UM0450
User manual

Getting started with the SN2X-PRIMER kit

Overview

The SN2X-PRIMER kit represents a ready-to-run ZigBee® network provided with two network nodes acting as the Coordinator and Router in compliance with standard ZigBee® specifications. Definitions for Coordinator, Router, and other ZigBee® concepts are provided in the following sections.

The main purpose of this evaluation kit is to demonstrate the main ZigBee® concepts and be open for further development. In fact, it will be possible to add more nodes and/or end devices, download an updated application version or connect an Insight Adapter for network monitoring.

This user guide describes how to operate the SN2X-PRIMER kit package, which consists of both Coordinator and Router boards and the required software.

The SN2X-PRIMER kit package contains two boards:

- MB622 (SN2X-PRIMER Coordinator), which is able to create a ZigBee network by enabling the joining and communication with other nodes
- MB623 (SN2X-PRIMER Router), which is able to join the ZigBee network and to communicate with the Coordinator

The software consists of:

- Applications executed on the two boards in order to have them working as ZigBee Coordinator and ZigBee Router respectively
- ZigBee protocol stack running to allow the network creation and nodes communication

More details on boards and software are provided in the following sections.

Due to the partnership between STMicroelectronics and Ember, and the total compatibility between the SN2xx and EM2xx (where xx may be 50 or 60) devices, certain documents have been kindly provided by Ember.

Contents

1 Description of the delivered package 3

1.1 MB622 coordinator board 3

1.2 MB623 router board 4

1.3 Board power supply 6

1.4 Power-save mode 6

2 Getting started 7

2.1 Types of networks 7

2.2 Menu commands description 7

2.3 Scenario 1: Setting up a ZigBee network 8

2.4 Scenario 2: Sending Unicast and Broadcast messages 9

2.5 Scenario 3: Displaying network parameters 11

2.6 Scenario 4: Modifying the network configuration 12

2.7 Scenario 5: Activating additional security features 12

2.7.1 ZigBee security levels 13

2.7.2 Typical network joining procedure 13

2.7.3 Security scenarios 13

3 Revision history 16

1 Description of the delivered package

The SN2X-PRIMER kit contains the following items:

- One Guarantee record card
- One MB622 (SN2X-PRIMER Coordinator) board
- One MB623 (SN2X-PRIMER Router) board
- One CD-ROM including the following documents:
  - Application source code for ST7 and SN250
  - User manual (this document)
  - MB622 and MB623 board schematics
  - SN250 and SN260 datasheets
  - Generic documentation about the ZigBee® stack and network topologies (Application Development Guide from Ember)

1.1 MB622 coordinator board

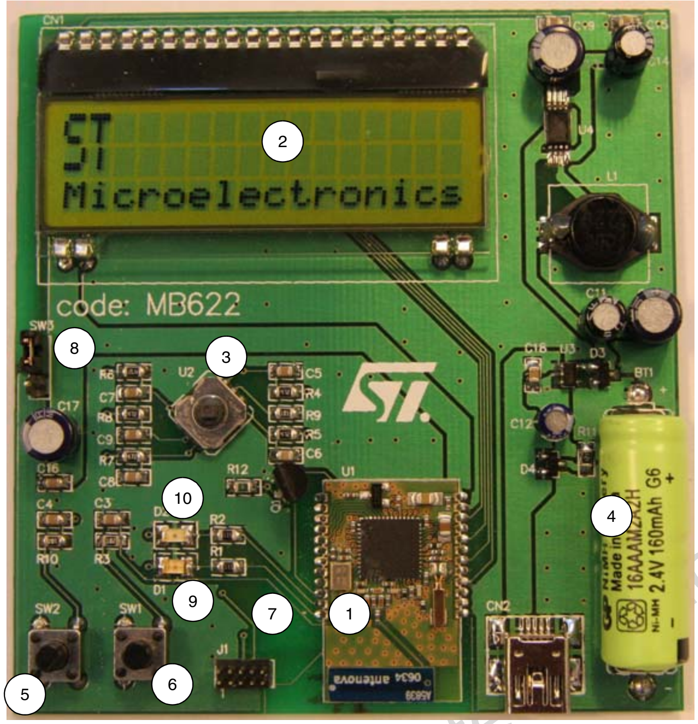
The MB622 (SN2X-PRIMER Coordinator) board (*Figure 1*) is designed to demonstrate all the main features of a ZigBee® Coordinator. Its main role is to create ZigBee® networks, to help connect with other nodes, and to communicate, depending the standard, with other nodes joining the network subsequently.

The main features of the MB622 board are an ST SN250 implementing the ZigBee® Coordinator, a simple and powerful user interface with a small LCD to display information and joystick to navigate, as well as a rechargeable battery.

Table 1. MB622 coordinator board main components

No.	Item	Description
1	SN250	ST ZigBee module executing the ZigBee stack and application
2	LCD	3-line display showing commands and their execution results
3	Joystick	Tool used to navigate and select commands within the menu
4	Battery	This supply is rechargeable by the USB connection
5	SW2	Board reset button
6	SW1	Board wake-up button
7	J1	SIF connector used to upload the new software into the SN250
8	SW3	Switch used to set the following configurations: – Configuration 1-2 (shown in *Figure 1*) provides the power supply to the board – Configuration 2-3 is used to upload the SN250 software
9	D1	LED toggled by pressing the SW1 on the MB623 Router.
10	D2	LED toggled by pressing the SW2 on the MB623 Router.

Figure 1. MB622 coordinator board



1.2 MB623 router board

The MB623 (SN2X-PRIMER Router) board (*Figure 2*) is designed to demonstrate the main features of a ZigBee node: its capability to join a ZigBee network and to communicate with the Coordinator.

Additionally, the MB263 board demonstrates how the ST SN260 is able to work as network co-processor jointly with an ST ST7Lite39 microprocessor. Using this solution, the application is executed in the ST ST7Lite39 and the ZigBee stack in the ST SN260. The ST ST7Lite39 and the ST SN260 communicate via the SPI communication protocol using a software interface called EZSP API.

This approach represents an alternative to re-using applications running on existing devices by using the ZigBee protocol for wireless network connections. Conversely, the approach with the ST SN250 can execute both the application and stack code in the same device.

The main features of the MB623 board are an ST SN260, an ST ST7Lite39 and a rechargeable battery.

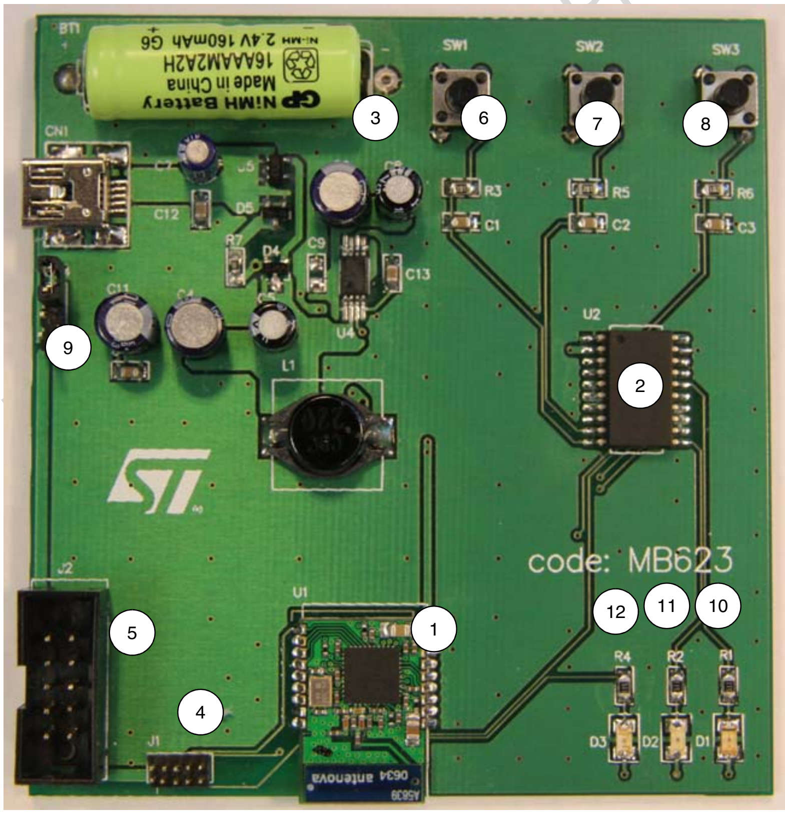
Table 2. MB623 router board main components

No.	Item	Description
1	SN260	ST ZigBee module executing the ZigBee stack.
2	ST7Lite39	ST microcontroller executing the application.

Table 2. MB623 router board main components (continued)

No.	Item	Description
3	Battery	This supply is rechargeable by the USB connection.
4	J1	SIF connector used to upload the new software into the SN260.
5	J2	ICC connector used to upload the software into the ST7Lite39.
6	SW1	When pressed, the MB623 Router sends a message to the MB622 coordinator to toggle the LED D1 on the MB622.
7	SW2	When pressed, the MB623 Router sends a message to the MB622 coordinator to toggle LED D2 on the MB622. It is also used as a wake-up button.
8	SW3	Board reset button.
9	SW4	Switch used to set the following configurations: – Configuration 1-2 (shown in *Figure 2*) provides the power supply to the board – Configuration 2-3 is used to upload the SN260 software
10	D1	This LED signals if the network is up and the MB623 Router is ready to send/receive messages.
11	D2	This LED is piloted using the commands on the MB622 Coordinator.
12	D3	This LED indicates SN260 network activity.

Figure 2. MB623 router board



1.3 Board power supply

The boards are supplied power by connecting a jumper in the 1-2 position (*Figure 3*) on switches SW3 and SW4 on boards MB622 and MB623 respectively.

Figure 3. Switch in 1-2 position

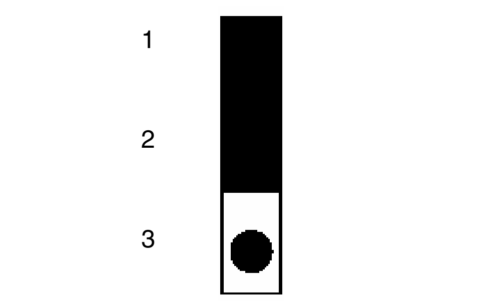
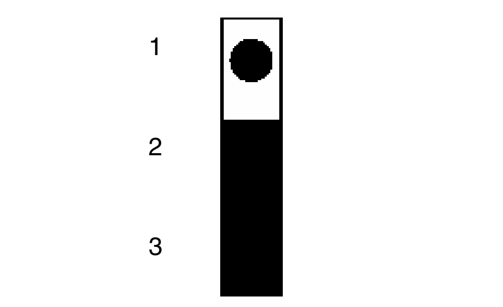


Figure 4. Switch in 2-3 position



To reprogram either the SN250 or the SN260, a jumper must be placed in the 2-3 position (*Figure 4*) on switches SW3 and SW4 for the MB622 and MB623 respectively. This will provide power to the SIF connectors used to download software.

Caution: Please take care that in order to correctly and efficiently recharge the boards' batteries, the USB cable must remain plugged in for at least 12 hours.

1.4 Power-save mode

The SN2X-PRIMER evaluation kit executes a power save mechanism for the Coordinator and the Router in order to increase the battery lifetime. If the Coordinator is not used for approximately 5 minutes, it sends a special broadcast sleep message (application defined) to all Routers to enter Power-save mode switching off the LCD, LEDs, and disabling the RF circuit. In this case, all messages sent to the Coordinator are lost.

The Router also automatically enters Power-save mode if it does not receive any message from the Coordinator or if the user does not press any buttons on the board for approximately 5 minutes. In this case, the Router switches OFF all LEDs, and both the SN260 and the ST7Lite39 are put in Power-save mode.

The Coordinator and the Router wake up when the user presses switches SW1 and SW2 on the Coordinator and Router boards, respectively.

The Coordinator and the Routers maintain all network parameters; the user does not have to form a new network.

2 Getting started

This section provides a complete description of possible commands and 5 typical use case scenarios:

Scenario 1: Setting up a ZigBee network

Scenario 2: Sending Unicast and Broadcast messages

Scenario 3: Displaying network parameters

Scenario 4: Modifying the network configuration

Scenario 5: Activating additional security features

2.1 Types of networks

ZigBee allows star, tree, and mesh network topologies using one coordinator, multiple routers and multiple end devices:

- *ZigBee Coordinator (ZC)* is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the ZigBee coordinator. The coordinator selects an appropriate channel after scanning for available channels and then selects the PAN ID.
- *ZigBee Router device* (ZR) provides routing services to network devices. Routers can also serve as end devices. Unlike normal end devices, routers are not designed to sleep and should generally remain on as long as the network is up.
- *ZigBee End devices* (ZED) are leaf nodes which communicate only with their parent nodes and, unlike router devices, cannot relay messages intended for other nodes. Depending on the network topology, end devices can be of several types:
  - *Sleepy end devices* power down their radio when idle, and thus save resources. Sleepy end devices are also sometimes known as RX-off-when-idle devices. This is a standard ZigBee device type.
  - *Non-sleepy end devices* remain powered during operation. These devices are known as RX-on-when-idle devices. This is a standard ZigBee device type.

2.2 Menu commands description

The user interacts with the SN2xx-PRIMER evaluation kit through the LCD and the joystick available on the coordinator (MB622) board.

By moving the joystick up, down, left or right, the user scrolls through the list of all available commands displayed on the LCD screen. The screen displays the commands in a circular menu. *Table 3* lists the menu commands.

To execute the selected command, press down on the joystick. After the command is launched, the LCD displays the result of the execution.

For example, to execute the **Show Channel** command, perform the following sequence:

1. Connect jumper SW3 in 1-2 position to switch on the coordinator board, or press switch SW2 to reset the board.
2. Scroll right to enter the first-level menu.
3. Scroll left or right to display **Show Channel** and press the joystick to confirm.

Table 3. First-level menu commands

Command Name	Description
Set Channel	Selects the current ZigBee channel. The valid channel range is 11 to 26.
Show Channel	Displays the current channel.
Set PanID	Selects the identification number a personal area network (PAN).
Show PanID	Displays the current PAN ID. The valid range is 0x0000 to 0x3FFF.
Form Network	Creates a new PAN.
Permit Joining	Enables other devices to join the PAN.
Show LQI	Displays the link quality indicator of the last message received.
Show EUI	Displays the Extended Unique Identifier (EUI) address of the coordinator.
Switch ON Router LED	Sends a unicast or a broadcast message to switch on the router LED.
Switch OFF Router LED	Sends a unicast or a broadcast message to switch off the router LED.
Leave Network	Leaves the network.
Neighbor table	Shows the neighbor table information. For more information, refer to *Table 4*.
Change security key	Activates the security features on the coordinator. The user can select and enable the three security scenarios supported by the kit.
LetItBee Version	Shows the firmware version of the SN2xx-PRIMER evaluation tool and the Ember ZigBee stack version.

2.3 Scenario 1: Setting up a ZigBee network

One of the main goals of the SN2X-PRIMER evaluation is to demonstrate the basic ZigBee network concepts used to form a simple two-node network using a *Coordinator* and a *Router* device.

Generally, all nodes belonging to the same network communicate (transmit and receive) on the same channel, or frequency. The personal area network identifier (PAN ID) is used to uniquely identify this network.

The kit comes with default channel and PAN ID values of “20” and “0x1CC” respectively. These values may be changed in the Coordinator (MB622) board before creating the network.

1. Connect jumper SW3 in 1-2 position to switch on the Coordinator board, or press switch SW2 to reset the board.
2. Scroll right to enter the first-level menu.
3. (Optional) Set new default channel value on the Coordinator board.
   a) Scroll left or right to display **Set Channel** and press the joystick to confirm.
   b) Scroll up or down to display channels and press the joystick to select channel.
4. (Optional) Set new default PAN ID value on the Coordinator board.
   a) Scroll left or right to display **Set PAN ID** and press the joystick to confirm.
   b) Scroll up or down, left or right to display numbers and press the joystick to select correct ID numbers.
5. Scroll left or right to display **Form Network** and press the joystick to confirm.
6. Scroll left or right to display **Permit Joining** and press the joystick to confirm.
7. Scroll up or down to select the number of seconds (between 0 and 99) to allow joining and press the joystick to confirm. If set to 0, joining is disabled. The Coordinator is now ready to accept requests from other devices that wish to join the network.
8. On the Router board, connect jumper SW4 in 1-2 position or press switch SW3 to reset the board. The Router starts to scan channels and will send a request to join available networks.

When the device is joined, the Coordinator board displays the Network ID (0x796E, for example) and the EUI (0080E100000009BE, for example). When the Router board is joined to a network, LED D1 is active (green).

The SN2X-PRIMER evaluation kit supports also the possibility to add other devices to the basic SN2xx-PRIMER 2-node network. In this case, the Coordinator LCD displays the parameters of all devices and the types of messages exchanged with the Coordinator.

For more information regarding networking aspects, please refer to the ZigBee and IEEE Std 802.15.4 specifications.

2.4 Scenario 2: Sending Unicast and Broadcast messages

The ZigBee standard supports two basic types of messages:

- *Unicast*, sent to a specific node ID based on an address table
- *Broadcast*, sent to all devices

Before sending a message, the application must construct the payload of the message. The message frame varies according to message type and security levels. Since much of the message frame is generated outside of the application, the key factor that must be considered is the maximum size of the originating message payload.

The ZigBee addressing scheme for messages is:

- *EUI-64*, a 64-bit globally unique address assigned to each device at manufacturing that never changes
- *Network Address*: a 16-bit unique network address assigned to each device when it joins the network; may change (due to conflicts)
- *Endpoint*, is a service point within a ZigBee device, it is 8-bit logical address.
- *Cluster ID*: a 16-bit field defined as “a related collection of attributes and commands”, which together define a communications interface between two devices. Cluster IDs and their associated message structures are defined by the application profile.

The Using the SN2X-PRIMER evaluation kit manages both *"Unicast"* and *"Broadcast"* messages types.

The Coordinator board is designed to send both Unicast and Broadcast messages, while the Router board can only send Unicast messages.

The activities linked to the messages management are highlighted by means of the LEDs available on the two boards.

To send a message from the Coordinator to the Router, use the **Switch ON Router LED** or **Switch OFF Router LED** command.

1. Ensure that the Router and Coordinator are joined and switched ON. See *Scenario 1: Setting up a ZigBee network*.
2. On the Coordinator board, scroll right to enter the first-level menu.
3. Scroll left or right to display **Switch ON Router LED** and press the joystick to confirm. Scroll down to display "Switch ON Router LED with Unicast msg" or "Switch ON Router LED with Broadcast msg" and press joystick to confirm the selected type of message.
   – For Unicast messages, the Router LED D2 (red) switches on or off, depending on the Switch ON or Switch OFF commands, immediately.
   – For Broadcast messages, the Router LED D2 (red) blinks several times before switching on or off, depending on the Switch ON or Switch OFF commands.

To send a message from the Router to the Coordinator, use switches SW1 and SW2 on the Router. The Router sends a Unicast message.

1. On the Router board, press switch SW1 to switch ON/OFF the Coordinator LED D1 (green).
2. Press switch SW2 to switch ON/OFF the Coordinator LED D2 (red).

When the Coordinator receives a message from the Router, the Coordinator LCD displays:

- the message type, unicast or broadcast
- the sender's network address
- and the cluster ID, Cluster1 for SW1 and LED D1 and Cluster2 for SW2 and LED D2

If the Coordinator receives either a Unicast or Broadcast message from another joined device, the LCD also displays the EUI-64 address of the sender.

It is possible to use the command list to select a router destination address, after the Unicast message type selection, in case more than one router is joined to the SN2X-PRIMER network.

The kit also provides information regarding the connection status between the nodes using the Coordinator LCD and the Router LED D1. In particular, when the Coordinator does not receive an acknowledgment by the Router, its LCD displays the "Failed – no network" message together with the message type (Unicast or Broadcast) and the destination node ID.

On the other hand, when the Router does not receive an acknowledgment from the Coordinator, its D1 LED starts to blink for a couple of seconds.

For more information regarding messaging aspects, please refer to the ZigBee and IEEE Std 802.15.4 specifications.

2.5 Scenario 3: Displaying network parameters

The network layer uses the knowledge on the quality of links between nodes in order to establish working routes and to optimize the reliability and efficiency of these routes.

Additionally, links in wireless networks may have an asymmetrical link quality due to noise variations in the local environment, receiver sensitivity and transmit power.

For the above reasons and other situations that may occur within networks, it is useful to store a set of network information in the neighbor table.

ZigBee routers keep track of inbound link quality in the neighbor table typically by averaging LQI (Link Quality Indication) measurements made by the physical layer.

To handle link asymmetry, routers obtain and store costs of outgoing links as measured by their neighbors by exchanging link status information via periodic one-hop broadcasts referred to as “neighbor exchange” or “link status” messages.

The neighbor exchange is automatically handled by the ZigBee stack and the application does not have to take care of this.

All the information contained in the neighbor table are used to understand the details of the network layer's operation and therefore to discover possible issues.

The SN2X-PRIMER displays the information stored in the Coordinator neighbor table through the **Neighbor Table** command.

Table 4 lists the data displayed in the neighbor table.

Table 4. Neighbor table data

Data	Description
ID	Network ID of the device joined. Values range from 0x0000 to 0xFFFF.
LQI	An exponentially weighted moving average of the link quality values of incoming packets from this neighbor as reported by the physical layer. Values range from 0x00 to 0xFF.
IC	The incoming cost for this neighbor, computed from the average LQI. Values range from 1 for a good link to 7 for a bad link.
OC	The outgoing cost for this neighbor, obtained from the most recently received neighbor exchange message from the neighbor. A value of zero means that a neighbor exchange message from the neighbor has not been received recently enough, or that our ID was not present in the most recently received one. Values range from 0x00 to 0xFF.
A	The number of aging periods elapsed since a neighbor exchange message was received from this neighbor. This is applicable in the mesh topology. Values range from 0x00 to 0xFF.
EUI	EUI address of the device joined. Values range from 0x0000000000000000 to 0xFFFFFFFFFFFFFFFF.

1. Ensure that the Router and Coordinator are joined and switched ON. See *Scenario 1: Setting up a ZigBee network*.
2. On the Coordinator board, scroll right to enter the first-level menu.
3. Scroll left or right to display **Neighbor Table** and press the joystick to confirm.
4. Scroll up or down to display the neighbor table information of all the joined nodes.

The SN2X-PRIMER *Coordinator* can show additional information using the following commands by scrolling right or left.

- **Show LQI**: link quality indicator of the last message received
- **Show EUI**: show the Coordinator EUI address
- **LetItBee Version**: shows the application version loaded in the SN250 and the current ZigBee stack version.

2.6 Scenario 4: Modifying the network configuration

In some circumstances it may be useful to change network parameters. In order to apply the changes, the *Coordinator* has to leave the network, change the network parameters, and then form again the network.

1. On the Coordinator board, scroll right to enter the first-level menu.
2. Scroll left or right to display **Leave Network** and press the joystick to confirm.
3. Change the network parameters as explained in *Scenario 1: Setting up a ZigBee network*.
4. Scroll left or right to display **Form Network** and press the joystick to confirm.
5. Scroll left or right to display **Permit Joining** and press the joystick to confirm.
6. On the Router(s), press switch SW3 to reset the board(s).

2.7 Scenario 5: Activating additional security features

ZigBee uses the basic security elements available in specification IEEE 802.15.4 as well as the following security features:

- 128-bit Advanced Encryption Standard (AES) encryption algorithms
- Strong, National Institute of Standards and Technology (NIST) approved security
- Defined key types (link, network)
- Defined key setup and maintenance (commercial, residential)
- Keys can be hardwired into an application
- CCM* (Unified/Simpler mode of operation with encryption-only and integrity-only capabilities)
- Trust Center
- Security that can be customized for the application

For more information regarding security aspects, please refer to the ZigBee and the IEEE Standard 802.15.4 specifications.

2.7.1 ZigBee security levels

For increased network security, three standard levels of security are defined in the 2007 ZigBee specifications:

- The *Residential* security service included in the ZigBee 2006 specification provides Network Layer security using a Network Key.
- The *Standard* security service included in the 2007 ZigBee Pro specification provides *Residential* security with a set of optional enhancements which include APS Layer security using Link Keys.
- The *High* security service included the 2007 ZigBee Pro specification provides the Standard security with the use of Entity Authentication, Permissions Table, and deriving Link Keys between devices.

The *Network Layer se*curity, provided with the *Residential* security service, uses a network-wide key for encryption and decryption. All devices authorized by the Trust Center (Coordinator) to join the network will receive a copy of the key, after joining, and will use it to encrypt and decrypt all transmissions.

The message to the joining device is encrypted using a preloaded Link Key for that joining device (known to both the Trust Center and the joining device) using APS Layer security.

The *Application Layer Security* provided with the *Standard* security service uses a peer-to-peer Link Key. Both devices must have already established this key with one another prior to sending APS Secured data. The Link Key is established with the Coordinator (Trust Center) after the device joins the network.

The SN2X-PRIMER evaluation tool uses the Standard security service to demonstrate the security features.

2.7.2 Typical network joining procedure

The typical network joining procedure in a ZigBee network with the Standard security level executes the following steps:

1. The joiner device sends a MAC Association Request to the parent device.
2. The Parent device answers with a MAC Association Response.
3. The joiner device is joined using the PAN but is still unauthenticated.
4. The Trust Center starts the authentication procedure.
5. The Trust Center sends the Network Key to the joiner device.
6. The Trust Center completes the procedure and authenticates the joiner device.

Note: In our case, both the parent and the Trust Center are the same device (Coordinator).

2.7.3 Security scenarios

The SN2X-PRIMER evaluation kit implements the following three security scenarios:

1. Preconfigured Link Key
2. Different Link Key
3. No preconfigured Link Key

Preconfigured link key

In this scenario, both Coordinator and Router devices have the same preconfigured Link Key known as “Key 1”.

During the joining procedure, the Router (joiner device) requests the network key and retrieves it encrypted using the device's preconfigured Link Key.

Only the devices with the same preconfigured Link Key can obtain the network key and can complete the joining authentication with success; otherwise, the device cannot communicate with the devices on the ZigBee network.

1. On the Coordinator board, scroll right to enter the first-level menu.
2. Scroll left or right to display **Form Network** and press the joystick to confirm.
3. Scroll left or right to display **Change security Key** and press the joystick. Select **Key 1 (Default)** and press the joystick to set the key and to allow its distribution within the network.
4. Scroll left or right to display **Permit Joining** and press the joystick to confirm.
5. Scroll up or down to select the number of seconds (between 0 and 99) to allow joining and press the joystick to confirm. If set to 0, joining is disabled. The Coordinator is now ready to accept requests from other devices that wish to join the network. The Coordinator displays the “Now Permit Joining with security key 01” message.
6. On the Router board, connect jumper SW4 in 1-2 position or press switch SW3 to reset the board. The Router starts to scan channels and will send a request to join available networks.

When the device is joined, the Coordinator board displays the Network ID (0x796E, for example) and the EUI (0080E100000009BE, for example) as a result of an application-level message sent by the Router. When the Router board is joined to a network, LED D1 is active (green).

Different link key

In this scenario, the Coordinator changes its Link Key from the preconfigured Key 1 to Key 2 and the Router maintains its original preconfigured key called Key 1.

The Router as first step executes the unauthenticated joining, and subsequently the Coordinator starts the authentication procedure to complete the joining process. As result, the Trust Center refuses the Router's authentication because it has a different link key and cannot join the network (PAN).

1. On the Coordinator board, scroll right to enter the first-level menu.
2. Scroll left or right to display **Form Network** and press the joystick to confirm.
3. Scroll left or right to display **Change security Key** and press the joystick. Scroll down to select **Key 2** and press the joystick to set the key and to allow its distribution within the network.
4. Scroll left or right to display **Permit Joining** and press the joystick to confirm.
5. Scroll up or down to select the number of seconds (between 0 and 99) to allow joining and press the joystick to confirm. If set to 0, joining is disabled. The Coordinator is now ready to accept requests from other devices that wish to join the network. The Coordinator displays the “Now Permit Joining with security key 02” message.
6. On the Router board, connect jumper SW4 in 1-2 position or press switch SW3 to reset the board. The Router starts to scan channels and will send a request to join available networks. The Coordinator displays the “Attempt to join with preconf. key” message followed by the EUI address.

Note: Because a different Link Key is used, the Router cannot join the network.

No preconfigured link key

In this scenario, the Router does not have a preconfigured Link Key and executes a joining procedure requesting a network key.

The Router initially joins in unauthenticated way and subsequently, during the authentication, the network key is sent from the Trust Center (Coordinator) to the Router unencrypted. The authentication phase represents a case where the security is at risk, but may be acceptable depending the type of application.

Additionally, the Router can also request the Link Key from the Trust Center (Coordinator) which will be sent encrypted with the network key.

1. On the Coordinator board, scroll right to enter the first-level menu.
2. Scroll left or right to display **Form Network** and press the joystick to confirm.
3. Scroll left or right to display **Change security Key** and press the joystick. Scroll down to select **No preconf. Key** and press the joystick to set the key and to allow its distribution within the network.
4. Scroll left or right to display **Permit Joining** and press the joystick to confirm.
5. Scroll up or down to select the number of seconds (between 0 and 99) to allow joining and press the joystick to confirm. If set to 0, joining is disabled. The Coordinator is now ready to accept requests from other devices that wish to join the network. The Coordinator displays the “Now Permit Joining with no preconf. Key” message.
6. On the Router board, connect jumper SW4 in 1-2 position or press switch SW3 to reset the board. The Router starts to scan channels and will send a request to join available networks. The Coordinator briefly displays the “Attempt to join with preconf. key” message followed by the EUI address.

When the device is joined, the Coordinator board displays the Network ID (0x796E, for example) and the EUI (0080E100000009BE, for example) as a result of an application-level message sent by the Router. When the Router board is joined to a network, LED D1 is active (green).

3 Revision history

Table 5. Document revision history

Date	Revision	Changes
04-Oct-2007	1	Initial release.

Please Read Carefully:

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan -
Malaysia - Malta - Morocco - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com