Z-Wave to IP Software/ Firmware Bridges the Worlds of Z-Wave and IoT

By Raoul Wijgergangs,
Vice President Z-Wave
Business

Abstract/Executive Summary:

The Z/IP Gateway bridges the low-power and ultra-reliable Z-Wave wireless communications protocol with the Internet of Things (IoT) by assigning a unique IP address to each device within a Z-Wave network. This provides the best of both worlds: a super reliable, low-power smart home network combined with standard Internet protocol on the LAN network. Z-Wave is already widely deployed in home security and home automation systems as the protocol of choice for low-power wireless communications. Now, with the Z/IP Gateway, every device in a Z-Wave network can be directly accessible over the Internet using IP communications. The Z/IP Gateway is a software/firmware technology that is incorporated into new Z-Wave controllers, effectively transforming these home automation hubs into gateways for IP communication with Z-Wave devices. With the Z/IP Gateway technology, product designers can add IoT connectivity to practically any device in the home with minimal power consumption and minimal added cost.

IoT – the Internet of Things – is a hot tech trend, envisioning a future where practically everything will be connected, but exactly how they will be connected remains fuzzy. While consumers may simply assume everything will have Wi-Fi, engineers know better. Wi-Fi has inherent problems with power consumption and topology that make it impractical for many battery-powered devices. On the other hand, the Z-Wave wireless mesh network communications protocol is perfectly suited to such applications. Z-Wave was created specifically to address the needs of the home security and home automation markets, replacing the wires that used to connect the door and window sensors of a home security system. With Z-Wave, a wireless magnetic door/window sensor can operate for years before the battery needs replacement.

The Z/IP Gateway, a feature of Z-Wave, makes it easy to combine the advantages of Z-Wave with the advantages of IoT by assigning a unique IP address to each device within a Z-Wave network. Designers can get all the benefits of Z-Wave, including low power consumption, easily extendible mesh networking, and very low cost per networked device, combined with all the benefits of IoT.

There are some in the industry who promote running IP all the way to the end nodes of a smart home network. This would result in extensive overhead of IP addressing to be sent using low-power devices. Typically the overhead with IP all the way to the end nodes would result in battery lives much shorter than Z-Wave battery nodes that “talk” to the internet with Z/IP.

The Z-Wave Protocol

Introduced over a decade ago , the Z-Wave protocol for wireless low-power communications features mesh networking for robust, extendable communications and 128-bit encryption for secure communications with locks and other security sensitive devices. All AC-powered plug-in Z-Wave devices automatically function as repeaters to extend the wireless network, which is based on sub-gigahertz radio frequencies using the ITU-T G.9959 specification for MAC and PHY layers.

Thanks to tight control over device definitions and allowable command class communications between devices, Z-Wave is the leader in end-to-end interoperability for home and security applications. Z-Wave signals are robust, featuring source routing with failover dynamic routing recovery. Devices incorporating Z-Wave can be lightweight and extremely low power (utilizing "FLiRS" Frequently Listening Routing Slave technology, where appropriate), while maintaining low latencies. (For more on FLiRS see Z-Wave Wireless Communications for Smart Devices and IoT | TechOnline). The large existing base of over 1200 Z-Wave products readily demonstrates that the technology is real, and is market proven, including deployment in nearly 100% of the U.S. monitored home security market. Z-Wave represents a one billion USD industry at retail in 2015, with 20 million Z-Wave pure smart home devices being added to the market in 2015.

Z-Wave and IP

Although IoT means different things to different people, for home applications it is widely seen as an extension of today's burgeoning smart home and home automation/home security markets. So it makes sense to adapt a widely used communications technology for IoT communications, and many existing OEMs using Z-Wave in their smart home products have asked for this capability.

Z-Wave is a communications network that is inherently bound by a home, building, or campus, sometimes referred to as a HAN (home area network). IP (Internet Protocol) is the open, worldwide standard for communicating over great distances. Traditionally, home automation and security systems have bridged these two worlds via a controller, a home-based gateway that communicates securely over the Internet to an end user, running software that effectively translates the user's requests to corresponding Z-Wave signals, such as to dim lights or change a thermostat.

The advantage of directly assigning an IP address to the light dimmer or thermostat is that it then opens up the possibility of devices in the home system communicating with many other applications beyond the end-user's remote control interface, thus enabling the flowering of the IoT vision in which devices and apps talk to each other. So the refrigerator can talk directly with the supermarket, so to speak. That vision of using IP as the lingua franca of the IoT is being fostered in part by organizations such as IPSO and IETF, both of which Z-Wave supports.

RF HANs such as Z-Wave were designed for lightweight, low latency, low power communications. IP was designed for a very different technology space, beginning with AC-powered desktop computers. Simply putting pure IP across a HAN will reduce both performance and battery life of devices. The new 6LowPan protocol in development addresses some of the power considerations, but there are still conflicts and difficulties in bridging between mesh routing and classical IP switch routing.

Z/IP & Z/IP GATEWAY: Z-Wave's Approach to IP

Z-Wave already has the advantage of being widely deployed and field tested, with over 1200 devices available, including everything from lamp dimmers and switches to motion and door and window sensors, alarms, thermostats, smoke and CO_2 detectors, window treatments and door locks. With over 35-million Z-Wave devices manufactured already, it is the largest existing ecosystem of interoperable home automation and security products.

Adding IP communications to this installed base, as well as future IoT products yet to be dreamed of, is not very complicated. Z-Wave is really just another Link Layer from an IP perspective. Because Z-Wave itself handles the transaction, including establishing the communication and error checking, it makes sense to use the UDP (User Datagram Protocol) connectionless form of IP transmission (as opposed to TCP, which would consume power at a much higher rate.) IP communications takes place through UDP Port 4123, which is already reserved for Z-Wave communications by IANA.

Z/IP is a Z-Wave Command Class encapsulation datagram for sending Z-Wave datagrams (Command Class messages) to Z/IP enabled devices. This makes Z/IP communication independent of the Link Layer. All that matters is that the receiving device supports IP / UDP4123 / Z/IP and Z/IP Command Classes.

The Z/IP Gateway application addresses today's needs, while also opening up a bright and flexible future for Z-Wave devices that support IP. Z/IP Gateway supports all 35-million existing Z-wave devices in the market. Intended for Z-Wave controllers, Z/IP Gateway creates a unique IP address for each device in the Z-Wave network, and facilitates IP communication to each device.

Z/IP Gateway's capabilities include:

- IPv6-compliant
- Z-Wave acts as Link Layer to IP
- Internet Protocol routing: Transmitting Z-Wave UDP/IP datagrams between Z-Wave devices and IP address
- Translating IP address to Z-Wave HomeID+NodeID
- DHCP Client (assigning NodeIDs to PAN device and assigning IP address to those devices)
- Full support for ICMP (Internet Control Message Protocol) ping of devices
- Caching of device capabilities, allowing IP devices to discover and identify all Z-Wave devices, including sleeping devices.

Z/IP Gateway utilizes Z-Wave's proven interoperable application layer Command Classes for command and control of the Z/IP Gateway application. This includes the Command Class for including and excluding devices in the Z-Wave network, a Command Class for NAT lookups, and configuration of the Z/IP router for DHCP or fixed IP address.

Development Tools for IoT Product Design

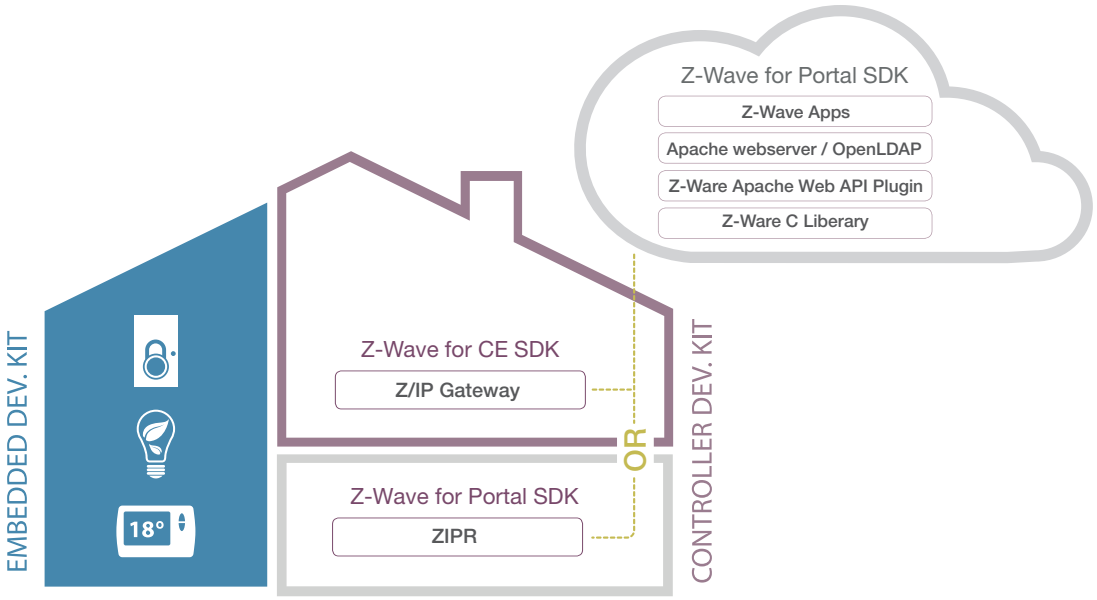
The Z/IP Gateway is a powerful IoT enabling technology for Z-Wave controllers. It provides a real router that is fully accessible from all devices it's connected to, providing full IP compatibility to the Z-Wave universe.
The Z-Wave Controller Development Kit, available from Sigma Designs, provides OEMs and others interested in creating central controllers, or hubs, for smart home, security, and IoT with everything needed to get started.
It includes these SDK building blocks:

- **Z/IP Gateway:** Application handling all communication between Z-Wave and Z/IP, similar to the way a home router handles communication between home PCs and the Internet. Handles all the Z-Wave housekeeping such as network management, Z-Wave Security, mailbox for battery driven devices, Z/IP packaging and multichannel support. Z/IP Gateway utilizes DTLS for LAN security, and can also connect to a remote server through a secure TLS1.1 tunnel, making it ideal for use with a portal server.

- **Z-Ware C Library:** The library contains a C API that can connect to a Z/IP Gateway and discover all connected Z-Wave devices, exposing them as software objects.

- **Z-Ware Apache Web API Plug-in:** Used to combine Z-Ware C Library and Z-Ware Apps with standard technologies, such as OpenLDAP and Apache Server, to form a starting point for portal solution developers. The Z-Ware Portal is designed to serve a Z/IP Gateway (including the ZIPR, described below), through secure IP tunnels.

- **Z-Ware Apps:** A collection of user interface samples for smart TVs, PCs, tablets, and smartphones. Designed with a focus on optimizing the consumer experience, Z-Ware Apps are easily customizable to include company names, logos and color schemes. Supplied as source code.



SILICON LABS

The Z-Wave for CE SDK includes all the software building blocks needed to design a smart home solution. It includes the Z/IP Gateway plus a host build environment in Ubuntu Linux, creating targets for the TI BeagleBone Black (a low-cost, open source, community-supported development platform for ARM Cortex-A8 processor developers.) The Z/IP Gateway connects to a USB controller reference design as default, but all of the Silicon Labs 500-Series Z-Wave modules and SoCs can also be used with the CE SDK. Serial API binaries are included in the kit. The Z-Ware C library is offered with an easy to understand C API for a developer to design an application on top of.

The ZIPR, a standalone adapter to implement Z/IP is also available. The ZIPR is a Z/IP Gateway that brings all Z-Wave devices on the market to the Internet of Things. The ZIPR is designed to be plugged into a user's home IP network, enabling applications residing on gateways, set-top boxes, TVs, mobile devices, and cloud services to communicate with and control Z-Wave devices on the Z-Wave mesh network. For connections outside the local IP network, the ZIPR supports secure TLS 1.1 TCP tunneling. The ZIPR is ideal for retrofitting existing Z-Wave networks with IP addresses for each device in the network. A ZIPR reference design is available from Silicon Labs; there are also ready-to-use retail versions of ZIPR available from DigiKey and Edge Electronics, along with Z-Wave development kits.

Conclusion

IoT's implementation requires paying careful attention to power consumption, signal security, added BoM costs, and network reliability. The Z-Wave protocol was designed from the ground up to address all these factors, and is ideally suited for IoT in a home or office environment. The Z/IP software/firmware bridges the worlds of Z-Wave and IoT, by assigning a unique IP address to each device in a Z-Wave network and facilitating communication over the Internet using standard IP protocols. This can make each of the devices in a Z-Wave mesh network directly accessible over the Internet. With over a decade of field-tested experience in millions of homes and offices, Z-Wave is already the world's leading choice for home automation and security networking. Combined with Z/IP technology, devices on a Z-Wave network can now be part of the IoT. Silicon Labs is the world's leading supplier of Z-Wave solutions to OEMs and controller software creators. For more information about Z/IP and Z-Wave, visit www.silabs.com