Software Design Specification

Z/IP Gateway Bootstrapping

Document No.:	SDS12089
Version:	
Description:	Procedures for zero configuration bring-up of a Z/IP Gateway - in existing IP networks as well as in a stand-alone mode. This document addresses interfacing on the IP backbone network. All operations on the Z-Wave side follows classic Z-Wave specification
Written By:	ABR;JRM;JBU;SAMBAT;SRAVELLA;DCHOW
Date:	
Reviewed By:	ABR;JRM;SAMBAT;AES;SRAVELLA;JFR
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2016-08-26	16:31:12	NTJ	Niels Thybo Johansen	

DOCUMENTATION DISCLAIMER

Copyright Notice

Trademark Notice

License Restrictions Warranty/Consequential Damages Disclaimer

Warranty Disclaimer

Restricted Rights Notice

Hazardous Applications Notice

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
4	20160823	ABR	All	First revision for public release

Table of Contents

Table of Figures

1 ABBREVIATIONS AND TERMS

Abbreviation / Term	Explanation
CER	Customer Edge Router
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System. The “telephone book” of the Internet
DNS-SD	DNS Service Discovery. Special use of DNS for discovering resources in a network such as printers or music repositories.
HAN	Home Area Network. Z-Wave is an example of a HAN technology.
IETF	Internet Engineering Task Force
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network. Ethernet and WiFi are examples of a LAN technology.
NAS	Network Attached Storage
NAT	Network Address Translation. Not to be confused with the NAPT used in most private LANs today. NAT is transparent to port numbers.
NAPT	Network Address and Port Translation. Widely used to in private and corporate IPv4 subnetworks. Maps all private addresses into one public address.
NDP	Neighbor Discovery Protocol. IPv6 protocol for auto configuration of nodes and related operations.
NPTv6	Network Prefix Translation version 6
P2P	Peer to Peer
RA	Router Advertisement
RS	Router Solicitation
Service Discovery	Covers the ability of consumer devices to identify local network resources without any user intervention. Service Discovery is a ZeroConf technology.
SSID	WiFi Service Set IDentifier. Identifies a wireless network.
UDP	User Datagram Protocol
ULA	Unique Local Address
WAN	Wide Area Network. Internet access technology. xDSL is an example of a WAN technology.
WLAN	Wireless LAN. WiFi is the most used technology for WLANs.
Z/IP	Z-Wave for IP
Z/IP Gateway	Application transparent mechanism that provides IP connectivity to classic Z-Wave nodes.
ZeroConf	Zero Configuration. Covers the ability of consumer devices to connect to a network and access the Internet and local network resources without any user intervention. DHCP and mDNS are technologies enabling Zeroconf applications.

2 INTRODUCTION

The Z/IP Gateway presents Z-Wave nodes as IP hosts. The Z/IP Gateway may be implemented as a stand-alone device or installed in existing networks with other Customer Premises Equipment (CPE). The Z/IP gateway function may be an integral component of a Customer Edge Router (CER).

RFC4191 [14] specifies how IPv6 routers may advertise prefixes of subnets that may be reached via these routers. Unfortunately only a subset of today's operating systems support RFC4191.
The Z/IP architecture is prepared for such functionality while it also supports existing IPv4 environments.

2.1 Terminology

A LAN is an IP based local network which typically runs over Ethernet or WiFi.
A HAN is a wireless network with a comparable coverage to a LAN but dedicated to sensor network technologies with extreme requirements to battery life.

The Z/IP Gateway provides application transparent connectivity between IP hosts in a LAN and Z-Wave nodes in a HAN.

A portal in the internet may allow internet connected users to control Z-Wave resources via a secure tunnel between the portal and the Z/IP Gateway. The internet is said to be a Wide Area Network (WAN).

2.2 Terms used in this document

The guidelines outlined in RFC 2119, [1] apply.
Essentially, the key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2.3 NAT behind NAT

Many home networks have a broadband router provided by the Internet Service Provider (ISP) and a WiFi router installed by the homeowner. What most homeowners do not realize is that they create what is technically called "NAT behind NAT". It makes life complicated to P2P technologies but these challenges can be overcome.

The homeowner connected the WAN (or "Internet") port of the WiFi router to a LAN port on the broadband router. Some broadband routers have a built-in switch, e.g. 4 ports. If the homeowner installs a network printer (or a Z/IP Gateway) in one of the other ports of the broadband router, "NAT behind NAT" becomes a problem. "NAT behind NAT" creates a partitioned network of two IP subnets.
The discovery protocol mDNS [17] [18], which is used by NAS boxes, network printers – and the Z/IP Gateway – is a so-called link-local technology. It only works in the IP subnet in which it operates.

The network setup outlined in Figure 1 allows the PC to discover the network printer while it cannot discover the media server and the Z/IP Gateway because they reside in another IP subnet than the PC.

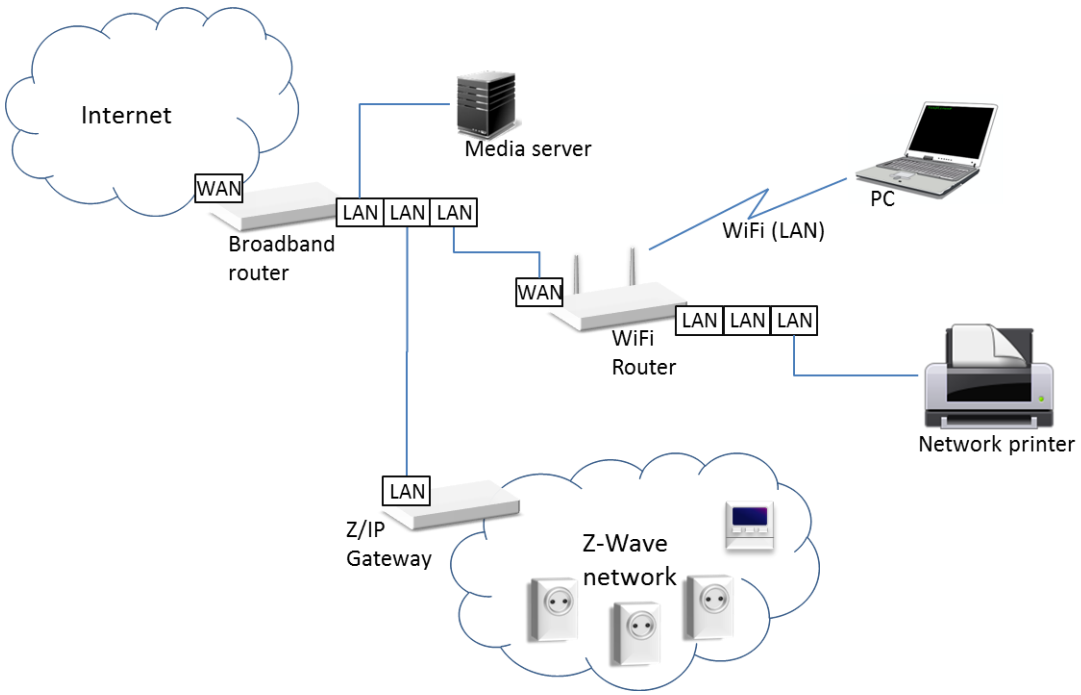

Figure 1, NAT behind NAT

This is a problem for network printers and the Z/IP Gateway but the problem is not caused by these devices. There is only one simple advice to the homeowner: Avoid “NAT behind NAT”.
This is unfortunately a useless advice since no average user knows what this means.

A better advice to the average user may be:

If you have a WiFi router after your broadband router, make sure only the WiFi router WAN port is connected to the broadband router.
If you do not have enough ports in your WiFi router, connect a normal switch (it has no WAN port) to one of the WiFi router ports and connect the remaining gear to the ports of the switch.

3 BOOTSTRAPPING USE CASES

This chapter defines a number of use cases which may be referenced by the following chapters.
It outlines desirable behavior in given situations.

3.1 **Simple demo mode** (Stand-alone control via WiFi)

A new Z/IP Gateway is unboxed. No LAN or WAN cables are connected.

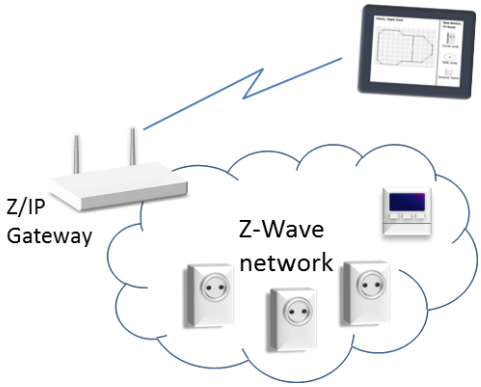

Figure 2, Simple demo mode

The user connects a tablet to the WiFi network using the SSID and passphrase printed on the back of the Z/IP Gateway.

A Z-Wave app is installed in the tablet. The Z-Wave app discovers the Z/IP Gateway. The user includes a number of Z-Wave nodes. The user can control Z-Wave resources from the Z-Wave app.

3.1.1 Technical assumptions

1. Z/IP Gateway enables the WiFi interface using the SSID printed on the back of the router.
2. Z/IP Gateway creates a new IPv6 ULA prefix for the LAN interface when factory defaulted.
3. Z/IP Gateway creates a new IPv6 ULA prefix for the Z-Wave HAN when factory defaulted.
4. Z/IP Gateway announces the IPv6 prefix of the LAN subnet.
5. The tablet auto-configures an IPv6 address from the IPv6 LAN prefix.
6. Z/IP Gateway announces the IPv6 HAN subnet prefix.
7. Z/IP Gateway announces new Z-Wave resources via mDNS.
8. A Z-Wave app is available for the tablet.
9. The tablet app discovers Z-Wave resources via mDNS.
10. The tablet app controls Z-Wave resources and Z-Wave Network Management via Z-Wave commands carried Z/IP packets.

3.2 **Always online mode** (Control via ISP portal)

(Functionality covered by 3.1 is included but not described in this use case).

A new Customer Edge Router (CER) with built-in Z/IP Gateway is unboxed. The CER is connected to the ISP broadband cable. No LAN cable is connected.

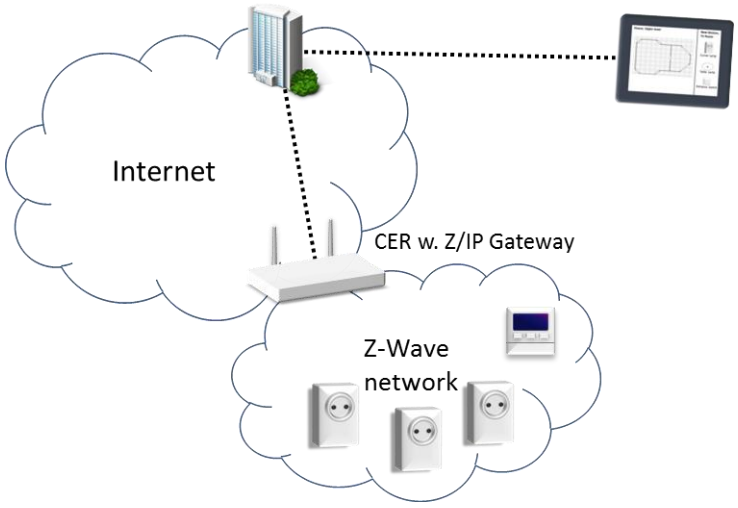

Figure 3, Always online mode

The CER automatically establishes internet access with the ISP backend.

The user navigates to the home control Portal in the Internet using a browser. The user creates a new user profile on the portal.
The user registers the Z/IP Gateway using the Remote Access code printed on the back of the CER.

The user includes a number of Z-Wave nodes. The user can control Z-Wave resources via the portal.

3.2.1 Technical assumptions

1. The CER implements firewall policies that by default deny inbound messages from the Internet [5], [6].
2. The CER DHCP server allocates IPv4 addresses for each Z-Wave node.
3. The Z/IP Gateway creates a secure tunnel to the portal using a pre-configured URL and keys.
4. The portal matches the user profile with the Z/IP Gateway Remote Access code.
   A security certificate confirms that this Z/IP gateway is the owner of this remote access code.
5. Classic web pages are served by the portal.
   Web pages are used to create a user profile, and manage and control Z-Wave resources.
6. Any web browser running on any client may be used to get access to the ISP portal.
7. No app is used and no web server is needed in the Z/IP Gateway
8. The user can only control Z-Wave resources when connected to the Internet.
9. No static IPv4 internet address is needed for the WAN interface.
10. No global IPv4 or IPv6 addresses are needed in the LAN.

3.3 **Legacy LAN** (Control via existing IPv4 LAN)

(Functionality covered by 3.1, 3.2 is included but not described in this use case).

A new Z/IP Gateway is unboxed.

The user connects the Z/IP Gateway LAN port to an existing router in the home.
The user connects a PC to a LAN port somewhere in the existing LAN.

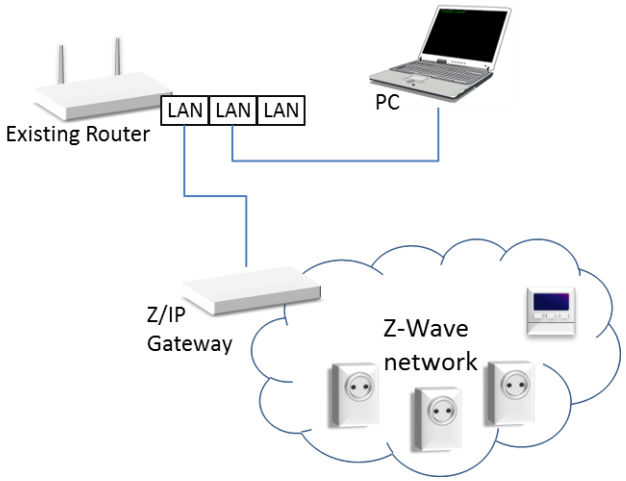

Figure 4, Legacy LAN

A Z-Wave application is installed in the PC. The application discovers the Z/IP Gateway. The user includes a number of Z-Wave nodes. The user can control Z-Wave resources from the application.

3.3.1 Technical assumptions

1. The Z/IP Gateway does not implement an IPv4 DHCP server or it is disabled.
2. The default gateway is announced via DHCPv4 by the existing router.
3. The Z/IP Gateway requests a new IPv4 address via DHCP for each new Z-Wave node added.
4. A new Z-Wave node is announced via mDNS.
5. Z-Wave nodes are reached using LAN addresses.

4 BACKBONE BOOTSTRAPPING FUNCTIONALITY

This chapter outlines how a Z/IP Gateway interfaces to a backbone network and enables communication to Z-Wave nodes from the backbone.

A Z/IP Gateway MUST support two usage configurations. Each configuration dictates allowed modes and support for a number of command classes.

1. **Service Provider Configuration (SP)**

   This configuration MUST limit the Z/IP Gateway to be operated in Portal Mode.
   It MUST NOT be possible to enable the Stand-Alone Mode

   a. Communication MUST use Secure Tunnel connection

   b. The Z/IP Gateway MUST accept the following command classes:

      - Z/IP Portal Command Class
      - Z/IP Gateway Command Class
      - Firmware Command Class

   c. If the Z/IP Gateway portal settings are locked, resetting it to factory default MUST NOT unlock it but the default firmware configuration MUST be restored.

2. **Consumer Electronics Configuration (CE)**

   This configuration MUST allow the Z/IP Gateway to be operated in either Portal Mode or Stand-Alone Mode.

   a. ***Portal Mode:***

   - The Z/IP Gateway MUST accept the following command classes via the Secure Tunnel connection,:

     - Z/IP Portal Command Class
     - Z/IP Gateway Command Class
     - Firmware Command Class

   - The Z/IP Gateway MUST accept the following command classes via local LAN access if the Z/IP Gateway is not locked:

     - Z/IP Portal Command Class
     - Z/IP Gateway Command Class
     - Firmware Command Class

   - The Z/IP Gateway MUST ignore the following command classes via local LAN access if the Z/IP Gateway is locked:

     - Z/IP Portal Command Class
     - Z/IP Gateway Command Class
     - Firmware Command Class

- Resetting the Z/IP Gateway to factory default MUST unlock it and the default firmware configuration MUST be restored. The default firmware configuration MAY make the Z/IP Gateway connect to a portal.

b. Stand-AIone Mode

- The Z/IP Gateway MUST accept the following command classes via the Secure Tunnel connection,:
    - Z/IP Portal Command Class
    - Z/IP Gateway Command Class
    - Firmware Command Class
- The Z/IP Gateway MUST accept the following command classes via local LAN access if the Z/IP Gateway is not locked:
    - Z/IP Portal Command Class
    - Z/IP Gateway Command Class
    - Firmware Command Class
- The Z/IP Gateway MUST ignore the following command classes via local LAN access if the Z/IP Gateway is locked:
    - Z/IP Portal Command Class
    - Z/IP Gateway Command Class
    - Firmware Command Class
- Resetting the Z/IP Gateway to factory default MUST unlock it and the default firmware configuration MUST be restored. The default firmware configuration MAY make the Z/IP Gateway connect to a portal.
- Resetting the Z/IP Gateway to factory default MUST NOT cause Z-Wave network parameters to be reset.

4.1 Factory defaulting a Z/IP Gateway

The following settings MUST be reset to their default values when a Z/IP Gateway is reset to factory defaults:

- Gateway mode.
- Gateway Peer Profile information.
- ZIP Gateway public certificate and private key.
- Portal CA certificate
- Gateway LAN address
- Gateway Portal prefix
- Default Gateway prefix
- Unsolicited IP address and port number

4.1.1 HAN settings

Z-Wave network parameters such as the NodeID and the HomeID MUST NOT be reset as part of the Z/IP Gateway factory default operation.

4.2 Operating a Z/IP Gateway in IPv4 environments

Due to the “NAT behind NAT” problem mentioned in section 2, it is RECOMMENDED that a Z/IP Gateway has no WAN port. If there is a WAN port, the user SHOULD be recommended only using the WAN port for connecting to a broadband modem or other Internet access devices.

The Z/IP framework natively maps a Z-Wave network into an IPv6 subnet. However, many consumer LANs use IPv4 and there is no routing protocol enabled. The average user is not able to create the required routing entries in the default gateway or in client devices.
To alleviate these issues, the Z/IP Gateway requests IPv4 addresses from the existing IPv4 network via DHCP and maps the IPv4 addresses to individual Z-Wave nodes. The IPv4 addresses may be private (NAT’ed) addresses [13] that cannot be accessed from the Internet. See section 5.2.4 for remote access.

The Z/IP Gateway implements an internal stateless NAT function from the LAN IPv4 address to the HAN ULA IPv6 address. The NAT function uses individual one-to-one address mappings in a table created during DHCP address allocation.
DHCP leases have to be refreshed to keep the claimed addresses. The typical lease time is 24 hours, which in DHCP means that the Z/IP Gateway tries to refresh the IPv4 addresses 12 hours after the most recent refresh.
The Z/IP Gateway indicates the preferred IPv4 address when refreshing the lease. There is a real risk that addresses are handed over to other LAN hosts if the Z/IP Gateway does not refresh the leases within the required interval, e.g. if the Z/IP Gateway is disconnected for a week.

4.3 Finding a Z/IP Gateway using mDNS

mDNS is a device discovery service standard defined by the IETF [17] [18]. Z/IP clients use mDNS to identify devices in the link-local domain and determine which Z-Wave command classes are supported by these devices via the Z-Wave service registered with the IETF.

4.4 Remote access from Portal

Customer premises are typically protected by a firewall built into the broadband router and most users have no means of controlling the firewall. For plug-and-play installation, the Z/IP Gateway performs firewall penetration from the inside by creating and maintaining a secure connection to a portal in the Internet.

To limit the number of support calls, Z/IP Gateways offered by a service provider may be preconfigured with the necessary URL, codes and certificates in order to automatically connect to the service provider portal as soon as an Internet connection is available.

5 REQUIREMENTS

This chapter presents requirements for Z/IP Gateway bootstrapping. The requirements are organized with reference to relevant interfaces and technologies.

5.1 WAN interface

A ZP Gateway SHOULD NOT feature a WAN port. However, the Z/IP Gateway may be an integrated component of a CER. In that case the CER MAY feature a WAN port dedicated to the Internet connection.

5.1.1 WAN DHCP Functionality

A WAN port MUST NOT enable address services such as DHCP or NDP at any time.
A Z/IP Gateway MUST NOT request IPv4 addresses for Z-Wave nodes via its WAN port.

5.2 LAN interface

A Z/IP Gateway MUST feature at least one LAN port for connecting to other LAN equipment in the consumer premises.

5.2.1 LAN addressing

A variety of IPv4 and IPv6 LAN addressing requirements must be met:

5.2.1.1 IPv4 DHCP Server

The Z/IP Gateway MAY be part of a CER. The CER SHOULD implement an IPv4 DHCP server.

The Z/IP Gateway MUST NOT enable a DHCP server after a factory default reset if it is not an integrated component of a CER.

5.2.1.2 LAN ULA IPv6 prefix allocation

The Z/IP Gateway MUST implement an IPv6 NDP service.

- New LAN and HAN IPv6 ULA prefixes MUST be auto-generated when the Z/IP Gateway resets the Z-Wave network parameters but MAY be specified manually by an administrator during operation.
  The ULA IPv6 prefixes MUST remain stable during the lifetime of Z-Wave Network.

- The Z/IP Gateway MUST advertise the LAN IPv6 ULA subnet prefix in an IPv6 NDP Prefix Information option to enable IPv6 address auto configuration.
  The Z/IP Gateway MUST advertise the HAN IPv6 ULA subnet prefix on the LAN in an IPv6 NDP Route Information option to enable host-based IPv6 routing.

- A Router Lifetime of 0 (zero) MUST be advertised for the HAN IPv6 ULA subnet prefix on the LAN in order to indicate that the Z/IP Gateway is useless as a default router to any other subnets than the HAN IPv6 ULA prefix.

5.2.1.3 Connecting to an existing LAN

A Z/IP Gateway may be added to an existing LAN.

If a routable IPv6 prefix is received from the network via IPv6 ND, the Z/IP Gateway LAN interface MUST join the advertised IPv6 network.

The Z/IP Gateway MUST implement an IPv4 DHCP client for requesting IPv4 addresses for individual Z-Wave nodes from a DHCP server in the network; e.g. the CER.

The Z/IP Gateway MUST request an IPv4 address for the Z/IP Gateway LAN interface via DHCP.

5.2.2 LAN Service Discovery support

A Z/IP Gateway MUST implement an mDNS responder service.

5.2.3 Secure Connection

The Z/IP Gateway must be able to exchange Z/IP Packets with other peers; Z/IP Gateways as well as portals.

The Z/IP Gateway MUST be able to initiate a secure connection to a preconfigured peer in order to penetrate any firewalls in consumer premises.
The Z/IP Gateway MUST support the Peer Set command of the Z/IP Gateway CC for definition of the peer profile to use.
TLS v1.1 over IPv4 TCP MUST be used for the secure connection.
The connection MUST be established with two-way handshake with RSA-1024 certificates and SHA-1 digest.
The Z/IP Gateway MUST establish the connection to port 44123 on the portal.
The Z/IP Gateway MUST transmit and accept IPv4 packets carrying tunneled IPv4 or IPv6 packets encrypted with AES-128.

NTP based time MUST be used for validation of certificates.

X509 [16] certificates MUST be used. Certificates and Keys MUST be either DER [20] or PEM [19] encoded.
DER encoded certificates and keys MUST be used on memory constrained ZIP Gateway platforms (e.g. ZIPR).

The Firmware Command Class MAY be used to update the certificates in the Z/IP Gateway

The following IPv6 packet format MUST be used for Z-Wave commands carried in Z/IP Packets transported via the secure connection:

IPv6 header [40 bytes]	**UDP header [8 bytes]**	**Z/IP Packet [N bytes]**

On successful connection, the Z/IP Gateway MUST send a keep-alive indication every 5 seconds.

The following keep-alive packet format MUST be used via the secure connection:

'K'	**'E'**	**'E'**	**'P'**	**'A'**	**'L'**	**'I'**	**'V'**	**'E'**	**'\0'**

The characters of the keep-alive packet MUST be encoded as ASCII upper case characters and terminated with the value 0 (zero).

The Z/IP Gateway MUST be able to establish a new connection in less than 4 minutes.
The Z/IP Gateway MUST be able to resume a broken connection in less than 10 seconds if the connection break occurred within the last 24 hours.

The Z/IP Gateway MUST attempt connection creation every 5 seconds if unconnected.

5.2.4 Remote access via Portal

The Portal MUST support TLSv1.1 cipher suites RSA-1024, AES-128 and HMAC-SHA1 [15]. The portal MUST hold X509 PEM encoded certificates and keys. The Z/IP Gateway CA public certificate MUST be included in the Portal trusted CA list and similarly, the portal CA public certificate MUST be included in the Z/IP Gateway trusted CA list. It is RECOMMENDED that a self-signed CA certificate is used.

If the “LAN IPv6 Address” was configured as all-zeroes in the previous Z/IP gateway Configuration Set command, the portal MUST initiate a Z/IP gateway discovery process (as described in section 5.2.2). Discovery packets MUST be sent with IPv6 UDP encapsulation through the secure connection.

The secure connection method described in 5.2.3 MUST be used for remote access to Z-Wave resources from a Portal.

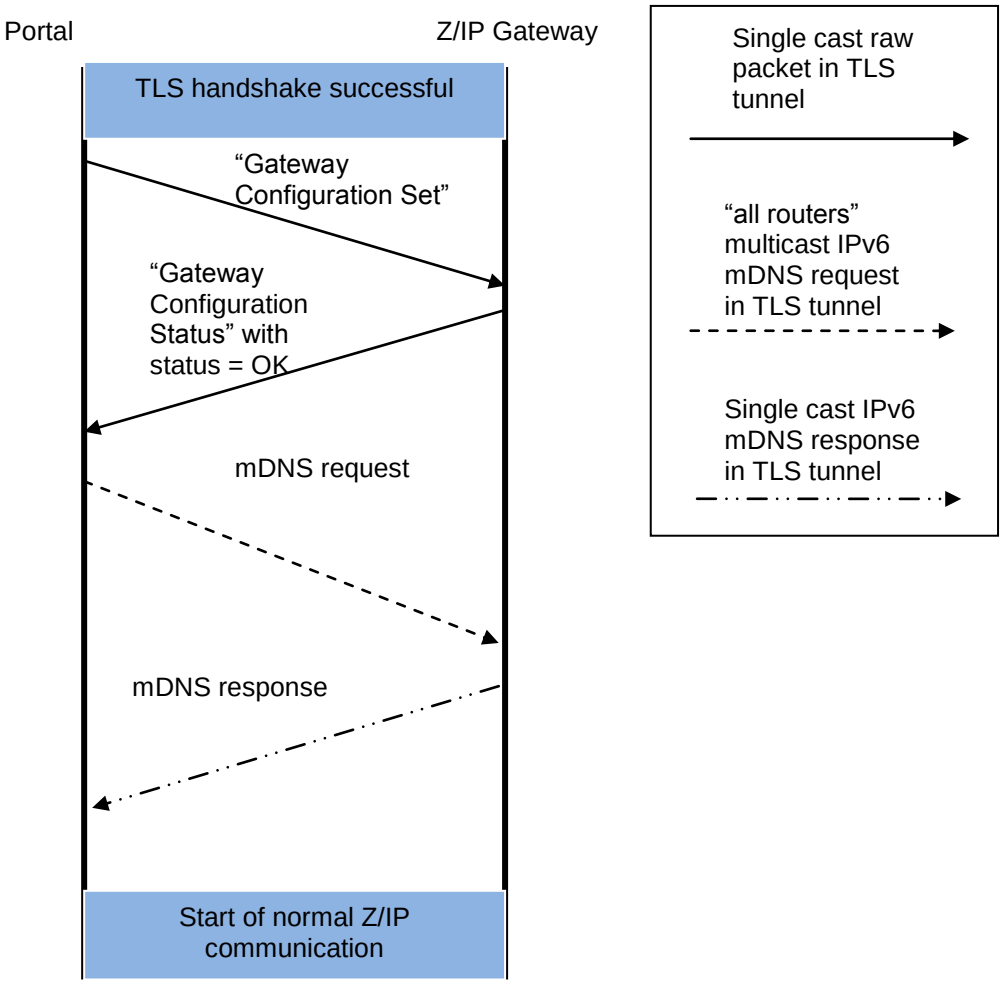

Figure 5 Frame flow between Portal and Z/IP Gateway

5.2.4.1 Choosing an interface for portal communication

If the Z/IP Gateway implements a WAN port and this WAN port is providing external connectivity, the Z/IP Gateway MUST use the WAN port for contacting the service provider portal.

If the Z/IP Gateway does not implement a WAN port the Z/IP Gateway MUST use the LAN port for contacting the service provider portal via the default gateway.

5.2.4.2 Pre-defined URL for portal communication

The Z/IP Gateway MUST support the Z/IP Gateway and Portal Command Classes.

When the Gateway Mode has been set to "Portal", the Z/IP Gateway MUST automatically establish a secure tunnel to the portal as soon as an internet connection is available.

After successful creation of a secure connection, the Z/IP Gateway MUST wait for a configuration block pushed from the portal. The configuration block MUST be pushed using the Gateway Configuration Set command of the Z/IP Portal CC.

The Z/IP Gateway MUST NOT accept any other communication via the secure portal connection before a valid configuration block has been received.

5.2.4.3 Authenticated Z/IP Gateway registration with portal

A unique remote access code helps the user identifying the Z/IP Gateway towards the portal and enables secure key exchange between portal and Z/IP Gateway.

The remote access code MUST be bundled with the certificate which is exchanged during creation of the secure tunnel. The remote access code and an associated 8 byte PIN code MUST be carried in the "Serial Number" field of the certificate along with 4 bytes of certificate serial number.

Certificate serial # (s4-s3-s2-s1)	Remote Access Code (EUI-64) (o3-o2-o1-FF-FF-m3-m2-m1)	Pin # (p8-p7-p6-p5-p4-p3-p2-p1)
4 bytes	8 bytes	8 bytes

The s4 byte is transmitted first and is the most-significant byte of the certificate serial number. The o3 byte is the most-significant byte of the Remote Access Code and p8 is the most significant byte of the Pin Code.

The Certificate serial # bytes s4-s1 MAY be encoded using any binary value with one exception: The s4 byte MUST have a value in the range 0x01..0x7F.

The Remote Access Code byte o3-m1 MUST be an IEEE MAC-48 identifier formatted as an IEEE EUI-64 identifier. An IEEE EUI-64 MUST be formed from an IEEE MAC-48 identifier by inserting the 16-bit value 0xFFFF in between the OUI-24(o3-o1) and the manufacturer-assigned serial number (m3-m1):

Remote Access Code (EUI-64) (o3-o2-o1-FF-FF-m3-m2-m1)

The bytes p1-p8 MUST be in the range 0x30..0x39, 0x41..0x5A, i.e. ASCII characters '0'..'9','A'..'Z'.

The Remote Access Code and Pin code MUST be available in printed documentation; preferably as a label on the Z/IP Gateway. The Pin code MUST be used during account registration to verify that it is the rightful owner of the Remote Access Code which is registering the device.

The Remote Access Code SHOULD be presented to the user as two hex characters per byte; using the ASCII characters '0'..'9','A'..'F', e.g. 001E32FFFF005976.

The Pin code SHOULD be presented to the user as 8 uppercase alphanumerical characters; using the ASCII characters '0'..'9','A'..'F', e.g. 17YH8TWQ.

A QR code SHOULD be available in printed documentation; containing a unique URL to the service provider portal that includes the Remote Access Code and the Pin code. If the user scans the QR code, a browser is opened directly into a wizard page for creation of a new user profile – or the user is directed to the login page if the remote access code has already been registered by the user.

5.2.4.4 Portal configuration support

5.3 Wireless LAN Interface (WiFi)

A Z/IP Gateway MAY incorporate a WiFi access point.
If available, the WiFi access point MUST be enabled by default. The interface MUST provide a bridged connection to the LAN port.

The sections below explicitly describe areas where the wireless LAN port MUST operate differently than specified in section 5.2.

5.3.1 WiFi Identification

A unique SSID helps the user determining which WiFi network to connect to.

The SSID of the WiFi network MUST be a unique label that can be recognized by the user. The RECOMMENDED label for the SSID is “ZIPxxxxxx” where “xxxxxx” is the WiFi MAC address of the Z/IP Gateway. Whichever SSID is used, the SSID MUST be available in printed documentation; preferably as a label on the Z/IP Gateway. It MUST be possible for an administrator to change the SSID.

All values described above MUST be restored during a factory default reset operation.

5.3.2 WiFi Security

WPA2 encryption MUST be enabled. The WPA2 passphrase MUST be a unique label. The RECOMMENDED WPA2 passphrase is a unique string for each Z/IP Gateway.
Whichever passphrase is used, the passphrase MUST be available in printed documentation; preferably as a label on the Z/IP Gateway.
It MUST be possible for an administrator to change the WPA2 passphrase.

The default administrator username SHOULD be a unique string for each Z/IP Gateway.
It SHOULD be possible to change the administrator username.

The default administrator password MUST be a unique string for each Z/IP Gateway. The administrator password SHOULD NOT be based on the serial number of the Z/IP Gateway.
Whichever default administrator password is used, the default administrator password MUST be available in printed documentation; preferably as a label on the Z/IP Gateway.
It MUST be possible for an administrator to change the password.

All values described above MUST be restored during a factory default reset operation.

5.4 HAN Interface

This section presents requirements specific to the HAN IP interface providing connectivity to the Z-Wave network.

5.4.1 HAN ULA IPv6 prefix allocation

Refer to section 5.2.1.2.

5.4.2 HAN node IPv4 connectivity

While the global IPv4 address pool has been exhausted, the majority of private networks may continue to run IPv4 for many years thanks to private addresses [12] and NAT [13]. Support for IPv4 is needed to ensure plug-and-play operation of Z/IP Gateways in existing IPv4 environments.

The Z/IP framework implements native IPv6 resources with ULA IPv6 addresses.
IPv4 connectivity to Z/IP resources MUST be provided via IPv4/IPv6 packet conversion and address translation.

5.4.2.1 IPv4 address allocation for a new Z-Wave node

A Z/IP Gateway only has one MAC address in the LAN. DHCP allows the Z/IP Gateway to represent multiple IPv4 addresses with just one MAC address.

The Z/IP Gateway MUST issue LAN DHCPv4 requests via the LAN interface to obtain an IPv4 address when a new node is added to the Z-Wave network.

The LAN DHCPv4 request MUST incorporate a “client identifier” [7]. The “client identifier” MUST be constructed by concatenating the lower case string “zw”, the HomeID represented as 8 lower case hex characters and the nodeID represented as 2 lower case hex characters.

The Z/IP Gateway MUST maintain DHCP leases by refreshing leases as defined in [7]. If leases have timed out, e.g. because of connection loss to the DHCP server or because the Z/IP Gateway has rebooted, the Z/IP Gateway MUST re-issue a DHCP request.

After a reboot the Z/IP Gateway MUST re-claim all IPv4 addresses from the LAN DHCPv4 server. This DHCP request MUST include the IPv4 address that was used until the DHCP lease timed out. The Z/IP Gateway MUST check if a new IPv4 address was assigned.

5.4.2.2 Leaving the network

If a Z-Wave node is removed from the network by the ZP Gateway, and the node has DHCP assigned addresses, the Z/IP Gateway MUST issue a DHCPRELEASE message [7] for the IP address of that node.

REFERENCES

[1] IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.
[2] Internet Assigned Numbers Authority, http://www.iana.org/
[3] IETF RFC 4443, Internet Control Message Protocol (ICMPv6), March 2006
[4] IETF RFC 1981, Path MTU Discovery for IP version 6
[5] NIST advisory CVE-2007-1338
[6] IETF RFC 6092, Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
[7] IETF RFC 2131, Dynamic Host Configuration Protocol
[8] IETF RFC 3633, IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
[9] IETF RFC 4861, Neighbor Discovery for IP Version 6 (IPv6)
[10] IETF RFC 4193, Unique Local IPv6 Unicast Addresses
[11] IETF RFC 6296, IPv6-to-IPv6 Network Prefix Translation
[12] IETF RFC 1918, Address Allocation for Private Internets
[13] IETF RFC 3022, Traditional IP Network Address Translator (Traditional NAT)
[14] IETF RFC 4191, Default Router Preferences and More-Specific Routes
[15] IETF RFC 4346 , The Transport Layer Security (TLS) Protocol Version 1.1
[16] IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[17] IETF RFC6763, DNS-Based Service Discovery
[18] IETF RFC6762, Multicast DNS
[19] IETF RFC 1421, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures
[20] Distinguished Encoding Rules (DER), Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), ITU-T