SIEMENS

N 148/23

IP Interface Secure

Application program description

Smart Infrastructure

2023-07-27

Supplementary information

Purpose of the application program description

The application program description contains detailed information on the parameters and communication objects of the ETS application program as well as a description of the functions that can be set via the different parameters.

Target audience of the application program description

The application program description is intended for people who want to commission the IP router or reconfigure it, who have a basic understanding of network technology and have successfully attended the following courses:

- KNX basics course
- IP fundamentals KNXnet/IP

Product documentation and support

Product documentation

Documents related the product, such as operating and installation instructions, application program description, product database, additional software and CE declarations can be downloaded from the following website:

http://www.siemens.com/gamma-td

Frequently asked questions

For frequently asked questions about the product and their solutions, see:

https://support.industry.siemens.com/cs/products?dtp=Faq&mfn=ps&lc=en-WW

Support

Contact details for additional questions relating to the product:

Tel.: +49 89 9221-8000

http://www.siemens.com/supportrequest

Contents

1 Information on IP-Router Secure and on the application program

Product family: System device
Product type: Coupler
Manufacturer: Siemens
Name: IP-Router Secure N 146/03
Order no.: 5WG1146-1AB03
Application: 091A CO IP Router Secure N 146/03 0040 03

System requirement:

- At least ETS 5.7.3

1.1 Cyber security disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html.

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under https://www.siemens.com/cert/en/cert-security-advisories.htm.

2 Function

2.1 Security functions of the IP router

The IP router supports the “**KNX IP Secure**” security standard and offers the following security functions, among others:

- Encrypted transfer of KNX telegrams between IP routers in the IP network
- Encrypted transfer of KNX telegrams between IP routers and PC software
- Secured access only from authenticated devices
- Secure commissioning via ETS

During secure commissioning via ETS, the device certificate printed onto the device (FDSK = Factory Default Setup Key) is imported and stored for this exact device in the ETS project.

ℹ For more information on KNX IP Secure, refer to the ETS software help or go to the following website: https://support.knx.org

ℹ Alternatively, insecure commissioning without KNX IP Secure is also possible. In this case, the device is insecure and responds like other KNX devices without IP Secure.

2.2 Functions of the IP router

The IP router is a rail-mounted device for installation in distributions. The device uses the KNXnet/IP standard and connects KNX lines to each other via data networks using the internet protocol (IP). At the same time, this device enables bus access from a PC or other data processing devices.

Connections and power supply

The connection to KNX is established using a bus connector terminal (black and red terminals). The connection to the data network (IP via 10 or 100BaseT (depending on the switch)) is established using an RJ45 socket.

The IP router also needs operating voltage in order to operate. The IP router can obtain this operation voltage via the network line using “Power over Ethernet” as per IEEE 802.3af. Alternatively, the operating voltage can be obtained via the second terminal block (white-yellow terminals) from an AC/DC 24 V safety extra low voltage supply or from a bus voltage supply (unchoked voltage, DC 29 V). As soon as the safety extra low voltage supply is connected to the second terminal block, operating voltage is drawn from it.

Remote access

Even if there is no direct network connection between a PC and an IP router, you can use a suitable network infrastructure for remote access to a KNX installation. Five simultaneous connections (remote accesses) are possible.

Setting up remote access [→ 22]

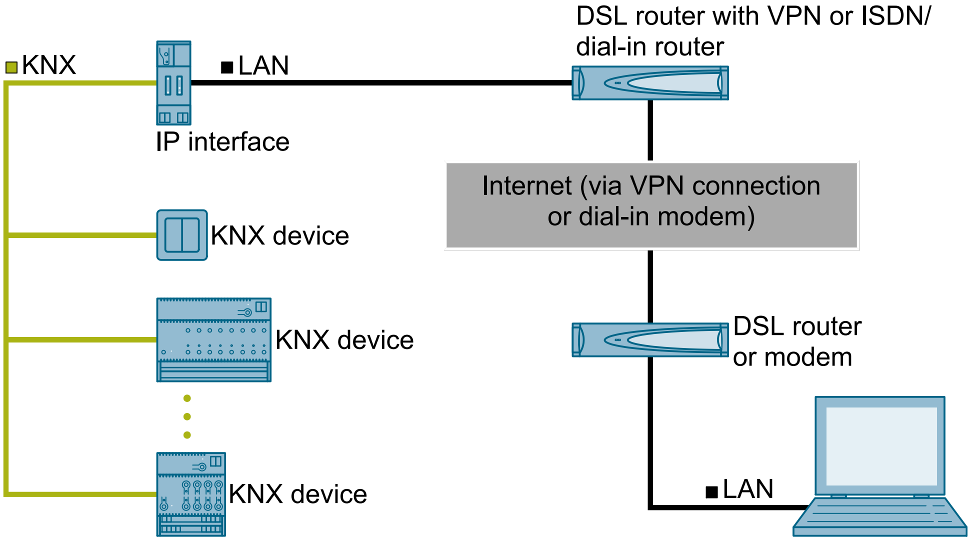


Fig. 1: Secure remote access

Additional functions

The IP router has the following attributes:

- Easy to connect to higher-level systems by using the internet protocol (IP)
- Secure access and data transfer via KNXnet/IP Secure
- Direct access to the KNX installation from every point in the IP network (KNXnet/IP tunneling)
- Fast communication between KNX lines, areas and systems (KNXnet/IP routing)
- Communication across buildings and properties (networking properties)
- Filtering and forwarding of telegrams according to
  - Physical address
  - Group address
- LED displays for
  - Operational readiness
  - KNX communication

  - IP communication
- Easy and secure configuration using ETS
- Easy to connect to visualization systems and facility management systems
- Slot for SD card (not in use)

2.3 Topology and routing functions

IP Router Secure can be used as an area or line coupler (KNXnet/IP routing).

In this context, two separate KNX bus lines within a data network are connected to each other data-wise. Galvanically, however, the KNX bus lines remain separated. This makes it possible to operate each bus line electrically independent from the other lines.

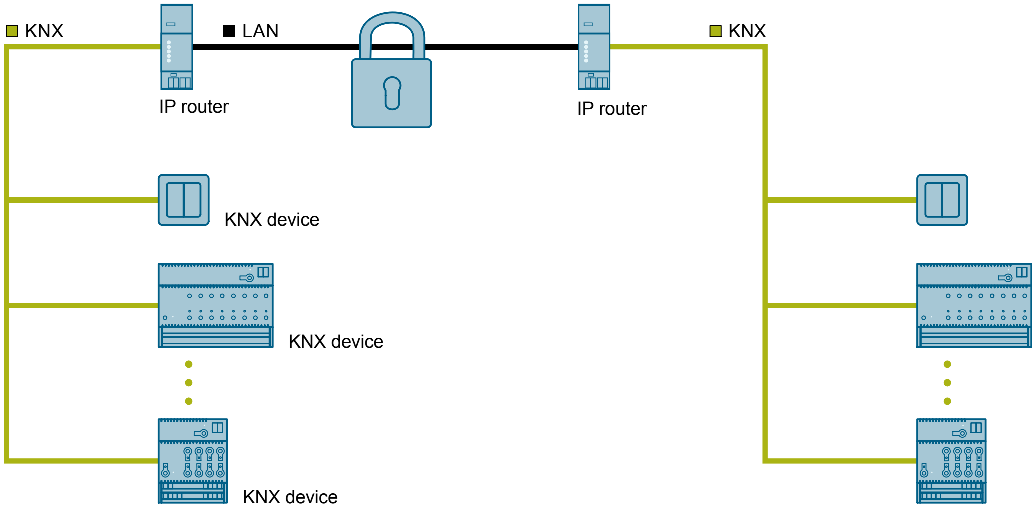


Fig. 2: Secure communication during operation

Functions when using the IP router as a line or area coupler

- Fast communication between KNX lines
- Option to extend an existing KNX system beyond the building by using LAN and WAN connections
- Direct forwarding of KNX data to every network user
- KNX remote configuration from every network access point
- Can be used in a new or an existing KNX network
- Reduces the bus load by means of filter tables, which determine which bus telegrams are forwarded to and from the bus line or blocked. The ETS software automatically generates the filter table when the device is configured and commissioned.
- When the physical address is assigned, ETS is used to automatically specify the coupler function (area coupler: main line 1 – 15; line coupler: line 1 – 15).

Requirements for use as a line coupler

- Network components must support IP multi-casting.
- Network/LAN routers must be set up in such a way that they forward IP multicast datagrams.
- The IP multicast address 224.0.23.12 has been reserved for KNXnet/IP routing.

When you assign the physical address, make sure that the IP router and line coupler in an installation receive topologically correct physical addresses.

To do this, see the following rules.

Notes on using the IP routers as a world (system) coupler (0.0.0)

When using the IP router as a world (system) coupler (0.0.0), secure communication is not possible.

When using the router as a world (system) coupler (0.0.0) and full extension of KNX lines incl. line amplifiers, it is no longer possible to reach all line segments due to the routing counter.

World (system) couplers communicate via routing. If this is not installed in the same network, a constantly open VPN tunnel that can transmit Multicast telegrams must be set up.

Rule for using the IP router as an area coupler

If an IP router is used as an area coupler with physical address x.0.0, no additional IP router may be topologically “underneath” this IP router, i.e. with a physical address x.y.0 (y=1...15).

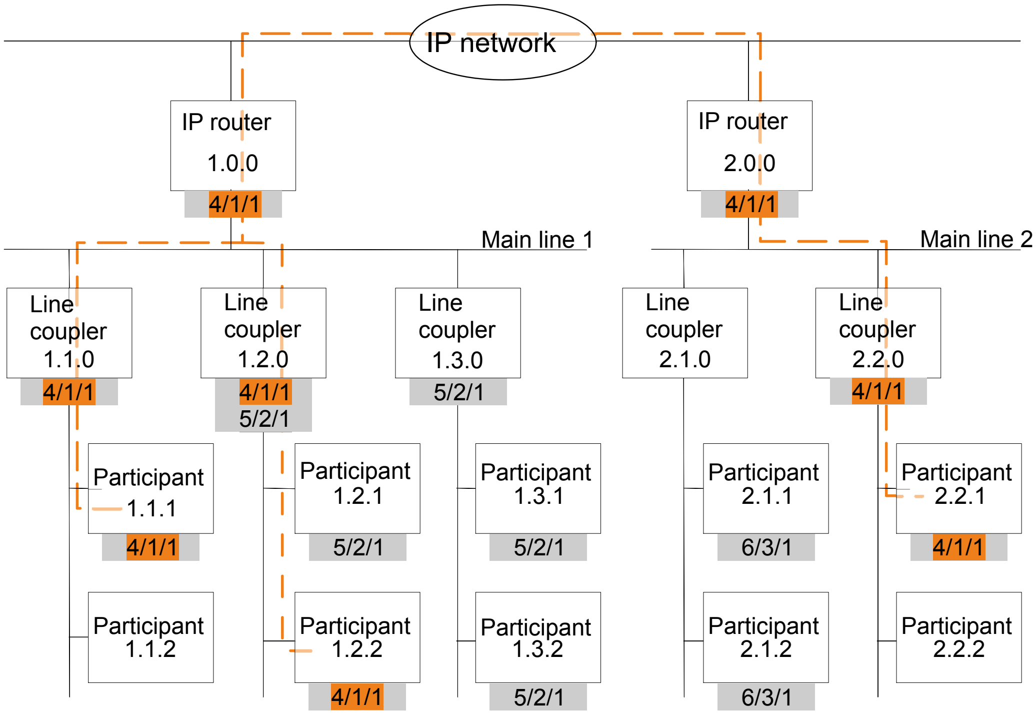


Fig. 3: IP-Router Secure as area coupler

x/x/x	Group address
x.x.x	Physical address (IP address)
– –	Path of a telegram from the sender to the recipients (example) Telegrams are only forwarded or received by devices with the same group address.

🟧 Example: Telegram is only forwarded or received by devices with group address 4/1/1.

Rule for using the IP router as a line coupler

If an IP router is used as a line coupler (e.g. 1.2.0), no IP router with corresponding area coupler address (e.g. 1.0.0) must be used “above” it in the system.

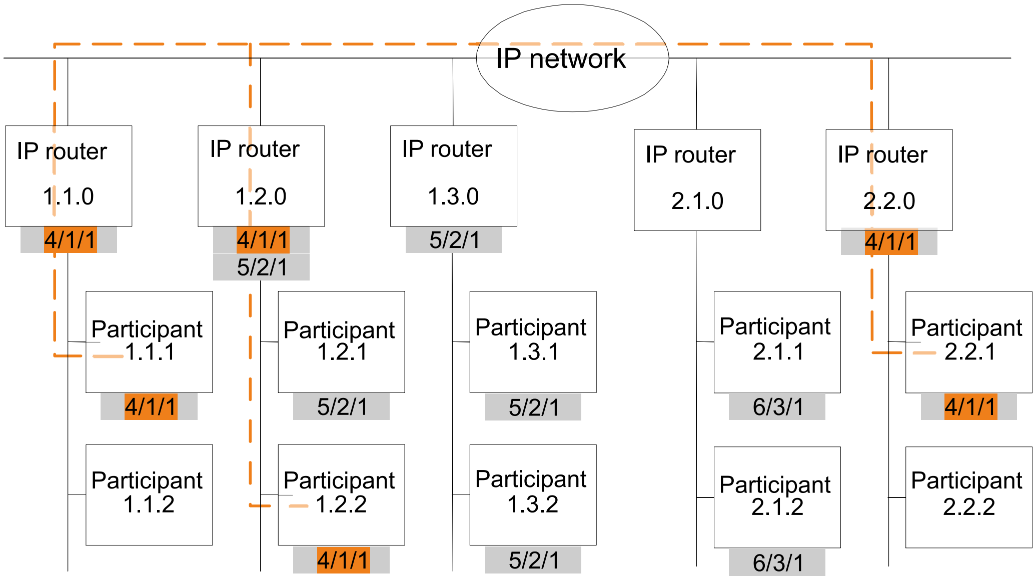


Fig. 4: IP-Router Secure as line coupler

x/x/x Group address

x.x.x Physical address (IP address)

— — Path of a telegram from the sender to the recipients (example)

Telegrams are only forwarded or received by devices with the same group address.

🟧 Example: Telegram is only forwarded or received by devices with group address 4/1/1.

Rule for using the IP router as an area and line coupler

The IP router can be used as an area or line coupler. The physical address has the structure x.y.0, with x=1…15 and y=1…15.

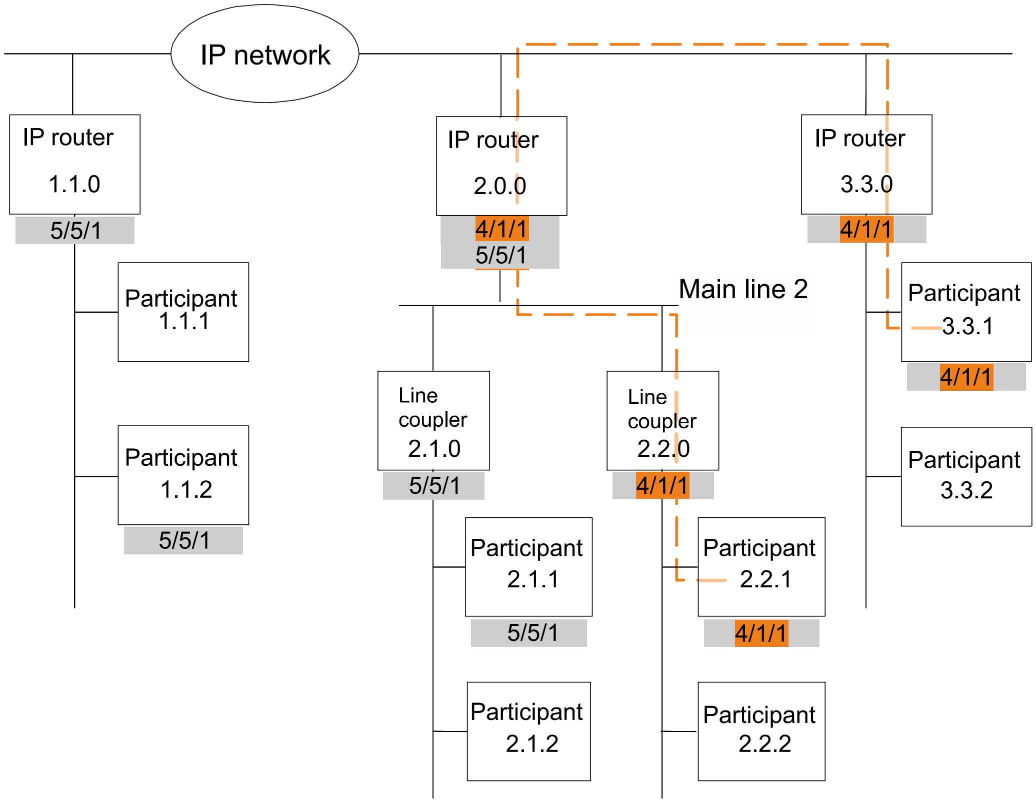


Fig. 5: IP-Router Secure as area and line coupler

x/x/x	Group address
x.x.x	Physical address (IP address)
— —	Path of a telegram from the sender to the recipients (example) Telegrams are only forwarded or received by devices with the same group address.
🟧	Example: Telegram is only forwarded or received by devices with group address 4/1/1.

2.4 Response on bus voltage failure and recovery

If the device detects a bus voltage failure on the bus line, this is stored as an error. In the same way, bus voltage recovery of the bus line is detected and the error is deleted internally. Depending on the configuration, both events are reported to KNXnet/IP.

3 Notes on secure data transfer

Instructions for secure operation of KNX IP Secure products

- Only operate the device in a protected network environment and do not allow direct access from the Internet.
- Additionally secure remote access to the device via a VPN connection.

  A virtual private network (VPN) establishes an encrypted and authorized connection (VPN tunnel) from a remote connection to a network via the internet. This VPN connection enables secure communication protected from eavesdropping between a remote device and the KNX installation.
- Only operate the device in secure mode. The device is in secure mode when the device has been commissioned via secure commissioning, secure tunneling is enabled and strong and different passwords are used.
- Set up a separate IP network with its own hardware for KNX communication.
- Use user IDs and strong passwords to restrict access to the (KNX) IP network.
- Restrict access to the (KNX)IP network to an authorized group of people using user IDs and strong passwords..
- Document network settings and give them to the building owner/operator or LAN administrator.
- Coordinate the administration of access rights to this KNXnet/IP device in an IP network with the respective IP network administrator.

Measures after replacing a device in the network

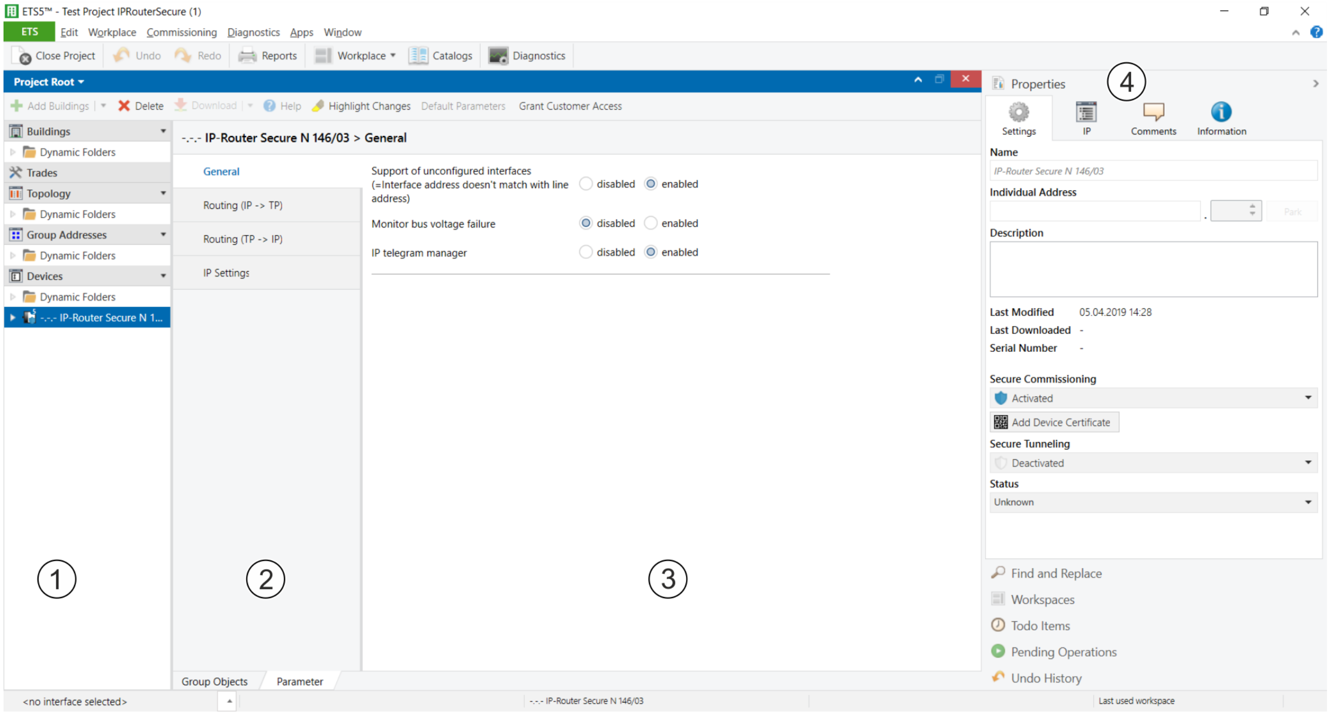
If an IP Router Secure or an IP Interface Secure in secure mode is stolen from a network or replaced due to a defect, secure commissioning has to be repeated for all other devices in the network. To do this, deactivate the“Secure commissioning“ option for each device in the settings of the project, activate the option again and load the data to the devices again. (There is no need to load the data into the device between deactivation and reactivation.)

Secure commissioning has to be repeated because it is not possible to exclude the possibility that the keys that are in the secure section of the device can be read. Recommissioning has the effect that new keys are generated and the old keys become worthless. The removed device no longer works in the network.

More information on KNX security

For more information on KNX security, including, for example, a security check, refer to the “KNX Secure” section on the KNX website (http://www.knx.org).

4 Structure of the setting options in ETS



-.-.- IP-Router Secure N 146/03 > General

Support of unconfigured interfaces (=Interface address doesn't match with line address) ○ disabled ● enabled

Monitor bus voltage failure ● disabled ○ enabled

IP telegram manager ○ disabled ● enabled

Name: IP-Router Secure N 146/03

Individual Address

Description

Last Modified 05.04.2019 14:28
Last Downloaded -
Serial Number -

Secure Commissioning: Activated

Secure Tunneling: Deactivated

Status: Unknown

Fig. 6: ETS overview

1 Tree view of the different sections (e.g. devices, topology and additional physical addresses)

2 Listing of parameter cards

3 Parameter area. In this area, parameters are set, enabled or disabled.

4 “Properties” section (e.g. configuration of IP and security, additional physical addresses)

Parameters that do not match the default settings can be highlighted in yellow by means of the ‘Highlight changes’ button.

5 Parameter

5.1 Parameters of the “general” parameter card

Support of unconfigured interfaces\r\n(=Interface address doesn't match with line address)

Parameter	Settings
Support of unconfigured interfaces\r\n(=Interface address doesn't match with line address)	disabled enabled

Function:

This parameter is used to set, e.g. whether interfaces with a topologically incorrect physical address are supported.

The following settings are possible:

- disabled:
  If this is set to ‘locked,’ interfaces that are not configured or configured incorrectly are not supported.
- enabled:
  If this is set to ‘enabled,’ interfaces can, for example, be used flexibly for setting parameters in several lines without the need to adapt the respective physical address.

Monitor bus voltage failure

Parameter	Settings
Monitor bus voltage failure	disabled enabled

Function:

This parameter is used to set whether voltage failure and voltage recovery of the bus line are reported via KNXnet/IP.

The following settings are possible:

- disabled:
  Information on bus voltage failure and bus voltage recovery is not forwarded.
- enabled:
  Information on bus voltage failure and bus voltage recovery is forwarded via KNXnet/IP.

IP telegram manager

Parameter	Settings
IP telegram manager	disabled enabled

Function:

This function is used to optimally use the telegram buffer between IP routers by Siemens and similar devices and thus avoids any loss of telegrams at high bus loads.

Note:

This function must be available and activated on all devices used. (On older Siemens devices, this function is active by default.)

For mixed operation with other devices that do not have this function, set this parameter to “disabled.”

The following settings are possible:

- disabled:
  The number of telegrams is not monitored. Telegrams can be lost.
- enabled:
  The telegram rate is limited. Only a certain number of telegrams are sent.

5.2 Parameters of the "Routing (IP > TP)" parameter card

Group telegrams of main group 0 to 13

Parameter	Settings
Group telegrams of main group 0 to 13	forward all block filter (normal)

Function:

This parameter determines the forwarding of telegrams with group addressing from KNXnet/IP to the line.

The following settings are possible:

- forward all:
  With this setting, all group-oriented telegrams are forwarded.
  This setting is used for testing purposes and must be reset to "filter (normal)" after successful testing. Otherwise there is an unnecessarily high bus load on all lines.
- block:
  With this setting, all group-oriented telegrams are blocked. This setting is used, e.g. for testing purposes during commissioning.
- filter (normal):
  With this setting, the entry in the filter table is checked before the decision is made as to whether the telegram is to be forwarded to the bus. The filter table automatically generated by ETS is loaded to the device.
  Note: The filter table must be loaded manually as soon as changes are made to cross-line group addresses.

Group telegrams of main group 14 to 31

Parameter	Settings
Group telegrams of main group 14 to 31	forward all block filter (normal)

Function:

This parameter determines the forwarding of telegrams with group addressing from KNXnet/IP to the line.

The following settings are possible:

- forward all:
  With this setting, all group-oriented telegrams are forwarded. This setting is used for testing purposes and must be reset to "filter (normal)" after successful testing. Otherwise there is an unnecessarily high bus load on all lines.
- block:
  With this setting, all group-oriented telegrams are blocked. This setting is used, e.g. for testing purposes during commissioning.
- filter (normal):
  With this setting, the entry in the filter table is checked before the decision is made as to whether the telegram is to be forwarded to the bus. The filter table automatic-

ally generated by ETS is loaded to the device.
Note: The filter table must be loaded manually as soon as changes are made to cross-line group addresses.

Individually addressed telegrams

Parameter	Settings
Individually addressed telegrams	block filter (normal)

Function:

This parameter is used to set the filter functions for the physically addressed telegrams.

The following settings are possible:

- block:
  With this setting, physically addressed telegrams are not forwarded.
  This setting must be used if KNX installations are commissioned in different KNX projects and the group-addressed telegrams are still supposed to be transferred (world/system coupler).
- filter (normal):
  With this setting, telegrams are filtered depending on the physical address of the IP router.
  Only telegrams whose target is in the next line are forwarded. All other telegrams are not forwarded.

Broadcast telegrams

Parameter	Settings
Broadcast telegrams	route block

Function:

This parameter is used to set the filter functions for the broadcast telegrams.

Irrespective of this setting, broadcast telegrams are always accepted by the IP router itself.

The following settings are possible:

- route:
  With this setting, telegrams are forwarded depending on the physical address of the IP router.
  Only telegrams whose target is in the next line are forwarded. All other telegrams are not forwarded.
- block:
  With this setting, broadcast telegrams are not forwarded.
  This setting must be used if KNX installations are commissioned in different KNX projects and the group-addressed telegrams are still supposed to be transferred (world/system coupler).

5.3 Parameters of the “Routing (TP > IP)” parameter card

Group telegrams of main groups 0 to 13

Parameter	Settings
Group telegrams of main groups 0 to 13	forward all block filter (normal)

Function:

This parameter determines the forwarding of telegrams with group addressing from the line to KNXnet/IP.

The following settings are possible:

- forward all:
  With this setting, all group-oriented telegrams are forwarded. This setting is used for testing purposes and must be reset to “filter (normal)” after successful testing. Otherwise there is an unnecessarily high bus load on all lines.
- block:
  With this setting, all group-oriented telegrams are blocked. This setting is used, e.g. for testing purposes during commissioning.
- filter (normal):
  With this setting, the entry in the filter table is checked before the decision is made as to whether the telegram is to be forwarded to the bus. The filter table automatically generated by ETS is loaded to the device.
  Note: The filter table must be loaded manually as soon as changes are made to cross-line group addresses.

Group telegrams of main group 14 to 31

Parameter	Settings
Group telegrams of main group 14 to 31	forward all block filter (normal)

Function:

This parameter determines the forwarding of telegrams with group addressing from the line to KNXnet/IP.

The following settings are possible:

- forward all:
  With this setting, all group-oriented telegrams are forwarded. This setting is used for testing purposes and must be reset to “filter (normal)” after successful testing. Otherwise there is an unnecessarily high bus load on all lines.
- block:
  With this setting, all group-oriented telegrams are blocked. This setting is used, e.g. for testing purposes during commissioning.
- filter (normal):
  With this setting, the entry in the filter table is checked before the decision is made as to whether the telegram is to be forwarded to the bus. The filter table automatically generated by ETS is loaded to the device.
  Note: The filter table must be loaded manually as soon as changes are made to cross-line group addresses.

Confirm group oriented telegrams

Parameter	Settings
Confirm group oriented telegrams	always only if routed

Function:

This parameter can be used to set when group telegrams are confirmed by the router.

The following settings are possible:

- always:
  Group telegrams are always confirmed by the router even if they are not forwarded to KNXnet/IP.
- only if routed:
  Group telegrams are only confirmed if they are forwarded to KNXnet/IP.

Individually addressed telegrams

Parameter	Settings
Individually addressed telegrams	block filter (normal)

Function:

This parameter is used to set the filter functions for the physically addressed telegrams.

The following settings are possible:

- block:
  With this setting, physically addressed telegrams are not forwarded.
  This setting must be used if KNX installations are commissioned in different KNX projects and the group-addressed telegrams are still supposed to be transferred (world/system coupler).
- filter (normal):
  With this setting, telegrams are filtered depending on the physical address of the IP router.
  Only telegrams whose target is in the next line are forwarded. All other telegrams are not forwarded.

Broadcast telegrams

Parameter	Settings
Broadcast telegrams	route block

Function:

This parameter is used to set the filter functions for broadcast telegrams.

Irrespective of this setting, broadcast telegrams are always accepted by the IP router itself.

The following settings are possible:

- route:
  With this setting, telegrams are forwarded depending on the physical address of the IP router.
  Only telegrams whose target is in the next line are forwarded. All other telegrams are not forwarded.
- block:
  With this setting, broadcast telegrams are not forwarded.
  This setting must be used if KNX installations are commissioned in different KNX projects and the group-addressed telegrams are still supposed to be transferred (world/system coupler).

5.4 Parameters of the “IP settings” parameter card

TTL (Time-to-Live) Unicast

Parameter	Settings
TTL (Time-to-Live) Unicast	0 ... 255

Function:

This parameter can be used to set the TTL value for the IP protocol. The default value is “128.” If the local network administrator specifies a different value, this value can be entered here.

The value specifies the number of intermediate stations (e.g. routers) which a data package may pass through between sender and receiver. If the value is set too low, data packages can get lost and are not received by the recipient.

6 Commissioning

6.1 Function in factory settings

The “KNXnet/IP routing” function is already active in the factory settings. If two IP routers are connected to each other via a LAN cable or several IP routers are connected via a hub/switch, bus telegrams are forwarded via the IP routers without further intervention.

In the factory settings, the configuration parameters are set as follows:

- Physical address of the IP router: Setting: “15.15.0” (= FF00 hex)
  - Specifying the name and physical address of the device [→ 20]
- Group telegrams: Respective settings: "filter (normal)”
  - Parameter: Group telegrams of the main groups 0 to 13 (IP – TP) [→ 15]
  - Parameter: Group telegrams of the main groups 0 to 13 (TP– IP) [→ 16]
  - Parameter: Group telegrams of the main groups 14 to 31 (IP – TP) [→ 15]
  - Parameter: Group telegrams of the main groups 14 to 31 (TP– IP) [→ 17]
- Confirmation of forwarded telegrams: Setting “only if routed”
  - Parameter: Confirm group telegrams (bus - IP) [→ 17]
- Support for unconfigured interfaces: Setting: "enabled”
  - Parameter: Support for unconfigured interfaces [→ 14]
- Filtering of physically addressed telegrams: Setting: "filter (depending on target and coupler address)”
  - Parameter: Physically addressed telegrams (IP– TP) [→ 16]
  - Parameter: Physically addressed telegrams (TP– IP) [→ 18]
- Forwarding “of broadcast telegrams: Setting: “route”
  - Parameter: Broadcast telegrams (IP– TP) [→ 16]
  - Parameter: Broadcast telegrams (TP– IP) [→ 18]
- Monitoring of the bus line on voltage failure: Setting: “disabled”
  - Parameter: Monitoring for bus voltage failure [→ 14]
- IP address assignment: Setting: “Obtain IP address automatically”
  - Assigning an IP address [→ 21]

6.2 Location of the device certificate QR code

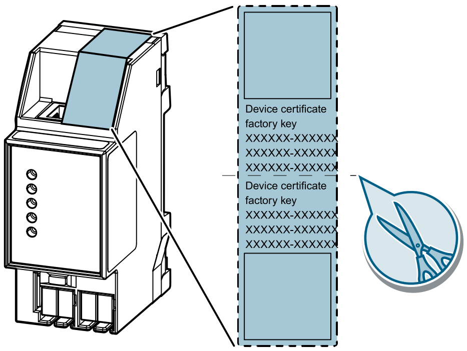


Fig. 7: Device certificate

The QR code of the device certificate is affixed to the device as a sticker. There is a duplicate QR code, which can be removed for easy commissioning.

6.3 Commissioning the device

Commissioning the device with “KNX IP Secure”

▷ A project is open in ETS.

1. Add the device to the project.
   ⇨ If the project is not yet password-protected, the ‘Set project password’ window appears.
2. Enter the password in the ‘New password’ and ‘Confirm password’ input fields, then click ‘OK’ to confirm.
   ⇨ The ‘Add device certificate’ window appears.
3. If you have a webcam, press the ‘...’ button and then scan the QR code sticker on the device.
4. If you do not have a webcam or are unable to read the QR code, enter the 6x6-character certificate key on the sticker on the device.
   ⇨ Once the certificate key has been entered correctly, a green checkmark appears at the end of the line. In addition, the serial numbers and the factory key of the device are displayed.
5. Compare the displayed serial number to the serial number on the device.
   ⇨ If the serial numbers do not match, the certificate key of a different device was entered and transfer of data will not work later on.
6. Press ‘OK’ to confirm the entries.
   ⇨ The device has been added to the project. The security functions of “KNX IP Secure” are activated automatically.

Commission device without “KNX IP Secure”

Commissioning without “KNX IP Secure”

Alternatively, the device can also be commissioned without KNX IP Secure. In this case, the device is insecure and responds like other KNX devices without the KNX IP Secure function.

To commission the device without KNX IP Secure, select the device in the ‘Topology’ or ‘Devices’ section and set the ‘Secure commissioning option’ to ‘Deactivated’ in the ‘Properties’ area of the ‘Settings’ tab.

6.4 Specifying the name and physical address of the device

A unique device name helps recognize and find the device in a KNXnet/IP visualization or within a project in ETS.

▷ The device has been added to the project.

1. Select the device in the ‘Topology’ or ‘Devices’ section.
2. In the ‘Properties’ section, switch to the ‘Settings’ tab.

3. In the ‘Name’ input field, enter a unique name of 30 characters maximum for the selected device.
4. In the ‘Physical address’ input field, enter the physical address of the device The address must be as yet unassigned.

   ⇨ The settings are saved automatically.

6.5 Assigning an IP address

> For details on the IP address and additional network settings, contact your local network administrator.

▷ The device has been added to the project.

1. Select the device in the ‘Topology’ or ‘Devices’ section.
2. In the ‘Properties’ section, switch to the ‘IP’ tab.
3. Make the desired IP address settings.

   ⇨ The settings are saved automatically in the ETS project.
4. Saving settings in the device. To do so, use the ETS software for full programming (menu item: “Program” > “Physical address & application program”).

The following settings are possible:

- **Obtain IP address automatically**
  If you select this option, the device is automatically assigned an IP address. This happens either via an DHCP service in the network or, if no DHCP service has been configured, via the device itself (AutoIP).
  The MAC address required for configuring the DHCP service can be read underneath this setting option or on a sticker on the device.
- **Use fixed IP address**
  When this option is selected, additional input fields are displayed in which the desired IP address for the device as well as a subnetwork screen and the standard gateway can be entered.

6.6 Setting up a multicast address

In the same way as for KNX (telegrams with group addresses), IP offers the option to send a message to several recipients at once. This form of IP communication is called “multicast” and the prerequisite for using it is that both sender and recipients are members of the same multicast group and the same multicast address as the target address. Messages are thus forwarded to all devices that use the same multicast address.

Multicast address 224.0.23.12 is reserved specifically for KNXnet/IP.

Multicast addresses 224.0.0.0 to 239.255.255.255 can be used for general access in a network. (For Byte 1 of the IP routing multicast address, only values between 224 and 239 are permissible because KNXnet/IP routing does not work with other values.)

1. In ETS, select the ‘Topology’ section.
2. In the ‘Properties’ section, switch to the ‘Settings’ tab.

3. Enter the desired multicast address in the ‘Multicast address’ input field.

   ⇨ The settings are saved automatically in the ETS project.

4. Saving settings in the device. To do so, use the ETS software for full programming (menu item: “Program” > “Physical address & application program”).

6.7 Setting up additional physical addresses

For stable device communication via KNXnet/IP tunneling, the device must use a separate physical address for each connection.

These additional addresses must not be identical to the physical address of the device and must not be used by any other bus device either.

When inserting the device into a project in ETS, additional physical addresses are automatically created for the device. These can be changed, if necessary.

> For additional information on assigning and changing physical addresses, refer to the ETS software help.

When the entire device is reset to factory settings, the physical addresses are reset: Resetting the device to factory settings [→ 25]

6.8 Setting up remote access

Even if there is no direct network connection between a PC and an IP router, you can use a suitable network infrastructure for remote access to a KNX installation. Five simultaneous connections (remote accesses) are possible.

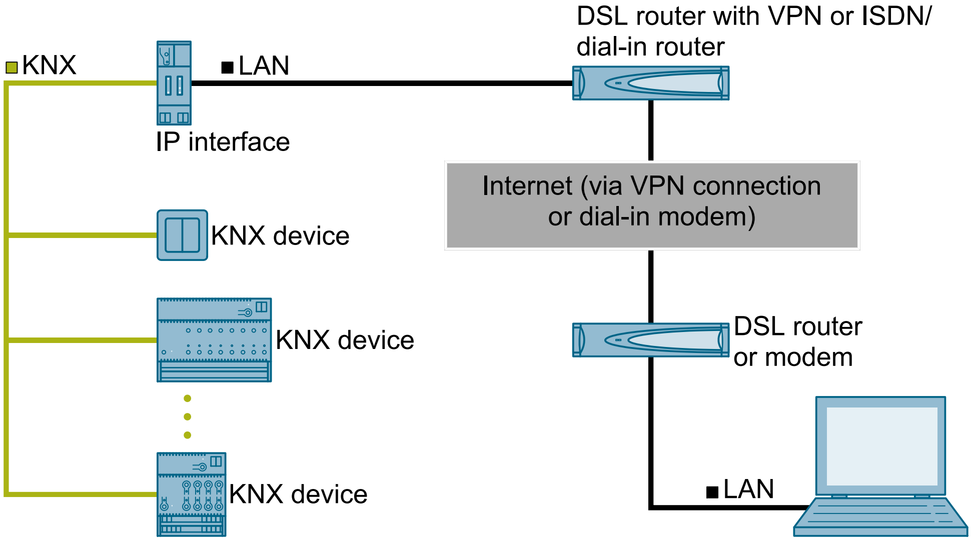

KNX
LAN
DSL router with VPN or ISDN/ dial-in router
IP interface
Internet (via VPN connection or dial-in modem)
KNX device
KNX device
DSL router or modem
KNX device
LAN

Fig. 8: Secure remote access

▷ The device must be reachable from outside of the own network.

◈ In the DSL router with VPN or in the ISDN/analogous dial-in router, create two separate protocol release (port extension tunnels) for the same port number for the UDP and TCP protocol.
The default port for KNX devices is port “3671.” The ports can be masked because the external port number differs from the internal port number.

7 Help in case of errors and problems

7.1 Frequently asked questions

Frequently asked questions

For frequently asked questions regarding the product and their solutions, see: https://support.industry.siemens.com/cs/ww/en/ps/faq

7.2 Possible errors

Description	Possible cause	Solution
When the device is commissioned, the following error message appears: “The physical address: x.y.z is being used by another device.”	Physical addresses have been used multiple times.	Check and/or reset physical addresses and re-assign. Setting up additional physical addresses [→ 22] Troubleshooting using ETS [→ 24]
When the device is commissioned, the following error message appears: “This is the certificate of another device.”	An incorrect device certificate was scanned or an incorrect certificate key entered.	Checking device certificates [→ 24]
Changes to the settings for the IP address were not copied to the device.	Only partial programming was performed.	Perform full programming of the device (physical address and application program) via the ETS software (menu item: ‘Program’ > ‘Physical address & application program’).
The settings for the Multicast address were not copied to the device.	Only partial programming was performed.	Perform full programming of the device (physical address and application program) via the ETS software (menu item: ‘Program’ > ‘Physical address & application program’).
KNX IP Secure routing is not possible.	The ETS detects dummy applications as non-secure.	Remove the dummy applications from the project.
The project cannot be opened.	The project password is unknown.	The project password cannot be reset. Create the project again, reset all devices to factory settings, and commission it again.

Description	Possible cause	Solution
A device cannot be added to the project.	A QR code for the device certificate is no longer available or cannot be assigned to a device. The 6X6-digit certificate key for the device certificate is unknown or can no longer be assigned to a device.	The device can no longer be commissioned and must be disposed of.

7.3 Troubleshooting using ETS

These are some of the troubleshooting options in ETS:

‘Diagnostics’ section

This section lets you check the physical address, group monitor, and bus monitor among other things.

‘Reports’ section

This area lets you export details on different areas of the project or print them directly.

ℹ For more information on ETS, see the online help of the ETS software.

7.4 Checking device certificates

1. Click the ‘ETS’ button in the menu bar.
2. Select the project from the list.
   - ⇨ Details on the project are shown on the right side.
3. Select the ‘Security’ tab page.
   - ⇨ A list of device certificates belonging to the project is displayed.

8 Resetting the device to factory settings

NOTICE	
!	**Loss of data due to resetting device!** When you reset the device, all parameters and settings entered are deleted. ● Ensure that the device is really supposed to be reset.

Resetting the device to factory settings

◈ Press the Learn button (at least 20 seconds) until the programming LED starts flashing quickly.

⇨ The programming LED flashes for 8 seconds.

⇨ The device has been reset to factory settings. All parameter settings have been deleted.

Index

Issued by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies