Use of the application program

Product family: Communication
Product type: Gateways
Manufacturer: IPAS GmbH

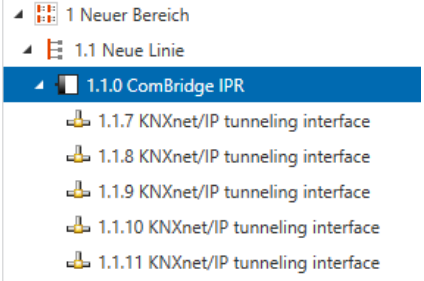
Name: 3622-NetInterface-01-0120
Order number: 3622-141-07-0B

Functions

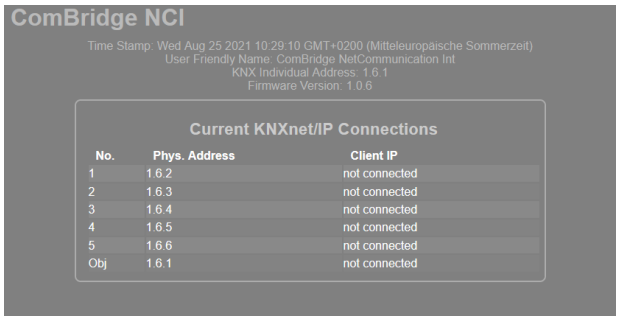
The ComBridge Net Communication Interface offers an easy and comfortable opportunity to parameter the KNX installation with ETS (KNXnet/IP tunnel protocol). There are up to 5 tunnel connections supported.
Client software products, such as ETS or visualizations, which are based on the KNXnet/IP tunnel protocol, can connect to the ComBridge NCI interface.

Using the tunnel connection

Use the IP network for a direct connection between a PC and the device.
Please remember that each tunnel connection has its own physical address which can be set with the ETS. This address must not yet exist in the KNX system.
In the ETS 5 and ETS application 1.2 all tunnel connections with the corresponding phy. Address displayed in the ETS and can be assigned easily:



Tip: Please see the website http://<ip> for an overview of already assigned addresses for the tunnels.

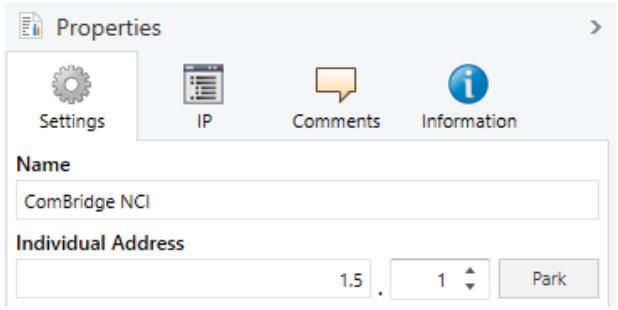


ETS configuration

The ETS configuration is used for principal device settings.

Device Name Setting

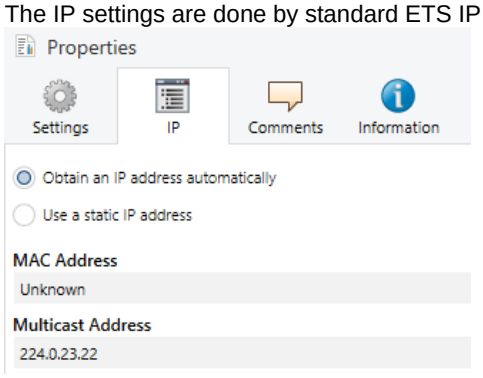
The device name, which is also displayed during the automatic search for KNXnet/IP devices, is also configured in the ETS properties:



Name	**ComBridge NCI**
The name of the device is set via this parameter so that it can be identified later on in the visualization.	

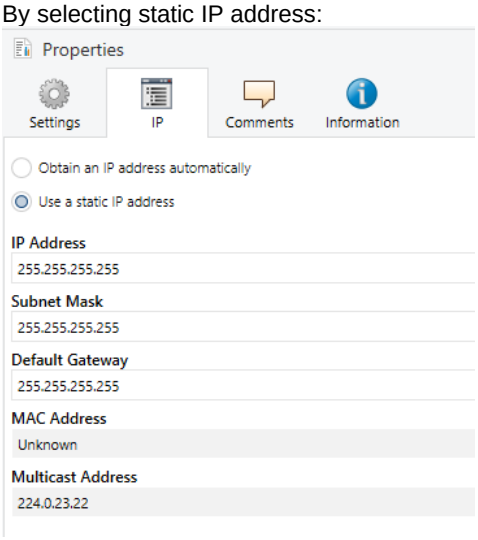
IP Settings

The IP settings are done by standard ETS IP panel:



IP address allocation	Use a static IP address **Obtain an IP Address automatically (DHCP)**
The ComBridge NCI can be allocated to either a fixed IP address or to a dynamic address which is assigned by a DHCP-Server.	

By selecting static IP address:



IP address	**255.255.255.255**
Here the standard IP address of the ComBridge NCI is pre-set. If a DHCP mode is set, this address is permanently overwritten by the addresses assigned by the DHCP-Server.	
Subnet Mask	**255.255.255.255**
Here the standard IP subnet mask of the ComBridge NCI is pre-set. If a DHCP mode is set, this mask is permanently overwritten by the address assigned by the DHCP-Server. If the device is configured without DHCP server (setting *fixed IP address*), the device needs to have the right subnet mask in order to work correctly.	
IP address Default Gateway	**255.255.255.255**
The role of the standard router is to send UDP telegrams which are addressed to a PC outside of the local network. If a DHCP mode is set, this address is always permanently overwritten by the DHCP server. If the DHCP server itself does not transmit any router address, it is assumed that no router is to be used. If the device is to be configured without a standard router, use the pre-set (invalid) address (**0.0.0.0**).	

A fixed IP address is recommended if a server is used as the visualization server, so that it can always be contacted.

Parameter

Enable Webserver	**no** yes
The ComBridge NCI Webserver is by default disabled. By using the parameter the Webserver can be activated.	
Enable Firmware Update Communication	**no** yes
This option has to be enabled to allow firmware update! Take care, due to security reasons, that this option is disabled again after firmware update has been executed.	

Disclaimer for Cyber Security

To protect systems, systems, machines and networks against online threats, it is necessary to implement a holistic, state-of-the-art security concept and to always keep it up to date.

You are responsible for preventing unauthorized access to your equipment, systems, machines and networks. These should only be connected to a network or the Internet if and as far as the connection is required and if adequate security precautions (eg firewalls or network segmentation) are available. In addition, the safety recommendations of IPAS GmbH must be observed. For more information, please contact your contact person at IPAS GmbH or visit our website.

IPAS GmbH strongly recommends that you use updates as soon as they become available, and always use the latest versions. Using versions that are no longer supported or using the latest updates may increase your risk of online threats. IPAS GmbH strongly recommends following safety recommendations on the latest security threats, patches and related measures.

