join Key Mode (see Common Table 80) may also be relaxed. By default, each device should have its own, unique join key. The Join Key Mode commands allow (at the risk of reduced security) the Join Key to be either the "well-known" key or a key common to all devices. This allows a customer to get the devices quickly provisioned to the network and then once the devices are on they can transition the network to a random network wide join key.

When Join Key Mode is relaxed, the Network Access Mode should be set to Quarantine, Whitelist or Lockdown. While in Quarantine mode all devices not previously in the network (i.e., not in the Network List) are Quarantined and must by authenticated by the network operator.

In other words, using these four commands with new networks it is possible to relax security to facilitate simple rapid network commissioning and, once the network is established, tighten security to make the network operational.

[9] If the whitelist is empty no devices are allowed to join.

[10] Field devices should support blacklists to prevent join requests from un-welcome devices. In other words, if a device detects a join request from a blacklisted device the join request must be discarded (i.e., not forwarded).

[11] Commands 821 and 822 control whether whitelists and blacklists are used for network access control.

6.5.4 Simple Key Management

The following four commands provide simple key management. The first three commands simplify creation and management of join keys. The last command (Change Key Now) allows all keys to be changed periodically. Security is enhanced by periodically changing the keys.

- Command 848 Generate Key.
- Command 849 Read Device's Join Key
- Command 850 Write Device's Join Key
- Command 851 Change Key Now

Generate Key is a simple command that generates and returns a key. This key could be used with the Write Join Key and Write Device's Join Key commands to provision a device for joining the network. Best practice would be for the host application to be connected and communicating with both the Gateway and the Field Device (via its maintenance port using Command 768). This simplifies provisioning and the actual key value never displayed to the user.

Alternatively, the Read Device's Join Key can be used. This generates a random Join Key and configures the Network Manager to allow the Field Device to join the network. Using the response the host application can provision the Field Device (via its maintenance port using Command 768).

In the worst-case scenario both of these approaches allow the Join key to be displayed to the user. The user can write the join key the Field Device (e.g., using a Handheld) at a later time[12].

The Change Key Now command allows a Host Application to force a key change (e.g., in reaction to a security concern or to comply with the plant's security policy).

These Commands along with Commands 814-816 (for whitelist/blacklist management) and Command 821-822 (for managing the network access mode) provide the application interfaces for Host Applications to implement plant security strategy.

[12] In any case, once a device joins the network its Join Key should be changed by the Network Manager. This best practice ensures no human knows the Join Key.

6.6 Device Lists

Gateway and Network Manager must maintain and provide access to device lists. These lists are wireless-specific; used to enumerate devices associated with a Network; and manage device access to the Network. Commands used to access device lists include:

- Command 814 Read Device List Entries - Read a device list
- Command 815 Add Device List Table Entry - Adds a device to active, white, black, or network list.
- Command 816 Delete Device List Table Entry
- Command 847 Transfer Network List to White List

Common Table 55 enumerates the lists (e.g., active, network, white and black lists). These lists are WirelessHART-centric and shall only identify WirelessHART devices. WirelessHART Adapter connected devices, for example, must never be included in a device list[13].

Whenever a device attempts to join the network its Join Key is authenticated. If access control (see Common Table 56) is enabled the Whitelist and Blacklist are consulted. For security procedures and requirement see Subsection 6.5.

When a device disappears from the Active Device List (e.g., due to a loss of connection[14]), the device is not removed from the Network list[15]. The device remains on the Network list until removed using Command 816.

When the device is not in the Active or Quarantined Device List, it can be removed directly from the Network List (i.e., if the device is not connected to the network). Otherwise the device must be decommissioned first. Quarantined devices and Access Points are also included in the Network list. The Gateway must maintain KPI statistics[16] for all devices on the Network list.

When a device is removed from the Active Device List via Command 816 (e.g., when depot-level service is required) the device is decommissioned[17] and dropped from the network.

[13] To identify all devices that may be accessed via a given WirelessHART Gateway see Command 84. Command 84 must identify and list all devices (i.e., the "Live List" see *Common Practice Specification*) in the Active Device List plus all devices connected to WirelessHART Adapters.

[14] A device is not connected (dropped from the Active list) upon either (1) detecting a Transport Layer failure; (2) reception of Path Down Alarm on all connections to the Field Device; or (3) the Gateway session does not exist

[15] Consequently, the Network list should capable of containing more devices then the Gateway will support. This allows, for example, for device replacement even when the Gateway is at its capacity.

[16] KPI Statistics are only kept until the power is cycled on the Gateway. Once the Gateway power is cycled, the statistics are reset/cleared.

[17] The device is decommissioned by: sending Command 771 with Join Mode Code set to "Don't attempt to Join"; and sending Command 42. Once restarted the device will not attempt to re-join the network.

6.7 Network Management Commands

The Network Manager is responsible for the system-wide operation of the network. In other subsections specific networking functions are addressed (e.g. security, routing, and mesh inter-connectivity). This subsection identifies commands and requirements for a variety of Network Management functions including:

- Bandwidth Management
- Network Maintenance
- Coexistence
- Device Management

6.7.1 Bandwidth Management

Congestion is perhaps the most serious threat to network stability. Bandwidth management is a key tool used by the Network Manager to manage network congestion. The following commands are used to request, allocate and manage the timetables used to manage bandwidth:

- Command 799 Request Timetable
- Command 800 Read Timetable
- Command 801 Delete Timetable
- Command 862 Read Timetable by ID
- Command 973 Write/Modify Timetable

Command 799 requests are generated by the requesting device and sent to the Network Manager (or Gateway if generated by a host application). The Network Manager may respond immediately is the requested bandwidth is known to be available or after compete a Delayed Response. Once the device has bandwidth (the full amount requested or something less) packets using the bandwidth are generated at up to that allocation.

Once the bandwidth is no longer needed the device must return it to the Network Manager using Command 801. If the Network Manager needs to reduce network congestion it can use Command 973 to modify the current timetable configuration.

If the device does not have the full amount of bandwidth it wants it must periodically, once per Health Report interval, issue a Command 799 to ask for more bandwidth. While the bandwidth is reduced the device must still continue to publish process data at the best speed possible consistent with the timetable setting.

The Network Manager also has flow controls that can be used to reduce network congestion[18]. The flow controls are managed using the following commands:

- Command 812 Read Packet Receive Priority
- Command 813 Write Packet Receive Priority

For example, Command 813 may be used by a Network Manager to block "Alarm" or "Normal" (see 8.1.4 DLPDU Specifier in *TDMA Data-Link Layer Specification*) priority messages across all or part of the network to immediately reduce congestion.

6.7.2 Network Maintenance

There are a number of network management commands allowing, for example, join priorities, timers (discovery, keep-alive, etc) and other general maintenance of the network by the Network Manager. This commands include:

- Command 795 Write Timer Interval;
- Command 796 Read Timer Interval;
- Command 808 Read Packet Time-to-Live;
- Command 809 Write Packet Time-to-Live;
- Command 810 Read Join Priority;
- Command 811 Write Join Priority;
- Command 819 Read Back-Off Exponent;
- Command 820 Write Back-Off Exponent;

Commands 795 and 796 read and write timers that control a variety of time values that can be used to tune Field Device network behavior. Common Table 43 contains the list of timers that may be fine-tuned. Other specifications define the timers themselves (e.g., health report intervals, keep alive times, etc.) and specify default values that enable reliable, responsive network behavior "out-of-the-box".

In general, no WirelessHART packet is ever discarded (i.e., once it is created in the originating device it will travel the network until it reaches its final destination). However there are two safeties that prevent packets from wandering the network indefinitely: "Time-To-Live" (TTL) and "Maximum PDU Age". The former (TTL) is managed using commands 808 and 809[19]. TTL is included in an NPDU field whose value is initialized when the PDU is created and decremented upon each hop the packet takes across the network. When TTL reaches 0 the packet must not be forwarded to another device (see *Network Management Specification* for more information). The Maximum PDU Age is managed using Commands 795 and 796. This allows time-based criteria to be established by the Network Manager to specify packet disposal to complement the TTL criteria.

Join Priority indicates to devices joining a WirelessHART network the preferred neighbor to join to. In general, Network Managers should set the join priority to a lower value the closer a device is to an Access Point. Commands 810 and 811 are used by the Network Manager to manage the Join Priority advertised by the Field Device.

WirelessHART enables flexible communication bandwidth utilization to allow on-demand use by devices in the form of "Shared Slots". Shared Slots allow multiple devices the opportunity to transmit a packet in the

[18] Network congestion (in the extreme) can cause a network-wide failure. Flow control can modulate communication traffic thus ensuring network survival. Both excessive congestion and flow control may result in packet loss.

[19] This allows TTL to be set (for example) to a large value when installing a device in a long large stringy network.

same slot. Should a collision occur the devices will "back-off" a random number of Shared Slots. Commands 819 and 820 allow the maximum back-off interval to be set.

6.7.3 Coexistence

Coexistence is a key WirelessHART requirement and strength. WirelessHART has both the ability to perform successfully in the presence of interference from other networks and protocols and the features to share the RF space. The following commands allow WirelessHART's sharing of the RF space to be tailored on an installation-by-installation basis

- Command 804 Read CCA Mode and Command 805 Write CCA Mode are used to manage the Clear Channel Assessment (CCA) settings in the device. CCA is an optional coexistence feature that allows a device to monitor the RF space and defer communications if the RF space is in use.
- Command 817 Read Channel Blacklist and Command 818 Write Channel Blacklist[20] allow one or more RF channels to be blacklisted. Blacklisting reserves RF channels for use by other protocols and become effective only upon rebooting the network.
- Command 797 Write Radio Transmit Power and Command 798 Read Radio Transmit Power allow the Field Device's Transmit Power to be adjusted based on the mesh density or to meet regulatory requirements.

For the IEEE 802.15.4 Physical Layer blacklisting and CCA generally provide limited benefits in practice. The modulation used by IEEE 802.15.4 is generally both tolerant and unobtrusive to other (at least IEEE compliant) protocol/modulation standards (e.g., IEEE 802.11 WiFi).

In most cases, due the frequency hopping and very short messages used by WirelessHART, the maximum transmit power should be used. This generally improves communications and enables long distances between nodes. However, it may be beneficial for the Transmit Power to be reduced, for example, in high-density networks (thousands of devices within a 100 meters diameter).

[20] Commands 817 and 818 are Gateway commands (i.e., the Gateway is the proxy for the Network Manager). Field Devices learn the Blacklist from advertisements detected during the join process.

6.7.4 Device Management

It is incumbent on the Network Manager to manage all of the device's network related properties and attributes. The commands in this section are used to manage a variety of device properties that do not fit well in the other subsections. These commands include:

- Command 781 Read Device Nickname Address and Command 962 Write Device Nickname Address allow the Network Manager to manage the device's short (16-bit) address. This Nickname must be set before the device can finish joining the network. Consequently, Command 962 is one of the first commands from the Network Manager to a device.

- Command 777 Read Wireless Device Capabilities provides s summary of the basic capabilities and capacities of the device. Network Manager should issue this command shortly after the device joins the network

- Command 786 Read Neighbor Property Flag and Command 971 Write Neighbor Property Flag Command for the Network Manager to set which neighbor is a clock source. Devices must have a neighbor as a clock source to ensure they remain synchronized to the network. Command 971 must be one of the first commands issued by the Network Manager when a device joins the network.

- Command 793 Write RTC Time Mapping and Command 794 Read RTC Time Mapping allow the calendar time (i.e. time of day) to be correlated to network time (driven by the ASN).

- Command 960 Disconnect Device is issued by the Network Manager to force a device off the network. Depending on the device's configuration (see Common Table 61 Join Mode Code) the device may not attempt to rejoin the network.

- Command 972 Suspend Device(s) and Command 856 Read Device Suspend Setting allow devices to be suspended. Suspending allows a device to be instructed to drop off the network and become quiescent for a time. Once time has lapsed the device must rejoin the network. Joining the network is very power intensive. Consequently, the suspension interval should be for many hours. If interaction with the device is not needed for a shorter time it is more power-efficient for the device to remain in-network.

- Command 978 Write Status Counter Mode allows the device to be configured for rollover or saturating status counters. All devices must default to rollover counters.

6.8 Net work Health Reporting and Status

In addition to supporting plant applications, WirelessHART also provides continuous measurements and statistics on the RF environment the network is operating in. Periodic reports and as-needed alarms provide critical information allowing the Network Manager to groom and tune the WirelessHART network. All Field Devices must support three periodic reports:

- Command 779 Report Device Health provides the device's communication statistics;
- Command 780 Report Neighbor Health List includes statistics indicating the quality of the communication with neighbors; and
- Command 787 Report Neighbor Signal Levels report signal levels for neighbors.

These reports must be published at the period specified by the "Health Report" time (see Common Tables 43 and Commands 795 and 796). Furthermore, the three commands may be dispatch as needed by Host Applications (e.g., Gateways and Network Managers)

In addition, Field Devices must spontaneously generate alarms when specified communication errors occur. Command requests must not be generated by Applications for these commands. Should a Field Device receive a command request for one of the alarm commands it must answer with "Access Restricted". The alarm commands include:

- Command 788 Alarm: "Path Failed". Path Failed indicates the Field Device is having difficulty maintaining contact with one of its linked neighbors.
- Command 789 Alarm: "Source Route Failed". A Source Route failure indicates a packet did not reach its final destination (e.g., one of the hops in the specified source route was unsuccessful).
- Command 790 Alarm: "Graph Route Failed". A Graph Route failure indicates a packet did not reach its final destination (the packet reached the end of the graph route and could not be forwarded).
- Command 791 Alarm: "Transport Layer Failed". The Transport Layer fails when retries to the peer end-destination are not successful. The Field Device has lost contact with one of its peer devices.

Further specifications on Source Route, Graph Route and Transport Layer Failure can be found in the *Network Management Specification*. Additional specifications on Path Failure alarms are in *TDMA Data-Link Layer Specification* and *Network Management Specification*.

6.9 Gateway Commands

Implementation of all commands in this section is required for all Gateways.

6.9.1 Device Identification

The only mandatory non-ambiguous way to identify and track (over time) a HART-enabled Field Device is using its Unique ID. Using TAG, I/O connection, or location in a network topology are (while important) problematic for identification purposes. The I/O System Commands (see *Common Practice Command Specification*) are based on the Field Device Unique ID.

However, some reports (e.g., health reports, topology listings etc.) only contain the Field Device Nickname (i.e., its WirelessHART network short address). Consequently, Host Applications be able to identify Field Devices using either the Unique ID or Nickname. Two commands are provided for this purpose:

- Command 832 Read Device Identity using Unique ID; and
- Command 841 Read Device Identity using Nickname.

Command 832 accesses the Nickname and Tag given the Unique ID. Conversely, if the Host Application knows the nickname (e.g., from Command 833 response), Command 841 provides the Unique ID and Tag given the Nickname.

6.9.2 Network Information and Statistics

Access is provided to detailed WirelessHART network topological and performance data. The four commands providing this access include:

- Command 833 Read Device's Neighbor Health provides statistics on communication performance between a Field Device and its neighbors.
- Command 834 Read Network Topology Information enables piecewise construction of a network diagram (topology).
- Command 840 Read Device's Statistics returns comprehensive summary of configuration, performance and KPIs for the Field Device.
- Command 846 Read Network Statistics summarizes overall network health, performance and KPIs.

Using Commands 833 and 834 a “picture” of the connections between Field Devices and communication routes (more specifically, graph routes) through the network can be constructed[21]. For example, Command 833 allows the neighbors a Field Device communicates with to be identified. This can be used to create diagram of the physical network topology. Command 834 then can be used to overlay the communication routes on to the topology.

Commands 840 and 846 provide KPIs and performance statistics. Command 846 summarizes overall network KPIs and network health. Command 840 provides a wide-range of Field Device-level statistics (more then 25 in all) on configuration, communications and performance. In effect, Command 846 provides a system level view of network performance while Command 840 allows detailed inspection of performance in one region of the network.

6.9.3 Network Management

While the Network Manager's prime directive is to ensure reliable, uninterrupted operation of the network, end user application objectives should provide guidance to on network operation and optimization. Four commands allow guidance to be provided to the Network Manager:

- Command 842 Write Device's Scheduling Flags and Command 843 Read Device's Scheduling Flags specify the application-specific role of a Field Device; and
- Command 844 Read Network Constraints and Command 845 Write Network Constraints provide network operation optimization guidance.

Commands 842 and 843 provides additional information to Network Managers about individual Field Devices. For example, an end-user can specify that a Field Device is a leaf node by setting the “Non-routing Device” bit. Another possibility is a device is transient; or if, the device is a rail car that periodically enters and exits a network, the “Transient” bit could be set. If Command 842 is not received for a Field Device the Network Manager must assume all Scheduling Flags are reset (i.e., the Field Device must not receive any special consideration by the Network Manager).

End-user application objectives must be considered as the Network Manager configures and maintains the network. While Commands 742 and 843 provide guidance at the Field Device-level, Commands 844 and 845 provide guidance to the Network Manager at the network-level. For example, using Command 845, an end-user can assign low communication latency priority over battery life.

[21] With a little creativity, the reliability of the interconnections can be imaged (e.g. by adding a third dimension or color proportional to signal levels and communication reliability).

6.9.4 Cache Management

All Gateways must cache command responses to ensure timely access to Field Device process data and status. Four commands allow limited Host Application control gateway caching. These commands are:

- Command 836 Flush Cached Responses for a Device
- Command 852 Read Stale Data Setpoints
- Command 853 Write Stale Data Timer
- Command 854 Write Stale Data Count Setpoint

The first, Command 836, flushes the current cache for the specified Field Device. The use of the command can drastically affect the normal communication performance and, consequently, is not recommended for normal host operation.

The last three are "stale data" commands providing a Host Application control over the Gateway marking process data and status in the cache as Stale or Bad. Command 852 reads the stale data settings and Commands 853 and 854 allow the settings to be configured.

Stale data is assessed in a two-step process using a timer and a counter. Every time data is updated late (or not at all[22]) the Stale Data Counter is incremented[23]. When the Stale Data Counter becomes too large the Process Data Status (See the Command Summary Specification) is marked "Bad" and the Stale Data Alarm is asserted[24] (See Command 840).

[22] Stale data counter must continue to be updated even when a device drops out of the network.

[23] The Stale Data Counter saturates (i.e., does not rollover).

[24] The Stale Data Alarm remains asserted until the data is updated on-time thus resetting the Stale Data Counter and the Stale Data Alarm.

7. COMMANDS

The following HART Commands are supported by WirelessHART Devices.

"Access Restricted" Response Code

Many Commands in this Specification include "Access Restricted" (code 16) as a valid Response Code. In general this code may be returned by devices under two conditions:

- Many Commands are restricted to use only by the Network Manager. For example, many write commands must only be issued by the Network Manager. In some cases, write commands are available to Host Applications (e.g., while provisioning) only when the device is not joined to the network.
- Depending on the device architecture, Access Restricted may be returned due to a failure of the radio transceiver or radio module[25]. If a radio-related failure is detected then "Radio Failure" (see Common Table 32) must be set in the Command 48 response data.

7.1 Command 768 Write Join Key

This command modifies the device's Join Key[26]. This command must be accepted if received: at any time from the Network Manager or via the local Maintenance Port. If received from any other source "Access Restricted" must be returned.

Device must allow the join key to be changed via the maintenance port at any time. This allows an operational device to be moved to another Network (See Command 773 Write Network ID).

Request Data Bytes

Byte	Format	Description
0-15	Unsigned-128	Key value

Response Data Bytes

Byte	Format	Description
0-15	Unsigned-128	Key value

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1 - 4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7 - 15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-64		Undefined
65	Error	Key change failed
66-127		Undefined

[25] If the radio module is restarting (i.e., it has NOT failed and thus unusable) or busy then the device must initiate a Delayed Response (i.e., the device must not return Access Restricted).

[26] When displayed to or entered by the end user, the Join Key shall always be displayed/edited in Hexadecimal Format

7.2 Command 769 Read Join Status

This command allows a host system or handheld device to monitor a field device as it transitions through the WirelessHART joining process. It is intended to assist an instrument technician or service people diagnose a device in the event it has difficulty joining the network.

The values returned in this command are latched once the device has joined.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0.7-0.4	Unsigned-4	Reserved, Must be set to 0
0.3-0.0	Enum-4	(Least Significant 4 Bits of Byte 0) Wireless Mode (See Common Table 51)
1-2	Bits-16	Join Status (See Common Table 52)
3	Unsigned-8	Number of available neighbors. The number of neighbors detected by the device
4	Unsigned-8	Number of Advertising Packets Received[27]
5	Unsigned-8	Number of join attempts. Too many join attempts will result in the device considering the join failed.
6-9	Time	Join retry timer (indicates the amount of time since the last join request was sent)
10-13	Time	Network search timer (indicates the amount of time listening for first advertisement)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7–127		Undefined

[27] Number of Advertising Packets Received increments once for every advertisement received and will roll over to zero and continue incrementing if more then 256 advertisements are received. Furthermore, this value must be latched by device upon the transition to Requesting Admission state (see *Network Management Specification*).

7.3 Command 770 Request Active Advertising

This command allows active, fast advertising to be requested. Often, this command is received locally by a field device[28] from a local maintenance tool (e.g., a handheld). When this happens the field device must begin a Delayed Response and issue its own Command 770 to the Network Manager. The Network Manager should configure or turn on fast advertising in the device and one or more of its neighbors. When the Network Manager responds, the field device must relay that response to the connected host application.

This command must be supported by all Gateways. When this command is received by the Gateway active, fast advertising should be enabled for the entire network.

Request Data Bytes

Byte	Format	Description
0-3	Time	Active Advertising Shed Time[29]. Setting the shed time to zero rescinds the request for active advertising (i.e., advertising should be returned to the normal rate).

Response Data Bytes

Byte	Format	Description
0-3	Time	Active Advertising Shed Time
4-7	Time	Advertising Period
8	Unsigned-8	Number of neighbors advertising in addition to this device.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4	Error	Passed Parameter Too Small
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted (e.g., device has not joined the network)
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-64		Undefined
65		Declined (e.g., operator overridden).
66 - 127		Undefined

[28] Field Devices must return "Access Restricted" when this command request is received via the wireless channel.

[29] If Active Advertising Shed Time is set to 0xFFFFFFFF then active advertising shall continue indefinitely. Similarly, if 0x00000000 is written to Active Advertising Shed Time then normal advertising rate will be resumed immediately.

7.4 Command 771 Force Join Mode

This command allows a host system or handheld device to force a field device into active join mode. The device must stay in the active search mode for at least the Active Search (i.e., Join) Shed Time.

7.4.1 Backward Compatibility Requirements

Previously this command did not allow the Maximum Number of Join Retries (maxJoinRetries) to be written. Consequently, if a field device receives only 5 data bytes in the request it must execute the command without returning Response Code 5 - "Too Few Data Bytes Received" and the value of maxJoinRetries must not be affected.

Request Data Bytes

Byte	Format	Description
0	Enum-8	Join Mode (see Common Table 61)
1-4	Time	Active Search Shed Time
5	Unsigned-8	maxJoinRetries. Maximum number of Join Retries

Response Data Bytes

Byte	Format	Description
0	Enum-8	Join Mode
1-4	Time	Active Search Shed Time
5	Unsigned-8	maxJoinRetries. Maximum Number of Join Retries

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4	Error	Passed Parameter Too Small
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted (e.g., device is joined to the network)
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-64		Undefined
65	Error	Force Join Declined
66-127		Undefined

7.5 Command 772 Read Join Mode Configuration

Reads the Join Mode and Shed Time. The Active Search (i.e., Join) Shed Time is the time a device must be in active search mode. After this time has expired, the device may go into Deep Sleep/Ultra Low Power mode.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	**Format**	**Description**
0	Enum-8	Join Mode (see Common Table 61)
1-4	Time	Active Search Shed Time
5	Unsigned-8	Maximum number of Join Retries (Defaults to 5)

Command-Specific Response Codes

Code	**Class**	**Description**
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7 - 15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 127		Undefined

7.6 Command 773 Write Network ID

This command configures the device to recognize the proper Network ID. For Field Devices, this command can only be issued by the Network Manager or via the maintenance port. All Other sources are responded to with "Access Restricted"

- If the device is not connected to the network, the Network ID is changed immediately. The device must enter power save mode and wait for the Force Join Mode command before beginning to actively search for the network.

- If the device is connected to the Network then the new ID will be used next Join.

When this command is received by a Gateway the Network ID is changed in the Gateway, Network Manager, Access Points and all devices currently in the network. The change remains pending until the network is restarted.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	New Network ID

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	New Network ID
2-3	Unsigned-16	Current Network ID (same as New Network ID if change is NOT pending)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Network ID change pending. New Network ID will be used next join or upon restarting the network.
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-64		Undefined
65	Error	Invalid Network ID (e.g., non production/factory use of 0xE000-0xEFFF)
66-127		Undefined

7.7 Command 774 Read Network ID

This command is used to read the current (or pending) setting of the DLL Network ID of the device.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	New Network ID
2-3	Unsigned-16	Current Network ID (same as New Network ID if change is NOT pending).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7		Undefined
8	Warning	Network ID change pending.
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 127		Undefined

7.8 Command 775 Write Network Tag

Writes the 32-byte Network Tag. The network tag is a proxy for the Network ID so that the network can be identified in a text form in at the application level. The same Network Tag should be written to all devices in the same network.

Request Data Bytes

Byte	Format	Description
0-31	Latin-1	Network Tag

Response Data Bytes

Byte	Format	Description
0-31	Latin-1	Network Tag

Note: The value returned in the response data bytes reflects the value actually used by the Field Device.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data bytes received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.9 Command 776 Read Network Tag

Reads the 32-byte Network Tag. The network tag is a proxy for the Network ID so that the network can be identified in a text form in at the application level.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-31	Latin-1	Network Tag

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 127		Undefined

7.10 Command 777 Read Wireless Device Capabilities

This structure is used by the Network Manager to determine operational characteristics of a Device. The peak packet rate and recovery time must be used by network managers to accommodate rechargeable or scavenging devices. Battery devices shall be able to sustain the peak packet rate specified lifetime of the device.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0.7-0.4	Bits-4	Wireless Capability Flags (see Common Table 75)
0.3-0.0	Enum-4	Power Source (See Common Table 44. Device Power Source)
1-4	Float	Peak packets per second
5-8	Time	Duration at peak packet load before power drained. Must be at least 1 hour. (Set to 24hours if not applicable)
9-12	Time	Time to recover from power drain (Set to zero if not applicable). While recovering, the device must be able to route 1 packet per second.
13	Signed-8	RSL (Receive Signal Level in dBm) threshold ‘good’ connection.
14-17	Time	Required Keep-Alive time. Device must perform a Keep-Alive at least this often.
18-19	Unsigned-16	Maximum number of neighbors
20-21	Unsigned-16	Maximum number of packet buffers

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
7-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.11 Command 778 Read Battery Life

NOT RECOMMENDED FOR NEW DESIGNS[30].

This command allows an application or the Network Manager to determine the current state of the battery on a Device.

Note: Careful design analysis of long-term battery performance is required to properly implement this command.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
1-2	Unsigned-16	Battery Life remaining in days. If the device does not have a battery or other energy storage component then the device may return 0xFFFF.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7–127		Undefined

[30] Battery-Life is a mandatory Device Variable for all battery-powered devices. Consequently, access to battery-Life via Command 9 is preferred over use of Command 778.

7.12 Command 779 Report Device Health

This command is periodically published to the Network Manager (see Command 795 and Common Table 43). The command response is transmitted at "Command" level priority.

All counters are reset just prior to the device joining the network. All counters must only be incremented and rollover to 0 upon overflow[31].

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	(Counter) Number of packets generated by this device
2-3	Unsigned-16	(Counter) Number of packets terminated by this device
4	Unsigned-8	(Counter) Number of Data-Link Layer MIC failures detected
5	Unsigned-8	(Counter) Number of Network Layer (Session) MIC failures Detected
6	Enum-8	Power Status (See Common Table 58)
7	Unsigned-8	(Counter) Number of CRC Errors detected
8	Unsigned-8	(Counter) Number of Unicast Nonce Counter Values not received. This value is incremented for each zero in Nonce Counter History that underflows.
9	Unsigned-8	Maximum packet buffer queue length since last report published.
10-13	Float	Average packet buffer queue length (over time). The length (depth) of the packet buffer calculated as a rolling average with an averaging period equal to the health-reporting interval.
14-17	Time	Average Latency of all packets from the Gateway/Network Manager since last join
18-21	Time	Variance of Latency from the Gateway/Network Manager to this node since last join.
22-25	Unsigned-32	Number of timely packet received. Indicates the number of packets containing setpoints or remote sensor values received within the expected update period. This counter, upon incrementing from 0xFFFF FFFF, rolls-over to 0 and continues incrementing. The counter is reset to 0 upon receiving a Device Reset or when the Network ID is changed.
26-29	Unsigned-32	Number of late or lost packets. Indicates the number of packets containing setpoints or remote sensor values NOT received within the expected update period. This counter must be incremented even if the device drops off the network and rejoins. This counter, upon incrementing from 0xFFFF FFFF, rolls-over to 0 and continues incrementing. The counter is reset to 0 upon receiving a Device Reset or when the Network ID is changed.
30	Unsigned-8	(Counter) Number of packets with Unknown Session received[32]. (May indicate a configuration or security problem.)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17 - 127		Undefined

[31] Some early WirelessHART devices implemented resetting counters not roll-over counters. These devices indicate their use of resetting counters in Command 777.

[32] The session is determined by the source address (network layer), if a packet is received from an unknown source the Unknown Session counter is incremented.

7.13 Command 780 Report Neighbor Health List

This command is used for two different purposes: (1) reading the entire neighbor list and (2) generating periodic reports from the device to the Network Manager. In the former, normal request response communication is used.

In the latter, the command response is periodically published to the network manager (see Command 795 and Common Table 43) providing statistics for linked neighbors only. When the report is generated, the command response is transmitted at "Command" level priority.

The neighbor table is a list with entries being added as neighbors are detected. Neighbors with links to device shall be at the beginning of the list and neighbors without links shall be at the end. Devices must allow all neighbors to be read with this command. Neighbor Flags must indicate "No links to this Neighbor" as needed.

Packet Statistics returned are counters that are only reset just prior to the device joining the network. The counters are incremented and rollover to 0 upon overflow. Statistics for neighbors must be maintained even if the Network Manager temporarily unlinks the neighbor[33].

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Neighbor table index. The neighbor table (like all lists in HART) is zero based (i.e., neighbor_table[0] is the first entry)
1	Unsigned-8	Number of Neighbor entries to read

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Neighbor table index
1	Unsigned-8	Number of Neighbor entries read
2	Unsigned-8	Total number of neighbors (linked or not) currently in the Neighbor Table.
3-4	Unsigned-16	Nickname of neighbor
5	Bit-8	Neighbor Flags (See Common Table 59)
6	Signed-8	Mean RSL (Receive Signal Level in dBm) since last report
7-8	Unsigned-16	(Counter) Packets transmitted to this neighbor
9-10	Unsigned-16	(Counter) Failed transmits - number of packets expecting an ACK and none was received
11-12	Unsigned-16	(Counter) Packets received from this neighbor
13- ...		Response bytes 3 - 12 will be repeated up to number of entries returned in response byte 1.

[33] If the Network Manager deletes the last link to a neighbor then that neighbor is immediately deleted from the neighbor table. When a neighbor is deleted the corresponding statistics are immediately discarded.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.14 Command 781 Read Device Nickname Address

This command allows the Network Manager and an application to read a Device's address.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17 - 127		Undefined

7.15 Command 782 Read Session

This command allows any host (e.g., Network Manager, Gateway, Handheld) to retrieve information about sessions from a Device[34]. Sessions are addressed by their position in the list of sessions on the device, and do not assume a particular implementation. Session indexes may change following addition or deletion of sessions.

"Session Index" may be modified and "Set to Nearest Value" Response Code returned.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

7.15.1 Backward Compatibility Requirements

Previously this command could read multiple sessions at a time. Now the command must return 1 and only 1 session. Byte 1 must be set to 1 in request and response. If Byte 1 set to anything other then 1 in request then the Response Code "Set to nearest value" must be returned by the device.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Session index (first entry shall always be 0)
1	Unsigned-8	Reserved. Must be set to 1

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Session index
1	Unsigned-8	Reserved. Must be set to 1
2	Unsigned-8	Number of sessions currently configured (i.e., the number of entries currently residing in the Session Table.
3	Enum-8	Session type. (See Common Table 48. Session Type Code)
4-5	Unsigned-16	Peer Device Nickname
6-10	Unsigned-40	Peer Device's Unique ID
11-14	Unsigned-32	Peer Device's Nonce Counter Value
15-18	Unsigned-32	The Device's Nonce Counter Value

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

[34] This command should only be sent directly to a field device. To access the Session Table in a Gateway or Network Manager use Command 855 Read Session (Extended) as this command only allows access to the first 256 Sessions in a Gateway or Network Manager.

7.16 Command 783 Read Superframe

This command allows any host to retrieve information about a Superframe assignment from a Device. Superframes are addressed by their position in the list of Superframes on the device, and do not assume a particular implementation. Superframe numbers may change following addition or deletion of Superframes.

"Superframe Index" may be modified and "Set to Nearest Value" Response Code returned.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not connected to the Network.

7.16.1 Backward Compatibility Requirements

Previously this command could read multiple Superframes at a time. Now the command must return 1 and only 1 Superframe. Byte 1 must be set to 1 in request and response. If Byte 1 set to anything other then 1 in request then the Response Code "Set to nearest value" must be returned by the device.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe index (first entry shall always be 0)
1	Unsigned-8	Reserved. Must be set to 1

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe index
1	Unsigned-8	Reserved. Must be set to 1
2	Unsigned-8	Number of superframes (enabled or disabled) currently configured
3	Unsigned-8	Superframe ID
4-5	Unsigned-16	Number of slots in this Superframe
6	Enum-8	Superframe mode flags (See Common Table 47)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.17 Command 784 Read Link

This command may be used by any host (e.g., Network Manager, Gateway, Handheld) to retrieve information about a link entry in a Device. Links are addressed by their position in the list of links on the device, and do not assume a particular implementation. Link indexes may change following addition or deletion of links.

"Link Index" may be modified and "Set to Nearest Value" Response Code returned.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not connected to the Network.

7.17.1 Backward Compatibility Requirements

Previously this command could read multiple links at a time. Now the command must return 1 and only 1 link. Byte 2 must be set to 1 in request and response. If Byte 2 set to anything other then 1 in request then the Response Code "Set to nearest value" must be returned by the device.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Link index (first entry shall always be 0)
2	Unsigned-8	Reserved. Must be set to 1

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Link index
2	Unsigned-8	Reserved. Must be set to 1
3-4	Unsigned-16	Number of links currently configured. Includes links in both enabled and disabled Superframes.
5	Unsigned-8	Superframe ID
6-7	Unsigned-16	Slot number in the superframe for this link
8	Unsigned-8	channelOffset for this link
9-10	Unsigned-16	Nickname of neighbor for this link (or 0xFFFF if broadcast link)
11	Bits-8	linkOptions (See Common Table 46)
12	Enum-8	linkType (See Common Table 45).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.18 Command 785 Read Graph List

This command reads one graph from the Graph Table in the device. The index is for reference only and the referenced graph may change if a graph before it on the list is deleted.

"Graph List Index" may be modified and "Set to Nearest Value" Response Code returned (e.g., if a read past the end of the list is attempted).

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Graph List index (first entry shall always be 0)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Graph List index
1	Unsigned-8	Total number of graphs currently configured.
2-3	Unsigned-16	Graph ID
4	Unsigned-8	Number of neighbors specified for this Graph ID.
5-6	Unsigned-16	Nickname of neighbor
7- ...		Response bytes 5 - 6 will be repeated up to number of entries returned in response byte 4.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., empty list)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.19 Command 786 Read Neighbor Property Flag

This command allows the any host (e.g., Network Manager, Gateway, Handheld) to read the properties of a neighbor of a Device.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname of neighbor

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname of neighbor
2	Bits	Neighbor Flags (see Common Table 59)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., Nickname = 0x0000)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Unknown Nickname
66-127		Undefined

7.20 Command 787 Report Neighbor Signal Levels

This command may be used for two different purposes: (1) reading the entire neighbor list and (2) generating periodic reports from the device to the Network Manager. In the former, normal request response communication is used by any host (e.g., Network Manager, Gateway, Handheld). In the latter, the command response is periodically published as a report to the Network Manager (see Command 795 and Common Table 43) indicating discovered (but not linked) neighbors only. When the report is generated, the command response is transmitted at "Command" level priority.

The neighbor table is a list with entries being added as neighbors are detected. Neighbors with links to device shall be at the beginning of the list and neighbors without links shall be at the end. Devices must allow all neighbors to be read with this command.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not connected to the Network.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Neighbor table index (first entry shall always be 0)
1	Unsigned-8	Number of Neighbor entries to read

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Neighbor table index
1	Unsigned-8	Number of Neighbor entries read
2	Unsigned-8	Total number of neighbors (linked or not) currently in the Neighbor Table.
3-4	Unsigned-16	Nickname of neighbor
5	Signed-8	RSL of neighbor in dB
6-8		Response bytes 3 - 5 will be repeated up to number of entries returned in response byte 1.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.21 Command 788 Alarm: "Path Failed"

The command notifies the Network Manager that the path to a neighbor failed. The command response is transmitted at "Command" level priority. This command must be transmitted every time the pathFailInterval lapses (see the *Network Management Specification*). This command shall only be published (i.e., a Command Request must not be issued and any Command 788 request must be rejected with "Access Restricted").

Request Data Bytes

Not Applicable

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname of neighbor to which path failure was detected

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.22 Command 789 Alarm: "Source Route Failed"

This command notifies the Network Manager that a source route failed. One response PDU shall be produced for each packet received with a bad source route. The command response is transmitted at "Command" level priority every time a source route failure is encountered (see the *Network Management Specification*). This command shall only be published (i.e., a Command Request must not be issued and any Command 789 request must be rejected with "Access Restricted").

Request Data Bytes

Not Applicable

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname of unreachable neighbor in the source route
2-5	Unsigned-32	Network-Layer MIC (i.e., the MIC generated using the session key) from the NPDU that failed routing

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.23 Command 790 Alarm: "Graph Route Failed"

This command notifies the Network Manager that a graph route failed. One response PDU shall be produced for each packet received with a bad graph route. The command response is transmitted at "Command" level priority every time a graph route failure is encountered (see the *Network Management Specification*). This command shall only be published (i.e., a Command Request must not be issued and any Command 790 request must be rejected with "Access Restricted").

Request Data Bytes

Not Applicable

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Graph ID of the failed route

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.24 Command 791 Alarm: "Transport Layer Failed"

This command notifies the Network Manager that a Transport Layer connection failed[35]. The command response is transmitted at "Command" level priority every time a session failure is encountered (see the *Network Management Specification*). This command shall only be published (i.e., a Command Request must not be issued and any Command 791 request must be rejected with "Access Restricted").

Request Data Bytes

Not Applicable

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname of unreachable peer in the end-to-ends Transport Layer

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

[35] If the device experiences a Transport Layer failure with the Network Manager (e.g., when requesting bandwidth using Command 799) the Transport Layer Alarm must be transmitted. After forwarding the Alarm PDU to its neighbor (i.e., the DLPDU was ACKed), the device must rejoin the network.

7.25 Command 793 Write RTC Time Mapping

This command allows the network manager to set the mapping of start of ASN 0 to human readable time (i.e., the real-time clock) on a device. This mapping can be to, for example, local time or UTC as needed to meet the plant/user practices.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0-2	Date	HART Date
3-6	Time	Time of Day

Response Data Bytes

Byte	Format	Description
0-2	Date	HART Date
3-6	Time	Time of Day

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4		Undefined
5	Error	Too Few Data Bytes Received
6-9		Undefined
9	Error	Invalid Date Code Detected
10-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.26 Command 794 Read RTC Time Mapping

This command allows a device (including the Network Manager) to read the mapping of ASN 0 to human readable time.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-2	Date	HART Date
3-6	Time	Time of Day

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
7-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.27 Command 795 Write Timer Interval

This command allows the interval for a timer on a Device to be set.

Response must return what is actually used by the device (e.g., reflecting any rounding or truncation performed by the device).

Request Data Bytes

Byte	Format	Description
0	Enum-8	Timer type. (See Common Table 43. Wireless Timer Code).
1-4	Unsigned-32	Timer interval (in milliseconds)

Response Data Bytes

Byte	Format	Description
0	Enum-8	Timer type. (See Common Table 43. Wireless Timer Code)
1-4	Unsigned-32	Timer interval (in milliseconds)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4	Error	Passed Parameter Too Small
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted (i.e., this command must be accepted only from the Network Manager)
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-64		Undefined
65	Error	Invalid timer type
66-127		Undefined

7.28 Command 796 Read Timer Interval

This command allows any host (e.g., Network Manager, Gateway, Handheld) to read the interval for a timer on a Device.

Response must return what is actually used by the device (e.g., reflecting any rounding or truncation performed by the device)

Request Data Bytes

Byte	Format	Description
0	Enum-8	Timer type. (See Common Table 43. Wireless Timer Code).

Response Data Bytes

Byte	Format	Description
0	Enum-8	Timer type. (See Common Table 43. Wireless Timer Code)
1-4	Unsigned-32	Timer interval (in milliseconds)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 64		Undefined
65	Error	Invalid timer type
66-127		Undefined

7.29 Command 797 Write Radio Transmit Power

It is used to configure the radio transmit power for a device or Access Point. If the device cannot accept the exact value sent from the application, it may respond with "Set to Nearest Possible Value".

> Note: Devices must support -10dBm, 0dBm and +10dBm.

Normally, this command must only be accepted when received from the Network Manager. However the device must accept this command when received via Maintenance Port while the device is not connected to the network.

Request Data Bytes

Byte	Format	Description
0	Signed-8	Transmit Power in dBm

Response Data Bytes

Byte	Format	Description
0	Signed-8	Transmit Power in dBm

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4	Error	Passed Parameter Too Small
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.30 Command 798 Read Radio Transmit Power

It is used to read the radio transmit power for a device or Access Point.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Signed-8	Transmit Power in dBm

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 127		Undefined

7.31 Command 799 Request Timetable

This command is used by wireless device to request connection to another device with specified bandwidth and latency characteristics. Response to this command indicates that the Network Manager accepted the request and will attempt to process it. Response to the request shall include device-unique Timetable ID.

On a heavily utilized network the Network Manager may decline requests for communication bandwidth or provide significantly less bandwidth than requested. When this occurs the device[36] must set the "Capacity Denied" status and the "More status available" bit in the Device Status byte. When the bandwidth provided is less than (but greater than zero) desired the device must continue requesting the bandwidth it needs once per health reporting interval.

The device must continue publishing process data using the available bandwidth even if the bandwidth provided is less than (but greater than zero) the bandwidth requested.

If the device receives a "Write Timetable" (see Command 973) on the same Timetable ID while awaiting a response to this command the device must reject the Write Timetable.

Host Applications may send this command to the Gateway[37] to request additional bandwidth for communication with the specified device.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID supplied by and specific to requesting device (must be in the range 0x00-0x7F)
1	Bits	Timetable Request Flags (See Common Table 39. Timetable Request Flags)
2	Enum	Timetable's Application Domain (See Common Table 40. Timetable Application Domain)
3-4	Unsigned-16	Nickname of the peer with which the Timetable is requested
5-8	Time	Period (Latency if Intermittent flag set)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID
1	Bits	Timetable Request Flags
2	Enum	Timetable's Application Domain
3-4	Unsigned-16	Nickname of the peer with which the Timetable is requested
5-8	Time	Period (Latency if Intermittent flag set)
9	Unsigned-8	Route ID for this Timetable ID

[36] Gateway must set the "Capacity Denied" bit in its Command 48 response when any device in the network has insufficient bandwidth.

[37] Use of this command is at the Host Application's discretion. Gateways must support this command.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-3		Undefined
4	Error	Passed Parameter Too Small (period/latency)
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7		Undefined
8	Warning	Set to Nearest Possible Value
9-13		Undefined
14	Warning	Communication bandwidth supplied significantly less than requested (i.e., reduced more than setting to nearest value).
15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-64		Undefined
65	Error	Timetable Request denied
66	Error	Unknown Timetable flag
67	Error	Unknown application domain
68	Error	Unknown Nickname
69	Error	Invalid Timetable ID.
70-127		Undefined

7.32 Command 800 Read Timetable

This command is used read details of a Timetable. If the service index is larger than the maximum of timetables currently in the device then the device should return the last entry and set the Response Code to "Set to nearest value".

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

7.32.1 Backward Compatibility Requirements

Previously this command could read multiple Timetables at a time. Now the command must return 1 and only 1 Timetable. Byte 1 must be set to 1 in request and response. If Byte 1 set to anything other then 1 in request then the Response Code "Set to nearest value" must be returned by the device.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable index (first entry shall always be 0)
1	Unsigned-8	Reserved. Must be set to 1

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable index
1	Unsigned-8	Reserved. Must be set to 1
2	Unsigned-8	Number of Timetables currently configured.
3	Unsigned-8	Timetable ID
4	Bits-8	Timetable Request Flags (See Common Table 39. Timetable Request Flags)
5	Enum-8	Timetable's Application Domain (See Common Table 40. Timetable Application Domain)
6-7	Unsigned-16	Nickname of the peer with which the Timetable is requested
8-11	Time	Period (Latency if Intermittent flag set)
12	Unsigned-8	Route ID

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7		Undefined
8	Warning	Set to nearest value
9-15		Undefined
16	Error	Access Restricted
17 - 127		Undefined

7.33 Command 801 Delete Timetable

This command notifies device of Timetable deletion. Only creator of the Timetable can delete the Timetable. If the owner of the Timetable does not generate this command the respondent must reject the command and return the "Delete not allowed" Response Code.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID
1	Unsigned-8	Reason. (See Common Table 49. Timetable Deletion Reason Codes)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID
1	Unsigned-8	Reason. (See Common Table 49. Timetable Deletion Reason Codes)
2	Unsigned	Number of Timetable entries remaining unconfigured.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data bytes received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Entry not found
66	Error	Invalid Reason Code
67	Error	Reason Code rejected, Timetable not deleted.
68	Error	Delete not allowed - requestor not Timetable owner
69-127		Undefined

7.34 Command 802 Read Route

This command allows the any host (e.g., Network Manager, Gateway, Handheld) to retrieve route. If the Route index is larger than the maximum of Routes currently in the device then the device must return the last entry and set the Response Code to "Set to nearest value".

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

7.34.1 Backward Compatibility Requirements

Previously this command could read multiple routes at a time. Now the command must return 1 and only 1 route. Byte 1 must be set to 1 in request and response. If Byte 1 set to anything other then 1 in request then the Response Code "Set to nearest value" must be returned by the device.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Route index (first entry shall always be 0)
1	Unsigned-8	Reserved. Must be set to 1

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Route index
1	Unsigned-8	Reserved. Must be set to 1
2	Unsigned-8	Number of routes currently configured
3	Unsigned-8	Number of Routes remaining unconfigured.
4	Unsigned-8	Route ID
5-6	Unsigned-16	Destination Nickname
7-8	Unsigned-16	Graph ID
9	Unsigned-8	Source-Route Attached (1=Attached, 0=None). Use Command 803 to read the Source-Route as needed.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to nearest value
9-15		Undefined
16	Error	Access Restricted
17 - 127		Undefined

7.35 Command 803 Read Source-Route

This command allows any host (e.g., Network Manager, Gateway, Handheld) to read the contents of a particular Source-Route. Broadcast addresses are not legal address values in Source-Routes and shall not be included in any responses for this command.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID
1	Unsigned-8	Number of hops
2-3	Unsigned-16	Nickname hop entry 0
4- ...		Repeated for number of entries indicated in response byte 1

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (bad Route ID)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17 - 64		Undefined
65	Error	Entry not found (no Source-Route associated with Route ID)
66-127		Undefined

7.36 Command 804 Read CCA Mode

This command allows an application to determine if Clear Channel Assessment (CCA) is enabled on a device.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Enum-8	CCA Mode. (See Common Table 76. CCA Mode Codes)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 127		Undefined

7.37 Command 805 Write CCA Mode

This command allows an application to determine if Clear Channel Assessment (CCA) is enabled on a device.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

CCA must be disabled while the device is not joined.

Request Data Bytes

Byte	Format	Description
0	Enum-8	CCA Mode. (See Common Table 76. CCA Mode Codes)

Response Data Bytes

Byte	Format	Description
0	Enum-8	CCA Mode

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., Invalid CCA mode)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7		Undefined
8	Warning	Set to nearest value
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.38 Command 806 Read Handheld Superframe

This command allows an application to determine if a particular device has the Handheld Superframe enabled. The Handheld Superframe is used between a device and a Handheld device specifically for maintenance purposes.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1-2	Unsigned-16	Number of slots in the Superframe
3	Bits-8	Superframe Mode Flags (See Common Table 47).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-8		Undefined
9	Error	No Handheld Superframe
10-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.39 Command 807 Request Handheld Superframe Mode

This command allows a Handheld device to request that a Device enable/disable the Handheld Superframe. The Handheld Superframe is used between a device and a Handheld device specifically for maintenance purposes.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1	Bits-8	Superframe Mode Flags (See Common Table 47).

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1	Bits-8	Superframe Mode Flags[38]

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., Invalid Superframe mode or ID)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-127		Undefined

[38] The "Handheld Superframe" bit must be set upon successful execution of this command. i.e., the Superframe can only enabled/disabled.

7.40 Command 808 Read Packet Time-to-Live

This command allows an application to determine what the current configuration is for a device Time-to-Live. The Time-to-Live is a parameter that determines how many hops deep a packet will go before it is discarded.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Currently configured Time-to-Live.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.41 Command 809 Write Packet Time-to-Live

This command allows the Network Manager to write the packet Time-to-Live. The Time-to-Live is a parameter that determines how many hops deep a packet will go before it is discarded. The TTL shall not be set to less than 8. Any attempt must result in TTL being set to 8 and the "Set to nearest value" Response Code returned.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager while connected to the network. This command is available, via the Maintenance Port, while not connected to the network.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Time-to-Live value.

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Time-to-Live value set.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7		Undefined
8	Warning	Set to nearest value
8-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.42 Command 810 Read Join Priority

This command reads the Join Priority currently being advertised by the device.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Join Priority.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.43 Command 811 Write Join Priority

This command allows the Network Manager write Join Priority. The Join Priority is included in advertisements and helps determine the neighbor used to convey the initial Join Request to the Network Manager. The Join-Priority shall not be set to more than 15. Any attempt must result in Join-Priority being set to 15 and the "Set to nearest value" Response Code returned.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Join priority.

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Join priority.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to nearest value
8-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.44 Command 812 Read Packet Receive Priority

This command allows an application to determine what the current configuration is for a device receive priority. The receive priority determines what packets a device will respond to and/or forward to other nodes.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Packet Receive Priority (0 - 3 see Common Table 64. Packet Receive Priority Code and the *TDMA Data-Link Layer Specification*).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.45 Command 813 Write Packet Receive Priority

This command allows the Network Manager to write receive priority. The receive priority determines what packets a device will respond to and/or forward to other nodes. The Packet Receive Priority shall not be set to more than 3. Any attempt must result in Packet Receive Priority being set to 3 and the "Set to nearest value" Response Code returned.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Enum-8	Receive Priority (0 – 3 see Common Table 64. Packet Receive Priority Code and the *TDMA Data-Link Layer Specification*)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Receive Priority (0 – 3).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to nearest value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.46 Command 814 Read Device List Entries

This command allows an application to retrieve the lists of devices that are indicated in the List ID. The list indices may change due to addition or deletion of entries. This command must be supported by Gateways. Common Table 55 enumerates the mandatory and optional device lists.

When the "Starting List index" is out of range it must set a valid value and " Number of list entries read" must be set to at least 1. Consequently, The "Set to Nearest Possible Value" Response Code must be returned as well.

Request Data Bytes

Byte	Format	Description
0	Enum	Device List Code (see Command Table 55)
1	Unsigned-8	Number of list entries to read
2-3	Unsigned-16	Starting List index (first entry shall always be 0)

Response Data Bytes

Byte	Format	Description
0	Enum	Device List Code
1	Unsigned-8	Number of list entries read
2-3	Unsigned-16	Starting List index
4-5	Unsigned-16	Total number of entries in the list
6-10	Unsigned-40	Device Unique ID
11…	Unsigned-40	Device Unique ID Repeated up to the number of list entries requested or the number of entries the Device has available

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (i.e. Device List Code not supported)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.47 Command 815 Add Device List Table Entry

This command allows the addition of a device to the indicated list. The Active Device List cannot be modified by this command. Any attempt to add an active device (i.e., on the Active Device List) to the blacklist will generate the response code "Device List Conflict".

Common Table 55 enumerates the mandatory and optional device lists.

Request Data Bytes

Byte	Format	Description
0	Enum	Device List Code (see Command Table 55)
1-5	Unsigned-40	Device Unique ID

Response Data Bytes

Byte	Format	Description
0	Enum	Device List Code (see Command Table 55)
1-5	Unsigned-40	Device Unique ID
6-7	Unsigned-16	Number of List Entries remaining unconfigured/unused

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., Device List Code not supported)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Device already in list
9-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	No more entries available
66	Error	Device List Conflict
67-127		Undefined

7.48 Command 816 Delete Device List Table Entry

This command allows deletion of devices from lists that are maintained in the Gateway/Network Manager. If a device is deleted from the Active Device List the Network Manager must reroute the traffic and disconnect the device.

This command must be supported by Gateways. Common Table 55 enumerates the mandatory and optional device lists.

Request Data Bytes

Byte	Format	Description
0	Enum	Device List Code (see Command Table 55)
1-5	Unsigned-40	Device Unique ID. If a Device Unique ID = 0 is specified (i.e., broadcast address) the complete list content is flushed.

Response Data Bytes

Byte	Format	Description
0	Enum	Device List Code (see Command Table 55)
1-5	Unsigned-40	Device Unique ID
6-7	Unsigned-16	Number of List Entries remaining unconfigured/unused

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., Device List Code not supported)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-15		Undefined
16	Error	Access Restricted
17-65		Undefined
66	Error	Device List Conflict
67-127		Undefined

7.49 Command 817 Read Channel Blacklist

This commands reads the current channel blacklist and the blacklist that will be used after the next restart.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Number of bits in current channel map array. This depends on the Physical Layer. (e.g., for 2.4GHz O-QPSK DSSS the array is 16bits long i.e., 2-bytes)
1-*n*	Bits	Current channel map array. This is an array of bits starting with the least significant bit (bit 0 in byte 0) and adding bytes as necessary until all bits are accounted for. Each bit corresponds to a channel. If the bit is set the channel will be used.
n+1–2n	Bits	Pending channel map array.. Each bit corresponds to a channel. If the bit is set the channel will be used after the next restart of the network[39].

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

[39] Field Devices may not be aware of pending blacklist changes and return the same values for "Pending channel map array" as "Current channel map array".

7.50 Command 818 Write Channel Blacklist

This command writes a new channel blacklist to the Network Manager. This blacklist will come into effect only after the Network is restarted.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Number of bits in new channel map array
1 – n	Bits	Pending channel map array. This is an array of bits starting with the least significant bit (bit 0 in byte 0) and adding bytes as necessary until all bits are accounted for. Each bit corresponds to a channel. If the bit is set the channel will be used after the next restart of the virtual gateway/network manager

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Number of bits in new channel map array
1 – n	Bits	Pending channel map array.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1 – 2		Undefined
3	Error	Passed parameter too large (i.e. number of bits exceeds maximum value)
4	Error	Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Illegal frequency channel bits (e.g. channel 16 for 2.4GHz 802.15.4 PHY)
66-127		Undefined

7.51 Command 819 Read Back-Off Exponent

Reads max back off exponent (not to exceed 7).

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Maximum Back-Off Exponent

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.52 Command 820 Write Back-Off Exponent

Writes max back off exponent (not to exceed 7).

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Maximum Back-Off Exponent (must be between 4 and 7)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Maximum Back-Off Exponent

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4	Error	Passed Parameter Too Small
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.53 Command 821 Write Network Access Mode

This command writes the network access mode. This can be used to restrict the access to the network. Only the Network Access Codes 0 and 4 are mandatory.

The access mode does not substitute the check for the device's credentials such as join key, tag or device id. The access mode provides additional checks.

Request Data Bytes

Byte	Format	Description
0	Enum	Network Access Mode Code (see Common Table 56)

Response Data Bytes

Byte	Format	Description
0	Enum	Network Access Mode Code

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.54 Command 822 Read Network Access Mode

This command reads the network access mode.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Enum	Network Access Mode Code(see Common Table 56)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 127		Undefined

7.55 Command 823 Request Session

This command requests a session from a handheld to a device. The session is unicast. Only authorized devices shall be granted a session.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Peer Device Nickname

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Peer Device Nickname
2-5	Unsigned-32	Peer Device's Nonce Counter Value
6-22	Unsigned-128	Key value

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too few data bytes received
6-15		Undefined
16	Error	Access restricted
17-64		Undefined
65	Error	Unknown Nickname
66	Error	Peer device has insufficient capacity to support another session.
67-127		Undefined

7.56 Command 832 Read Device Identity using Unique ID

This command returns the identity information for the indicated device

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of the device

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of the device
5-6	Unsigned-16	Nickname
7-38	Latin-1	Long Tag

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-127		Undefined

7.57 Command 833 Read Device's Neighbor Health

It returns information regarding the quality of the connection to each linked or unlinked neighbors a device has. Command 840 allow hosts to determine how many neighbors a device has in its Neighbor Table. This command can then be issued as many times as needed to determine the specific information about each neighbor connection.

If an application makes requests for this information from each device attached to a Wireless Gateway, then a picture/graph of the quality of the network can be built.

7.57.1 Backward Compatibility Requirements

Previously this command could read multiple neighbors at a time. Now the command must return 1 and only 1 neighbor. Byte 6 must be set to 1 in request and response. If Byte 6 set to anything other then 1 in request then the Response Code "Set to nearest value" must be returned by the Gateway.

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of Device
5	Unsigned-8	Neighbor index number (first entry shall always be 0)
6	Unsigned-8	Reserved. Must be set to 1.

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of Device
5	Unsigned-8	Neighbor index number
6	Unsigned-8	Reserved. Must be set to 1
7-8	Unsigned-16	Neighbor Nickname (2 byte address)
9	Signed-8	RSL of communication received at this device from Neighbor
10-13	Unsigned-32	Packets transmitted to the neighbor
14-17	Unsigned-32	Failed transmits to the neighbor (number of packets expecting an ACK and none was received).
18-21	Unsigned-32	Packets received from neighbor
22	Bits-8	Neighbor Flags (See Common Tables 59)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to nearest value
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
65	Error	Invalid Neighbor table index
66-127		Undefined

7.58 Command 834 Read Network Topology Information

Returns the number of Graph configured in the device and the configuration of the specified Graph. This command can then be issued as many times as needed to determine the specific graph id's that the device is participating in.

If an application makes requests for this information from each device attached to a Wireless Gateway, then a picture/graph of all the network topology can be built.

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of the device information is being requested
5-6	Unsigned-16	Graph index number (first entry shall always be 0)

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of the device information is being requested
5-6	Unsigned-16	Graph index number
7-8	Unsigned-16	Total number of Graphs configured in this device
9-10	Unsigned-16	Graph ID for this index
11-12	Unsigned-16	Number of Neighbors returned
13-14	Unsigned-16	Neighbor 1
15…		Response bytes 13 - 14 will be repeated up to number of entries returned in response byte 11-12.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-64		Undefined
65	Error	Entry not Found
66-127		Undefined

7.59 Command 835 Read Burst Message List

THIS COMMAND IS NOT RECOMMENDED FOR NEW DESIGNS.

It returns the Burst Mode List that the requested device participates in. By reading Command 835 the application layer can determine how many burst mode commands a particular device is participating in.

If an application makes requests for this information from each device attached to a Wireless Gateway, then a list of all Burst Mode Traffic in the system can be determined.

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Device Unique ID

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Device Unique ID
5	Unsigned-8	Number of different burst commands received from this device
6-7	Unsigned-16	Command Number being Burst
8-11	Unsigned-32	Number of Burst packets received
etc		Repeat bytes 6-11 for each burst mode command

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-127		Undefined

7.60 Command 836 Flush Cached Responses for a Device

Instructs the Gateway to flush the cached responses from a Field Device.

WARNING: This command should not be used unless it is absolutely necessary. Use of this command will degrade the network performance and increase battery usage while the Gateway rebuilds it cache.

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID for device to flush all cached responses for. Cached response shall only be flushed for a single designated device per command.

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID for device to flush all cached responses for.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.61 Command 837 Reserved

Revision 1 of this document included this command. This command must not be implemented in any device.

7.62 Command 838 Reserved

Revision 1 of this document included this command. This command must not be implemented in any device.

7.63 Command 839 Reserved

Revision 1 of this document included this command. This command must not be implemented in any device.

7.64 Command 840 Read Device's Statistics

This command returns the number of graphs, frames, and links that a device has currently active. This is information the Gateway has available and can respond with immediately.

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of the device

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID of the device
5-6	Unsigned-16	Number of Graphs configured
7-8	Unsigned-16	Number of Superframes configured
9-10	Unsigned-16	Number of Links configured
11	Unsigned-8	Number of Neighbors (linked and not linked)
12-15	Time	Average communication Latency (node➔ Gateway/Network Manager)
16-17	Unsigned-16	Number of Joins
18-20	Date	Date of most recent Join
21-24	Time	Time-of-day of most recent Join
25-28	Unsigned-32	Number of packets generated by this device
29-32	Unsigned-32	Number of packets terminated by this device
33-36	Unsigned-32	Number of Data-Link Layer MIC failures detected
37-40	Unsigned-32	Number of Network Layer (Session) MIC failures detected
41-44	Unsigned-32	Number of CRC Errors detected
45-48	Unsigned-32	Number of Unicast Nonce Counter Values not received **by** the device. This value is incremented for each zero in Nonce Counter History that underflows.
49-52	Unsigned-32	Number of Unicast Nonce Counter Values not received **from** the device.
53-56	Time	Standard Deviation of Latency (node➔Gateway/Network Manager).
57-60	Time	Average communication Latency (Gateway/Network Manager➔node)
61-64	Time	Standard Deviation of Latency (Gateway/Network Manager ➔node).
65-98	Float	Percent Availability (node➔ Gateway/Network Manager)
69-73	Float	Percent Availability (Gateway/Network Manager ➔node)
73	Unsigned-16	Maximum packet buffer queue length
75-78	Float	Average packet buffer queue length (over time)
79.0 -79.2	Enum-3	Wireless Device Connection Status (see Common Table 77)
79.4-79.7	Bits-5	Wireless Device Health Status (See Common Table 78)
80	Unsigned-8	(Counter) Number of packets with bad or unknown Session received by device. (May indicate a configuration or security problem.)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-127		Undefined

7.65 Command 841 Read Device Identity using Nickname

This command returns the identity information for the indicated device

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname
2-6	Unsigned-40	Unique ID of the device
7-38	Latin-1	Long Tag

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-127		Undefined

7.66 Command 842 Write Device's Scheduling Flags

This command allows users to request special consideration for a device when the Network Manager is creating schedules.

This command shall only be supported by Gateways and Network Managers. This information must not be written to the device. This command must not be supported by other devices (e.g., Field Devices, Adapters)

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Device Unique ID
5	Bits	Device Scheduling Flags (see Common Table 62)

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Device Unique ID
5	Bits	Device Scheduling Flags

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too few data byte received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Unsupported Property Flag detected, Device Property Flags adjusted
9	Error	Invalid Property Flag
8-15		Undefined
16	Error	Access Restricted
17–64		Undefined
65	Error	Unknown Unique ID
66-127		Undefined

7.67 Command 843 Read Device's Scheduling Flags

This command reads the device properties that a network manager may consider when creating schedules.

This command shall only be supported by Gateways and Network Managers. This information must not be supported in other devices (e.g., Field Devices).

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Device Unique ID

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Device Unique ID
5	Bits	Device Scheduling Flags (see Common Table 62)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-127		Undefined

7.68 Command 844 Read Network Constraints

This command reads the current setting of the Network Management Strategy and the number of Request/Response messages per 10 seconds.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Enum-8	Network Optimization Flags (see Common Table 63. Network Optimization Flags)
1	Unsigned-8	Number of Request/Response Message Pairs per 10s

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-127		Undefined

7.69 Command 845 Write Network Constraints

This is Gateway Command.

This command writes the current setting of the Network Management Strategy and the number of Request/Response messages per 10 seconds. Minimum value for Number of Request/Response Messages per 10 seconds is 1.

Request Data Bytes

Byte	Format	Description
0	Enum-8	Network Optimization Flags (see Common Table 63. Network Optimization Flags)
1	Unsigned-8	Number of Request/Response Messages per 10s

Response Data Bytes

Byte	Format	Description
0	Enum-8	Network Optimization Flags
1	Unsigned-8	Number of Request/Response Messages per 10s

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection (illegal or unsupported strategy)
3-4		Undefined
5	Error	Too few data bytes received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Set to nearest value
9-15		Undefined
16	Error	Access restricted
17-127		Undefined

7.70 Command 846 Read Network Statistics

This command summarizes overall network health.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-3	Float	Throughput. Average number of packets per second communicated to/from Network Manager and Gateway.
4-7	Float	Percent Network Utilization.
8-11	Float	Percent Availability.
12-15	Time	Average Latency.
16-19	Tme	Standard Deviation of Latency.
20-23	Float	Packet Error Rate.
24-27	Unsigned-32	Dropped packets. Number of dropped packets (as indicated by unicast nonce underflow) by all devices (Network Manager, Gateway, and devices on Active list).
28-31	Unsigned-32	Unsuccessful Joins. The number of join requests received that do not result in the requesting device reaching the Quarantine state. This includes reject join requests (e.g., device not on the whitelist, join key failure, etc.)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
16	Error	Access restricted
17-127		Undefined

7.71 Command 847 Transfer Network List to White List

This command copies the Network List into the White List. Before the transfer the White List is flushed; after the execution of this command, the White List content will be the same as the Network List

The Network List is not affected.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Number of devices copied to the Whitelist

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-15		Undefined
16	Error	Access restricted
17-127		Undefined

7.72 Command 848 Generate Key

This command is to be used by an application to get a random key from the Security Manager embedded in the Gateway. Since the application cannot talk directly to the Security Manager, the Gateway is used as a proxy to get a key from the Security Manager. This key may be used, for example, to write a new join key to a device.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved. Must be set to zero (0)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved. Must be set to zero (0)
1-16	Unsigned-128	Random Key Value

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data bytes received
6	Error	Device-Specific Command Error
7-15		Undefined
16	Error	Access restricted
17-127		Undefined

7.73 Command 849 Read Device's Join Key

Reads a new random join key for the specified device. This command can be used to provision a device prior to it being added to a network. If the device is not already on the White list it is added to it. The Network list is unaffected (the device is neither added to or deleted from the Network list).

This command will return an error if the device is on the Active or Quarantine list. The command will return an error if the network is closed (i.e., no devices can be added to the network).

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved to allow the size of the key to be specified in the future. Must be set to zero (0)
1-5	Unsigned-40	Unique ID of Device

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved.
1-5	Unsigned-40	Unique ID of Device
6-21	Unsigned-128	Random Key Value. Default is 128-bit key or 16 bytes.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data bytes received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8		Undefined
9	Error	Device Active or Quarantined.
10	Error	Network closed. New devices cannot be added.
11	Error	Number of network device cannot be increased.
12-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.74 Command 850 Write Device's Join Key

Writes the specified Join Key to the identified device. A Security Manager may use this command to change the Join Key associated with a device. The Join Key for this device will be updated in the Gateway/Network Manager. The device will be added to the White list (if necessary). If the identified device is Active or Quarantined the key in the device will be changed.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved to allow the size of the key to be specified in the future. Must be set to zero (0)
1-5	Unsigned-40	Unique ID of Device
6-21	Unsigned-128	Random Key Value. Join Key for the selected device.

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved.
1-5	Unsigned-40	Unique ID of Device
6-21	Unsigned-128	Join Key for the selected device

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data bytes received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-9		Undefined
10	Error	Network closed. New devices cannot be added.
11	Error	Number of network device cannot be increased.
12-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.75 Command 851 Change Key Now

Instructs the Security Manager embedded in the Gateway to change the keys (Network, Join or Sessions) in the specified device. The broadcast address must be specified to change the Network Key.

This command must be immediately responded to and contains the estimated time required to complete the key changes. The record of the device join key must only be updated after confirming the join key in the device has been successfully updated.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved. Must be set to zero (0)
1-2	Bits-16	Change Key Flags (see Common Table 79)
3-7	Unsigned-40	Unique ID of Device. When set to broadcast address (i.e., 0x0000.0x000000) the keys in all devices will be changed.

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Reserved. Must be set to zero (0)
1-2	Bits-16	Change Key Flags
3-7	Unsigned-40	Unique ID of Device
8-11	Time	Estimated time to complete key change

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data bytes received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8		Undefined
9	Error	Unique ID must be broadcast address to change Network Key (Key Change request failed)
10-15		Undefined
16	Error	Access restricted
17-64		Undefined
65	Error	Unknown Unique ID
66-127		Undefined

7.76 Command 852 Read Stale Data Setpoints

This command is to be used by an application to read the Stale Data Timer and Counter Setpoint. When the Stale Data Timer expires:

- The Stale Data Count must be incremented;
- The Process Data Status for the corresponding process variables (Discrete Variable, Device Variable, etc) must be set to "BAD" (see *Command Summary Specification*); and
- "Update Failure" Response Code must be returned when Host Applications read the process data.

When the Stale Data Count exceeds the setpoint the Stale Data Alarm is set (See Command 840 and Common Table 78 Wireless Device Health Status). The Stale Data Count (and Stale Data Alarm) is reset when a burst message is received before the Stale Data Timer expires.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-3	Float	Stale Data Timer (Defaults to 100%). The percent of the Burst Message Maximum Update Time that, when exceeded, cause the Stale Data Count to increment by 1.
4	Unsigned-8	Stale Data Count Setpoint (defaults to 3). The count that, when exceeded, causes the Stale Data Alarm to be signaled (see Command 840).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access restricted
17-127		Undefined

7.77 Command 853 Write Stale Data Timer

Writes the percent of the maximum burst period that a burst message can be late before the stale data count is incremented.

Request Data Bytes

Byte	Format	Description
0-3	Float	Stale Data Timer (Defaults to 100%). The percent of the Burst Message Maximum Update Time that, when exceeded, cause the Stale Data Count to increment by 1.

Response Data Bytes

Byte	Format	Description
0-3	Float	Stale Data Timer.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4	Error	Passed Parameter Too Small
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37 - 127		Undefined

7.78 Command 854 Write Stale Data Count Setpoint

Writes the stale data count.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Stale Data Count Setpoint (defaults to 3). The count that, when exceeded, causes the Stale Data Alarm to be signaled.

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Stale Data Count

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-2		Undefined
3	Error	Passed Parameter Too Large
4	Error	Passed Parameter Too Small
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7	Error	In Write Protect Mode
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37 - 127		Undefined

7.79 Command 855 Read Session (Extended)

This command allows a host application to retrieve information about sessions from a Gateway or Network Manager[40]. Sessions are addressed by their position in the list of sessions on the device, and do not assume a particular implementation. Session indexes may change following addition or deletion of sessions.

"Session Index" may be modified and "Set to Nearest Value" Response Code returned.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Session index (first entry shall always be 0)

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Session index
2	Unsigned-8	Number of sessions currently configured (i.e., the number of entries currently residing in the Session Table.
3	Enum-8	Session type. (See Common Table 48. Session Type Code)
4-5	Unsigned-16	Peer Device Nickname
6-10	Unsigned-40	Peer Device's Unique ID
11-14	Unsigned-32	Peer Device's Nonce Counter Value
15-18	Unsigned-32	The Device's Nonce Counter Value

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value
9-15		Undefined
16	Error	Access Restricted
17-127		Undefined

[40] This command should only be sent to a Gateway or Network Manager. To access the Session Table in a Field Device Command 782 Read Session should be used.

7.80 Command 856 Read Device Suspend Setting

Reads the current suspension settings from a device.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Time at which to suspend device (ASN)
5-9	Unsigned-40	Time at which to resume device (ASN)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7–31		Undefined
32	Error	Busy
63-127		Undefined

7.81 Command 857 Read Security Level Advertised

Security Level Supported is included in all advertisements and indicates the security protocols supported by the Network Manager. All Network Managers must support at least the "Join Keyed" security type (See Common Table 53). This command allows the Security Level included in Advertisements generated by the device to be read.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Enum-8	Security Level Supported. Defaults to "Join Keyed". (See Common Table 53. Security Type Codes).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.82 Command 858 Reset Availability Statistics

Instructs the Gateway to reset the availability statistics.

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID for device to reset availability statistics for (broadcast address resets availability for entire network).

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Unique ID for device.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.83 Command 859 Read Active Advertising Status

This command returns the current advertising settings. When this command is received from a local maintenance tool (e.g., a handheld) the values for the Field Device are returned. This command must be supported by all Gateways. When this command is received by the Gateway the median advertising rate for the entire network is returned.

Request Data Bytes

Byte	Format	Description

Response Data Bytes

Byte	Format	Description
0-3	Time	Active Advertising Shed Time. Returns the time remaining before active advertising ceases (or 0x00000000 if active advertising has stopped)
4-7	Time	Current Advertising Period (median value if response is from Gateway).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted (e.g., device has not joined the network)
17- 127		Undefined

7.84 Command 860 Read Join Key Mode

This command reads the join key mode currently employed by the Network Manager.

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0	Enum	Join Key Mode Code(see Common Table 80)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-5		Undefined
6	Error	Device Specific Command Error
7–31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33 - 127		Undefined

7.85 Command 861 Write Join Key Mode

This command writes the Join Key Mode.

This command supports an optional mode where the Join Key is common to all devices. This allows a customer to get the devices quickly provisioned to the network and then once the devices are on they can transition the network to a random network wide join key.

Warning: Use of this command dramatically reduces network security and will make the plant network vulnerable to attack and disruption.

Request Data Bytes

Byte	Format	Description
0	Enum	Join Key Mode Code (see Common Table 80)

Response Data Bytes

Byte	Format	Description
0	Enum	Join Key Mode Code

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

7.86 Command 862 Read Timetable by ID

This command reads the Timetable specified by the Timetable ID.

This command must be rejected with a response code of 16 (Access Restricted) if the device is not joined to the Network.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID
1	Bits-8	Timetable Request Flags (See Common Table 39. Timetable Request Flags)
2	Enum-8	Timetable's Application Domain (See Common Table 40. Timetable Application Domain)
3-4	Unsigned-16	Nickname of the peer with which the Timetable is requested
5-8	Time	Period (Latency if Intermittent flag set)
9	Unsigned-8	Route ID

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device Specific Command Error
7-15		Undefined
16	Error	Access Restricted
17 - 127		Undefined

7.87 Command 960 Disconnect Device

This command allows the network manager to force a device off the network, clear all its network information and rejoin the network.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Reason. (See Common Table 50. Disconnect Cause Codes)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Reason. (See Common Table 50. Disconnect Cause Codes)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.88 Command 961 Write Network (Data-Link) Key

This command allows the Network Manager to write the Network (Data-Link) Key on a Device. If this is the first Network (Data-Link) Key written to a device joining the network, then this command must be truncated[41] after the Key Value[42]. In this case, the Network (Data-Link) Key will become effective immediately.

If this command is received while a key change is pending the key and the execution time of the pending key change shall be overwritten. If the execution time is less than the current ASN the "Invalid execution time" Response Code shall be returned.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0-15	Unsigned-128	Key value
16-20	Unsigned-40	Execution time for command (ASN).

Response Data Bytes

Byte	Format	Description
0-15	Unsigned-128	Key value
16-20	Unsigned-40	Execution time for command (ASN)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Key change failed
66	Error	Invalid execution time
67-127		Undefined

[41] The Host Application request must be 16 bytes or at least 21 bytes long. Otherwise the Field Device must return "Too Few Bytes Received".

[42] When the request is truncated the response must also be truncated.

7.89 Command 962 Write Device Nickname Address

This command allows the Network Manager to set a Device's Nickname.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Invalid Nickname
66-127		Undefined

7.90 Command 963 Write/Modify Session

This command allows the Network Manager to write the session parameters required to establish a session between the device the message is addressed to and the peer device contained in the request.

If this is a new session or for immediate Session Key changes, then the execution time can be truncated[43] off the end of the command[44]. When truncated the session and the Session Key will become effective immediately. If this command is received while a modification to the session is pending the key and the execution time of the pending session change shall be overwritten. If the execution time is less than the current ASN the "Invalid execution time" Response Code shall be returned.

Sessions are identified by session type and peer device. If this command is modifying an existing session then the peer nonce counter is ignored. The response always includes the values actually used by the device. When a new key is written to the session the old key must be retained to allow for out-of-order packet reception. The old key must be discarded after 2 * "Maximum PDU Age"

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Enum-8	Session type. (See Common Table 48. Session Type Code)
1-2	Unsigned-16	Nickname of peer device
3-7	Unsigned-40	Peer Unique ID
8-11	Unsigned-32	Peer Nonce counter value
12-27	Unsigned-128	Key value
28	Unsigned-8	Reserved should be set to 0
29-33	Unsigned-40	Execution time for command (ASN).

Response Data Bytes

Byte	Format	Description
0	Enum-8	Session type. (See Common Table 48. Session Type Code)
1-2	Unsigned-16	Nickname of peer device
3-7	Unsigned-40	Peer Unique ID
8-11	Unsigned-32	Peer Nonce counter value
12-27	Unsigned-128	Key value
28	Unsigned-8	Number of sessions remaining
29-33	Unsigned-40	Execution time for command (ASN).

[43] The Host Application request must be 29 bytes or at least 34 bytes long. Otherwise the Field Device must return "Too Few Bytes Received"

[44] When the request is truncated the response must also be truncated.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., Nickname = 0x0000)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	No more entries available
66	Error	Invalid execution time
67	Error	Session type invalid
68-127		Undefined

7.91 Command 964 Delete Session

This command is used by the Network Manager to delete an end-to-end session key on a Device. Execution of this command must have no affect on Routes, Timetables or other tables in the device.

This command cannot be used to delete the join session.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Enum-8	Session type. (See Common Table 48. Session Type Code)
1-2	Unsigned-16	Nickname of peer device

Response Data Bytes

Byte	Format	Description
0	Enum-8	Session type. (See Common Table 48. Session Type Code)
1-2	Unsigned-16	Nickname of peer device
3	Unsigned-8	Number of sessions remaining

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., bad session type)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Session with given peer device does not exist
66-127		Undefined

7.92 Command 965 Write/Modify Superframe

This command allows the Network Manager to write or modify a Superframe in a Device. If a Superframe with the specified Superframe ID is found, the operation shall be considered a modification. Otherwise, a new Superframe shall be added. Execution time of the command specifies when the actual modification takes place - this allows synchronous network-wide operation.

The execution time can be truncated[45] off the end of the command[46]. When truncated, the Superframe will be modified immediately[47].

The properties of the Superframe (e.g., number of slots, Handheld flag) may only be modified while the Superframe is inactive. If the Superframe is shortened then any link associated with the slots eliminated shall be deleted.

If this command is received while a change to the Superframe is pending then the pending modifications shall be overwritten. If the execution time is less than the current ASN the "Invalid execution time" Response Code shall be returned.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

A device must only support one Handheld Superframe. If the received command attempts to create a second Handheld Superframe the "Invalid Superframe mode" Response Code must be returned.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1-2	Unsigned-16	Number of slots in the Superframe
3	Bits-8	Superframe Mode Flags (See Common Table 47).
4	Unsigned-8	Reserved should be set to 0
5-9	Unsigned-40	Execution time of command (ASN).

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1-2	Unsigned-16	Number of slots in the Superframe
3	Bits-8	Superframe Mode Flags
4	Unsigned-8	Number of Superframes remaining
5-9	Unsigned-40	Execution time of command (ASN).

[45] The Host Application request must be 5 bytes or at least 10 bytes long. Otherwise the Field Device must return "Too Few Bytes Received"

[46] When the request is truncated the response must also be truncated.

[47] For example, the Superframe may be created, activated, or deactivated immediately. Also the other Superframe properties may be modified immediately while the Superframe is inactive.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted (e.g., attempt to modify an active Superframe)
17-64		Undefined
65	Error	No more entries available
66	Error	Invalid execution time
67	Error	Invalid number of slots
68	Error	Invalid Superframe mode
69-127		Undefined

7.93 Command 966 Delete Superframe

This command allows the Network Manager to delete a Superframe in a Device. When executed by the device all links associated with the Superframe must also be deleted.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1	Unsigned-8	Number of remaining Superframe entries

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Entry not found
66-127		Undefined

7.94 Command 967 Add Link

This command is used by the network manager to add a link assignment to a device. The link is uniquely identified by the combination of following key parameters:

<Superframe ID, slot number, neighbor address >

Modification of existing links is not supported. A network manager must delete an existing link and then write a new link to accomplish a modify operation.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1-2	Unsigned-16	Slot number in the Superframe for this link
3	Unsigned-8	channelOffset for this link
4-5	Unsigned-16	Nickname of neighbor for this link (or 0xFFFF if broadcast, discovery, join link)
6	Bits-8	linkOptions (See Common Table 46. Link Option Flag Codes)
7	Enum-8	linkType (See Common Table 45. Link Type).

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1-2	Unsigned-16	Slot number in the Superframe for this link
3	Unsigned-8	channelOffset for this link
4-5	Unsigned-16	Nickname of neighbor for this link
6	Bits-8	linkOptions
7	Enum-8	linkType
8-9	Unsigned-16	Number of link entries remaining

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., nickname = 0x0000)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	No more links available
66	Error	Link already exists
67	Error	Unknown Superframe ID
68	Error	Invalid slot number
69	Error	Invalid link options (e.g., neither transmit nor receive set)
70	Error	Invalid channel offset
71	Error	Invalid link type
72	Error	No more neighbors available
73-127		Undefined

7.95 Command 968 Delete Link

This command allows the network manager to delete a link assignment in a Device. The link is uniquely identified by the combination of following key parameters:

<Superframe ID, slot, neighbor address>

Execution of this command must not delete any Graph-Edge or Superframe. Deleting a the last link to a neighbor deletes the neighbor from the Neighbor Table

This command must be rejected with a Response Code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1-2	Unsigned-16	Slot number in the Superframe for this link
3-4	Unsigned-16	Nickname of neighbor for this link

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Superframe ID
1-2	Unsigned-16	Slot number in the Superframe for this link
3-4	Unsigned-16	Nickname of neighbor for this link
5-6	Unsigned-16	Number of link entries remaining unconfigured

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Link not found
66-127		Undefined

7.96 Command 969 Add Graph Edge

This command is used by the Network Manager to add a neighbor to a graph thus defining another graph-edge. A Graph (and its edges) with an ID less than 256 is specified by a Superframe and its transmit links. In that case edges are added to the Graph by writing a transmit link to new neighbor for that Superframe-Graph.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Graph ID (must greater than 255)
2-3	Unsigned-16	Nickname of neighbor

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Graph ID
2-3	Unsigned-16	Nickname of neighbor
4	Unsigned-8	Number of edges remaining unconfigured

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., nickname = 0x0000, 0xFFFF; Graph ID = 0xFFFF)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	No more entries available (one or both of graph or edge table)
66	Error	Unknown Nickname
67	Error	Can't add edge when Superframe is used as graph equivalent.
68-127		Undefined

7.97 Command 970 Delete Graph Edge

This command is used by the Network Manager to delete a neighbor from the graph defined in the device. In effect, this command deletes a graph-edge. If the Graph ID < 256 then the Response Code "Invalid Selection" must be returned.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Graph ID (must be greater than 255)
2-3	Unsigned-16	Nickname of neighbor

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Graph ID
2-3	Unsigned-16	Nickname of neighbor
4	Unsigned-8	Number of connections remaining

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid Selection (e.g., nickname = 0x0000, Graph ID <256)
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Entry not found
66-127		Undefined

7.98 Command 971 Write Neighbor Property Flag

This command allows the Network Manager to set properties of a neighbor on a Device.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname of neighbor
2	Bits	Neighbor Flags (see Common Table 59)

Response Data Bytes

Byte	Format	Description
0-1	Unsigned-16	Nickname of neighbor
2	Bits	Neighbor Flags. (The flag "No links to this Neighbor" must be reset in the response data).

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted (e.g., Neighbor not linked)
17-64		Undefined
65	Error	Unknown Nickname
66	Error	Invalid neighbor property
67-127		Undefined

7.99 Command 972 Suspend Device(s)

This command allows the Network Manager to suspend the operation of one or more devices. Whether the command may be sent to all devices on the network or an individual device based on the addressing used. If this command is received while a suspend command is pending then the pending suspend setting shall be overwritten.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Time at which to suspend device (ASN)
5-9	Unsigned-40	Time at which to resume device (ASN)[48]

Response Data Bytes

Byte	Format	Description
0-4	Unsigned-40	Time at which to suspend device (ASN)
5-9	Unsigned-40	Time at which to resume device (ASN)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Invalid suspend time
66	Error	Invalid resume time
69-127		Undefined

[48] ASN Time to Resume accuracy is subject to drift as Field Device's clock not synchronized to network while suspended.

7.100 Command 973 Write/Modify Timetable

This command is used by the Network Manager to create a new Timetable or modify an existing Timetable quota. The Network Manager may issue this command to restrict or reduce previously allocated bandwidth (e.g., during a network disturbance). When this command is used to reduce previously allocated bandwidth the recipient device must set the "Capacity Denied" status and the "More status available" bit in the Device Status byte if the bandwidth restriction can result in a process upset/disturbance.

If this command is received while the device is awaiting a response to a Request Timetable (see Command 799) on the same Timetable ID the device must respond to this command with an "Open Transaction Pending" error.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID. If the Network Manager is creating a new Timetable then the Timetable ID must be in the range 0x80-0xFF.
1	Bits-8	Timetable Request Flags (See Common Table 39)
2	Enum-8	Timetable's Application Domain (See Common Table 40)
3-4	Unsigned-16	Nickname of the peer with which the Timetable is requested
5-8	Time	Period (Latency if Intermittent flag set)
9	Unsigned-8	Route ID

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Timetable ID for this request
1	Bits-8	Timetable Request Flags
2	Enum-8	Timetable's Application Domain
3-4	Unsigned-16	Nickname of the peer with which the Timetable is requested
5-8	Time	Period (Latency if Intermittent flag set)
9	Unsigned-8	Route ID
10	Unsigned-8	Number of Timetables remaining.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Set to Nearest Possible Value (period/latency)
9-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	No more entries available
66	Error	Invalid Timetable ID.
67	Error	Open Transaction Pending
68	Error	Invalid Application Domain
69	Error	Unknown Correspondent Nickname (no session exists)
70	Error	Unknown Route ID
71	Error	Correspondent Nickname and Route Correspondent mismatch
72-127		Undefined

7.101 Command 974 Write/Modify Route

This command allows the Network Manager to create or modify a Route[49].

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID
1-2	Unsigned-16	Destination Nickname
3-4	Unsigned-16	Graph ID. Setting Graph ID to 0xFFFF indicates this is a Source Route only.

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID
1-2	Unsigned-16	Correspondent Nickname
3-4	Unsigned-16	Graph ID
6	Unsigned-8	Number of Routes remaining.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	No more entries available
66	Error	Unknown Nickname (no Session for that correspondent device)
67	Error	Unknown Graph ID (Graph ID does not exist)
68-127		Undefined

[49] A session for the destination of the route must exist prior to creating a route to it.

7.102 Command 975 Delete Route

This command allows the network manager to delete a route that was previously written. It is deleted using the Route ID that was used to write the route information. If the Route has an attached Source-Route then the Source-Route is also deleted.[50]

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID
1	Unsigned-8	Number of unconfigured Routes remaining.
2	Unsigned-8	Number of unconfigured Source-Routes remaining.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	Invalid route id
66-127		Undefined

[50] A route may specify a Graph Route, a Source-Route (see Command 976) or both. Since a Source-Route is associated with and has only Route (See "Network Layer Data Model" in the Network Management Specification) it must be deleted when its (parent) Route is deleted.

7.103 Command 976 Write/Modify Source-Route

This command is used by the Network Manager to write a source route. Broadcast addresses are not legal address values in this command and shall not be included in Source-Routes or the requests or responses for this command.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID
1	Unsigned-8	Number of hops
2-3	Unsigned-16	Nickname hop entry 0
4- ...	Unsigned-16	Repeated for number of entries indicated in request byte 1

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID
1	Unsigned-8	Number of hops
2-3	Unsigned-16	Nickname hop entry 0
4- ...	Unsigned-16	Repeated for number of entries indicated in response byte 1
n	Unsigned-8	Number of unconfigured Source-Route entries left

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-7		Undefined
8	Warning	Broadcast addresses deleted in response.
9-15		Undefined
16	Error	Access Restricted
17-64		Undefined
65	Error	No more entries available
66	Error	Invalid Route ID
67	Error	Invalid Nickname (Nickname = 0x0000, 0xFFFF)
68	Error	Invalid number of hops
67-127		Undefined

7.104 Command 977 Delete Source-Route

This command is used by the Network Manager to delete a source route. The Route itself is unaffected (i.e., Command 975 must be used to delete Routes)

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Route ID
1	Unsigned-8	Number of unconfigured Source-Routes remaining.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-65		Undefined
66	Error	Invalid Route ID
67-127		Undefined

7.105 Command 978 Write Status Counter Mode

This command is used to configure the device to use saturating status counters or roll-over counters. When configured for saturating counter the status counters will count up from zero and reset after each health report. If the status counter reaches its maximum possible value (e.g., 255 for one byte counters) then the value will saturate at its maximum. When set for rollover operation the counters never reset. Upon incrementing the status while at the counter's maximum value, the counter will rollover to zero.

Network Managers and Gateways must function correctly with status counters configured in either operating mode.

This command must be accepted if received: at any time from the Network Manager; or via the local Maintenance Port while not connected to the network. If received from any other source or the Maintenance Port while connected to the Network the device must return "Access Restricted".

Request Data Bytes

Byte	Format	Description
0	Enum	Counter Mode (1=Saturating; 0=Roll-Over Counter)

Response Data Bytes

Byte	Format	Description
0	Unsigned-8	Counter Mode (1=Saturating; 0=Roll-Over Counter)

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6	Error	Device-Specific Command Error
7	Error	In Write Protect Mode
8-15		Undefined
16	Error	Access Restricted
17-127		Undefined

7.106 Command 979 Write Security Level Supported

Security Level Supported is included in all advertisements and indicates the security protocols supported by the Network Manager. All Network Managers must support at least the "Join Keyed" security type (See Common Table 53). This command allows the Network Manager to change the Security Level included in Advertisements generated by the device.

This command must be rejected with a response code of 16 (Access Restricted) if the source address is any device other than the Network Manager.

Request Data Bytes

Byte	Format	Description
0	Enum-8	Security Level Supported (See Common Tables 53 Security Type Codes)

Response Data Bytes

Byte	Format	Description
0	Enum-8	Security Level Supported

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1		Undefined
2	Error	Invalid selection
3-4		Undefined
5	Error	Too Few Data Bytes Received
6-15		Undefined
16	Error	Access Restricted
17-127		Undefined

8. MODULE-SPECIFIC WIRELESS-ONLY COMMANDS

Wireless Module-Specific Command (numbers 64,512-64,765) may be generated as long as they meet the following requirements

- They must meet all the requirements for HART Commands (see the *Command Summary Specification*).
- No commands shall be created that limit or degrade the operation of compliant WirelessHART products.
- No Commands shall be created that reduce the ability to replace a Device from one manufacturer with that from another manufacturer without degrading system performance. The devices must have equivalent capabilities (e.g., you should be able to replace a pressure transmitter with a pressure transmitter from another manufacturer).
- Use of commands in this range must be disclosed, reviewed and approved by HCF prior to product release.
- The first 2 bytes of each request/response for all module-specific, wireless-only commands must be the of the wireless module's Expanded Device Type Code.

If the first two bytes in the command request do not match the wireless module's Expanded Device Type Code then the command must be rejected and the "Expanded Device Type Code Error" (RC #37) Response Code must be returned.

8.1 Command 64,512 Read Wireless Module Revision

All WirelessHART devices must support this command.

In some cases, the wireless transceiver module is manufactured by a company other than the device manufacturer. This command supports the identification of the transceiver manufacturer.

This returns: the Expanded Device Type, Manufacturer, and revision levels.

Command Summary Specification requirements must be met.

If a transceiver module is replaced resulting in changes in the commands supported by the device, the device's Expanded Device Type and revisions must be changed accordingly (see revision rules in *Command Summary Specification*. This will also require a new DD to be registered for the device.

The device including module must comply with the HART Protocol revision returned in Command 0

Request Data Bytes

Byte	Format	Description
None		

Response Data Bytes

Byte	Format	Description
0-1	Enum	Expanded Device Type of the wireless module (see Common Table 1, Device Type Codes and the *Command Summary Specification*, Section 6).
2-3	Enum	Manufacturer Identification Code (see Common Table 8, Manufacturer Identification Codes)
4	Unsigned-8	Device Revision Level (refer to the *Command Summary Specification*)
5	Unsigned-8	Software Revision Level of this device. Levels 254 and 255 are reserved.
6	Unsigned-8	Hardware Revision Level of the electronics in this particular device. Does Not Necessarily Trace Individual Component Changes.

Command-Specific Response Codes

Code	Class	Description
0	Success	No Command-Specific Errors
1-15		Undefined
16	Error	Access Restricted
17-31		Undefined
32	Error	Busy (A DR Could Not Be Started)
33	Error	DR Initiated
34	Error	DR Running
35	Error	DR Dead
36	Error	DR Conflict
37-127		Undefined

ANNEX A. CONFIGURATION CHANGED AND WIRELESSHART COMMAND USE TABLE

The following table summarizes the WirelessHART Commands that must be supported by different types of devices and whether a given command affects the Configuration Changed bit and counter.

Device Type abbreviations are as follows:

WD Wireless Field Device; Wireless Discrete Adapter or Wireless Process Adapter as Slave

WDM Wireless Field Device; Wireless Discrete Adapter or Wireless Process Adapter as Master in wireless network

GW Gateway as Slave

NMM Network Manager as Master or recipient (e.g. for health reports)

NMS Network Manager as Slave (e.g. request bandwidth, session, etc.)

AP Access Point

The abbreviations in the columns are:

Y Yes. The Configuration Changed bit and counter are affected

N No. The Configuration Changed bit and counter are un-affected

M Mandatory. Device must implement the command

M(N) Mandatory - Network Manager Only

R Recommended. Device should implement the command

Table 1. WirelessHART Command Usage Summary

Command	CC	Device Type					
		NMM	NMS	WD	WDM	AP	GW
Command 768 Write Join Key	N			M			
Command 769 Read Join Status	N			M			
Command 770 Request Active Advertising	N		M	M	M		M
Command 771 Force Join Mode	Y			M			
Command 772 Read Join Mode Configuration	N	M		M			
Command 773 Write Network ID	Y			M		M	M
Command 774 Read Network ID	N	M		M		M	M
Command 775 Write Network Tag	Y			R			M
Command 776 Read Network Tag	N			R			M
Command 777 Read Wireless Device Capabilities	N	R		M		M	
Command 778 Read Battery Life	N						
Command 779 Report Device Health	N	M		M		M	
Command 780 Report Neighbor Health List	N	M		M		M	
Command 781 Read Device Nickname Address	N			M		M	
Command 782 Read Session	N			M			
Command 783 Read Superframe	N			M		M	
Command 784 Read Link	N			M		M	
Command 785 Read Graph List	N			M		M	
Command 786 Read Neighbor Property Flag	N			M			
Command 787 Report Neighbor Signal Levels	N	M		M		M	
Command 788 Alarm: "Path Failed"	N	M		M		M	
Command 789 Alarm: "Source Route Failed"	N	M		M		M	
Command 790 Alarm: "Graph Route Failed"	N	M		M		M	
Command 791 Alarm: "Transport Layer Failed"	N	M		M			
Command 793 Write RTC Time Mapping[51]	N			M			R

[51] Optional for Gateway, the Gateway may utilize other sources.

		Device Type					
Command	**CC**	**NMM**	**NMS**	**WD**	**WDM**	**AP**	**GW**
Command 794 Read RTC Time Mapping	N	R		M			M
Command 795 Write Timer Interval	N	M		M(N)		M	
Command 796 Read Timer Interval	N	M		M		M	
Command 797 Write Radio Transmit Power[52]	Y	M		M(N)		M	
Command 798 Read Radio Transmit Power	N	M		M		M	
Command 799 Request Timetable	N		M		M		M
Command 800 Read Timetable	N			M			
Command 801 Delete Timetable	N	M	M	M	M		
Command 802 Read Route	N			M			
Command 803 Read Source-Route	N			R			
Command 804 Read CCA Mode	N			M		M	
Command 805 Write CCA Mode	N	M		M(N)		M	
Command 806 Read Handheld Superframe	N	M		M			
Command 807 Request Handheld Superframe Mode	N			M			
Command 808 Read Packet Time-to-Live	N	R		M		M	
Command 809 Write Packet Time-to-Live[53]	N	M		M(N)		M	
Command 810 Read Join Priority	N			M		M	
Command 811 Write Join Priority	N	M		M(N)		M	
Command 812 Read Packet Receive Priority	N			M		R	
Command 813 Write Packet Receive Priority	N	M		M(N)		R	
Command 814 Read Device List Entries	N			R			M
Command 815 Add Device List Table Entry	Y			R			M
Command 816 Delete Device List Table Entry	Y			R			M
Command 817 Read Channel Blacklist	N			M		M	M
Command 818 Write Channel Blacklist[54]	Y					M	M
Command 819 Read Back-Off Exponent	N			M		M	
Command 820 Write Back-Off Exponent	N	M		M(N)		M	
Command 821 Write Network Access Mode	Y						M
Command 822 Read Network Access Mode	N						M
Command 823 Request Session	N		M				
Command 832 Read Device Identity using Unique ID	N						M
Command 833 Read Device's Neighbor Health	N						M
Command 834 Read Network Topology Information	N						M
Command 835 Read Burst Message List	N						
Command 836 Flush Cached Responses for a Device	N						M
Command 840 Read Device's Statistics	N						M
Command 841 Read Device Identity using Nickname	N						M
Command 842 Write Device's Scheduling Flags	Y						M
Command 843 Read Device's Scheduling Flags	N						M
Command 844 Read Network Constraints	N						M
Command 845 Write Network Constraints	Y						M
Command 846 Read Network Statistics	N						M
Command 847 Transfer Network List to White List	Y						R

[52] In addition, Device must accept this command via the maintenance port when not connected to network.
[53] In addition, Device must accept this command via the maintenance port when not connected to network.
[54] Gateway Only

Command	CC	Device Type					
		NMM	NMS	WD	WDM	AP	GW
Command 848 Generate Key	N						R
Command 849 Read Device's Join Key	N						R
Command 850 Write Device's Join Key	Y						R
Command 851 Change Key Now	Y						M
Command 852 Read Stale Data Setpoints	N						M
Command 853 Write Stale Data Timer	Y						M
Command 854 Write Stale Data Count Setpoint	Y						M
Command 855 Read Session (Extended)	N						M
Command 856 Read Device Suspend Setting	N			M			
Command 857 Read Security Level Advertised	N			M		M	M
Command 858 Reset Availability Statistics	N						M
Command 859 Read Active Advertising Status	N			M			M
Command 860 Read Join Key Mode	N						M
Command 861 Write Join Key Mode	Y						M
Command 862 Read Timetable by ID	N						M
Command 960 Disconnect Device	N	M		M(N)			
Command 961 Write Network (Data-Link) Key	N	M		M(N)			
Command 962 Write Device Nickname Address	N	M		M(N)			
Command 963 Write/Modify Session	N	M		M(N)			
Command 964 Delete Session	N	M		M(N)			
Command 965 Write/Modify Superframe	N	M		M(N)			
Command 966 Delete Superframe	N	M		M(N)			
Command 967 Add Link	N	M		M(N)			
Command 968 Delete Link	N	M		M(N)			
Command 969 Add Graph Edge	N	M		M(N)			
Command 970 Delete Graph Edge	N	M		M(N)			
Command 971 Write Neighbor Property Flag	N	M		M(N)			
Command 972 Suspend Device(s)	N	M		M(N)			
Command 973 Write/Modify Timetable	N	M		M(N)			
Command 974 Write/Modify Route	N	M		M(N)			
Command 975 Delete Route	N	M		M(N)			
Command 976 Write/Modify Source-Route	N			R(N)			
Command 977 Delete Source-Route	N			R(N)			
Command 978 Write Status Counter Mode	Y			R(N)			
Command 979 Write Security Level Supported	N			M			
Command 64,512 Read Wireless Module Revision[55]				M		M	M[56]

[55] Command 64,512 must be supported when (and only when) device specific wireless commands are implemented in the device. See Section 8 for more information.

[56] Gateway only supports Command 64,512 when an Access Point is integrated into the Gateway/Portal.

ANNEX B. REVISION HISTORY

B1. Revision 2.0 (12 June 2012)

Most list-based read commands converted to read a single entry per WG request to allow for future forward compatibility.

All clarifications and corrections integrated from HART 7.1 (addenda).

Over 120 additional issues recorded in HCFTracker have been addressed and integrated into this revision.

Health reports clarified and enhanced to meet NAMUR Key Performance Indicator (KPI) requirements.

Commands 837-839 were applicable to all I/O systems not just WirelessHART Gateways. Consequently, these commands were deprecated and similar commands will be added in the future to the *Common Practice Command Specification* (HCF_SPEC-151).

Commands 846-862 and 977-979 added. These commands were added to enhance KPI-related reporting, allow for future protocol expansion, provide simple security and key management facilities and simplify (e.g., whitelist) device list management.

Clarifications were added as a precursor to finalizing Gateway test requirements.

Section 6 was rewritten and enhanced to specify the application of WirelessHART Commands and to clarify command requirements.

B2. Revision 1.0 (5 September, 2007)

Initial Revision