

ZIGBEE ROUTER R0
REFERENCE MANUAL



Table of Contents

1. Overview	1
2. Features	2
3. Installation	4
3.1. Mains Powered Operation	4
3.2. Low-Voltage Operation	4
4. Initial Device Start-Up	5
5. Man-Machine interface (MMI)	7
5.1. Power-Cycle Sequencing Factory Reset	8
6. Zigbee Interface	10
6.1. Device Anatomy	10
6.2. Installation Code	10
6.2.1. Format according to Zigbee recommendations	10
6.2.2. Historic ubisys-proprietary formats	11
6.3. Application Endpoint #0 - Zigbee Device Object	11
6.4. Application Endpoint #232 - Device Management	12
6.4.1. Basic Cluster (Server)	13
6.4.2. Over-the-Air Upgrade Cluster (Client)	13
6.4.3. Zigbee Direct Cluster (Server)	14
6.4.4. Works With All Hubs Cluster (Server)	14
6.5. Application Endpoint #242 - Zigbee Green Power	14
6.5.1. Green Power Cluster (Server)	14
7. Physical Dimension	17
8. Ordering Information	18
9. General Terms & Conditions Of Business	19
10. Declaration Of Conformity	20
11. Revision History	22
12. Contact	23

1. Overview

Thank you for purchasing the ubisys Zigbee Router R0.

You have decided for a high-quality product with first-rate support!

This reference manual provides operating and maintenance instructions, interface specifications, command references and more. It is primarily intended for system integrators, not end-users.

An installation guide specific to your region is available as a separate document and is included in printed form in the product package.

If you have any questions or need additional support, please visit the support pages that best fit your background:

If you are a consumer (private household) or installer, please visit the Smart Home support pages at <http://www.ubisys.de/en/smarthome/support.html> for contact details.

As a commercial customer, please visit the Engineering support pages at <http://www.ubisys.de/en/engineering/support.html> for contact details.

Copyright© 2014-2023 ubisys technologies GmbH, Düsseldorf, Germany.
All rights reserved.

2. Features

- Zigbee 3.0 Router including Zigbee Direct ^[1] and Green Power Proxy features
- Reliable, unattended, maintenance-free operation; designed for in-wall flush-mounting
- Made in Germany using high-quality, enduring parts for many years of life expectancy
- Low power dissipation: 0.2W ^[2]
- On-board MCU: Advanced 32-bit ARM micro-controller running at 64MHz with 96KB SRAM [2023 generation; first generation: 48MHz, 64KB SRAM]
- IEEE 802.15.4 radio: 10dBm transmit power ^[3], -98dBm receiver sensitivity (-101dBm when Bluetooth is disabled) ^[4]
- On-board inverted-F antenna
- Leverages Zigbee stack for best-in-class reliability and performance
- Leverages ubisys IEEE 802.15.4 MAC (1st generation) or Qorvo IEEE 802.15.4 MAC (2nd generation)
- Supports all channels in the 2.4 GHz band, i.e. channels 11-26 as per IEEE 802.15.4: Primary = { 11, 15, 20, 25 }; Secondary = { 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24, 26 }
- Supports joining centralized and distributed security networks as router
- Supports forming simple centralized security networks as Coordinator and Trust Center
- Supports forming distributed security networks as router
- Three pre-configured Trust Center Link-Keys for joining:
 - Global Default Trust Center Link-Key (“ZigBeeAlliance09”)
 - Zigbee 3.0 Global Distributed Security Link-Key ^[5]
 - Device-individual link-key derived from installation code – also printed as text and QR barcode
- Extended neighbour table with up to 78 entries for routers and end-devices - more than three times the capacity required by the standard (25)
- Extended routing table with up to 96 entries for ad hoc and many-to-one routes - nearly ten times the capacity required by the standard (10)
- Extended buffering for sleeping end-devices with up to 24 buffers - 24 times the capacity required by the standard (1)
- Extended APS duplicate rejection table with up to 64 slots - 64 times the capacity required by the standard (1)
- Extensive transmit and receive queues for optimum through-put and minimum packet drop rate
- Reliable and scalable network-wide broadcasts featuring passive acknowledgments
- Reliable packet forwarding with automatic network-level retries
- Very sophisticated routing algorithm for reliable ad hoc routing – avoids routing loops even in case of concurrent route requests with overlapping source/destination
- Firmware upgradable over-the-air during normal operation using Zigbee OTA Upgrade Cluster
- Man-Machine-Interface: A push-button and a LED for network steering, factory reset etc.
- Flame retardant housing (V-0); black, RAL 9005

- [1] 2nd generation; not included in 1st generation
- [2] 2nd generation; 1st generation: 0.3W
- [3] 2nd generation; 1st generation: 5dBm
- [4] 2nd generation; 1st generation did not support Bluetooth
- [5] Since application firmware 1.05. Prior, pre-certification key (D0:...:DF)

3. Installation

3.1. Mains Powered Operation

Please refer to the hardware installation guide, which was included in the product package. It provides detailed installation instructions.

3.2. Low-Voltage Operation

Instead of applying dangerous mains voltage to the Router R0, you may connect a low-voltage DC source to the supply lines of R0. Its built-in universal power supply is able to operate from both kinds of supplies, direct and alternating current. First generation hardware can run off 12V_~ or higher, e.g. 12V_~, 24V_~, or 48V_~ supplies. Second generation hardware requires at least 24V_~, i.e. use e.g. a 24V_~ or 48V_~ supply.

For DC operation, connect the DC ground (0V, “minus”, negative) of your power supply to the phase input of R0 (marked “L”, brown) and the DC supply voltage (24...48V_~, “plus”, positive) to the neutral input of R0 (marked “N”, blue). Once powered, you should observe the normal device start-up behaviour (the green LED will flash a few times).

The built-in universal power supply can accept up to 400V_~, which is an absolute maximum rating.

If you are not using a safe low-voltage power-supply, utilizing the services of a professional installer/electrician is imperative.

4. Initial Device Start-Up

The router will search for an open Zigbee network to join when you first apply power to it.

Open the Zigbee network for joining and then power-up the device.

R0 will blink quickly to indicate a search in progress. Once a search cycle is complete it will either blink five times slowly to indicate it has joined a network, or blink three times quickly to indicate a joining failure – for example no network found, not permitted onto the network, etc. It will continue to search for a network in case of failure.

Subsequently, when the device is power-cycled, it will blink five times slowly to indicate it is operating as a router on the network, ten times slowly to indicate that it is operating as a coordinator and trust center or blink quickly to indicate it is searching for a network to join. When commissioned, the router's LED will remain off after the five/ten blink cycles during normal operation. Afterwards, it will turn on only for as long as it is permitting other devices to join the network.

After reboot, if the device is properly commissioned, it resumes operation doing a "silent rejoin", i.e. it does not broadcast a device announcement in this case. After joining a network, the device will prolong the joining window by three minutes via a fresh ZDO permit joining request ^[6]

[6] Stretching the joining duration is done in products with ubisys Zigbee Stack version 1.48 or above.

5. Man-Machine interface (MMI)

R0 offers a push-button behind a tiny hole in the front-face of the device, as well as a LED right next to it. This man-machine interface provides access to a menu. In addition, it provides a handy shortcut to factory reset the device ^[7].



To factory reset the device, keep the button pressed for approximately 10 seconds until the LED starts to flash. This is equivalent to selecting menu item #5. Notice that the device also supports a power-cycle sequencing factory reset as detailed in [Section 5.1](#)

To enter the menu, press and hold the push-button for more than a second until you see three short flashes followed by a sequence of one blink, pause, one blink, pause, etc. This indicates that you have successfully entered the menu. With each short button press (less than a second), you advance through the menu. For example, pressing the button once brings you to the second menu item, which R0 indicates by two blinks, pause, two blinks pause, etc. Once you have reached the menu item that you want to run, press and hold the button for more than a second to execute the selected item. The exact meaning of each menu item depends on the particular device and may vary from firmware version to firmware version.

This is the menu for Router R0 running firmware version 1.01 and above ^[8]:

Menu Item #	Operation
1	Zigbee Commissioning: Network Steering While in this mode a single press on the button instigates ZigBee Network Steering (“EZ-mode”). If the device is on a network it will open the network for new devices for three minutes, otherwise it will attempt to join an open network. If the network is already open, the device will close the network instead such that repetitive presses toggle the network permit joining state. The LED is on, when the network is open for new devices, and off otherwise.
2	Zigbee Commissioning: Finding & Binding Instigates the ZigBee Finding & Binding procedure (“EZ-mode”) on an initiator or target endpoint. Target endpoints will enter identify mode for three minutes. Initiator endpoints will query targets and create suitable bindings to these targets. After leaving the menu in this mode, the first button press starts the selection of the endpoint and each subsequent press (within half a second) increments the endpoint number. Once the desired endpoint is reached, wait for the LED to blink the selected number of times. Then, press a single time to accept the selection or wait for three seconds to cancel the command. The LED will blink one time to confirm an affirmative choice, or two times to indicate the request has been cancelled. This menu item is not implemented on router R0.
3	Zigbee Commissioning: Clear Bindings Clears bindings on an initiator endpoint. Select this menu item and leave menu mode. Afterwards the device expects the selection of an initiator endpoint. The first button press starts the selection of the endpoint and each subsequent press (within half a second) increments the endpoint number. Once the desired endpoint is reached, wait for the LED to blink the selected number of times. Then, press a single time to accept the selection or wait for three seconds to cancel the command. The LED will blink one time to confirm an affirmative choice, or two times to indicate the request has been cancelled. This mode is active for one round only. Afterwards the device reverts to mode #1. This menu item is not implemented on router R0.

Menu Item #	Operation
4	<p>Zigbee Commissioning: Set Device Role and Factory Reset</p> <p>Selects the Zigbee device role for this device on the network, resets the remaining settings to factory defaults and restarts the device. Select this menu item and leave menu mode. Afterwards the device expects the selection of an option. The first button press starts the selection of the option and each subsequent press (within half a second) increments the option number. Once the desired option is reached, wait for the LED to blink the selected number of times. Then, press a single time to accept the selection or wait for three seconds to cancel the command. The LED will blink one time to confirm an affirmative choice, or two times to indicate the request has been cancelled. The following options are available:</p> <p>Option #1: Join an existing Zigbee network as router Option #2: Form a new distributed security network as the first router Option #3: Form a new centralized security network as the coordinator and trust center</p>
5	<p>Factory Reset</p> <p>Put the device into the same state as it was when it left the factory, then reboot. The only exception is the outgoing network security frame counter, which is preserved across factory resets. The device will broadcast a network leave indication ^[9].</p>
6	<p>Zigbee Commissioning: Advanced Commands</p> <p>Provides a number of advanced Zigbee commissioning command options. Select this menu item and leave menu mode. Afterwards the device expects the selection of an option. The first button press starts the selection of the option and each subsequent press (within half a second) increments the option number. Once the desired option is reached, wait for the LED to blink the selected number of times. Then, press a single time to accept the selection or wait for three seconds to cancel the command. The LED will blink one time to confirm an affirmative choice, or two times to indicate the request has been cancelled. The following options are available:</p> <p>Option #1: Perform a simple reset (reboot), then continue operating seamlessly (silent re-join) Option #2: Perform a simple reset (reboot), then re-join the network Option #3: Perform a full factory reset, including security frame counters and preserved settings</p>
7	Reserved for internal use. Do not leave the menu in this mode.

5.1. Power-Cycle Sequencing Factory Reset

It is possible to instigate a factory reset using a special power-cycle sequence ^[10]. This is equivalent to selecting menu item #5, with the advantage that you need no access to the device itself (only to its power supply).

1. Power the device for at least 20 seconds.
2. Interrupt the power supply for at least ten seconds ^[11].
3. Reapply power for less than ten seconds but more than half a second ^[12].
Notice that at the end of this cycle, the device is off and should remain off for at least ten seconds ^[13].
4. Repeat the previous step two more times, for a total of three short power cycles.
5. Apply power to the device and leave it powered on.

The device will now factory reset and reboot.

[7] The 10-second-press factory reset (equivalent to menu item #5) is available since firmware version 1.02.

[8] Notice: Prior versions have different menu items. Only the factory reset command (menu item #5) is identical across all released versions of the firmware.

[9] Since application firmware 1.03. Previously, the factory reset would result in a silent leave.

[10] Since application firmware 1.06

[11] Since application firmware 2.2.0; prior, this was one second

[12] Since application firmware 2.2.0; prior, this was less than two seconds but more than half a second

[13] Since application firmware 2.2.0; prior, this was one second

6. Zigbee Interface

Please refer to the following IEEE and Zigbee Alliance documents, which apply to this product:

[R1] IEEE Standard 802 - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)

[R2] Zigbee Specification, Revision 23, Document No. 05-3474-23

[R3] Zigbee Cluster Library Specification, Revision 8, Document No. 07-5123-08

[R4] Zigbee Base Device Behavior Specification, Version 3.0.1, Document No. 16-02828-012

[R5] Zigbee PRO Green Power Feature Specification, Version 1.1.1, Document No. 14-0563-18

[R6] Zigbee Home Automation Public Application Profile 1.2, Revision 29, Document No. 05-3520-29

[R7] Zigbee Direct 1.0, Revision 29, Document No. 05-3520-29

[R8] QR Code Requirements, Revision 8, Document No. 18-01000-008

6.1. Device Anatomy

The routers main task is to act as a range extender by improving network connectivity and meshing capabilities as well as acting as a connection point (“parent”) for sleeping end-devices. As such, it does not provide any particularly useful application endpoints, except for device management.

This router provides four Zigbee application endpoints:

Endpoint #	Profile	Application
0 (0x00)	0x0000: Zigbee Device Profile	Zigbee Device Object (ZDO) - standard management features
232 (0xE8)	0x0104: Common Profile (HA)	Device Management (0x0008) ^[14]
242 (0xF2)	0xA1E0: Green Power Profile	Zigbee Green Power Proxy ^[15]

Notice: Eariler firmware versions included endpoint 200 (0xC8), which contained a legacy private application. This application is deprecated and has been removed in firmware version 2.2.0.

The ubisys Zigbee manufacturer ID is 0x10F2. This manufacturer code is used to identify OTA upgrade images, for accessing manufacturer-specific ZCL attributes and commands etc.

6.2. Installation Code

This router contains an installation code, a device-individual pre-shared secret (PSK). Is is used to derive a pre-configured link key or to function as a PSK for asymmetric key negotiation and authentication as provided by Zigbee 2023 and later revisions. It is printed on the back of the router’s housing in text format and as a two-dimensional barcode (QR code). The format specified in [R4], section 10.1.1 is used, i.e. 128-bit installation code + 16-bit CRC.

6.2.1. Format according to Zigbee recommendations

All recent ubisys products follow the Connectivity Standards Alliance (former Zigbee Alliance) best practices for Zigbee QR codes. Please refer to [R8] for a detailed description of the data format.

For example, an R0 label could contain information like this:

```
1 Z:001FEE00000000FF#I:0F7C1CD805F91649EBA84580AA1CB432F51A%G#M:R0%M:10F2
```

6.2.2. Historic ubisys-proprietary formats

The QR code contains additional information as illustrated in the following example:

```
1 ubisys2/R0/001FEE00000000FF/0F7C1CD805F91649EBA84580AA1CB432F51A/21
```

Here, “ubisys2” is the data format identifier, R0 is the model string, followed by the EUI-64, the installation code, and a checksum that covers the entire information (including model, EUI-64 and installation code), all separated by a single slash character ('/'). The check sum is an unsigned 8-bit integer, which is calculated by performing a byte-wise exclusive-or (XOR, “⊗”) of the ASCII characters of the model string, the binary representation of the EUI-64 (in big endian format), and the binary representation of the install code.

For the example above, this calculation yields:

```
1 52 ('R') ⊗ 30 ('0') ⊗
2 00 ⊗ 1F ⊗ EE ⊗ 00 ⊗ 00 ⊗ 00 ⊗ 00 ⊗ FF ⊗
3 0F ⊗ 7C ⊗ 1C ⊗ D8 ⊗ 05 ⊗ F9 ⊗ 16 ⊗ 49 ⊗ EB ⊗ A8 ⊗ 45 ⊗ 80 ⊗ AA ⊗ 1C ⊗ B4 ⊗ 32 ⊗ F5
   ⊗ 1A = 21
```



The data format “ubisys1” is identical to “ubisys2” except for the check sum, which is present, but invalid. If you encounter “ubisys1” labels, then do not verify the trailing check sum field.

6.3. Application Endpoint #0 - Zigbee Device Object

Please refer to the Zigbee Specification [R2] for details on the Zigbee Device Object (ZDO) and the protocol used for over-the-air communication, called the Zigbee Device Profile (ZDP). Notice that the ZDP is fundamentally different from typical application endpoints, which build on the Zigbee foundation framework and the Zigbee Cluster Library (ZCL).

The ubisys Zigbee Router R0 supports the following ZDO services:

Primitive	Description
nwk_addr_req/ nwk_addr_rsp	Network address request/response Translates a 64-bit IEEE address into a 16-bit network short address. Use only when really required, because this message employs a network-wide broadcast (flooding)
ieee_addr_req/ ieee_addr_rsp	IEEE address request/response Translates a 16-bit network short address into a 64-bit IEEE address.
node_desc_req/ node_desc_rsp	Node descriptor request/response Returns information such as the manufacturer ID, power supply, etc.
power_desc_req/ power_desc_rsp ^[16]	Power descriptor request/response Returns information such as the power source and mode.
active_ep_req/ active_ep_rsp	Active endpoints request/response Returns a set of available application endpoints on the device.
simple_desc_req/ simple_desc_rsp	Simple descriptor request/response Returns a descriptor for a certain application endpoint with a list of available services (clusters).
match_desc_req/ match_desc_rsp	Match descriptor request/response Searches for a certain cluster or set of clusters and returns the matching endpoints, if any.
device_annce	Device announcement Advertises the presence of a new device in the network.

Primitive	Description
parent_annce/ parent_annce_rsp ^[17]	Parent announcement/response This is part of the Zigbee 2015 end-device child management feature.
system_server_discovery_req/ system_server_discovery_rsp ^[18]	System server discovery request/response Provides the ability to discover system servers, in particular the network manager.
bind_req/ bind_rsp	Bind request/response Creates an application binding
unbind_req/ unbind_rsp	Unbind request/response Removes an application binding
mgmt_nwk_discovery_req/ mgmt_nwk_discovery_rsp ^[19]	Management: Network discovery request/response Instructs the device to perform a network discovery and report the results back.
mgmt_lqi_req/ mgmt_lqi_rsp	Management: Neighbor table request/response Returns information about neighboring devices, including the link quality, device type etc.
mgmt_rtg_req/ mgmt_rtg_rsp	Management: Routing table request/response Returns information about routes established on the device.
mgmt_bind_req/ mgmt_bind_rsp	Management: Binding table request/response Returns information about application bindings on the device.
mgmt_leave_req/ mgmt_leave_rsp	Management: Leave request/response Makes the device leave the network or removes one of its end-device children.
mgmt_permit_joining_req/ mgmt_permit_joining_response	Management: Permit joining request/response Opens the network for new devices to join.
mgmt_nwk_update_request/ mgmt_nwk_update_notification ^[19]	Management: Network update request/response/notification Performs energy scans, instigates a channel change or assigns the network manager.



Binding table operations are supported, but not useful for a pure router (range extender).

6.4. Application Endpoint #232 - Device Management

This endpoint provides device management functions using standard Zigbee foundation paradigms and the Zigbee Cluster Library [R3]. You may use the standard ZCL frames to enumerate, read and write attributes, configure attribute reporting, invoke commands, etc.

The application endpoint exposes the following clusters:

Cluster	Direction	Description
0x0000	Inbound (Server)	Basic Provides basic information about the device, such as the manufacturer ID, vendor and model name, stack profile, ZCL version, production date, hardware revision etc. Allows a factory reset of attributes, without the device leaving the network.
0x003D	Inbound (Server)	Zigbee Direct Configuration ^[20] Allows configuration of the Zigbee Direct Device functionality that is part of this product. In particular, it provides a means for disabling (and reenabling) the Zigbee Direct (Bluetooth) interface, and configuring anonymous join timeouts.
0x0019	Outbound (Client)	OTA Upgrade Pull-oriented firmware upgrade. Searches the network for mating servers and allows the server to control all stages of the upgrade process, including which image to download, when to download, at what rate and when to install the downloaded image.
0x1217::0xFC57	Inbound (Server)	Works With All Hubs ^[21] Amazon Works With All Hubs proprietary cluster. Allows management of advanced Zigbee stack features related to security, robustness, resilience and diagnostics.

Notice: The initial firmware release contained an Identify server cluster. Versions after 1.00 of R0 do not include the Identify server cluster any more. Other ubisys products still include the client side of Identify for Finding & Binding, which moot for a pure range extender like the ubisys R0.

Notice: Earlier versions contained the Commissioning server cluster for commercial deployments. This kind of commissioning is deprecated and the cluster has been removed in version 2.0.0.

6.4.1. Basic Cluster (Server)

The basic cluster might be accessible via more than one endpoint. Most of its attributes are singleton attributes, i.e. all instances of the cluster share the same attribute value storage.

Attributes supported:

Attribute	Type	Description
0x0000	unsigned8, read-only	ZCLVersion The version of the cluster library
0x0001	unsigned8, read-only	ApplicationVersion The application version
0x0002	unsigned8, read-only	StackVersion The stack version
0x0003	unsigned8, read-only	HWVersion Specifies the hardware revision number
0x0004	string, read-only	ManufacturerName "ubisys"
0x0005	string, read-only	ModelIdentifier "R0 (5501)"
0x0006	string, read-only	DateCode "YYYYMMDD-XX-FBV", where YYYY = year, MM = month, DD = day of production (hardware), XX = production facility, V = factory block version. For example, "20130411-DE-FB0" refers to a device built April 11, 2013 in Germany and programmed with factory block format version 0.
0x0007	enum8, read-only	PowerSource Always set to mains-powered, single phase (regardless of the connected supply voltage)
0x0010	string, persistent	LocationDescription Empty string by default. Might be set by commissioning software during installation
0x0011	unsigned8, persistent	PhysicalEnvironment "Unspecified" by default. Might be set by commissioning software during installation

Cluster commands supported:

Command	Description
0x00	Reset to factory defaults. Restores the values of all attributes of all clusters across all endpoints to their factory fresh default settings. Does not affect network settings or bindings. Notice: In earlier versions, up to and including version 1.02, the command did actually behave like a leave command with factory reset. This command has been deprecated and is no longer supported since version 1.03. Use <code>mgmt_leave_req</code> , instead.

6.4.2. Over-the-Air Upgrade Cluster (Client)

The original image type for R0 is 0x7B0A. Later, image type 0x7B2A has been introduced with a new boot-loader, new factory block and new persistent storage version. This has been superseded by 0x7B3A, which incorporates a new boot-loader. The latter image types have been introduced to prevent inadvertent installation of incompatible firmware versions and are all related to first generation hardware. For 0x7B0A the final version migrates to 0x7B2A; similarly, for 0x7B2A the final version migrates to 0x7B3A, which is the current image type for first generation hardware. The image type for second generation hardware is 0x7B4A. The latest firmware in Zigbee OTA image format and

important historic firmware images (like the final versions that perform migration) are available publicly on our support web pages. This allows upgrading of devices in the field using third-party OTA servers and back-ends. If you operate the Router R0 together with the Zigbee/Ethernet Gateway ubisys G1, the latest firmware for R0 will always be available automatically and you do not need to request it explicitly.

6.4.3. Zigbee Direct Cluster (Server)

TBD

6.4.4. Works With All Hubs Cluster (Server)

TBD

6.5. Application Endpoint #242 - Zigbee Green Power

This endpoint provides the Zigbee Green Power feature according to the 2015 edition of the specification, i.e. including support for Green Power Devices with IEEE EUI-64 and bidirectional commissioning. The Zigbee traffic between Proxies and Sinks utilizes standard Zigbee foundation paradigms and the Zigbee Cluster Library [R3]. You may use the standard ZCL frames to enumerate, read and write attributes, invoke commands, etc.

The application endpoint exposes the following clusters:

Cluster	Direction	Description
0x0021	Outbound (Client)	Zigbee Green Power Proxy Allows sinks on the network to configure this device as a "Proxy", i.e. access point for Zigbee Green Power Devices into the Zigbee mesh network.

6.5.1. Green Power Cluster (Server)

The client-side of the Green Power cluster provides the Zigbee Green Power Proxy functionality, i.e. makes the device act as an "access point" for Green Power Devices (GPDs). This implementation supports unidirectional and bidirectional [22] GPDs.

Attributes supported:

Attribute	Type	Description
0x0010	unsigned8, read-only	gpsMaxSinkTableEntries The number of proxy table entries supported by this device
0x0011	extended raw binary, read-only, persistent	ProxyTable Entries in the proxy table create a link between Green Power Devices and Green Power Sinks
0x0016	bitmap24, read-only	gppFunctionality Indicates Green Power features and building blocks supported by this device
0x0017	bitmap24, read-only	gpsActiveFunctionality Allows to disable certain Green Power features on this device
0x0020	bitmap8, persistent	gpSharedSecurityKeyType Determines the security key type to use for devices with bidirectional commissioning capabilities, i.e. out-of-the-box individual key, shared GP key, etc.
0x0021	key128, persistent	gpSharedSecurityKey The 128-bit AES-CCM* key that is being used to secure Green Power data frames
0x0022	key128, persistent	gpLinkKey The 128-bit AES-CCM* key that is being used to deliver keying material to Green Power devices

Cluster commands supported:

Command	Description
0x01	GP Pairing Creates, updates or removes proxy table entries
0x02	GP Proxy Commissioning Mode Makes the proxy enter commissioning mode for a particular sink, or leave commissioning mode
0x06	GP Response Tunnels GP data frames from a sink to a bidirectional Green Power Device
0x0B	GP Proxy Table Request Allows to query the proxy table for a certain Green Power Device or read out the table in chunks

Cluster commands transmitted:

Command	Description
0x00	GP Notification Tunnels GP frames from a Green Power Device to one or more sinks or groups of sinks
0x04	GP Commissioning Notification Tunnels GP frames from a Green Power Device to a sink in commissioning mode
0x0B	GP Proxy Table Response Conveys a set of proxy table entries to a sink or management application

- [14] In application versions 1.00 and 1.09+. In application versions 1.01 up to and including 1.08 device ID 0x0507, "Physical Device", had been used.
- [15] Since application version 1.04.
- [16] Available in Zigbee stack version 1.60 and above. Legacy ZCP requirement – do not use in applications.
- [17] Available in Zigbee stack version 1.56 and above.
- [18] Available in Zigbee stack version 1.50 and above.
- [19] Available in Zigbee stack version 1.61 and above.
- [20] Only available on 2nd generation hardware
- [21] Since firmware version 2.2.0
- [22] Bidirectional communication is currently limited to the commissioning stage

7. Physical Dimension

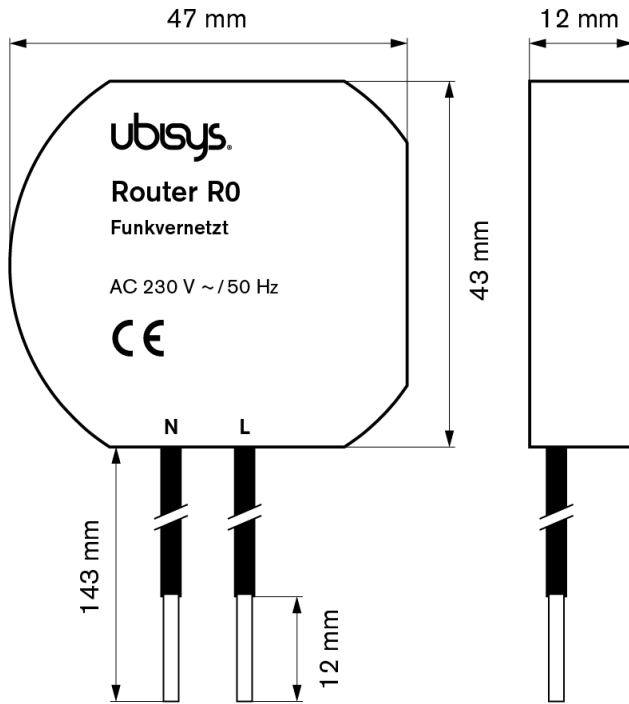


Figure 1. Flush-mount In-wall Zigbee Router R0 – Dimensions

8. Ordering Information

The following tables list the product variants available. Use the specified order code for your orders. Please contact ubisys support if you require any customization.

Brand	Order Code	Description
ubisys	1168	Zigbee Router R0 (in-wall, flush-mount)

The housing is flame retardant (V-0), Color: Black, RAL 9005.

9. General Terms & Conditions Of Business

When placing your order you agree to be bound by our General Terms & Conditions of Business, "Allgemeine Geschäftsbedingungen", which are available for download here:

www.ubisys.de/en/smarthome/terms.html

10. Declaration Of Conformity



We – ubisys technologies GmbH, Neumannstraße 10, 40235 Düsseldorf, Germany – declare under our sole responsibility that the ubisys Router R0 with order codes as detailed in [Chapter 8](#) under the trade name “ubisys” to which this declaration relates are in conformity with the following directives and standards:

Directive/Standard	Description/Scope
2014/53/EU	Radio Equipment Directive (RED)
2014/30/EU	Electromagnetic Compatibility Directive (EMC)
2014/35/EU	Low Voltage Directive (LVD)
2012/19/EU	Waste Electrical and Electronic Equipment Directive (WEEE)
2011/65/EU	Restriction of Hazardous Substances Directive (RoHS)
EN IEC 60669-2-1:2022+A11:2022	Switches for household and similar fixed electrical installations - Part 2-1: Particular requirements - Electronic control devices (IEC 60669-2-1:2021)
EN 50663:2017	Generic standard for assessment of low power electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (10 MHz - 300 GHz)
EN 62479:2010	Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)
EN IEC 61000-3-2:2019+A1:2021	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions (equipment input current ≤ 16 A per phase)
EN 61000-3-3:A2:2013+A1:2019+A2:2021	Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current ≤ 16 A per phase and not subject to conditional connection
ETSI EN 301 489-1 V2.2.3 (2019-11)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements; Harmonised Standard for ElectroMagnetic Compatibility
ETSI EN 301 489-17 V3.2.4 (2020-09)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for Broadband Data Transmission Systems; Harmonised Standard for ElectroMagnetic Compatibility
ETSI EN 300 328 V2.2.2 (2019-07)	Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz band; Harmonised Standard for access to radio spectrum
IEEE 802.15.4:2020	IEEE Standard 802 – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)
Zigbee 3.0	Zigbee 2017 with Green Power

Düsseldorf, Germany

October 29, 2025

Place of issue

Date of issue

Dr.-Ing. Arasch Honarbacht

Managing Director, Head of Research & Development

Full name of Authorized Signatory

Title of Authorized Signatory



Signature

Seal

11. Revision History

Revision	Date	Remarks
1.0	11/14/2014	Initial Public Version
1.1	11/17/2014	Added documentation about "ubisys2" QR-code format and note about issue with "ubisys1" check sum.
1.2	11/24/2014	Announced support for Zigbee 3.0 via OTA upgrade. Added information about joining and rejoining behavior to start-up section. Added information about APS duplicate rejection table size.
1.3	01/06/2015	Includes documentation of Zigbee Network Steering ("EZ-mode") in firmware revisions 1.01 and above.
1.4	01/19/2015	Added a note about removal of Identify server cluster in firmware revisions 1.01 and above.
1.5	08/12/2015	Improved network steering in firmware revision 1.02 (toggle permit joining) and shortcut to factory reset by 10-second extended press.
1.6	11/02/2015	Starting with firmware revision 1.03, when the device is factory reset, it will broadcast a network leave indication.
1.7	11/11/2015	Updated the ZDO description to include enhancements and additions made for Zigbee 2015 platform compliance
1.8	19/11/2015	Enhancements made in firmware revision 1.04 include added support for Zigbee Green Power and further changes to align with Zigbee 3.0 requirements.
1.9	09/13/2016	Updated to Zigbee 3.0 Certified Product in application firmware 1.05; added information about the power-cycle sequence factory reset in application firmware 1.06. Corrected description of element data type for switch configuration (should have been 0x41 instead of 0x48).
2.0	09/19/2019	Application firmware 1.09 uses range extender device type instead of physical device (0x0507)
2.1	09/16/2021	Update Declaration of Conformity
2.2	10/29/2025	Update Declaration of Conformity

12. Contact

ubisys technologies GmbH
Neumannstr. 10
40235 Düsseldorf
Germany

T: +49. 211. 54 21 55 - 19
F: +49. 211. 54 21 55 - 99

www.ubisys.de
info@ubisys.de