Software Design Specification

Z-Wave Network-Protocol Command Class Specification

Document No.:	SDS13784
Version:	8
Description:	The document describes the Z-Wave Command Classes and associated Commands used by Z-Wave enabled products at the Network and Protocol level.
Written By:	JFR;NOBRIOT;BBR;DEWASSIE
Date:	2019-01-04
Reviewed By:	BBR;JFR;NOBRIOT;SAMBAT;KMALMKJAER;JRM;DEWASSIE
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2019-01-04	09:41:08	NTJ	Niels Johansen	

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20170102	NOBRIOT	ALL 4.7 4.10 4.12 4.1 4.4	Transferred content from [2] and [3] Integrated approved content from Open Review 2016C and 2016D: • Updated the Powerlevel Command Class • Clarified Z/IP Command Class regarding how to handle conflicting encapsulation settings Added the Z/IP 6LoWPAN Command Class Added the Inclusion Controller Command Class Added the version 2 of some of the Network Management Command Classes
2	20170402	NOBRIOT	4.4.11	Integrated approved content from Open Review 2017A: • Obsoleted the Network Management Primary Command Class, version 1
3	20170702	NOBRIOT	4.1 4.6 4.4.10 4.4.13	Moved IP Association and Z/IP Naming and Location to [15] Integrated approved content from 2017B Open Review: • Clarified Inclusion Controller Command Class regarding how to advertise it in the NIF depending on the node's network role. Added Node Provisioning Command Class, version 1 Added Network Management Inclusion Command Class, version 3 Added Network Management Installation and Maintenance, version 2
4	20171002	NOBRIOT	4.1 4.6	Added clarifications for Inclusion Controller Command Class and Node Provisioning Command Class
5	20180110	NOBRIOT	4.9 & 4.10 4.11 4.4.6.8 & 4.4.8.15 4.4.7.3 4.6 4.13, 4.14 & 4.15	Integrated approved content from Open Review 2017D: • Refactored and clarified Z/IP Command Class, version 2 and 3 • Added Z/IP Command Class, version 4 • Clarified Network Management Basic Node Command Class, version 1 and Network Management Inclusion Command Class, version 1 regarding when Learn Mode and Add Mode interruption attempt may be ignored • Added a missing byte in the Learn Mode Set Status Command frame format • Removed Node Provisioning Command Class from the beta state and adjusted TLV names and requirements • Clarified Z/IP Gateway Command Class, Z/IP ND Command Class and Z/IP Portal Command Class regarding Z/IP Packet encapsulation
6	20180305	BBR	All	Added Silicon Labs template
7	20180409	NOBRIOT	4.4.1	Integrated approved content from Open Review 2018A: • Clarified how to handle network management CCs and secondary network role.
8	20190101	DEWASSIE	4.4.13	Contributions 2018D: • Removed a non-valid requirement in Network Management Installation and Maintenance Command Class

Table of Contents

Table of Figures

Table of Tables

1 ABBREVIATIONS

Abbreviation	Explanation
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
LSB	Less significant bit
mDNS	Multicast DNS
MSB	Most significant bit
NIF	Node Information Frame
NOP	No Operation (Command Class)
PAN	Personal Area Network
WAN	Wide Area Network
Z/IP	Z-Wave for IP

2 INTRODUCTION

Commands classes are divided in four categories:

- Application Command Classes [16]
- Management Command Classes [15]
- Transport-Encapsulation Command Classes [14]
- Network-Protocol Command Classes

The list of defined Command Classes with their associated category is available in [13].

This document describes the Command Classes designed for Network or Protocol specific purposes. It includes any command class used for:

- Network or protocol management
- Bridging or Z/IP communication
- RF related operations

Read this document in conjunction with [1] for Z-Wave devices and [10] for Z-Wave Plus devices.

2.1 Precedence of definitions

Device Class, Device Type and Command Class Specifications approved as final version during the Device Class, Device Type and Command Class Open Review process have precedence over this document until integrated into this document.

2.2 Terms used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document MUST be interpreted as described in IETF RFC 2119 [6].

Statements containing the IETF RFC 2119 [6] key words are at times marked with unique requirement numbers in the margin. The requirements numbers have the following syntax: CC:xxxx.xx.xx.xx.xxx with each x being an hexadecimal digit.

This document defines functionalities as deprecated or obsoleted.

The term "obsolete" means that the functionality MUST NOT be supported in new implementations applying for certification.

A controller SHOULD provide controlling capabilities of the actual functionality for backwards compatibility with legacy devices.

The term "deprecated" also indicates an obsolete definition, but it permits new implementations applying for certification.

Thus, the term “deprecated” means that the functionality SHOULD NOT be supported in new implementations applying for certification. Often, another substitute functionality is REQUIRED if the deprecated functionality is implemented.

A controller SHOULD provide controlling capabilities of the actual functionality for backwards compatibility with legacy devices.

3 COMMAND CLASS OVERVIEW

General Command Class overview and rules are described in the Application Command Class Specification [16] and are valid for the Command Classes presented in this document..

No additional considerations apply for the Network-Protocol Command Classes.

4 COMMAND CLASS DEFINITIONS

The following subchapters contain definitions of Network and Protocol Command Classes.

4.1 Inclusion Controller Command Class, version 1

The Inclusion Controller Command Class is used after a node's network inclusion between the SIS and an inclusion controller to inform each other of the remaining setup required for the included node.

Examples of such setup operations could be Z-Wave Plus Lifeline configuration or Security 2 bootstrapping.

If the S2 bootstrapping is handled by a SIS after the Z-Wave network inclusion has been handled by an inclusion controller, the joining node will detect two different NodeIDs for Network inclusion and S2 bootstrapping. The NodeID of the including controller is not relevant for the authentication of the joining node. Therefore, the joining node MUST NOT abort the S2 bootstrapping in response to a changing NodeID.

CC:0074.01.00.11.001

CC:0074.01.00.11.002 The SIS, inclusion controller and joining node MUST follow the frame flow illustrated in Figure 1.

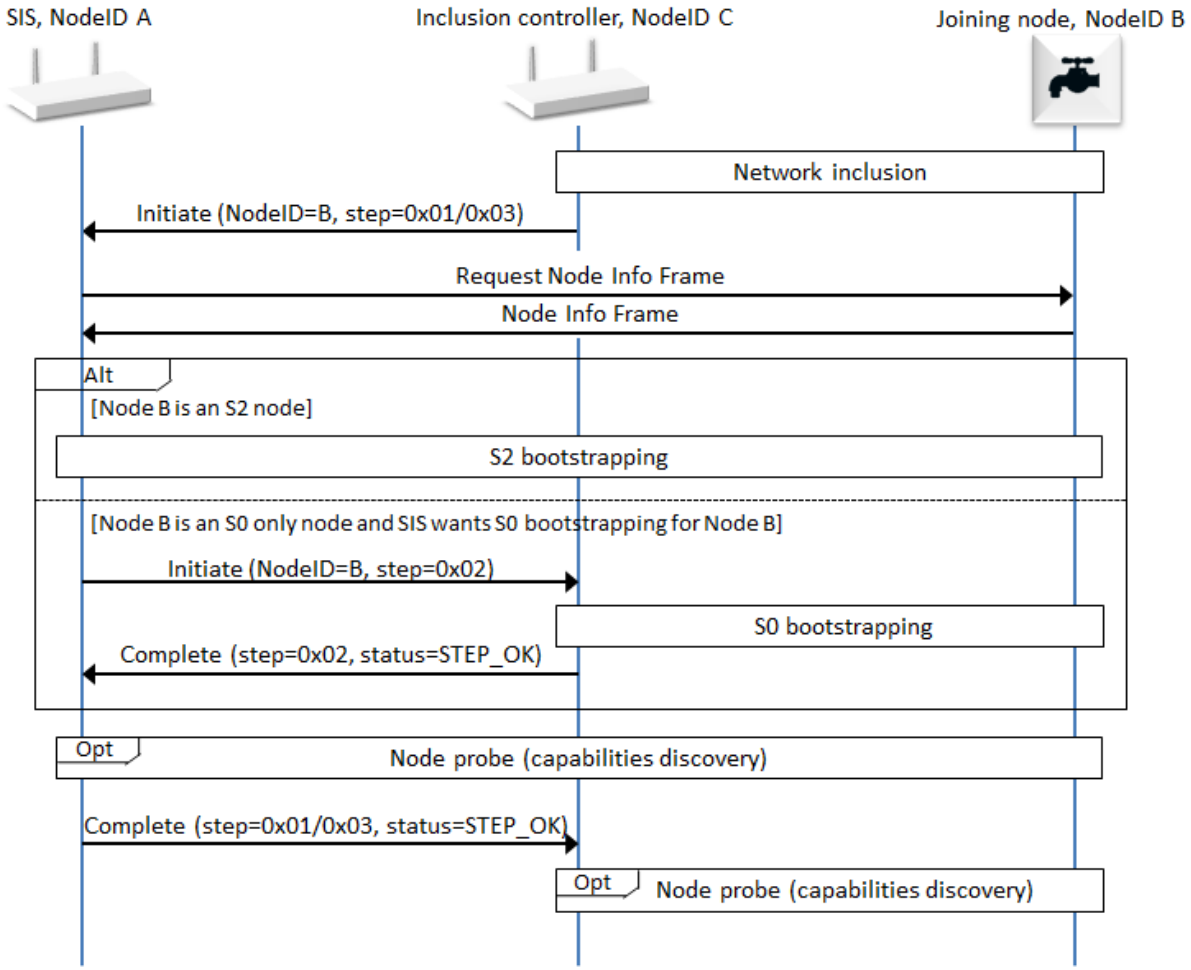

Figure 1 Inclusion Controller frame flow

CC:0074.01.00.11.003 The SIS, inclusion controller and joining node MUST comply with the following steps:

1. **Inclusion Controller, C,** performs network inclusion of Joining Node, B.
2. CC:0074.01.00.11.004 **Inclusion Controller, C,** MUST send Inclusion Controller Initiate to SIS, A, immediately following the network inclusion.
3. CC:0074.01.00.11.005 **SIS, A,** MUST request a Node Info Frame from Joining Node, B.
4. CC:0074.01.00.11.006 **Joining Node, B,** MUST respond to SIS, A, with a Node Info Frame

Option 1: If Joining Node B supports S2:

5. CC:0074.01.00.11.007 **SIS, A,** MUST start the Security 2 bootstrapping as described in Security 2 Command Class [14], including user dialogs.
6. CC:0074.01.00.11.008 **Joining Node, B,** MUST accept being S2 bootstrapped by the SIS

Option 2: If Joining Node, B does not support S2 and supports S0

7. If **SIS, A** wants S0 bootstrapping performed for **Joining Node, B**, it will send an Inclusion Controller Initiate(S0_INCLUSION) to **Inclusion Controller, C**
8. CC:0074.01.00.11.00A **Inclusion Controller, C** MUST perform S0 bootstrapping if it has the S0 network key after receiving Inclusion Controller Initiate(S0_INCLUSION)
9. CC:0074.01.00.11.00B **Inclusion Controller, C** MUST return an Inclusion Controller Complete to **SIS, A** to indicate if S0 bootstrapping attempt took place and if it was successful.

Following the Security bootstrapping, regardless whether it failed, successful or was not applicable:

10. CC:0074.01.00.12.001 **SIS, A,** SHOULD perform any probing needed of the Joining Node, B.
11. CC:0074.01.00.11.009 **SIS, A,** MUST send an Inclusion Controller Complete Command to the Inclusion Controller, C.
12. CC:0074.01.00.12.002 **Inclusion Controller, C,** SHOULD perform any probing needed of the Joining Node, B.

4.1.1 Compatibility Considerations

4.1.1.1 Node Information Frame (NIF)

CC:0074.01.00.21.002 A supporting node MUST always advertise the Inclusion Controller Command Class in its NIF, regardless of the security bootstrapping outcome when having the SIS or Inclusion Controller role.

CC:0074.01.00.23.001 A supporting node MAY keep or remove the Inclusion Controller Command Class in/from its NIF if it has the primary or secondary controller role.

4.1.1.2 Legacy controllers

If an Inclusion Controller that does not support the Inclusion Controller Command Class includes a new node in a network, the SIS will never receive an Inclusion Controller Initiate Command.
CC:0074.01.00.22.001 If no Initiate Command has been received approximately 10 seconds after a new node has been added to a network, the SIS SHOULD start interviewing the newly included node (step 10 above).

CC:0074.01.00.21.003 If an Inclusion Controller includes a node and the SIS does not support the Inclusion Controller Command Class, the Inclusion Controller MUST perform S0 bootstrapping immediately after inclusion if applicable.

4.1.2 Inclusion Controller Initiate Command

This command is used to ask a receiving node to perform specific steps in the inclusion/bootstrapping process.

The initiate command asks the controller to perform a specific step of the inclusion process. The Inclusion Controller Initiate Command is first sent from an inclusion controller to the SIS, then the SIS MAY choose to perform the rest of the inclusion by itself or it MAY ask the inclusion controller to perform one or more of the inclusion steps.

CC:0074.01.01.13.001

CC:0074.01.01.11.001 This command MUST be sent through highest common Security Class of the SIS and Inclusion Controller, if no common Security Class exists, non-secure is allowed. Inclusion Controllers MUST send this command following a successful network inclusion.

CC:0074.01.01.11.002 This command MUST NOT be issued via multicast addressing.
A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_INCLUSION_CONTROLLER							
Command = INITIATE							
Node ID							
Step ID							

Node ID

CC:0074.01.01.11.003 This field is used to indicate the NodeID of the node being included.
The receiving node MUST perform the steps on the NodeID indicated by this field

Step ID

CC:0074.01.01.11.004 This field is used to indicate which step is to be performed on the specified.
The field MUST comply with Table 1

Table 1, Inclusion Controller Initiate::Step ID encoding

Value	Identifier	Description
0x01	PROXY_INCLUSION	This value MUST be used only when: • The sending node is the inclusion controller • The receiving node is the SIS This value is used to indicate the SIS that it MUST take over the node inclusion and perform S2 bootstrapping if relevant. The SIS MUST return an Inclusion Controller Complete Command when the step has been completed. The SIS MAY ask the inclusion controller to perform some of the steps by itself before returning an Inclusion Controller Complete Command.
0x02	S0_INCLUSION	This value MUST be used only when: • The sending node is the SIS • The receiving node is the inclusion controller This value is used to indicate to the inclusion controller that it MUST perform S0 bootstrapping. The inclusion controller MUST reply with an Inclusion Controller Complete Command when the S0 bootstrapping has been performed (or attempted).
0x03	PROXY_INCLUSION_REPLACE	This value MUST be used only when: • The sending node is the inclusion controller • The receiving node is the SIS This value is identical to PROXY_INCLUSION but is used in case the newly included node has replaced a failed node. This value is used to indicate the SIS that it MUST take over the node inclusion and perform S2 bootstrapping if relevant. The SIS MUST return an Inclusion Controller Complete Command when the step has been completed. The SIS MAY ask the inclusion controller to perform some of the steps by itself before returning an Inclusion Controller Complete Command.

All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.1.3 Inclusion Controller Complete Command

CC:0074.01.02.11.001 This command MUST be sent after a controller has completed the requested inclusion steps.

CC:0074.01.02.11.002 This command MUST be sent using the highest common Security Class of the SIS and Inclusion Controller. If no common Security Class exists, non-secure transmission is allowed.

CC:0074.01.02.11.003

CC:0074.01.02.11.004 An inclusion controller MUST perform optional node interview after receiving a Inclusion Controller Complete Command with Step ID, PROXY_INCLUSION. A SIS MUST do its device probe before sending the COMPLETE command with step ID PROXY_INCLUSION.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_INCLUSION_CONTROLLER							
Command = COMPLETE							
Step ID							
Status							

Step ID

This field is used to indicate the step that has been completed.

CC:0074.01.02.11.005 A sending node MUST set this field to the same value as the last received Inclusion Controller Initiate Command.

Status

CC:0074.01.02.11.006 This field is used to indicate the status of the advertised Step ID.
It MUST comply with Table 2.

Table 2, Inclusion Controller Complete::Status encoding

Value	Status CODE identifier	Description
0x01	STEP_OK	The performed step was completed without error.
0x02	STEP_USER_REJECTED	The step was rejected by user
0x03	STEP_FAILED	The step failed, because of a communication or protocol error.
0x04	STEP_NOT_SUPPORTED	The step failed, because it Is not supported by the sending node.

All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.2 IP Configuration Command Class, version 1 [OBSOLETED]

THIS COMMAND CLASS HAS BEEN OBSOLETED

New implementations MUST NOT use the IP configuration Command Class. Refer to the Z/IP and Network management Command Classes.

The IP Configuration Command Class is used to configure network identifiers for IPV4 devices. The intended use of the command class is illustrated in the figure below.

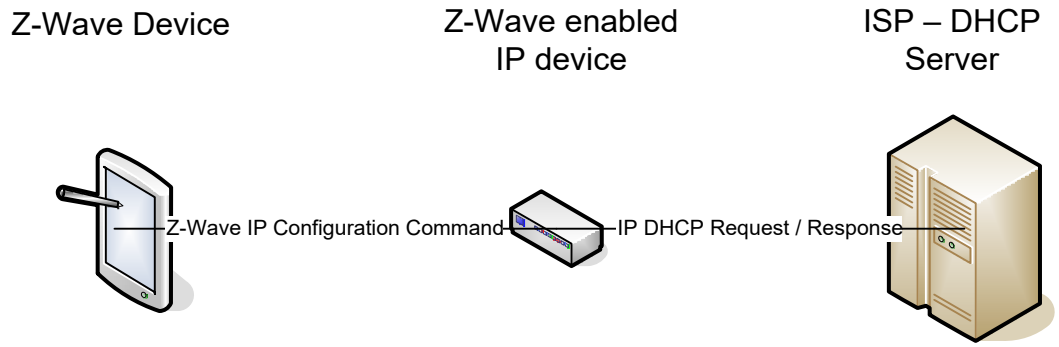

Figure 2, Configuration of network identifiers for IPV4 devices

In the figure the Z-Wave Remote to the left, sends an IP Configuration Command to the Z-Wave enabled IP device, telling it to acquire its configuration using DHCP. The Z-Wave enabled IP device will now perform a standard DHCP IP request to the DHCP server over an IP based network.

Another example might be where the Z-Wave Remote statically configures the Z-Wave enabled IP device with fixed IP, subnet, DNS etc. by sending an IP Configuration Command.

Note that this class is only intended for IPV4 and not IPV6 support.

4.2.1 IP Configuration Set Command

The IP Configuration Set Command used to configure IPV4 settings in a device.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_IP_CONFIGURATION							
Command = IP_CONFIGURATION_SET							
Reserved						Auto IP	Auto DNS
IP Address 1							
IP Address 2							
IP Address 3							
IP Address 4							
Subnet Mask 1							
Subnet Mask 2							
Subnet Mask 3							
Subnet Mask 4							
Gateway 1							
Gateway 2							
Gateway 3							
Gateway 4							
DNS1 1							
DNS1 2							
DNS1 3							
DNS1 4							
DNS2 1							
DNS2 2							
DNS2 3							
DNS2 4							

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Auto IP (1 bit)

If Auto IP bit is set, the following fields are ignored: IP Address, Subnet Mask, and Gateway. And are allocated by DHCP or BOOTP instead.

Auto DNS (1 bit)

The Auto DNS if set indicates to ignore DNS1 and DNS2 and allocate DNS by DHCP instead. Note that some devices might not support Auto DNS without Auto IP set.

IP Address (32 bits)

The IP Address indicates the static IP address of the device itself. The first byte is the most significant byte.

Subnet mask (32 bits)

The Subnet Mask determines the portion of the IP address that represents the subnet. The first byte is the most significant byte.

Gateway (32 bits)

The Gateway indicates the default gateway that serves as an access point to another network. The first byte is the most significant byte.

DNS1 (32 bits)

The DNS1 allows the use of domain name system (DNS) server names instead of using numerical IP addresses for management packet routing. In case the device will not need DNS, and SHOULD NOT query it from DHCP then leave field as all zeroes. The first byte is the most significant byte.

DNS2 (32 bits)

The DNS2 provides a secondary DNS server name. In case only one DNS server is available or the device will not need DNS then leave field as all zeroes. The first byte is the most significant byte.

4.2.2 IP Configuration Get Command

The IP Configuration Get Command is used to request the IPV4 settings in a device.

The IP Configuration Report Command MUST be returned in response to this command.

This command MUST NOT be issued via multicast addressing.
A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_IP_CONFIGURATION							
Command = IP_CONFIGURATION_GET							

4.2.3 IP Configuration Report Command

The IP Configuration Report Command used to return IPV4 settings in a device.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_IP_CONFIGURATION							
Command = IP_CONFIGURATION_REPORT							
Reserved						Auto IP	Auto DNS
IP Address1							
IP Address2							
IP Address3							
IP Address4							
Subnet Mask1							
Subnet Mask2							
Subnet Mask3							
Subnet Mask4							
Gateway1							
Gateway2							
Gateway3							
Gateway4							
DNS11							
DNS12							
DNS13							
DNS14							
DNS21							
DNS22							
DNS23							
DNS24							
LeaseTime1							
LeaseTime2							
LeaseTime3							
LeaseTime4							

Refer to explanation of parameters in IP Configuration Set Command description.

Lease Time (32 bits)

The lease time specifies the time the IP address has been granted, if Auto IP is being used (in seconds). If the device does not know its lease period it MUST return 0 for the lease time fields.

4.2.4 IP Configuration DHCP Release Command

The IP Configuration DHCP Release Command used to release the DHCP lease.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_IP_CONFIGURATION							
Command = IP_CONFIGURATION_RELEASE							

4.2.5 IP Configuration DHCP Renew Command

The IP Configuration DHCP Renew Command used to force the renewal of the DHCP lease.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_IP_CONFIGURATION							
Command = IP_CONFIGURATION_RENEW							

4.3 Mailbox Command Class, version 1

The Mailbox Command Class is intended for IP based gateway deployments with distributed mailbox resources. One example is a constrained gateway device which is offloaded by another IP host with sufficient memory to host the Mailbox Service. The Mailbox Service may be hosted by a LAN host or an Internet server.

The Mailbox Command Class allows any mailbox capable device to either make itself into a Mailbox Service, or utilize another Mailbox Service in the network.

4.3.1 Mailbox Framework

The Mailbox Command Class describes a framework that consists of two specific Mailbox Modes described below:

1. **Mailbox Proxy,** which forwards mailbox requests to a Mailbox Service.
2. **Mailbox Service,** which accepts the forwarded mailbox requests and stores them until the designated recipient announces that it is awake.

A mailbox device MAY support one or both of the two Mailbox Modes. However, a mailbox device MUST NOT take both Mailbox Modes in a network.

Before configuring Mailbox Proxy forwarding, a configuring node MUST ensure that the forwarding and receiving devices support their respective required modes. The information can be found using the Mailbox Configuration Get Command and Mailbox Configuration Report Command.

4.3.1.1 Mailbox Proxy

The Mailbox Proxy device forwards all received frames that are destined for a non-listening node to the configured Mailbox Service. Before forwarding the frame, it MUST be attempted to send the frame to the node first as it may be awake following a manual activation or inclusion. If the Mailbox Proxy can deliver the frame to the non-listening node, the Mailbox Proxy MUST NOT forward the frame to the Mailbox Service.

The Mailbox Proxy MUST support the Wake Up Command Class.

4.3.1.2 Mailbox Service

The Mailbox Service serves as a conventional mailbox, with the addition that it may receive forwarded frames from a Mailbox Proxy. A Mailbox Service may have a finite mailbox queue capacity, which is reported in the Mailbox Configuration Report. The Mailbox Service MUST NOT communicate with a Z/IP client directly, since it may not be able to route messages to the client.

4.3.1.3 Frame flow

Figure 3 illustrates the communication between a Z/IP Client (1) attempting communication to a non-listening node (4). The communication is passing through the Mailbox Proxy (2) which initially will attempt direct communication with (4). If failing to reach (4), the frame will be forwarded to the Mailbox Service (3) using the Mailbox Queue Command with Push Operation.

Following the Mailbox Queue push, the Mailbox Service will send a Mailbox Queue Command with Waiting Operation to the proxy, piggybacking the original UDP command on the message. The Proxy will build a “NACK Waiting” Z/IP Command targeted for the Z/IP node, based on the piggy backed message from the Proxy Service. The Proxy Service MUST also append the Expected Delay header extension to the “NACK Waiting” Z/IP Command. This step MUST be repeated every 60s seconds as long as the message is in the mailbox.

Upon wake-up, the non-listening node (4) will transmit a Wake Up Notification to the Mailbox Proxy (2), which must be configured using the Wake Up Command Class. Whenever the Mailbox Proxy (2) receives a Wake Up Notification, the notification will be forwarded as a Z/IP Packet to the Mailbox Service (4). The Mailbox Service inspects the queue to see if there are any frames for (4) and responds with either an empty Mailbox Queue Command Pop operation with “Last” bit set to 1 or any frames that may be in queue, finishing with the last frame having “Last” bit set to 1.

Mailbox Proxy (2) receives the Mailbox Queue Pop frame on which it performs a Virtual Node Rewrite to match the original sender of the UDP frame of the Mailbox Queue Pop command. The frame is sent from the virtual node to (4) followed by a “Wake Up No More Information” Command. Any eventual reports will be replied to the virtual node that forwards them to (1). The proxy MUST send a Mailbox Queue Command with ACK operation to the Proxy Service when it has delivered the frame and potentially the “No more information”

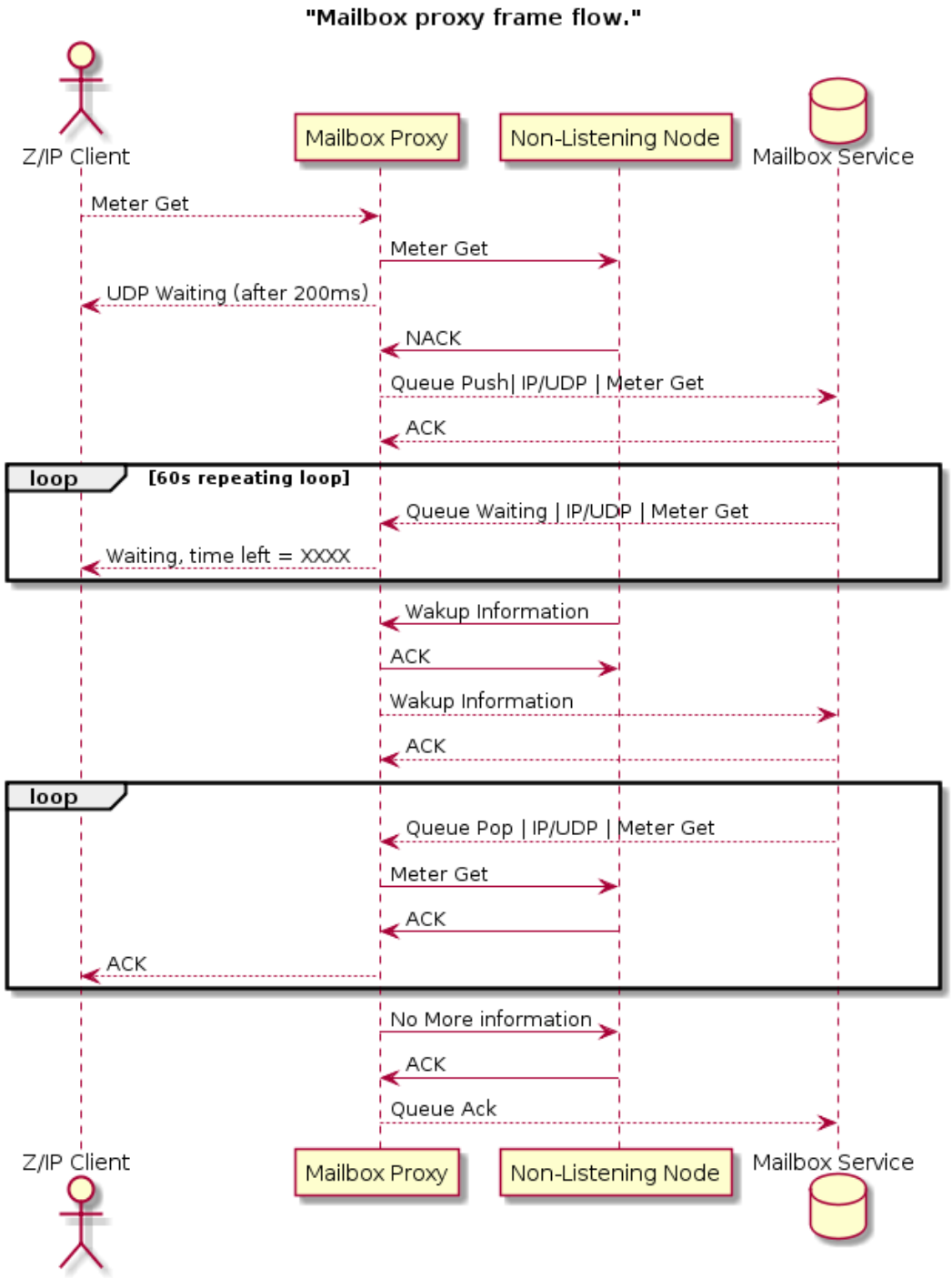

Figure 3, Mailbox Frame flow

4.3.2 Mailbox Configuration Get Command

The Mailbox Configuration Get Command is used to request the Mailbox configuration from a supporting device.

The Mailbox Configuration Report command MUST be returned in response to a Mailbox Configuration Get command.

This command MUST NOT be issued via multicast addressing.
A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_MAILBOX							
Command = MAILBOX_CONFIGURATION_GET							

4.3.3 Mailbox Configuration Set Command

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_MAILBOX							
Command = MAILBOX_ CONFIGURATION_SET							
Reserved					Mode		
Forwarding Destination IPv6 Address – Byte 1							
…							
Forwarding Destination IPv6 Address – Byte 16							
UDP Port Number - Byte 1							
UDP Port Number - Byte 2							

Reserved (5 bits)

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Mode (3 bits)

The Mode field is used to advertise the Mailbox mode to be configured in the node. This field MUST be encoded according to Table 3.

Table 3, Mailbox Configuration Set::Mode encoding

Value	Description
0x00	Disable Mailbox Service Disable Mailbox Proxy forwarding
0x01	Enable Mailbox Service
0x02	Enable Mailbox Proxy forwarding

Forwarding Destination IPv6 Address (16 bytes)

If the Mailbox Proxy Forwarding is enabled in the Mode field, the Forwarding Destination IPv6 Address field MUST specify the Forwarding Destination IPv6 Address. The field MUST specify an IPv6 formatted address of the Mailbox Service to receive forwarded mailbox packages. If the Forwarding Destination is identified by an IPv4 address this field MUST be formatted as an IPv4-mapped IPv6 address [8].

If the Mailbox Proxy Forwarding is not enabled in the Mode field, the Forwarding Destination IPv6 Address MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

UDP Port Number (2 bytes)

This field indicates the UDP Port number of the Mailbox Service running at the Forwarding Destination.

If the Mailbox Proxy Forwarding is not enabled in the Mode field, this field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

4.3.4 Mailbox Configuration Report Command

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_MAILBOX							
Command = MAILBOX_ CONFIGURATION_REPORT							
Reserved			Supported Modes		Mode		
Mailbox Capacity – Byte 1							
Mailbox Capacity – Byte 2							
Forwarding Destination IPv6 Address – Byte 1							
…							
Forwarding Destination IPv6 Address – Byte 16							
UDP Port Number – Byte 1							
UDP Port Number – Byte 2							

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Supported Modes (2 bits)

The Supported Modes bit field is used to advertise the functionalities supported by the node. This field MUST be encoded according to Table 4

Table 4, Mailbox Configuration Report::Supported Modes encoding

Bit Value	Description
0x01	Mailbox Service supported
0x02	Mailbox Proxy supported

Mode (3 bits)

Refer to 4.3.3 Mailbox Configuration Set Command.

Mailbox Capacity (2 bytes)

This field advertises the number of frames (at a maximum of 1280 bytes per frame) that may be stored in the mailbox while waiting for a Wake Up Notification.

A value of 0 MUST indicate that the mailbox will only support mailbox forwarding to another Mailbox Service.

A value of 0xFFFF MUST indicate that the mailbox in effect have no storage limitation.

Forwarding Destination IPv6 Address (16 bytes)

Refer to 4.3.3 Mailbox Configuration Set Command.

UDP Port Number (2 bytes)

Refer to 4.3.3 Mailbox Configuration Set Command.

4.3.5 Mailbox Queue Command

The Mailbox Queue Command is a container for various operations between a mailbox proxy and a Mailbox Service.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_MAILBOX							
Command = MAILBOX_QUEUE							
Reserved				Last	Operation		
Queue Handle							
Mailbox Entry – Byte 1							
…							
Mailbox Entry – Byte N							

Reserved (6 Bit)

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Last (1 bit)

The Last field is used to indicate if the current mailbox frame is the last in the queue for the specific device. The Last bit only applies when the “Pop” Operation is used.

The value 1 MUST indicate that the frame is the last on the queue.

The value 0 MUST indicate that more frames will follow.

Operation (3 bits)

The encoding of the Operation field MUST be according to Table 5.

Table 5, Mailbox Queue::Operation

Value	Description
0x00	Push. Queue a message from the proxy to the Mailbox Service
0x01	Pop. Dequeue a message from the Mailbox Service to the Mailbox Proxy for delivery on the PAN
0x02	Waiting. Service->Proxy: send waiting messages to the client.
0x03	Ping. Service->Proxy: send UDP ping messages to the client.
0x04	ACK. Proxy->Service: Frame has been delivered. Service->Proxy: Frame has been queued.
0x05	NACK. Proxy->Service: Frame was not queued. Wait for ACK before attempting queuing. Service->Proxy: Node is not responding. Keep in queue.
0x06	Queue Full. Proxy->Service: The capacity of the Mailbox Service has been reached. Wait until queue has been emptied.

All other values are reserved and MUST NOT be used by a sending node.
Reserved values MUST be ignored by a receiving node.

Queue Handle (8 bits)

The Queue Handle field is used to identify the queue this message belongs to. A service uses this handle with the source IP of the MAILBOX_QUEUE message to identify the queue to which a message belongs to.

Mailbox Entry (N Bytes)

The Mailbox Entry field contains the entire received UDP Package. Including, ZIP headers and Z-Wave Payload.

To avoid duplicate entries, the Mailbox Service MUST maintain a list of CRC16 checksums for each mailbox entry. All mailbox entries MUST be unique, if a matching CRC16 exists for an incoming package, the incoming package MUST be discarded.

When WAITING timer elapses the mailbox MUST send a WAITING message to all clients that has posted entries to the mailbox.

4.3.6 Mailbox Wake Up Notification Command

This command allows a mailbox proxy resource to notify a Mailbox Service resource that a wake up device is currently awake.

A Mailbox Proxy resource MAY send this command to a Mailbox Service resource.
A Mailbox Service resource MUST NOT send this command to a mailbox proxy resource.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_MAILBOX							
Command = MAILBOX_WAKEUP_NOTIFICATION							
Queue Handle							

Queue Handle (8 bits)

This field is used to specify the actual queue handle to send notification to.

4.3.7 Mailbox Failing Node Command

This command allows a mailbox proxy resource to notify a Mailbox Service resource that a wake up device is no longer available.

A Mailbox Proxy resource MAY send this command to a Mailbox Service resource.
A Mailbox Service resource MUST NOT send this command to a mailbox proxy resource.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_MAILBOX							
Command = MAILBOX_NODE_FAILING							
Queue Handle							

Queue Handle (8 bits)

This field is used to specify the actual queue.

A receiving Mailbox Service resource MUST discard all state information and enqueued messages for the actual queue.

4.3.8 Frame Flow diagrams Examples

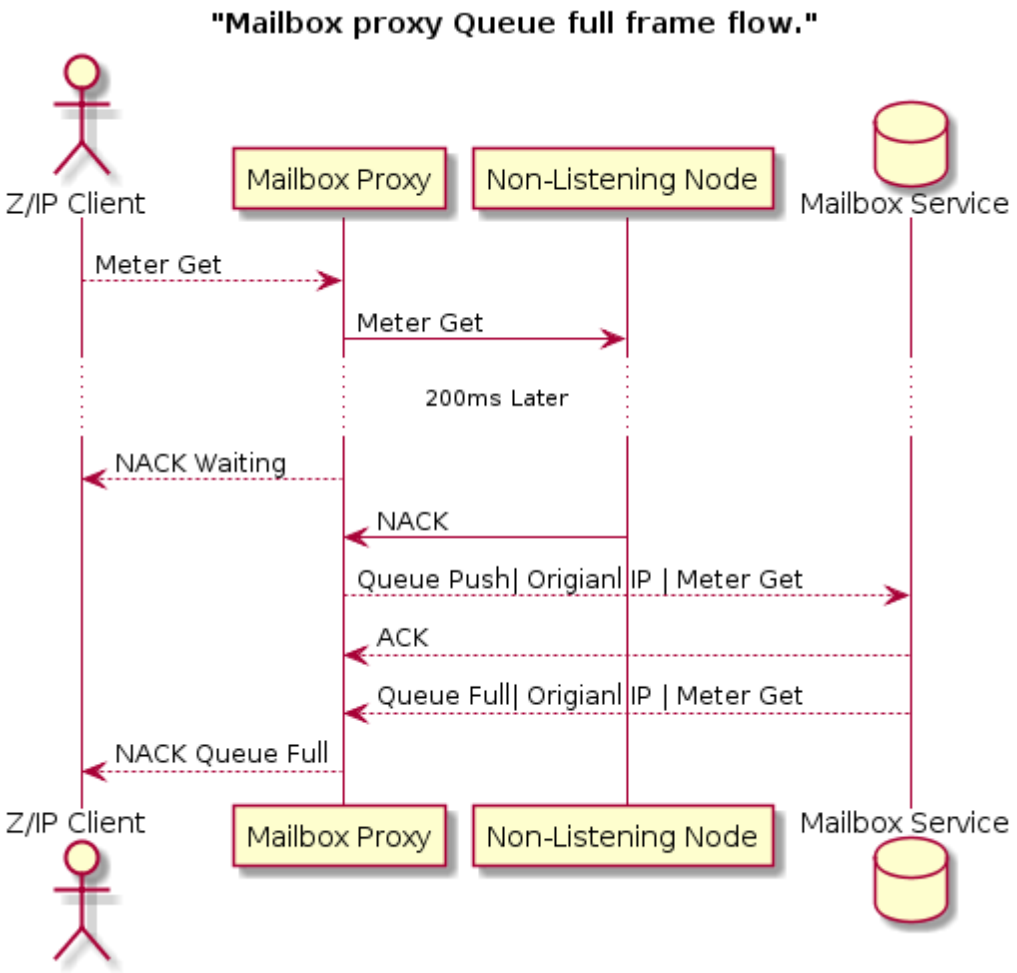

Figure 4, Mailbox proxy queue full frame flow

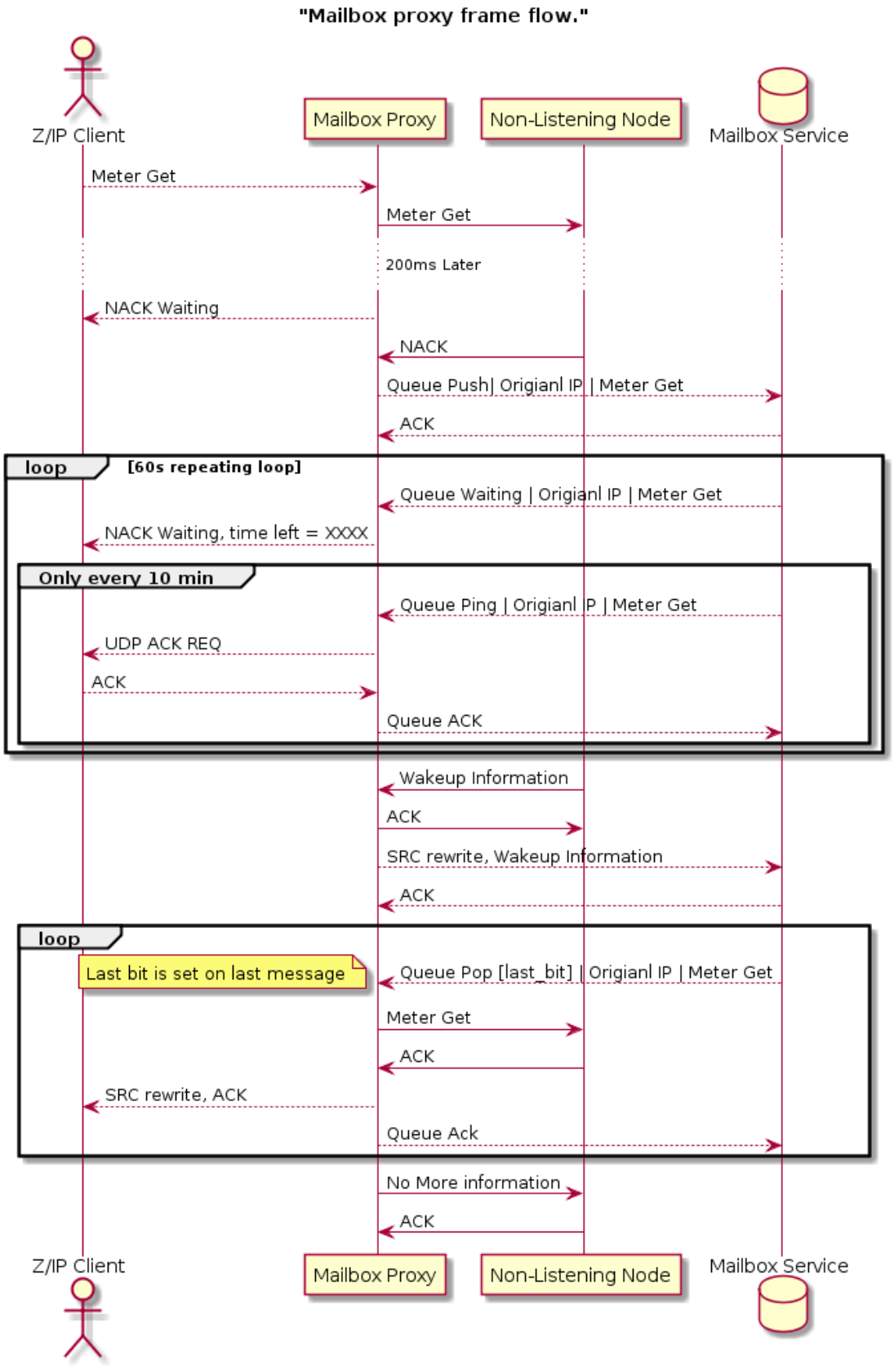

Figure 5, Normal frame flow

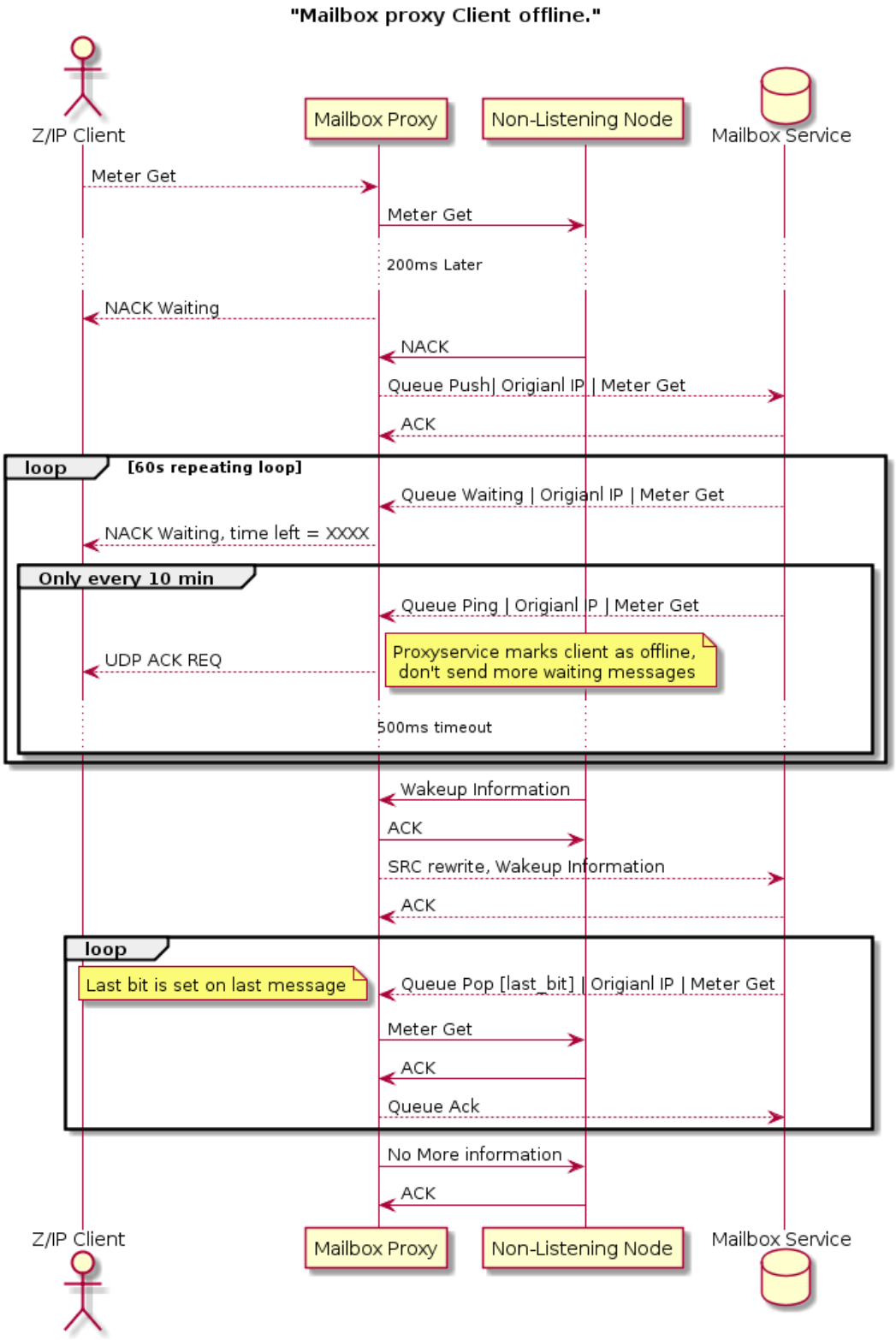

Figure 6, Z/IP Client goes offline and stops replying to UDP ping

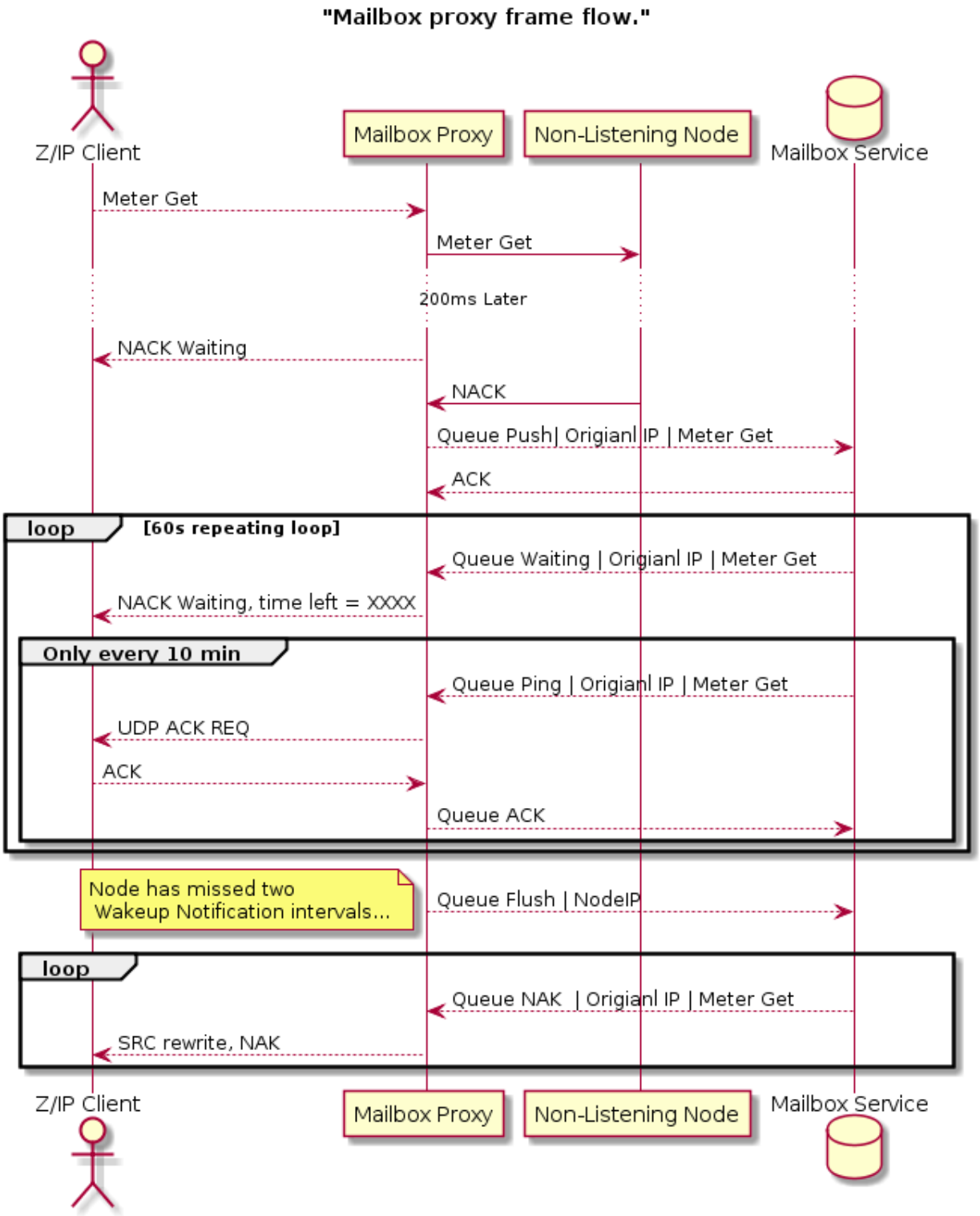

Figure 7, Sleeping node misses 2 wakeup intervals and proxy tells service to flush queue

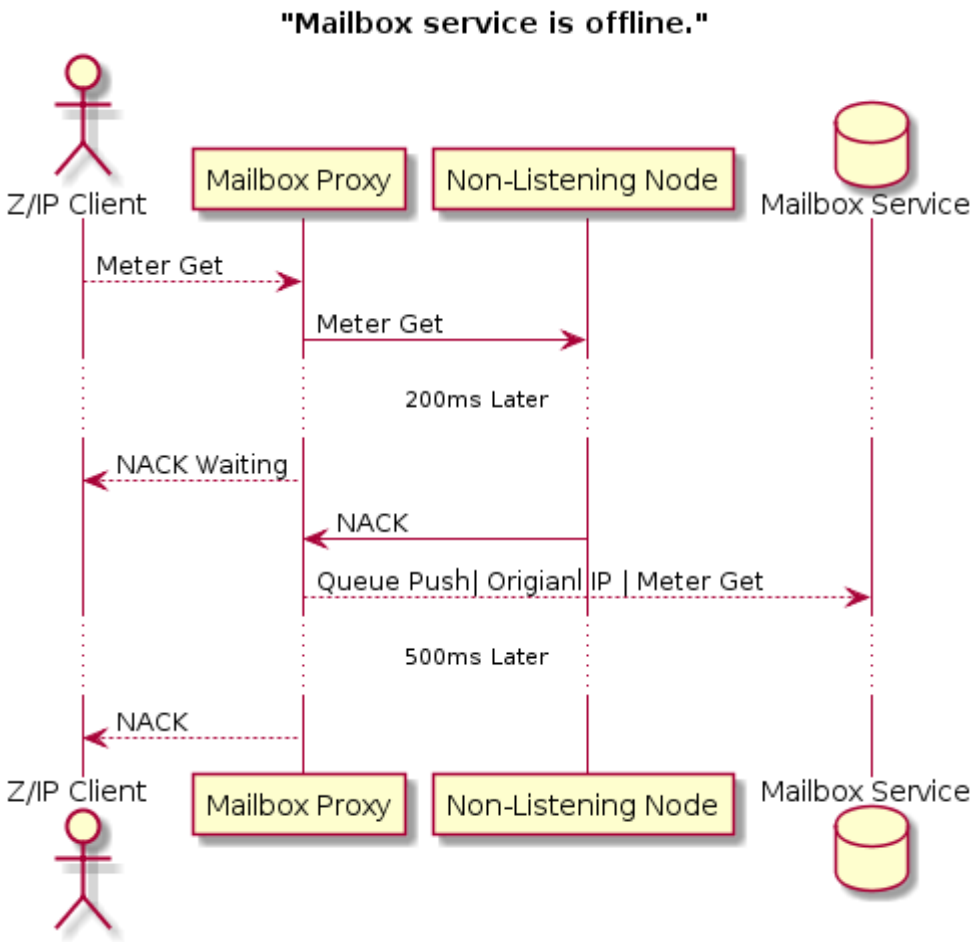

Figure 8 Mailbox Service is offline

4.4 Network Management Command Classes

4.4.1 Compatibility considerations

CC:0000.00.00.21.001 The commands defined in the following sections may span more than the available payload length in Z-Wave frames. If the command payload does not fit in a single frame, commands MUST be fragmented using the Transport Service Command Class.

CC:0000.00.00.21.002 When using IP transport, the IP UDP data segment length limit of 1280 bytes MUST be respected.

CC:0000.00.00.22.001 There is a risk that a controlling node would try to issue Network Management commands to a controller which does not support functionality due to its Network role (i.e. Secondary controller). A controller SHOULD adjust its NIF (or S0/S2 Commands Supported Report Command) based on its network role after inclusion.

CC:0000.00.00.21.004 When a node has the SIS, Primary controller or Inclusion controller role, it MUST support:

- Network Management Inclusion Command Class
- Network Management Basic Command Class
- Transport Service Command Class

CC:0000.00.00.21.005 When a node has the secondary controller role, it MUST support:

- Network Management Basic Command Class

The Z-Wave Network Management commands are organized as follows

Command Class	Purpose
Network Management Proxy	The command class is used to report the list of nodes present in a Z-Wave Network and report the secure/non-secure capabilities of each of those nodes Version 2 of this command class extends the node capability reporting to Multi Channel End Points.
Network Management Basic Node	The command class is used to remotely control network management operations related to including supporting nodes into a Z-Wave network. The available functionalities are : • Enable Learn mode • Request a node to broadcast its Node Information Frame • Request a node to request a network topology update to the SUC • Reset a controller to the factory default state Version 2 of this command class extends the learn mode activation commands In order to support S2 and adds the following functionality: • Request a node to report its S2 DSK.

Command Class	Purpose
Network Management Inclusion	This command class is used to remotely control network management operations related to including other nodes into a Z-Wave network. The available functionalities are : • Enable Add mode • Remove a node from the network • Remove a Failed NodeID from the network • Replace a Failed NodeID in the network • Request the node to ask a specific node to perform a Neighbor update. • Instruct the supporting node to assign a return route to another slave node • Instruct the supporting node to remove return routes in another slave node Version 2 of this command class extends the Add/Remove/Replace commands to support S2 and adds the following functionality: • A supporting node can be instructed which S2 keys to grant to a joining node. • A supporting node can be provided a DSK input for S2 authentication.
Network Management Primary	This command class is used to remotely trigger a controller change operation.
Network Management Installation and maintenance	This command class is used for maintenance and optimization purposes. The available functionalities are : • Manipulate priority routes (working routes) • Request network statistics recorded by the node.

4.4.1.1 Sequence Number management

The following text applies to all sequence numbers used by Network Management Command Classes.

CC:0000.00.00.21.006 Each sequence number MUST be generated from an 8-bit counter that is incremented by 1 whenever a new sequence number is generated. When a node powers up, the sequence counter MUST be initialized to a random value.

CC:0000.00.00.23.001 All command classes referring to this section MAY use the same global counter.

CC:0000.00.00.21.007 When responding to a request command, a responding node MUST echo the sequence number used by the requesting node.

CC:0000.00.00.21.008 When receiving response to a request command, the requesting node MUST verify that the response carries the same sequence number as the request command.

4.4.2 Scope of Network Management

Network management commands may be used in a number of scenarios. Three scopes have been identified:

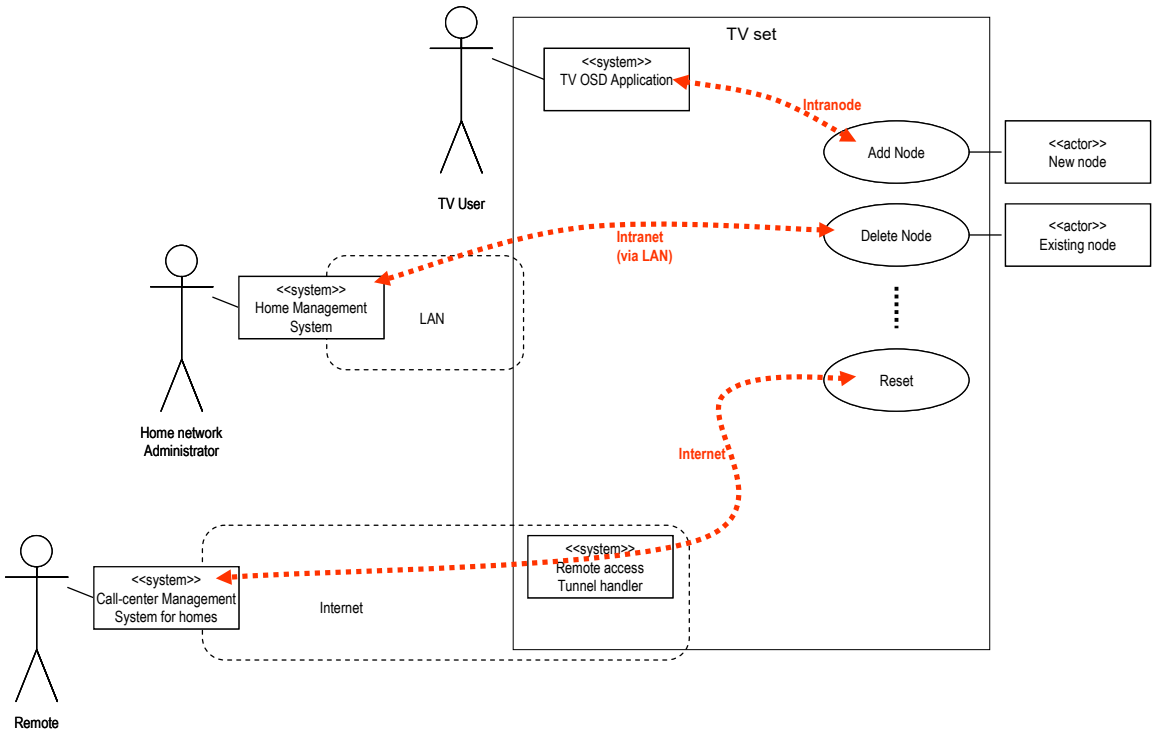

Figure 9, Scope of network management

4.4.2.1 Intranode

When used in an intranode configuration, the network management command classes are primarily used for implementation convenience. As an example, a software module of the Z/IP Gateway application may be used to provide a standard IP-based interface for other Linux applications inside a set-top box. In this way an application programmer does not have to bother about serial port communication, Telnet command parsing, etc.

4.4.2.2 Intranet (LAN)

Managed building automation systems may implement one central network manager controlling a number of geographically distributed Z/IP Gateways via the network management command classes. Each Z/IP Gateway may be instructed to perform local inclusion or exclusion of nodes; thus creating a large infrastructure segmented into subnets.

4.4.2.3 Internet (WAN)

The help desk of a service provider may provide support from a remote call center via the Internet. This enables the deployment of border routers, remote controls and plug-in modules in consumer environments without relying on the technical interest and/or capabilities of the user.

4.4.3 Security considerations

CC:0000.00.00.42.001 Network management is a powerful toolbox. From an application level, it SHOULD be ensured that the user does not unintentionally reset the controller or remove nodes.

CC:0000.00.00.41.001 At the same time it MUST be ensured that it is not possible for unauthorized persons to inject malicious commands into the network, e.g. resetting the primary controller to default factory settings.

CC:0000.00.00.41.002 All Network Management Command Class MUST be sent securely when used on a Z-Wave network, using at least Z-Wave Security 0 Command Class, version 1. When used on the LAN side other means of security should be used.

If the network management commands are carried in IP packets over Z-Wave, a minimum level of security is automatically applied since S0 network security is mandatory for all Z/IP traffic.

CC:0000.00.00.42.002 When Z-Wave network management commands are carried over IP LAN and WAN media (intranet & internet) the IP traffic SHOULD be using secure communication. A Z/IP Gateway MAY allow a LAN-based IP host to send un-encrypted Network Management commands to a controller via the Z/IP Gateway. Support for un-encrypted Network Management commands SHOULD be disabled by default and after a factory reset.

4.4.3.1 Designing for single-threading and limited transmit buffer

CC:0000.00.00.41.003 In order to support constrained CPU platforms, the Z-Wave API has been designed for single-threaded operation. A node MUST ignore Network Management command if already processing or executing another Network Management command.

CC:0000.00.00.42.003 A node SHOULD NOT ignore the command if it is identical to the command currently being processed/executed (e.g. Add Node Command with mode: Stop when Add Mode is active)

CC:0000.00.00.41.004 A node MUST return status messages to the node that actually initiated the operation.

CC:0000.00.00.41.005
CC:0000.00.00.42.004 An controlling node MUST time out waiting for a status message. If not receiving a status message within at least 10 seconds, the node SHOULD re-send the Network Management command using the same sequence number to allow the target node to detect duplicates.

CC:0000.00.00.43.001 A receiving node MAY return a “busy” indication. Doing so could however lead to transmit buffer overflows. Care should be taken to avoid this during implementation.

CC:0000.00.00.41.006 The Z-Wave Ack does not necessarily indicate that the command is being executed, but that it has been received by the protocol. The sending application MUST wait for the Network Management command callback, or time out.

4.4.4 Network Management Proxy Command Class, version 1

The Network Management Proxy Command Class provides functions to access basic network information such as the list of nodes currently present in the Z-Wave network.

4.4.4.1 Node List Get Command

This command is used to request the network node list from local storage in a node.

CC:0052.01.01.11.001 The Node List Report Command MUST be returned in response to this command.

CC:0052.01.01.11.002 This command MUST NOT be issued via multicast addressing.

CC:0052.01.01.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = COMMAND_NODE_LIST_GET (0x01)							
Seq No							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

4.4.4.2 Node List Report Command

This command carries node data requested with the Node List Get Command.

In addition, when a node has been added to or removed from the network or when the Z/IP Gateway
CC:0052.01.02.11.001 has acquired the SIS role, the Z/IP Gateway MUST send an unsolicited Node List Report with the new network information to the unsolicited destination.
CC:0052.01.02.12.001 If the unsolicited destination itself has initiated the node addition or removal, this command SHOULD
CC:0052.01.02.11.002 NOT be sent.
If no unsolicited destination has been set, the gateway MUST NOT send a Node List Report upon network changes.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = COMMAND_NODE_LIST_REPORT (0x02)							
Seq No							
Status							
Node List Controller ID							
Node List Data 1							
...							
Node List Data 29							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Status (8 bits)

CC:0052.01.02.11.003 This field indicates the status of Node List data carried in the command. The field MUST take one of the following values:

- 0x00: The Node List Data contains the latest updated node list.
- 0x01: The Node List Data may be outdated.

Node List Controller ID (1 byte)

The Node List Controller ID is a NodeID pointing at a controller, which keeps latest updated node list. The value 0x00 indicates that Node List Controller ID is unknown.

CC:0052.01.02.12.002 The Node List Controller SHOULD provide up-to-date information, but the actual freshness of data depends on the network construction. If a portable controller is primary there may be no access to the most recent network data. In that case the user may have to manually wake up the portable controller and initiate a controller replication to an always listening secondary controller.

No explicit Z-Wave route is provided for reaching the Node List Controller. The requesting node may use methods such as explorer discovery or Controller Network Update if the node does not already hold a working route to the indicated Node List Controller.

The Node List Controller ID may not support Network Management Proxy Command Class.

Node List Data (29 bytes)

This field carries a complete bitmap presenting all included nodes as a set bit (‘1’) while unused NodeIDs are presented as a (‘0’). The first bit in the bitmap represents NodeID 1; the last bit represents NodeID 232.

A receiving node can use the Node Info Cached Get Command to get information on individual node properties.

4.4.4.3 Node Info Cached Get Command

This command is used to request node capabilities that have been cached by another node. The command works as a proxy function provided by the node list controller. The purpose is to preserve the bandwidth of the Z-Wave network and to provide access to properties of sleeping nodes.

CC:0052.01.03.11.001 The Node Info Cached Report Command MUST be returned in response to this command.

CC:0052.01.03.13.001 CC:0052.01.03.11.002 A Z/IP client MAY issue the Node Info Cached Get command as an IPv4 broadcast or an IPv6 ‘all routers’ multicast packet. A Z/IP Gateway MUST accept such a packet and return a Node Info Cached Report in response.

CC:0052.01.03.11.003 A Node Info Cached Report returned by a Z/IP Gateway in response to an IP multicast packet MUST be delayed by a random delay in the range 0..450msec as more than one Z/IP Gateway may be responding.

CC:0052.01.03.11.004 The Z/IP Gateway MUST respond to an IP multicast by returning a unicast IP packet.

CC:0052.01.03.13.002 A Z/IP Client MAY time out waiting for Node Info Cached Report commands after 500msec.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = COMMAND_NODE_INFO_CACHED_GET (0x03)							
Seq No							
Reserved				Max Age			
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Reserved

CC:0052.01.03.11.005 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Max Age (4 bits)

CC:0052.01.03.12.001 The maximum age of the Node Info frame, given in 2^n minutes. If the cache entry does not exist or if it is older that the value given in this field, the Z/IP Gateway SHOULD attempt to get a fresh Node Info Frame before responding to this command.

A value of 15 means infinite, i.e. No Cache Refresh. A value of 0 means force update.
The values 1..15 allow for cache timeouts in the range 2min, 4min, …, 11days – and infinite.

NodeID (1 byte)

CC:0052.01.03.11.006 This field MUST indicate the NodeID for which the receiving node is to return cached data.
The value 0x00 MUST be interpreted as the ID of the queried network management node.

4.4.4.4 Node Info Cached Report Command

This command is used for returning cached node information.

<table>
<tr><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td colspan="8">Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY</td></tr>
<tr><td colspan="8">Command = COMMAND_NODE_INFO_CACHED_REPORT (0x04)</td></tr>
<tr><td colspan="8">Seq No</td></tr>
<tr><td colspan="4">Status</td><td colspan="4">Age</td></tr>
<tr><td>List.</td><td colspan="7">Z-Wave Protocol Specific Part</td></tr>
<tr><td>Opt. Func.</td><td colspan="7">Z-Wave Protocol Specific Part</td></tr>
<tr><td colspan="8">Reserved</td></tr>
<tr><td colspan="8">Basic Device Class</td></tr>
<tr><td colspan="8">Generic Device Class</td></tr>
<tr><td colspan="8">Specific Device Class</td></tr>
<tr><td colspan="8">Command Class 1 *)</td></tr>
<tr><td colspan="8">...</td></tr>
<tr><td colspan="8">Command Class N *)</td></tr>
</table>

*) Command classes may be extended ⇒ spanning two bytes for one command class

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Status (4 bits)

CC:0052.01.04.11.001 This field is used to indicate the Node Info Cached information status.
This field MUST comply with Table 6.

Table 6, Node Info Cached Report::Status parameter encoding

Value	Status identifier	Description
0x00	STATUS_OK	The requested NodeID could be found and up-to-date information is returned.
0x01	STATUS_NOT_RESPONDING	The requested NodeID could be found but fresh information could not be retrieved.
0x02	STATUS_UNKNOWN	The NodeID is unknown.

Age (4 bits)

CC:0052.01.04.11.002 This field indicates the age of the Node Info frame, i.e. the time elapsed since the data has been received by the actual node. This field MUST be expressed in “2^n minutes”. This field’s value MUST be rounded down, i.e.12 minutes MUST be reported as 2^3 = 8 minutes and not as 2^4 = 16 min.

List. (1 bit)

The listening bit is set to 1 if this node is always listening for commands and 0 if the node does not listen for commands.

Opt. Func. (1 bit)

The Optional Functionality bit indicates if true (== ‘1’) the node supports more command classes in addition to the ones covered by the device classes listed in this message. The additional command classes follow the device class fields.

Reserved

CC:0052.01.04.11.003 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Z-Wave Protocol Specific Part

CC:0052.01.04.11.004 This field is the protocol specific part of the NIF. It MUST be set as received in the Node Information Frame.

Basic Device Class (1 byte)

This field indicates the Basic Device Class of the actual node. The Basic Device Classes are listed in [1]

Generic Device Class (1 byte)

This field indicates the Generic Device Class of the actual node. The Generic Device Classes are listed in [1] for Z-Wave and [10] for Z-Wave Plus

Specific Device Class (1 byte)

This field indicates the Specific Device Class of the actual node. The Specific Device Classes are listed in [1] for Z-Wave and [10] for Z-Wave Plus

Command Class (N bytes)

This field indicates the command classes implemented by the actual node.

CC:0052.01.04.11.005 The Security Scheme 0 Mark MUST be used to delimit Command Classes available non-securely and securely.

CC:0052.01.04.11.006 The Support/Control Mark MUST be used before and after the Security Scheme 0 Mark if it was present in the node's NIF.

CC:0052.01.04.11.007 A Command Class field structure example is shown in Table 7. The field MUST comply with Table 8.

Table 7, Command Class field structure example

Description	Command Class field content							
	7	6	5	4	3	2	1	0
Non-secure Supported Command Classes	Command Class 1 *)							
	…							
	Command Class M *)							
Support/Control Mark	0xEF							
Non-secure Controlled Command Classes	Command Class 1 *)							
	…							
	Command Class K *)							
Security Scheme 0 Mark	0xF1							
	0x00							
S0 Secure Supported Command Classes	Command Class 1 *)							
	…							
	Command Class L *)							
Support/Control Mark	0xEF							
S0 Secure Controlled Command Classes	Command Class 1 *)							
	…							
	Command Class P *)							

*) Command classes may be extended ⇒ spanning two bytes for one command class

Table 8, Special Command Class identifiers

Command Class ID	Description
0x20..0xEE	Command Class identifier
0xF101..0xFFFF	Extended Command Classes identifier
0xEF	Command Class Support/Control Mark Anything between this mark and the next mark is Controlled and not supported
0xF100	Security Scheme 0 Command Class Mark. Command Classes following this Mark are supported or controlled with Security Scheme 0

4.4.5 Network Management Proxy Command Class, version 2

4.4.5.1 Compatibility considerations

CC:0052.02.00.21.001 The Network Management Proxy Command Class, version 2 is backwards compatible with Network Management Proxy Command Class, version 1. A node supporting Network Management Proxy Command Class, version 2 MUST also support Network Management Proxy Command Class, version 1.

All commands not mentioned in this version remain unchanged from version 1.

The following command has been extended to support S2 bootstrapping information:

- Node Info Cached Report

The following commands have been added to support Multi Channel End Point probing:

- Network Management Multi Channel End Point Get Command
- Network Management Multi Channel End Point Report Command
- Network Management Multi Channel Capability Get Command
- Network Management Multi Channel Capability Report Command
- Network Management Multi Channel Aggregated Members Get Command
- Network Management Multi Channel Aggregated Members Report Command

4.4.5.2 Node Info Cached Report Command

This command is used for returning cached node information.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = COMMAND_NODE_INFO_CACHED_REPORT (0x04)							
Seq No							
Status				Age			
List.	Z-Wave Protocol Specific Part						
Opt. Func.	Z-Wave Protocol Specific Part						
Granted Keys							
Basic Device Class							
Generic Device Class							
Specific Device Class							
Command Class 1 *)							
...							
Command Class N *)							

*) Command classes may be extended ⇒ spanning two bytes for one command class

Fields not described in this version remain unchanged from version 1.

Granted Keys (8 bits)

This field is used to indicate which network keys were granted during bootstrapping.

CC:0052.02.04.11.001 This field MUST be treated as a bitmask and comply with Table 28

Command Class (N bytes)

Refer to 4.4.4.4 Node Info Cached Report Command and Table 8.

CC:0052.02.04.11.002 The Security Command Class Mark (0xF100) MUST indicate command classes supported using the highest listed Security Key in the Granted Key field value.

4.4.5.3 Network Management Multi Channel End Point Get Command

This command is used to query the number of Multi Channel End Points and other relevant Multi Channel attributes.

CC:0052.02.05.11.001 The Network Management Multi Channel End Point Report Command MUST be returned in response to this command unless it is to be ignored.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = NM_MULTI_CHANNEL_END_POINT_GET (0x05)							
Seq No							
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

NodeID (1 byte)

CC:0052.02.05.11.002 This field MUST indicate the NodeID for which the receiving node is to return cached data.
If the specified NodeID does not exist, this command MUST be ignored.

4.4.5.4 Network Management Multi Channel End Point Report Command

This command is used to advertise the number of Multi Channel End Points implemented by a node.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = NM_MULTI_CHANNEL_END_POINT_REPORT (0x06)							
Seq No							
NodeID							
Reserved							
Res	Individual End Points						
Res	Aggregated End Points						

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

NodeID (1 byte)

CC:0052.02.06.11.001 This field MUST indicate the NodeID for which the receiving node is to return cached data.

Reserved / Res

CC:0052.02.06.11.002 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Individual End Points (7 bits)

CC:0052.02.06.11.003 This field MUST advertise the number of individual End Points implemented by this node.

CC:0052.02.06.11.004 The value MUST be in the range 0..127.
The sum of the values advertised by the Individual End Points and Aggregated End Points fields MUST be in the range 0..127.

Aggregated End Points (7 bits)

CC:0052.02.06.11.005 This field MUST advertise the number of Aggregated End Points implemented by this node.

CC:0052.02.06.11.006 The value MUST be in the range 0..127.
The sum of the values advertised by the Individual End Points and Aggregated End Points fields MUST be in the range 0..127.

CC:0052.02.06.11.007 If no Aggregated End Points are implemented, this field MUST advertise the value 0 (zero).

4.4.5.5 Network Management Multi Channel Capability Get Command

This command is used to query the capabilities of one individual End Point or Aggregated End Point.

CC:0052.02.07.11.001 The Network Management Multi Channel Capability Report Command MUST be returned in response to this command unless it is to be ignored.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = NM_MULTI_CHANNEL_CAPABILITY_GET (0x07)							
Seq No							
NodeID							
Res	End Point						

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

NodeID (1 byte)

CC:0052.02.07.11.002 This field MUST indicate the NodeID for which the receiving node is to return cached data.

Res

CC:0052.02.07.11.003 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

End Point (7 bits)

CC:0052.02.07.11.004 This field MUST specify a valid End Point as advertised by the Multi Channel End Point Report.
If the specified End Point does not exist, this command MUST be ignored.

4.4.5.6 Network Management Multi Channel Capability Report Command

This command is used to advertise the generic and specific device class and the supported command classes of one End Point.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = NM_MULTI_CHANNEL_CAPABILITY_REPORT (0x08)							
Seq No							
NodeID							
Command Class Length							
Res	End Point						
Generic Device Class							
Specific Device Class							
Command Class 1 *)							
…							
Command Class N *)							

*) Command classes may be extended ⇒ spanning two bytes for one command class

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

NodeID (1 byte)

CC:0052.02.08.11.001 This field MUST indicate the NodeID for which the receiving node is to return cached data.

Res (1 bit)

CC:0052.02.08.11.002 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Command Class Length (1 byte)

CC:0052.02.08.11.003 This field MUST advertise the length in bytes of the Command Class field.

End Point (7 bits)

CC:0052.02.08.11.004 This field MUST advertise a valid End Point as advertised by the Multi Channel End Point Report.

Generic Device class (8 bits)

This field indicates the Generic Device Class of the advertised End Point.

Specific Device class (8 bits)

This field indicates the Specific Device Class of the advertised End Point.

Command Class (N bytes)

CC:0052.02.08.11.005 This field MUST advertise Command Classes supported or controlled by the End Point in question. Refer to 4.4.4.4 Node Info Cached Report Command and Table 8.

CC:0052.02.08.11.006 The Security Command Class Mark (0xF100) MUST indicate command classes supported using the highest listed Security Key in the Granted Key field value.

4.4.5.7 Network Management Multi Channel Aggregated Members Get Command

This command is used to query the members of an Aggregated End Point.

CC:0052.02.09.11.001 The Network Management Multi Channel Aggregated Members Report Command MUST be returned in response to this command unless it is to be ignored.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = NM_MULTI_CHANNEL_AGGREGATED_MEMBERS_GET (0x09)							
Seq No							
NodeID							
Res	Aggregated End Point						

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

NodeID (1 byte)

CC:0052.02.09.11.002 This field MUST indicate the NodeID for which the receiving node is to return cached data. This command MUST be ignored if the NodeID field is not valid.

Res

CC:0052.02.09.11.003 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Aggregated End Point (7 bits)

CC:0052.02.09.11.004 This field MUST specify an Aggregated End Point.
This command MUST be ignored if the End Point does not exist or is not an Aggregated End Point.

4.4.5.8 Network Management Multi Channel Aggregated Members Report Command

This command is used to advertise the members of an Aggregated End Point.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY							
Command = NM_MULTI_CHANNEL_AGGREGATED_MEMBERS_REPORT (0x0A)							
Seq No							
NodeID							
Res	Aggregated End Point						
Number of Members							
Res	Member Endpoint 1						
…							
Res	Member Endpoint N						

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

NodeID (1 byte)

CC:0052.02.0A.11.001 This field MUST indicate the NodeID for which the receiving node is to return cached data.

Res

CC:0052.02.0A.11.002 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Aggregated End Point (7 bits)

CC:0052.02.0A.11.003 This field MUST advertise an Aggregated End Point.

CC:0052.02.0A.11.004 If the command is returned in response to a Multi Channel Aggregated Members Get, this field MUST advertise the same value as was received in the Multi Channel Aggregated Members Get command.

Number of Members (8 bits)

CC:0052.02.0A.11.005 This field MUST advertise the number of members of the aggregated End Points

Member Endpoint (N * 7 bits)

CC:0052.02.0A.11.006 This list is used to advertise the End Point members of the Aggregated End Point advertised in the Aggregated End Point field. The length of the list MUST be determined from the Number of Members field. This field MUST be omitted if the Number of Members field is set to 0.

CC:0052.02.0A.11.007 Each object in the list is a 7-bit End Point ID. The addressing bit (Res) MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

4.4.6 Network Management Basic Node Command Class, version 1

The Network Management Basic Node Command Class provides functions to get nodes included into a Z-Wave network, enabling nodes to request network updates and resetting itself factory default state.

4.4.6.1 Default Set Command

This command is used to set the Controller back to the factory default state.

CC:004D.01.06.11.001 The Default Set Complete Command MUST be returned in response to this command. A receiving node MUST return the DEFAULT_SET_BUSY status if it is already busy executing another network management command.

CC:004D.01.06.11.002 This command MUST NOT be issued via multicast addressing.

CC:004D.01.06.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

CC:004D.01.06.12.001 This function SHOULD be used with care as it could render a network unusable if the primary controller in an existing network is set back to default. If a node is set to default while it is still a member of a network, the node will become a failing NodeID in that network.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_DEFAULT_SET (0x06)							
Seq No							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

4.4.6.2 Default Set Complete Command

This command is used to indicate if the Default Set operation was executed successfully or not.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_DEFAULT_SET_COMPLETE (0x07)							
Seq No							
Status							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Status (8 bits)

CC:004D.01.07.11.001 This field indicates the status of the default set operation. This field MUST comply with Table 9.

Table 9, Default Set Complete::Status encoding

Value	Identifier	Description
0x06	DEFAULT_SET_DONE	The Default Set operation has been completed successfully.
0x07	DEFAULT_SET_BUSY	The Default Set operation has not been executed because the node is busy.

4.4.6.3 Learn Mode Set Command

This command is used to allow a node to be added to (or removed from) the network. When a node is added to the network, the node is assigned a valid Home ID and NodeID.
This command allows a controlling application to request the transmission of Node Information Frames (NIFs) in regular intervals until included, removed or until learn mode is disabled again.

CC:004D.01.01.12.001 Learn mode SHOULD be enabled only when necessary, and it SHOULD always be disabled again as quickly as possible. However, to ensure a successful synchronization of the inclusion process the device SHOULD be able to stay in learn mode at least 5 seconds.

CC:004D.01.01.11.006 The Learn Mode Set Status Command MUST be returned in response to this command unless it is to be ignored.

CC:004D.01.01.11.002 This command MUST NOT be issued via multicast addressing.
CC:004D.01.01.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_LEARN_MODE_SET (0x01)							
Seq No							
Reserved							
Mode							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Reserved

CC:004D.01.01.11.004 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Mode (8 bits)

CC:004D.01.01.11.005 The Mode field controls operation. This field MUST comply with Table 10.

Table 10, Learn Mode Set::Mode parameter encoding

Value	Identifier	Description
0x00	ZW_SET_LEARN_MODE_DISABLE	Stop the learn mode of the node. The command MAY be ignored if Learn Mode was not activated. The command MAY be ignored if network inclusion or security bootstrapping is ongoing.
0x01	ZW_SET_LEARN_MODE_CLASSIC	Start the learn mode on the controller and accept only being included in direct range
0x02	ZW_SET_LEARN_MODE_NWI	Start the learn mode on the controller and accept routed inclusion.

C:004D.01.01.13.001

Examples of Learn Mode activation and deactivation are given in 4.4.6.8.1 Z/IP Client requesting a node to interrupt Learn Mode

4.4.6.3.1 Learn mode in a controller

If the receiving node is a controller, it receives and stores the node list and routing table for the network during inclusion. This information transmitted as part of the controller replication. This function will most likely change the capabilities of the controller.

4.4.6.4 Learn Mode Set Status Command

This command is used to indicate the progress of the Learn Mode Set command.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_LEARN_MODE_SET_STATUS (0x02)							
Seq No							
Status							
Reserved							
New NodeID							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Status (8 bits)

CC:004D.01.02.11.001 This field indicates the outcome of the learn mode and MUST comply with Table 11.

Table 11, Learn Mode Status::Status parameter encoding

Value	Identifier	Description
0x06	LEARN_MODE_DONE	The learn process is complete and the controller is now included into (or excluded from) the network. If the node supports S0 or S2, it indicates that the network inclusion and security bootstrapping were completed successfully (This include the case where the node was granted no S2 key).
0x07	LEARN_MODE_FAILED	The learn process failed in some general way
0x09	LEARN_MODE_SECURITY_FAILED	The learn process is complete and the node was included in a network but security bootstrapping failed. The node is **not** operating securely.

Reserved

CC:004D.01.02.11.002 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

New NodeID (1 byte)

The NodeID assigned to the new node by another primary controller or inclusion controller.
If the node was removed from the network or if the Status field is different than LEARN_MODE_DONE, this field MUST be set to 0x00.

4.4.6.5 Node Information Send Command

This command is used to trigger a receiving node to issue a Node Information Frame (NIF).

CC:004D.01.05.11.001 A node receiving this command MUST send a Node Information Frame to the indicated NodeID with the indicated transmission options. No status message is returned for this command.

CC:004D.01.05.13.001 CC:004D.01.05.12.001 CC:004D.01.05.13.002 A management application MAY use this message to make a node identify itself towards a Z-Wave remote control during association operations. This command SHOULD NOT be used while learn mode is activated. Instead, periodic Node Information Frame transmissions MAY be enabled along with learn mode; refer to 4.4.6.1.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_NODE_INFORMATION_SEND (0x05)							
Seq No							
Reserved							
Destination NodeID							
tx Options							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Destination NodeID (1 byte)

CC:004D.01.05.13.003 This field indicates the NodeID of the node that will receive the Node Information frame. The NodeID MAY be set to the broadcast NodeID to reach all nodes within direct range.

CC:004D.01.05.12.002 Acknowledgement SHOULD NOT be requested when broadcasting.

tx Options (1 byte)

CC:004D.01.05.11.002 This field allows a management application to specify if the Node Information frame is to be sent with special properties. This field MUST be treated as a bitmask and MUST comply with Table 12.

Table 12, Node Information Send::Tx Options encoding

Value	Option flag identifier	Description
0x00	NULL	Transmit at normal power level without any transmit options.
0x01	TRANSMIT_OPTION_ACK	Request acknowledgment from destination node. Allow routing.
0x02	TRANSMIT_OPTION_LOW_POWER	Transmit at low output power level (1/3 of normal RF range)
0x10	TRANSMIT_OPTION_NO_ROUTE	Send only in direct range
0x20	TRANSMIT_OPTION_EXPLORE	Resolve new routes via explorer discovery if existing routes fail

CC:004D.01.05.12.003 It is RECOMMENDED for a sending node to use the TRANSMIT_OPTION_NO_ROUTE tx Option and the broadcast NodeID in this command.

4.4.6.6 Network Update Request Command

This command is used to request network topology updates from the SUC/SIS node.

CC:004D.01.03.11.001 A node MUST NOT use this command if no SUC is present in the network.

The SUC can only handle one network update at a time, so care should be taken not to have multiple controllers in the network ask for updates at the same time.

CC:004D.01.03.12.001 This command will generate a lot of network activity that will use bandwidth and stress the SUC. Therefore, network updates SHOULD be requested as seldom as possible.

CC:004D.01.03.11.002 The Network Update Request Status Command MUST be returned in response to this command.

CC:004D.01.03.11.003 This command MUST NOT be issued via multicast addressing.

CC:004D.01.03.11.004 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_NETWORK_UPDATE_REQUEST (0x03)							
Seq No							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

4.4.6.7 Network Update Request Status Command

This command is used to indicate if the Network Update Request command execution has completed successfully or not.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_NETWORK_UPDATE_REQUEST_STATUS (0x04)							
Seq No							
Status							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Status (1 byte)

This field is used to indicate the status of the Network Update process.

CC:004D.01.04.11.001 This field MUST comply with Table 13.

Table 13, Network Update Request Status::Status parameter encoding

Value	Status identifier	Description
0x00	ZW_SUC_UPDATE_DONE	The update process succeeded
0x01	ZW_SUC_UPDATE_ABORT	The update process aborted because of an error
0x02	ZW_SUC_UPDATE_WAIT	The SUC node is busy
0x03	ZW_SUC_UPDATE_DISABLED	The SUC functionality is disabled
0x04	ZW_SUC_UPDATE_OVERFLOW	The controller requested an update after more than 64 changes have occurred in the network. The controller has to make a replication.

4.4.6.8 Use cases and frame flows

4.4.6.8.1 Z/IP Client requesting a node to interrupt Learn Mode

The frame flow for interrupting Learn Mode is shown in Figure 10.

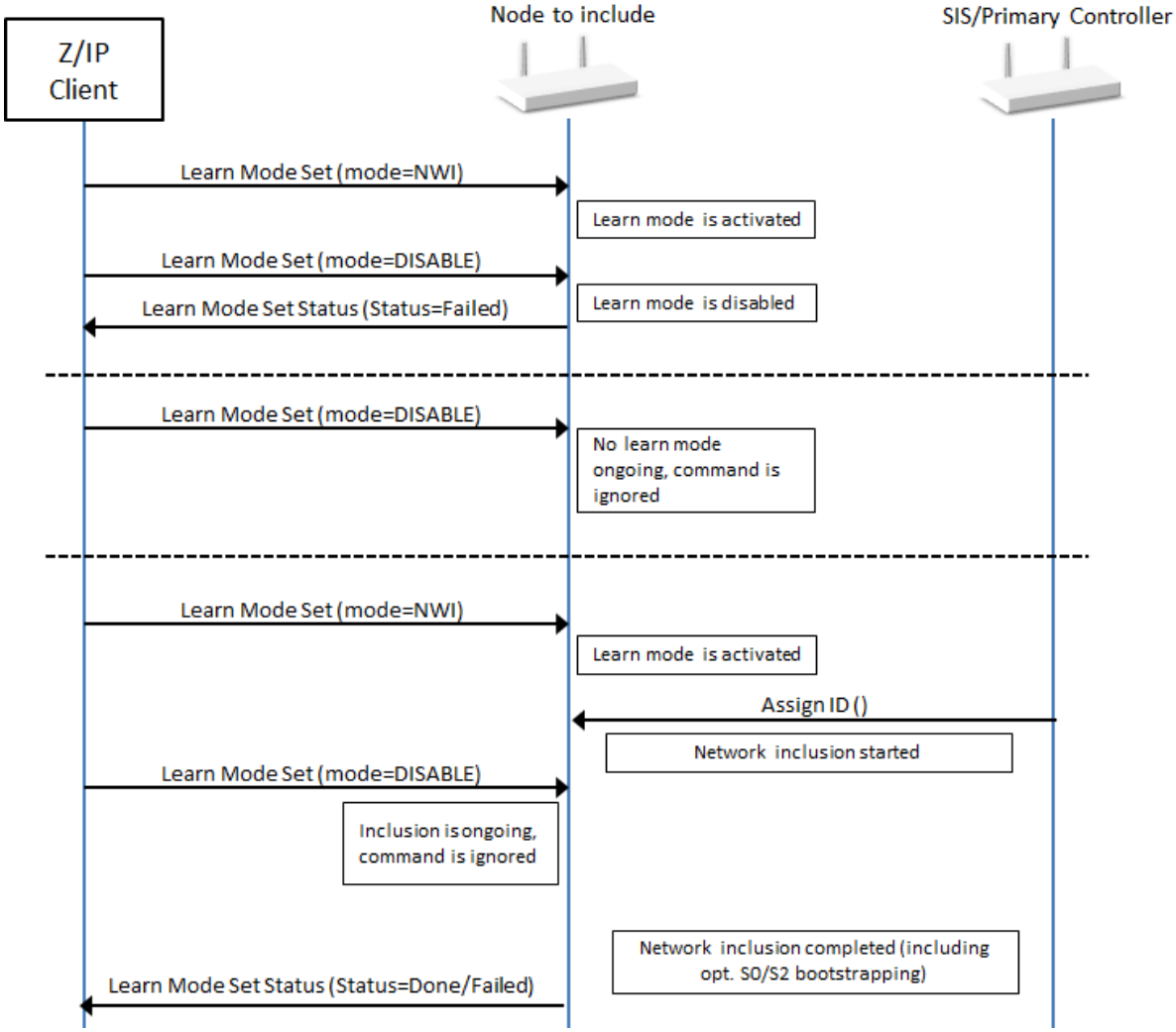

Figure 10, Z/IP Client interrupting learn mode

4.4.7 Network Management Basic Node Command Class, version 2

4.4.7.1 Compatibility considerations

CC:004D.02.00.21.001 The Network Management Basic Command Class, version 2 is backwards compatible with Network Management Basic Command Class, version 1. A node supporting Network Management Basic Command Class, version 2 MUST also support Network Management Basic Command Class, version 1.

All commands not mentioned in this version remain unchanged from version 1.

The following commands are introduced to allow a GUI to display the DSK of a S2 node and advertise interview status:

- DSK Get Command
- DSK Report Command

The following commands have been extended to return information about the S2 bootstrapping outcome and the node interview process after activating Learn Mode:

- Learn Mode Set Command
- Learn Mode Set Status Command

4.4.7.2 Learn Mode Set Command

This command is used to allow a node to be added to (or removed from) the network. When a node is added to the network, the node is assigned a valid Home ID and NodeID.
This command allows a controlling application to request the transmission of Node Information Frames (NIFs) in regular intervals until included, removed or until learn mode is disabled again.

CC:004D.02.01.12.001 Learn mode SHOULD be enabled only when necessary, and it SHOULD always be disabled again as quickly as possible. However, to ensure a successful synchronization of the inclusion process the device SHOULD be able to stay in learn mode at least 5 seconds.

CC:004D.02.01.11.001 The Learn Mode Set Status Command MUST be returned in response to this command.

CC:004D.02.01.11.002 This command MUST NOT be issued via multicast addressing.
CC:004D.02.01.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_LEARN_MODE_SET							
Seq No							
Reserved							Return interview status
Mode							

Fields not described in this version remain unchanged from version 1.

Return Interview Status (1 bit)

This field is used to request that the receiving node returns an additional Learn Mode Set Status Command when the node interview is completed.

CC:004D.02.01.11.004 The value 0 MUST indicate that the receiving node MUST return a Learn Mode Set Status Command when the learn mode is over.
The value 1 MUST indicate that the receiving node MUST return a Learn Mode Set Status Command when learn mode is over and an additional Learn Mode Set Status Command with status set to LEARN_MODE_INTERVIEW_COMPLETED when the inclusion node interview is over.

An illustration is given in Figure 11.

4.4.7.3 Learn Mode Set Status Command

This command is used to indicate the progress of the Learn Mode Set command.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_LEARN_MODE_SET_STATUS (0x02)							
Seq No							
Status							
Reserved							
New Node ID							
Granted Keys							
KEX Fail Type							
DSK 1							
…							
DSK 16							

Fields not described in this version remain unchanged from version 1.

Status (8 bits)

CC:004D.02.02.11.001 This field indicates the outcome of the learn mode and MUST comply with Table 14.

Table 14, Learn Mode Status version 2::Status parameter encoding

Value	Identifier	Description	Version
0x06	LEARN_MODE_DONE	The learn process is complete and the controller is now included into (or excluded from) the network. If the node supports S0 or S2, it indicates that the network inclusion and security bootstrapping were completed successfully (This include the case where the node was granted no S2 key).	1
0x07	LEARN_MODE_FAILED	The learn process failed in some general way	1
0x09	LEARN_MODE_SECURITY_FAILED	The learn process is complete and the node was included in a network but security bootstrapping failed. The node is **not** operating securely.	1

0x0A	LEARN_MODE_INTERVIEW_COMPLETED	This status is used to report that the post-inclusion interview is completed after network inclusion	2

Granted Keys (8 bits)

CC:004D.02.02.11.002 This field is used to indicate which network keys were granted during bootstrapping.
This field MUST be treated as a bitmask and comply with Table 28.

KEX Fail Type (8 bits)

CC:004D.02.02.11.003 This field is used to indicate which error occurred in case S2 bootstrapping was not successful.
This field MUST comply with Table 29.

DSK (16 bytes)

This field is used to indicate the DSK of the including controller that performed S2 bootstrapping to the node.
This information can be used for post inclusion verification.

4.4.7.4 DSK Get Command

This command is used to request the S2 DSK of a node.

CC:004D.02.08.11.001 The DSK Report Command MUST be returned in response to this command.

CC:004D.02.08.11.002 This command MUST NOT be issued via multicast addressing.
CC:004D.02.08.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_DSK_GET (0x08)							
Seq No							
Reserved							Add mode

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Add mode (1 bit)

This field is used to request the Add Mode or Learn Mode DSK.
S2 Controllers may have 2 key pairs, one static key pair used for Learn mode (being included in a

network) and one dynamic key pair changing at each bootstrapping used for Add mode (including other nodes in the network).

CC:004D.02.08.11.004 The value 0 MUST indicate that the node MUST return its Learn Mode DSK
The value 1 MUST indicate that the node MUST return its Add Mode DSK:

CC:004D.02.08.11.005 A node not supporting an Add Mode dynamic key pair MUST return its Learn Mode DSK.

4.4.7.5 DSK Report Command

This command is used by a node to advertise its DSK.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC							
Command = COMMAND_DSK_REPORT (0x09)							
Seq No							
Reserved							Add mode
DSK 1							
…							
DSK 16							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Add mode (1 bit)

This field is used to indicate if the Add Mode or Learn Mode DSK is advertised in this command.

CC:004D.02.09.11.001 The value 0 MUST indicate that the node advertises its Learn Mode DSK
The value 1 MUST indicate that the node advertises its Add Mode DSK.

DSK (16 bytes)

This field is used to transmit the S2 DSK. For details, refer to [14].

4.4.7.6 Use cases and frame flows

4.4.7.6.1 Z/IP Client requesting a node to report node interview status.

The frame flow for returning status messages at the end of Learn mode and the end of the post-inclusion device interview is shown in Figure 11.

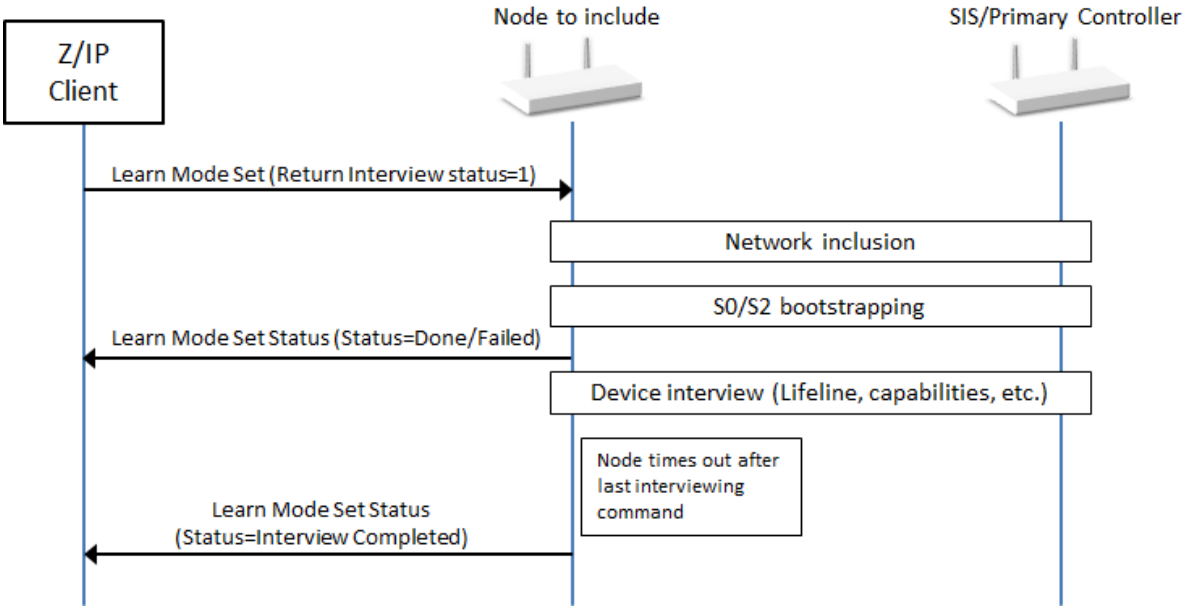

Figure 11, Node advertising the end of the interview process

4.4.8 Network Management Inclusion Command Class, version 1

The Network Management Inclusion Command Class provides functionality only available in a primary controller, inclusion controller or SIS. Since this is a dynamic property, there is a risk that a remote host tries to use commands in a controller which has become secondary in the meantime.

4.4.8.1 Node Add Command

This command is used to activate or de-activate add mode on a controller.

The process of adding a node is started by the network management application sending a Node Add command to a controller. The network management application receives a status message later on

CC:0034.01.01.13.001 indicating if the inclusion attempt was successful or not. If NWI inclusion was used, the calling application MAY re-issue this command if more nodes are to be included.

CC:0034.01.01.12.001 The Add Mode SHOULD be disabled after a certain time to avoid adding another node unexpectedly. It is RECOMMENDED to have a timer that disables the Node Add state after a given time without any activity.

CC:0034.01.01.11.001 Add Mode MUST be de-activated after any inclusion attempt, even if interrupted.

CC:0034.01.01.11.008 The Node Add Status Command MUST be returned in response to this command unless it is to be ignored.

CC:0034.01.01.11.003 This command MUST NOT be issued via multicast addressing.

CC:0034.01.01.11.004 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD (0x01)							
Seq No							
Reserved							
Mode							
tx Options							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Reserved

CC:0034.01.01.11.005 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Mode (1 byte)

This field is use to indicate to the receiving node if the Add Mode must be activated or de-activated.
CC:0034.01.01.11.006 This field MUST comply with Table 15.

Table 15, Node Add::Mode parameter encoding

Value	Identifier	Description
0x01	ADD_NODE_ANY	Add any type of node to the network.
0x05	ADD_NODE_STOP	Stop Add Mode. The command MAY be ignored if Add Mode was not activated. The command MAY be ignored if network inclusion or security bootstrapping is ongoing.

CC:0034.01.01.13.003

Examples of Add Mode activation and deactivation are given in 4.4.8.15.1 Z/IP Client requesting a node to interrupt Add Mode..

tx Options (1 byte)

CC:0034.01.01.11.007 The tx Options field allows a controlling node to specify if transmissions MUST use special properties. This field MUST be treated as a bitmask and MUST comply with Table 16.

Table 16, Node Add::Tx Options encoding

Value	Option flag identifier	Description
0x00	NULL	Transmit at normal power level without any transmit options.
0x02	TRANSMIT_OPTION_LOW_POWER	Transmit at low output power level (1/3 of normal RF range)
0x20	TRANSMIT_OPTION_EXPLORE	Allow network-wide inclusion

CC:0034.01.01.12.002 If the Mode is set to NODE_ADD_ANY, it is RECOMMENDED to set this field to TRANSMIT_OPTION_EXPLORE.

CC:0034.01.01.13.002 Installer scenarios with a requirement for more confidential transfer of network security keys MAY set the flag TRANSMIT_OPTION_LOW_POWER. This requires that the new node is included in direct range of the including controller.

4.4.8.2 Node Add Status Command

This command is used to report the result of the Node Add Command or report that a new node was included.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD_STATUS (0x02)							
Seq No							
Status							
Reserved							
New NodeID							
Node Info Length							
List.	Z-Wave Protocol Specific Part						
Opt. Func.	Z-Wave Protocol Specific Part						
Basic Device Class							
Generic Device Class							
Specific Device Class							
Command Class 1 *)							
...							
Command Class N *)							

*) Command classes may be extended ⇒ spanning two bytes for one command class

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Status (1 byte)

CC:0034.01.02.11.001 This field indicates the outcome of the add mode and MUST comply with Table 17.

Table 17, Node Add Status::Status parameter encoding

Value	Status identifier	Description
0x06	ADD_NODE_STATUS_DONE	The new node has been included in the network. If the new node and controller support S0 or S2, it indicates that the network inclusion and security bootstrapping were completed successfully (This include the case where the node was granted no S2 key).
0x07	ADD_NODE_STATUS_FAILED	The process failed, no new node was added in the network.
0x09	ADD_NODE_STATUS_SECURITY_FAILED	Node has been included but the security bootstrapping failed.

Reserved

CC:0034.01.02.11.002 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

New NodeID (1 byte)

CC:0034.01.02.11.005 This field MUST indicate the assigned NodeID to the newly added node. This field is valid if Status is different than NODE_ADD_STATUS_FAILED.
This field MUST be set to 0x00 if no NodeID was assigned to the included node.

Node Info Length (1 byte)

CC:0034.01.02.11.004 This field is used to indicate the length in bytes of the encapsulated Node Information fields. This field MUST be included in the length calculation. The value MUST indicate the length of the following fields:

- Node Info Length (this field)
- List / Z-Wave Protocol Specific Part
- Opt Func / Z-Wave Protocol Specific Part
- Basic Device Class
- Generic Device Class
- Specific Device Class
- Command Class

List. (1 bit)

Refer to 4.4.4.4 Node Info Cached Report Command.

Opt. Func. (1 bit)

Refer to 4.4.4.4 Node Info Cached Report Command.

Z-Wave Protocol Specific Part

Refer to 4.4.4.4 Node Info Cached Report Command.

Basic Device Class (1 byte)

Refer to 4.4.4.4 Node Info Cached Report Command.

Generic Device Class (1 byte)

Refer to 4.4.4.4 Node Info Cached Report Command.

Specific Device Class (1 byte)

Refer to 4.4.4.4 Node Info Cached Report Command.

Command Class (N bytes)

Refer to 4.4.4.4 Node Info Cached Report Command and Table 8.

4.4.8.3 Node Remove Command

This command is used to activate or de-activate node remove mode. The remove operation only works in direct range between the controller and the node that is to be removed.

CC:0034.01.03.12.001 The Node Remove mode SHOULD be disabled after a certain time to avoid removing another node unexpectedly. It is RECOMMENDED to have a timer that disables the Node Remove mode after a given time without any activity.

CC:0034.01.03.11.001 Node Remove mode MUST be de-activated after any removal attempt, even if interrupted.

CC:0034.01.03.11.007 The Node Remove Status Command MUST be returned in response to this command unless it is ignored.

CC:0034.01.03.11.003 This command MUST NOT be issued via multicast addressing.

CC:0034.01.03.11.004 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_REMOVE (0x03)							
Seq No							
Reserved							
Mode							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Reserved

CC:0034.01.03.11.005 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Mode (1 byte)

CC:0034.01.03.11.006 This field is use to indicate to the receiving node if the node removal process must be activated or de-activated. This field MUST comply with Table 18.

Table 18, Node Remove::Mode parameter encoding

Value	Mode identifier	Description
0x01	REMOVE_NODE_ANY	Remove any type of node from the network
0x05	REMOVE_NODE_STOP	Stop the node removal process. The command MAY be ignored if the remove process was not activated. The command MAY be ignored if network exclusion is ongoing.

CC:0034.01.03.13.001

The process of removing a node is started by sending this command with Mode set to REMOVE_NODE_ANY. The removal process is complete when a Node Remove Status command with status set to NODE_REMOVE_STATUS_DONE is returned.

4.4.8.4 Node Remove Status Command

This command is used to advertise the status of a node removal attempt.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_REMOVE_STATUS							
Seq No							
Status							
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management

Status (1 byte)

CC:0034.01.04.11.001 This field is used to advertise status of a node removal attempt. This field MUST comply with Table 19.

Table 19, Status parameter of Node Remove Status encoding

Value	Status identifier	Description
0x06	REMOVE_NODE_STATUS_DONE	The node has now been removed and the controller is ready to continue normal operation again. Removed NodeID is returned.
0x07	REMOVE_NODE_STATUS_FAILED	The remove process failed (no node was removed)

NodeID (1 byte)

CC:0034.01.04.12.001 This field is used to advertise the NodeID that was attempted to be removed from the network.
This field SHOULD be set to 0x00 if no attempt has been made.

4.4.8.5 Failed Node Remove Command

This command is used to remove a non-responding node.

CC:0034.01.07.11.001 A non-responding node is put onto the failed NodeID list by a controller when detected. In case the node responds again at a later stage, it is removed from the failed NodeID list. A node MUST be on the failed NodeID list and as an extra precaution also fail to respond before it is removed. Responding nodes MUST NOT be removed.

CC:0034.01.07.11.002 The Failed Node Remove Status Command MUST be returned in response to this command when the removal attempt has been made.

CC:0034.01.07.11.003 This command MUST NOT be issued via multicast addressing.
CC:0034.01.07.11.004 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_FAILED_NODE_REMOVE							
Seq No							
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management

NodeID (1 byte)

CC:0034.01.07.11.005 This field is used to specify the NodeID of the failing node which MUST be removed.

4.4.8.6 Failed Node Remove Status Command

This command is used to report the results of a failed node removal attempt.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_FAILED_NODE_REMOVE_STATUS							
Seq No							
Status							
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management

Status (1 byte)

CC:0034.01.08.11.001 This field is used to advertise status of the failed node removal process. This field MUST comply with Table 20.

Table 20, Status parameter of Failed NodeID Remove::Status encoding

Value	Status identifier	Description
0x01	DONE	The process was completed successfully.
0x00	FAILED_NODE_NOT_FOUND	The requested process failed. The NodeID was not found in the controller list of failing nodes.
0x02	FAILED_NODE_REMOVE_FAIL	The requested process failed. Reasons include: * Controller is busy * The node responded to a NOP; thus the node is no longer failing.

The removal process may fail if the requested NodeID responds to requests. The error message FAILED_NODE_REMOVE_FAIL does not indicate why the removal operation failed.

CC:0034.01.08.12.001 A network management application SHOULD issue a NOP for the requested NodeID to test if the node is actually responding again.

NodeID (1 byte)

This field is used to specify the NodeID of the failing node which was attempted to be removed.

4.4.8.7 Failed Node Replace Command

This command is used to replace a non-responding node with a new one reusing the NodeID of the failed node.

A non-responding node is put onto the failed NodeID list in the controller. In case the node responds
CC:0034.01.09.11.001 again at a later stage then it is removed from the failed NodeID list. A node MUST be on the failed NodeID list and as an extra precaution also fail to respond before it is removed or replaced. Responding nodes MUST NOT be removed.

CC:0034.01.09.11.008 The Failed Node Replace Status Command MUST be returned in response to this command when the replacement attempt has been made unless it is ignored.

CC:0034.01.09.11.003 This command MUST NOT be issued via multicast addressing.
CC:0034.01.09.11.004 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_FAILED_NODE_REPLACE (0x09)							
Seq No							
NodeID							
tx Options							
Mode							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management

NodeID (1 byte)

CC:0034.01.09.11.005 This field is used to specify the NodeID of the failing node which MUST be replaced.

tx Options (1 byte)

CC:0034.01.09.11.006 The tx Options field allows a controlling node to specify if transmissions MUST use special properties. The field MUST comply with Table 21.

Table 21, Failed Node Replace::Tx Options encoding

Value	Option flags	Description
0x00	NULL	Transmit at normal power level without any transmit options.
0x02	TRANSMIT_OPTION_LOW_POWER	Transmit at low output power level (1/3 of normal RF range)

Mode (1 byte)

CC:0034.01.09.11.007 This field is use to indicate to the receiving node if the node replacement process must be activated or de-activated. This field MUST comply with Table 22.

Table 22, Failed Node Replace::Mode encoding

Value	Mode identifier	Description
0x01	START_FAILED_NODE_REPLACE	Initiate a failed node replace process.
0x05	STOP_FAILED_NODE_REPLACE	Cancel a failed node replace process. The command MAY be ignored if no replaced failed process is active. The command MAY be ignored if network inclusion is ongoing.

CC:0034.01.09.13.001

4.4.8.8 Failed Node Replace Status Command

This command is used to indicate the status of a failed node replacement attempt.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_FAILED_NODE_REPLACE_STATUS							
Seq No							
Status							
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management

Status (1 byte)

CC:0034.01.0A.11.001 This field is used to advertise status of the node replacement process. This field MUST comply with Table 23.

Table 23, Status parameter of Failed Node Remove ID::Status encoding

Value	Status identifier	Description
0x04	DONE	The process was completed successfully.
0x05	FAILED_NODE_REPLACE_FAIL	The requested process failed. Reasons include: * Controller is busy * The node responded to a NOP; thus the node is no longer failing.
0x09	FAILED_NODE_REPLACE_SECURITY_FAILED	Replace completed successfully but security handshake failed.

The replace process may fail if the requested NodeID responds to requests. The error message FAILED_NODE_REMOVE_FAIL does not indicate why the removal operation failed.

CC:0034.01.0A.12.001 A network management application SHOULD issue a NOP for the requested NodeID. If a response is received the user SHOULD be notified that the node must be removed using the normal removal operation.

NodeID (1 byte)

This field is used to specify the NodeID of the failing node which was attempted to be replaced.

4.4.8.9 Node Neighbor Update Request Command

This command is used to instruct a node with NodeID to perform a Node Neighbor Update operation in order to update the topology on the controller.

CC:0034.01.0B.11.001 The Node Neighbor Update Status Command MUST be returned in response to this command when the neighbor search is completed.

CC:0034.01.0B.11.002 This command MUST NOT be issued via multicast addressing.

CC:0034.01.0B.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_NEIGHBOR_UPDATE_REQUEST							
Seq No							
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management

NodeID (1 byte)

CC:0034.01.0B.11.004 This field is used to specify the NodeID of the failing node which MUST perform the Node Neighbor Update operation.

4.4.8.10 Node Neighbor Update Status Command

This command is used to report the status of a Node Neighbor Update operation.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_NEIGHBOR_UPDATE_STATUS							
Seq No							
Status							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management

Status (1 byte)

CC:0034.01.0C.11.001 This field is used to advertise status of the neighbor update operation. This field MUST comply with Table 24.

Table 24, Node Neighbor Update Status::Status encoding

Value	Status identifier	Description
0x22	NEIGHBOR_UPDATE_STATUS_DONE	New neighbor list received
0x23	NEIGHBOR_UPDATE_STATUS_FAIL	Getting new neighbor list failed

4.4.8.11 Return Route Assign Command

This command is used to make a controller assign static return routes (up to 4) to a slave node. This allows the slave nodes to communicate directly with other nodes.

Up to 5 different destinations can be allocated return routes. Attempts to assign new return routes when all 5 destinations already are allocated will be ignored.
Allocated return routes can only be cleared using the Return Route Delete Command.

The controller calculates the shortest routes from the slave node (Source NodeID field) to the destination node (Destination NodeID field) and transmits the return routes to the slave node (Source NodeID field).

CC:0034.01.0D.11.001 The Return Route Assign Complete Command MUST be returned in response to this command when the route assignment is completed.

CC:0034.01.0D.11.002 This command MUST NOT be issued via multicast addressing.
CC:0034.01.0D.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_RETURN_ROUTE_ASSIGN							
Seq No							
Source NodeID							
Destination NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Source NodeID (1 byte)

This field is used to specify the NodeID of the node which will be assigned the return route.

Destination NodeID (1 byte)

This field is used to specify the destination NodeID for which the Source NodeID will have a route assigned.

4.4.8.12 Return Route Assign Complete Command

This command is used to indicate the status of a return route assignment attempt.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_RETURN_ROUTE_ASSIGN_COMPLETE							
Seq No							
Status							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Status (1 byte)

CC:0034.01.0E.11.001 This field is used to advertise status of the return route assignment attempt. This field MUST comply with Table 25.

Table 25, Return Route Assign Complete::Status encoding

Value	Option identifier	Description
0x00	TRANSMIT_COMPLETE_OK	Successfully transmitted
0x01	TRANSMIT_COMPLETE_NO_ACK	No acknowledgement is received before timeout from the destination node. Acknowledgement is discarded in case it is received after the time out.
0x02	TRANSMIT_COMPLETE_FAIL	Not possible to transmit data because the Z-Wave network is busy (jammed).

4.4.8.13 Return Route Delete Command

This command is used to make a controller delete all static return routes from a slave node. Allocated return routes can only be removed using this command. All return routes are cleared when using this command.

CC:0034.01.0F.12.001 After issuing this command, an application SHOULD issue Return Route Assign Commands to create return routes for all relevant associations.

CC:0034.01.0F.11.001 The Return Route Delete Complete Command MUST be returned in response to this command.

CC:0034.01.0F.11.002 This command MUST NOT be issued via multicast addressing.

CC:0034.01.0F.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_RETURN_ROUTE_DELETE (0x0F)							
Seq No							
NodeID							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

NodeID (1 byte)

CC:0034.01.0F.11.004 This field is used to specify the NodeID of which the return routes MUST be deleted.

4.4.8.14 Return Route Delete Complete Command

This command is used to indicate the status of a return route deletion attempt.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_RETURN_ROUTE_DELETE_COMPLETE (0x10)							
Seq No							
Status							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Status (1 byte)

CC:0034.01.10.11.001 This field is used to advertise status of the return route deletion attempt. This field MUST comply with Table 26.

Table 26, Return Route Delete Complete::Status encoding

Value	Option identifier	Description
0x00	TRANSMIT_COMPLETE_OK	Successfully transmitted
0x01	TRANSMIT_COMPLETE_NO_ACK	No acknowledge is received before timeout from the destination node. Acknowledge is discarded in case it is received after the time out.
0x02	TRANSMIT_COMPLETE_FAIL	Not possible to transmit data because the Z-Wave network is busy (e.g. jammed).

4.4.8.15 Use cases and frame flows

4.4.8.15.1 Z/IP Client requesting a node to interrupt Add Mode.

The frame flow for interrupting Add Mode is shown in Figure 12.

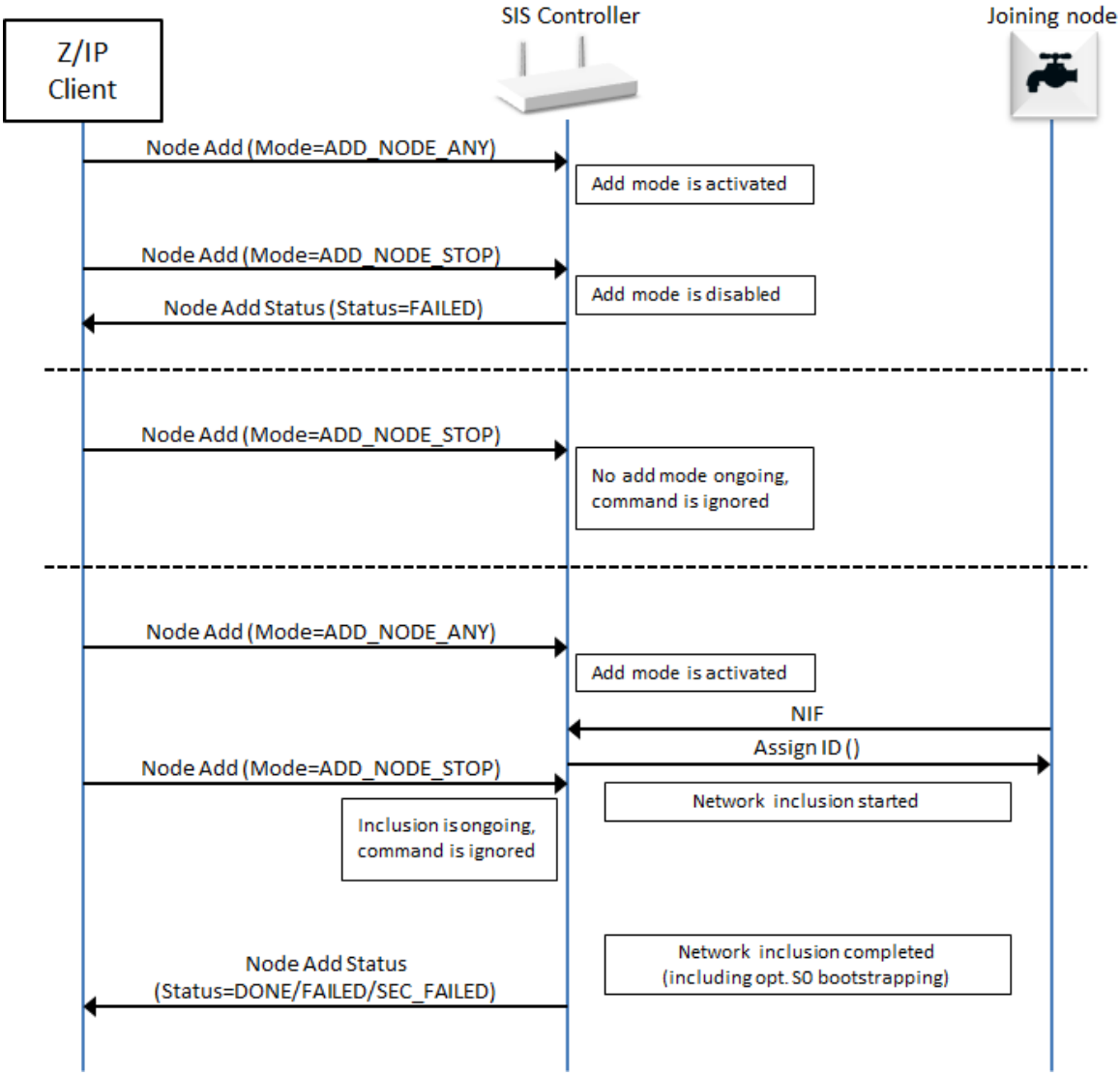

Figure 12, Z/IP Client requesting a node to interrupt Add Mode

4.4.9 Network Management Inclusion Command Class, version 2

4.4.9.1 Compatibility considerations

CC:0034.02.00.21.001

The Network Management Inclusion Command Class, version 2 is backwards compatible with Network Management Inclusion Command Class, version 1. A node supporting Network Management Inclusion Command Class, version 2 MUST also support Network Management Inclusion Command Class, version 1.

All commands not mentioned in this version remain unchanged from version 1.

The following commands are introduced to support the multiple security keys and DSK functionalities of the Security 2 Command Class:

- Node Add Keys Report Command
- Node Add Keys Set Command
- Node Add DSK Report Command
- Node Add DSK Set Command

The following command has been extended to support the new S2/inclusion controller bootstrapping process:

- Node Add Command
- Node Add Status Command
- Failed Node Replace Command
- Failed Node Replace Status Command

Use-cases and frames flows for the new functionalities of this Command Class are shown in 4.4.9.10 Use cases and frame flows

4.4.9.2 Node Add Command

This command is used to add nodes to the Z-Wave network.

CC:0034.02.01.11.005 The Node Add Status Command MUST be returned in response to this command unless it is to be ignored.

CC:0034.02.01.11.002 This command MUST NOT be issued via multicast addressing.
CC:0034.02.01.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD (0x01)							
Seq No							
Reserved							
Mode							
tx Options							

Fields not described in this version remain unchanged from version 1.

Mode (1 byte)

CC:0034.02.01.11.004 This field is use to indicate to the receiving node which mode to use for the inclusion of a new node. This field MUST comply with Table 27.

Table 27, Encoding of Node Add :: Mode parameter

Value	Identifier	Description	Version
0x01	NODE_ADD_ANY	Add any type of node to the network and allow Security 0 bootstrapping	1
0x05	NODE_ADD_STOP	Stop Add Mode. The command MAY be ignored if Add Mode was not activated. The command MAY be ignored if network inclusion or security bootstrapping is ongoing.	1
0x07	NODE_ADD_ANY_S2	Add any type of node to the network and allow Security 0 or Security 2 bootstrapping	2

CC:0034.02.01.13.001

Examples of Add Mode activation and deactivation are also given in 4.4.8.15.1 Z/IP Client requesting a node to interrupt Add Mode..

4.4.9.3 Node Add Status Command

This command is used to report the result of a node inclusion.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD_STATUS (0x02)							
Seq No							
Status							
Reserved							
New NodeID							
Node Info Length							
List.	Z-Wave Protocol Specific Part						
Opt. Func.	Z-Wave Protocol Specific Part						
Basic Device Class							
Generic Device Class							
Specific Device Class							
Command Class 1 *)							
...							
Command Class N *)							
Granted Keys							
KEX Fail Type							

*) Command classes may be extended ⇒ spanning two bytes for one command class

Fields not described in this version remain unchanged from version 1.

Command Class (N bytes)

Refer to 4.4.4.4 Node Info Cached Report Command and Table 8.

CC:0034.02.02.11.001 The Security Command Class Mark (0xF100) MUST indicate command classes supported using the highest listed Security Key in the Granted Key field value.

Granted Keys (8 bits)

CC:0034.02.02.11.002 This field is used to indicate which network keys were granted during bootstrapping.
This field MUST be treated as a bitmask and comply with Table 28

Table 28, Node Add Status::Granted keys encoding

Bit	Description
0	Indicates the Unauthenticated Security Class Key
1	Indicates the Authenticated Security Class Key
2	Indicates the Access Control Security Class Key
7	Indicates the Security 0 Network Key

KEX Fail Type (8 bits)

CC:0034.02.02.11.003

This field is used to indicate which error occurred in case S2 bootstrapping was not successful. This field MUST comply with Table 29.

Table 29, Node Add Status::Kex Fail Type encoding

Value	KEX Fail Type Identifier	Description
0x00	-	Bootstrapping was successful
0x01	KEX_FAIL_KEX_KEY	Key failure indicating that no match exists between requested/granted keys in the network.
0x02	KEX_FAIL_KEX_SCHEME	Scheme failure indicating that no scheme is supported by controller or joining node specified an invalid scheme.
0x03	KEX_FAIL_KEX_CURVES	Curve failure indicating that no curve is supported by controller or joining node specified an invalid curve.
0x05	KEX_FAIL_DECRYPT	Node failed to decrypt received frame.
0x06	KEX_FAIL_CANCEL	User has cancelled the S2 bootstrapping.
0x07	KEX_FAIL_AUTH	The Echo KEX Set/Report frame did not match the earlier exchanged frame.
0x08	KEX_FAIL_KEY_GET	The joining node has requested a key, which was not granted by the including node at an earlier stage.
0x09	KEX_FAIL_KEY_VERIFY	Including node failed to decrypt and hence verify the received frame encrypted with exchanged key.
0x0A	KEX_FAIL_KEY_REPORT	The including node has transmitted a frame containing a different key than what is currently being exchanged.

4.4.9.4 Node Add Keys Report Command

This command is used to inform which S2 keys have been requested during S2 bootstrapping.

CC:0034.02.11.11.001 The Node Add Keys Set Command MUST be returned in response to this command.

CC:0034.02.11.11.002 This command MUST NOT be issued via multicast addressing.

CC:0034.02.11.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD_KEYS_REPORT (0x11)							
Seq No							
Reserved							Request CSA
Requested Keys							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Request CSA (1 bit)

This field is used to indicate if the joining node is requesting CSA (Client-Side Authentication, refer to [14]).

CC:0034.02.11.11.004 The value 1 MUST indicate that the node requests CSA.
The value 0 MUST indicate that the node does not request CSA.

Requested Keys (1 bytes)

This field is used to advertise the requested keys by the joining node.

CC:0034.02.11.11.005 This field MUST be treated as a bitmask and comply with Table 28

4.4.9.5 Node Add Keys Set Command

This command is used to inform an S2 bootstrapping controller which keys must be granted to the node being bootstrapped.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD_KEYS_SET							
Seq. No							
Reserved						Grant CSA	Accept
Granted Keys							

Seq. No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Grant CSA (1 bit)

CC:0034.02.12.11.001 This field is used to indicate if the S2 bootstrapping controller MUST allow CSA for Authentication. (refer to [14]).

CC:0034.02.12.11.002 The value 1 MUST indicate that the node MUST allow CSA.
The value 0 MUST indicate that the node MUST NOT allow CSA.

Granted Keys (8 bits)

This field is used to indicate which network keys were granted during bootstrapping.
CC:0034.02.12.11.003 This field MUST be treated as a bitmask and comply with Table 28.

CC:0034.02.12.11.004 This field MUST be set to 0x00 if the Accept field is set to 0.

Accept (1 bit)

This field is used to indicate if the S2 bootstrapping process is accepted by the user and must continue.

CC:0034.02.12.11.005 The value 0 MUST indicate that the S2 bootstrapping is not accepted and MUST be interrupted.
The value 1 MUST indicate that the S2 bootstrapping is accepted and MUST continue.

4.4.9.6 Node Add DSK Report Command

This command is used to report the DSK of the node being S2 bootstrapped and indicates whether an input is needed for node authentication.

CC:0034.02.13.11.001 The Node Add DSK Set Command MUST be returned in response to this command.

CC:0034.02.13.11.002 This command MUST NOT be issued via multicast addressing.

CC:0034.02.13.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD_DSK_REPORT							
Seq No							
Reserved				Input DSK Length			
DSK 1							
…							
DSK 16							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Input DSK Length (4 bits)

CC:0034.02.13.11.004 This field is used to indicate how many DSK bytes MUST be input as a minimum to authenticate the node being included.

CC:0034.02.13.11.005 The value 0 MUST indicate that no user input is necessary (e.g. Unauthenticated Security Class or CSA has been granted).

DSK (16 bytes)

This field is used to transmit the DSK of the node being S2 bootstrapped. Refer to [14].

4.4.9.7 Node Add DSK Set Command

This command is used to indicate the S2 bootstrapping controller if the DSK is accepted and report the user input when needed.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD_DSK_SET							
Seq No							
Accept	Reserved			Input DSK Length			
Input DSK 1							
…							
Input DSK N							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Input DSK Length (4 bits)

This field indicates the length in bytes of the DSK input by the user.

CC:0034.02.14.11.001 This field MUST be set to the same or a higher value than the “Input DSK Length” field value received in the Node Add DSK Report Command that caused this command to be returned.

CC:0034.02.14.11.002 The value 0 MUST indicate that no user input has been done (e.g. Unauthenticated Security Class, CSA has been granted or user refused to input DSK).

Input DSK (N bytes)

CC:0034.02.14.11.003 This field indicates the DSK input by the user. A receiving node (Z/IP gateway) MUST overwrite the part of the DSK with the Input DSK contained in this frame

CC:0034.02.14.11.004 The length of this field in bytes MUST be according to the Input DSK Length field value. If the Input DSK Length is set to 0, this field MUST be omitted.

Accept (1 bit)

This field is used to indicate if the DSK Report is accepted by the user and if S2 bootstrapping must continue.

CC:0034.02.14.11.005 The value 0 MUST indicate that the DSK Report is not accepted and S2 bootstrapping MUST be interrupted.
The value 1 MUST indicate that the DSK Report is accepted and S2 bootstrapping MUST continue.

4.4.9.8 Failed Node Replace Command

This command is used to replace a non-responding node with a new one in having the same NodeID.

CC:0034.02.09.11.005 The Failed Node Replace Status Command MUST be returned in response to this command unless it is to be ignored.

CC:0034.02.09.11.002 This command MUST NOT be issued via multicast addressing.
CC:0034.02.09.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_FAILED_NODE_REPLACE							
Seq No							
NodeID							
tx Options							
Mode							

Fields not described in this version remain unchanged from version 1.

Mode (1 byte)

This field indicates the type of operation for the failed replace process.
CC:0034.02.09.11.004 This field MUST comply with Table 30

Table 30, Failed Node Replace::Mode encoding

Value	Identifier	Description	Version
0x01	START_FAILED_NODE_REPLACE	Initiate a failed node replace process.	1
0x05	STOP_FAILED_NODE_REPLACE	Cancel a failed node replace process. The command MAY be ignored if no replaced failed process is active. The command MAY be ignored if network inclusion is ongoing	1
0x07	START_FAILED_NODE_REPLACE_S2	Initiate a failed node replace process and allow S2 bootstrapping for the new node	2

CC:0034.02.09.13.001

4.4.9.9 Failed Node Replace Status Command

This command is used to indicate the progress of the Replace Failed Node Command.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_FAILED_NODE_REPLACE_STATUS							
Seq No							
Status							
Node ID							
Granted Keys							
KEX Fail Type							

Fields not described in this version remain unchanged from version 1.

Granted Keys (8 bits)

This field is used to indicate which network keys were granted during bootstrapping.
CC:0034.02.0A.11.001 This field MUST be treated as a bitmask and comply with Table 28

KEX Fail Type (8 bits)

Refer to 4.4.9.3 Node Add Status Command and Table 29.

4.4.9.10 Use cases and frame flows

4.4.9.10.1 Z/IP Client with SIS or Primary controller including an S2 node

The frame flow for an S2 capable node inclusion using the Network Management Inclusion Command Class is shown in Figure 13.

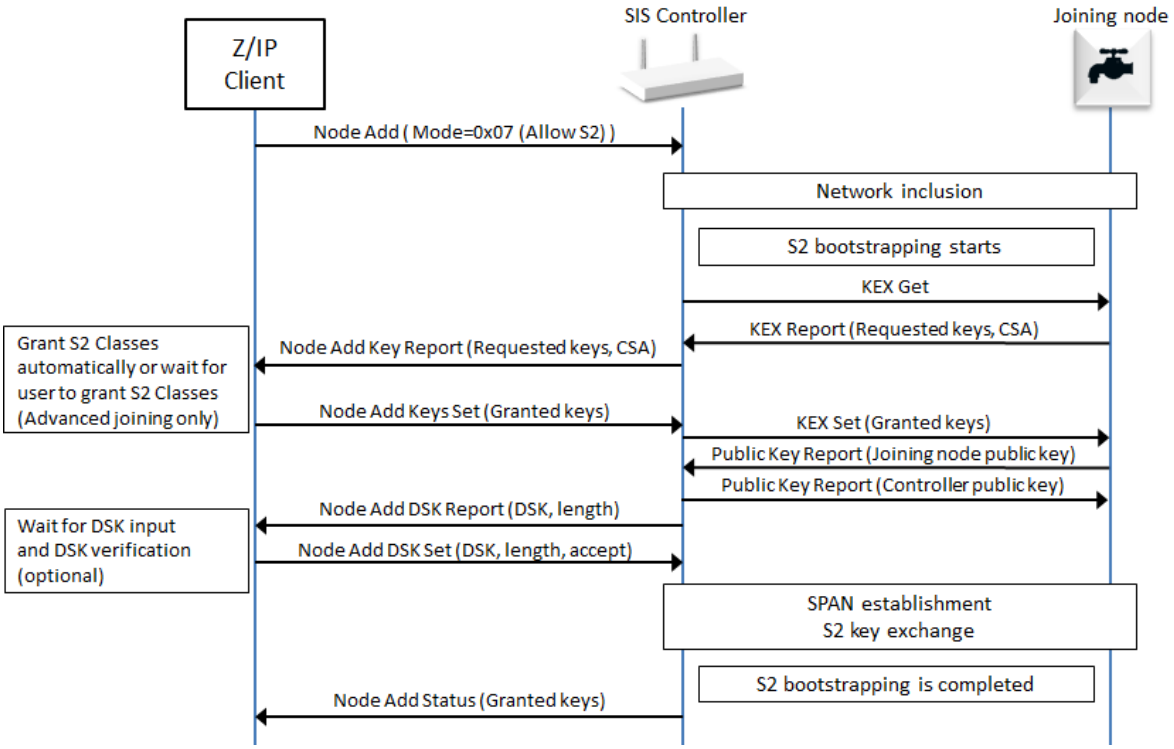

Figure 13, Node inclusion with a SIS/Primary controller

4.4.9.10.2 Z/IP Client with an S2 inclusion controller including an S2 node

When performing S2 bootstrapping, the unsolicited destination of the Z/IP Gateway will receive a unsolicited Node Add S2 Keys Report from the Z/IP Gateway. The Z/IP Client at this point has two options:

CC:0034.02.00.11.001

1. Automatically grant requested S2 Classes without presenting a user dialog in the S2 Keys Report step. In this case, the Z/IP Client MUST present a user dialog in next step before sending the DSK Set

CC:0034.02.00.11.002
CC:0034.02.00.13.001

2. Using advanced joining where the user MUST confirm the specific keys being requested in a dialog, before continuing to next step. In this case, the Z/IP MAY present a user dialog in next step before sending the DSK Set, if required by the S2 Classes being granted.

This is done without the SIS having entered Add Node mode. From this point on the S2 inclusion frame flow is same as when including through the SIS.

The frame flow for the node inclusion when an S2 capable inclusion controller has been used for including a new S2 capable node is shown in Figure 14.

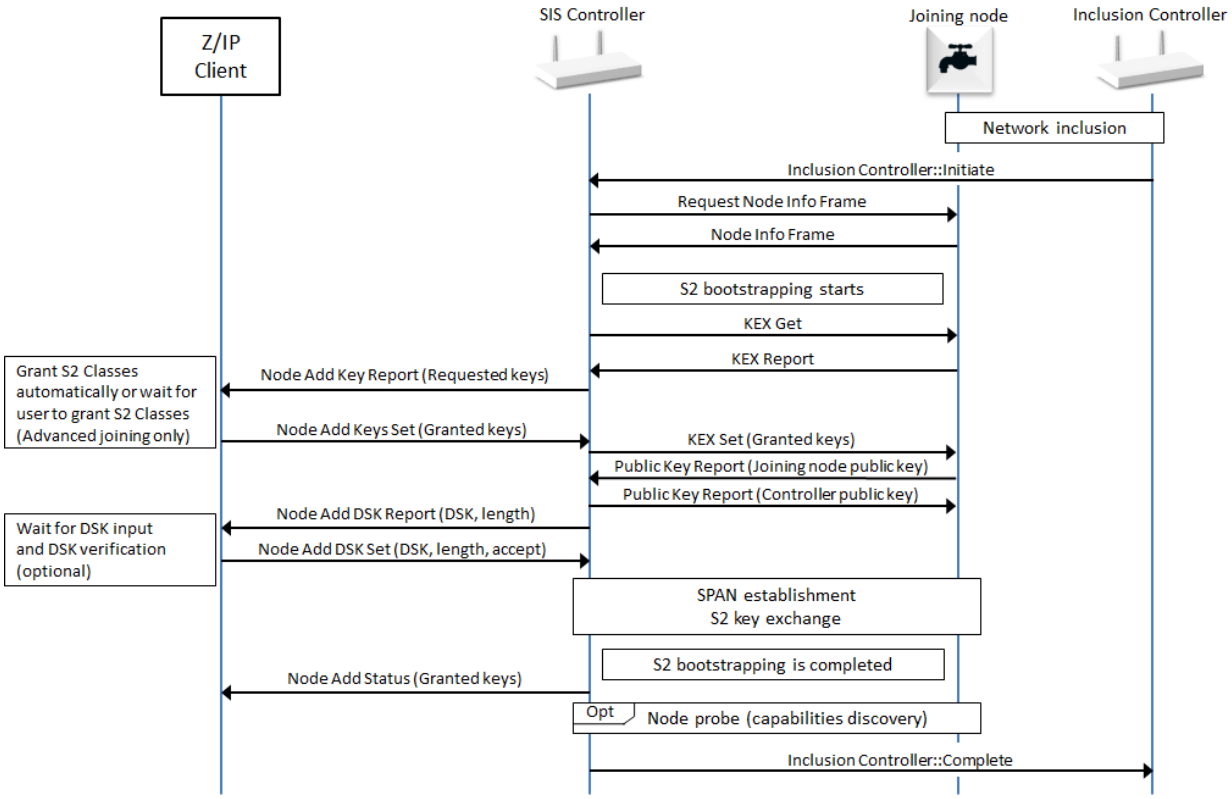

Figure 14, Node inclusion with an S2 inclusion controller

4.4.9.10.3 Z/IP Client with an S2 inclusion controller including an S0 node

CC:0034.02.00.13.002

The unsolicited destination of the Z/IP Gateway will receive an unsolicited Node Add Status Report from the Z/IP Gateway. The unsolicited destination Z/IP Client MAY show a dialog informing that a node was included by an inclusion controller.

The frame flow for an S0 capable node inclusion using an S2 capable inclusion controller including is shown in Figure 15.

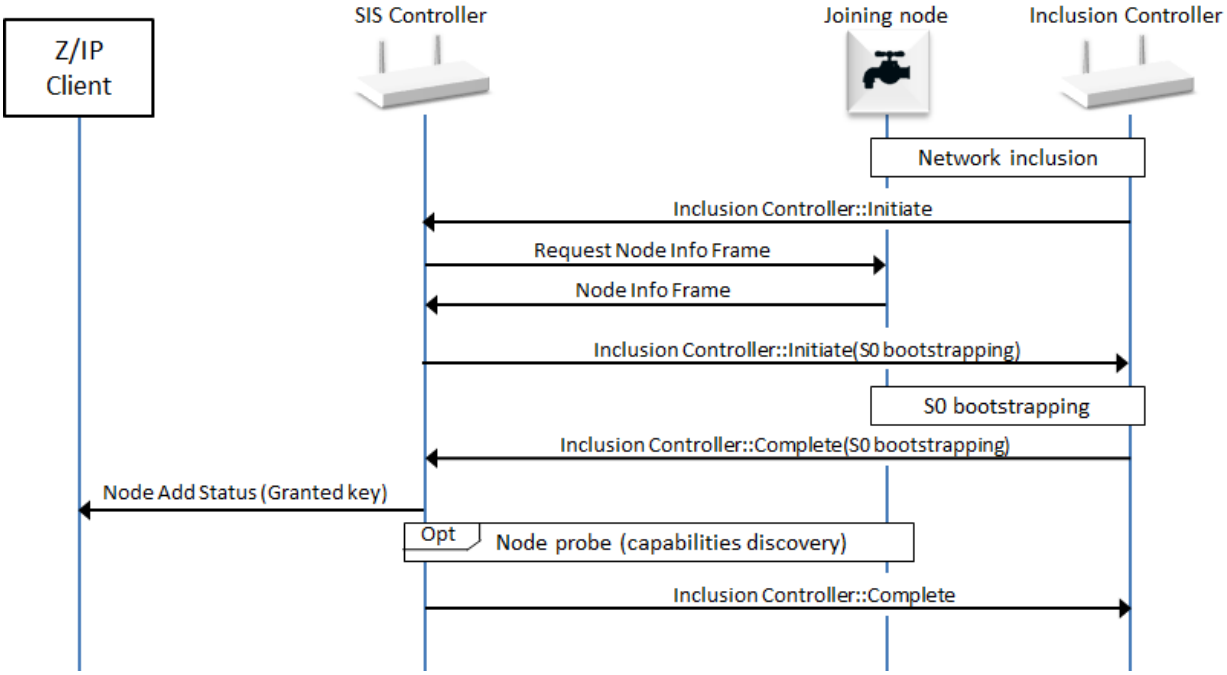

Figure 15, S0 node inclusion with an S2 inclusion controller

4.4.10 Network Management Inclusion Command Class, version 3

4.4.10.1 Compatibility considerations

The Network Management Inclusion Command Class, version 3 is backwards compatible with the Network Management Inclusion Command Class, version 2.

CC:0034.03.00.21.001 A node supporting the Network Management Inclusion Command Class, version 2 MUST also support the Network Management Inclusion Command Class, version 2.

CC:0034.03.00.21.002 All commands and fields not mentioned in this version MUST remain unchanged from version 2.

The following command has been extended to support the report of a Smart Start node:

- Node Add Status Command

The following commands are introduced in order to support the Smart Start functionality:

- Included Node Information Frame Report Command
- Smart Start Join Started Command

CC:0034.03.00.21.003 Frame flows for the new functionalities of this Command Class are shown in 4.4.10.5 Usage and frame flows. A Z/IP Gateway MUST comply with 4.4.10.5 Usage and frame flows.

CC:0034.03.00.21.004 A supporting node MUST issue the Node Add Status Command, Included Node Information Frame Report Command and the Smart Start Join Started Command to the first and the second unsolicited destinations.

4.4.10.1.1 Command Class dependencies

CC:0034.03.00.21.005 A node supporting the Network Management Inclusion Command Class, version 3 MUST also support the Node Provisioning Command Class, version 1.

4.4.10.2 Node Add Status Command

This command is used to report the result of the Node Add Command or report that a new node was included.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_NODE_ADD_STATUS (0x02)							
Seq No.							
Status							
Reserved							
New NodeID							
Node Info Length							
List.	Z-Wave Protocol Specific Part						
Opt. Func.	Z-Wave Protocol Specific Part						
Basic Device Class							
Generic Device Class							
Specific Device Class							
Command Class 1 *)							
…							
Command Class N *)							
Granted Keys							
KEX Fail Type							
Reserved				DSK Length			
DSK 1							
…							
DSK L							

CC:0034.03.02.11.001 Fields not described below MUST remain unchanged from version 2.

Status (8 bits)

CC:0034.03.02.11.002 This field indicates the outcome of the add mode and MUST comply with Table 31.

Table 31, Node Add Status::Status parameter encoding

Value	Status identifier	Description	Version
0x06	ADD_NODE_STATUS_DONE	The new node has been included in the network. If the new node and controller support S0 or S2, it indicates that the network inclusion and security bootstrapping were completed successfully. (This includes the case where the node was granted no S2 key)	1
0x07	ADD_NODE_STATUS_FAILED	The process failed, no new node was added in the network. Version 3: This status is also used if the node failed a smart start inclusion and has been removed. In this case, it may attempt the inclusion again.	1
0x09	ADD_NODE_STATUS_SECURITY_FAILED	Node has been included but the security bootstrapping failed	1

DSK Length (5 bits)

CC:0034.03.02.11.003 This field MUST indicate the length of the DSK field in bytes.

CC:0034.03.02.11.004 This field MUST be set to 0 if the added node does not support the S2 Command Class.

CC:0034.03.02.11.005 This field MUST be set to 16 if the added node supports the S2 Command Class.

DSK (L bytes)

CC:0034.03.02.11.006 This field MUST advertise the DSK of the node that has been added to the network.

CC:0034.03.02.11.007 The length of this field (in bytes) MUST be according to the DSK Length field value. This field MUST be omitted if the DSK Length field is set to 0.

4.4.10.3 Included Node Information Frame Report Command

CC:0034.03.19.11.006 This command MUST be sent to the (first and second) unsolicited destinations when an Included NIF (INIF) is received and the following conditions are fulfilled:

- The advertised NHID matches an entry in the provisioning list
- The advertised HomeID is different than the current network HomeID.

CC:0034.03.19.11.007 A node issuing this command MUST subsequently issue a Node Provisioning Report Command for the matched entry in the provisioning list.

With the two commands, a Z/IP client can use the relevant information to guide the user on how to perform a reset operation on the device.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_INCLUDED_NIF_REPORT (0x19)							
Seq No.							
Reserved				DSK Length			
DSK 1							
…							
DSK N							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Reserved

CC:0034.03.19.11.002 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

DSK Length (5 bits)

CC:0034.03.19.11.008 This field MUST indicate the length of the DSK field in bytes.
CC:0034.03.19.11.009 This field MUST be set to 16.

DSK (N bytes)

CC:0034.03.19.11.00A This field MUST advertise the DSK of the provisioning list entry that has been matched from the NHID in the received INIF.

CC:0034.03.19.11.00B The length of this field (in bytes) MUST be according to the DSK Length field value.

4.4.10.4 Smart Start Join Started Command

CC:0034.03.15.11.001 This command MUST be sent to the (first and second) unsolicited destinations when a Smart Start inclusion starts.

CC:0034.03.15.11.002 The Add Node Status Command MUST be issued after the Smart Start inclusion and S2 bootstrapping attempts took place.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION							
Command = COMMAND_SMART_START_JOIN_STARTED_REPORT (0x15)							
Seq No.							
Reserved				DSK Length			
DSK 1							
…							
DSK N							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

DSK Length (5 bits)

CC:0034.03.15.11.003 This field MUST indicate the length of the DSK field in bytes.

CC:0034.03.15.11.004 This field MUST be set to 16.

DSK (N bytes)

This field is used to advertise the DSK for the Provisioning List entry which starts the Smart Start inclusion process.

CC:0034.03.15.11.005 The length of this field (in bytes) MUST be according to the DSK Length field value.

4.4.10.5 Usage and frame flows

4.4.10.5.1 Z/IP Gateway adding a Smart Start node that is on the provisioning list.

The frame flow for a Smart Start inclusion of a node previously added on the provisioning list is shown in Figure 16.

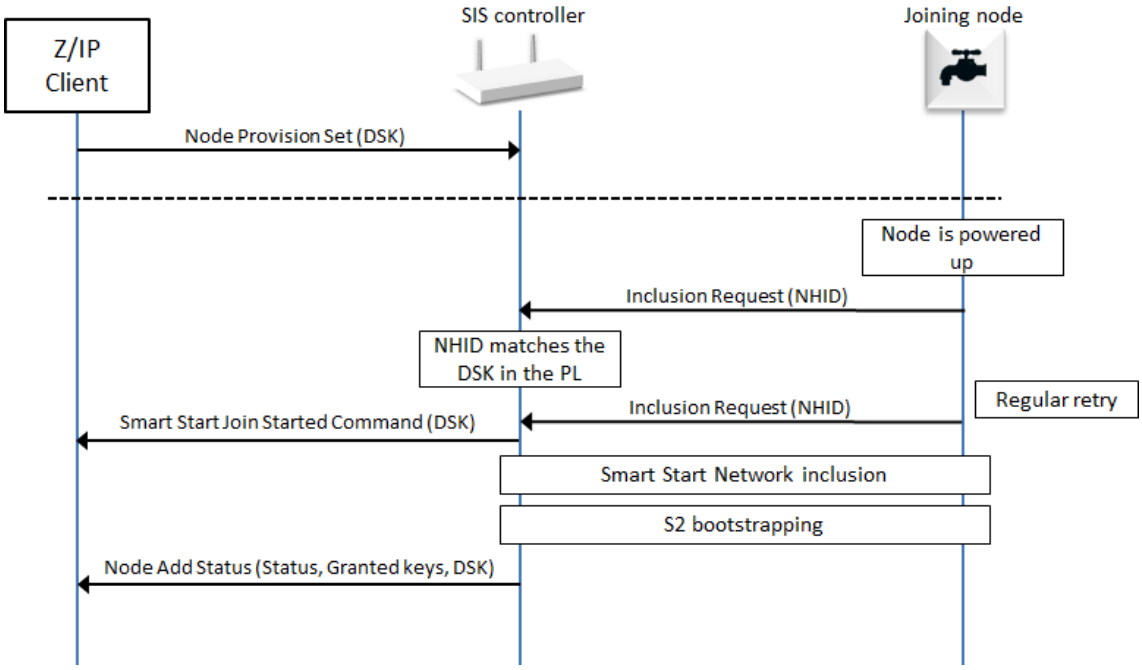

Figure 16, Smart Start inclusion

4.4.10.5.2 Z/IP Gateway adding a Smart Start node that is subsequently added on the provisioning list.

The frame flow for a Smart Start inclusion of a node subsequently added on the provisioning list is shown in Figure 17.

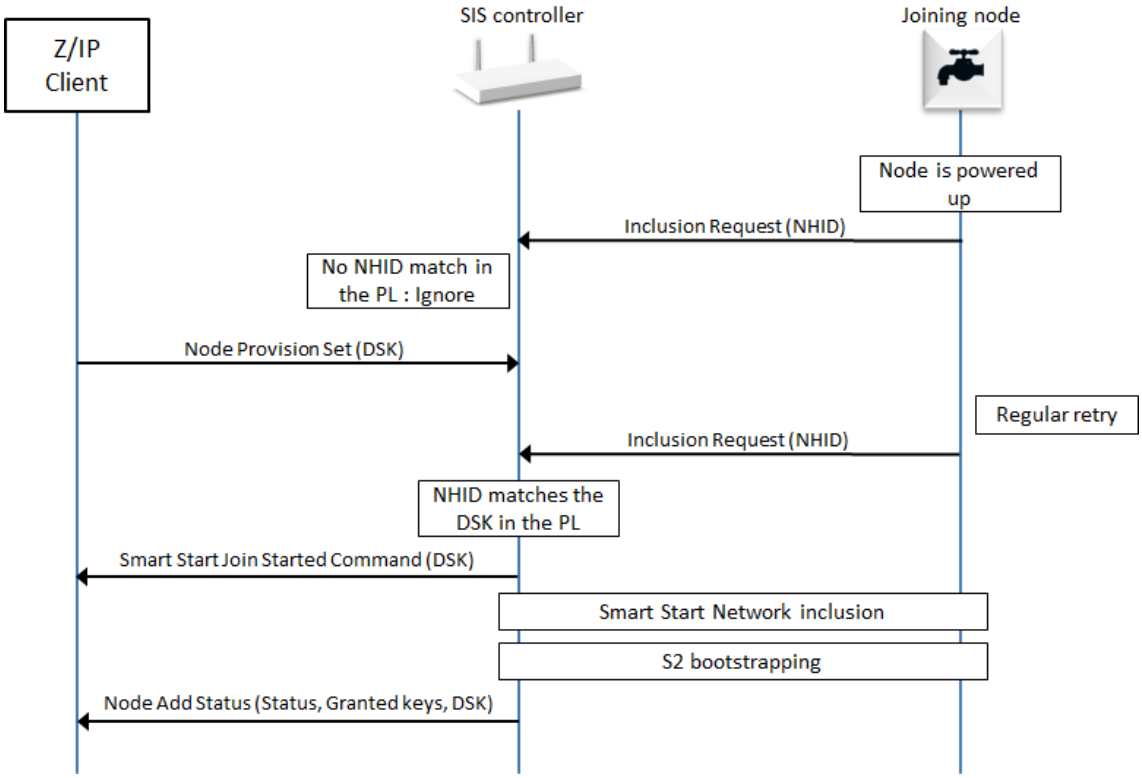

Figure 17, Smart Start inclusion (2)

4.4.10.5.3 Z/IP Gateway receiving an INIF from a node (the provisioning list) included in another network.

The frame flow for a Smart Start inclusion of a node included in another network is shown in Figure 18.

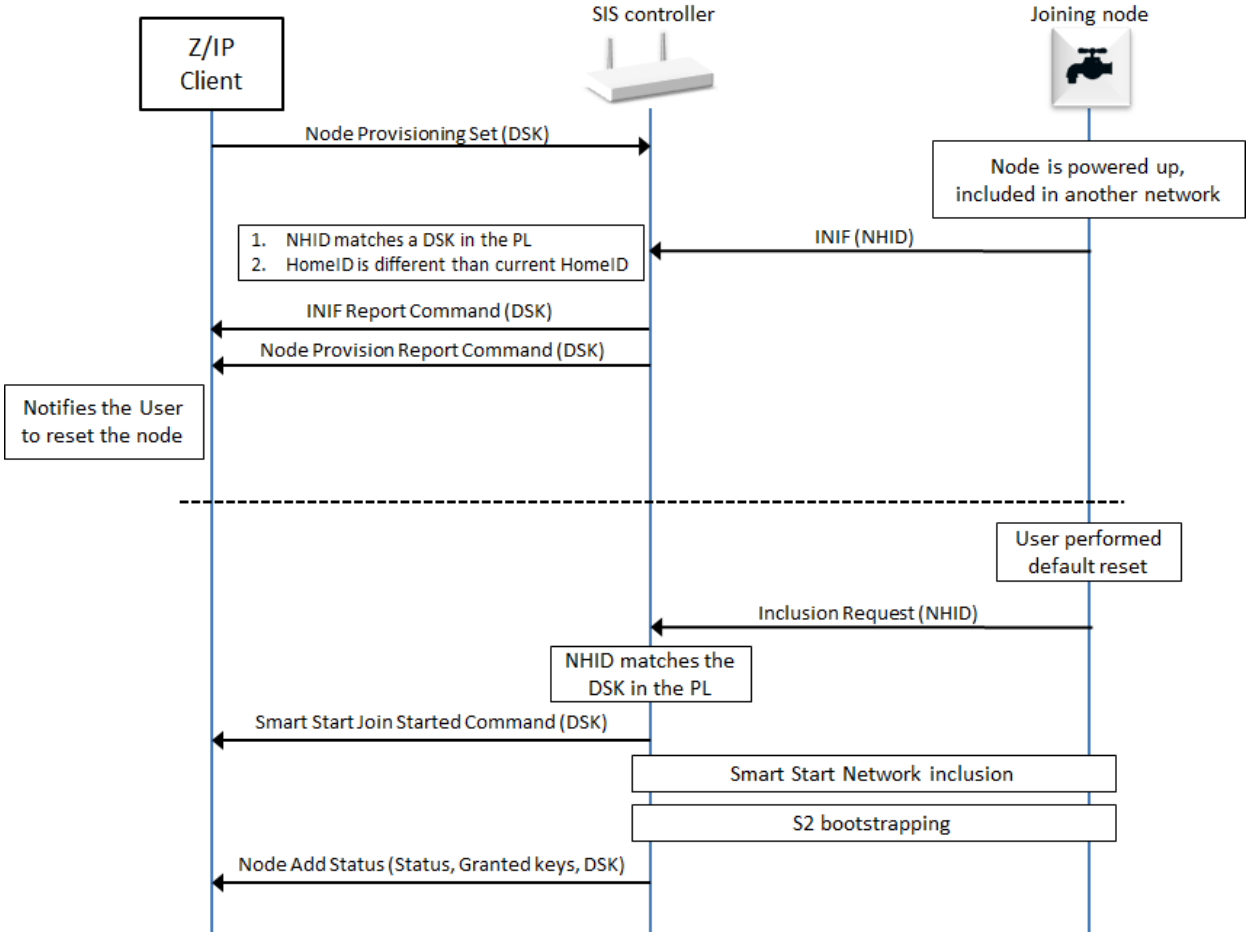

Figure 18, Smart Start inclusion (3)

4.4.10.5.4 Z/IP Gateway including an S2 only node that is on the provisioning list

The frame flow for an S2 only node (non-Smart Start) inclusion is shown in Figure 19. The Z/IP Client can decide to automatically grant the requested S2 keys or ask the user for confirmation.

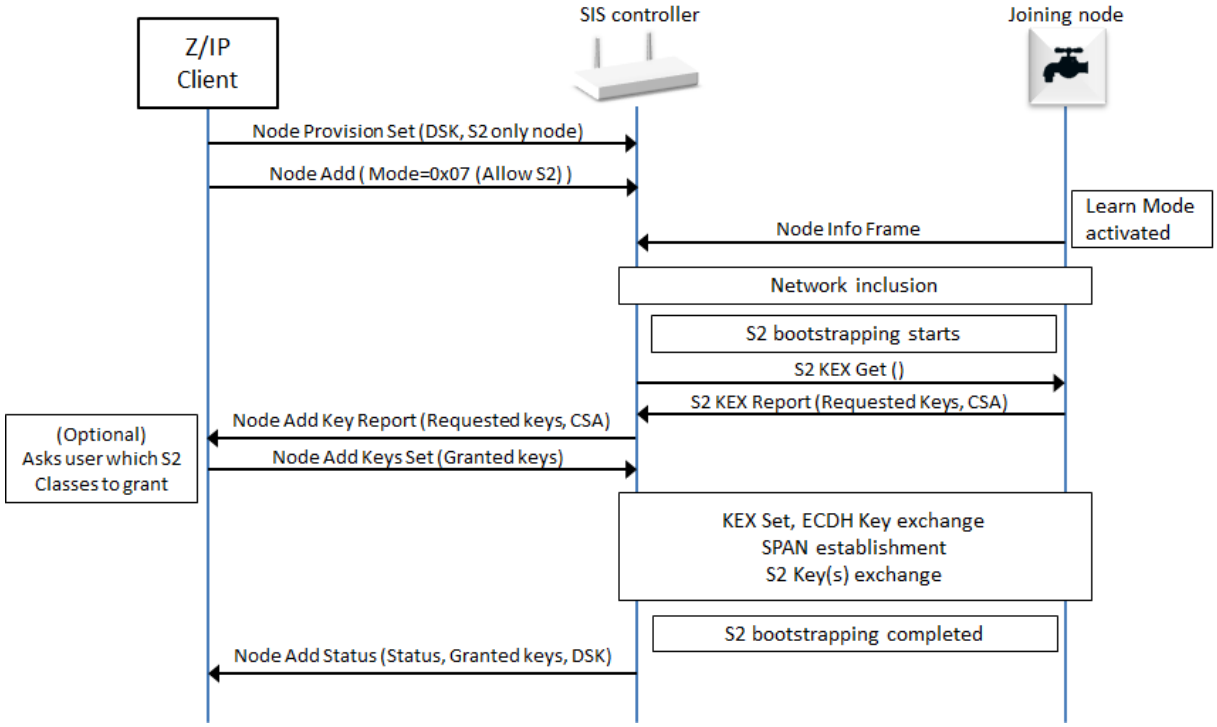

Figure 19, S2 Only Node inclusion with user interaction

4.4.11 Network Management Primary Command Class, version 1 [OBSOLETED]

THIS COMMAND CLASS HAS BEEN OBSOLETED

CC:0054.01.00.11.001 New implementations MUST NOT support this Command Class.

The Network Management Primary Command Class provides functions to pass on the primary role to another controller.

4.4.11.1 Controller Change Command

This command is used to add a controller node to the network and assign the primary controller role to the included controller.

This command has the same functionality as Node Add with the exception that the new controller will become the primary controller and the controller adding the node will become secondary.

CC:0054.01.01.11.001 The Controller Change Status Command MUST be returned in response to this command.

CC:0054.01.01.11.002 This command MUST NOT be issued via multicast addressing.
CC:0054.01.01.11.003 A receiving node MUST ignore this command if it is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PRIMARY							
Command = COMMAND_CONTROLLER_CHANGE							
Seq No							
Reserved							
Mode							
tx Options							

Seq No (1 byte)

Refer to 4.4.1.1 Sequence Number management.

Reserved

CC:0054.01.01.11.004 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Mode (1 byte)

CC:0054.01.01.11.005 This field is use to indicate to the receiving node if the controller change mode must be activated or de-activated. This field MUST comply with Table 32.

Table 32, Controller Change::Mode encoding

Value	Mode identifier	Description
0x02	CONTROLLER_CHANGE_START	Start the process of creating a new primary controller for the network
0x05	CONTROLLER_CHANGE_STOP	Stop the controller change and report a failure

tx Options (1 byte)

CC:0054.01.01.11.006

The tx Options field allows a controlling node to specify if transmissions MUST use special properties.. This field MUST be treated as a bitmask and MUST comply with Table 33

Table 33, Controller Change::Tx Options encoding

Value	Option identifier	Description
0x00	NULL	Transmit at normal power level without any transmit options.
0x02	TRANSMIT_OPTION_LOW_POWER	Transmit at low output power level (1/3 of normal RF range)
0x20	TRANSMIT_OPTION_EXPLORE	Resolve new routes via explorer discovery if existing routes fail

4.4.11.2 Controller Change Status Command

This command is used to advertise the outcome of the Controller Change attempt.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NETWORK_MANAGEMENT_PRIMARY							
Command = COMMAND_CONTROLLER_CHANGE_STATUS							
Seq No							
Status							
Reserved							
New NodeID							
Node Info Length							
List.	Z-Wave Protocol Specific Part						
Opt. Func.	Z-Wave Protocol Specific Part						
Basic Device Class							
Generic Device Class							
Specific Device Class							
Command Class 1 *)							
...							
Command Class N *)							

*) Command classes may be extended ⇒ spanning two bytes for one command class

For fields' description, refer to 4.4.8.2 Node Add Status Command.

4.4.12 Network Management Installation and Maintenance Command Class, version 1

The Network Management Installation and Maintenance Command Class is used to access statistical data. Data relating to the transmission of an actual frame may be obtained via the Z/IP Packet Installation and Maintenance Header Extension.

- **All Transmissions / Route Information:**
  - **Packet Error Count (PEC)** – Also sometimes referred to as PER.
    The number of unsuccessful transmissions experienced by the device.
  - **Transmission Counter (TC)** – Number of frames sent by the specified device.
  - **Neighbors (NB)** – Information on known neighbors for a specified device.
  - **Network Management - Priority Route Set**
  - **Network Management - Priority Route Get**
  - **Network Management - Priority Route Report**

4.4.12.1 Priority Route Set

This command is used to set the network route to use when sending commands to the specified NodeID.

CC:0067.01.01.12.001 The use of this command is NOT RECOMMENDED.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = PRIORITY_ROUTE_SET							
NodeID							
Repeater 1 [First repeater]							
Repeater 2							
Repeater 3							
Repeater 4 [Last repeater]							
Speed							

NodeID (1 byte)

CC:0067.01.01.11.001 This field is used to specify the destination NodeID for which a last working route MUST be set.

Repeater (4 bytes)

This field is used to specify repeaters for the route. Each byte represents a NodeID and the first field (Repeater 1) is the first repeater of the route.

CC:0067.01.01.11.002 The value 0x00 MUST indicate that the byte does not represent a repeater. If the route is shorter than four repeaters, unused repeaters fields MUST be set to 0x00. If Repeater 1 is set to 0x00, it means that the Last Working Route is direct (nodes are within direct reach).

Speed (1 byte)

CC:0067.01.01.11.003 This field is used to indicate which speed MUST be used for the route. This field MUST comply with Table 34.

Table 34, IME Speed Encoding

Value	Speed
0x01	9.6 kbit/sec
0x02	40 kbit/sec
0x03	100 kbit/sec

4.4.12.2 Priority Route Get

This command is used to query the current network route from a node for a given destination.

CC:0067.01.02.11.001 The Priority Route Report MUST be returned in response to this command.

CC:0067.01.02.11.002 This command MUST NOT be issued via multicast addressing.

CC:0067.01.02.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = PRIORITY_ROUTE_GET							
NodeID							

NodeID (1 byte)

This field is used to specify the NodeID destination for which the current network route is requested.

4.4.12.3 Priority Route Report

This command is used to advertise the current network route in use for an actual destination NodeID.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = PRIORITY_ROUTE_REPORT							
NodeID							
Type							
Repeater 1 – 1 [First repeater]							
Repeater 2 – 1							
Repeater 3 – 1							
Repeater 4 – 1 [Last repeater]							
Speed -1							

Type (1 byte)

CC:0067.01.03.11.001 This field is used to indicate the route type. It MUST comply with Table 35. A node MUST return the route with the highest priority value if several routes are available at the node.

Table 35, Route type encoding

Value	Identifier	Description	Priority
CC:0067.01.03.11.002 0x00	-	There is no route defined for the target NodeID. In this case, the Repeater and Speed fields MUST be set to 0x00 and ignored by a receiving node.	4 (lowest)
0x01	ZW_PRIORITY_ROUTE_ZW_LWR	The returned route is a last working route. The Last Working route is the last successful route used between the sender and receiver.	2
0x02	ZW_PRIORITY_ROUTE_ZW_NLWR	The returned route is a next to last working route. It is a route which was Last Working Route and has been replaced by a new route.	3
0x10	ZW_PRIORITY_ROUTE_APP_PR	The returned has been determined by the application	1 (highest)

Repeater (4 bytes)

Refer to 4.4.12.1 Priority Route Set.

Speed (1 byte)

Refer to 4.4.12.1 Priority Route Set.

4.4.12.4 Statistics Get

This command is used to query Installation and Maintenance statistics from a node.

CC:0067.01.04.11.001 The Statistics Report MUST be returned in response to this command.

CC:0067.01.04.11.002 This command MUST NOT be issued via multicast addressing.

CC:0067.01.04.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = STATISTICS_GET							
NodeID							

NodeID (1 byte)

This field is used to specify the NodeID for which statistics are requested.

4.4.12.5 Statistics Report

This command is used to report Installation and Maintenance statistics recorded by a node.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = STATISTICS_REPORT							
NodeID							
Statistics – Type 1							
Statistics – Length 1							
Statistics – Value 1							
…							
Statistics – Type N							
Statistics – Length N							
Statistics – Value N							

NodeID (1 byte)

CC:0067.01.04.11.004 This field MUST carry the same value as received in the Statistics Get Command.

Statistics (N bytes)

CC:0067.01.04.11.005 CC:0067.01.04.13.001 The statistics field MUST be formatted as cascaded Type-Length-Value (TLV) structures. The Z/IP Gateway MAY send any combination of TLV structures. Valid types are shown in Table 36.

Table 36, Statistics Get::Type encoding

Name	Statistics – Type	Statistics - Length (Bytes)
Route Changes (RC)	0	1
Transmission Count (TC)	1	1
Neighbors (NB)	2	n
Packet Error Count (PEC)	3	1
Sum of transmission times (TS)	4	4
Sum of transmission times squared (TS2)	5	4

CC:0067.01.04.11.006 All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.4.12.5.1 Route Changes (RC)

7	6	5	4	3	2	1	0
Statistics - Type = 0x00							
Statistics – Length = 1							
Statistics – Value = Route Changes							

Route Changes (1 byte)

The RC field is used to advertise the number of routing attempts needed to reach a destination. The number is a combination of Last Working Route (LWR) changes and Jitter measurements during transmission attempts between the Z/IP Gateway and the Z-Wave device.

RC is incremented automatically by the Z/IP Gateway when either of the below conditions are true:

- Last Working Route changed from the transmission of one command to the next
- $T_n - T_{n-1} > 150$ms *where T_n and T_{n-1} = the time needed to complete a transmission of a command*
  - IF 2 channel and FLIRS node, RC: $T_n = T_n \bmod 1100$
  - IF 3 channel and FLIRS node, RC cannot increment based on time calculation

4.4.12.5.2 Transmission Count (TC)

7	6	5	4	3	2	1	0
Statistics - Type = 0x01							
Statistics – Length = 1							
Statistics – Value = Transmission Count							

Transmission Count (1 byte)

Total number of transmissions sent by all Z/IP Clients through the Z/IP GW to the specified Z-Wave destination node.

4.4.12.5.3 Neighbors (NB)

7	6	5	4	3	2	1	0
Statistics - Type = 0x02							
Statistics – Length = N * 2							
Statistics – Value = NodeID 1							
Statistics – Value = Repeater 1	Reserved		Statistics – Value = Speed 1				
…							
Statistics – Value = NodeID N							
Statistics – Value = Repeater N	Reserved		Statistics – Value = Speed N				

NodeID (N * 1 byte)

The NodeID of the actual neighbor.

Speed (N * 4 bits)

Table 37, Statistics Report::Speed Encoding

Bitmask	Speed
0x01	9.6 kbit/sec
0x02	40 kbit/sec
0x04	100 kbit/sec

CC:0067.01.04.11.007 All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

Repeater (N * 1 bit)

If this bit is set then the node is a repeater.

4.4.12.5.4 Packet Error Count (PEC)

7	6	5	4	3	2	1	0
Statistics - Type = 0x03							
Statistics – Length = 1							
Statistics – Value = Packet Error Count							

Packet Error Count (1 byte)

CC:0067.01.04.11.008 Also sometimes referred to as PER. PEC is measured by the Gateway. The PEC value MUST be incremented each time the Gateway detects a failing transmission for each specific Z-Wave destination node.

4.4.12.5.5 Sum of transmission times (TS)

7	6	5	4	3	2	1	0
Statistics - Type = 0x04							
Statistics – Length = 4							
Statistics – Value = Sum of transmission times 1 (MSB)							
Statistics – Value = Sum of transmission times 2							
Statistics – Value = Sum of transmission times 3							
Statistics – Value = Sum of transmission times 4 (LSB)							

Sum of transmission times (4 bytes)

The sum of all transmission times. This may be used to calculate the average transmission time. The time is given as a 32-bit unsigned integer MSB in milliseconds.

$$\langle T \rangle = \frac{1}{N}\sum_{i}^{N} T_i$$

Where N is the number of transmissions.

4.4.12.5.6 Sum of transmission times squared (TS2)

7	6	5	4	3	2	1	0
Statistics - Type = 0x05							
Statistics – Length = 4							
Statistics – Value = Sum of transmission times squared 1 (MSB)							
Statistics – Value = Sum of transmission times squared 2							
Statistics – Value = Sum of transmission times squared 3							
Statistics – Value = Sum of transmission times squared 4 (LSB)							

Sum of transmission times squared (4 bytes)

The sum of the square of all transmission times. This may be used to calculate the variance of the transmission time. The time is given as a 32 bit unsigned integer MSB in milliseconds^2.

The Variance may be calculated as follows:

$$\langle T^2 \rangle = \frac{1}{N}\sum_{i}^{N} {T_i}^2$$

(König-Huygens theorem)

Where N is the number of transmissions.

A high variance is a sign of a bad link.

4.4.12.6 Statistics Clear

This command is used to clear all statistic registers maintained by the node.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = STATISTICS_CLEAR							

A receiving node MUST set all counters to 0.

4.4.12.7 Use Cases

4.4.12.7.1 Intranode network management: TV OSD System controlling lamps

Intranode network management is the process close to Z-Wave API programming. No messages ever leave the device. Messages only flow between different software modules.

Use Case: TV OSD System (island mode)

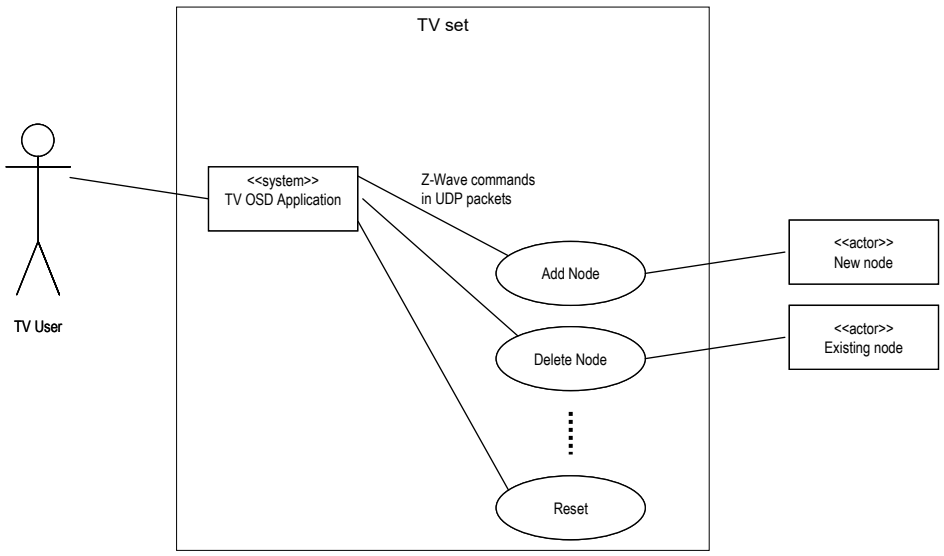

Figure 20, TV OSD System controlling lamps

Using UDP/IP for carrying the messages allows for a simple integration interface between applications designed by different partners.

4.4.12.7.2 Intranet network management: Remote controlling a primary controller

Intranet network management extends the use of command messages to separate physical devices. Messages flow between software modules but the modules reside in separate physical entities having individual IP addresses – or at least separate NodeIDs.

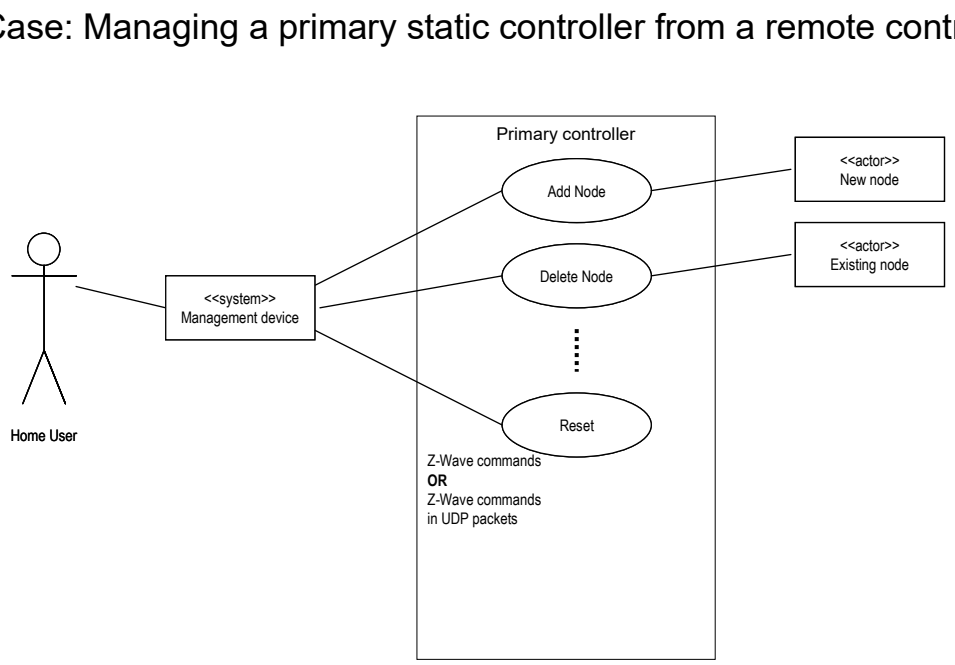

Figure 21, Managing a primary static controller from a remote control

Network management via messages allows for sophisticated interfaces to the primary controller of a network. Controllers with SUC/SIS capability may also leverage from the Network Management command classes.

4.4.12.7.3 Internet network management #1: Call-center support for TV OSD user

Internet network management uses the same command messages. Messages flow between software modules but the modules reside in separate physical entities in a non-trusted environment such as the Internet. Remote access technologies should be used to protect the communication.

In this use case a TV user may call the service provider for support in adding a new lamp to the network.

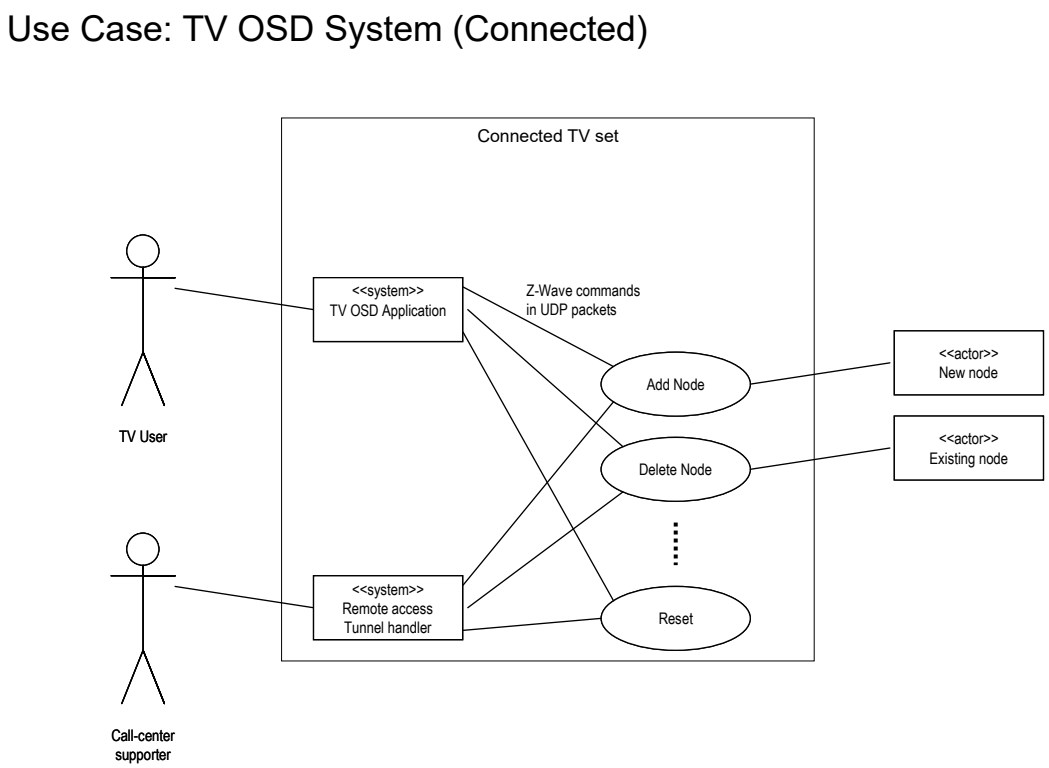

Figure 22, TV OSD System

4.4.12.7.4 Internet network management #2: Remote management of Z/IP Network

In this use case a user may use an IP based home control management system running in the LAN for setting up the Z/IP network. The user may use normal UDP transport in the LAN environment. Due to the critical nature of the network management command classes the user however should use remote access protection technologies over LAN as well as over Internet. The benefit of designing a home control system using remote access protection by default is that it may be moved from a location in the LAN to any place in the Internet and work completely unaffected.

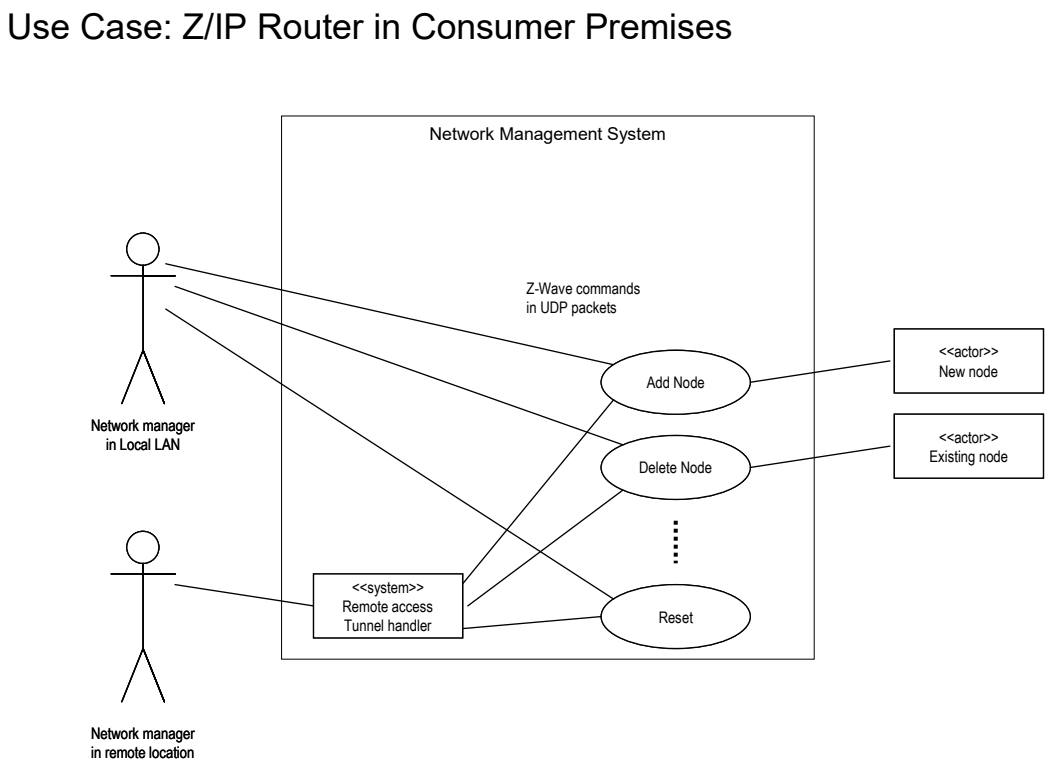

Figure 23, Z/IP Router in consumer premises

4.4.12.7.5 Traffic flow: Gathering node information

The following sequence diagram introduces a new concept of gathering Node Information.

The node list provides an overview of the nodes in the network; as good as the Z/IP gateway can provide this information. Using that node list, the requesting host may request information on individual nodes from the Z/IP Gateway. The “Node Info Cached Get” command reports all supported and controlled classes.

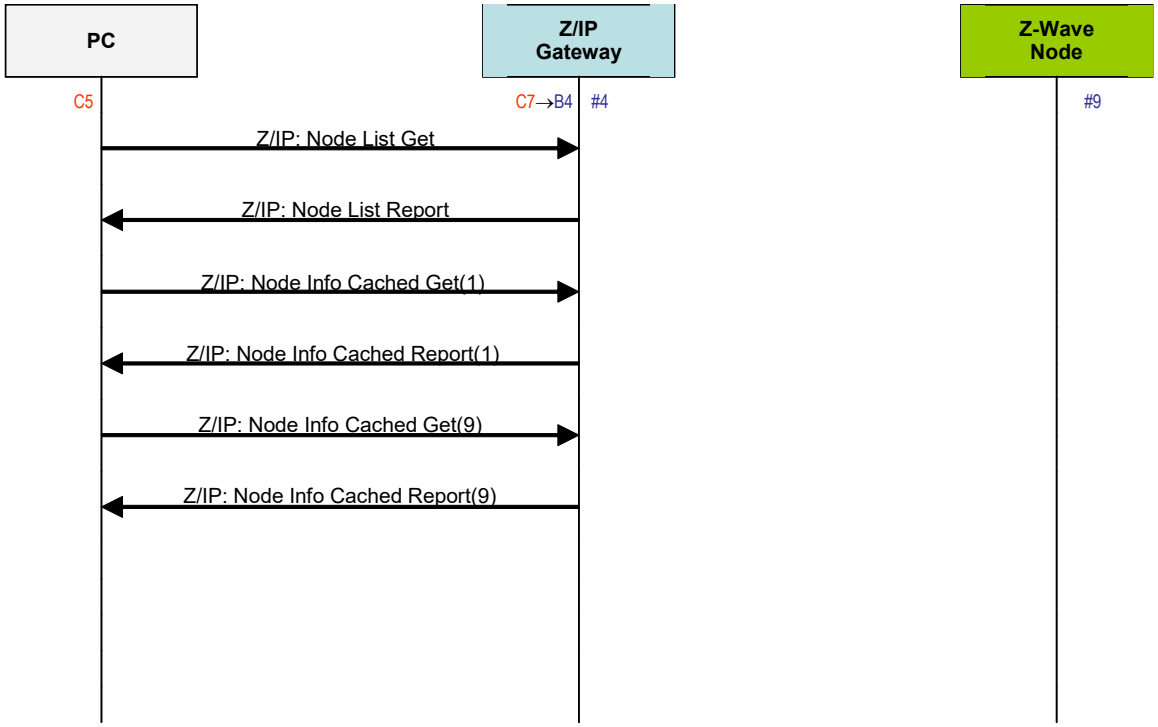

Figure 24, Gathering node information

4.4.13 Network Management Installation and Maintenance Command Class, version 2

4.4.13.1 Compatibility considerations

The Network Management Installation and Maintenance Command Class, version 2 is backwards compatible with the Network Management Installation and Maintenance Command Class, version 1.

CC:0067.02.01.21.002 All commands and fields not mentioned in this version MUST remain unchanged from version 1.

The following commands have been added to allow a supporting node to report the RSSI it measured in each channel of the network:

- RSSI Get Command
- RSSI Report Command

4.4.13.2 RSSI Get Command

This command is used to query the measured RSSI on the Z-Wave network from a node.

CC:0067.02.07.11.001 The RSSI Report Command MUST be returned in response to this command.

CC:0067.02.07.11.002 This command MUST NOT be issued via multicast addressing.

CC:0067.02.07.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = COMMAND_RSSI_GET (0x07)							

4.4.13.3 RSSI Report Command

This command is used to advertise the measured RSSI on the Z-Wave network for each used channel.

7	6	5	4	3	2	1	0
COMMAND_CLASS = NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE							
COMMAND = COMMAND_RSSI_REPORT (0x08)							
Channel 1 RSSI							
Channel 2 RSSI							
Channel 3 RSSI							

Channel 1 RSSI (8 bits)

CC:0067.02.08.11.001 This field MUST carry the measured RSSI value on channel 1.

CC:0067.02.08.11.002 This field MUST be encoded as using signed representation in the dBm unit and according to Table 38.

Channel 2 RSSI (8 bits)

CC:0067.02.08.11.003 This field MUST carry the measured RSSI value on channel 2.

CC:0067.02.08.11.004 This field MUST be encoded as using signed representation in the dBm unit and according to Table 38.

Channel 3 RSSI (8 bits)

CC:0067.02.08.11.005 This field MUST carry the measured RSSI value on channel 3, if applicable.

CC:0067.02.08.11.006 This field MUST be encoded as using signed representation in the dBm unit and according to Table 38.

Table 38, RSSI encoding

Value (signed)	Description
127 (0x7F)	RSSI_NOT_AVAILABLE. This value is returned for unused channels or if no RSSI measurement is available.
126 (0x7E)	RSSI_MAX_POWER_SATURATED This value is returned if the measured RSSI is above the maximum power.
125 (0x7D)	RSSI_BELOW_SENSITIVITY. This value is returned if the measured RSSI is below the receiver's sensitivity.
-32..-94 (0xE0..0xA2)	These values represent the actual RSSI measurement value from respectively -32 dBm to -94 dBm

CC:0067.02.08.11.007 All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.5 No Operation Command Class, version 1

The No Operation Command Class is used to check if a node is reachable by sending a Command less frame to the specified destination. Feature used by the Z-Wave protocol in many situations e.g. checking that an excluded node is non-responding. This Command can also be used on application level e.g. checking if a SUC/SIS is reachable from a new node in the network. This command class contains no command identifier and data.

Notice: It is not necessary to announce the No Operation Command Class in the NIF.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NO_OPERATION							

4.6 Node Provisioning Command Class, version 1

The Node Provisioning Command Class is used to manage a list of unique nodes (Node Provisioning List) in a Smart Start enabled controller or gateway.

4.6.1 Terminology

Smart start allows a controller to include new nodes in a network (or keep them out) without user interaction.

A Smart Start enabled controller or gateway maintains a Node Provisioning List or Provisioning List (PL). The Provisioning List is a list of unique nodes and their additional associated meta data necessary for performing their network inclusion and security bootstrapping.

A Provisioning List entry represents a node and its associated data. Provisioning List entries may also be used for ignoring nodes.

A Z/IP Client or controller can read and edit the Provisioning List entries of a Z/IP Gateway or controller using this Command Class.

4.6.2 Compatibility considerations

CC:0078.01.00.22.001 This Command Class MAY be carried in Z/IP Packets or in Z-Wave frames. However, this Command Class SHOULD only be used in Z/IP Packets.

CC:0078.01.00.21.001 A node supporting this Command Class MUST support at least 232 entries in its Node Provisioning List.

4.6.3 Security considerations

This Command Class allows a controlling node to include new nodes in the Z-Wave network and grant them all the security keys.

CC:0078.01.00.41.001 A node supporting this Command Class MUST NOT support it in a Z-Wave network if its highest Security Class is lower than S2 Access Control.

4.6.4 Node Provisioning Set Command

This command is used to create or update an entry in the node provisioning list of a supporting node.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NODE_PROVISIONING							
Command = COMMAND_NODE_PROVISIONING_SET (0x01)							
Seq No							
Reserved				DSK Length			
DSK 1							
…							
DSK N							
Meta Data Extension 1 (Optional)							
…							
Meta Data Extension M (Optional)							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Reserved

CC:0078.01.01.11.001 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

DSK Length (5 bits)

CC:0078.01.01.11.002 This field MUST indicate the length of the DSK field in bytes.

CC:0078.01.01.11.003 This field MUST be set to 16.

DSK (N bytes)

This field is used to advertise the DSK for the entry being added or updated.

CC:0078.01.01.11.004 A receiving node MUST add a new entry in the provisioning list if it does not have any entry with the advertised DSK value.

CC:0078.01.01.11.00D A receiving node MUST ignore a command attempting to create a new entry if the Provisioning List is full.

CC:0078.01.01.11.005 A receiving node MUST update the corresponding entry in the provisioning list if it already has an entry with the advertised DSK value.

CC:0078.01.01.11.006 The length of this field (in bytes) MUST be according to the DSK Length field value.

Meta Data Extension (M bytes)

This field is used to carry additional metadata associated to the node.

CC:0078.01.01.13.001 This field MAY contain zero, one or several extensions.

CC:0078.01.01.11.007 Each extension MUST comply with 4.6.10 Meta Data extension format and [22].

CC:0078.01.01.11.009 If the Bootstrapping mode Type (0x36) is omitted from this command, the Bootstrapping mode value 1 (Smart Start Mode) MUST be assumed by the receiving node when creating a new entry.

CC:0078.01.01.11.00B If the SmartStart Inclusion Setting Type (0x34) is omitted from this command, the Inclusion setting value 0 (Pending) MUST be assumed by the receiving node when creating a new entry that has a SmartStart Bootstrapping mode.

CC:0078.01.01.11.00A The Network Status Type (0x37) MUST NOT be carried in this command. The Network Status Type (0x37) MUST be ignored if received in this command.

4.6.5 Node Provisioning Delete Command

This command is used to delete one or all entries in the node provisioning list of a supporting node. Already included nodes will stay in the Z-Wave network even if no more corresponding node provisioning list entry is kept by the controller.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NODE_PROVISIONING							
Command = COMMAND_NODE_PROVISIONING_DELETE (0x02)							
Seq No							
Reserved				DSK Length			
DSK 1							
…							
DSK N							

Seq No (8 bits)

Refer to 4.4.1.1 Sequence Number management.

DSK Length (5 bits)

CC:0078.01.02.11.001 This field MUST indicate the length of the DSK field in bytes.
CC:0078.01.02.11.002 This field MUST be set to 0 or 16.

CC:0078.01.02.11.003 The value 0 MUST indicate that the receiving node MUST delete all entries in its Node Provisioning List.
CC:0078.01.02.11.004 The value 16 MUST indicate that the receiving node MUST delete the entry in its Node Provisioning List that match the advertised value in the DSK field.

DSK (N bytes)

This field is used to advertise the DSK for the entry being deleted.

CC:0078.01.02.11.005 A receiving node MUST delete the corresponding entry from the Node Provisioning List if it has an entry with the advertised DSK value.
CC:0078.01.02.11.006 A receiving node MUST ignore this command if it has no entry with the advertised DSK value.

CC:0078.01.02.11.007 The length of this field (in bytes) MUST be according to the DSK Length field value.
This field MUST be omitted if the DSK Length field is set to 0.

4.6.6 Node Provisioning Get Command

This command is used to request the metadata information associated to an entry in the node Provisioning List of the receiving node.

CC:0078.01.05.11.001 The Node Provisioning Report Command MUST be returned in response to this command.

CC:0078.01.05.11.002 This command MUST NOT be issued via multicast addressing.

CC:0078.01.05.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NODE_PROVISIONING							
Command = COMMAND_NODE_PROVISIONING_GET (0x05)							
Seq No							
Reserved			DSK Length				
DSK 1							
…							
DSK N							

Seq No. (8 bits)

Refer to 4.4.1.1 Sequence Number management.

DSK Length (5 bits)

CC:0078.01.05.11.004 This field MUST indicate the length of the DSK field in bytes.

CC:0078.01.05.11.005 This field MUST be set to 16.

DSK (N bytes)

This field is used to advertise the DSK for the entry being requested.

CC:0078.01.05.11.006 A receiving node MUST return the corresponding DSK entry if it has an entry matching the requested DSK in its Provisioning List.

CC:0078.01.05.11.007 A receiving node MUST return a report containing no DSK (DSK Length set to 0) if the requested DSK value is not in its Provisioning List.

CC:0078.01.05.11.008 The length of this field (in bytes) MUST be according to the DSK Length field value.

4.6.7 Node Provisioning Report Command

This command is used to advertise the contents of an entry in the node Provisioning List of the sending node.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NODE_PROVISIONING							
Command = COMMAND_NODE_PROVISIONING_REPORT (0x06)							
Seq No							
Reserved			DSK Length				
DSK 1 (Optional)							
…							
DSK N (Optional)							
Meta Data Extension 1 (Optional)							
…							
Meta Data Extension M (Optional)							

Seq No. (8 bits)

Refer to 4.4.1.1 Sequence Number management.

DSK Length (5 bits)

CC:0078.01.06.11.001 This field MUST indicate the length of the DSK field in bytes.

CC:0078.01.06.11.002 This field MUST be set to 0 or 16

CC:0078.01.06.11.003 The value 0 MUST indicate that the requested DSK is not present in the Provisioning List.

DSK (N bytes)

CC:0078.01.06.11.004 This field is used to advertise the DSK for the Provisioning List entry being advertised.

CC:0078.01.06.11.005 The length of this field (in bytes) MUST be according to the DSK Length field value. This field MUST be omitted if the DSK Length field is set to 0.

Meta Data Extension (M bytes)

This field is used to carry additional metadata associated to the Provisioning List entry.

CC:0078.01.06.13.001 This field MAY contain several extensions.

CC:0078.01.06.11.006 Each extension Type, Length and Value MUST comply with 4.6.10 Meta Data extension format and [22].

CC:0078.01.06.13.002 A supporting node MAY set the critical flag to 0 even when advertising critical extensions.

CC:0078.01.06.11.007 If the DSK Length field is set to 0, this field MUST be omitted.

If the DSK Length field is not set to 0:

CC:0078.01.06.11.008
- A sending node MUST advertise the SmartStart Inclusion Setting extension (type 0x34)

CC:0078.01.06.11.009
- A sending node MUST advertise the Bootstrapping mode extension (type 0x36)

CC:0078.01.06.11.00B
- A sending node MUST advertise the Network Status extension (type 0x37)

CC:0078.01.06.11.00A
- A sending node MUST advertise all other extension data kept in the Provisioning List

4.6.8 Node Provisioning List Iteration Get Command

This command is used to read the entire the provisioning list of a supporting node.

CC:0078.01.03.11.001 The Node Provisioning List Iteration Report Command MUST be returned in response to this command unless it is to be ignored.

CC:0078.01.03.11.002 This command MUST NOT be issued via multicast addressing.

CC:0078.01.03.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

CC:0078.01.03.11.004 A sending node MUST follow the frame flow in 4.6.11.1.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NODE_PROVISIONING							
Command = COMMAND_NODE_PROVISIONING_LIST_ITERATION_GET (0x03)							
Seq No.							
Remaining Counter							

Seq No. (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Remaining Counter (8 bits)

CC:0078.01.03.11.005 This field is used to iterate over the Provisioning List. The field indicates the remaining amount of entries in the Provisioning List. This field MUST be in the range 0x01..0xFF.

CC:0078.01.03.11.006 This field MUST be set to 0xFF to start a new iteration. A supporting node MUST return the first entry and the actual amount of remaining entries in the returned report, i.e. If the Provisioning list has 3 elements the first response Remaining Count field MUST be set to 2.

CC:0078.01.03.11.007 A sending node MUST subsequently set this field to the returned value “Remaining Count” value received in the returned Report if the “Remaining Count” value is higher than 0x00. A supporting node MUST ignore this field if it is not set to the expected next iteration value.

CC:0078.01.03.11.008 This command MUST be ignored by a supporting node if this field is set to a value lower than 0xFF and no iteration has been started.

Refer to 4.6.11.1.

4.6.9 Node Provisioning List Iteration Report Command

This command is used to advertise the contents of an entry in the Provisioning List of the sending node.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_NODE_PROVISIONING							
Command = COMMAND_NODE_PROVISIONING_LIST_ITERATION_REPORT (0x04)							
Seq No.							
Remaining Count							
Reserved			DSK Length N				
DSK 1 (Optional)							
…							
DSK N (Optional)							
Meta Data Extension 1 (Optional)							
…							
Meta Data Extension M (Optional)							

Seq No. (8 bits)

Refer to 4.4.1.1 Sequence Number management.

Remaining Count (8 bits)

CC:0078.01.04.11.001 The field MUST indicate the remaining amount of entries in the Provisioning List iteration. This field MUST be in the range 0x00..0xFE.

DSK Length (5 bits)

CC:0078.01.04.11.002 This field MUST indicate the length of the DSK field in bytes.
CC:0078.01.04.11.003 This field MUST be set to 0 or 16.

CC:0078.01.04.11.004 The value 0 MUST indicate that the Provisioning List of the sending node is empty or the Provisioning List Entry has been deleted after the start of the iteration.
CC:0078.01.04.11.005 The value 16 MUST indicate that the sending node advertises the DSK of a Provisioning List entry.

DSK (N bytes)

This field is used to advertise the DSK for the Provisioning List entry being advertised.

CC:0078.01.04.11.006 The length of this field (in bytes) MUST be according to the DSK Length field value. This field MUST be omitted if the DSK Length field is set to 0.

Meta Data Extension (M bytes)

This field is used to carry additional metadata associated to the Provisioning List entry.

CC:0078.01.04.13.001 This field MAY contain several extensions.
CC:0078.01.04.11.007 Each extension Type, Length and Value MUST comply with 4.6.10 Meta Data extension format and [22].

CC:0078.01.04.13.002 A supporting node MAY set the critical flag to 0 even when advertising critical extensions.

CC:0078.01.04.11.008 If the DSK Length field is set to 0, this field MUST be omitted.

If the DSK Length field is not set to 0:

CC:0078.01.04.11.009 • A sending node MUST advertise the SmartStart Inclusion Setting extension (type 0x34)
CC:0078.01.04.11.00A • A sending node MUST advertise the Bootstrapping mode extension (type 0x36)
CC:0078.01.04.11.00C • A sending node MUST advertise the Network Status extension (type 0x37)
CC:0078.01.04.11.00B • A sending node MUST advertise all other extension data kept in the Provisioning List

4.6.10 Meta Data extension format

CC:0078.01.00.11.001 Each Meta Data extension MUST be parsed according to the following format:

7	6	5	4	3	2	1	0
Meta Data Type							Critical
Length							
Value 1 (Optional)							
…							
Value L (Optional)							

Meta Data Type (7 bits)

This field is used to advertise the type of the data contained in the corresponding extension.

CC:0078.01.00.11.002 For the list of defined valid extensions, refer to [22]. Values not defined in [22] are reserved and MUST NOT be used by a sending node.

Critical (1 bit)

This field is used to advertise the criticality of the extension.

CC:0078.01.00.11.003 A supporting node MUST discard and ignore the entire command if this flag is set to '1' and the Meta Data Type field advertises a value that the node does not support.

CC:0078.01.00.12.001 A controlling node which controls only (i.e. does not support this Command Class) SHOULD keep the Provisioning List entry in its record even if this flag is set to '1' and the node does not know what the extension means.

CC:0078.01.00.11.004 If this flag is set to '0' and the Meta Data Type field advertises a value that the receiving node does not support, the actual extension MUST be ignored and left out the provisioning list entry.

CC:0078.01.00.11.005 In this case, a receiving node MUST continue processing of the encapsulation command after the discarded extension.

Length (8 bits)

CC:0078.01.00.11.006 This field MUST indicate the length of the corresponding Value field in bytes.

Value (L bytes)

CC:0078.01.00.11.007 This field MUST indicate the value of the Meta Data type being advertised in the extension.

CC:0078.01.00.11.008 The length of this field (in bytes) MUST be according to the corresponding Length field value .This field MUST be omitted if the corresponding Length field is set to 0.

CC:0078.01.00.11.009 The encoding of this field MUST be interpreted with the Meta Data Type field as defined in [22].

4.6.11 Usage and frame flows

4.6.11.1 Z/IP Client requesting the entire Node Provisioning list.

The frame flow for Z/IP client requesting the entire Provisioning List of a supporting node is shown in Figure 25.

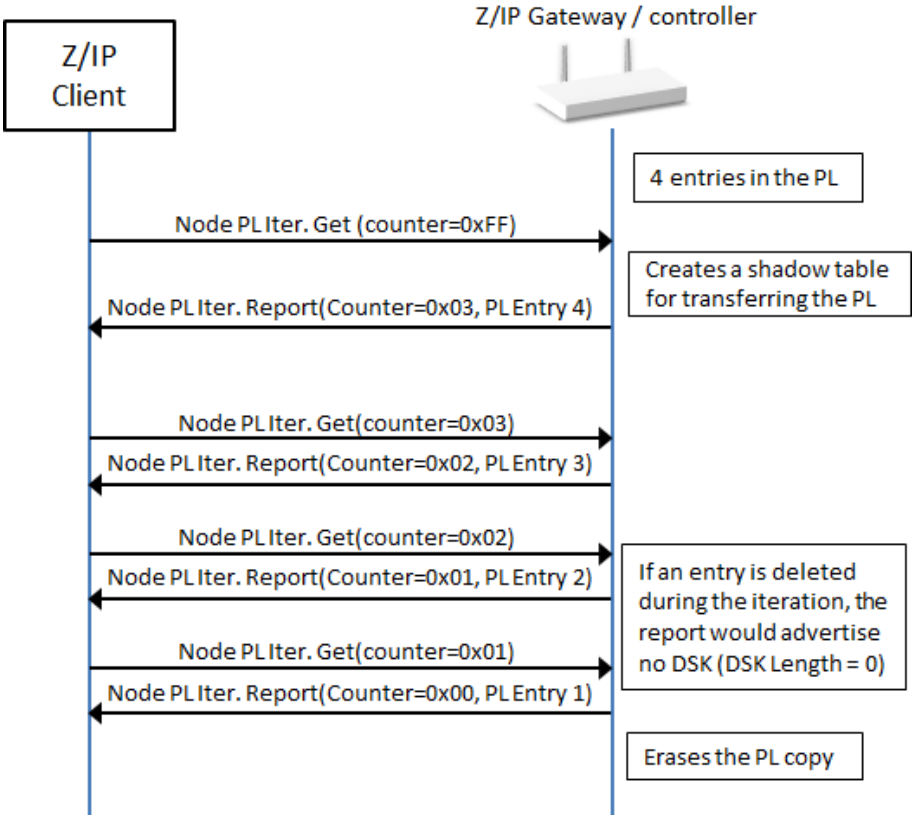

Figure 25, Reading the entire Node Provisioning List

4.7 Powerlevel Command Class, version 1

The Powerlevel Command Class defines RF transmit power controlling Commands useful when installing or testing a network. The Commands makes it possible for supporting controllers to set/get the RF transmit power level of a node and test specific links between nodes with a specific RF transmit power level.

NOTE: This Command Class is only used in an installation or test situation.

4.7.1 Powerlevel Set Command

This command is used to set the power level indicator value, which should be used by the node when transmitting RF, and the timeout for this power level indicator value before returning the power level defined by the application.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_POWERLEVEL							
Command = POWERLEVEL_SET							
Power level							
Timeout							

Power level (8 bits)

CC:0073.01.01.11.001 This field indicates the power level value that the receiving node MUST set.

CC:0073.01.01.11.002 This field MUST be encoded according to Table 39:

Table 39, Powerlevel Set::Power level encoding

Value	Description
0x00	NormalPower
0x01	minus1dBm
0x02	minus2dBm
0x03	minus3dBm
0x04	minus4dBm
0x05	minus5dBm
0x06	minus6dBm
0x07	minus7dBm
0x08	minus8dBm
0x09	minus9dBm

CC:0073.01.01.11.003 All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

Timeout value is ignored if Power level is set to normalPower.

Timeout (8 bits)

The time in seconds the node should keep the Power level before resetting to normalPower level. It is fundamental, that the timeout IS implemented and followed by the application, for keeping the network consistent. Valid values are 1-255 resulting in timeouts from 1 second to 255 seconds.

4.7.2 Powerlevel Get Command

This command is used to request the current power level value.

CC:0073.01.02.11.001 The Powerlevel Report Command MUST be returned in response to this command.

CC:0073.01.02.11.002 This command MUST NOT be issued via multicast addressing.

CC:0073.01.02.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_POWERLEVEL							
Command = POWERLEVEL_GET							

4.7.3 Powerlevel Report Command

This command is used to advertise the current power level.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_POWERLEVEL							
Command = POWERLEVEL_REPORT							
Power level							
Timeout							

Power level (8 bits)

This value is the current power level indicator value in effect on the node.

CC:0073.01.03.11.001 This field MUST be encoded according to Table 39.

If the returned value is normalPower, the timeout value is ignored.

Timeout (8 bits)

The time in seconds the node has back at Power level before resetting to normal Power level.

4.7.4 Powerlevel Test Node Set Command

This command is used to instruct the destination node to transmit a number of test frames to the specified NodeID with the RF power level specified. After the test frame transmissions the RF power level is reset to normal and the result (number of acknowledged test frames) is saved for subsequent read-back. The result of the test may be requested with a Powerlevel Test Node Get Command.

CC:0073.01.04.12.001 A receiving node SHOULD return an unsolicited Powerlevel Test Node Report Command when it completed the Powerlevel test initiated by this command.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_POWERLEVEL							
Command = POWERLEVEL_TEST_NODE_SET							
Test NodeID							
Power level							
Test frame count (MSB)							
Test frame count (LSB)							

Test NodeID (8 bits)

The test NodeID that should receive the test frames.

CC:0073.01.04.12.002 A power level test will not work with a test NodeID which is either a sleeping or FLiRS node. A controller SHOULD NOT initiate a powerlevel test towards sleeping or FLiRS nodes.

Power level (8 bits)

The power level indicator value to use in the test frame transmission.

CC:0073.01.04.11.001 This field MUST be encoded according to Table 39.

Test frame count (16 bits)

The Test frame count field contains the number of test frames to transmit to the Test NodeID. The first byte is the most significant byte. Valid Test frame count range is 1..65535.

4.7.5 Powerlevel Test Node Get Command

This command is used to request the result of the latest Powerlevel Test.

CC:0073.01.05.11.001 The Powerlevel Test Node Report Command MUST be returned in response to this command.

CC:0073.01.05.11.002 This command MUST NOT be issued via multicast addressing.

CC:0073.01.05.11.003 A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_POWERLEVEL							
Command = POWERLEVEL_TEST_NODE_GET							

4.7.6 Powerlevel Test Node Report Command

This command is used to report the latest result of a test frame transmission started by the Powerlevel Test Node Set Command.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_POWERLEVEL							
Command = POWERLEVEL_TEST_NODE_REPORT							
Test NodeID							
Status of operation							
Test frame acknowledged count (MSB)							
Test frame acknowledged count (LSB)							

Test NodeID (8 bits)

This field advertises the NodeID of the node, which is or has been under test.

CC:0073.01.06.11.001 If a test has been performed, this field MUST reflect the NodeID used in the last test initiated with the Powerlevel Test Node Set Command.

CC:0073.01.06.11.002 CC:0073.01.06.13.001 If no test has been performed, this field MUST be set to 0. In this case, the Status of operation and Test frame acknowledged count fields MAY be ignored.

CC:0073.01.06.13.002 CC:0073.01.06.13.003 It is OPTIONAL to save the last Powerlevel test result in the NVM. If a node saves the last Powerlevel test result in the volatile memory, it MAY set this field to 0 after going to sleep or losing power.

Status of operation (8 bits)

CC:0073.01.06.11.003 This field indicates the result of the last test initiated with the Powerlevel Test Node Set Command. It MUST be encoded according to Table 40..

Table 40, Powerlevel Test Node Report::Status of operation encoding

Value	Description
0x00	Test Failed No frame was returned during the test
0x01	Test Success At least 1 frame was returned during the test
0x02	Test in Progress The test is still ongoing

CC:0073.01.06.11.004 All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

CC:0073.01.06.13.004 CC:0073.01.06.11.005 A controller MAY return “Test Failed” for a non-existing NodeID without carrying the test. However, it MUST return “Test in Progress” if carrying the test even if it knows that the test will fail.

Test frame acknowledged count (16 bits)

This field indicates the number of test frames transmitted, which the Test NodeID has acknowledged. The first byte is the most significant byte.

4.8 Z/IP Command Class, Version 1 [OBSOLETED]

THIS COMMAND CLASS VERSION HAS BEEN OBSOLETED

CC:0023.01.00.11.001 New implementations MUST use the Z/IP Command Class Version 2.

4.9 Z/IP Command Class, Version 2

The Z/IP Command Class is a special Command Class intended for encapsulation of Z-Wave commands in IP packets.

Z/IP Packets may be exchanged between IP hosts running over physical layers such as Ethernet or WiFi.

4.9.1 Security considerations

This Command Class is used to encapsulate Z-Wave Commands in an IP network. A Z/IP Gateway will forward some of the encapsulated Z-Wave commands into the Z-Wave Network.

The Z-Wave nodes may use encryption to protect the integrity of the Z-Wave network (refer to Security 0 and Security 2 Command Classes). IP nodes should always assume to be in a hostile network and support an encryption mechanism, such as DTLS.

If an IP node implements IP LAN security (DTLS or equivalent):

CC:0023.02.00.41.001
- Z/IP Packet received via secure IP channel MUST be accepted and a Z/IP Gateway MUST forward the optional Z-Wave Command in the Z-Wave network.

- Z/IP Packet received via non-secure IP channel:

CC:0023.02.00.41.002
  - Z/IP Discovery Command Class MUST be accepted.

CC:0023.02.00.41.003
  - All other encapsulated Command Classes MUST be discarded.

If an IP node does not implement IP LAN security (DTLS or equivalent):

CC:0023.02.00.41.004
- All Z/IP Packet received via non-secure IP channel MUST be accepted.

4.9.2 Interoperability considerations

CC:0023.02.00.32.001 Any Z-Wave Command Class SHOULD be sent encapsulated in a Z/IP Packet if a transmission takes place in an IP network.

CC:0023.02.00.31.001 Commands part of this Command Class MUST NOT be encapsulated in a Z/IP Packet Command.

4.9.3 Z/IP Packet Command

IP→UDP:4123→Z/IP Packet Command→Optional Z-Wave command
IP→UDP:41230→DTLS→Z/IP Packet Command→Optional Z-Wave command

CC:0023.02.02.11.001 A Z/IP Packet Command MUST be carried in a UDP packet, using destination port 4123 when no LAN security is used.

CC:0023.02.02.11.002 A Z/IP Packet Command MUST be carried in a UDP packet, using destination port 41230 when DLTS is used.

CC:0023.02.02.11.003 A node returning an answer to a Z/IP Packet (Ack/NAck Response) MUST swap the UDP source and destination ports.

The Z/IP Packet may carry a Z-Wave command or it may be used to communicate positive or negative acknowledgement for the delivery of another Z/IP Packet.

CC:0023.02.02.11.004 The Z/IP Packet MUST NOT be used for transmission between native Z-Wave nodes. The Z/IP Packet is intended for transport of encapsulated Z-Wave commands inside IP packets in an IP environment.

For that reason, normal Z-Wave MAC layer frame size limitations do not apply to this command, however Z-Wave MAC Layer frame size and Z-Wave Transport Service Command Class size limitations apply to the Z-Wave Command field.

<table>
<tr><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td colspan="8">Command Class = COMMAND_CLASS_ZIP (0x23)</td></tr>
<tr><td colspan="8">Command = COMMAND_ZIP_PACKET (0x02)</td></tr>
<tr><td rowspan="2">Ack Request</td><td rowspan="2">Ack Response</td><td rowspan="2">NAck Response</td><td colspan="3">(NAck flags)</td><td colspan="2" rowspan="2">Reserved</td></tr>
<tr><td>Waiting</td><td>Queue Full</td><td>Option Error</td></tr>
<tr><td>Header ext. included</td><td>Z-Wave Cmd Included</td><td>More Information</td><td>Secure Origin</td><td colspan="4">Reserved</td></tr>
<tr><td colspan="8">Seq No</td></tr>
<tr><td>Res</td><td colspan="7">Source End Point</td></tr>
<tr><td>Bit address</td><td colspan="7">Destination End Point</td></tr>
<tr><td colspan="8">Header extension 1 (Optional)</td></tr>
<tr><td colspan="8">...</td></tr>
<tr><td colspan="8">Header extension N (Optional)</td></tr>
<tr><td colspan="8">Z-Wave Command 1 (Optional)</td></tr>
<tr><td colspan="8">...</td></tr>
<tr><td colspan="8">Z-Wave Command M (Optional)</td></tr>
</table>

CC:0023.02.02.11.005 A receiving node MUST inspect the header flags in order to determine the offset to use for accessing the optional fields. If the packet contains invalid data, e.g. the ACK_RES and NACK_RES bits are both set to 1 or if the length of the extended header does not add up, a receiving node MUST ignore the packet.

Ack Request (1 bit)

CC:0023.02.02.11.006 This flag signals that the receiving node MUST return an Ack or NAck message in response to the actual Z/IP Packet.

CC:0023.02.02.11.007 This field MUST be encoded according to Table 41.

Table 41, Z/IP Packet::Ack Request Flag encoding

Value	Description
'1'	Return Ack or NAck
'0'	No confirmation needed

CC:0023.02.02.11.008 If this flag is set to 1, the Z/IP Packet MUST contain a Z-Wave Command. A receiving node MUST discard the packet if this flag is set to 1 but no Z-Wave Command is included.

This field is intended for delivery acknowledgement for Z-Wave Commands encapsulated in Z/IP packets.

CC:0023.02.02.12.001 Z-Wave link-level acknowledgement SHOULD always be used between Z-Wave nodes when Z-Wave is used as link layer.

CC:0023.02.02.11.009 A Z/IP Gateway MUST return a “NAck+Waiting” indication no later than 200ms after receiving an Ack Request if the Z-Wave Command is still being processed or pending delivery.

CC:0023.02.02.13.001 A sending node that has requested an Ack and has waited for more than 300ms without receiving an Ack or NAck indication MAY conclude that the Z-Wave Command is lost and retransmit the Z/IP Packet.

CC:0023.02.02.11.00A In case of successful delivery to a Z-Wave node, a Z/IP Packet with *Ack Response* indication MUST be returned by the Z/IP Gateway upon reception of the Z-Wave Ack.

CC:0023.02.02.11.00B In case of successful delivery to a Z/IP node, the Z/IP node itself MUST return a Z/IP Packet with *Ack Response* indication.

Ack Response (1 bit)

CC:0023.02.02.11.00C This flag MUST be used to indicate that the destination has received the Z-Wave Command encapsulated in a preceding Z/IP packet.

CC:0023.02.02.11.00D This field MUST NOT be interpreted as a confirmation that the destination has accepted the application command carried in the Z-Wave Command field.

CC:0023.02.02.11.00E This field MUST be encoded according to Table 42.

Table 42, Z/IP Packet::Ack Response Flag encoding

Value	Description
'1'	This Z/IP Packet acknowledges a preceding packet that requested an Ack Response
'0'	This Z/IP Packet does not acknowledge a preceding packet that requested an Ack Response. A receiving node MUST inspect the NAck Response field

CC:0023.02.02.11.00F

CC:0023.02.02.11.010 If this field is set to 1, the *Seq No* field value MUST be the same as the Z/IP packet being acknowledged.

NAck Response (1 bit)

CC:0023.02.02.11.011 This flag MUST be used to indicate that the destination has not (yet) received the Z-Wave Command encapsulated in a preceding Z/IP Packet.

CC:0023.02.02.11.012 This field MAY be set to 1 by intermediate nodes such as a Z/IP Gateway. This field MUST be encoded according to Table 43.

Table 43, Z/IP Packet::NAck Response Flag encoding

CC:0023.02.02.11.013

Value	Desription
'1'	This Z/IP Packet negatively acknowledges a preceding packet that requested an Ack Response. (i.e. the Z-Wave Command was not delivered to the destination) A receiving node MUST inspect the *NAck flags* fields.
'0'	This field and the *NAck flags* fields may be ignored.

CC:0023.02.02.11.014 If this field is set to 1, the *Seq No* field value MUST be the same as the Z/IP packet being negatively acknowledged.

If this field is set to 1 but none of the *NAck flags* field is set to 1, the Z-Wave Command was lost but no specific reason is provided.

(NAck flags) Waiting (1 bit)

CC:0023.02.02.12.002 This flag is a companion flag to the *NAck Response* flag. It SHOULD be inspected only if the *NAck Response* flag field is set to 1 and SHOULD be ignored otherwise.

CC:0023.02.02.11.015 This flag MUST be ignored if the *Queue Full* flag is set to 1.

CC:0023.02.02.11.016 This flag MUST be used to indicate that the destination may have a long response time. i.e. the Z-Wave Command has not timed out yet and is pending delivery. This field MUST be encoded according to Table 44.

Table 44, Z/IP Packet::Waiting Flag encoding

Value	Description
'1'	Waiting: the preceding Z/IP Packet encapsulated Z-Wave Command is not yet delivered to the destination and delivery will be attempted later on
'0'	Not waiting: the preceding Z/IP Packet encapsulated Z-Wave Command will not be delivered later on.

CC:0023.02.02.13.002
CC:0023.02.02.12.003
CC:0023.02.02.11.017

An “Expected Delay” Option MAY be returned by a Z/IP Gateway, indicating how long it should take before the final delivery acknowledgment status is known, refer to 4.11.3.1. A sending node SHOULD use this information to provide better user responsiveness. A default value of 90 seconds MUST be used by the sending node if no “Expected delay” Option is provided.

A Z/IP “NAck+Waiting” indication is returned for every packet that is queued up. If a sending node triggers to queue up three Z-Wave Commands, it will receive a “NAck+Waiting” indication after each packet. It may be desirable to queue up three configuration commands if the intention is to perform a few configuration changes and allow a battery node to return to sleep.

CC:0023.02.02.12.004

If a sending node wants to transfer larger amounts of data or commands, e.g. probing capabilities or downloading a new firmware image, it is RECOMMENDED to send a single Z/IP Packet using the *More Information* field to make the destination node stay awake. When a Z/IP *Ack Response* indication is returned to the sending node, it can start transferring packets at a higher rate.

CC:0023.02.02.11.018

A Z/IP Gateway MUST return a “NAck+Waiting” indication no later than 200ms after receiving an *Ack Request* indication if the Z-Wave Command is still pending delivery.

CC:0023.02.02.11.019

If a message has been delayed for more than 60 seconds, an intermediate receiver, such as a Z/IP Gateway, MUST transmit a new “NAck+Waiting” indication every 60 seconds to let the sending node know that it is still operational.

CC:0023.02.02.13.003

A sending node waiting for more than 90 seconds after receiving a “NAck+Waiting” indication MAY conclude that the Z-Wave Command is lost and retransmit a new Z/IP Packet.

CC:0023.02.02.11.01A

A Z/IP Gateway issuing a “NAck+Waiting” indication MUST subsequently issue an *Ack Response* indication when the Z-Wave Command has been delivered.

CC:0023.02.02.11.01B

A Z/IP Gateway MUST return a Z/IP *NAck Response* indication if the Z-Wave Command delivery is aborted or not successful.

(NAck flag) Queue Full (1 bit)

CC:0023.02.02.12.005 This flag is a companion flag to the *NAck Response* flag. It SHOULD be inspected only if the *NAck Response* flag is set to 1 and SHOULD be ignored otherwise.

CC:0023.02.02.11.01C This flag MUST be used by a Z/IP Gateway for packets targeting battery nodes, in a busy network, during bulk data transfers or route re-discovery.

CC:0023.02.02.13.004 This flag MAY also be returned for always listening Z-Wave destinations.

CC:0023.02.02.11.01D A sending node MUST wait for at least 10 seconds before re-transmitting a new Z/IP Packet.

CC:0023.02.02.11.01E This flag MUST be returned by a Z/IP Gateway if there is no more room in the queue system used for delivering Commands into the Z-Wave network. This field MUST be encoded according to Table 45.

Table 45, Z/IP Packet::Queue Full Flag encoding

Value	Description
'1'	Queue is full: the preceding Z/IP Packet Command is discarded and will not be delivered to the destination
'0'	Queue OK

(NAck flag) Option Error (1 bit)

CC:0023.02.02.12.006 This flag is a companion flag to the *NAck Response* flag. It should only be inspected if the *NAck Response* flag is set to 1 and SHOULD be ignored otherwise.

CC:0023.02.02.11.01F This flag MUST be set to 1 if a critical option is not recognized by the receiving node and the entire Z/IP Packet was discarded.

CC:0023.02.02.11.020 This flag MUST NOT be set to 1 if an elective option is not recognized by the receiving node. Elective options MUST be silently ignored by a receiving node.

Table 46, Z/IP Packet::Option Error Flag encoding

Value	Description
'1'	Option Error: A critical extension was not understood and the entire Z/IP Packet was discarded
'0'	(no error)

CC:0023.02.02.12.007 A node setting this flag to 1 SHOULD include the offending Option in the “NAck+OptionError” indication returned to the originating node.

CC:0023.02.02.11.021 A node receiving a “NAck+OptionError” indication MUST NOT process the Z/IP Packet Options in the *Header Extension* field as it is only included for debugging purposes.

Header extension Included (1 bit)

This flag is used to indicate that a *Header Extension* field is included in the Z/IP Packet. Refer to the *Header Extension* field description below.

CC:0023.02.02.11.022 This flag MUST be encoded according to Table 47.

Table 47, Z/IP Packet::Header Extension Included Flag encoding

Value	Description
'1'	Header Extension field MUST be included in the Z/IP Packet
'0'	Header Extension field MUST NOT be included in the Z/IP Packet

Reserved

CC:0023.02.02.11.023 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Z-Wave Command Included (1 bit)

This flag is used to indicate that a *Z-Wave Command* field is included in the Z/IP packet. Refer to the *Z-Wave Command* field description below.

CC:0023.02.02.11.024 This flag MUST be encoded according to Table 48.

Table 48, Z/IP Packet::Z-Wave Command Included Flag encoding

Value	Description
'1'	Z-Wave Command field MUST be included in the Z/IP Packet
'0'	Z-Wave Command field MUST NOT be included in the Z/IP Packet

CC:0023.02.02.11.025 If a Z/IP Packet is received with payload length = 0 and the “Z-Wave command included” bit set to 1, a receiving node MUST treat the Z/IP Packet as if the “Z-Wave command included” bit was set to 0.

More Information (1 bit)

This flag is used to indicate the Z/IP Gateway that it should prevent a sleeping node from returning to sleep during the next minute.

CC:0023.02.02.11.026 This flag MUST indicate that more Z/IP Packets with Z-Wave Commands will be subsequently transmitted. A sending node knowing that it will be sending more commands to the destination node MAY set this flag to 1.

CC:0023.02.02.13.005

CC:0023.02.02.11.027 This flag MUST be encoded according to Table 49

Table 49, Z/IP Packet::More Information Flag encoding

Value	Description
'1'	The Z/IP Gateway should keep the sleeping node awake
'0'	The Z/IP Gateway should put the sleeping node to sleep

Secure Origin (1 bit)

This field indicates if the Z-Wave Command is to be treated securely.

CC:0023.02.02.11.028 The value 1 MUST indicate that the Z-Wave Command MUST be treated securely (i.e. it was or will be sent using encryption in the Z-Wave network).

CC:0023.02.02.11.029 The value 0 MUST indicate that the Z-Wave Command MUST NOT be treated securely. (i.e. it was or will be sent non-securely in the Z-Wave network)

CC:0023.02.02.11.02A A Z/IP Gateway forwarding the contents of an encrypted Z-Wave frame MUST set the Secure Origin flag to '1'.

CC:0023.02.02.11.02B A Z/IP Gateway forwarding the contents of a non-encrypted Z-Wave frame MUST set the Secure Origin flag to '0'.

CC:0023.02.02.11.02C A Z/IP Gateway MUST inspect the Secure Origin flag when forwarding a Z-Wave Command contained in a Z/IP Packet from an IP network to a Z-Wave network.

CC:0023.02.02.11.02D A Z/IP Gateway MUST NOT use secure communication via Z-Wave if this flag is set to '0' and MUST use secure communication via Z-Wave if this flag is set to '1'.

Seq No (8 bits)

This field is used to identify Z/IP Packet duplicates or retransmissions.

CC:0023.02.02.11.02E This field MUST carry a unique sequence number. Each sequence number MUST be generated from an 8-bit counter that is incremented by 1 whenever a new sequence number is generated. When a node powers up, the sequence counter MUST be initialized to a random value.

CC:0023.02.02.13.006 The counter MAY be shared with other Command Classes.

CC:0023.02.02.11.02F Retransmitted Z/IP packets MUST carry the same value as the original Z/IP Packet. A Z/IP Ack or NAck packet MUST carry the same Seq No value as the Z/IP packet being acknowledged.

CC:0023.02.02.11.030 Multiple Z/IP Packets may be received in case of link-layer retransmissions. Z/IP Packet duplicates MUST be ignored by a receiving node.

Source End Point (7 bits)

This field is used to indicate the originating end point from which the Z-Wave Command was sent.

CC:0023.02.02.11.031 This field MUST be in the range 0..127.

The Source End Point value 0 represents the Root Device. Refer to the Multi Channel Command Class for more details.

Bit address (1 bit)

This field is used to advertise if the *destination End Point* field is specified as a bit mask.

CC:0023.02.02.11.032 The value 0 MUST indicate that the Destination End Point field is specified as a single End Point.

CC:0023.02.02.11.033 The value 1 MUST indicate that the Destination End Point field is specified as a bit mask. Only destination end points 1..7 are bit addressable.

CC:0023.02.02.11.034 Bit addressing MUST NOT be used if the encapsulated command is a request (requiring a reply from the destination).

Destination End Point (7 bits)

This field is used to indicate the destination End Point of the actual Z-Wave Command.

CC:0023.02.02.11.035 If the *Bit address* field is set to 0, this field MUST carry a single End Point identifier value in the range 0..127.

CC:0023.02.02.11.036 The value 0 MUST represent the Root Device. Values in the range 1..127 MUST represent an actual End Point.

CC:0023.02.02.11.037 If the *Bit address* field is set to 1, this field MUST use the following encoding:

- Bit 0 in the Destination End Point indicates if End Point 1 is a destination
- Bit 1 in the Destination End Point indicates if End Point 2 is a destination
- …

CC:0023.02.02.11.038 The bit value 0 MUST be used to advertise that the corresponding End Point is not a destination.
The bit value 1 MUST be used to advertise that the corresponding End Point is a destination.

Header Extension (variable)

CC:0023.02.02.11.039 This field is used for advertising additional Z/IP Packet Options that are necessary in certain cases. A Z/IP node MUST support and parse this field.

CC:0023.02.02.11.03A This field MUST be omitted if the *Header extension Included* field is set to 0.

CC:0023.02.02.11.03B If the *Header Extension Included* field is set to 1, this field MUST be formatted as follows:

7	6	5	4	3	2	1	0
Header Extension Length							
Z/IP Packet Option 1, 1							
…							
Z/IP Packet Option P, 1							
…							
Z/IP Packet Option 1, N							
…							
Z/IP Packet Option P, N							

Header Extension Length (1 byte)

CC:0023.02.02.11.03C This field MUST indicate the combined length in bytes of the Z/IP Header Extension Length and all the Z/IP Packet Options included in the Z/IP Header Extension.

CC:0023.02.02.11.03D This field MUST be in the range 1..255. The length of the *Header Extension* field cannot exceed 255 bytes.

Z/IP Packet Option (variable)

CC:0023.02.02.11.03E Each Z/IP Packet Option MUST be treated parsed as a block using the following format:

7	6	5	4	3	2	1	0
Critical	Option Type						
Option Length							
Option Data 1 (Optional)							
...							
Option Data L (Optional)							

CC:0023.02.02.11.03F A receiving node MUST accept receiving supported options in any order.

(Z/IP Packet Option) Critical (1 bit)

This field is used to indicate if the whole Z/IP Packet Command must be ignored if the option is not recognized by the receiving node.

CC:0023.02.02.11.040 The value 0 MUST indicate that the option is elective and a receiving node MUST ignore this option only and continue processing the frame if the option is not recognized.

CC:0023.02.02.11.041 The value 1 MUST indicate that the option is critical and a receiving node MUST discard the entire Z/IP Packet Command and return a Z/IP Packet Command with the *Option Error* flag set to 1 if the option is not recognized.

CC:0023.02.02.11.042 An option MUST be considered as recognized even if:

- The *Option Length* field is set to a greater value than expected
- Reserved fields in the *Option Data* field are not set to 0.

CC:0023.02.02.11.043 An option MUST NOT be considered as recognized when:

- The *Option Type* field is set to an unknown value.
- A field value in the *Option Data* field value which is out of expected range or seems to be using reserved values.

(Z/IP Packet Option) Option Type (7 bits)

This field is used to indicate which format to use for parsing the corresponding *Option Data* field. The list of defined Option Type is specified in 4.11.3

CC:0023.02.02.11.044 A receiving node MUST accept supported Z/IP Packet Options in any order.

(Z/IP Packet Option) Option Length (8 bits)

CC:0023.02.02.11.045 This field MUST indicate the length of the corresponding *Option Data* field in bytes.

(Z/IP Packet Option) Option Data (L bytes)

CC:0023.02.02.11.046 This field is used to carry the actual Option data. It MUST be parsed and interpreted using the corresponding *Option Type* field value.

CC:0023.02.02.11.047 The size of this field in bytes MUST be according the corresponding Option Length field. This field MUST be omitted if the corresponding *Option Length* field is set to 0.

Z-Wave Command (M bytes)

CC:0023.02.02.11.048 This field carries a complete Z-Wave command. This field MUST be formatted according to the corresponding command class as defined in [14], [15], [16] and in this specification.

CC:0023.02.02.12.008 A sending Z/IP client SHOULD be aware that this command will be transmitted over a Z-Wave network and therefore respect the Z-Wave Command length limitations. A Z/IP Client SHOULD limit the length of this field to 45 bytes for non-S2 destination nodes and 117 bytes for S2 supporting nodes.

CC:0023.02.02.11.049 This field MUST be omitted if the *Z-Wave Cmd Included* field is set to 0.

4.10 Z/IP Command Class, version 3

The Z/IP Packet Command Class, version 3 adds the support of the Encapsulation Format Info Option to the Z/IP Packet Option types.

4.10.1 Compatibility considerations

Z/IP Packet Command Class, version 3 is backwards compatible with the Z/IP Packet Command Class, version 2.

CC:0023.03.00.21.001 A device supporting Z/IP Packet Command Class, version 3 MUST support Z/IP Packet Command Class, version 2.

CC:0023.03.00.21.002 All fields and commands not described in this version MUST remain unchanged from version 2.

CC:0023.03.00.21.003 A node supporting the Z/IP Packet Command Class, version 3 MUST support the Encapsulation Format Information Option and respect the requirements specified in 4.11.3.4 Encapsulation Format Information Option.

4.10.2 Z/IP Packet Command

CC:0023.03.02.11.001 The frame structure MUST remain unchanged from version 2.

Secure Origin (1 bit)

This field is superseded by the Encapsulation Format Information Option.

CC:0023.03.02.11.002 A version 3 sending node MUST use the Encapsulation Format Information Option with a version 3 receiving node.

CC:0023.03.02.11.003 This field MUST be ignored by a receiving node if an Encapsulation Formation Information Z/IP Option is included in the Z/IP Packet.

4.11 Z/IP Command Class, version 4

The Z/IP Packet Command Class, version 4 adds the support of a Keep Alive command in order to prevent the closure of a Z/IP DTLS session and introduces new Z/IP Packet Options.

4.11.1 Compatibility considerations

Z/IP Packet Command Class, version 4 is backwards compatible with the Z/IP Packet Command Class, version 3.

CC:0023.04.00.21.001 A device supporting Z/IP Packet Command Class, version 4 MUST support Z/IP Packet Command Class, version 3.

CC:0023.04.00.21.002 All fields and commands not described in this version MUST remain unchanged from version 3.

CC:0023.04.00.21.003 A node supporting the Z/IP Packet Command Class, version 4 MUST respect the requirements specified in 4.11.3.5 Z-Wave Multicast Addressing Option.

The Z/IP Keep Alive Command is introduced in this version in order to prevent a DTLS session to time out between a Z/IP Client and server. The default DTLS timeout configured in Z/IP deployments is 60 seconds, i.e. a peer will close the DTLS connection if no command is sent or received in 60 seconds.

The Installation and Maintenance Report Option is extended with new TLVs and a new option is added to indicate a receiving client the addressing method that has been used on the Z-Wave network.

4.11.2 Z/IP Keep Alive Command

This command is used to as a Keep Alive probe for a DTLS session between two IP nodes.

CC:0023.04.03.21.001 This command SHOULD be issued at a minimum interval of 25 seconds and at a maximum interval of 55 seconds after the last sent or received command in order to prevent session closure.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP (0x23)							
Command = COMMAND_ZIP_KEEP_ALIVE (0x03)							
Ack Request	Ack Response	Reserved					

Reserved

CC:0023.04.03.11.001 This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Ack Request (1 bit)

This field is used by a sending node to request an acknowledgement for this command from a receiving node.

CC:0023.04.03.11.002 The value 1 MUST indicate that an acknowledgement is requested.
The value 0 MUST indicate that an acknowledgement is not requested.

CC:0023.04.03.11.003 If this flag is set to 1, a receiving node MUST return a Z/IP Keep Alive Command with the *Ack Response* flag set to 1.

CC:0023.04.03.11.004 This field MUST NOT be set to 1 if the Ack Response field is set to 1.

Ack Response (1 bit)

This field is used by a node to acknowledge that it received a Z/IP Keep Alive Command with the *Ack Request* flag set to 1.

CC:0023.04.03.11.005 The value 1 MUST indicate that this command is an acknowledgement for a received Z/IP Keep Alive Command.
The value 0 MUST indicate that this command is not an acknowledgement

CC:0023.04.03.11.006 This field MUST NOT be set to 1 if the Ack Request field is set to 1.

4.11.3 List of defined Z/IP Packet Options

The list of defined Z/IP Packet Option Types is listed in Table 50 and each type is defined in the following subsections.

CC:0023.00.02.11.001 A sending node using a given option MUST support as a minimum the version indicated in Table 50 for the Z/IP Command Class.

Table 50, Z/IP Packet Option types

Option Type	Type value	Class	Version
Expected delay	1	Elective	2
Installation and Maintenance Get	2	Elective	2
Installation and Maintenance Report	3	Elective	2
Encapsulation Format Information	4	Critical	3
Z-Wave Multicast Addressing	5	Elective	4

CC:0023.00.02.11.002 All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

CC:0023.00.02.11.003 A receiving node MUST accept supported options in any order.

4.11.3.1 Expected Delay Option

This option is used to advertise an expected delay when issuing a Z/IP Packet command with "NAck+Waiting" indication.

7	6	5	4	3	2	1	0
Critical = 0	Option Type = ZIP_OPTION_EXPECTED_DELAY = 1						
Option Length = 3							
Seconds 1 (MSB)							
Seconds 2							
Seconds 3 (LSB)							

Critical (1 bit)

CC:0023.00.02.11.004 The Critical field MUST be set to 0.

Option Type (7 bits)

CC:0023.00.02.11.005 The Option Type field MUST be set to 0x01 to indicate the Expected Delay Option.

Option Length (8 bits)

CC:0023.00.02.11.006 The Option Length field MUST indicate the length of the Seconds field.

Seconds (24 bits)

CC:0023.00.02.11.007 The Seconds field MUST indicate the expected time in seconds before issuing a new Z/IP Packet Command with a new status.

4.11.3.2 Installation and Maintenance Get Option

This option is used to request a receiving node to return a Z/IP Packet Command containing the Installation and maintenance Report Option.

CC:0023.00.02.11.008 In order to trigger an Installation and Maintenance Report to be returned, a sending node MUST:

- Add this Option in the Z/IP Packet Command
- Add a Z-Wave Command in the Z/IP Packet Command (NOP Command Class MAY be used if the sending node does not have any other Z-Wave Command to transmit)
- Set the *Ack Request* flag to 1 in the Z/IP Packet Command

CC:0023.00.02.11.009 A receiving node MUST:

- Return a Z/IP Packet Command containing the Installation and Maintenance Report Z/IP Option after the transmission of the contained Z-Wave Command to the destination.
- If returned, the Installation and Maintenance Report Z/IP Option MUST advertise the statistics associated to the Z-Wave Command transmission.

CC:0023.00.02.13.001 A receiving MAY ignore the request for an Installation and Maintenance Report if it does not support this Option.

7	6	5	4	3	2	1	0
Critical = 0	Option Type = INSTALLATION_MAINTENANCE_GET = 2						
Option Length = 0							

4.11.3.3 Installation and Maintenance Report Option

This option is used to advertise Z-Wave transmission data about the communication between the Z/IP Gateway and a Z-Wave device in the network.

The Installation and Maintenance Report Option is used for data relating to the transmission of an actual frame. Statistical data may be accessed via the Network Management Installation and Maintenance Command Class.

7	6	5	4	3	2	1	0
Critical = 0	Option Type = INSTALLATION_MAINTENANCE_REPORT = 3						
Option Length							
IME – Type 1							
IME – Length 1							
IME - Value 1, 1							
...							
IME - Value L, 1							
…							
IME – Type N							
IME – Length N							
IME - Value 1, N							
...							
IME - Value L, N							

Critical (1 bit)

CC:0023.00.02.11.00A The Critical field MUST be set to 0.

Option Length (1 byte)

CC:0023.00.02.11.00B This field MUST indicate the combined length (in bytes) of the following IME-TLV fields.

IME – Type / Length / Value (TLV) (variable)

CC:0023.00.02.11.00C This field is used to carry values advertising Z-Wave transmission statistics. Each TLV block MUST be encoded according to one of the Types defined in Table 51 and in the following subsections.

CC:0023.00.02.11.00D A sending node using a given TLV MUST support as a minimum the version indicated in Table 51 for the Z/IP Command Class.

CC:0023.00.02.13.002 The Z/IP Gateway MAY send any combination of the IME TLVs when using this Z/IP Packet Option.

Table 51, Z/IP Packet::IME-Type/Length/Value encoding

IME – Type	Name	IME – Length	Version
0x00	Route Changed	1 byte	2
0x01	Transmission Time (TT)	2 bytes	2
0x02	Last Working Route (LWR)	5 bytes	2
0x03	RSSI	5 bytes	4
0x04	ACK channel	1 byte	4
0x05	Transmit channel	1 byte	4
0x06	Routing scheme	1 byte	4
0x07	Routing attempts	1 byte	4
0x08	Last failed link	2 bytes	4

All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.11.3.3.1 Route Changed (3 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x00							
IME – Length = 1							
IME – Value = Route Changed							

Route Changed (8 bits)

This field is used to indicate if the last working route was changed for the current transmission.

CC:0023.00.02.11.00E If the last working route was changed, this field MUST be set to 0x01.
If the last working route was not changed, this field MUST be set to 0x00.

4.11.3.3.2 Transmission Time (4 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x01							
IME – Length = 2							
IME – Value = Transmission Time 1 (MSB)							
IME – Value = Transmission Time 2 (LSB)							

Transmission Time (16 bits)

CC:0023.00.02.11.00F This field is used to indicate the time it took to send the command until the reception of an Ack. The value MUST be encoded using unsigned representation and MUST be specified using the ms (milliseconds) unit.

4.11.3.3.3 Last Working Route (7 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x02							
IME – Length = 5							
IME – Value = Repeater 1							
IME – Value = Repeater 2							
IME – Value = Repeater 3							
IME – Value = Repeater 4							
IME – Value = Speed							

CC:0023.00.02.11.010 This TLV is used to advertise the last used Working Route. If multiple Last Working Routes exist, this MUST be the one used to transmit the frame.

Repeater 1-4 (4 bytes)

This field contains the NodeID of the repeaters used for the last working route.

CC:0023.00.02.11.011 The value 0 MUST indicate that the actual repeater was not used.
Values in the range 1..232 MUST indicate an actual NodeID used as repeater.

CC:0023.00.02.11.012 The first Repeater byte set to 0 MUST indicate that no more repeaters were used for the transmission. If the first Repeater byte is set to 0, it means that the Last Working Route (LWR) is a direct transmission.

Speed (8 bits)

CC:0023.00.02.11.013 This field is used to advertise the transmission speed used to reach the destination node. This field MUST be encoded according to Table 52.

Table 52, IME Speed Encoding

Value	Speed
0x01	9.6 kbit/sec
0x02	40 kbit/sec
0x03	100 kbit/sec

All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.11.3.3.4 RSSI (7 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x03							
IME – Length = 5							
IME – Value = RSSI hop 1							
IME – Value = RSSI hop 2							
IME – Value = RSSI hop 3							
IME – Value = RSSI hop 4							
IME – Value = RSSI hop 5							

The IME - Values advertise the RSSI value measured in the incoming direction (back towards the source of the message).

RSSI Hop (5 bytes)

CC:0023.00.02.11.014 The RSSI values MUST be encoded as using signed representation in the dBm unit and according to Table 53.

Table 53, RSSI encoding

Value (signed)	Description
0x7F (127)	RSSI_NOT_AVAILABLE. This value is returned for unused hops or if no RSSI measurement is available.
0x7E (126)	RSSI_MAX_POWER_SATURATED This value is returned if the measured RSSI is above the maximum power.
0x7D (125)	RSSI_BELOW_SENSITIVITY. This value is returned if the measured RSSI is below the receiver’s sensitivity.
…	Reserved
0xE0 (-32)	-32 dBm
0xDF (-33)	-33 dBm
…	…
0xA2 (-94)	-94 dBm
0xA1 (-95)	Reserved
…	Reserved
0x80 (-128)	Reserved

4.11.3.3.5 ACK channel (3 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x04							
IME – Length = 1							
IME – Value = ACK channel							

ACK channel (8 bits)

This value reports the RF channel on which the ACK for this frame was received.

4.11.3.3.6 Transmit channel (3 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x05							
IME – Length = 1							
IME – Value = Transmit channel							

Transmit channel (8 bits)

This value reports the RF channel on which the Z-Wave Command was transmitted.

4.11.3.3.7 Routing scheme (3 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x06							
IME – Length = 1							
IME – Value = Routing scheme							

Routing scheme (8 bits)

This value reports the routing scheme that was used to find the successful route for delivering the Z-Wave Command.

CC:0023.00.02.11.015 The Routing scheme value MUST encoded according to Table 54

Table 54, Routing Scheme IME::Routing Scheme encoding

Value	Description
0x00	Idle
0x01	Direct transmission (no routing)
0x02	Application static route
0x03	Last working route
0x04	Next to last working route
0x05	Return route or controller auto route
0x06	Direct resort
0x07	Explorer frame

All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.11.3.3.8 Routing attempts (3 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x07							
IME – Length = 1							
IME – Value = Routing attempts							

Routing attempts (8 bits)

This TLV reports the number of routing attempts that were performed before successfully delivering the Z-Wave Command.

4.11.3.3.9 Failed link (4 bytes)

7	6	5	4	3	2	1	0
IME - Type = 0x08							
IME – Length = 2							
IME – Value = Failed Link Neighbor NodeID 1							
IME – Value = Failed Link Neighbor NodeID 2							

Failed Link Neighbor NodeID (16 bits)

This TLV is used if the transmission of the Z-Wave Command failed. The value reports the neighbor NodeIDs of the failing link in the last attempted route.

CC:0023.00.02.12.001 If the last node failed, Failed Link Neighbor NodeID 2 SHOULD be set to 0x00.

4.11.3.4 Encapsulation Format Information Option

The Encapsulation Format Information Option is used to carry information about the Z-Wave encapsulations that were or must be used to communicate between the Z-Wave node and the sending host (e.g. a Z/IP Gateway).

The purpose of this Option is to preserve the encapsulation between a Z-Wave node and a host (e.g. Z/IP Gateway).

CC:0023.00.02.11.016 A Z/IP Gateway MUST use the encapsulation indicated in the Encapsulation Format Information Option when transmitting Z/IP Commands over in a Z-Wave Network.

CC:0023.00.02.11.017 A Z/IP Gateway receiving a Z-Wave Command that must be forwarded over an IP network MUST indicate in the Encapsulation Format Information Option what the Z-Wave encapsulation was.

CC:0023.00.02.11.018 If a Z/IP client receives this Option and the Z-Wave Command requires to return a response, the Z/IP client MUST apply the encapsulation indicated by the Option when sending a reply.

CC:0023.00.02.13.003 A Z/IP client MAY use this Option to dictate the encapsulation format when sending unsolicited messages.

7	6	5	4	3	2	1	0
Critical = 1	Option Type = ENCAPSULATION_FORMAT_INFO = 4						
Option Length = 2							
Security 2 Security Class							
Reserved							CRC16

Critical (1 bit)

CC:0023.00.02.11.019 This field indicates that the whole frame MUST be discarded if the extension is not supported. This field MUST be set to 1 when using the Encapsulation Format Info Option.

Option Type (7 bits)

CC:0023.00.02.11.01A The Type field MUST be set to 4 for the Encapsulation Format Information Option.

Option Length (8 bits)

CC:0023.00.02.11.01B The Option Length field MUST indicate the length of the Option Data fields, which is currently defined as 2 bytes long.

Security 2 Security Class (1 byte)

CC:0023.00.02.11.01C This Security 2 Security Class field indicates which Security 2 Security Class MUST be used for communication with the target node.

CC:0023.00.02.11.01D A receiving node MUST replace previous information about a node's secure capabilities with the information contained in this field and attempt subsequent communication with the target node using the highest security key contained in this command.

CC:0023.00.02.11.01E This field MUST be encoded as a bit field and according to Table 55.

Table 55, Security 2 Security Class field encoding

Bit set to 1	Security 2 – Security Class
None	NON_SECURE
0	S2_UNAUTHENTICATED
1	S2_AUTHENTICATED
2	S2_ACCESS_CONTROL
7	S0

CRC16 (1 bit)

The CRC16 field indicates whether communication with the target node use CRC16 encapsulation or not.

CC:0023.00.02.11.01F The value 1 MUST indicate that CRC16 encapsulation is used and MUST be used for subsequent communication with the Z-Wave node.

CC:0023.00.02.11.020 The value 0 MUST indicate that CRC16 encapsulation is not used and MUST NOT be used for subsequent communication with the Z-Wave node.

CC:0023.00.02.11.021 The CRC16 field MUST NOT be set to 1 if the Security 2 Security Class field is different than "NON_SECURE"

4.11.3.5 Z-Wave Multicast Addressing Option

This option is used to advertise if Multicast Addressing has been used by the sending node in the Z-Wave network.

CC:0023.00.02.12.002 A Z/IP Client SHOULD NOT use this option when sending a Z/IP Packet Command.

CC:0023.00.02.11.022 A Z/IP Gateway supporting Z/IP Command version 4 or newer MUST use this option in a Z/IP Packet Command if forwarding a command that has been received using Multicast addressing from a Z-Wave node.
The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Critical = 0	Option Type = ZWAVE_MULTICAST_ADDRESSING = 5						
Option Length = 0							

Critical (1 bit)

CC:0023.00.02.11.023 The Critical field MUST be set to 0.

Option Type (7 bits)

CC:0023.00.02.11.024 The Option Type field MUST be set to 0x05 to indicate the Z-Wave Multicast Addressing Option.

Option Length (8 bits)

CC:0023.00.02.11.025 The Option Length field MUST indicate the length of the Option Data field.

CC:0023.00.02.11.026 No Option Data is currently defined for this option; this field MUST be set to 0 and the Option Data field MUST be omitted.

4.12 Z/IP 6LoWPAN Command Class, version 1

The Z/IP 6LoWPAN Command Class supports the transmission of IPv6 Packets over Z-Wave networks.

The Z/IP 6LoWPAN Command Class, version 1 is defined by [17].

4.13 Z/IP Gateway Command Class, version 1

The Z/IP gateway Command Class is used for configuration and management of a Z/IP gateway, e.g. to enable portal communication.

4.13.1 Interoperability considerations

The Z/IP Gateway Command Class is intended for use together with the Z/IP Portal Command Class to provide a streamlined workflow for preparing and performing installation of Z/IP Gateways in consumer premises. Section 4.15.1.1 presents the concepts of tunnel creation, maintenance and bootstrapping of a Z/IP Gateway.

A Z/IP Gateway may operate in a standalone environment where it is only accessed locally or it may create a tunnel to a portal provider to allow remote access.

Commands defined in this Command Class MUST be encapsulated in Z/IP Packets.

4.13.2 Gateway Mode Set Command

Any host may send the Gateway Mode Set command during initial configuration of the gateway. Most likely, a service provider or an OEM will use the command in a central facility when preparing deployment at customer premises.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = GATEWAY_MODE_SET							
Mode							

Mode (1 byte)

This field sets the communication mode of the Z/IP Gateway

Table 56, Gateway Mode Set::Mode encoding

Value	Mode
0x01	Stand-alone (default)
0x02	Portal

If Mode is set to “Stand-alone”, the Z/IP Gateway MUST NOT do any attempts to create secure tunnels to other peers in the LAN or in the Internet.
The default mode SHOULD be “Stand-alone”. By default, peer profiles SHOULD NOT be defined.

A Mode value set to “Portal” MUST be ignored if the actual gateway does not support the Z/IP Portal Command Class, If Mode is set to “Portal”, the Z/IP Gateway MUST use the peer profile defined with

the Gateway Peer Set command to create a secure connection to the portal server.
Once the Z/IP Gateway has been configured for portal connection creation, the Z/IP Gateway SHOULD be locked for unauthorized access by issuing a Gateway Lock Set; refer to 4.13.8.

4.13.3 Gateway Mode Get Command

The Gateway Mode Get command is used to request the current Z/IP Gateway operational mode.

The Gateway Mode Report Command MUST be returned in response to this command except if the Z/IP Gateway is locked with the Gateway Lock Set command and the Hide parameter of the Gateway Lock Set command was enabled.
In that case, the Gateway Mode Get command MUST be silently ignored.

This command MUST NOT be issued via multicast addressing.
A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = GATEWAY_MODE_GET							

4.13.4 Gateway Mode Report Command

This command is used to advertise the mode.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = GATEWAY_MODE_REPORT							
Mode							

Mode (1 byte)

This field indicates the communication mode of the Z/IP Gateway.

Refer to 4.13.2 and Table 56 for details.

4.13.5 Gateway Peer Set Command

The Peer Set Command is used to define one or more peers to which the Z/IP Gateway connects. The peer may be a portal server or one or more Z/IP Gateways.

A Peer Set command MUST always carry the peer identity as an IPv6 address and an IP port number. The command SHOULD also specify the symbolic peer name as a FQDN.

If the Gateway Mode is set to “Portal”, there MUST NOT be defined more than one Peer profile.
If the Gateway Mode is set to “Stand-alone”, there MUST NOT be defined any peer profiles.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = GATEWAY_PEER_SET							
Peer Profile							
IPv6 Address 1							
..							
IPv6 Address 16							
Port 1							
Port 2							
Reserved		Peer Name Length					
Peer Name 1 (UTF-8) (Optional)							
... (Optional)							
Peer Name N (UTF-8) (Optional)							

Peer Profile (8 bits)

This field identifies the actual peer profile.

The value 0 (zero) is reserved for future use.
The first peer profile MUST be number 1.

IPv6 Address

Full IPv6 address with no compression. The address SHOULD be in the ULA IPv6 prefix or in a globally routable IPv6 prefix. The address MAY be an IPv4-mapped IPv6 address.
The field MUST NOT carry a link-local IPv6 address.

The IPv6 address MAY be specified as ::/128 (all zeros), i.e. the unspecified address. If setting the IPv6 address field to the unspecified IPv6 address, the Peer Name field MUST be set to a DNS-resolvable FQDN.

Port (16 bits)

This field MUST carry the port number that the peer is listening on. The peer SHOULD use port number 44123 [20].

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Peer Name Length (6 bits)

May be any value from 0 to 63. The value indicates the number of Peer Name bytes following this field. The number of readable characters may be less since some UTF-8 characters are represented by two or more bytes.

Peer Name (N bytes) (optional)

This field is only present if the Peer Name Length field has a value greater than zero.

The Peer Name field MUST be formatted as a UTF-8 based FQDN string such as “example.com”.

Only if that fails, the Z/IP Gateway SHOULD try connecting to the peer using the Peer Name and the Port.

A Z/IP Gateway SHOULD try connecting to the peer using the IPv6 address and the Port.

4.13.6 Gateway Peer Get Command

The Gateway Peer Get Command is used to request active peer profiles.

The Gateway Peer Report Command MUST be returned in response to this command except if the Z/IP Gateway is locked with the Gateway Lock Set command and the Hide parameter of the Gateway Lock Set command was enabled.
In that case, the Gateway Peer Get command MUST be silently ignored.

This command MUST NOT be issued via multicast addressing.
A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = GATEWAY_PEER_GET							
Peer Profile							

Peer Profile (8 bits)

This field identifies the actual peer profile.

A requesting host SHOULD start specifying the Peer Profile value 1 (one). This will cause the Z/IP Gateway to indicate the number of actual peers in the returned Gateway Peer Report command.

4.13.7 Gateway Peer Report Command

The Gateway Peer Report Command is used to report details of a peer profile.

A Gateway Peer Report command MUST always carry the peer address as an IPv6 address and MUST include the peer resource name if it was previously specified.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = GATEWAY_PEER_REPORT							
Peer Profile							
Peer Count							
IPv6 Address 1							
..							
IPv6 Address 16							
Port 1							
Port 2							
Reserved			Peer Name Length				
Peer Name 1 (UTF-8) (Optional)							
.. (Optional)							
Peer Name N (UTF-8) (Optional)							

Peer Profile

This identifier is used to identify the actual peer profile.

The value 0 (zero) is reserved for future use.

Peer Count (8 bits)

This field indicates the number of peer profiles currently defined.
If the Peer Count field has the value 0, all other fields of the Gateway Peer Report MUST be 0.

IPv6 Address

This field MUST carry a full IPv6 address with no compression.

Port (16 bits)

This field MUST carry the port number that the peer is listening on. The peer SHOULD use port number 44123 [20].

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Peer Name Length (6 bits)

May be any value from 0 to 63. The value indicates the number of Peer Name bytes following this field. The number of readable characters may be less since some UTF-8 characters are represented by two or more bytes.

Peer Name (N bytes) (optional)

This field is only present if the Peer Name Length field has a value greater than zero.

The Peer Name field MUST be formatted as a UTF-8 based FQDN string such as “example.com”.

If the Peer Count value is zero, the Resource Name string MUST be unspecified (zero-length).

4.13.8 Gateway Lock Set Command

The Lock Set command MUST lock down access to configuration parameters in the Z/IP Gateway relating to secure connections and portal login. Once the Z/IP Gateway has been locked, it MUST NOT be possible to unlock the device. Two exceptions apply:

- A factory default reset MUST unlock the Z/IP Gateway and revert settings to default.
- An unlock command received via an authenticated secure connection to the portal MUST unlock the Z/IP Gateway.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = GATEWAY_LOCK_SET							
Reserved						Show	Lock

Lock (1 bit)

This field controls if Z/IP Gateway configuration parameters may be changed by the customer.

The value 0 MUST indicate that the parameters are unlocked and can be changed by the customer.
The value 1 MUST indicate that the parameters are locked and cannot be changed by the customer.The Z/IP gateway MUST accept to receive the Lock=1 flag from any connection.
The Z/IP gateway MUST NOT accept to receive the Lock=0 flag from any connection; except for an authenticated secure connection to the portal.

To prevent users and trojan viruses from creating tunnels to rogue portals, the Z/IP Gateway SHOULD automatically lock access to secure tunnel configuration parameters 24 hours after a factory default reset.

Show (1 byte)

This field controls if Z/IP Gateway configuration parameters may be read by the customer after the Z/IP Gateway has been locked.

The value 0 MUST indicate that parameters are not available to the customer.
The value 1 MUST indicate that parameters are available to the customer.

If the Show parameter is '0' the Z/IP Gateway MUST NOT respond to any queries for Z/IP Gateway parameters.

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

4.13.9 Unsolicited Destination Set Command

The Unsolicited Destination Set Command is used to configure the destination information that the Z/IP Gateway must use for incoming unsolicited frames.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = UNSOLICITED_DESTINATION_SET							
Unsolicited IPv6 Destination 1							
…							
Unsolicited IPv6 Destination 16							
Unsolicited Destination Port 1							
Unsolicited Destination Port 2							

Unsolicited IPv6 Destination (16 bytes)

Unsolicited Z-Wave frames received from any Z-Wave node MUST be forwarded to the Unsolicited IPv6 Destination address.

Unsolicited Destination Port (2 bytes)

Unsolicited Z-Wave frames received from any Z-Wave node MUST be forwarded to the Unsolicited IPv6 Destination Port. Byte 1 is the Most Significant byte.

The Unsolicited IPv6 Destination Port SHOULD be port 4123.

IPv6 enabled Z-Wave nodes MAY send Z-Wave commands encapsulated in Z/IP Packets to the Unsolicited IPv6 Destination address. The Z/IP Gateway MUST translate the destination port of Z/IP

Packets destined for the Unsolicited IPv6 Destination address from port 4123 to the port number defined for the Unsolicited Destination Port.

4.13.10 Unsolicited Destination Get Command

The Unsolicited Destination Get Command is used to request the destination information that the Z/IP Gateway uses for incoming unsolicited frames.

The Unsolicited Destination Report Command MUST be returned in response to this command.

This command MUST NOT be issued via multicast addressing.
A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = UNSOLICITED_DESTINATION _GET							

4.13.11 Unsolicited Destination Report Command

The Unsolicited Destination Report Command is used to report the destination information that the Z/IP Gateway uses for incoming unsolicited frames.

The command format is outlined below:

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = UNSOLICITED_DESTINATION_REPORT							
Unsolicited IPv6 Destination 1							
…							
Unsolicited IPv6 Destination 16							
Unsolicited Destination Port 1							
Unsolicited Destination Port 2							

Unsolicited IPv6 Destination (16 bytes)

Refer to 4.13.9

Unsolicited Destination Port (2 bytes)

Refer to 4.13.9

4.13.12 Application Node Info Set Command

The Application Node Info Set Command is used to set the application specific part of the Node Information that a Z/IP Gateway returns when queried by a Z-Wave node.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = COMMAND_APPLICATION_NODE_INFO_SET							
Command Class 1 *)							
...							
Command Class N *)							

*) Command classes may be extended ⇒ spanning two bytes for one command class

Command Class (N bytes)

See description in 4.4.4.4 Node Info Cached Report Command and in Table 8.

4.13.13 Application Node Info Get Command

The Application Node Info Get Command is used to request the Node Information that a Z/IP Gateway returns when queried by a Z-Wave node.

The Application Node Info Report Command MUST be returned in response to this command.

This command MUST NOT be issued via multicast addressing.
A receiving node MUST NOT return a response if this command is received via multicast addressing. The Z-Wave Multicast frame, the broadcast NodeID and the Multi Channel multi-End Point destination are all considered multicast addressing methods.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = COMMAND_APPLICATION_NODE_INFO_GET							

4.13.14 Application Node Info Report Command

The Application Node Info Report Command is used to report the Node Information that a Z/IP Gateway returns when queried by a Z-Wave node. Only the application specific part is returned.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_GATEWAY							
Command = COMMAND_APPLICATION_NODE_INFO_REPORT							
Command Class 1 *)							
...							
Command Class N *)							

*) Command classes may be extended ⇒ spanning two bytes for one command class

Command Class (N bytes)

Refer to 4.13.12.

4.14 Z/IP ND Command Class, version 1

Z/IP ND Command Class builds on the same principles as IPv6 ND [4], [5] and is inspired by the frame formats. Z/IP ND does however not implement the full range of functions defined for IPv6 ND.

4.14.1 Interoperability considerations

Z/IP ND commands allow a Z/IP Gateway to translate between an IPv6 address and a Z-Wave NodeID (Link-Layer address) when requested by an IP host located in a Z-Wave HAN or anywhere else in an IPv6 environment.

The Z/IP ND Commands are not intended for classic Z-Wave applications. Z/IP ND messages MUST always be carried in UDP datagrams without Z/IP Packet encapsulation.

4.14.2 Security considerations

The commands defined in this Command Class MUST always be accepted by a receiving node, regardless of whether IP security (such as DTLS) was used for the transmission.

4.14.3 Z/IP Node Solicitation Command

The Z/IP Node Solicitation Command is used to resolve an IPv6 address of a Z-Wave node to the NodeID (Link-Layer address) of that node in its actual Z-Wave HAN / IP subnet.
Several IPv6 addresses MAY be resolved to the same NodeID.

The Zip Node Solicitation MUST be transmitted in unicast to the Z/IP Gateway of the actual Z/IP HAN. A Z/IP Gateway MUST NOT respond to Zip Node Solicitation commands received via multicast.

A Zip Node Advertisement MUST be returned in response to the Zip Node Solicitation.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_ND							
Command = COMMAND_ZIP_NODE_SOLICITATION							
Reserved							
NodeID = 0							
IPv6 Address 1							
…							
IPv6 Address 16							

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

NodeID (8 bits)

The NodeID field is not used in the Zip Node Solicitation. The field MUST be set to zero by a transmitting host and ignored by a receiving host.

IPv6 Address (16 bytes)

The IP address of the target Z-Wave node. It MUST NOT be a multicast address.

4.14.4 Z/IP Inverse Node Solicitation Command

The Z/IP Inverse Node Solicitation Command is used to resolve a NodeID (link-layer address) of a Z-Wave node to an IPv6 address of that node in its actual Z-Wave HAN / IP subnet.

The Zip Inverse Node Solicitation MUST be transmitted in unicast to the Z/IP Gateway of the actual Z/IP HAN. A Z/IP Gateway MUST NOT respond to Zip Inverse Node Solicitation commands received via multicast.

A Zip Node Advertisement MUST be returned in response to the Zip Inverse Node Solicitation.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_ND							
Command = COMMAND_ZIP_INV_NODE_SOLICITATION							
Reserved				Local	Reserved		
NodeID							

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Local (1 bit)

The flag indicates that the requester would like to receive the site-local address (a.k.a. ULA) even if a global address exists. The flag is typically used by a configuration tool when creating an association between HAN nodes within the same site. Using ULA addresses for intra-HAN association serves to decouple long-term associations in the home from frequently changing global prefixes.

NodeID (8 bits)

The NodeID (Link-Layer Address) that is to be resolved to an IPv6 address.

4.14.5 Z/IP Node Advertisement Command

The Z/IP Node Advertisement Command is sent by a Z/IP Gateway in response to a unicast Zip Node Solicitation or a unicast Zip Inverse Node Solicitation. The Zip Node Advertisement SHOULD advertise valid information in both the IPv6 Address and NodeID fields if such information.

A Zip Node Advertisement MUST NOT be transmitted in unsolicited messages.
A Zip Node Advertisement MUST NOT be transmitted in multicast.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_ND							
Command = COMMAND_ZIP_NODE_ADVERTISEMENT							
Reserved					Local	Validity	
NodeID							
IPv6 Address 1							
…							
IPv6 Address 16							
Home ID 1							
…							
Home ID 4							

Reserved

This field MUST be set to 0 by a sending node and MUST be ignored by a receiving node.

Local (1 bit)

The flag indicates that the requester asked for the site-local address (a.k.a. ULA).
A ULA address is returned. A global address may exist.

Validity (2 bits)

A two-bit codeword that indicates the validity of the returned information.

Table 57, Zip Node Advertisement::Validity parameter encoding

Value	Validity identifier	Comment
0x00	INFORMATION_OK	The Node Advertisement contains valid information in both the IPv6 Address and NodeID fields.
0x01	INFORMATION_OBSOLETE	The information in the IPv6 Address and NodeID fields is obsolete. No node exists in the network with this address information. The information should only be used to inform a user that the actual node is no more present in the network.
0x02	INFORMATION_NOT_FOUND	The responding Z/IP Gateway could not locate valid information. IPv6 Address and NodeID fields MUST be ignored.

All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

NodeID (8 bits)

The NodeID MUST correspond to the IPv6 Address contained in this Zip Node Advertisement message.

IPv6 Address (16 bytes)

The IPv6 Address MUST correspond to the NodeID contained in this Zip Node Advertisement message.

An IPv6 host may have more than one IPv6 address.
If the Zip Node Advertisement is a response to a Zip Node Solicitation, the IPv6 Address MUST be the same as the one carried in the Zip Node Solicitation.

A Z/IP Gateway returning a Zip Node Advertisement in response to a Zip Inverse Node Solicitation may have several IPv6 addresses to choose from. The reported IPv6 Address MUST be selected according to the following priority list:

If “local” flag is set:

1. Unique Local Address (ULA) prefix

If “local” flag is not set:

1. Global routable address
2. Unique Local Address (ULA) prefix

In other words, if the Z/IP node has a globally routable address then that address MUST be reported. Else the locally routable address constructed from a ULA prefix and the NodeID MUST be reported.

If a Z/IP Inverse Node Solicitation command is transmitted in an IPv6 packet the returned Z/IP Node Advertisement MUST carry the IPv6 address of the actual node.

If a Z/IP Inverse Node Solicitation command is transmitted in an IPv4 packet the returned Z/IP Node Advertisement MUST carry the IPv4 address of the actual node formatted as an IPv4-mapped IPv6 address [8].

The IP address carried in the Z/IP Node Advertisement MAY be all zeros. The reason may be that the Z/IP Gateway is still waiting for a DHCP response after including a new node. A Z/IP client MAY re-issue another a Z/IP Inverse Node Solicitation command after a delay of 2 seconds. The delay MUST be doubled before each new attempt. The delay SHOULD be capped at 32 seconds.

Home ID (4 bytes)

Unique network address of the link layer network. All nodes in a Z-Wave network share the same Home ID. The Home ID MAY be used for bookkeeping of complete node information in managed installations.

4.15 Z/IP Portal Command Class, version 1

The Z/IP Portal Command Class is used for configuration and management communication between a Z/IP portal server and a Z/IP gateway through a secure connection.

The Z/IP Portal command class is intended for use together with the Z/IP Gateway command class to provide a streamlined workflow for preparing and performing installation of Z/IP Gateways in consumer premises.

4.15.1 Interoperability considerations

This Command Class MUST NOT be used outside trusted environments, unless via a secure connection. This Command Class SHOULD be further limited for use only via a secure connection to an authenticated portal server.

Commands defined in this Command Class MUST be encapsulated in Z/IP Packets.

4.15.1.1 On the use of Z/IP Gateway and Z/IP Portal command classes

This section presents the concepts of tunnel creation, maintenance and bootstrapping of a Z/IP Gateway.

A secure connection is established by the Z/IP gateway connecting to a peer. The Z/IP Gateway::Gateway Peer Set command is used to define a peer.

A secure connection to a portal is a special case of the general secure connection. When connecting to a portal, the Z/IP Gateway is operated in portal mode; having most network configuration parameters pushed from the portal. In Portal mode, the Z/IP Gateway only accepts the creation of one peer.

The gateway Mode Set command controls whether the Z/IP gateway operates as a normal IP router; learning IP network information from the network or if the configuration is pushed from a portal.

A Z/IP Gateway has two modes of operation, each mode determines how the Z/IP Gateway can be configured and how it should react to a number of command classes. The mode of operation is determined by the customer depending on the type of product they wish to develop.

1. **Service Provider (SP) (Only Portal Mode available)**

    a. *Through Secure Tunnel connection (Locked & Unlocked):* MUST accept Portal & Gateway Command Classes, Firmware Command Class

    b. *Factory default:* Device remains locked, and attempts communication to portal, reverts to default firmware configuration.

    c. Any other attempt to use above command classes MUST be ignored

2. **Consumer Electronics (CE) (Portal and Stand-Alone Mode available)**

    a. *Portal Mode:*

        i. *Through Secure Tunnel connection (Locked & Unlocked):* MUST accept Portal & Gateway Command Classes, Firmware Command Class

        ii. *Local Access (Unlocked only):* MUST accept Portal & Gateway Command Classes, Firmware Command Class

        iii. Any other attempt to use above command classes MUST be ignored

        iv. Factory default: Device is unlocked, and may connect to portal if there is a default configuration containing portal configuration

    b. Stand-Alone Mode

        i. *Local access (Unlocked only):* MUST accept Portal & Gateway Command Classes, Firmware Command Class

        ii. Any other attempt to use above command classes MUST be ignored

        iii. Factory default: Device is unlocked, and may connect to portal if there is a default configuration containing portal configuration

3. Gateway Lock MUST prevent any configuration parameter in Portal and Gateway from being modified locally. Configuration through portal is always allowed.

4. Only the secure tunnel is considered a trusted environment when locked. When unlocked the LAN is also considered "trusted".

5. In all cases, a Factory Default does not perform Z-Wave Default set, meaning the Z-Wave network is left intact. If required, Network Management Default Set MAY be called manually following a Factory Default.

4.15.2 Gateway Configuration Set

The command is used by a portal server to push settings to a Z/IP Gateway via a secure connection.

The Z/IP gateway MUST return a Gateway Configuration Status message in response to a Gateway Configuration Set message.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_PORTAL							
Command = GATEWAY_CONFIGURATION_SET							
LAN IPv6 Address 1							
…							
LAN IPv6 Address 16							
LAN IPv6 Prefix Length							
Portal IPv6 Prefix 1							
…							
Portal IPv6 Prefix 16							
Portal IPv6 Prefix Length							
Default Gateway IPv6 Address 1							
…							
Default Gateway IPv6 Address 16							
PAN IPv6 Prefix 1							
…							
PAN IPv6 Prefix 16							

LAN IPv6 Address (16 bytes)

The LAN IPv6 address MUST be assigned to the LAN interface of the Z/IP Gateway in the consumer premises network. The LAN IPv6 address MUST be used in combination with the LAN IPv6 prefix length.

If the LAN IPv6 address is all zeros, the gateway MUST auto-configure a /64 IPv6 ULA prefix for use by IPv6 enabled hosts in the consumer premises network.

The LAN IPv6 prefix MUST be advertised in IPv6 RAs on the LAN.

LAN IPv6 Prefix Length (1 byte)

The LAN IPv6 prefix length MUST be used by the LAN interface of the Z/IP Gateway in the consumer premises network.

Portal IPv6 Prefix (16 bytes)

The Z/IP Gateway MUST route all IP traffic for the Portal IPv6 Prefix into the secure connection connecting the Z/IP Gateway to the Portal network.
The Portal IPv6 Prefix MUST be used in combination with the Portal IPv6 prefix length.

Portal IPv6 Prefix Length (1 byte)

The Portal IPv6 prefix length MUST be used to scope the routing entry created for the Portal IPv6 Prefix by the Z/IP Gateway.

Default Gateway IPv6 Address (16 bytes)

The Z/IP Gateway MUST send IP packets to the default gateway if the Z/IP Gateway has no routing information for the actual prefix; i.e the prefix is neither the LAN nor the PAN.

The Z/IP Gateway MAY be an address in the Portal IPv6 Prefix.

PAN IPv6 Prefix (16 bytes)

The PAN IPv6 address MUST be assigned to the PAN interface of the Z/IP Gateway. The PAN IPv6 address MUST be scoped by a /64 IPv6 prefix.

If the PAN IPv6 address is all zeros, the gateway MUST auto-configure a /64 IPv6 ULA prefix for use by Z-Wave nodes.

4.15.3 Gateway Configuration Status

The message is submitted by a Z/IP Gateway to confirm the reception and processing of a Gateway Configuration Get to a portal.

The Z/IP gateway MUST return a Gateway Configuration Status message in response to a Gateway Configuration Set message.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_PORTAL							
Command = GATEWAY_CONFIGURATION_STATUS							
Status							

Status (1 byte)

Table 58, Gateway Configuration Status::Status encoding

Value	Status indication
0x01	Invalid Configuration Block
0xFF	OK

All other values are reserved and MUST NOT be used by a sending node. Reserved values MUST be ignored by a receiving node.

4.15.4 Gateway Configuration Get

The message is used by a portal to read back configuration settings from a Z/IP Gateway via a secure connection.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_PORTAL							
Command = GATEWAY_CONFIGURATION_GET							

4.15.5 Gateway Configuration Report

The message is used by a Z/IP Gateway to return actual settings to a portal via a secure connection.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_PORTAL							
Command = GATEWAY_CONFIGURATION_REPORT							
LAN IPv6 Address 1							
…							
LAN IPv6 Address 16							
LAN IPv6 Prefix Length							
Portal IPv6 Prefix 1							
…							
Portal IPv6 Prefix 16							
Portal IPv6 Prefix Length							
Default Gateway IPv6 Address 1							
…							
Default Gateway IPv6 Address 16							
PAN IPv6 Prefix 1							
…							
PAN IPv6 Prefix 16							

LAN IPv6 Address (16 bytes)

Actual IPv6 address assigned to the LAN interface of the Z/IP Gateway in consumer premises.

An all zeros address may have been configured by the portal using a Gateway Configuration Set command. The portal MUST accept receiving an auto-configured /64 IPv6 ULA address even if an all-zeros address was specified previously.

LAN IPv6 Prefix Length (1 byte)

Actual LAN IPv6 prefix length used by the LAN interface of the Z/IP Gateway in consumer premises.

Portal IPv6 Prefix (16 bytes)

Actual IPv6 Prefix used by the Z/IP Gateway to reach the portal end of the secure tunnel.

Portal IPv6 Prefix Length (1 byte)

Actual IPv6 Prefix Length used by the Z/IP Gateway to reach the portal end of the secure tunnel.

Default Gateway IPv6 Address (16 bytes)

Actual IPv6 default gateway address used by the Z/IP Gateway to reach off-link subnet prefixes.

PAN IPv6 Prefix (16 bytes)

Actual IPv6 Prefix used by the Z/IP Gateway to construct IPv6 addresses for Z-Wave nodes.

It may be the ULA prefix if ::/128 was specified in the set.

4.15.6 Gateway Unregister

The message is used by a portal to force the client to close the existing tunnel.

7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_ZIP_PORTAL							
Command = GATEWAY_UNREGISTER							

REFERENCES

[1] Silicon Labs , SDS10242, Software Design Spec., Z-Wave Device Class Specification.

[2] Silicon Labs , SDS12657, Z-Wave Command Class Specification A-M.

[3] Silicon Labs , SDS12652, Z-Wave Command Class Specification N-Z.

[4] IETF RFC 4861, Neighbor Discovery for IP version 6 (IPv6), http://tools.ietf.org/pdf/rfc4861.pdf

[5] IETF RFC 3122, Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification, http://tools.ietf.org/pdf/rfc3122.pdf

[6] IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, http://tools.ietf.org/pdf/rfc2119.pdf

[7] IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, http://tools.ietf.org/pdf/rfc2460.pdf

[8] IETF RFC 4291, IP Version6 Addressing Architecture, http://tools.ietf.org/pdf/rfc4291.pdf

[9] Silicon Labs , SDS11846, Z-Wave Plus Role Types Specification.

[10] Silicon Labs , SDS11847, Z-Wave Plus Device Types Specification.

[11] Graphical UI elements, http://en.wikipedia.org/wiki/Graphical_user_interface_elements

[12] Silicon Labs , SDS13425. Z-Wave Plus Assigned Manufacturer IDs.

[13] Silicon Labs , SDS13548, List of defined Z-Wave Command Classes

[14] Silicon Labs , SDS13783, Z-Wave Transport-Encapsulation Command Class Specification

[15] Silicon Labs , SDS13782, Z-Wave Management Command Class Specification

[16] Silicon Labs , SDS13781, Z-Wave Application Command Class Specification

[17] IETF RFC 7428, Transmission of IPv6 Packets over ITU-T G.9959 Networks, https://tools.ietf.org/pdf/rfc7428.pdf

[18] Silicon Labs , SDS11633, Software Design Spec., Z/IP Resource Directory.

[19] Silicon Labs , SDS11756, Software Design Spec., Z/IP DNS Discovery Support.

[20] IANA Service Name and Transport Protocol Port Number Registry http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

[21] Silicon Labs , SDS13968, Smart Start User Input Identifier Registry

[22] Silicon Labs , SDS13944, Node Provisioning Information Type Registry (QR code, Z/IP Gateway, Smart Start)

[23]