Software Design Specification

IP Architecture Framework for Z-Wave (Z/IP)

Document No.:	SDS11445
Version:	3
Description:	Concepts and use cases
Written By:	ABR;JFR;BBR
Date:	2018-03-06
Reviewed By:	BBR
Restrictions:	RD Only

Approved by:

Date	CET	Initials	Name	Justification
2018-03-06	09:25:35	NTJ	Niels Thybo Johansen	

CONFIDENTIAL

REVISION RECORD				
Doc. Rev	**Date**	**By**	**Pages affected**	**Brief description of changes**
1	20100415	ABR	ALL	Based on SDS11445-2A. This new doc is to describe ALL parts of the Z/IP Framework. SDS11445 going forward describes the features supported by official dev. kits. SDS11445 must be generated by removing confidential text from this document.
2	20101015	ABR	Most	Added AGI, AAGI, NWD, NWA, Battery Support, Security
2	20110701	ABR	Most	Added Network Management
3	20110912	ABR	Some	Editorial clarification prior to phase one review
4	20180306	BBR	All	Added Silicon Labs template

Table of Contents

1 TERMINOLOGY

The following terms and abbreviations are used throughout the document

Abbreviation	Explanation
HAN	Home Area Network. A network with coverage for an entire home. Z-Wave is a HAN technology.
PAN	Personal Area Network. Term used for same class of networks as HAN.
Network management	With Z-Wave Network Management, it is possible to manage a Z-Wave network by remote controlling the primary controller. Several use cases in this document address this feature.
Z/IP	Z-Wave for IP. A framework defining mechanisms for • Transport of IP packets over a physical Z-Wave infrastructure • Transport of Z-Wave application commands in 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

2.1 Purpose of document

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.

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

2.2 Audience and prerequisites

Zensys R&D and partners.

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 FEATURE DOCUMENTATION

Table 1 presents the required documentation for each phase of Z/IP Router design.
Each new line adds additional functionality.

Stage	Features	Documents	Comment
1	Classic Z-Wave	10242 11060	Device Class Specification Command Class Specification
2	Basic Gateway	11445, 11467 11468	IP access to Classic Z-Wave nodes; UDP & Ping No Z/IP nodes No remote access
3	+ Network Management	11444, 11528, 11769, 11770	Serial API ported to Z-Wave command classes.

Table 1, Development stages and the required documentation

4 IP CONNECTIVITY

The Z/IP framework provides IP connectivity between IP applications in an IP environment and Z-Wave nodes. Connectivity is achieved via the Z/IP Router and the embedded Z/IP gateway function.
IP communication inside the HAN is also supported. The Z/IP framework supports IPv6 only.

4.1 Talking to Classic Z-Wave nodes

4.1.1 Controlling Classic Z-Wave nodes from IP applications

The first application space to benefit from IP connectivity is Z-Wave home control.
Thanks to the Z/IP Gateway function IP applications may send Z-Wave application commands to any legacy Z-Wave node via any IP infrastructure, including LAN or the Internet.
Users with IP experience will appreciate the support for ICMP Echo, also known as Ping.

IP services for classic Z-Wave nodes are limited to Z-Wave Home Control (UDP port 4123) and Ping (ICMP Echo).

4.1.2 Forwarding traffic from classic Z-Wave nodes to IP applications

Z-Wave Sensor reports and sensor initiated commands may be forwarded to IP applications for centralized processing or forwarding to remote locations in the Internet.
Traffic is forwarded to an IP destination previously registered in the Z/IP Gateway. This feature is known as “Forwarding unsolicited Z-Wave traffic”.

4.2 Remote Access to Z/IP Networks

Users may control Z-Wave nodes or access Z/IP nodes from outside the home premises, e.g. from a smart phone. Many consumer routers offer proprietary VPN solutions for secure access to private networks. Most of the solutions do not scale well for service providers wanting to support 1000’s of consumers.

The Z/IP Framework does not mandate any particular technology for secure access from remote locations.

5 ROUTING MODES IN A Z-WAVE NETWORK

Z-Wave nodes use Z-Wave source routing to transport Z-Wave commands between nodes.

5.1 The Z-Wave Protocol

The Z-Wave Protocol is the routing protocol used between classic Z-Wave nodes. It uses source routing to control the flow of Z-Wave frames from an originator to a destination via up to 4 repeater nodes.

The Z-Wave protocol provides retransmission of singlecast frames; potentially via multiple routes. Multicast and broadcast are supported in direct range with no acknowledgment.

It is possible to deliver frames securely via singlecast. This is not possible for multicast and broadcast as a challenge-response algorithm is used between two nodes at a time.

Recently, Explorer route discovery has been added to Z-Wave; enabling on-demand route re-discovery when needed. The explorer tool suite at the same time offers network-wide inclusion and other advanced features. Controllers implementing explorer discovery still has to implement the complete route management system used by earlier generations of Z-Wave controllers in order to be backwards compatible.

6 APPLICATION LAYER SERVICES

The Z-Wave eco system provides access to a wealth of information on node capabilities.

6.1 Node Information

All nodes report the basic properties via the Node Information frame. Information includes Device Type information as well as additional information such as Command Classes which are supplements to the default properties of the device type.

. An IP host in the LAN just sends commands in the same way as to listening nodes.

6.2 Network Management

The Network Management command classes [2] allow a host to initiate network management related tasks in Z-Wave nodes. The Network Management command classes are native command classes. The required support functions for use in an IPv6 environment are described in [9],[10].

A Z/IP Router MUST implement support for Z-Wave Network Management.

7 USE CASES

7.1 Basic operations

7.1.1 Use case: Z-Wave node included with Z/IP Router as primary controller

User includes a Z-Wave node via the Z/IP Router web interface. After inclusion, the node may be pinged and controlled from an IP application, e.g. the command line utility ZW_Send.

1. User clicks “Add Node” in the Z/IP Router web interface
2. The Z/IP Router enables learn mode
3. The user plugs in the new node. If the node needs a button press for initiating inclusion, the button is pressed.
4. Using the subnet prefix configured in the Z/IP Router, the IP address of the new node can now be pinged.

7.1.2 Use case: User controls devices in customer premises via service provider

User logs in securely to a personal profile in service provider web portal. The service provider web portal establishes secure connection to Z/IP router in customer premises.

Basic assumption: Z/IP Router is configured with URL of service provider server. Z/IP Router frequently sends keep-alive messages to service provider portal..Secure tunnelling is used to maintain data integrity through the Internet. The specific VPN technology to use is out of scope of this document.

1. User logs into the web portal of the service provider
2. Web page shows status of Z/IP Router: Yellow check mark
    a. [red cross] if no keep-alive messages have been received recently
    [yellow check mark] if keep-alive messages are received at low rate
    [green check mark] if keep-alive messages are received at high rate
    b. Show all Z-Wave devices as grey until receiving first keep-alive message or if Z/IP Router status is red.
3. Server waits for next keep-alive message
4. Web page status of Z/IP Router: Green check mark.
    a. Z/IP Router is allowed to send more frequent keep-alive messages while user is logged in and is active.
    b. Read back status of all Z-Wave devices in (visible part of) web page.
5. User clicks various icons...
    a. Due to the asynchronous timing of keep-alive messages, the web server application queues up the commands until next transmit opportunity.

b. Icons are updated locally to reflect user action; e.g. dark to light, red to green, etc. if deviations are detected.

c. Option: Server sends a “Get” command to each object manipulated by the user to verify the operation.

d. Option:The user may press “Refresh” to force a complete status read-back from all devices presented in the user interface.

7.1.3 Use case: User controls devices in customer premises via direct login to web page

User establishes direct secure connection to Z/IP router in customer premises.

Basic assumption: Z/IP router has globally accessible IP address.

1. Z/IP Router operates a password-protected web page accessed via HTTPS.
   The web page provides access to network management and device control – just as the service provider version discussed earlier.
   This version is more responsive but offers no support. Also it is free of charge, where the service provider version is likely to have a subscription fee.

7.1.4 Use case: Installer sets up new equipment in a hotel room

The light control management server is located in the basement. The management server may be reached via Wi-Fi all over the hotel.

The installer carries a Wi-Fi enabled tablet showing the web GUI of the light control management server.

1. Installer right-clicks the room in the floor plan of the hotel - or chooses the room number from a list
   a. Light control management server looks up the Z/IP Router to use
2. Installer clicks <add new modules> on web GUI of the management server
   a. Light control management server enables Z/IP Router NWI learn mode
   b. Z-Wave network management command is sent securely
3. Four new modules are included via Network-wide inclusion – one at a time
4. The new modules are presented to the installer (IPv6 address and node information)
   a. The entire node list is accessible to the installer.
5. Installer can now ping the new modules and read back values
6. Installer wants to associate all lamp modules to a new door switch, and selects all lamp modules in the list of new devices
7. Installer clicks <Map devices to new control device>
   (Note that Inclusion and Association is combined into one operation)

   a. Light control management server enables NWI learning in the Z/IP Router

8. The installer connects the wall switch and activates inclusion

   a. The wall switch sends out an NWI inclusion request

   b. The Z/IP Router in NWI learn mode intercepts the request

   c. The wall switch is included

   d. Default gateway and IPv6 address are assigned to the wall switch.

   e. The light control management server sets up association from wall switch to lamp modules

7.2 Security

A classic Z-Wave network co-exists with other Z-Wave networks. The homeID effectively prevents one network from disturbing the other. This is a simple and robust solution when all guys are good guys. In a more hostile world, however, there is a need for more protection.

Traffic is secured in the wireless domain but attacks may come from the Internet.

7.2.1 Use case: DDoS attack via the Internet

1. The access router is flooded with Internet traffic.
   The firewall keeps the traffic from reaching the LAN side of the router.

2. Users are prevented from remotely controlling their devices via the service provider portal but all local operations are not affected.

   a. Alternative option: The attack targets the service provider. It affects more subscribers' ability to control devices remotely, but this attack also does not get control over the devices.

3. The attack quickly attracts attention from the attacked users and/or the service provider

4. Conclusion: While annoying, hackers do not get control over devices.

   a. DDoS attacks only work effectively when targeting a few victims. It is not effective to attack a high number of private households by attacking customer premises access routers.

   b. The more likely target is the server of service providers or alarm companies; thus preventing local alarm systems from delivering alarm reports.

   c. Thanks to the proposed mailbox mechanism, it is possible to configure new target addresses in sensors even when the sensors are not able to get in contact with the actual target address.

7.2.2 Use case: Remote intrusion attack (IPv6)

1. A hacker manages to punch holes through the firewall and gets access to the LAN behind the access router.

2. With IPv6, all nodes potentially have a globally unique IP address

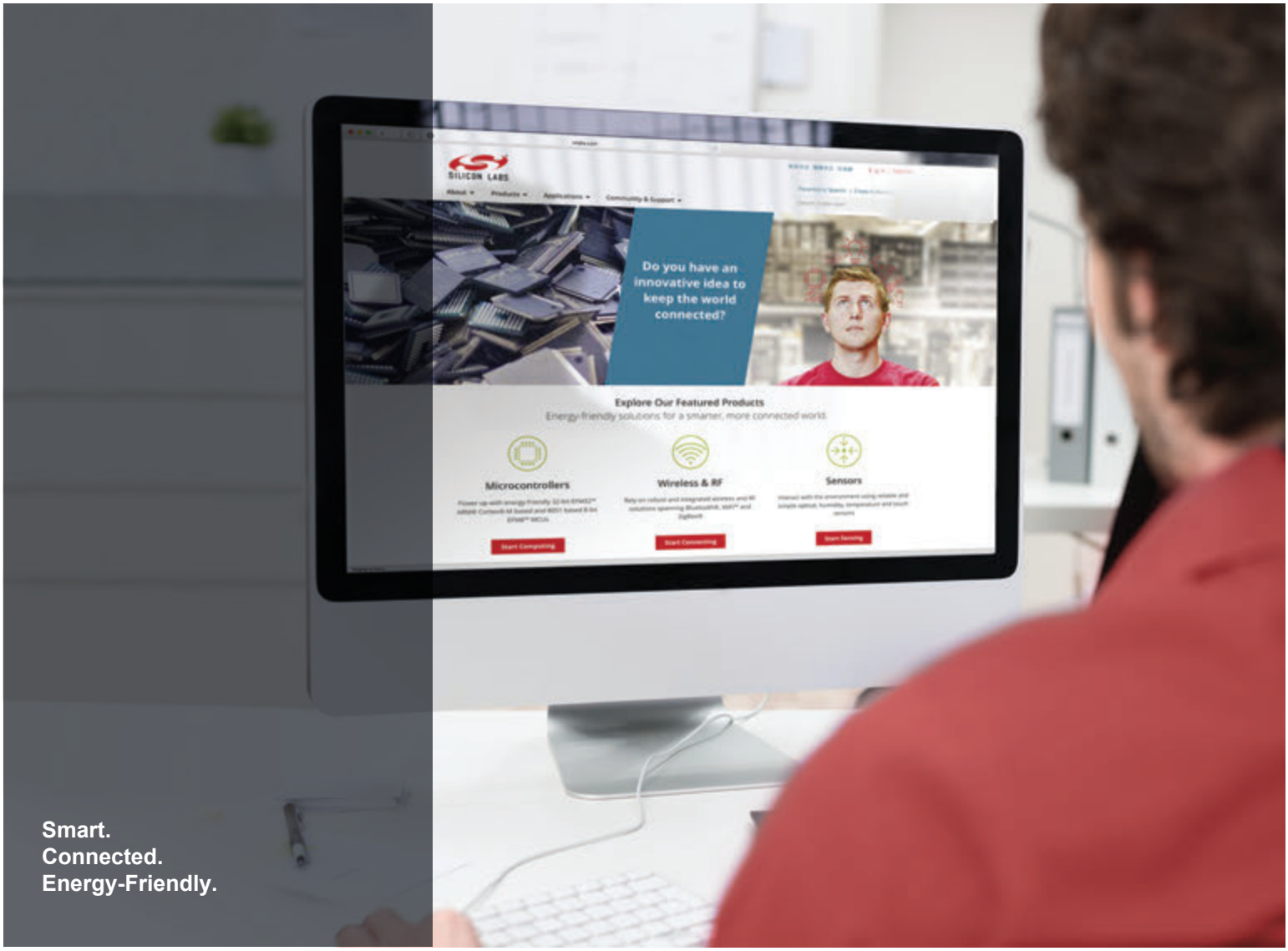
3. The Z/IP Router maps to a smaller subnet. Using IPv6 Router Announcements, the Z/IP Router informs the access router that it provides access to the Z/IP HAN IP subnet.

4. Users get a /64 or even a /56 prefix assigned by the ISP.
   Guessing random 128 bit addresses for home control devices is difficult.The last part of IPv6 addresses is formed from HomeID and NodeID. Thus, it must be expected that addresses are addresses are not really hard to guess.
   Most likely hackers start collecting lists of live IPv6 address ranges just as they currently trade email lists for spam mail distribution.

5. Conclusion: Nodes may have globally unique addresses. It is possible to address a node from anywhere in the network. Sending a Z/IP encapsulated BasicGet packet to a node will make it return a response.
   It is a requirement that a firewall prevents unwanted traffic from entering the LAN and ultimately the Z/IP HAN. The Z/IP Router MAY implement Access Control Lists (ACL) or equivalent mechanisms to prevent unwanted traffic from entering the network.

REFERENCES

[1] INS11418, Z-Wave Starter Kit - SerialAPI - Appl. Prg. Guide
[2] SDS11777, Z-Wave Network Management Command Classes
[3] SDS11386, Command classes for full IP support in Z/IP networks
[4] PSP11465, Z/IP - Z-Wave for IP; Router Requirements
[5] SDS11468, Z/IP - Z-Wave for IP; Gateway Requirements
[6] SDS11506, Z/IP: IANA Assignment of the Z-Wave UDP Port (4123)
[7] SDS10242, Z-Wave Device Class Specification
[8] SDS11814, Z/IP Command Class Specification
[9] SDS11769, ZIP-ND: IPv6 address resolution for Z/IP applications
[10] SDS11770, Z/IP: Z-Wave network Management for IP hosts (Guideline)
[11]



Products
www.silabs.com/products

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

SILICON LABS®

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

http://www.silabs.com