Supporting ZDOs with the XBee API

The ZigBee Device Profile is a management and discovery service layer supported on all ZigBee devices. Like all other profiles, the ZigBee Device Profile defines a set of clusters that can be used to perform a variety of advanced network management and device discovery operations. Since the ZigBee Device Profile is supported to some extent on all ZigBee devices, many ZigBee Device Profile cluster operations can be performed on a variety of ZigBee devices, regardless of the stack or chipset manufacturer.

The ZigBee Device Profile has an application profile identifier of 0x0000. All ZigBee devices support a reserved endpoint called the ZigBee Device Objects (ZDO) endpoint. The ZDO endpoint runs on endpoint 0 and supports clusters in the ZigBee Device Profile. All devices that support the ZigBee Device Profile clusters support endpoint 0.

ZDO services include the following features:

- View the neighbor table on any device in the network
- View the routing table on any device in the network
- View the end device children of any device in the network
- Obtain a list of supported endpoints on any device in the network
- Force a device to leave the network
- Enable or disable the permit-joining attribute on one or more devices

Supporting the ZDP with the XBee API

The XBee API provides a simple interface to the ZigBee Device Objects endpoint.

The explicit transmit API frame (API ID 0x11) allows data transmissions to set the source and destination endpoints, cluster ID, and profile ID. ZDO commands can be sent by setting the source and destination endpoints to the ZDO endpoint (0x00), the profile ID to the ZigBee Device Profile ID (0x0000), and the cluster ID to the appropriate ZDO cluster ID.

The data payload must contain a sequence number as the first byte (transaction sequence number), followed by all required payload bytes for the ZDO. Multi-byte fields must be sent in little endian byte order.

To receive ZDO commands and responses, the AO (API Output) command must be set to 1. This enables the explicit receive API frame (API ID 0x91) which indicates the source and destination endpoints, cluster ID, and profile ID.

The following section outlines common ZDO commands including the following:

ZDO Command	Cluster ID
Network (16-bit) Address Request	0x0000
Network (16-bit) Address Response	0x8000
IEEE (64-bit) Address Request	0x0001
IEEE (64-bit) Address Response	0x8001
Node Descriptor Request	0x0002
Node Descriptor Response	0x8002
Simple Descriptor Request	0x0004
Simple Descriptor Response	0x8004
Active Endpoints Request	0x0005
Active Endpoints Response	0x8005
Match Descriptor Request	0x0006
Match Descriptor Response	0x8006
Complex Descriptor Request	0x0010
Complex Descriptor Response	0x8010
User Descriptor Request	0x0011
User Descriptor Response	0x8011
User Descriptor Set	0x0014
Management Network Discovery Request	0x0030
Management Network Discovery Response	0x8030
Management LQI (Neighbor Table) Request	0x0031
Management LQI (Neighbor Table) Response	0x8031
Management Rtg (Routing Table) Request	0x0032
Management Rtg (Routing Table) Response	0x8032
Management Leave Request	0x0034
Management Leave Response	0x8034
Management Permit Join Request	0x0036
Management Permit Join Response	0x8036
Management Network Update Request	0x0038
Management Network Update Notify	0x8038

NOTE: At the time of this writing, the XBee ZB 2x41 firmware does not support the match descriptor, complex descriptor, user descriptor, and management network discovery ZDOs. These commands can be sent with the API, but remote XBees will not respond to these ZDOs at this time. Future firmware releases might add support for these.

ZDO Clusters

Network Address Request

Cluster ID: 0x0000
Description: Broadcast transmission used to discover the 16-bit (network) address of a remote device with a matching 64-bit address.

Field Name	Size (bytes)	Description
IEEE Address	8	64-bit address of a device in the network whose 16-bit (network) address is being discovered
Request Type	1	0x00 – Single device response. (Only the device with a matching IEEE address responds.) 0x01 – Extended response. (The device with a matching IEEE address responds AND sends a list of the 16-bit addresses of devices in its associated device list starting at 'Start Index' until the next entry won't fit in the data payload.
Start Index	1	Indicates the starting index in the associated device list to return 16-bit addresses. Only used if extended response is requested.

Network Address Response

Cluster ID: 0x8000
Description: Indicates the 16-bit (network) address of a remote whose 64-bit address matched the address in the request. If an extended response was requested, this will also include the 16-bit addresses of devices in the associated device list.

Field Name	Size (bytes)	Description
Status	1	
IEEE Address	8	Indicates the 64-bit address of the responding device
Network Address	2	Indicates the 16-bit address of the responding device
Number of Addresses	0/1	Returns the number of addresses in the packet. Byte not included in response if an extended response was not requested.
Start Index	0/1	Starting index into the associated device list for this report. Multiple requests might be necessary to read all devices in the list.
Network Addresses of Associated Device List	Variable	List of all 16-bit addresses in the associated device list.

IEEE Address Request

Cluster ID: 0x0001
Description: Unicast transmission used to discover the 64-bit (IEEE) address of a remote device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose 64-bit (network) address is being discovered
Request Type	1	0x00 – Single device response. (Only the device with a matching IEEE address responds.) 0x01 – Extended response. (The device with a matching IEEE address responds AND sends a list of the 16-bit addresses of devices in its associated device list starting at 'Start Index' until the next entry won't fit in the data payload.
Start Index	1	Indicates the starting index in the associated device list to return 16-bit addresses. Only used if extended response is requested.

IEEE Address Response

Cluster ID: 0x8001
Description: Indicates the 64-bit (IEEE) address of a remote whose 16-bit address matched the address in the request. If an extended response was requested, this will also include the 16-bit addresses of devices in the associated device list.

Field Name	Size (bytes)	Description
Status	1	
IEEE Address	8	Indicates the 64-bit address of the responding device
Network Address	2	Indicates the 16-bit address of the responding device
Number of Addresses	0/1	Returns the number of addresses in the packet. Byte not included in response if an extended response was not requested.
Start Index	0/1	Starting index into the associated device list for this report. Multiple requests might be necessary to read all devices in the list.
Network Addresses of Associated Device List	Variable	List of all 16-bit addresses in the associated device list.

Node Descriptor Request

Cluster ID: 0x0002
Description: Transmission used to discover the node descriptor of a device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose node descriptor is being requested.

Node Descriptor Response

Cluster ID: 0x8002
Description: Indicates the node descriptor of the device.

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Node Descriptor	Variable	See node descriptor below.

Node Descriptor

Name	Size (bits)	Description
Logical Type	3	Indicates the logical device type: 000 – Coordinator 001 – Router 010 – End device
Complex Descriptor Available	1	0 – Complex descriptor not supported 1 – Complex descriptor supported
User Descriptor Available	1	0 – User descriptor not supported 1 – User descriptor supported
Reserved	3	
APS flags	3	Not supported. Set to 0
Frequency Band	5	bit0 – 868 MHz bit1 – Reserved bit2 – 900 MHz bit3 – 2.4 GHz bit4 – Reserved
MAC capability flags	8	Bit0 – Alternate PAN coordinator Bit1 – Device Type Bit2 – Power source Bit3 – Receiver on when idle Bit4-5 – Reserved Bit6 – Security capability Bit7 – Allocate address
Manufacturer Code	16	Indicates the manufacturer's code assigned by the ZigBee Alliance.
Maximum Buffer Size	8	Maximum size in bytes, of a data transmission (including APS bytes)
Maximum incoming transfer size	16	Maximum number of bytes that can be received by the node.
Server mask	16	
Maximum outgoing transfer size	16	Maximum number of bytes that can be transmitted by this device, including fragmentation.
Descriptor capability field	8	Bit0 – Extended active endpoint list available Bit1 – Extended simple descriptor list available

Simple Descriptor Request

Cluster ID: 0x0004
Description: Transmission used to discover the simple descriptor of a device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose simple descriptor is being requested.
Endpoint	1	The endpoint on the destination from which to obtain the simple descriptor.

Simple Descriptor Response

Cluster ID: 0x8004
Description: Indicates the simple descriptor of the device.

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Length	1	Length of the simple descriptor
Simple Descriptor	Variable	See simple descriptor below.

Simple Descriptor

Name	Size (bits)	Description
Endpoint	8	The endpoint on the node to which this descriptor refers.
Application profile ID	16	The profile ID supported on this endpoint.
Application device ID	16	Specifies the device description identifier supported on the device
Application device version	4	The version of the device description supported on this endpoint.
Reserved	4	
Input cluster count	8	The number of input clusters supported on this endpoint.
Input cluster list	Variable	The list of input clusters supported on this endpoint. Each cluster is 2 bytes in size. This field is not included if the input cluster count is 0.
Output cluster count	8	The number of output clusters supported on this endpoint.
Output cluster list	Variable	The list of output clusters supported on this endpoint. Each cluster is 2 bytes in size. This field is not included if the output cluster count is 0.

Active Endpoints Request

Cluster ID: 0x0005
Description: Transmission used to discover the active endpoints on a device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose active endpoint list being requested.

Active Endpoints Response

Cluster ID: 0x8005
Description: Indicates the list of active endpoints supported on the device.

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Active Endpoint Count	1	Number of endpoints in the following endpoint list
Active Endpoint List	Variable	List of endpoints supported on the destination device. One byte per endpoint.

Match Descriptor Request

Cluster ID: 0x0006
Description: Broadcast or unicast transmission used to discover the device(s) that supports a specified profile ID and/or clusters.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose power descriptor is being requested.
Profile ID	2	Profile ID to be matched at the destination.
Number of Input Clusters	1	The number of input clusters in the In Cluster List for matching. Set to 0 if no clusters supplied.
Input Cluster List	2 * Number of Input Clusters	List of input cluster IDs to be used for matching.
Number of Output Clusters	1	The number of output clusters in the Output Cluster List for matching. Set to 0 if no clusters supplied.
Output Cluster List	2 * Number of Input Clusters	List of output cluster IDs to be used for matching.

Match Descriptor Response

Cluster ID: 0x8006
Description: If a descriptor match is found on the device, this response contains a list of endpoints that support the request criteria.

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Length	1	The number of endpoints on the remote device that match the request criteria.
Match List	Variable	List of endpoints on the remote that match the request criteria.

Complex Descriptor Request

Cluster ID: 0x0010
Description: Transmission used to discover the complex descriptor on a device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose complex descriptor is being requested.

Complex Descriptor Response

Cluster ID: 0x8010
Description: Indicates the complex descriptor of the device.

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Length	1	The number of bytes (size) of the complex descriptor
Complex Descriptor	Variable	

User Descriptor Request

Cluster ID: 0x0011
Description: Transmission used to discover the user descriptor on a device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose user descriptor is being requested.

User Descriptor Response

Cluster ID: 0x8011
Description: Indicates the user descriptor of the device.

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Length	1	The number of bytes (size) of the user descriptor
User Descriptor	Variable	

User Descriptor Set

Cluster ID: 0x0014
Description: Transmission used to set the user descriptor on a device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose user descriptor is being requested.
Length	1	Length of the user descriptor (up to 16 bytes).
User Descriptor	Up to 16	The user descriptor that should be set on the remote.

Management Network Discovery Request

Cluster ID: 0x0030
Description: Unicast transmission used to cause a remote device to perform a network scan (to discover nearby networks).

Field Name	Size (bytes)	Description
Scan Channels	4	Bitmap indicating the channel mask that should be scanned. Examples (big endian byte order): Channel 0x0B = 0x800 Channel 0x10 = 0x10000 Channel 0x1A = 0x4000000 All Channels (0x0B – 0x1A) = 0x07FFF800
Scan Duration	1	Time to scan on each channel
Start Index	1	Start index in the resulting network list.

Management Network Discovery Response

Cluster ID: 0x8030
Description: Response to a network discovery request.

Field Name	Size (bytes)	Description
Status	1	
Network Count	1	The total number of networks discovered.
Start Index	1	The starting point in the network list.
Network List Count	1	The number of network list descriptors included in this response.
Network List	Variable	A list of descriptors, one per discovered network.

Network List Descriptor

Name	Size (bits)	Description
Extended PAN ID	64	The 64-bit extended PAN ID of the network
Channel	8	Current logical channel of the network.
Stack Profile	4	Indicates the stack profile of the network
ZigBee Version	4	ZigBee protocol version of the network
Beacon Order	4	MAC layer beacon order.
Superframe Order	4	MAC layer superframe order.
PermitJoining	1	0 – Joining is not enabled 1 – Joining is currently enabled
Reserved	7	Reserved

Management LQI (Neighbor Table) Request

Cluster ID: 0x0031
Description: Unicast transmission used to cause a remote device to return the contents of its neighbor table.

Field Name	Size (bytes)	Description
Start Index	1	Start index in the neighbor table to return neighbor entries. The response cannot include more than 2-3 entries. Multiple LQI requests may be required to read the entire neighbor table.

Management LQI (Neighbor Table) Response

Cluster ID: 0x8031
Description: Indicates the neighbor table contents of the device.

Field Name	Size (bytes)	Description
Status	1	
Neighbor Table Entries	1	The total number of neighbor table entries
Start Index	1	The starting point in the neighbor table
Network Table List Count	1	The number of neighbor table entries in this response
Neighbor Table List	Variable	A list of neighbor table entries.

Neighbor Table Entry

Name	Size (bits)	Description
Extended PAN ID	64	The 64-bit extended PAN ID of the neighboring device
Extended Address	64	64-bit address of the neighboring device
Network Address	16	The 16-bit address of the neighboring device
Device Type	2	The type of neighbor: 0x0 – ZigBee coordinator 0x1 – ZigBee router 0x2 – ZigBee end device 0x3 – Unknown
Receiver On When Idle	2	Indicates if the neighbor's receiver is enabled during idle times. 0x0 – Receiver is off 0x1 – Receiver is on 0x02 – Unknown
Relationship	3	The relationship of the neighbor with the remote device: 0x0 – Neighbor is the parent 0x1 – Neighbor is a child 0x2 – Neighbor is a sibling 0x3 – None of the above 0x4 – Previous child
Reserved	1	Set to 0.
Permit Joining	2	Indicates if the neighbor is accepting join requests. 0x0 – Neighbor not accepting joins 0x1 – Neighbor is accepting joins 0x2 – Unknown
Reserved	6	Set to 0.
Depth	8	The tree depth of the neighbor device. A value of 0x00 indicates the device is the ZigBee coordinator for the network.
LQI	8	The estimated link quality of data transmissions from this neighboring device.

Management Rtg (Routing Table) Request

Cluster ID: 0x0032
Description: Unicast transmission used to cause a remote device to return the contents of its routing table.

Field Name	Size (bytes)	Description
Start Index	1	Start index in the routing table to return routing table entries. The response cannot include more than a handful of entries. Multiple routing table requests may be required to read the entire routing table.

Management Rtg (Routing Table) Response

Cluster ID: 0x8032
Description: Indicates the routing table contents of the device.

Field Name	Size (bytes)	Description
Status	1	
Routing Table Entries	1	The total number of routing table entries
Start Index	1	The starting point in the routing table
Routing Table List Count	1	The number of routing table entries in this response
Routing Table List	Variable	A list of routing table entries.

Routing Table Entry

Name	Size (bits)	Description
Destination Address	16	The 16-bit address of the destination device
Status	3	Status of the route: 0x0 – Active 0x1 – Discovery Underway 0x2 – Discovery Failed 0x3 – Inactive 0x4 – Validation Underway
Memory Constrained Flag	1	Indicates if the device is a low-memory concentrator
Many-to-One Flag	1	Flag indicating the destination is a concentrator (ssued a many-to-one request).
Route Record Required	1	Flag indicating if a route record message should be sent to the device prior to the next data transmission.
Reserved	2	
Next-hop Address	16	16-bit address of the next hop.

Management Leave Request

Cluster ID: 0x0034
Description: Transmission used to cause a remote device to leave the network.

Field Name	Size (bytes)	Description
Device Address	8	Address of the device the command is addressed to. See section 3.2.2.1.6 for details.
Options	1	Bitfield: 0x01 – Rejoin (If set, the device is asked to rejoin the network.) 0x02 – Remove Children (If set, the device should remove its children)

Management Leave Response

Cluster ID: 0x8034
Description: Indicates the status of a leave request.

Field Name	Size (bytes)	Description
Status	1	Indicates the status of a leave request.

Management Permit Join Request

Cluster ID: 0x0036
Description: Unicast or broadcast transmission used to cause a remote device or devices to enable joining for a time.

Field Name	Size (bytes)	Description
Permit Duration	1	Specifies the time that joining should be enabled (in seconds). If set to 0xFF, joining is enabled permanently.
Trust Center Significance	1	If set to 1 and the remote is a trust center, the command affects the trust center authentication policy. Otherwise, it has no effect.

Management Permit Joining Response

Cluster ID: 0x8036
Description: Indicates the status of a permit joining request.

Field Name	Size (bytes)	Description
Status	1	Indicates the status of a permit joining request.

Management Network Update Request

Cluster ID: 0x0038

Description: Unicast transmission used to cause a remote device to do one of several things:

- Update the channel mask and network manager address (if scan duration = 0xFF)
- Change the network operating channel (if scan duration = 0xFE)
- Request to scan channels and report the results (if scan duration < 6)

Field Name	Size (bytes)	Description
Scan Channels	4	Bitmap indicating the channel mask that should be scanned. Examples (big endian byte order): Channel 0x0B = 0x800 Channel 0x10 = 0x10000 Channel 0x1A = 0x4000000 All Channels (0x0B – 0x1A) = 0x07FFF800
Scan Duration	1	Set as described above to invoke the desired command.
Scan Count	0/1	If scan duration < 6, specifies the number of energy scans to conduct and report. This can result in multiple responses being sent.
Network Update ID	0/1	Set by the network channel manager
Network Manager Address	0/2	If scan duration = 0xFF, indicates the network address of the network manager (who has network manager bit set in its node descriptor)

Management Network Update Notify

Cluster ID: 0x8038

Description: Indicates the RF conditions near the device.

Field Name	Size (bytes)	Description
Status	1	Status of the Management Network Update notify command.
Scanned Channels	4	List of channels scanned by the request.
Total Transmissions	2	Count of the total transmissions reported by the device.
Transmission Failures	2	Sum of the transmission failures reported by the device
Scanned Channels List Count	1	The number of records contained in the energy values list.
Energy Values	Variable	The result of an energy measurement made on the scanned channels, one byte per energy measurement. 0xFF – Too much interference on the channel.

API Examples

Example 1 – Send a broadcast transmission to discover the 16-bit address of a device with a 64-bit address of 0x0013A200 44332211 using the Network Address Request ZDO (cluster ID = 0x0000). Format the command to also discover the 16-bit addresses of its children (if any).

To send this command, use the following fields:
0x11 – API ID (transmit request)
0x00 – frame ID (set to 0 to disable transmit status)
0x00000000 0000FFFF – 64-bit address for a broadcast transmission
0xFFFE – 16-bit address for a broadcast transmission
0x00 – source endpoint (ZDO endpoint)
0x00 – destination endpoint (ZDO endpoint)
0x0000 - Cluster ID (Network Address Request)
0x0000 – Profile ID (ZigBee Device Profile ID)
0x00 – Broadcast radius
0x00 – Transmit options

In the ZDO payload, first set a transaction sequence number, and then follow with the required payload for the network address request ZDO. The following bytes will be inserted into the data payload portion of the API frame:
0x01 – Transaction sequence number (arbitrarily chosen)
0x44332211 00A21300 – IEEE (64-bit) address of target device (little endian byte order)
0x01 – Request type (extended device request)
0x00 – Start Index

Next, calculate the length and checksum bytes to construct the final API frame.
Length = count all bytes after the length bytes, excluding the checksum
Checksum = (0xFF – SUM(all bytes after length))

Final API Frame:
7E 00 1F 11 00 00000000 0000FFFF FFFE 00 00 0000 0000 00 00 01 44332211 00A21300 01 00 92

Example 2 - Send a broadcast transmission to discover the 64-bit address of a device with a 16-bit address of 0x3344 using the IEEE Address Request ZDO (cluster ID = 0x0001).

To send this command, use the following fields:
0x11 – API ID (transmit request)
0x00 – frame ID (set to 0 to disable transmit status)
0x00000000 0000FFFF – 64-bit address for a broadcast transmission
0xFFFE – 16-bit address for a broadcast transmission
0x00 – source endpoint (ZDO endpoint)
0x00 – destination endpoint (ZDO endpoint)
0x0001 - Cluster ID (IEEE Address Request)
0x0000 – Profile ID (ZigBee Device Profile ID)
0x00 – Broadcast radius
0x00 – Transmit options

In the ZDO payload, first set a transaction sequence number, and then follow with the required payload for the IEEE address request ZDO. The following bytes will be inserted into the data payload portion of the API frame:
0x02 – Transaction sequence number (arbitrarily chosen)
0x4433 – Network (16-bit) address of target device (little endian byte order)
0x00 – Request type (single device request)
0x00 – Start Index

Next, calculate the length and checksum bytes to construct the final API frame.
Length = count all bytes after the length bytes, excluding the checksum
Checksum = (0xFF – SUM(all bytes after length))

Final API Frame:
7E 00 19 11 00 00000000 0000FFFF FFFE 00 00 0001 0000 00 00 02 4433 00 00 79

Example 3 – Send a broadcast transmission to discover the node descriptor of a device with a 16-bit address of 0x3344.

To send this command, use the following fields:
0x11 – API ID (transmit request)
0x00 – frame ID (set to 0 to disable transmit status)
0x00000000 0000FFFF – 64-bit address for a broadcast transmission
0xFFFE – 16-bit address for a broadcast transmission
0x00 – source endpoint (ZDO endpoint)
0x00 – destination endpoint (ZDO endpoint)
0x0002 - Cluster ID (Node Descriptor Request)
0x0000 – Profile ID (ZigBee Device Profile ID)
0x00 – Broadcast radius
0x00 – Transmit options

In the ZDO payload, first set a transaction sequence number, and then follow with the required payload for the node descriptor request ZDO. The following bytes will be inserted into the data payload portion of the API frame:
0x03 – Transaction sequence number (arbitrarily chosen)
0x4433 – Network (16-bit) address of target device (little endian byte order)

Next, calculate the length and checksum bytes to construct the final API frame.
Length = count all bytes after the length bytes, excluding the checksum
Checksum = (0xFF – SUM(all bytes after length))

Final API Frame:
7E 00 17 11 00 00000000 0000FFFF FFFE 00 00 0002 0000 00 00 03 4433 77

Example 4 – Send a unicast data transmission to read the neighbor table of a router with 64-bit address 0x0013A200 40401234 using the LQI Request ZDO (cluster ID = 0x0031).

To send this command, use the following fields:
0x11 – API ID (transmit request)
0x00 – frame ID (set to 0 to disable transmit status)
0x0013A200 40401234 – 64-bit address of the destination
0xFFFE – 16-bit address (0xFFFE if unknown)
0x00 – source endpoint (ZDO endpoint)
0x00 – destination endpoint (ZDO endpoint)
0x0031 - Cluster ID (LQI Request)
0x0000 – Profile ID (ZigBee Device Profile ID)
0x00 – Broadcast radius
0x00 – Transmit options

In the ZDO payload, first set a transaction sequence number, and then follow with the required payload for the LQI request ZDO. The following bytes will be inserted into the data payload portion of the API frame:

0x76 – Transaction sequence number (arbitrarily chosen)
0x00 – Start index

Next, calculate the length and checksum bytes to construct the final API frame.
Length = count all bytes after the length bytes, excluding the checksum
Checksum = (0xFF – SUM(all bytes after length))

Final API Frame:
7E 0016 11 00 0013A200 40401234 FFFE 00 00 0031 0000 00 00 76 00 CF

Example 5 – Send a unicast data transmission to have a remote router perform an energy scan on all channels using a ZDO Management Network Update Request (cluster ID = 0x0038). In this example, the 64-bit address of the router is 0x0013A200 40522BAA.

To send this command, use the following fields:
0x11 – API ID (transmit request)
0x00 – frame ID (set to 0 to disable transmit status)
0x0013A200 40522BAA – 64-bit address of the destination
0xFFFE – 16-bit address (0xFFFE if unknown)
0x00 – source endpoint (ZDO endpoint)
0x00 – destination endpoint (ZDO endpoint)
0x0038 - Cluster ID (Management Network Update Request)
0x0000 – Profile ID (ZigBee Device Profile ID)
0x00 – Broadcast radius
0x00 – Transmit options

In the ZDO payload, first set a transaction sequence number, and then follow with the required payload for the network update request ZDO. The following bytes will be inserted into the data payload portion of the API frame:

0x01 – Transaction sequence number (arbitrarily chosen)
0x00F8FF07 – Scan channels (all 16 channels, little endian byte order)
0x03 – Scan duration
0x02 – Scan count (perform 2 energy scans)
The Network Update ID & Network Manager Address fields are not required for this operation.

Next, calculate the length and checksum bytes to construct the final API frame.
Length = count all bytes after the length bytes, excluding the checksum
Checksum = (0xFF – SUM(all bytes after length))

Final API Frame:
7E 001B 11 00 0013A200 40522BAA FFFE 00 00 0038 0000 00 00 01 00F8FF07 03 02 99

Example 6 – Parse a Management Network Update Notify response received in response to example 5 to extract energy data on the scan channels mask.

Recall that the AO command must be set on an API device to receive ZDO responses.

Suppose the following API frame is received.

API Frame
7E 002D 91 0013A200 40522BAA 06FC 00 00 8038 0000 01 01 00 00F8FF07 1D00 0000 10 54 5E 69 5B 4B 48 44 48 55 55 57 46 51 41 44 4B 6E

Decoded API Frame
0x7E – Start delimiter
0x002D – Length
0x91 – Explicit receive API frame
0x0013A200 40522BAA – 64-bit address of the remote (who performed the energy scan)
0x06FC – 16-bit address of the remote
0x00 – Source endpoint (ZDO endpoint)
0x00 – Destination endpoint (ZDO endpoint)
0x8038 – Cluster ID (Management network update notify)
0x0000 – Profile ID (ZigBee Device Profile ID)
0x01 – Rx options (packet was acknowledged)
0x010000F8FF071D00000010545E… 41444B – Data payload
0x6E – Checksum

The data payload bytes can be interpreted as a ZDO management network update notify packet. Recall that the first byte in the data payload is a transaction sequence number that matches the sequence number of the request.

Data Payload Bytes (Management Network Update Notify)
0x01 – Transaction sequence number used in request
0x00 – Status (SUCCESS)
0x00F8FF07 – Channel mask (16 channels enabled, represented in little endian byte order)
0x1D00 – Total transmissions (0x001D = 29)
0x0000 – Transmission failures
0x10 – Scanned channel count
0x54 – 1st channel in channel mask energy level (channel 0x0B)
0x5E – 2nd channel in channel mask energy level (channel 0x0C)
…
0x4B – last channel in channel mask energy level (channel 0x1A)

In the Ember stack, to convert energy levels to dBm units, do the following
Energy(dBm) = (energy level – 154)

For example, the energy level reported on channel 0x0B (0x54) is (84 – 154) = -70dBm. As a general rule, lower raw energy value readings indicate lower RF energy on the channel.

The energy level representation and conversion equations might be different for other (non-Ember) platforms.

Example 7 – Parse the network address response (extended response) received from a device with a 64-bit address of 0x0013A200 404A2257. Use the data in the response to determine the 16-bit address of the device and to determine the addresses of its end device children.

Recall that the AO command must be set on an API device to receive ZDO responses.

Suppose the following Explicit Rx API frame is received.

API Frame
7E 0022 91 FFFFFFFF FFFFFFFF 0848 00 00 8000 0000 01 01 00 57 22 4A 40 00 A2 13 00 48 08 01 00 AA AC 45

Decoded API Frame
0x7E – Start delimiter
0x0022 – Length
0x91 – Explicit receive API frame
0xFFFFFFFF FFFFFFFF – 64-bit source address (all 0xFFs if network layer did not include a source 64-bit address)
0x0848 – 16-bit source address
0x00 – Source endpoint (ZDO endpoint)
0x00 – Destination endpoint (ZDO endpoint)
0x8000 – Cluster ID (Network Address Response)
0x0000 – Profile ID (ZigBee Device Profile ID)
0x01 – Receive options (packet was acknowledged)
0x010057224A4000A2130048080100AAAC – Data payload
0x45 – Checksum (0xFF – SUM(all bytes after length))

The data payload bytes can be interpreted into a network address response. Recall that the first byte in the data payload is a transaction sequence number that matches the sequence number of the request.

Data Payload Bytes (Network Address Response)
0x01 – Transaction Sequence Number
0x00 – Status (SUCCESS)
0x57224A40 00A21300 – 64-bit address of the responder (in little endian byte order)
0x4808 – 16-bit address of the responder (in little endian byte order).
0x01 – Number of associated devices (end device children)
0x00 – Start index (starting index in the child table list)
0xAAAC – 16-bit address of the child (in little endian byte order)

From the ZDO Network Address Response, we have identified the following:

- The remote with 64-bit address 0x0013A200 404A2257 has a 16-bit address of 0x0848.
- The remote has one end device child.
- The end device child of the remote has a 16-bit address of 0xACAA.