ALERT2™ MANT Protocol Specification

January 2025
Version 1.2

ALERT2™ Protocol Technical Working Group - Technical Working Group of the Standards and Guidance Committee of the National Hydrologic Warning Council

Revision history

Date	Version	Description	Author
13 Apr 2009	1.0	"Adding a Layer…" revised	R Chris Roark
Feb 2010	1.0	Draft Spec Version 1 from above	James Logan, Ilse Gayl
1 Sep 2010	1.0	Final Draft Spec Ver. 1	Ilse Gayl
7 Apr 2011	1.1	Version 1.1 Draft	R Chris Roark
22 Apr 2011	1.1	Version 1.1 Draft for TWG Comment	R Chris Roark, Don Van Wie
Sep 2024	1.2	Version 1.2 Draft for TWG Comment	David Van Wie

Release history

Date	Version	Status	Audience	Approval
1 Sep 2010	1.0	Released to web site	Public	TWG, Ilse Gayl
1 Mar 2012	1.1	Final	Public	TWG, Don Van Wie
6 Jan 2025	1.2	Final	Public	TWG, David Van Wie

Document management register

Document	File reference

Review Status

Reviewer	Date Reviewed	Version Reviewed

Release Signatories

Approval	Name	Signature	Date

Contact details

National Hydrologic Warning Council
2480 W. 26th Ave., Suite 156-B
Denver, CO 80211

ALERT2™ Protocol Technical Working Group
Technical Working Group of the Standards and Guidance Committee of the
National Hydrologic Warning Council

Current and Historical Membership Information
is Available at the NHWC Website

Contents

List of Figures

Acknowledgement

The ALERT2™ MANT Layer Protocol Specification is derived from the document “Adding a Layer for the ALERT2™ Protocol” by Chris Roark, March 3, 2009, revised April 13, 2009.

1 Overview

This document contains the specification for Version 1.1 of the MANT layer of the ALERT2™ protocol suite. ALERT2™ is the next generation successor to the ALERT (Automated Local Evaluation in Real Time) protocol, widely in use for the transmission of hydrologic and meteorologic data used to support flood preparedness and public safety decision making. The ALERT2™ protocol suite is optimized for the connectionless transmission of short messages by radio, and offers improved channel efficiency, greater flexibility, error detection and forward error correction, and many other features not available in ALERT.

The need to meet three primary criteria of the existing ALERT community drove the development of the ALERT2™ protocol, and in particular, the AirLink Layer. These three criteria are:

1. The protocol must reside in the public domain, and not require proprietary methods or services.
2. The protocol must provide a common air interface, i.e. the "on-the air" modulation and framing is compatible with multiple brands of commercial, off-the-shelf radio transceivers readily available to manufacturers, system integrators and users.
3. The protocol must address the limitations of ALERT – primarily low channel capacity and high data loss – while providing bit and packet error rate performance equal to or better than legacy 300 bps ALERT.

This document is intended primarily for those interested implementing the ALERT2™ protocols in software and hardware.

1.1 Protocol Architecture

The ALERT2™ protocol suite has a three-layer architecture.

The Application Layer supports the encoding and decoding of data into and out of formats and structures used by ALERT2™ applications. At the Application Protocol Device (APD), data is formed into structures understood by the receiving application software. Similarly, the MANT Protocol and AirLink Protocol devices add information to the Application data that are understood by other MANT and AirLink Protocol devices respectively. Each layer provides independent functionality and operates asynchronously to the others. Physically, all three layers may be integrated into a single device, or separated into three physical devices. When the MANT Protocol and AirLink Protocol are implemented by a single device it is referred to as an Intelligent Network Device (IND); its interface is by the Intelligent Network Device Application Program Interface (IND API) specification.

The Network and Transport (MANT) layer provides the addressing, port multiplexing, acknowledgement, and other services to logically transport application and network control data across the ALERT2™ radio network. When the MANT layer receives an Application Protocol Data Unit (PDU) from the Application Protocol Device, it provides the requested services, adds a header to the Application PDU to form a MANT PDU and forwards the MANT PDU to the AirLink layer. When the MANT layer receives a MANT PDU from the AirLink layer, it inspects the attached MANT Header and provides the appropriate services to the PDU, and sends the Application PDUs to the application port on the Application Protocol Device. The MANT layer exchanges information with other MANT layer devices on the network using MANT PDUs to provide network services, configuration and control.

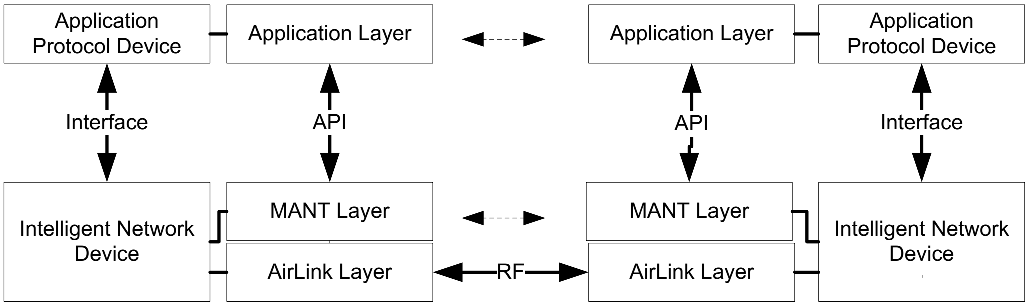
Application Protocol Device
Application Layer
Application Layer
Application Protocol Device
Interface
API
API
Interface
Intelligent Network Device
MANT Layer
MANT Layer
Intelligent Network Device
AirLink Layer
RF
AirLink Layer

Figure 1-1 ALERT2™ Physical and Logical Architecture

The AirLink Protocol modem transmits the PDUs received from the MANT layer since its last transmission. An AirLink frame is created and transmitted at a time determined by the type of media access selected and that method's configuration parameters. The AirLink Frame is created by aggregating all buffered PDUs, adding an AirLink Header, and blocking, scrambling and forward error correcting this aggregate to form an AirLink Frame Payload. The final AirLink Frame is created by pre-pending a preamble and adding a tail. The AirLink Protocol modem controls an FM transceiver's Push to Talk (PTT) as required and transforms the digital data frame into an analog signal sent to the audio input of an FM radio. An AirLink Protocol modem receives and creates MANT PDUs to send to the MANT layer device by reversing the transmission process. When an AirLink Frame is detected on the RF media, the audio waveform is converted to a bit stream, forward error correction decoded and framed into the MANT PDUs.

Figure1.1 illustrates the flow of data through the protocol layers, and associates them with one possible physical architecture.

1.2 The MANT Layer

Version 1.1 of the MANT specification defines services for both an Application Layer Protocol Device as an originating and terminating modem[1] and services for network operations such as a repeater. Unless specifically defined otherwise, the protocol services defined below apply to all uses of the MANT layer protocol device.

The MANT layer protocol device interface is via the IND API. This specification provides the methods for:

1. An Application layer Protocol Device sending and receiving Application Layer PDUs;
2. An external AirLink layer device (e.g. Demodulator & Decoder) providing MANT PDUs for repeater operations; and
3. A user terminal or APD sending IND configuration information.

The MANT protocol adds a header to Application Protocol Data Units (Application PDUs) to create MANT Protocol Data Units. The header is minimally 6 bytes, but may be extended in length to provide certain protocol services. It also contains a flag to allow the inclusion of a second embedded header.

The MANT Version 1.1 layer provides the following protocol services:

1. Addressing: adding the IND or APD specified Source Address and extending the MANT header to include the IND or APD specified Destination Address;
2. Application Port Multiplexing: identifying to which Application Layer protocol the App PDU is to be delivered;
3. Path List: adding the Source Address of each IND a MANT PDU traverses in the network as a list in the MANT header;
4. Hop Limit: limiting a MANT PDU to a specific number repeats, optional;
5. Echo Suppression: the ability, when Path List is enabled on a MANT PDU, to prevent repeating a MANT PDU that already has been transmitted once by this IND.
6. Time stamping: inserting a time stamp into the Application PDU header, if time is available, for known Application Protocol types;
7. Pass/Reject Listing: the ability to configure lists of Source or Destination addresses in the IND to either explicitly pass or exclude address from being repeated by this IND;
8. Best Effort network service; and
9. Acknowledged Datagram Service, a reliable end point to end point datagram service.

[1] Traditionally, modem means a device that only provides modulation and demodulation of a signal onto a media. Current use of the term modem includes devices with much more functionality. For example, a commercial "GPRS wireless modem" provides the TDMA media access, packet processing, forward error correction and significant additional functionality. In this specification, the term modem is used to convey the concept of transforming data for a communications medium; it is not defined with explicit functionality.

10. Over-the-Air IND configuration service

The specifications below, except as noted, define the MANT processing only for an IND operating as an originating modem or as a repeater. Except as noted, the only MANT processing an IND device provides at the terminating modem end is to output the parsed MANT PDUs according to the IND API.

Since most of the ALERT replacement implementations will be one-way self-reporting sites, the expectation is that there will be a demand for separate encoding and decoding devices for the near future. This document may at times discuss the MANT device in the context of two separate devices: an Encoder & Modulator (originating MANT layer device) and a Demodulator & Decoder (a device providing AirLink decoding, possibly interfaced to a MANT layer device for repeater operation). Integration of the two into a single cost-effective modem/IND is desirable, however, and nothing in the descriptions or standards in this document is intended to prohibit such an implementation.

2 MANT PDU and Header

2.1 MANT PDU

The ALERT2™ MANT PDU shall contain a MANT payload and a MANT header. The MANT header must be pre-pended to the payload. The MANT Payload provided by an APD or other device must be composed of byte elements. Unless the IND is requested to provide a service that requires inspection of the Payload (e.g. time stamping) the MANT layer protocols do not inspect the Payload, so its byte ordering or endian is not specified.

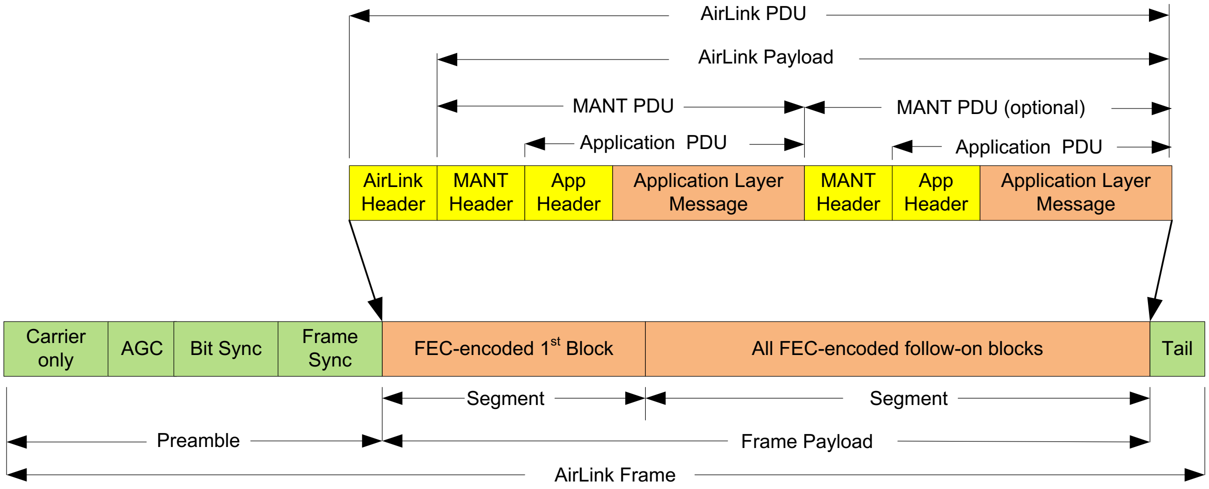

Figure 2-1 ALERT2™ Frame Terminology

To clarify terminology: for each layer, its payload plus the header it adds constitutes the layer's Protocol Data Unit (PDU). When passed from the application layer to the MANT, the application PDU becomes the MANT Payload. When the MANT header is added, that becomes the MANT PDU. At the AirLink layer, multiple MANT PDUs may be aggregated to form the AirLink payload, which in turn becomes the AirLink PDU when the AirLink header is pre-pended.

2.2 MANT Header

The following table lists the fields contained in the MANT Header; those enclosed in brackets are optional:

Field Name	**Field Length (bits)**	**Description**
Version	2	Current version is 0x0[2]; used for backward compatibility
Protocol ID	3	Network Protocol requested: best efforts, broadcast = 0; end to end reliable datagram service = 1.
Time Stamp Service Request flag	1	No TS service requested = 0; TS service requested = 1.
Add Path Service Request flag	1	No Add Path Service requested = 0; Add Path Service Requested = 1.
Destination Address (DA) included in header	1	MANT header is not extended to include a 16 bit Destination Address = 0; MANT header contains a 2 byte Destination Address immediately following the Source Address (SA) field.
Port	4	The Application or MANT protocol port number.
Encrypted Payload	1	Payload is not encrypted = 0; Payload encrypted = 1.
Reserved Bits field	2	Reserved for future use: encoded as 0x0 in Version 0.
ACK flag	1	Used to acknowledge a MANT PDU for End to End Reliable Datagram Service
Added Header flag	1	Provided for extensibility; MANT Payload begins immediately following the MANT header = 0; Additional header begins immediately following the MANT header.
Hop Limit	3	The maximum hops before the MANT PDU is discarded; when set to 0x7 the PDU is never discarded.
Payload Length	12	The MANT payload length in bytes.
Source Address	16	The Source Address of the originating IND.
[Destination Address]	[16]	When the DA included flag is set, this is the appended Destination Address.
[MANT PDU ID field]	[8]	MANT PDU ID field must be included when End to End Reliable Datagram Service Protocol ID is requested.

[2] Numeric values are represented in hexadecimal by prefacing them with “0x”.

[Number of Added Source Address]	[8]	When the Add Path Service Request bit is set, this counter must be the number of 2 byte SAs appended to the header.
[Source Address list]	[N*16]	The list of appended Source Addresses when the Add Path Service Request bit is set. N is the "Number of Added Source Addresses" field. Note: this field will not exist if N = 0.

Figure 2-2 MANT header field Name, Length and Description

As shown above, the MANT header must be a minimum of 36 bits. The header bit ordering must be as shown in the above table, where the most significant bit of the Version field is transmitted first, and must be the most significant bit of the most significant byte of the MANT header.

When no Destination Address is included in the header, the least significant bit of the least significant byte of the Source Address must immediately precede the first bit of the Payload.

2.2.1 Version

The Version field represents the MANT Protocol Version of the MANT header and MANT processing. For this Version 1.1 of the MANT Protocol Specification, an IND creating a MANT header must assign a 0x0 value to the Version field.

For this Version 1.1 of the MANT Protocol Specification, an IND receiving a MANT PDU for processing that contains a Version field not equal to 0x0 must discard the MANT PDU.

2.2.2 Protocol ID

The Protocol ID field shall be 3 bits, defining the type of communication service requested. There are two communication protocols defined by Version 1.1 of the MANT Protocol Specification:

1. Best Efforts, Broadcast: Protocol ID = 0; and
2. End to End Reliable Datagram Service, Broadcast: Protocol ID = 1.

MANT processing for Best Efforts, Broadcast shall be only to create the required MANT header as specified herein, append the MANT header to the Payload and send the MANT PDU to the AirLink layer.

MANT processing for End to End Reliable Datagram Service, Broadcast provides for acknowledged delivery services for an individual MANT Payload.

2.2.3 Time Stamp Service Request field

The Time Stamp Service Request (TSSR) field shall be a single bit flag. When set in a MANT header it indicates that the Payload has requested that the IND insert a time stamp if possible.

When the IND processes Payloads as an originating modem, it shall use the TS Request configuration parameter, as provided by the APD or during IND setup, to define the time stamp processing when creating MANT PDUs from APD Payloads. If the IND has a clock maintaining UTC time and the TS Request is set[3] the IND must inspect the configuration Port field. If the Port field is 0x0, the Application Layer Self-Reporting Protocol, or 0x1, the Application Layer Concentration Protocol (see the Application Layer Specification), the IND must insert a UTC 2 byte time stamp (with a format specified in the Application Layer Specification) and set the "Time Stamp" bit in the Application Layer header Control Byte. It shall then create this Payload's MANT header with the TSSR bit flag reset.

If the TS Request is set, but the IND does not have a clock maintaining UTC time or the Port field is not 0x0 or 0x1, the IND shall not insert a time stamp into the Application Layer Payload and shall create this Payload's MANT header with the TSSR bit flag set.

If the TS Request configuration parameter is reset, the IND shall not insert a time stamp in the Payload and shall then create this Payload's MANT header with the TSSR bit flag reset.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall inspect the MANT header for the TSSR bit flag. If set, and if the IND has a clock maintaining UTC time, the IND must inspect the MANT header Port field. If Port field is 0x0, the Application Layer Self-Reporting Protocol, or 0x1, the Application Layer Concentration Protocol (see the Application Layer Specification), the IND must insert a UTC 2 byte time stamp (with a format specified in the Application Layer Specification) and set the "Time Stamp" bit in the Application Layer header Control Byte. It shall then clear the MANT header TSSR bit flag.

If the TSSR is set in the MANT header, but the IND does not have a clock maintaining UTC time or the Port field is not 0x0 or 0x1, the IND shall not insert a time stamp into the Application Layer Payload and shall not clear the MANT header TSSR bit.

[3] In the context of single bit fields, "set" means value '1', and "cleared" or "reset" means value 0.

2.2.4 Add Path Service Request field

The Add Path Service Request (APSR) field shall be a single bit flag. It is used to request that the Source Address of a node that repeats this MANT PDU be appended to the MANT header. It's used for network diagnostics and must be set in order to enable Echo Suppression Service (specified below). Each node that repeats a MANT PDU appends its Source Address to a list of SAs. By inspecting the list at the final destination, the network path the MANT PDU traversed is evident.

When the IND processes Payloads as an originating modem, it shall use the Add Path Request configuration parameter, as provided by the APD or during IND setup, to define the Add Path processing when creating MANT PDUs from APD Payloads. When the Add Path Request configuration parameter is set, the IND shall insert the one byte "Number of Added Source Address" field filled with a value of 0x0 at the end of the MANT header and shall create this Payload's MANT header with the APSR bit flag set. When the Add Path Request configuration parameter is clear the IND shall not insert the "Number of Added Source Address" field at the end of the MANT and shall create this Payload's MANT header with the APSR bit flag reset.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall inspect the MANT header for the APSR bit. If set, the IND shall increment the one byte "Number of Added Source Address" field at the end of the MANT header, and shall append its 2 byte Source Address to this MANT header. It shall not change the APSR bit flag value in the MANT header. If the APSR bit flag is clear in the MANT header of a received MANT PDU, the IND shall not append its Source Address to the MANT header and shall not change the value of the MANT header APSR bit.

2.2.5 Destination Address included in header

The Destination Address Included in header (DAI) field shall be a single bit flag field. It is used to identify that the MANT header is extended by a 2-byte Destination Address. The Destination Address is used for Pass/Reject List Service and other communication protocols.

When the IND processes payloads as an originating modem, it shall use the Include Destination in header configuration parameter, as provided by the APD or during IND setup, to define whether a Destination Address is appended and the DAI bit flag is set in the created MANT header. When the Include Destination in header configuration parameter is set, the IND shall insert its 2 byte Destination Address immediately following the Source Address, and shall set the DAI bit in the MANT header when creating MANT PDUs from APD Payloads. If the Include Destination in header configuration parameter is reset, the IND shall not insert its Destination Address and shall ensure the DAI bit is clear in the MANT header when creating MANT PDUs from APD Payloads.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU containing a MANT header and Payload and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall not modify the DAI bit and shall not add or remove any appended Destination Address. It may be required to inspect the MANT header for the DAI bit and the Destination Address, if appended, for Pass/Reject List Service or other communications protocols.

2.2.6 Port

The Port field shall be a 4 bit field. It is used to identify to which Application layer or MANT layer protocol to send the MANT Payload. In MANT Version 1.1 the known ports are:

- Application Layer Self-Reporting Protocol (0x0),
- Application Layer Concentration Protocol (0x1), and
- IND Configuration & Control Protocol (0x80).

When the IND processes Payloads as an originating modem, it shall use the Port configuration parameter, as provided by the APD or during IND setup to define the value inserted in the created MANT header. The IND shall fill the Port field with the low order 4 bits of the Port configuration parameter when creating MANT PDUs from APD Payloads.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall not modify the Port field. It may inspect the Port field to determine whether the Port field is a known MANT Port which may cause the IND to process the Payload. The only known MANT Port defined in MANT Version 1.1 is the IND Configuration and Control Protocol, specified below.

2.2.7 Encrypted Payload field

The encrypted payload field shall be a single bit field. It is used to identify MANT PDUs containing an encrypted payload.

See the MANT Encryption Service protocol specification, below, for further information on MANT PDU encryption and this field.

2.2.8 Reserved Bits field

The Reserved Bits field shall be a 2 bit field. It is reserved for future use. When an IND creates a MANT Version 1.1 header, the Reserved Bits field shall be filled with the value 0x0.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall not modify the Reserved Bits field.

2.2.9 ACK bit field

The ACK bit field shall be a single bit field. It is used in conjunction with the End to End Reliable Datagram Service protocol.

See the End to End Reliable Datagram Service protocol specification, below, for the complete specification of this field.

2.2.10 Added Header field

The Added Header (AH) field shall be a single bit flag field. It is reserved for future use and provided for extensibility. When AH flag is reset, the MANT Payload begins immediately following the MANT header. In a future MANT Version, when AH flag is set, an additional header begins immediately following the MANT header.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall not modify the Added Header bit.

2.2.11 Hop Limit field

The Hop Limit field shall be a 3 bit field. When specified at the originating modem it limits the number of times a MANT PDU is repeated. When a repeater receives a MANT PDU for retransmission it inspects the received Hop Limit field. If its value is '0' the repeater discards the MANT PDU, otherwise, unless the Hop Limit field equals '7', the repeater decrements the Hop Limit field and inserts the modified Hop Limit in the MANT header for retransmission. Creating a MANT header at an originating modem with a Hop Limit value of '7 disables Hop Limit processing. This disabled mode is not recommended for most network architectures due to the possibility of repeaters continuously echoing MANT PDUs. Creating a MANT header with a Hop Limit value of '0' means that it will not be retransmitted by any repeater; this may be useful in restricting some sites to direct point to point paths.

When the IND processes Payloads as an originating modem, it shall use the Hop Limit configuration parameter, as provided by the APD or during IND setup to define the value inserted in the created MANT header. The IND shall fill the Hop Limit field with the low order 3 bits of the Hop Limit configuration parameter when creating MANT PDUs from APD Payloads.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall inspect the MANT header Hop Limit field. If its value is 0x7, the IND shall not modify the MANT Hop Limit field. If its value is between 0x01 and 0x06, it will decrement the received Hop Limit field and insert the modified Hop Limit field in the MANT header for retransmission. If the Hop Limit field is '0' the IND shall discard this MANT PDU and shall not send it to the AirLink for transmission.

2.2.12 Payload Length field

The Payload length field shall be a 12 bit field. Its value is the number of bytes in the MANT Payload.

When the IND processes Payloads as an originating modem, it shall calculate a Payload Length from the length provided by the APD when an Application Layer PDU is sent to the IND, adjusted for any MANT changes to the Payload (e.g. Time Stamp service). If the length is greater than the maximum MANT Payload of 4096 bytes, the IND will discard the Application PDU and, depending on the configuration of the IND I/O parameters, send an error message to the APD. If the length is less than the maximum payload length, the IND shall fill the Payload Length field with the low order 12 bits of the length when creating MANT PDUs from APD Payloads.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall not modify the Payload Length field unless it changes the Payload length (e.g. Time Stamp Service). If the IND changes the Payload Length, is must adjust the Payload Length field in the MANT header to the changed value. It shall also check that the new length is not greater than the maximum MANT Payload (see the paragraph above); if it is, the IND shall discard this MANT PDU and shall not send it to the AirLink for transmission.

2.2.13 Source Address field

The Source Address field shall be a 16 bit field. Its value is the Source Address of the originating device.

When the IND processes Payloads as an originating modem, it shall use the Source Address configuration parameter, as provided by the APD or during IND setup to define the value inserted in the created MANT header. The IND shall fill the Source Address field with the 2 bytes of Source Address configuration parameter, most significant byte first when creating MANT PDUs from APD Payloads.

When the IND is processing an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall not modify the Source Address field in the received MANT header. The IND may be required to inspect the Source Address field for MANT processing (e.g. Pass/Reject List Service processing).

2.2.14 Destination Address field, optional

The Destination Address field shall be a 16 bit field optionally appended to the MANT header immediately following the Source Address field.

When the IND processes Payloads as an originating modem, it shall use the Include Destination Address configuration parameter, as provided by the APD or during IND setup to define the whether to append a Destination Address to the MANT header. If the Include Destination Address configuration parameter is set, the IND shall fill the Destination Address field with the 2 bytes of Destination Address configuration parameter, as provided by the APD or during IND setup, most significant byte first when creating MANT PDUs from APD Payloads.

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall not modify the Destination Address field in the received MANT header. The IND may be required to inspect the Destination Address field for MANT processing (e.g. Pass/Reject List Service processing).

2.2.15 MANT PDU ID field, optional

The MANT PDU ID field shall be an 8 bit field optionally appended to the MANT header immediately following the Destination Address field. A MANT header must not be created containing a MANT PUD ID field without the existence of a Destination Address field and a Protocol ID field value of 0x02.

See the End to End Reliable Datagram Service protocol specification, below, for the complete specification of this field.

2.2.16 Number of Added Source Addresses field, optional

The Number of Added Source Addresses field shall be an 8 bit field optionally appended to the MANT header immediately following the Source Address or Destination Address field. A MANT header must not be created containing a Number of Added Source Addresses field without the APSR bit flag set.

See the Add Path Service Request field above for the specified use of this field.

2.2.17 Source Address List field, optional

The Source Addresses list field shall be a field containing from zero to six Source Addresses, (0 to 12 bytes), appended immediately following the Number of Added Source Addresses field. The limit of six SA is consistent with Hop Limit maximum count, except for the “unlimited” Hop Limit case. A MANT header must not be created containing a Source Address List field without the APSR bit flag set.

See the Add Path Service Request field above for the specified use of this field.

3 MANT Service Protocols

In addition to the MANT Services described above, other MANT Service Protocols are available. Some utilize multiple MANT header fields.

3.1 Echo Suppression MANT Service Protocol

The Echo Suppression MANT Service Protocol provides another method to eliminate undesirable propagation of MANT PDUs in an ALERT2™ network. Unless Add Path Service is enabled, Echo Suppression Service is not effective.

Echo Suppression MANT Service Protocol shall be enabled or disabled at an IND by the Echo Suppression configuration parameter, as provided by the APD or during IND setup.

When Echo Suppression is enabled, and the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND shall inspect the MANT header for the APSR bit flag. If the APSR bit flag is set, it must inspect the list of Source Addresses appended by the Add Path Service. If the IND identifies its own Source Address in the Source Address List field, the IND shall discard this MANT PDU; it must not be sent to the AirLink for transmission. If the IND's Source Address is not identified in the Source Address List field this MANT PDU shall be processed, as necessary, in accordance with the information in the other MANT header fields, for retransmission.

The Echo Suppression Service Protocol takes precedence over the Hop Limit field, to the extent that if Echo Suppression Service is enabled and the IND identifies its Source Address in the Source Address List field, the MANT PDU is discarded regardless of the value in the Hop Limit field.

Unless Echo Suppression discards the MANT PDU it does not disable any other MANT service, (e.g. if the Hop Limit is 0, the MANT PDU will be discarded independent of the Echo Suppression Service processing).

3.2 Pass/Reject List MANT Service Protocol

The Pass/Reject List MANT Service Protocol provides another method to eliminate undesirable propagation of MANT PDUs in an ALERT2™ network. It also enables routing MANT PDUs by configuring static Source and Destination pass and reject tables at repeaters.

The IND shall provide a minimum of one list each for storing Source Addresses named, respectively:

- Source Address Pass list; and
- Source Address Reject list.

It is recommended that an IND provide a minimum of one list each for storing Destination Addresses named, respectively:

- Destination Address Pass list; and
- Destination Address Reject list.

Each list shall be capable of being enabled or disabled. Each list shall be capable of containing individual addresses and inclusive ranges of contiguous addresses. It is recommended that an IND contain a minimum of 2 lists of each type of list, although only one list of each of the 4 types shown above shall be enabled at any one time.

If the Source Address Pass list is enabled, the IND shall inspect the SA field in the header of all received MANT PDUs; if the IND’s SA is not one of the Addresses in the Source Address Pass list the MANT PDU shall be marked for discarding. If the IND’s Source Address is in the Source Address Pass list the IND shall not mark the MANT PDU for discarding based on Source Address Pass list processing. If the Source Address Pass list is enabled but empty, the IND shall mark all MANT PDUs for discarding. If no Source Address Pass list is enabled, the IND shall not mark any MANT PDUs for discarding based on Source Address Pass list processing.

If the Source Address Reject list is enabled, the IND shall inspect the SA field in the header of all received MANT PDUs; if the IND’s SA is one of the Addresses in the Source Address Reject list the MANT PDU shall be marked for discarding. If the IND’s Source Address is not in the Source Address Reject list the IND shall not mark the MANT PDU for discarding based on Source Address Reject list processing. If the Source Address Reject list is enabled but empty, the IND shall not mark any MANT PDUs for discarding based on Source Address Reject list processing. If no Source Address Reject list is enabled, the IND shall not mark any MANT PDUs for discarding based on Source Address Reject list processing.

If the Destination Address Pass list is enabled, the IND shall inspect the DA field, if available in the header, of all received MANT PDUs; if the IND’s DA is not one of the Addresses in the Destination Address Pass list the MANT PDU shall be marked for discarding. If the IND’s Destination Address is in the Destination Address Pass list, or there is no DA field in the received MANT header, the IND shall not mark the MANT PDU for discarding based on Destination Address Pass list processing. If the Destination Address Pass list is enabled but empty, the IND shall mark all MANT PDUs for discarding. If no Destination Address Pass list is enabled, the IND shall not mark any MANT PDUs for discarding based on Destination Address Pass list processing.

If the Destination Address Reject list is enabled, the IND shall inspect the DA field, if available in the header, of all received MANT PDUs; if the IND's DA is one of the Addresses in the Destination Address Reject list the MANT PDU shall be marked for discarding. If the IND's Destination Address is not in the Destination Address Reject list, or there is no DA field in the received MANT header, the IND shall not mark the MANT PDU for discarding based on Destination Address Reject list processing. If the Destination Address Reject list is enabled but empty, the IND shall not mark any MANT PDUs for discarding based on Destination Address Reject list processing. If no Destination Address Reject list is enabled, the IND shall not mark any MANT PDUs for discarding based on Destination Address Reject list processing.

After the Pass List and Reject List processing above, for the enabled Pass and Reject Lists, any MANT PDU marked for discarding shall be discarded and not sent to the AirLink for retransmission.

3.3 End to End Reliable Datagram Service Protocol

End to End Reliable Datagram Service (EERDS) communications Protocol provides an Application Layer Protocol Device a method to ensure the delivery of an Application Layer PDU. When EERDS protocol is selected, the IND requests an acknowledgement from the final destination. When an acknowledgement is received, the IND informs the APD of EERDS success. If an acknowledgement is not received within a configured retry delay period, the IND will resend the MANT PDU containing the Application Layer PDU. If an acknowledgement is not received after a configurable number of retransmissions, the IND informs the APD of EERDS failure.

When EERDS is requested at an originating IND, the IND must:

- create the MANT header with:
    - the Protocol ID field set to the EERDS Protocol ID (0x1);
    - the current Destination Address configuration parameter added; and
    - the MANT PDU ID added.
- retain a copy of the MANT PDU; and
- initialize a retransmission counter for that retained MANT PDU.

The MANT PDU ID shall be incremented on every new EERDS MANT PDU creation. Each time the MANT PDU ID is incremented, the IND shall inspect all retained MANT PDU headers for a MANT PDU ID equal to the new MANT PDU ID value. If a MANT PDU ID is discovered in the retained MANT PDUs, the IND must discard that MANT PDU and inform the APD that EERDS failed on that Application Layer PDU. On the first (since IND restart) instance of an EERDS request, the IND shall set the MANT PDU ID to an initial value '0'. When the MANT PDU ID increments to decimal value 256, the IND shall reset the MANT PDU ID to value '0'.

A MANT PDU EERDS Acknowledgement shall occur for a retained MANT PDU when the originating IND receives a MANT PDU from the AirLink where:

- the Protocol ID field value is equal to the EERDS Protocol ID (0x01);
- the ACK field bit is set;
- the received SA matches the retained MANT PDU DA;
- the received DA matches the retained MANT PDU SA; and
- the MANT PDU ID matches the retained MANT PDU ID.

When a MANT PDU EERDS Acknowledgement occurs for a retained MANT PDU, the IND shall discard that retained MANT PDU and inform the APD of the EERDS success.

If the IND does not receive an EERDS Acknowledgement before the retry delay period for a retained EERDS MANT PDU, the IND shall inspect the retained MANT PDU's retransmission counter. If the count equals the configured number of retransmissions parameter, the IND shall discard the retained MANT PDU and shall inform the APD of the EERDS failure. If the count is less than the configured number of retransmissions parameter, the IND shall retransmit the retained MANT PDU and increment this retained MANT PDU's retransmission counter.

If an IND receives an EERDS Acknowledgement that does not match any of the currently retained EERDS MANT PDUs (i.e. the combination of SA, DA and MANT PDU ID), the IND shall ignore the EERDS Acknowledgement. (The IND shall not discard the received MANT PDU, unless there is no MANT Payload in the MANT PDU that contained the EERDS Acknowledgement.)

When the IND processes an arriving MANT PDU as a repeater, i.e. when the input to the IND is a MANT PDU from the AirLink and the repeater IND's Source Address is not the Destination Address in the received MANT header, the IND EERDS protocol shall not modify the MANT PDU.

When the IND processes an arriving MANT PDU which includes a Destination Address, and that received Destination Address equals the IND's Source Address, and the Protocol ID field is set to EERDS, the IND must create and an Acknowledgement MANT PDU, as specified above. The MANT header fields not specified in the Acknowledgement shall be defined according to the current configuration parameters of the IND. The created MANT PDU shall be sent as soon as possible to the AirLink for transmission on the radio network.

3.4 MANT Configuration & Control Protocol

Configuration and control of an IND may be done over the radio network by using MANT Port 0x80 protocol, the MANT Configuration and Control Protocol. A MANT Port is conceptually the same as an Application Layer Protocol; the difference is that the MANT PDU Payload is not forwarded to the Application Layer, but utilized at the MANT Layer. In the MANT Configuration and Control Protocol, the MANT PDU Payload contains the configuration parameters that change the IND configuration. The configuration parameters are encoded in the MANT Payload using the identical binary TLV encoding used for the asynchronous serial binary interface defined in the IND API specification, except that the first byte, the <SOH> byte is not included. The MANT Payload is then the concatenation of one or more binary Type, Length and Value structures.

For example, a MANT Payload containing the bytes: 0x18 0x02 0x11 0x33 0x78 0x00 would be processed by the IND as a configuration of its Source Address (type 0x18, length 0x2) to the value 0x1133 (decimal 4403) and Save Configuration in non-volatile memory (type 0x78, length 0x00) command.

When the IND processes an arriving MANT PDU where the MANT header contains a Destination Address equal to the IND's Source Address, and the Port field value is the MANT Configuration and Control Protocol, the IND shall parse the Payload in accordance with the specifications for the "Binary Asynchronous Serial Interface" section IND API specification, except that the initial <SOH> is not included. The IND shall process only those commands listed in the "Protocol Services configuration" table in the "Binary Asynchronous Serial Interface" section. Any Type, Length, Value structures not defined in that table shall be ignored.

3.5 MANT PDU Encryption and Authentication Protocol

The MANT PDU Encryption and Authentication Protocol supports the transmission of confidential data in an ALERT2 network (encryption) and provides a means to validate that messages received via an ALERT2 network were sent by an authorized sender (authentication). Encryption is implemented at the MANT layer, concealing the payload while leaving the header in plain text. Repeaters, therefore, need not know how to decrypt a message in order to process it, and plain text and encrypted messages can coexist on the same system.

3.5.1 Encryption and Authentication Overview

The core encryption algorithm used in ALERT2 is AES-128, in the counter mode of operation. Counter mode (CTR) is particularly well suited to low-bandwidth applications because it introduces no message-size overhead. In CTR mode, the sender and the receiver both need to know a secret key and one additional piece of shared information, called a nonce. The nonce need not be secret, but should never be reused with the same key.

This protocol defines a simple authentication scheme: if a message can be successfully decrypted using a shared encryption key, it is considered to be genuine. In order for an encrypted message to be transmitted and received successfully, both the sender and the receiver must use the same secret key. In short, anyone possessing the encryption key is authenticated. This means that system maintainers must have a process for retiring keys in the case that a key is compromised, and should cycle keys on a regular schedule.

A word of caution is warranted here: it is difficult to prevent a determined attacker with physical access to a programmed ALERT2 device from recovering an encryption key. However, ALERT2 IND manufacturers should take reasonable precautions to secure encryption keys on remote devices.

3.5.2 Modes of Attack

In addition to traditional attacks on the encryption algorithm or the key, a security solution for ALERT2 needs to be concerned with replay attacks and forgeries.

In a replay attack, the attacker need not know how to decrypt a message. Instead, the attacker simply records the message and plays it back later. For example, an attacker might record the command used to turn on a warning siren during a planned test, and then attempt to broadcast that same message, unaltered, at a later time.

In a forgery, an attacker attempts something similar - leaving the encrypted payload of a message intact, but modifying the message metadata. For example, taking an "open the gate" message intended for site A, changing the destination address to site B, and then transmitting it.

By using an ever-increasing message ID and a cryptographic hash, we can protect against both types of attacks. In CTR mode, we combine this message ID with the source address of the MANT PDU and use that as the nonce.

3.5.3 Implementation

If encryption is enabled, before transmitting a MANT PDU, the IND shall prepend a 3-byte Encrypted Message ID (EMID) to the beginning of the MANT payload. The EMID value shall begin at zero, and shall increment by one each time the IND creates an encrypted MANT PDU. The value of the EMID should be stored to non-volatile memory after it has been incremented. Users may set the next EMID value using the EMID API command, or reset the EMID to zero by changing the encryption keys. The same Source Address and Encryption Key should never be reused with the same EMID, and the receiving device will refuse to decrypt messages with an EMID that is less than or equal to the last valid EMID received. In the event that a device needs to be replaced, the EMID must be set to a value greater than the last transmitted message, but it is not necessary to set the EMID to exactly the next value in the sequence; so long as it is greater than the last EMID sent by the device and it is not too close to the maximum value, any number will work. Alternatively, if the encryption keys are changed, the EMID can be reset to 0. This is preferable if the replaced device was compromised (e.g. stolen).

In order to ensure message integrity, the IND shall compute the SHA-1 hash of the MANT header, first masking the hop limit bits so they are always zero, and excluding the number of added source addresses and the source address list, concatenated with the MANT payload, including the EMID. The IND shall truncate this hash, retaining only the most significant 4 bytes, and append it, most significant byte first, to the MANT payload. The payload length field in the header shall be updated to reflect the additional 7 bytes of payload.

The IND shall then encrypt the MANT payload, starting after the EMID and including the hash, using AES-128 in CTR mode. The Initialization Vector used for the AES-CTR mode encryption consists of the two-byte source address and the three-byte EMID value in the high bits, and zeros in the low bits. (CTR mode is a block cipher operating on fixed chunks of data 128-bits in size; it will increment the lower-bits of the IV with each new block.) If a source-address specific encryption key is set for an outgoing MANT message, the IND will use that for encryption. Otherwise, the global one will be used.

Upon receipt of a MANT message with the encryption flag set, the receiving IND compares the EMID at the start of the payload block to the EMID of the last valid message received from the same source address (stored in non-volatile memory). If the received EMID is not strictly greater than the last valid EMID received, the message shall be discarded. Note: regardless of whether the transmitters in the system are using a general purpose encryption key or a site specific encryption key, the transmitter maintains a single, monotonically incrementing EMID value, while the receiver maintains an EMID value for each source address from which it has received encrypted messages. Further, it is possible for the transmitter to be configured to send MANT PDUs using different source addresses -- either through independent source address configuration or through the IND API -- but the transmitter still retains a single EMID and encryption key used across these addresses. EMID values are reset when encryption keys are changed.

If the EMID transmitted with the MANT payload is greater than the EMID stored on the device (from the last successfully decoded message), the IND should decrypt the MANT payload using either the general purpose key or a Source Address Specific key, if one is present. After decrypting the message, the receiving IND should compute the SHA-1 hash of the MANT header and the decoded payload, and compare the result to the received hash value. If the values do not match, the message shall be discarded. If the message is found to be valid, the EMID associated with the Source Address of the message shall be updated in non-volatile memory, and the IND shall output the decrypted results.

The Encrypted Payload bit shall only be set when the contents of the payload are actually encrypted. After successful decryption, this bit shall be cleared when the message is output.

In order to ensure backwards compatibility, the "Add Timestamp" flag shall be set to 0 on an encrypted MANT packet.

3.5.4 Key Generation

To support a user-friendly and portable mechanism for key generation, it is recommended that user-facing applications implement a process where a 16-byte binary key can be generated from a variable length passphrase by using the first 16-bytes of the SHA256 hash of the passphrase.

For example, the passphrase “this is my passphrase” would generate the key “53:57:CE:17:87:33:55:2B:11:76:D4:30:6E:C2:B1:5D”.

3.5.5 Example

Consider the following MANT PDU:

	Header									Payload										
Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Value	03	00	10	0b	03	e8	06	40	00	70	01	08	12	12	03	24	13	22	02	76

Figure 3-1 MANT PDU before encryption

When encrypted using an EMID of 850 (decimal) and a 16-byte encryption key of “keep me secret!!” the encryption process is as follows.

- Update the MANT PDU with the EMID, set the encrypted flag, and increase the payload length

	Header									EMID			Payload										
Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Value	03	08	10	12	03	e8	06	40	00	00	03	52	70	01	08	12	12	03	24	13	22	02	76

Figure 3-2 MANT PDU with EMID added, encryption flag set, and length updated. Note that the payload does not yet contain the 4-byte hash despite the longer length field in the header.

- Compute the SHA1 hash of the updated MANT PDU, masking the hop limit bits and removing the source address list. Retain the first four bytes of the hash.

	Header								EMID			Payload										
Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Value	03	08	00	12	03	e8	06	40	00	03	52	70	01	08	12	12	03	24	13	22	02	76

Figure 3-3 MANT PDU as input to SHA1 algorithm

Note that the MANT is shown with hop limit bits masked and the source address list removed. The resulting hash begins with "**72 5d b2 b2**".

- Encrypt the payload using AES-128 in CTR mode

Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Key	6b	65	65	70	20	6d	65	20	73	65	63	72	65	74	21	21
IV	03	e8	00	03	52	00	00	00	00	00	00	00	00	00	00	00

Figure 3-4 Encryption key and initialization vector

The key is defined externally as "keep me secret!!", and the Initialization Vector consists of the two-byte source address and the three-byte EMID value followed by zeros.

	Header									EMID			Payload											Hash			
Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Plaintext	03	08	10	12	03	e8	06	40	00	00	03	52	70	01	08	12	12	03	24	13	22	02	76	72	5d	b2	b2
Encrypted	03	08	10	12	03	e8	06	40	00	00	03	52	11	46	df	21	a1	e0	fb	1e	42	5c	93	1a	7c	62	50

Figure 3-5 Plaintext input and encrypted output

The resulting payload leaves the header and the EMID in plain text while scrambling the payload and the hash.

4 Glossary

Abbreviation	Description
APD	Application Program Device – a device that implements the application layer protocols
APD Payload	Application Program Device Payload – the input to an IND from for transmission on the ALERT2 network, typically an Application Layer PDU.
API	Application Program Interface – the means and specifications for communication between programs; in this document it refers to the interface with an Intelligent Network Device
APSR	Add Path Service Request – a 1-bit field in the MANT header used to request that each IND add its source address as it forwards a frame
DA	Destination Address – the Source Address of the IND to which a PDU is directed
DAI	Destination Address included in header – a 1-bit MANT header field used to indicate that the destination address is added to the header
EERDS	End-to-End Reliable Datagram Service – a MANT protocol used to confirm delivery of application PDUs
flag	A one bit informational field. To “set” a flag means make its value ‘1’. A flag is “set” when its value is ‘1’ To “clear” or “reset” a flag means to make its value ‘0’. A flag is “cleared” or “reset” when its value is ‘0’.
IND	Intelligent Network Device – A device that implements both the AirLink and MANT protocols, e.g., an Encoder & Modulator or a Demodulator & Decoder integrated with an Encoder & Modulator (a repeater).
MANT	The middle layer of the ALERT2™ 3-layer protocol stack. It is responsible for network and transport services
PDU	Protocol Data Unit – a unit of data containing a control header and a data payload that is exchanged between peer layers
SA	Source Address – the 16 bit identifier of the originating IND
TSSR	Time Stamp Service Request - a 1-bit MANT header field used to request that the receiving IND add a timestamp to certain MANT PDUs
UTC	Universal Coordinated Time, also known as Greenwich Mean Time (GMT)

`

5 Revisions

Beginning with Version 1.2, changes to the specification are summarized here.

5.1 Version 1.2

- Add MANT Encryption and Authorization Protocol
  - Add Encrypted Payload flag to the MANT Header in Section 2.2. Because this field uses one of the existing reserved bit fields in the header, it is backwards compatible. Devices implementing an older version of the specification will create new MANT PDUs with the field set to 0 (unencrypted) and will not modify the header.
  - Add Section 3.5: MANT PDU Encryption and Authentication Protocol

`

The ALERT Version 2 protocol would not have been possible without the dedication, time and energy of members of ALERT2™ Protocol Technical Working Group. The NHWC would like to thank the member organizations that allowed their people to provide their time.

For more information
Visit our website at www.hydrologicwarning.org
Send an email request to president@hydrologicwarning.org