



Software Release Note

Z/IP GW SDK 2.11.01

Version:	4
Description:	-
Written By:	JRM;BBR
Date:	2018-03-05
Reviewed By:	AES;JBU;MDUMBARE;TMORTENSEN;CRASMUSSEN;KMALMKJAER;NTJ
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2018-03-05	14:39:16	NTJ	Niels Thybo Johansen	

This document is the property of Silicon Labs. The data contained herein, in whole or in part, may not be duplicated, used or disclosed outside the recipient for any purpose. This restriction does not limit the recipient's right to use information contained in the data if it is obtained from another source without restriction.



REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20170301	JRM	ALL	Initial version
3	20170515	JRM	ALL	Updated for version 2.61 / SDK 2.11.01
4	20180305	BBR	All	Added Silicon Labs template

Table of Contents

1	ABBREVIATIONS	1
2	INTRODUCTION	2
2.1	Purpose	2
2.2	Audience and prerequisites	2
3	Z/IP SDK DESCRIPTION	3
4	Z/IP GATEWAY SDK 2.11.01 FEATURES	4
4.1	Transparent Gateway	6
4.1.1	IP Support for Z-Wave Nodes	6
4.2	SIS support.....	6
4.3	Unsolicited Forwarding	6
4.4	WiFi Support.....	7
4.5	Security Mechanisms	7
4.5.1	Security Command Class.....	7
4.5.2	Security 2 Command Class.....	7
4.5.3	Z/IP LAN Security.....	7
4.5.4	Remote Access	8
4.5.4.1	Remote Configuration	8
4.6	Network Management Command Classes.....	8
4.7	Z/IP Discovery	9
4.8	Resource & Service Discovery (mDNS).....	9
4.9	Z/IP Neighbor Discovery: IPv6 and IPv4 Address resolution for Z/IP Applications	9
4.10	IP Association Proxy	9
4.11	Mail Box Command Class – Support for Not Always Listening Nodes	10
4.12	Installation and Maintenance Framework	10
4.13	Transport Service	11
4.14	Z/IP Packet Command Class Version 3.....	11
4.15	Network Management Command Classes Version 2	11
4.16	Z/IP Gateway SDK 2.11.01 DevKit Contents	12
5	CERTIFICATION	14
	REFERENCES	15

1 ABBREVIATIONS

The following terms and abbreviations are used throughout the document

Abbreviation	Explanation
FLiRS	Frequently listening Routing Slave A battery-powered node type which may be reached within a few 100 ms. Typically used for applications such as door bells, networked smoke alarms, etc.
NWI	Network-wide Inclusion With network-wide inclusion, nodes may be scattered all over a house and still be included without being in direct range. This simplifies creation of bigger networks and allows a central static controller to handle the inclusion process without the need for a special inclusion controller carried around the house.
NWA	Network-wide Association The natural companion to Network-wide Inclusion. With NWA, Z-Wave networks may be managed from a central light controller in a hotel or from a remote call center supporter. NWA is purely IP-based and works over any physical layer. Several use cases in this document address this feature.
Remote network management	The Primary controller is in the heart of Z-Wave. With Z-Wave remote network management, it is possible to remotely manage a Z-Wave network by remote controlling the primary controller. Several use cases in this document address this feature.
Wake-up Node	A battery-powered node type which stays in low power mode for long periods. When waking up, it may just do a single measurement before returning to sleep. The node autonomously decides when to send a report or a WakeUpNotification to a mailbox node. WakeUpNotifications may be sent at very long intervals.
Z/IP	Z-Wave for IP. A framework defining mechanisms for <ul style="list-style-type: none"> • Transport of IP packets over a physical Z-Wave infrastructure • Transport of Z-Wave application commands in IP packets
Z/IP Node	A Z-Wave node capable of exchanging and processing IP packets
Z/IP Packet	A Z/IP packet is a UDP packet carrying a Z-Wave command with a pre-pended Z/IP header.

2 INTRODUCTION

The Z/IP Gateway Software Development Kit enables developers to write applications for the Z/IP Framework.

2.1 Purpose

The Z/IP framework extends the application scope of Z-Wave services from a classic Z-Wave wireless network to the networked world of IP; including the Internet.

This document provides an architectural overview of the Z/IP design philosophy and the mechanisms developed.

2.2 Audience and prerequisites

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

- 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.

3 Z/IP SDK DESCRIPTION

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

- **Z/IP Gateway.** Allows Z-Wave nodes to be controlled from an IP environment and appear as IP hosts in an IP network.
 - **Binary for BeagleBone Black platform**
 - **Linux x64 Debian Package**
 - **Source code**
- **Ubuntu 16.04 LTS 64-bit Virtual Machine** with environment setup for compilation.
- **Python Graphical Z/IP Client:** Test Sample application for testing Network Management functionality of the Z/IP Gateway.
- **Documentation, Framework and Guide.**

IMPORTANT NOTE:

- The Z/IP Gateway for this SDK **MUST** use DevKit 6.x or newer SerialAPI Bridge running on a 500-series chip. (Static Controller is **NOT** usable).
- A minimum of 32K NVM **MUST** be available for the SerialAPI.
- When operating as a secondary controller the Z/IP Gateway 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.
- When implementing Multi Command Command Class support in the Z/IP Client at the unsolicited destination the Z/IP Client **MUST** forward commands encapsulated in the Multi Command to the Z/IP Gateway if it implements that specific Command Class. The Z/IP Client **MUST** then aggregate the responses and send the responses to device sending the original Multi Command.

4 Z/IP GATEWAY SDK 2.11.01 FEATURES

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 2.11.01 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 Singlecast, no support for Multicast or Broadcast.
- Z-Wave nodes are identified by IPv6 and IPv4 host addresses
- IPv6 and IPv4 Ping (ICMP Echo) support
- SIS support
- Security 0 and Security 2 support
- Z/IP-ND: IPv6 and IPv4 address resolution for Z/IP Applications.
- Remote Access & Configuration
- Unsolicited forwarding to two destinations
- Resource & Service Discovery (mDNS) [2] [3]
- IP Association Proxy
 - Max 232 still apply for PAN (including IP Nodes)
- Mail Box Service – Support for Non-Listening
 - Configurable through CC
- Z/IP LAN Security using DTLS
- Installation and Maintenance framework
 - EEPROM Backup
 - Firmware Update of Z-Wave module attached to the Z/IP Gateway
 - Historical and current transmission statistics.
- WiFi support

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

Command Class	Type	Version	Secure Only	LAN NIF	PAN GW NIF	Appended PAN Node NIF	Controlled	Moved to Non-Secure**	Pre-Inclusion NIF
Security	Encapsulation	1		X	X		X		X
Security 2		1		X	X		X		X
Transport Service		2		X	X		X		X
Multi Channel*		4					X		
CRC16		1			X	X		X	X
Supervision		1			X	X			X
Network Management Basic	Network Management	2	X	X	X				
Network Management Inclusion**		2	X	X	X				
Network Management Proxy		2	X	X	X				
Network Management Installation Maintenance		1	X	X	X				
Inclusion Controller**		1			X	X		X	X
Wake Up*		2						X	
Z/IP	Z/IP	3		X		X	X		
Z/IP Portal		1	X	X					
Z/IP Gateway		1	X	X					
Z/IP Naming		1	X	X		X			
Z/IP ND		1			X				
IP Association		1	X				X		
Firmware Update	Application	5	X	X	X				
Mailbox		1	X	X			X		
Application Status		1		X	X		X		X
Power Level		1	X	X	X			X	X
ZWavePlus Info		2		X	X		X		X
Manufacturer Specific		2	X	X	X		X	X	X
Version		2	X	X	X		X	X	X
Association*		2					X		
Multi Channel Association*		3					X		

* These command classes are only controlled by the Z/IP Gateway and not listed in any NIF and will not answer to Version requests.

** Command classes that will be removed when not operating as an inclusion controller

*** When included into a non-secure network, the following command classes are moved to the Non-Secure NIF

NOTE: When operating in Secondary mode, the Z/IP Gateway must be defaulted to operate again.

4.1 Transparent Gateway

Z/IP Packets are carried in UDP packets on port 4123. The Z/IP Gateway MUST be able to decode Z/IP Packet headers and forward extracted Z-Wave commands to the node identified by the given IPv6 or IPv4 address.

4.1.1 IP Support for Z-Wave Nodes

The Z/IP Gateway MUST perform 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 MUST intercept all IP packets and if possible, emulate the requested service by using equivalent features of Z-Wave.

- The Z/IP Gateway MUST emulate 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 MUST use the Z-Wave NOP command to emulate the ping, and respond using ICMP reply to the requesting address. See [1].
- The Z/IP Gateway MUST forward the Z-Wave payload of any Z/IP Packet received for a classic Z-Wave node to the node. It MUST also handle Z/IP ack, and perform same ACK check on Z-Wave if requested. See [1].

4.2 SIS support

The Z/IP Gateway MAY act as a SIS in a Z-Wave network, but it will not relinquish its role to another controller. SIS MUST be enabled by default by the Z/IP Gateway. A SerialAPI with SIS support MUST be used.

There are no controls available for managing the SIS functionality.

4.3 Unsolicited Forwarding

The Z/IP Gateway provides a remote and local configuration option for forwarding unsolicited Z-Wave frames to an IPv6 address. This allows a network administrator to create a message sink somewhere in an IP infrastructure. The Z/IP Gateway MUST forward 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.

Z/IP Gateway supports a secondary unsolicited destination to be configured through the configuration file. The secondary destination cannot be configured remotely.

4.4 WiFi Support

The Z/IP Gateway supports running in WiFi client mode, through a customized relay configuration.

4.5 Security Mechanisms

A number of mechanisms are in place to protect the communication over the different communication channels, such as over Z-Wave, LAN and WAN.

4.5.1 Security Command Class

The Z/IP Gateway **MUST** communicate securely to 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 **MAY** transmit the normal Z/IP Packet to the Z/IP Gateway, which **MUST** perform the security encapsulation to the end node. It is up to the LAN administrator to ensure that communication on the LAN is secure or use appropriate measures as described in 4.5.3 and 4.5.4.

4.5.2 Security 2 Command Class

Security 2 provides amongst others, the following key features:

- Authenticated Elliptic Curve Diffie-Hellman key-exchange
- Single Frame security
- Secure Multicast

The Z/IP Gateway **MUST** communicate 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. If a LAN Z/IP Client wishes to communicate with a secure Z-Wave node, it **MAY** transmit the normal Z/IP Packet to the Z/IP Gateway, which **MUST** select the highest known common security encapsulation to the end node. It is up to the LAN administrator to ensure that communication on the LAN is secure.

4.5.3 Z/IP LAN Security

Z/IP LAN security provides a secure connection for clients, and other Z/IP Gateways, connecting to the Z/IP Gateway. The Z/IP LAN Security framework **MUST** provide 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 1.0 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.

4.5.4 Remote Access

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 MUST initiate 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 MUST be encrypted with Advanced Encryption Standard (AES) 128.

The Remote Access capabilities of the Z/IP Gateway are described in detail in [5].

4.5.4.1 Remote Configuration

In addition to local configuration it is possible to push Z/IP Gateway configuration remotely. It is possible to specify the following (see [5]):

- 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

4.6 Network Management Command Classes

Control of the Z-Wave network is carried out through a number of Network Management Command Classes.

The Z/IP Gateway supports the following Network Management Command Classes:

- **Network Management Inclusion:** Support for Adding/Removing, Set Default, Failed Node Replacement and Removal and Requesting Node Neighbor Update
- **Network Management Basic:** Support for entering Learn Mode, Node Information Send and Request Network Update

- **Network Management Proxy:** Support for Node List Get and Node Info Cached Get

These three command classes enable network management and access to simple network topology information.

4.7 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 MUST reply with Z/IP Node Info Cached Report and their IP address contained.

4.8 Resource & Service Discovery (mDNS)

The mDNS service allows an IP application automatically 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 MUST announce 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 MUST be dynamically multi-casted on the LAN backbone. The mDNS resource announcements MUST contain detailed information about the underlying node/endpoint such as its device type and supported command classes and IPv6 address(es).

The names of the mDNS resources MAY be statically generated.

4.9 Z/IP Neighbor Discovery: IPv6 and IPv4 Address resolution for Z/IP Applications

To allow Z/IP applications to understand the concept of Z-Wave Node IDs a translation service MUST be provided by the Z/IP Gateway to translate the Node ID into the appropriate IPv6 and IPv4 address.

Node IDs may reach a Z/IP application which for example uses the Network Management Command Classes, and can thus be translated into an IPv6 or IPv4 address that the Z/IP application is capable of communicating with. Refer to the Z/IP ND Command Class.

4.10 IP Association Proxy

The IP Association Proxy extends the Z-Wave addressing domain, by allowing Z-Wave devices to communicate with any IPv6 enabled device that supports the Z/IP Framework on either another Z-Wave network or a separate IP application.

Z-Wave IP Associations are created between two Z/IP resources identified by an IP address and an endpoint ID. The Z/IP Gateway MUST emulate the IP properties of Z/IP Nodes for Z-Wave nodes:

- Association from one Z-Wave 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 node: Send an Association Set Command to the association source encapsulated in a Multi Channel frame.
- Association from a node 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 less Node IDs for physical devices.

4.11 Mail Box Command Class – Support for Not Always Listening Nodes

The Mail Box MUST provide support for any IP application to communicate with nodes support the Wake Up Command Class without them having to implement or understand the Wake Up Command class. The principle of the mail box functionality means that sending application does not need any knowledge about the receiving node sleeping state. The sending application MUST receive a “Delayed” packet each minute, indicating that ACK is expected at a later point, and that the application SHOULD NOT attempt retransmission.

The queue size of the mailbox is currently limited to 500 entries.

In addition, the Mailbox supports the Mailbox Command Class, which allows a lightweight Z/IP Gateway to offload the mailbox functionality to a more powerful mailbox service such as a portal.

4.12 Installation and Maintenance Framework

The Installation and Maintenance Framework provides a method for gathering statistics and perform 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

In addition it is possible for a Z/IP Client to perform a backup for the EEPROM attached to the Z/IP Gateway for backup purposes.

Firmware update for the Z-Wave module attached to the Z/IP Gateway, can be performed through the Firmware Command Class, through the Z/IP Gateway.

4.13 Transport Service

The Transport Service Command Class version 2 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

4.14 Z/IP Packet Command Class Version 3

The Encapsulation Format Info Header Extension is added to the Z/IP Packet Command Class Version 2. The extension serves two purposes:

1. Indication of the encapsulations used when the frame was received by the Z/IP Gateway
2. Which encapsulations should be used by the Z/IP Gateway when sending a frame

The extension is marked as Critical which means a receiving Z/IP Client MUST interpret the extension or drop the entire frame.

This extension MUST be used to ensure Answer-As-Asked policy is adhered to.

4.15 Network Management Command Classes Version 2

Version 2 of the following Network Management Command Classes is added, to provide required Security 2 functionality:

- Network Management Inclusion
 - Updated Add / Remove / Replace
- Network Management Basic

- Updated Learn Mode
- New DSK Get/Report
- Network Management Proxy
 - Updated Node Info Cached Get / Report

4.16 Z/IP Gateway SDK 2.11.01 DevKit Contents

The Z/IP Gateway 2.11.01 Development Kit MUST contain the following components:

- Documentation:
 - ZTS, Z/IP Security 2 in Z/IP Gateway
 - ZTS, Z/IP Gateway Source Code Documentation
 - ZTS, Z/IP Gateway Tutorial
 - Z-Wave & IP Basics
 - Compilation
 - Installation
 - Troubleshooting
 - Sample Code
 - PyZIP User Guide
 - ZTS, Z-Wave Command Class specifications
 - 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)
- Binary:
 - Z/IP Gateway 2.61, for BeagleBone Black, Linux 32-bit

- Z/IP Gateway 2.61, for Linux x64
- Source:
 - Z/IP Gateway 2.61
 - PyZIP 1.16 – Python Graphical Z/IP Client for testing

5 CERTIFICATION

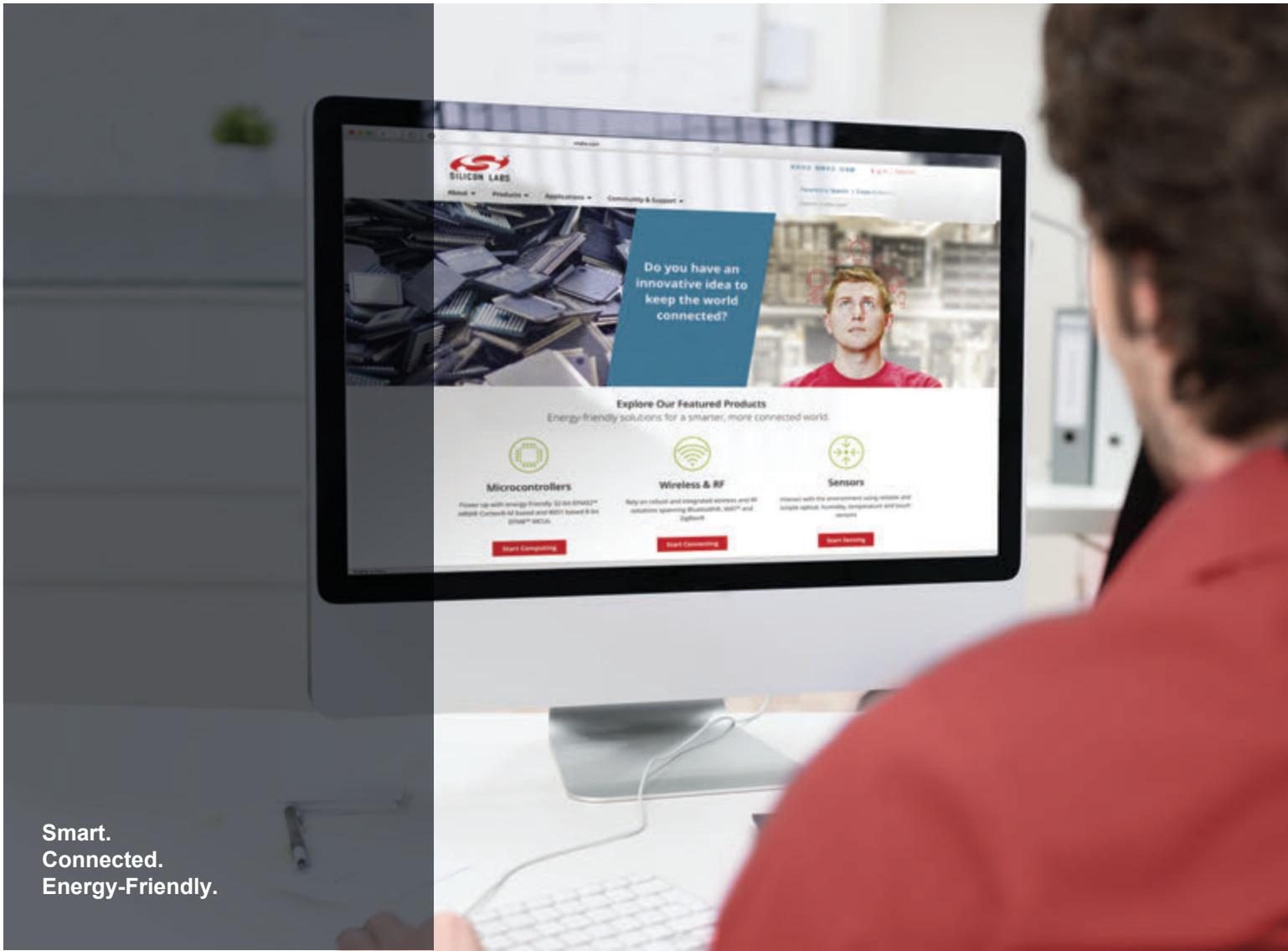
Z/IP Gateway must undergo certification as part of a system. It cannot be certified as a standalone product.

Z/IP Gateway 2.61 (SDK 2.11.01) has passed Z-Wave Certification in conjunction with Z-Ware 0.5.

The functionality that Z/IP Gateway SDK 2.11.01 provides has been verified to be in compliance with Z-Wave+ Certification requirements for controllers.

REFERENCES

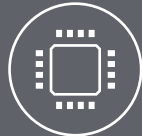
- [1] SDS11445, Silicon Labs, IP Architecture Framework for Z-Wave (Z/IP)
- [2] SDS11756, Silicon Labs, Z/IP DNS Discovery support (DNS-SD, mDNS)
- [3] SDS11633, Silicon Labs, Z/IP Resource Directory (RD, DNS-SD, mDNS)
- [4] SDS12938, Silicon Labs, Z/IP LAN Security
- [5] SDS12089, Silicon Labs, Z/IP Gateway Bootstrapping (ZIP, IPv4, IPv6, Router, NAT, DHCP, tunnel, remote access)
- [6] INS12503, Silicon Labs, Z/IP Gateway Porting Process



Smart.
Connected.
Energy-Friendly.



Products
www.silabs.com/products



Quality
www.silabs.com/quality



Support and Community
community.silabs.com

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 without the specific written consent of Silicon Labs. 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.

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-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.



SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

<http://www.silabs.com>