Z/IP Gateway SDK 7.16.00
June 10, 2021

The Z/IP Gateway emulates the behavior of IP enabled Z-Wave devices so that IP applications may interact with Z-Wave devices via normal IP routing principles. The Z/IP Gateway decodes Z/IP Packet headers and forwards extracted Z-Wave commands to the node identified by the given IPv6 or Ipv4 address.

These release notes cover Z/IP Gateway SDK version(s):

7.16.00

This release is a pre-certification Z-Wave LR release, all specifications needed for LR are available as 2020C contribution, through the Z-Wave Alliance AWG

Z-Wave

NEW FEATURES

- Various fixes
- Z-Wave Long Range support
- Pre-certified for Z-Wave Long Range

Compatibility and Use Notices

If you are new to the Z-Wave Gateway SDK, see Using This Release.

The audience of this document is Z-Wave Partners and Silicon Labs customers interested in evaluating the Z/IP Framework. The reader must be familiar with the following:

- Basic IP terminology, such as routing, ping, UDP, subnet, etc.
- Basic Z-Wave network creation and maintenance

While not used consequently throughout the document, the guidelines outlined in IETF RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels” are followed in many sections. Essentially, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

Contents

1 Improvements

- This release is a pre-certification Z-Wave Release. The 7.16.1 release will be Z-Wave certified.
- Pre-certified for Z-Wave Long Range. Pre-certified means that the final version of the Long Range certification tests were not available at the time of this release. The LR certification will be performed based on the 2020C specifications test suites and is anticipated to begin ultimo July, 2021. This release is a pre-certification Z-Wave LR release, all specifications needed for LR are available as 2020C contribution, through the Z-Wave Alliance AWG.
- Various fixes. See section 2 for details.

2 Fixed Issues

Fixed in release 7.16.00

ID#	Description
ZGW-3169	Conversion from EEPROM 7.14.1 to 7.15.2 fails due to virtual node list is mistakenly read as 2 byte node list.
ZGW-3157	Gateway wrongly determines whether supporting Command Schedule Get and Report due to mismatch between Command Analyzer and ZWave_custom_cmd_class.xml
ZGW-3141	Correct the misleading assert prints in Resource Directory
ZGW-3137	Fix S0 sessions leak
ZGW-3140	Make Network Management Proxy commands backward compatible

3 Known Issues in the Current Release

Issues in bold were added since the previous release.

ID	Description	Workaround
ZGW-1035	Z/IP Gateway will queue and delay incoming DTLS Client Hello requests while attempting to deliver a frame to a FliRS device. Delay may be multiple seconds if the FliRS device is not working.	
ZGW-633	In some situations, NACK Waiting is sent late. This occurs if the internal queues are locked or are long. The queues are locked when exercising the mailbox or performing network management operations. A Z/IP client might time out on a frame delivery even though the frame is in fact going to be delivered. ACK/NACK will be received on delivery.	Extend timers in the client or if possible be aware that the queues are locked due to network management operations.
ZGW-2707	The Z/IP Gateway does not reply multichannel encapsulated S2 secure command supported Get command.	Z/IP Client should not advertise multichannel as a supported command class.
ZGW-2948	LibZWaveIP transmits data over Ipv4 while connecting over Ipv6	
ZGW-3025	Network keys are sent over UART in plaintext (see 5.3.1)	Secure GW product against physical tampering
ZGW-3006	Dynamic TX Power is not forwarded via IMA. Z/IP Clients are not informed of the dynamic TX power used to send a particular frame.	
ZGW-3104	The Z/IP Gateway cannot supports network sizes exceeding 750 nodes. The Long Range specification allows even larger networks.	
ZGW-3153	Migration to Long Range (LR) Z/IP Gateway from a LR gateway not based on Z/IP Gatway does not work. The migrated LR Z/IP Gateway will not be operational.	

4 Removed and Deprecated Items

4.1 Firmware Update targets

All firmware targets except target 0 are deprecated in Firmware Update Command Class. It is only possible to update a firmware target 0 (i.e. the Z-Wave chip Flash memory). The other firmware targets have been deprecated because it is unsafe to update them individually. It is recommended to use the backup/restore functionality of the ZGW instead. It will safely update the information previously exposed through the firmware targets.

4.2 Back-off during polling

The Z/IP Gateway no longer performs back off when Z/IP clients are polling Z-Wave devices. This must be handled by the clients. The change improves scalability of large networks. As mandated by *SDS11846: Z-Wave Plus Role Type Specification section 3.7*, a Z-Wave controller must rate-limit polling of devices in the network. Previously, the Z/IP Gateway would automatically apply rate limiting to requests from Z/IP clients. This functionality has now been removed in order to improve large network scalability. As a consequence, Z/IP clients must now adhere to the requirements in *SDS11846: Z-Wave Plus Role Type Specification*.

5 Using This Release

The Z/IP Gateway Software Developers Kit contains the following components:

- Debian packages:
  - Z/IP Gateway 7.16.00, for Raspberry Pi 3B+
  - Z/IP Gateway 7.16.00, for Linux i386
- Source code:
  - Z/IP Gateway 7.16.00
  - libzwaveip 7.16.00

Documentation:

- INS12503, Z/IP Gateway Porting Process
- SDS12938, Z/IP LAN Security
- SDS12089, Z/IP Gateway Bootstrapping
- SDS11756, Z/IP DNS Discovery support (DNS-SD, mDNS)
- SDS11633, Z/IP Resource Directory (RD, DNS-SD, mDNS)
- SDS11445, IP Architecture Framework for Z-Wave (Z/IP)
- SDS13944, Node Provisioning Information Type Registry (QR code, Z/IP Gateway, SmartStart)
- Z/IP Security 2 in Z/IP Gateway
- Z/IP Gateway Source Code Documentation
- Z/IP Gateway User Guide (Z-Wave & IP Basics, Compilation, Installation, Troubleshooting, Sample Code)
- libzwaveip documentation in the file libzwaveip-7.16.00.release-docs.zip

Additionally, the following documentation can be found in https://www.silabs.com/products/wireless/mesh-networking/z-wave/specification:

- Z-Wave Command Class specifications

5.1 Key Features of Z/IP Gateway SDK

The Z/IP Gateway SDK 7.16.00 provides the following features:

- Transparent gateway: IP applications reach Z-Wave nodes via IP addresses. Z/IP Packets originating from LAN IP applications are terminated and forwarded as Z-Wave commands to Z-Wave Nodes. See *the Z/IP Command Class Specification*.
    - Supports only Z-Wave Single cast
    - Z-Wave nodes are identified by IPv6 and IPv4 host addresses
    - IPv6 and IPv4 Ping (ICMP Echo) support
    - Z/IP-ND: IPv6 and IPv4 address resolution for Z/IP Applications
- SmartStart Auto-inclusion; Supports only Add Node
- SIS support
- Security 0 and Security 2 support
- Remote Access and Configuration
- Forwarding of unsolicited messages to up to two IP destinations
- Resource & Service Discovery (mDNS) (see *SDS11756: Silicon Labs, Z/IP DNS Discovery support (DNS-SD, mDNS)*)
- IP Association Proxy
- Mail Box Service – Support for Non-Listening nodes
- Z/IP LAN Security using DTLS
- Installation and Maintenance framework
- NVM Backup
- Firmware Update of Z-Wave module attached to the Z/IP Gateway
- Historical and current transmission statistics
- Wi-Fi support
- Migration to Z/IP Gateway 7.11.x from non-Z/IP Gateways (See section 5.1.5).
- Back-up/Recover (See section 5.1.6)
- Z-Wave Long Range support

The Z/IP Gateway implements support for two sets of command classes, one set for the IP / LAN side and one set for the Z-Wave / PAN side.

5.1.1 LAN-Side Features

The command classes listed in Table 1 is supported on the LAN side of the Z/IP Gateway.

Table 1, Supported command classes on LAN side

Command Classes	Version
Application Status	1
CRC16	1
Firmware Update	5
Inclusion Controller	1
Security 2	1
Security	1
Supervision	1
Time	1
Transport Service	2
Z-Wave Plus Info	2
Indicator	3
Manufacturer Specific	2
Power Level	1
Version	3
Network Management Basic	2
Network Management Inclusion[1]	4
Network Management Proxy	4
Network Management Installation Maintenance	4
Node Provisioning	1
Z/IP	5
Z/IP Gateway	1
Z/IP Naming	1
Z/IP Portal	1
Z/IP ND	2
Mailbox	2

Note that the Network Management Inclusion command class will be removed if the gateway is a Secondary Controller. In addition, the Node Provisioning command class is supported if the Z/IP Gateway is a SIS with Access Control security class.

The following command classes are added to the LAN-side NIF of the PAN nodes. The Z/IP clients may send these command classes to the PAN nodes. If it does, the Z/IP Gateway will intercept and handle them.

- IP Association
- Z/IP
- Z/IP Naming

5.1.1.1 IP Support for Z-Wave Nodes

The Z/IP Gateway performs an inspection of each IP Packet received to check if the receiving node is a classic Z-Wave node. In the case of a Z-Wave node, the Z/IP Gateway intercepts all IP packets and, if possible, emulates the requested service by using equivalent features of Z-Wave.

- The Z/IP Gateway emulates an IP Ping (ICMP/ICMPv6 Type 8: Echo Request). If a Ping request is received by the Z/IP Gateway for a Z-Wave node, the Z/IP Gateway uses the Z-Wave NOP command to emulate the ping and respond using ICMP Reply to the requesting address. See *SDS11445: Silicon Labs, IP Architecture Framework for Z-Wave (Z/IP)*.
- The Z/IP Gateway forwards the Z-Wave payload of any Z/IP Packet received for a classic Z-Wave node to the node. It also handles Z/IP ACK and performs same ACK check on Z-Wave if requested. See *SDS11445: Silicon Labs, IP Architecture Framework for Z-Wave (Z/IP)*.

5.1.1.2 Unsolicited Forwarding

The Z/IP Gateway provides a remote and local configuration option for forwarding unsolicited Z-Wave frames to an IP address. This allows a network administrator to create a message sink somewhere in an IP infrastructure. The Z/IP Gateway forwards all Z-Wave frames to the configured address unless the Z-Wave frame appears to be a response to some request which previously entered the Z-Wave network via the Z/IP Gateway.

The Z/IP Gateway supports forwarding of unsolicited messages to up to two unsolicited destinations. The first unsolicited destination can be configured remotely using Z/IP Gateway Command Class (*SDS13784: Z-Wave Network-Protocol Command Class Specification*), or it can be configured using the configuration file (i.e., zipgateway.cfg). The secondary unsolicited destination can only be configured using the configuration file. A detailed information of the configuration file can be found in the CONFIGURATION FILE section of the Doxygen documentation

5.1.1.3 Remote Access and Configuration

The Z/IP Gateway provides a means of Remote Access through a secure Transport Layer Security (TLS) v1.1 based Transmission Control Protocol (TCP)/IPv4 connection over port 44123 to a portal, with a Domain Name System (DNS) resolvable Uniform Resource Locator (URL), outside the home network, synchronized by an internal Network Time Protocol (NTP) client.

The Z/IP Gateway initiates this connection to the portal: attempting connection every 5 seconds on failure. On connection, the Z/IP Gateway sends a keep-alive every 5 seconds. On some platforms it may take a considerable amount of time to establish the secure tunnel, as it uses a 2-way handshake with RSA-1024 certificates with Secure Hash Algorithm (SHA)-1 digest. If the connection breaks down, the Z/IP Gateway MUST support session resumption within 24 hours in less than 10 seconds. After connection has been set up, Z/IP packets over this connection are encrypted with Advanced Encryption Standard (AES) 128.

The Remote Access capabilities of the Z/IP Gateway are described in detail in *SDS12089: Silicon Labs, Z/IP Gateway Bootstrapping (ZIP,IPv4, IPv6, Router, NAT, DHCP, tunnel, remote access)*. In addition to local configuration, it is possible to push Z/IP Gateway configuration remotely. It is possible to specify the following:

- Stand-alone or Portal – if the Z/IP Gateway should connect to a Portal through a Remote Access connection
- Setting the peer address of the Portal
- Lock / Unlock configuration
- Configuration of LAN and Z-Wave IPv6 and IPv4 prefixes and addresses

5.1.1.4 Wi-Fi Support

The Z/IP Gateway supports running in Wi-Fi client mode. This is achieved by relaying the packets coming through the wlan interface to the virtual Linux network interfaces using customized relay configuration. Detailed information of the configuration can be found in the wireless section of the Doxygen documentation.

5.1.1.5 Z/IP LAN Security

Z/IP LAN security provides a secure connection for clients connecting to the Z/IP Gateway. The Z/IP LAN Security framework provides a means of securing the communication paths between:

- Z/IP Clients
- Z/IP Clients and Z/IP Gateways
- Z/IP Gateways

Secure Z/IP UDP frames are ordinary Z/IP frames wrapped in a DTLS wrapper. DTLS is the datagram version of TLS. Z/IP LAN Security default UDP port number is 41230.

Z/IP LAN Security currently only supports the Pre-Shared-Key (PSK) Key Exchange Algorithm.

5.1.1.6 Z/IP Discovery

A Non-DTLS encapsulated Z/IP Node Info Cached Get command may be used to discover the IPv6 or IPv4 address of the Z/IP Gateway, by sending the request as Broadcast, requesting Node ID #0. Any Z/IP Gateway on the network replies with Z/IP Node Info Cached Report and their IP address contained.

5.1.1.7 Resource and Service Discovery (mDNS)

The mDNS service allows an IP application automatically to discover all Z-Wave nodes available on any Z/IP Gateway on the backbone. The application will receive information about all nodes added to the network as well as any changes that may be made.

The mDNS discovery service announces all nodes and node endpoints as individual mDNS resources (see IETF RFC 6763). As new nodes are added and removed from the Z-Wave network, the mDNS resource changes are dynamically multi-casted on the LAN backbone. The mDNS resource announcements contain detailed information about the underlying node/endpoint, such as its device type and supported command classes and IPv6 address(es).The detailed information can be found in *SDS11756: Silicon Labs, Z/IP DNS Discovery support (DNS-SD, mDNS)*.

The names of the mDNS resources may be statically generated.

5.1.1.8 Z/IP Neighbor Discovery: IPv6 and IPv4 Address Resolution for Z/IP Applications

To allow Z/IP applications to communicate with Z-Wave devices identified by Node IDs, the translation service is provided by the Z/IP Gateway to translate the Node ID into the appropriate IPv6 and IPv4 address.

The Z/IP Cleint application is only capable of communication with the Z-Wave devices using IPv6 or IPv4 addresses. While the Z/IP Client application is communicating with the Z-Wave devices, Node IDs of the devices may reach a Z/IP Client application, which, for example, uses the Network Management Command Classes described in *SDS13784: Z-Wave Network-Protocol Command Class Specification*. In this case, the Node ID can be translated into an IPv6 or IPv4 address using the Z/IP ND Command Class presented in *SDS13784: Z-Wave Network-Protocol Command Class Specification*.

5.1.1.9 IP Association Proxy

The IP Association Proxy extends the Z-Wave addressing domain by allowing Z-Wave devices to communicate with a Z/IP Client. Z-Wave IP Associations are created between two Z/IP resources, each identified by an IP address and an endpoint ID. The main benefit of using IP Associations is to associate a PAN node with a Z-Wave node in a different PAN, or even a generic Z/IP Client controlling anything. But it can also be used as a convenient way for setting up associations between two nodes in the PAN. Associations between endpoints on multichannel devices in the PAN are handled in the following ways:

- Association from one Z-Wave root node to another: Send Association Set Command to the association source in a Z-Wave frame.
- Association from a Multi Channel End Point to another Multi Channel End Point: Send a Multi Channel Association Set Command to the association source encapsulated in a Multi Channel frame.
- Association from a Multi Channel End Point to a root node: Send an Association Set Command to the association source encapsulated in a Multi Channel frame.
- Association from a node not supporting Multi Channel CC to a Multi Channel End Point: Send an Association Set Command to the association source encapsulated in a Z-Wave frame. The association targets a virtual node in the Z/IP Gateway. Create a companion association from the virtual node to the Multi Channel End Point.

Note: IP Association Proxy uses the Node IDs of the Z-Wave PAN, so any association against an IP address will allocate and use a Z-Wave Node ID, leaving fewer Node IDs for physical devices.

5.1.1.10 Mailbox Command Class – Support for Not Always Listening Nodes

The Mailbox provides support for any Z/IP Client to communicate with nodes that support Wake Up Command Class without them having to implement or understand the Wake Up Command class. The sending Z/IP Client needs no knowledge about the sleeping state of the receiving node. The Z/IP Client receives a “Delayed” packet (Z/IP NAK Waiting) each minute, indicating that ACK is expected at a later point and that the Z/IP Client should not attempt retransmission.

The queue size of the mailbox is currently limited to 2000 entries.

The Z/IP Gateway supports the Mailbox Command Class (*SDS13784: Z-Wave Network-Protocol Command Class Specification*), which allows a lightweight Z/IP Gateway to offload the mailbox functionality to a more powerful mailbox service such as a portal.

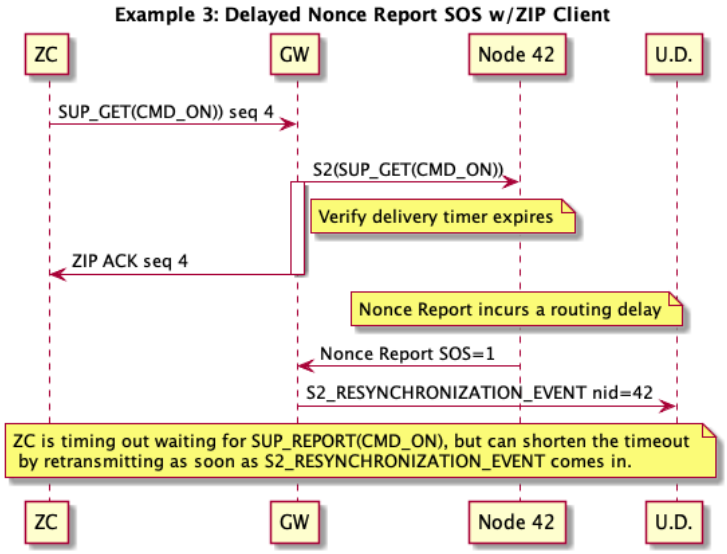
5.1.1.11 S2 Nonce Resynchronization Notification

In order to exchange Security2 encrypted messages, two peer nodes must maintain nonce synchronization. Re-synchronization causes message delays and loss, and Security2 is designed to keep resynchronizations few and far apart. When a loss-of-synchronization is detected, the Security2 layer will attempt one retransmission of the frame. If that results in another loss-of-synchronization the transmission is considered failed and upper layers are notified of the transmission failure.

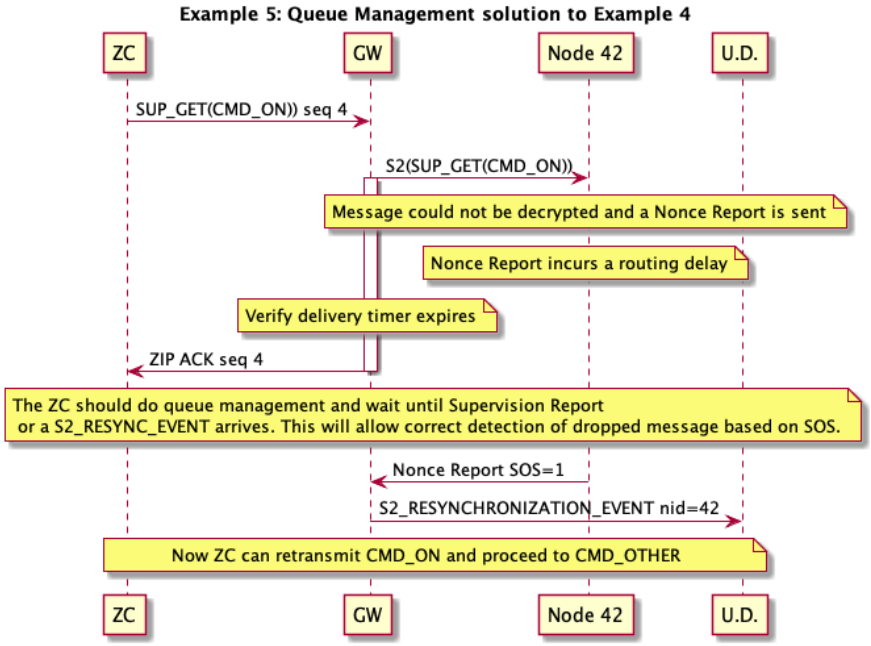
In a very specific edge case, the Z/IP Client application can recover faster from a synchronization error by knowing when a peer node sends a Nonce Report with Singlecast Out Of Sync to the Z/IP Gateway. This feature makes that information available to the application in the form of the new command S2_RESYNCHRONIZATION_EVENT in the Network Management Installation and Maintenance Command Class. The Z/IP Packet is sent to the Unsolicited Destination (U.D.).

It is entirely optional to use the S2_RESYNCHRONIZATION_EVENT, and it is safe for the Z/IP client to ignore it.

The S2_RESYNCHRONIZATION_EVENT can be used to detect a dropped message in the following scenario (ZC = ZIP Client, U.D.=unsolicited destination):



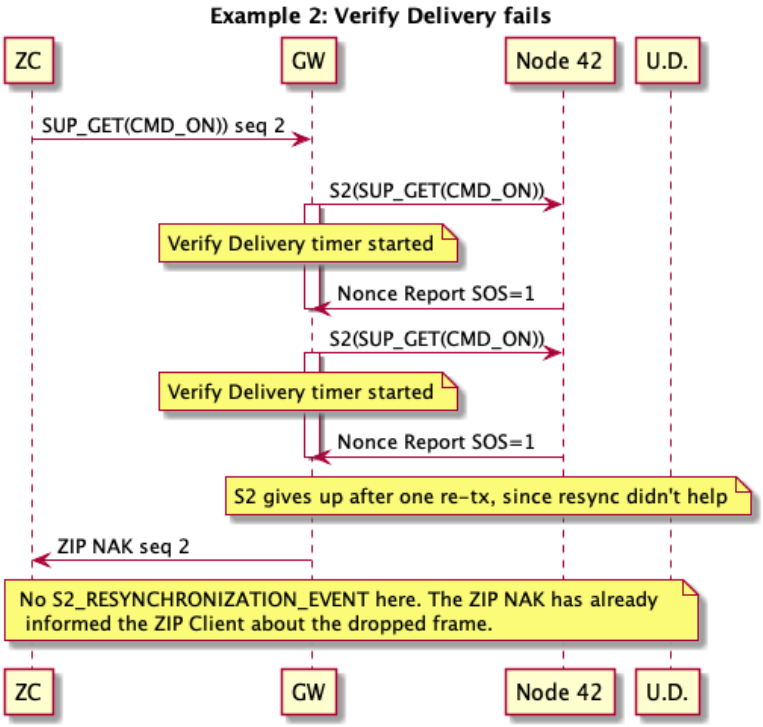
The feature relies on the Application Layer never “overlapping” transmissions. This diagram illustrates how to do this:



By observing the queuing discipline shown in Example 5, the Application can reliable initiate faster retransmissions when a Nonce Report SOS comes in after the Verify Delivery timeout. Faster in this case, means faster than the timeout waiting for the Supervision Report.

The queuing discipline is needed because the on-air format of the S2 Nonce Report does not contain a linkable identifier to the encrypted message. This in turn makes it impossible for the Nonce Notification feature to identify which individual transmissions was delayed or lost due.

Supervision Encapsulation is the usual way to obtain this guarantee of delivery. Waiting for the Supervision Report is a necessary part of the queue management, but the wait can be shortened in case a Nonce Report SOS is received after the Verify Delivery timeout and before the Supervision Report timeout.



S2_RESYNCHRONIZATION events will also be emitted if the GW is doing Verify Delivery to one node, while receiving a Nonce Report with SOS=1 from another node.

Feature Specification

This command is used to notify the Z/IP Client application the occurrence of S2 Nonce Resynchronization event. This will allow the client application to recover faster from a synchronization error that may cause message delay and loss.

The Z/IP Gateway MUST send this command to the Unsolicited destinations 1 and 2 when the Gateway received Nonce Report with SOS flag equal to 1 while Verify Delivery to the sending node is inactive.

The Z/IP Gateway MUST NOT send this command in the following cases:

- The Z/IP Gateway received the Nonce Report with SOS flag equals to 1 and Verify Delivery to sending node is active.
- The Z/IP Gateway received the Nonce Report with SOS flag equals to 1 and the ZIP NAK is sent to the Z/IP Client application.
- The Z/IP Gateway received the Nonce Report with SOS flag equals to 1 when the sending node cannot decrypt the frame sent from the Gateway.
- The Z/IP Gateway received Nonce Get (i.e., node coming out of power reset)

The S2_RESYNCHRONIZATION_EVENT will be delivered as quickly as possible (with minimum delay, but best effort) but may experience queuing delays in the Gateway (e.g. until other unrelated transmissions have been Z/IP ACK'ed). The packet is sent without ZIP Acknowledgments or retransmissions. The timing of the S2_RESYNCHRONIZATION_EVENT cannot be linked to the transmission that triggered it unless the Z/IP client application observes the queuing discipline described above to avoid overlapped transmissions.

The Z/IP Gateway will filter out S2 frames with duplicate sequence numbers before signaling an S2_RESYNCHRONIZATION_EVENT.

The support for this feature can be detected by the Z/IP Clients by the Z/IP Gateway advertising support for version 3 of Network Management Installation and Maintenance Command Class.

The format of the S2_RESYNCHRONIZATION_EVENT ZIP Packet is:

7	6	5	4	3	2	1	0
Command Class = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
Command = S2_RESYNCHRONIZATION_EVENT							
NodeID							
Reason (1 byte)							
Extended NodeID (MSB)							
Extended NodeID (LSB)							

Command (1 byte)

Value	Explanation
0x00 .. 0x08	Defined in SDS13784 Z-Wave Network-Protocol Command Class Specification
0x09	S2_RESYNCHRONIZATION_EVENT

NodeID (1 byte)

The NodeID field contains the NodeID of the peer node triggering a nonce resynchronization.

This field MUST be set to 0xFF if the NodeID triggering a nonce resynchronization is greater than 255.

Reason (1 byte)

The reason field contains the detailed reason for the Resynchronization event. This field MUST encoded as described in **Error! Reference source not found.**. This field MUST use signed encoding.

The following values are defined

Value	Explanation
0	SOS_EVENT_REASON_UNANSWERED A Nonce Report with SOS=1 was received at an unexpected time and no response was sent. Application may use this information to abort Supervision Report timeout if the remote nodeid matches. The Nonce Report was unanswered because the retransmission was performed while the S2 layer was idle or transmitting to another nodeID. In this case, a frame to NodeID was most likely lost. If the ZIP Client had only only one frame outstanding with NodeID, it can safely be assumed that the frame was lost. Note: Supervision Encapsulation should be used to acknowledge outstanding frames.
1-255	Reserved

Extended NodeID (2 bytes)

This field is used to advertise the NodeID of the peer node triggering a nonce resynchronization.

This field MUST be set to the actual NodeID that was triggered a Nonce resynchronization.

How To Use

This event is informational. The Z/IP client can safely ignore these events. The Z/IP client may also choose to optimize frame transmission in certain edge cases based on these events. See Intended Use section above.

To use most effectively, the Application (Z/IP Client) should maintain queuing discipline as illustrated in the Example 5. This means that the Z/IP client should use Supervision Encapsulation for all Set commands and only have one outstanding frame to one node in the

network at any time. This affords the application delivery confirmation for all messages, but can also lead to long timeouts waiting for Supervision Reports.

When an S2_RESYNCHRONIZATION_EVENT with Reason = SOS_EVENT_REASON_UNANSWERED is received, the Application can abort waiting for a Supervision Report on the dropped frame and take appropriate action instead. Depending on the application, appropriate actions could include

- Retransmission of message (but watch out for infinite loops)
- Skipping of message
- Reporting of permanent node problems in case of repeated resynchronization events.

5.1.2 PAN-Side Features

The Z/IP Gateway acts as a SIS when the Gateway has started its own network or joined another network that does not have a controller which manages the SIS functionality. The Z/IP Gateway will not relinquish its role to another controller. By default, the SIS functionality is enabled by the Gateway, and a SerialAPI with SIS support must be used.

5.1.2.1 Supported Command Classes

The Z/IP Gateway advertises the command classes shown in Table 2 in pre-inclusion NIF while it is in Learn mode and is waiting to join another PAN side Z-Wave network.

Table 2, List of supported command class in pre-inclusion NIF

Command Classes	Version
Application Status	1
CRC16	1
Inclusion Controller	1
Security	1
Security 2	1
Supervision	1
Time	1
Transport Service	2
Z-Wave Plus Info	2
Multi Command	1
Indicator	3
Manufacturer Specific	2
Power Level	1
Version	3

After the gateway has joined a network, the command classes that are supported by the gateway depend on the gateway inclusion security class level. Table 3 presents the list of supported command classes, their version, and their required security class. The command classes that will be included in Security Commands Supported Report depend on granted security class. The securely added state is active when the GW has started its own network, is alone in the network, or has been added to another secure network.

Table 3: Supported Command Classes with their required Security Class

Command Classes	Version	Required Security Classes
Application Status	1	None
CRC16	1	None
Inclusion Controller	1	None
Security	1	None
Security 2	1	None
Supervision	1	None
Time	1	None
Transport Service	2	None
Z-Wave Plus Info	2	None
Multi Command	1	None
Indicator	3	Highest granted Security Class
Manufacturer Specific	2	Highest granted Security Class
Power Level	1	Highest granted Security Class
Version	3	Highest granted Security Class
Firmware Update	5	Highest granted Security Class
Network Management Basic	2	Highest granted Security Class
Network Management Inclusion[1]	4	Highest granted Security Class
Network Management Proxy	4	Highest granted Security Class
Network Management Installation Maintenance	4	Highest granted Security Class
Node Provisioning	1	Access Control

Note: Node Provisioning command class is only supported when the Gateway is SIS.

If the secure Z/IP Gateway inclusion is failed, the Z/IP Gateway only supports the command classes shown in Table 4.

Table 4, Supported command classes when secure inclusion of the Z/IP Gateway is failed

Command Classes	Version
Application Status	1
CRC16	1
Inclusion Controller	1
Security 2	1
Supervision	1
Time	1
Transport Service	2
Z-Wave Plus Info	2
Multi Command	1
Indicator	3
Manufacturer Specific	2
Power Level	1
Version	3

5.1.2.2 Command Class Controlled by Gateway

Table 5 shows the command classes controlled by the Z/IP Gateway in a Z-Wave network.

Table 5, Command classes controled by Z/IP Gateway

Command Classes	Version
CRC16	1
Inclusion Controller	1
Security	1
Security 2	1
Z-Wave Plus Info	2
Association	2
Manufacturer Specific	2
Multi Channel	4
Multi Channel Association	3
Transport Service	2
Version	3
Wake Up	2

5.1.2.3 Security Mechanisms

Security mechanisms are in place to protect the communication over a Z-Wave network. With respect to that, Security CC and Security 2 CC are introduced to secure communications in a Z-Wave Network. Detailed descriptions of the command classes can be found in *SDS13783: Z-Wave Transport-Encapsulation Command Class Specification*.The ZIP Gateway supports both command classes.

5.1.2.3.1 Security Command Class

The Z/IP Gateway communicates securely with Z-Wave nodes that support the Z-Wave Security Command Class. All security is terminated in the Z/IP Gateway and never leaves the Z-Wave network. If a LAN Z/IP Client wishes to communicate with a secure Z-Wave node, it needs to transmit the normal Z/IP Packet to the Z/IP Gateway using the Z/IP Lan Security (DTLS) encapsulation mechanisms.

5.1.2.3.2 Security 2 Command Class

The Z/IP Gateway also provides transparent and automatic support for Security 2. Security 2 provides, among others, the following key improvements over the first generation Z-Wave Security Command Class:

- Authenticated Elliptic Curve Diffie-Hellman key-exchange
- Single Frame security
- Secure Multicast (not yet supported by the Z/IP Gateway)

The Z/IP Gateway communicates using Security 2 to Z-Wave nodes that support Z-Wave Security 2 Command Class. All Security is terminated in the Z/IP Gateway and never leaves the Z-Wave network.

5.1.2.4 Transport Service

The Z/IP Gateway supports the Transport Service Command Class version 2 that accommodates the transfer of datagrams larger than the Z-Wave frame size. The command class provides the following features:

- Reliable Checksum
- Transport protocol style transmission, providing means for fragmentation of frames exceeding the PHY frame length, re-transmission of missing fragments and robust error handling

5.1.3 SmartStart

SmartStart inclusion uses Network-Wide Inclusion (NWI) mechanisms to include new nodes. The Z/IP Gateway maintains a Provisioning List that enables touch-free inclusion of any device added to the list.

SmartStart devices carry a QR code which contains meta data that allows a UI to present relevant information to the installer, such as device type, product ID, etc. The QR code also contains the Security 2 DSK, which is also used by SmartStart to determine if the device is in the provisioning list..

Z/IP Gateway provides the following:

- API for maintaining a Provisioning List of DSKs and Provisioning Strings of SmartStart and Security 2 devices that may be included to the network
    - Provisioning List may be used for Security 2and SmartStart inclusion.
- Responding to Smart Start inclusion requests based on their presence in the Provisioning List
- SmartStart devices are automatically removed from network if SmartStart / Security 2 bootstrapping does not complete successfully.
    - Devices will self-reset and request inclusion again.
- As long as there are entries in the Provisioning List that are pending inclusion, SmartStart mode will be enabled and Z/IP Gateway will be listening for inclusion requests.
- SmartState Mode is determined based on entries in the Provisioning List.

The Z/IP Gateway supports SmartStart inclusion of other nodes through the Node Provisioning Command Class and version 3 of Network Management Inclusion Command Class.

5.1.4 Installation and Maintenance Framework

The Installation and Maintenance Framework provides a method for gathering statistics and performing network maintenance. The following statistics and maintenance may be carried out through this framework:

- Last Transmission:
  - Transmission Time
  - Route Changes
  - Last Working Route
- All Transmissions / Route Information:
  - Packet Error Count
  - Transmission Counter
  - Neighbors
  - Last Working Route max transmit power reduction
  - Network Management - Priority Route Set
  - Network Management - Priority Route Get
  - Network Management - Priority Route Report

5.1.5 Migration from non-Z/IP Gateways to Z/IP Gateway

The Z/IP Gateway software bundle contains a set of tools, which can be used to migrate from an existing controller. To perform the migration two files must be provided:

- A bridge controller firmware file from the latest Z-Wave SDK, for the Z-Wave module installed.
- A JSON file describing network information, such as security keys and node information. This file must be kept secure since it contains important information about a Z-Wave network such as the security keys.

Additionally, the Z/IP Gateway must be installed and configured according to the manual.

A script is provided to support a simple migration process where the controller/gateway hardware and the Z-Wave module are re-used (see section "Migrating to Z/IP Gateway from Third-Party Gateways" in the gateway manual, provided as html documents with the Z/IP Gateway software bundle).The migration process supports the protocol SDKs listed in Table **6**.

Migration with controller/gateway hardware replacement is also possible, e.g., replacing a 6. xx controller with a 7.xx controller; however, this process is a little more involved. See section "Migrating to Z/IP Gateway from Third-Party Gateways" in the gateway manual, provided as html documents with the Z/IP Gateway software bundle.

When migrating an inclusion controller, the Non-Listening nodes cannot be probed, so the JSON must contain full information on those devices.

When migrating, there will be a downtime of ~60 seconds, due to flashing of the module firmware.

Note*:* Migration/import of the following items are currently not supported:

- Mailbox queued messages to sleeping node. If the Z/IP client disables the mailbox, the JSON file must contain complete information about sleeping nodes.
- IMA statistics.
- If a given Z-Wave node information is not correctly provided in the JSON file, the consecutive nodes will not be imported to the Z/IP Gateway network and the behavior is undefined.
- If a node has endpoints, the list of the endpoints must be provided in JSON file.

The SerialAPI SDK versions supported as migration targets are listed in Table 6.

5.1.6 Back-up and Recover the Z-Wave Network on the Z/IP Gateway devices

The Z/IP Gateway state can be backed up to a file in less than 30 seconds. The back-up file can be used to recover the Z-Wave network and the persistent gateway state on the same Z/IP Gateway device or on a new physical device with the same architecture. Recovering a back-up works with the same or newer versions of the gateway software and with the same or newer versions of the Z-Wave protocol and chip, including 500-series to 700-series conversion.

Recover supports the Z-Wave SDKs listed in Table 6.

Table 6,Supported SDK for Import and Backup/recover

Functionality	Gecko DSK Versions
700	7.13.01, 7.13.02, 7.13.03, 7.13.04, 7.13.05, 7.14.00, 7.14.01, 7.14.02, 7.15.01, 7.15.02, 7.15.03, 7.15.04 (Migration to Long Range is not supported due to ZGW-3153)
6.8x	6.81.01, 6.81.02, 6.81.03, 6.81.04, 6.81.05, 6.81.06, 6.82.01
6.6x	6.60.00, 6.61.00

Note: The back-up contains security data and must be kept secure. In addition, it is not recommended to perform backup/recovery of the gateway while performing firmware update, and configuring/managing the Z/IP Gateway using the Z/IP Gateway Command Class.

5.1.7 Persisting the S2 SPAN Table

The Z/IP GW persists the S2 SPAN synchronization with each node on shutdown.Without persistence, a Z/IP gateway would lose S2 synchronization and re-synchronization would be required on the next communication with each node following a restart.
The S2 SPAN table is automatically persisted prior to shutdown and unpersisted on startup. See the Z/IP Gateway User Guide for information on how to start up and shutdown the gateway. The Z/IP Gateway will automatically load the most recent persisted S2 SPAN data on start-up. The SPAN table is stored in the Z/IP Gateway database file along with Resource Directory information and other stored network data. It is recommended to limit the number of shutdowns and startups to avoid flash storage wear-out.

5.1.8 Long Range Support

The Z/IP Gateway now supports Z-Wave Long Range. As a prerequisite, the attached SerialAPI module must be using firmware 7.15.0 or later. To accommodate the 16-bit nodeIDs used in Z-Wave LR, a number of Z/IP Command Classes have been updated. These include ZIP_ND, Network Management Inclusion, Network Management IMA and others. Furthermore, a new value for the Bootstrapping Mode Information Type has been defined for use with the Node Provisioning Command class.
Z-Wave End-nodes built for the US RF region using SDK 7.15.0 or later can be included in either normal or Long Range mode. SmartStart entries using the Long Range value for the Bootstrapping Mode Information Type will include the matching node in Long Range mode instead of normal mode. These SmartStart entries can for example be created with the command-line sample app included with libzwaveip.

5.1.9 Mailbox Queueing of Network Management Commands (ZGW-2981)

The following network management commands will now be queued in the mailbox when sent to sleeping nodes:

- RETURN_ROUTE_ASSIGN
- RETURN_ROUTE_DELETE
- NODE_INFO_CACHED_GET
- NODE_INFORMATION_SEND
- NODE_NEIGHBOR_UPDATE_REQUEST

The frameflow is similar to other (non-network management) messages sent til sleeping nodes. The Z/IP Gateway will return Z/IP Nack-Waiting until the sleeping node wakes up and the message can be delivered. At that time a Z/IP Ack will be returned to the Z/IP Client. Messages are deliverd first-in-first-out, in the same order as sent by the Z/IP Clients.

5.2 Platform Requirements

- Hardware requirements:
  - ARM, validated on Raspberry Pi 3B+
  - MIPS (big-endian), validated on 8devices – Lima board. No reference platform is provided, developers must refer to their own toolchain to compile the Z/IP Gateway source code for MIPS platform
  - 32-bit architecture
  - 64-bit architecture only supported through 32-bit compatibility libraries
- Software requirements:
  - OpenSSL 1.1.X library
  - Debian Stretch for Raspberry Pi 3B+ platform
  - Ubuntu 18.04
- SerialAPI requirements:
  - SDK MUST use DevKit 6.x or newer SerialAPI Bridge running on a Z-Wave 500 chip or Z-Wave 700 chip
  - A minimum of 32K NVM MUST be available for the SerialAPI
  - While using Z-Wave 700 chip, the region frequency must be set through the configuration file (zipgateway.cfg)

5.3 Important Notes

- When the Z/IP Gateway operating as a secondary controller, it will not provide access to & from the Z-Wave PAN; it will, however, allow Network Management from the LAN to put it into Learn Mode to upgrade it to SIS. No other operations can be guaranteed to work.
- The Time Command Class expects the time and timezone to be correctly set locally on the Z/IP Gateway (e.g., using an NTP server) to function properly. The Time Command Class module relies on the time.h library and 32-bits platforms will be affected by the general Year 2038 problem on Unix-like operating systems.
- Static Controller SerialAPI binary is NOT usable with this version of Z/IP Gateway SDK.
- The Z/IP Gateway SDK does not support for Multicast or Broadcast features.
- The Z/IP Gateway SDK does not support for Smart Start Learn Mode.

If you are a first-time user, Z-Wave documentation is installed with the SDK. See INS14281: Z-Wave 700 Getting Started for Controller Devices for instructions.

5.3.1 UART Connection Security

The current implementation of the Z-Wave SerialAPI Controller (also known as NCP/Network Connected Processor) requires that the host application create and send the network keys to the controller over the un-encrypted UART interface. This is important to understand since,

1. It is not currently possible to authenticate the NCP meaning that the host has no way to detect if a malicious actor has tampered with the NCP.
2. It may be possible for an attacker with physical access to sniff the keys over the UART.

It is therefore recommended that tamper-resistant products designs incorporate additional measures to prevent and/or detect physical access to the NCP module as well as the host hardware platform."

5.4 Technical Support

You can contact Silicon Laboratories support at http://www.silabs.com/support.

6 Legal

6.1 Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications.

Application examples described herein are for illustrative purposes only.

Silicon Labs reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Labs shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

6.2 Trademark Information

Silicon Laboratories Inc.® , Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world’s most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISOmodem®, Micrium, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress®, Zentri, Z-Wave and others are trademarks or registered trademarks of Silicon Labs.

ARM, CORTEX, Cortex-M0+, Cortex-M3, Cortex-M33, Cortex-M4, TrustZone, Keil and Thumb are trademarks or registered trademarks of ARM Holdings.

Zigbee® and the Zigbee logo® are registered trademarks of the Zigbee Alliance.

Bluetooth® and the Bluetooth logo® are registered trademarks of Bluetooth SIG Inc.

All other products or brand names mentioned herein are trademarks of their respective holders.