SIEMENS

Desigo V6.0

BACnet Router PXG3.M and PXG3.L
Engineering and configuration

Engineering

PDF help

Building Technologies

Edition notice

Technical specifications and availability subject to change without notice.

Edition: 2016-03-24

Document ID: A6V10429115_en--_a

Contents

1 Cyber security disclaimer

Products, solutions and services from Siemens include security functions to ensure the secure operation of building automation and control, fire safety, security management, and physical security systems. The security functions on these products, solutions and services are important components of a comprehensive security concept.

Drafting, implementing and managing a comprehensive and up-to-date security concept, customized to individual needs, is nevertheless necessary, and may result in additional plant- or site-specific preventive measures to ensure secure operation of your site regarding building automation and control, fire safety, security management, and physical security. These measures may include, for example, separating networks, physically protecting system components, user training, multi-level defensive measures, etc.For additional information on security as part of building technology and our product, solution and service offerings, please contact your Siemens sales representative or project department. We strongly recommend to always comply with our security advisories on the latest security threats, patches and other related measures.

http://www.siemens.com/cert/en/cert-security-advisories.htm

2   BACnet router PXG3.M/L

This document handles the following topics:

XWP Engineering

BACnet-Router used on the Desigo building automation and control network should be engineered as a rule in XWP (network configurator). This ensures a conflict-free network configuration.

Typical network configuration:
See: Engineering a router (XWP) [➜ 7]

Other typical uses of the BACnet router are displayed based on network topologies.
See: Network with NAT router (examples) [➜ 18]

As an engineering example we depict the connection of two building automation and control networks over a private IT-LAN or the Internet.
See: Engineer network with NAT router (example) [➜ 19]

Node setup and configuration

The created router configuration is loaded to the router using the SSA-DNT program. The SSA-DNT program is launched directly from XWP.
See: Configuring router (Node Setup) [➜ 13]

SSA-DNT program functions are described.
See: SSA-DNT program description [➜ 30]

Online

BACnet routers can be configured, operated, and monitored online. The local website on the router is used here. The web pages and their functions are described.
See: Changing a router configuration online [➜ 16]

Notes:

- The operating system language setting in Regional Settings determines the user interface language of SSA-DNT.
- The web page language can be set on each web page (top right).

3 Engineering a router (XWP)

The networks and the BACnet routers PXG3.M/L are engineered in Desigo XWP.

The following example illustrates how an BACnet/IP network is connected to a BACnet MS/TP network and/or a BACnet/LonTalk network.
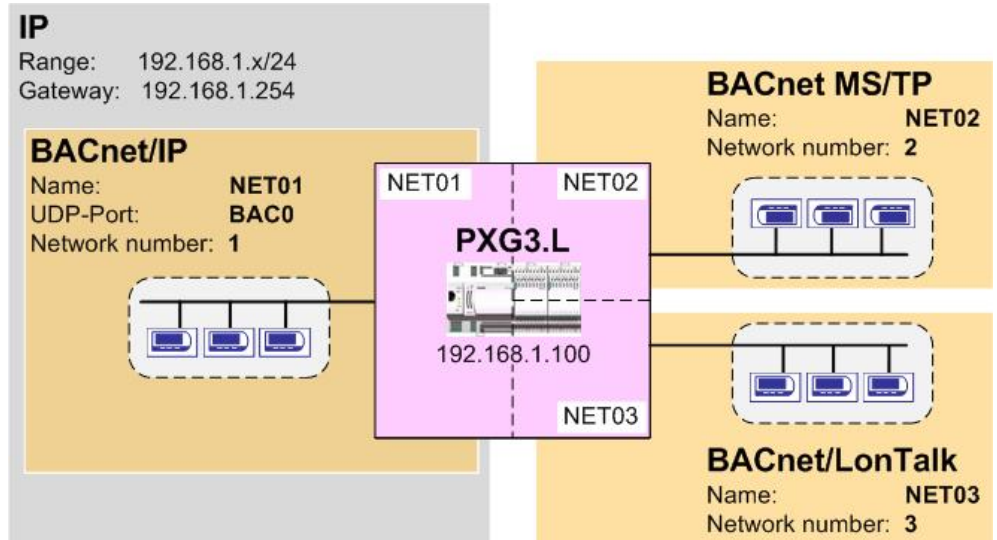
The following table illustrates the relevant settings of the example.

| Networks (specified by the network managers)			
LAN	IP network (private)	Name: Range: Gateway:	LAN 192.168.1.x/24 192.168.1.254
NET01	BACnet/IP network	Name: Network number: Subnet mask: Standard gateway:	NET01 1 255.255.255.0 192.168.1.254
NET02	BACnet MS/TP network	Name: Network number: Baud rate	NET02 2 76800
NET03	BACnet/LonTalk network	Name: Network number:	NET03 3

BACnet router PXG3.L		
Name	BNR01	
1.Port	LonTalk	
	Segment	SEG01 [LonTalk...]
	Node ID	100 (default)
	Subnet ID	1 (default)
2.Port	UDP/IP	
	Segment	SEG01 [UDP/IP...]
	IP address	192.168.1.100
	UDP port number	BAC0 [0xBAC0]
	Support BDT	True
	Support FDT	False

3.Port	MS/TP	
	Segment	SEG01 [MS/TP...]
	Address	0 (default)
	Max Master	Largest master-device address value. (default: 127)
Device number	XWP assigned an available device number. (default: 1)	
Password	Min. 6 characters	

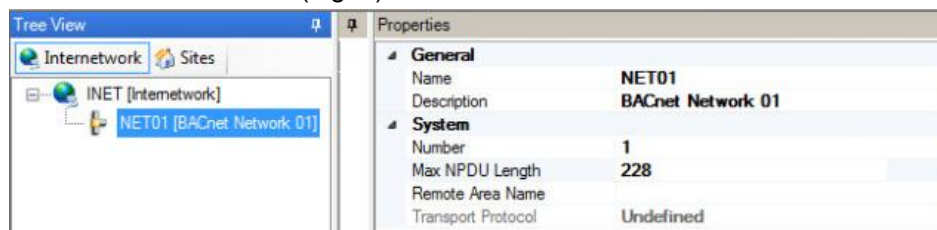## Creating the network topology in XWP

Three different BACnet networks are created in XWP:

- BACnet/IP
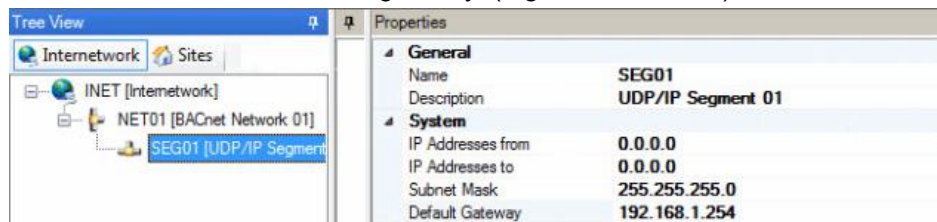
- BACnet MS/TP

- BACnet/LonTalk
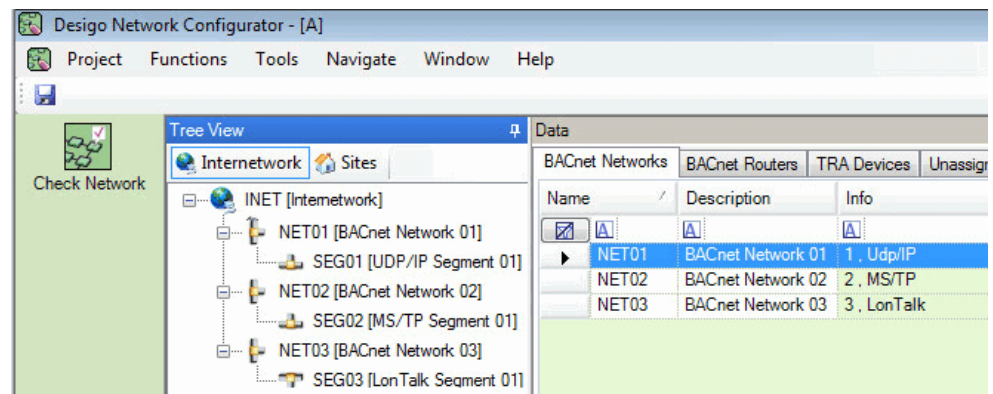
Add and configure BACnet/IP network

1. Add and rename new BACnet network.

2. Define network number. (e.g. 1)

3. Add and rename new UDP/IP segment.

   ⇨ **Max NPDU length** is set for UDP/IP: **1497**

4. Enter subnet mask and default gateway. (e.g. 192.168.1.254)

Add and configure BACnet MS/TP network

1. Add and rename new BACnet network.

2. Define network number. (e.g. 2)

3. Add and rename new MS/TP segment.
   ⇨ **Max NPDU length** is set for MS/TP: **501**

4. Define Baud rate. (e.g. 76800)

Add and configure BACnet/LonTalk network

1. Add and rename new BACnet network.

2. Define network number. (e.g. 3).

3. Add and rename new LonTalk segment.
   ⇨ **Max NPDU length** is set for LonTalk: **228**
   ⇨ The default value for LonTalk can be taken over.

Create router configuration in XWP

In XWP, create one BACnet router and connect it to the networks.

Create and configure the BACnet router

1. Add and rename new BACnet router PXG3.L. (e.g. BNR01)

2. Configure **1.Port** (LonTalk):

   – **Segment:** Select segment for BACnet/LonTalk network. (e.g. SEG03)
   – **Node-ID**: **100** (default)
   – **Subnet-ID**: **1** (default)

3. Configure **2.Port** (UDP/IP):

   The UDP/IP port is on the LAN side (e.g. 2.Port). The corresponding Ethernet connection on the device is: 1 ⛛ or ⛛ 2

   – **Segment:** Select segment for BACnet/IP network.
   – **IP-Address**: Enter the IP address for the BACnet router. (e.g. 192.168.1.100)
   – **UDP port number**: Enter the UDP port number for the BACnet/IP network. (e.g. BAC0)
     Notes: The UDP port number BAC0[47808] is entered as "0xBAC0".

– **Support BDT**: True (enabled).

4. Configure **3.Port** (MS/TP):

Properties	
▲ **System**	
Option Modules	**<None>**
▲ Ports	**(3)**
▷ 1. Port	**LonTalk**
▷ 2. Port	**Udp/IP**
▲ 3. Port	**MS/TP**
Segment	**SEG01 [MS/TP Segment 01] on NET02 [BACnet**
Address	**0**
Max Master	**127**
Max Info	**10**
Slave proxy	**False**
Auto slave discovery	False

– **Segment:** Select segment for MS/TP network.
  The Baud rate is inherited from MS/TP segment 01.
– **Address**: **0** (default)
– **Max.Master**: Largest master-device address value. (default: 127)

5. **Access password**: Enter router password. Min. 6 characters
   Note: Set up a different password for each project (no country-wide passwords).
   User strong passwords:
   - Use capital letters
   - User lowercase letters
   - Use numbers
   - Use special characters
   - At least 8 characters per password

The BACnet router configuration is not created.

Tree View	中
Internetwork	Sites

- INET [Internetwork]
  - BNR01 [PXG Router 01]
    - NET01 [BACnet Network 01]
      - SEG01 [UDP/IP Segment 01]
    - NET02 [BACnet Network 02]
      - SEG02 [MS/TP Segment 01]
    - NET03 [BACnet Network 03]
      - SEG03 [LonTalk Segment 01]

Properties

General	
Type	PXG3.L
Name	BNR01
Description	PXG Router 01
Panel	<None>
Author	<None>
Location	
System	
Option Modules	<None>
Ports	(3)
1. Port	LonTalk
Segment	SEG01 [LonTalk Segment 01]
Node ID	100
Subnet ID	1
Neuron ID	000000000000
2. Port	Udp/IP
Segment	SEG01 [UDP/IP Segment 01]
IP Address	192.168.1.100
Use DHCP	False
UDP Port Number	0xBAC0
Support BDT	True
Support FDT	False
Public NAT IP address	0.0.0.0
BDT	(1)
Ethernet Address	000000000000
Web port	
Host name	
DNS server 1	0.0.0.0
DNS server 2	0.0.0.0
Domain	
Allow HTTP connection	False
HTTP port number	80
HTTPS port number	443
3. Port	MS/TP
Segment	SEG01 [MS/TP Segment 01]
Address	0
Max Master	127
Max Info	10
Slave proxy	False
Auto slave discovery	False
SNMP	
Enabled	False
Read Community	
System Version	Desigo V5.1
Firmware version	
Serial number	
Device Name	BNR01
Device ID	0x02100801
Device ID Mode	Predefined
Device number	1
Access Password	
Device Instance Number	1050625
Max APDU Length	206
UTC time synchronization master	<Undefined>
GMT time zone	GMT+01:00 Berlin, Rome

| !	**NOTICE**
	Open ports leave open the possibility that communication can be interrupted or misused. Unauthorized access to customer plants can result in system faults or the loss of automation stations.
	Possible consequences: High costs for troubleshooting and poor reputation. 1. Open only those ports on a firewall (e.g. external switch) that are absolutely necessary for BAC systems. All other post must remain closed. 2. Only enable SNMP on the router if it is used.

4 Configuring router (Node Setup)

The router configuration created in XWP is loaded to the router using the SSA-DNT program.

Create network connection to router

▷ The router is operational and **unconfigured**.

▷ The commissioning laptop is connected to the router (via LAN or USB cable).
See: Connecting the cable to the IP device [➜ 37]

▷ A network connection (via USB or LAN) is configured.
See: Configuring a network connection [➜ 38]

▷ XWP is connected to the same physical segment (LON or IP) as the automation station.

1. Open the XWP project in **Network Configurator**.

2. Right-click the router in the Network Configurator. Select **Node Setup**.

⇨ The SSA DNT program starts. The task **Set up node** is active (left column).
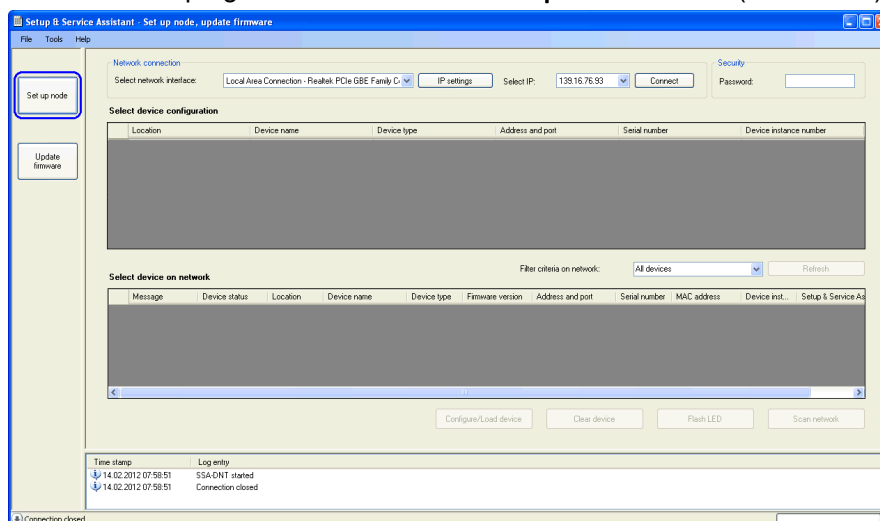

See also: SSA-DNT program description [➜ 30]

⇨ The password for the router configuration is automatically applied (top right). A background password query is carried out when accessing the device.

3. Configure the network connection:

– Select the configured network interface.
– Select the configured IP address.
– Click **Connect**.
⇨ The LAN or USB network connection is established (log entry).
The status of the network connection is displayed (lower left hand side of the pane).
⇨ For a USB network connection, the connected device is listed immediately in the **Select device on network** table and can be configured without additional identification.

4. Click **Network scan**.

   ⇨ The network is scanned (log entry).

⇨ The discovered devices (room automation stations, routers, etc.) are displayed. (**Select device on network** table).

⇨ Unconfigured devices are displayed with **Message** = Unconfigured and **device instance number** = 4194303.

⇨ **Note**: An active firewall may prevent access to the device. Either the corresponding firewall pane is displayed or no devices are found with **Network scan**. Not even the service pin triggers a reaction. Check with your network administrator for detailed procedures.

Configuring a router

1. Set the filter criteria for the network (e.g. PXG3.L). (**Select device on network** table).

2. Select the router.
   Identify the router in the following ways:

   – Press the service pin on the device.
     The device sends out an identification signal.
     Highlight the device of the last ID signal.

     OR
   – Select the router. Click **Flash**.
     The flash command is outputted to the highlighted device to identify it. An LED of the device flashes for about 10 seconds.

3. Select the device configuration for the router. (**Select device configuration** table).

4. Check to see if the identified router (highlighted) should be configured as per the selected device configuration (highlighted also).
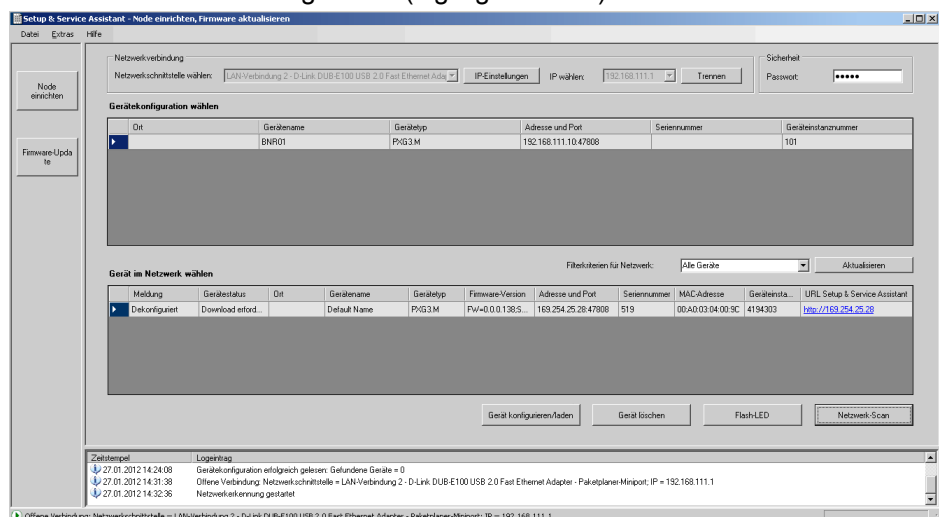
Note: You can only use **Configure/load device** if the following conditions are met:

   – The identified device is NOT configured. (Delete first any existing configuration, see below).
   – Device type and serial number of the identified device and the engineered device configuration match.

5. Click **Configure/load device**. Wait until configuration is complete.

    ⇨ Configuration is started (log entry).
    ⇨ The device is restarted.
    ⇨ The values in the tables are updated.
    ⇨ Successful configuration is displayed (log entry).
    ⇨ **Configure/load device** requires about 2 to 4 minutes (including device restart).

6. Check the router configuration online.
    See: Changing a router configuration online [➙ 16]

Notes:

●   Multiple devices can be configured in sequence using a LAN connection to the device. You do not need to wait each time for a complete configuration.

●   Conversely, in the event of a USB connection, connection to other routers on the network is interrupted if the directly connected router restarts.

●   An additional password prompt is displayed in the log window when the password is invalid (window top right).
    Note the following password rules: Minimum 6 characters, case-sensitive. The factory password is not accepted.

Deleting an existing configuration

1. Select a router. (**Select device on network** table).

2. Click **Delete device**.

    ⇨ Beginning and end of a procedure is displayed in the log window (takes about 1 to 2 minutes).
    ⇨ Table **Select device on network** is updated (**Device status** = unconfigured, **Device status** = Download required, **Device name** = Default Name, **Device instance number** = 4194303).

⇨ The router no longer is configured (factory setting).

Notes:

●   An additional password prompt is displayed in the log window when the password is invalid (window top right).

●   Multiple routers can be deleted in sequence using a LAN connection to the router. You do not need to wait for deletion to complete.

●   Conversely, in the event of a USB connection, connection to other routers on the network is interrupted if the directly connected router restarts.

See also

  ▤ Configuring router (Node Setup) [➙ 13]
  ▤ Defining proxy server settings [➙ 41]

5 Changing a router configuration online

Each router has a web server. Use SSA-DNT or a browser (e.g. Internet Explorer >V10) to access the homepage of the router (URL). The router configuration can be read and edited online.

Establishing a web connection to a router (web server)

▷ The router is configured. The device is connected.

▷ The SSA-DNT program was launched from XWP.

1. Click **Network scan** in SSA-DNT.

   ⇨ The discovered devices are displayed in the **Select device on network** table.

2. Click the link to the router. (**Select device on network** table; **URL Setup & Service Assistant** column).

   ⇨ The project password (window top right) is checked. If necessary, another password query is displayed.

   ⇨ The router overview page (homepage) opens.

3. Select a subpane in the left navigation pane.

   ⇨ The device and network settings are displayed.

4. Change the properties as required.

5. Select **Save and log out** in the upper navigation pane.

Notes:

● All entries are executed directly in the SSA and regularly saved every 30 minutes in non-volatile memory on the device. It is immediately saved with **Save and log out**. No data is saved on the commissioning laptop.

● The web page language can be set on each web page (top right).

Web connection using a browser

If you know the IP address of the device, you can enter the address in the browser or save it under Favorites. This opens the homepage without SSA DNT, but you must still enter the password.

	⚠ CAUTION
i	**Possible security issues** If the factory-set password is still set, enter a new password for the router by reconfiguring the router. See Configuring router (Node Setup) [➜ 13]

Check your proxy server settings for the browser if the status page does not open.
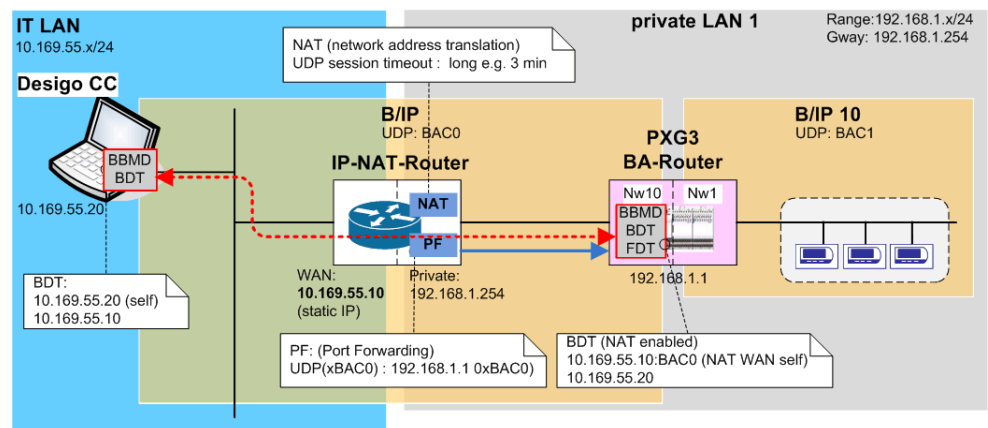See: Defining proxy server settings [➜ 41]

6 Network with NAT router (examples)

The following is a listing of various BACnet network configuration that integrate a management station (Desigo Insight or CC) over a router (NAT, BACnet).

Foreign device to single private LAN
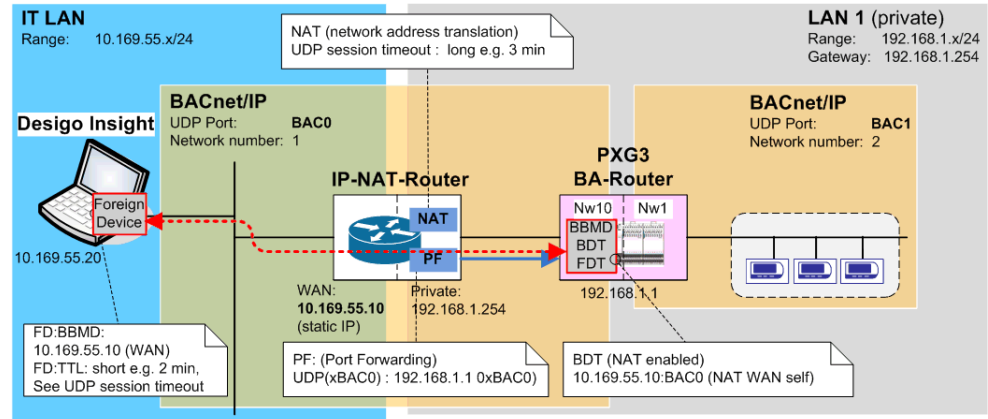
BACnet Broadcast Management Device to single private LAN

Simple IP-Router (NAT, PF)		BACnet/IP-Broadcast forwarding Port forwarding
BACnet-Router		BBMD with static BDT table
		BBMD with dyn. FDT table
BACnet Foreign Device		

BBMD	BACnet Broadcast Management Device	**BDT**	Broadcast Distribution Table
NAT	Network Address Translation	**FDT**	Foreign Device Table (BACnet)
PF	Port forwarding		

7 Engineer network with NAT router (example)

The following example illustrates how to connect two BACnet/IP networks over a private IT-LAN with NAT. NAT devices are used where the public IP address must be static, e.g. IP routers such as ADSL modems. We strongly recommend VPN tunneling with BACnet NAT for security reasons.
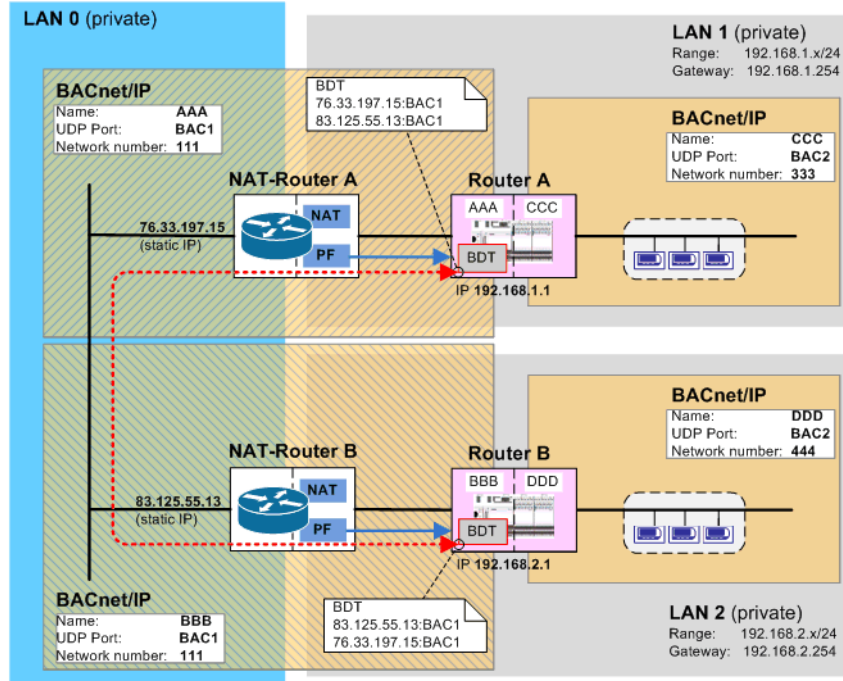
The two BACnet/IP networks **CCC** and **DDD** are connected to one another over the private IT-LAN (LAN0).

BACnet/IP networks **AAA** and **BBB** are used, which form a common network from a technical standpoint (restriction in XWP: The same UDP port **BAC1** and same network number **111**).

BACnet routers **BNR01** and **BNR02** set up the connection over the NAT devices **NAT-Router A** and **NAT-Router B**.

The following table illustrates the relevant settings of the example.

Networks (Network managers specify the information)			
LAN0	IP network (IT-LAN, private) or IP network (Internet, public)		
LAN1	IP network (private)	Range Gateway	192.168.**1**.x/24 192.168.**1**.254
LAN2	IP network (private)	Range Gateway	192.168.**2**.x/24 192.168.**2**.254
AAA	BACnet/IP network	UDP Network number	BAC**1** 111
BBB	BACnet/IP network	UDP Network number	BAC**1** 111
CCC	BACnet/IP network	UDP Network number	BAC**2** 333
DDD	BACnet/IP network	UDP Network number	BAC**2** 444

NAT-Router		
	NAT-Router A	NAT-Router B
Public IP address (static IP, provided by NAT router)	76.33.197.15	83.125.55.13
Port forwarding to BACnet router (must be configured on each NAT router)	UDP(xBAC1) 192.168.**1**.1	UDP(xBAC1) 192.168.**2**.1

Desigo XWP is used to configure the networks and BACnet routers. The following table provides the relevant settings as an overview (example):

BACnet router PXG3.L				
	BNR01		BNR02	
Port	2.Port (LAN0 side)	4.Port (LAN1 side)	2.Port (LAN0 side)	4.Port (LAN2 side)
Segment	SEG_AAA	SEG_CCC	SEG_AAA	SEG_DDD
IP address	192.168.**1**.1	192.168.**1**.1	192.168.**2**.1	192.168.**2**.1
UDP port number	BAC**1**	BAC**2**	BAC**1**	BAC**2**
Support BDT	True	True	True	True
Support FDT	...	...	...	...
NAT IP address (public)	76.33.197.15 (NAT router A)	---	83.125.55.13 (NAT router B)	---
BDT	76.33.197.15 (NAT router A) 83.125.55.13 (NAT router B)	192.168.**1**.1	83.125.55.13 (NAT router B) 76.33.197.15 (NAT router A)	192.168.**2**.1

The first UDP/IP port is on the LAN0 side (e.g. 2.Port). The corresponding Ethernet connection on the device is: 1 ⊞

The second UDP/IP port is on the LAN1/2 side (e.g. 4.Port). The corresponding Ethernet connection on the device is: ⊞2

Variant: The BACnet/IP network **CCC** or **DDD** can be defined as MS/TP network or LonTalk network.

| !	*NOTICE*
	Open ports leave open the possibility that communication can be interrupted or misused. Unauthorized access to customer plants can result in system faults or the loss of automation stations.
	Possible consequences: High costs for troubleshooting and poor reputation. 1. Open only those ports on a firewall (e.g. external switch) that are absolutely necessary for BAC systems. All other post must remain closed. 2. Only enable SNMP on the router if it is used.

## Creating the network topology in XWP

Four BACnet/IP networks are created in XWP: **AAA**, **BBB**, **CCC**, **DDD**
One UDP/IP segment is created on each BACnet/IP network.
Important: The two BACnet/IP networks **AAA** and **BBB** form a common network from a technical viewpoint and must have the same network number.
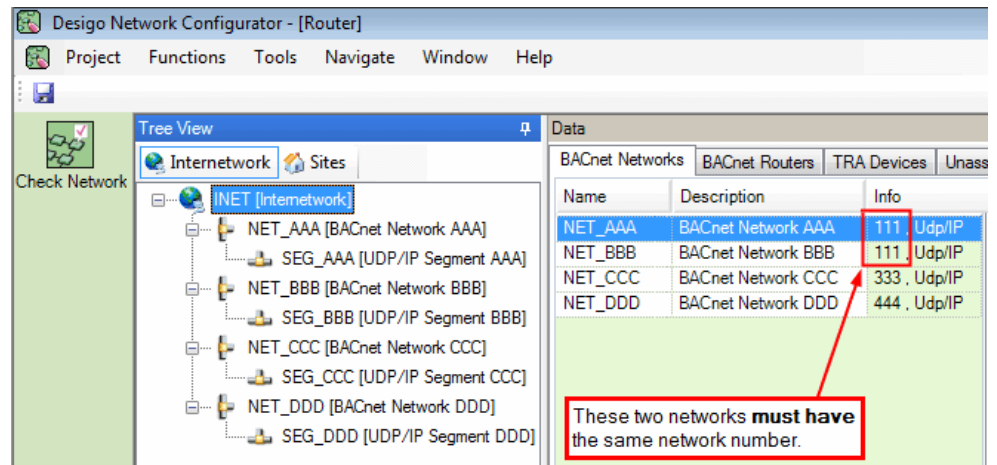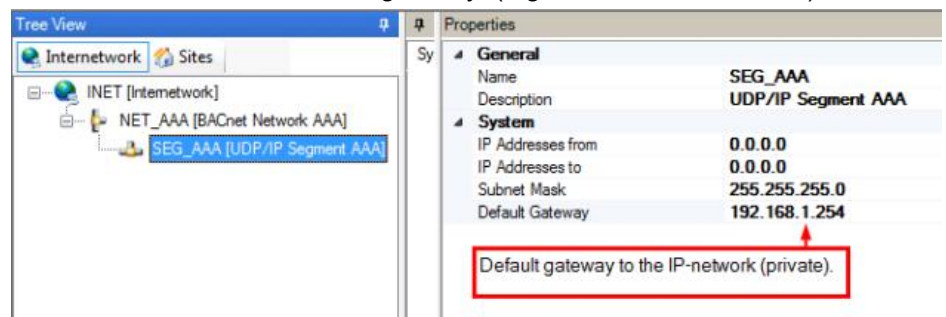

Add and configure BACnet/IP network (AAA: LAN0 side)

1. Add and rename new BACnet network. (e.g. AAA)
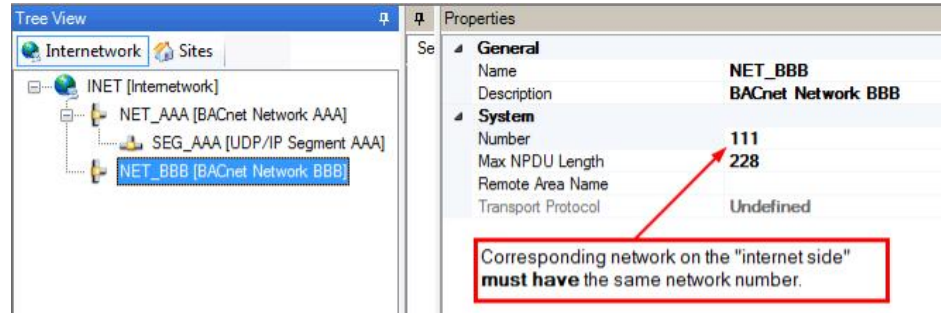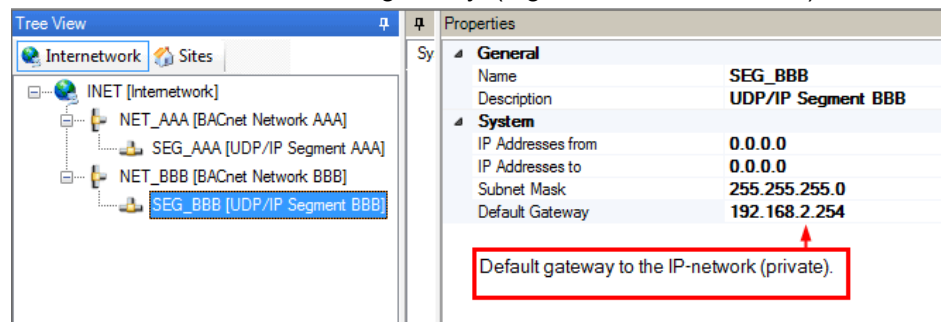
2. Define network number. (e.g. 111)
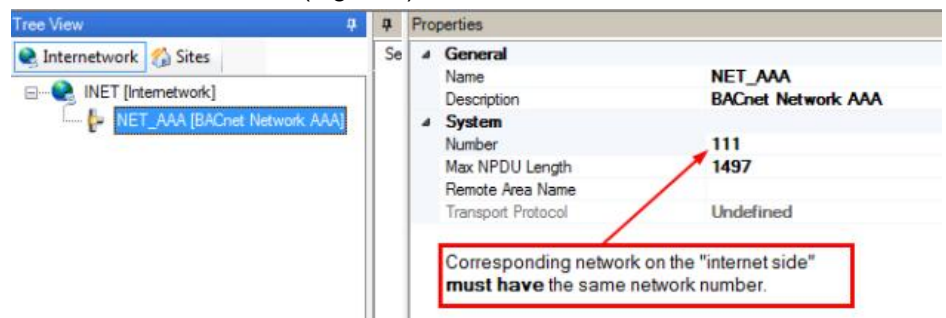
3. Add and rename new UDP/IP segment. (e.g. SEG_AAA)

4. Enter subnet mask and default gateway. (e.g. **LAN1**: 192.168.**1**.254)

Add and configure BACnet/IP network (BBB: LAN0 side)

1. Add and rename new BACnet network. (e.g. BBB)

2. Define network number. Important: Same network number as network AAA.
   (e.g. 111).
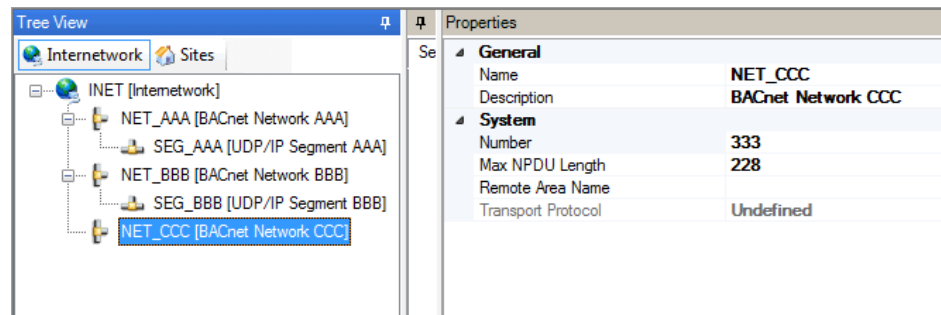
3. Add and rename new UDP/IP segment. (e.g. SEG_BBB)

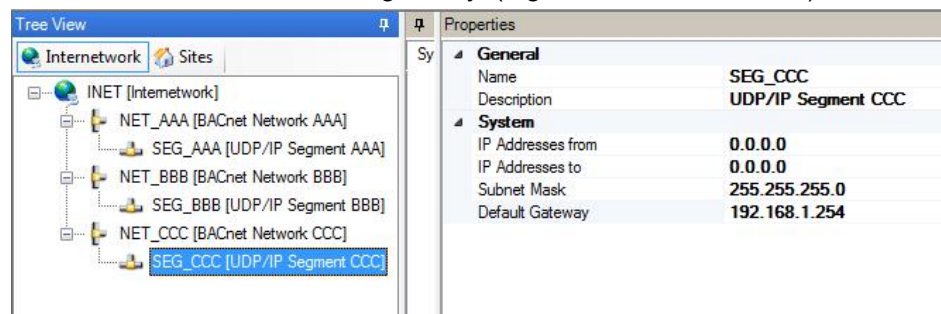4. Enter subnet mask and default gateway. (e.g. **LAN2**: 192.168.**2**.254)

Add and configure BACnet/IP network (CCC: LAN1 side)

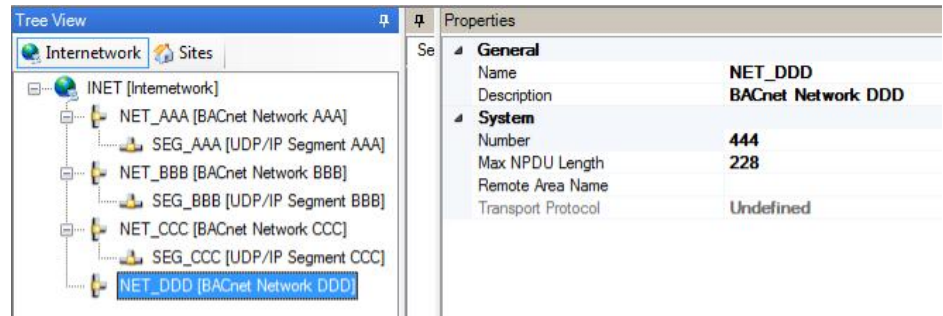1. Add and rename new BACnet network. (e.g. CCC)

2. Define network number. (e.g. 333).

3. Add and rename new UDP/IP segment. (e.g. SEG_CCC)

4. Enter subnet mask and default gateway. (e.g. **LAN1**: 192.168.**1**.254)

Add and configure BACnet/IP network (DDD: LAN2 side)

1. Add and rename new BACnet network. (e.g. DDD)

2. Define network number. (e.g. 444).

3. Add and rename new UDP/IP segment. (e.g. SEG_DDD)

4. Enter subnet mask and default gateway. (e.g. **LAN2**: 192.168.**2**.254)
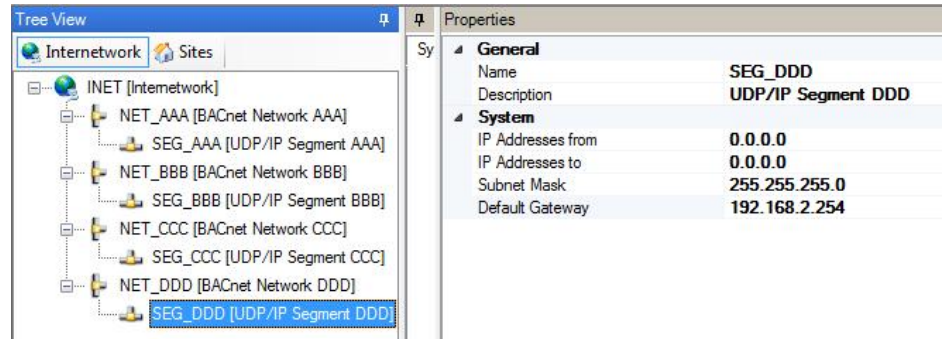
Create router configuration in XWP

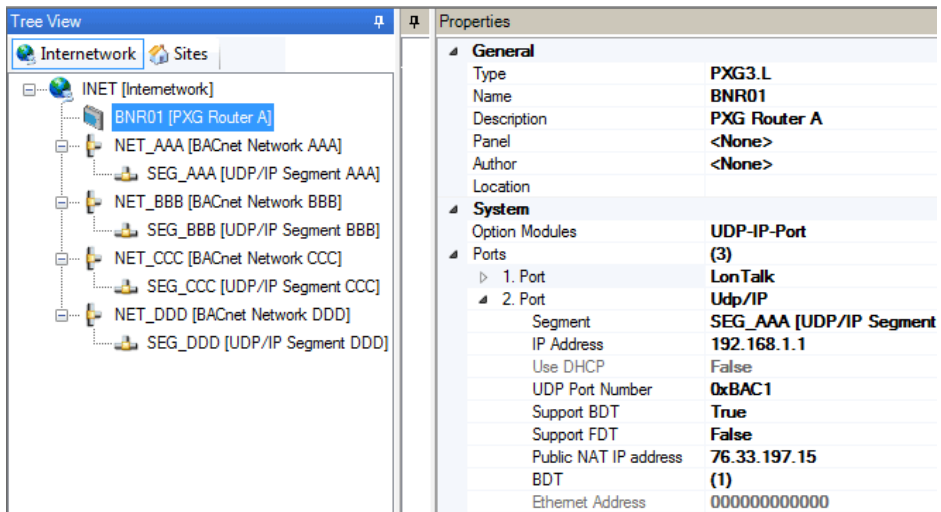In XWP, two BACnet routers, **BNR01** and **BNR02** are created and connected to the networks.

Important: Each BACnet router requires an additional UDP/IP port.

The first UDP/IP port defines the LAN0-side interface (e.g. 2.Port). Ethernet device connection: 1 🖧

The second UDP/IP port defines the LAN1/2-side interface (e.g. 4.Port). Ethernet device connection: 🖧 2

Create and configure the first BACnet router

1. Add and rename new BACnet router. (e.g. BNR01)

2. Configure **2.Port** (UDP/IP port on the LAN0 side):

   – **Segment:** Select segment for network **AAA** (LAN0 side). (e.g. SEG_AAA)
   – **IP address**: Enter the IP address for the BACnet router **BNR01**. (e.g. 192.168.**1**.1)
   – **UDP port number**: Enter common UDP port number of the networks **AAA** and **BBB** (LAN0 side). (e.g. BAC1)
      Notes: The UDP port numbers for **2.Port** (LAN0 side) and **4.Port** (LAN1 side) must be different. The port number BAC1[47809] is entered as "0xBAC1".
   – **Support BDT**: True (enabled).
   – **Public NAT IP address**: Public address of router **NAT-Router A**. (e.g. 76.33.197.15)
   – Set up additional BDT entry for **NAT router B**:

      Click **BDT** ⋯ in the entry field. BACnet router **BNR01** is already entered.
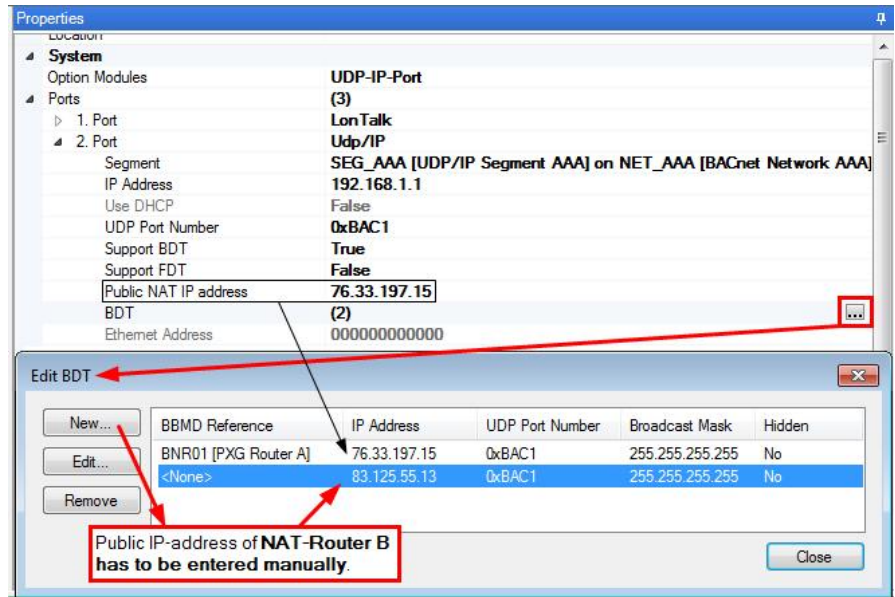
Create new entry for **NAT router B** with the public address and UDP port number. (e.g. 83.125.55.13 and 0xBAC1)

3. Set up addition BACnet UDP/IP port.

    –   Click **Option module** ... in the entry field.

    –   Select **UDP-IP port**. **Add**.

    ⇨   The additional port **4.Port** is set up.
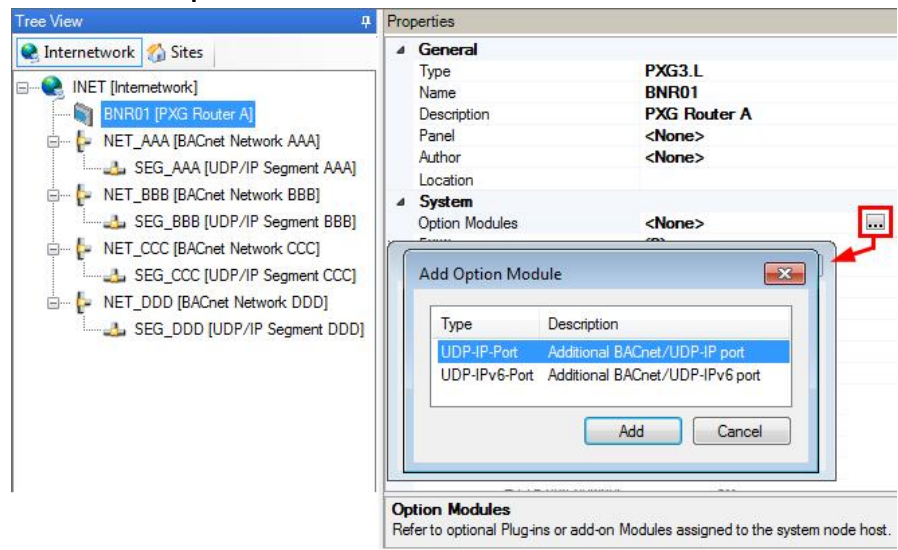
4. Configure 4.Port:

    –   **Segment:** Select segment for network **CCC** (LAN1 side). (e.g. SEG_CCC)
    –   **IP address**: Enter the IP address for the BACnet router **BNR01**. Same address as in **2.Port**. (e.g. 192.168.**1**.1)
        Note: The only way to correct an incorrect address entry after the fact is to delete the router and create is again.
    –   **UDP port number**: Enter the UDP port number for network **CCC** (LAN1 side). (e.g. 0xBAC2)
        Notes: The UDP port numbers for **2.Port** (LAN0 side) and **4.Port** (LAN1 side) must be different.
    –   **Support BDT**: True (enabled).

– **BDT**: No entry required. The BACnet router IP address **BNR01** is already entered.
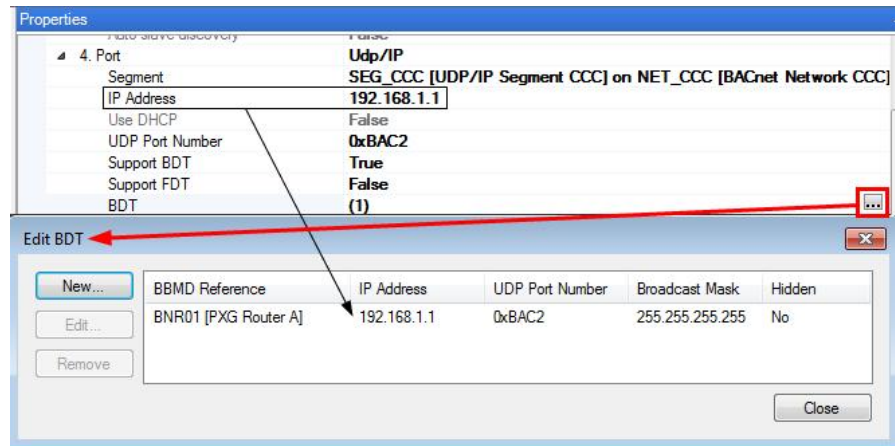
5. **Access password**: Enter router password. Min. 6 characters

⇨ The **BNR01** configuration is created.

Tree View

- INET [Internetwork]
  - BNR01 [PXG Router A]
    - NET_AAA [BACnet Network AAA]
      - SEG_AAA [UDP/IP Segment AAA]
    - NET_BBB [BACnet Network BBB]
      - SEG_BBB [UDP/IP Segment BBB]
    - NET_CCC [BACnet Network CCC]
      - SEG_CCC [UDP/IP Segment CCC]
    - NET_DDD [BACnet Network DDD]
      - SEG_DDD [UDP/IP Segment DDD]

Internetwork | Sites

Properties

| Property	Value
General	
Type	PXG3.L
Name	BNR01
Description	PXG Router A
Panel	<None>
Author	<None>
Location	
System	
Option Modules	UDP-IP-Port
Ports	(4)
1. Port	LonTalk
2. Port	Udp/IP
Segment	SEG_AAA [UDP/IP Segr
IP Address	192.168.1.1
Use DHCP	False
UDP Port Number	0xBAC1
Support BDT	True
Support FDT	False
Public NAT IP address	76.33.197.15
BDT	(2)
Ethernet Address	000000000000
Web port	
Host name	
DNS server 1	0.0.0.0
DNS server 2	0.0.0.0
Domain	
Allow HTTP connection	False
HTTP port number	80
HTTPS port number	443
3. Port	MS/TP
4. Port	Udp/IP
Segment	SEG_CCC [UDP/IP Segr
IP Address	192.168.1.1
Use DHCP	False
UDP Port Number	0xBAC2
Support BDT	True
Support FDT	False
BDT	(1)
Ethernet Address	000000000000
SNMP	
Enabled	False
Read Community	
System Version	Desigo V6.0
Firmware version	
Serial number	
Device Name	BNR01
Device ID	0x02100801
Device ID Mode	Predefined
Device number	1
Access Password	
Device Instance Number	1050625
Max APDU Length	1476
UTC time synchronization master	<Undefined>
GMT time zone	GMT+01:00 Berlin, Rom

Create and configure second BACnet router

Configure in the same way as for BACnet router **BNR01**.

1. Add and rename new BACnet router. (e.g. BNR02)

2. Configure **2.Port** (UDP/IP port on the LAN0 side):

   – **Segment:** Select segment for network **BBB** (LAN0 side). (e.g. SEG_BBB)
   – **IP address**: Enter the IP address for the BACnet router **BNR02**. (e.g. 192.168.**2**.1)
   – **UDP port number**: Enter common UDP port number of the networks **AAA** and **BBB** (LAN0 side). (e.g. BAC1)
   Notes: The UDP port numbers for **2.Port** (LAN0 side) and **4.Port** (LAN2 side) must be different.
   – **Support BDT**: True (enabled).
   – **Public NAT IP address**: Public address of router **NAT router B**. (e.g. 83.125.55.13)
   – Set up additional BDT entry for **NAT router A**:

   Click **BDT** [...] in the entry field. BACnet router **BNR02** is already entered.
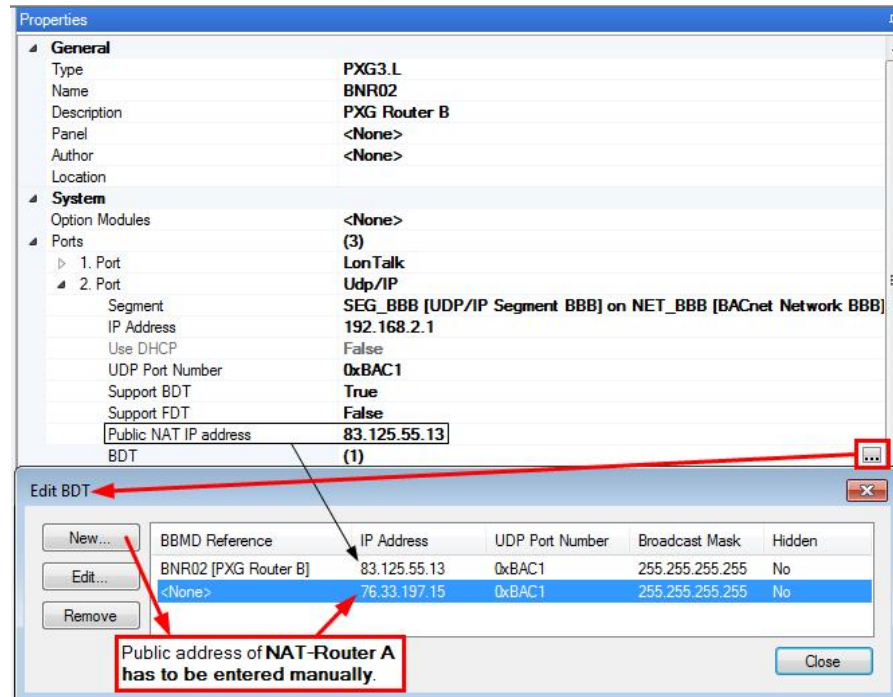
   Create new entry for **NAT router A** with the public address and UDP port number. (e.g. 76.33.197.15 and 0xBAC1)

3. Set up addition BACnet UDP/IP port.

   – Click **Option module** [...] in the entry field.
   – Select **UDP-IP port**. Add.
   ⇨ The additional port **4.Port** is set up.

4. Configure **4.Port**:

   – **Segment:** Select segment for network **DDD** (LAN2 side). (e.g. SEG_DDD)
   – **IP address**: Enter the IP address for the BACnet router **BNR02**. Same address as in **2.Port**. (e.g. 192.168.**2**.1).
   Note: The only way to correct an incorrect address entry after the fact is to delete the router and create is again.

- **UDP port number**: Enter the UDP port number for network **DDD** (LAN2 side). (e.g. 0xBAC2)
Notes: The UDP port numbers for **2.Port** (LAN0 side) and **4.Port** (LAN2 side) must be different.
- **Support BDT**: True (enabled).
- **BDT**: The BACnet router IP address **BNR02** is already entered.

5. Run a network check.

⇨ The following error message can be ignored since a double use was set up no purpose:
"Network 'AAA [BACnet network AAA (LAN0) -> Property 'Network number' is already used by another network."
"Network 'BBB [BACnet network BBB (LAN0) -> Property 'Network number' is already used by another network."

⇨ The **BNR02** configuration is created.

Tree View	Properties	
Internetwork Sites	General	
INET [Internetwork]	Type	PXG3.L
BNR01 [PXG Router A]	Name	BNR02
BNR02 [PXG Router B]	Description	PXG Router B
NET_AAA [BACnet Network AAA]	Panel	<None>
SEG_AAA [UDP/IP Segment AAA]	Author	<None>
NET_BBB [BACnet Network BBB]	Location	
SEG_BBB [UDP/IP Segment BBB]	System	
NET_CCC [BACnet Network CCC]	Option Modules	UDP-IP-Port
SEG_CCC [UDP/IP Segment CCC]	Ports	(4)
NET_DDD [BACnet Network DDD]	1. Port	LonTalk
SEG_DDD [UDP/IP Segment DDD]	2. Port	Udp/IP
	Segment	SEG_BBB [UDP/IP Segr
	IP Address	192.168.2.1
	Use DHCP	False
	UDP Port Number	0xBAC1
	Support BDT	True
	Support FDT	False
	Public NAT IP address	83.125.55.13
	BDT	(2)
	Ethernet Address	000000000000
	Web port	
	Host name	
	DNS server 1	0.0.0.0
	DNS server 2	0.0.0.0
	Domain	
	Allow HTTP connection	False
	HTTP port number	80
	HTTPS port number	443
	3. Port	MS/TP
	4. Port	Udp/IP
	Segment	SEG_DDD [UDP/IP Segr
	IP Address	192.168.2.1
	Use DHCP	False
	UDP Port Number	0xBAC2
	Support BDT	True
	Support FDT	False
	BDT	(1)
	Ethernet Address	000000000000
	SNMP	
	Enabled	False
	Read Community	
	System Version	Desigo V6.0
	Firmware version	
	Serial number	
	Device Name	BNR02
	Device ID	0x02100802
	Device ID Mode	Predefined
	Device number	2
	Access Password	
	Device Instance Number	1050626
	Max APDU Length	1476
	UTC time synchronization master	<Undefined>
	GMT time zone	GMT+01:00 Berlin, Rom

8   SSA-DNT program description

The SSA DNT (**D**iscovery and **N**ode Setup **T**ool) includes the following program elements.

Menu

Menu	Function
File > Close	Close the SSA-DNT program.
Tools > Options	Path to the folder containing the firmware images. **Additional file selection**: Activates an input row in the **Firmware update** window to manually select the firmware file.
Tools > Add new PXG3... configuration.	Opens the **Add router configuration** window. A new device configuration can be created for a specified device type (router).
Help > Contents	Opens the PDF help. Select the language for the PDF help via the operating system's **Regional and Language Options**.

Taskbar (left, vertical)

Button	Function
Set up node	Opens the **Set up node** window.
Updating firmware	Goes to the **Update firmware** window. The entry field opens if no firmware library definition file is found.
Remote load	Goes to the **Connect to subnetwork** window.

Set up node window
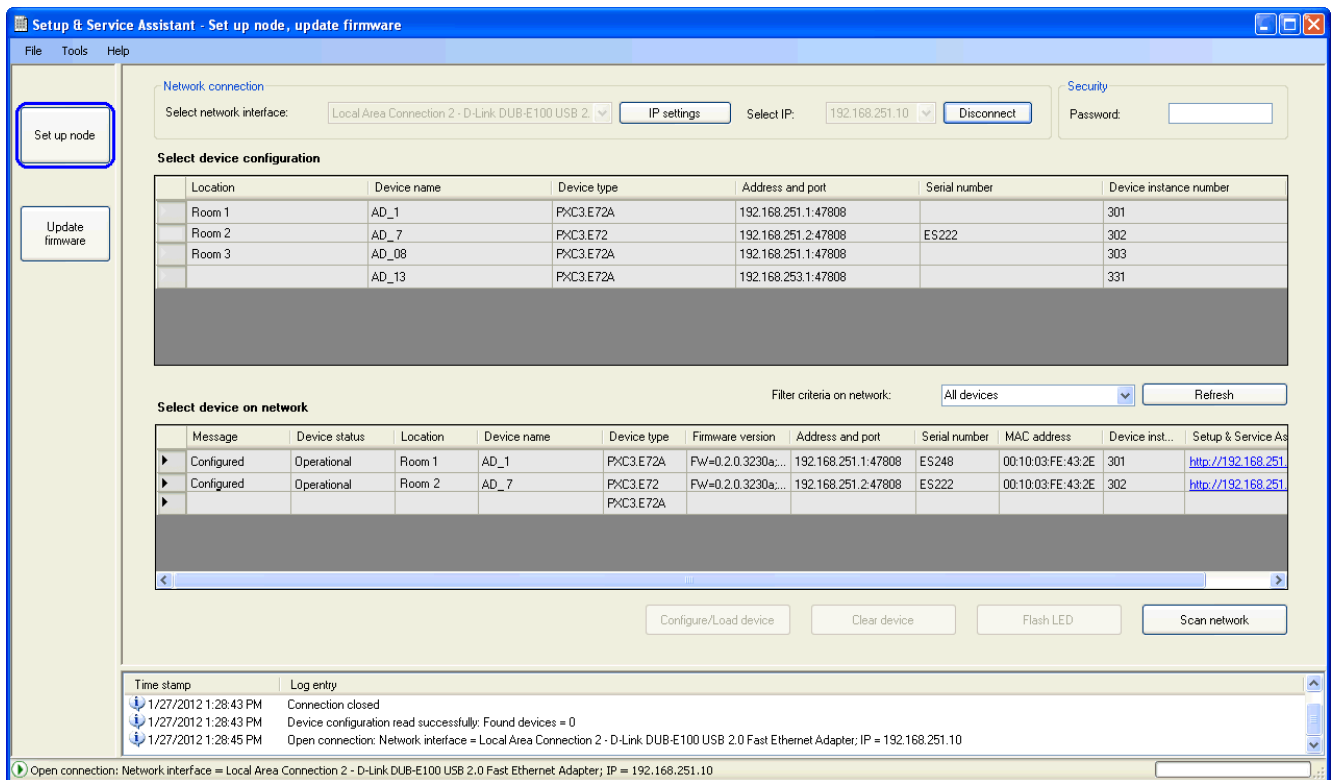
Network connection	
Select the network interface.	Select a configured network interface. See also:Connecting the cable to the IP device [➜ 37]
IP settings	Open the pane **Network connections** with the existing network connections and wizard for new connections. See also:Configuring a network connection [➜ 38]
Select IP.	Select a configured IP address for the network interface.
Connect **Disconnect**	Connects/disconnects a network connection (IP).

Safety	
Password	Project password to access the IP device. The project password is checked automatically when a connection is established (as project manager).

The **Select device configuration** table shows the available device configurations. The device configurations for a TRA project are read from Pack & Go. The device configuration for the router can be created in SSA-DNT (Tools > Add new PXG3... configuration).

Select device configuration	
Location	Engineered description of the device's mounting location.
Device name	Engineered device name.
Device type	Engineered device type.
Address and port	Engineered IP address and UDP port.
Serial number	Device serial number saved in the project.
Device instance number	Engineered device instance number.

Right-click a cell to display the following context menu.

Context menu	
Find the proper serial number.	The network is searched for a device with the serial number in this line and displayed in table **Select device on network**.
Find the proper device type.	The network is searched for all devices with the the device type from this line and displayed in table **Select device on network**.

The **Select device on network** table (Desigo TRA only, no Desigo V5 automation stations) displays all IP devices (room automation stations, routers, etc.) on the (IP) network.

The table values are updated upon a network scan, after pressing the service button on the device, or by configuring the device.

Select device on network		
Message	Device status message.	
	Configured	Device is configured.
	Unconfigure	Device has the factory setting (status after the command **Delete device**).
	Service pin pressed.	The service pin from this device is pressed.
	Time set Configuring Restarting	Device runs the command **Configure/load device**.
	Authentication failed	Password check failed (status after the command **Delete device**).
Device state	Device status.	
	Ready for operation	Device is operational.
	Receive wink.	Device executes command **Flash**.
	Download required	Device has the factory setting (status after the command **Delete device**).
Location	Description of the device's mounting location (configured).	
Device name	Device name (configured).	
Device type	Device type (specific to the device).	
Firmware version	Firmware version of the device (device-specific).	
Address and port	Engineered IP address and UDP port (configured).	
Serial number	Serial number (specific to the device).	

Select device on network		
MAC address	MAC address (device-specific).	
Device instance number	...	Device instance number (configured).
	4194303	Device not configured.
URL Setup & Service Assistant	http://...	Device homepage address (device-specific).

The filter limits the network search to the selected device type.

Filter	
Filter criteria for the network.	Device type selection.
Refresh	Searches for the selected device type on the network and lists the devices in the **Select device on network** table.

| Button	
Read back	Reads the configuration parameters of the selected IP device and saves them to a file. (Only web interface PXG3 W100 at this time).
Configure/load device	Configure both network (node setup) and device. Load the configuration data (for field bus and field devices) in the room automation station. Prerequisite: The device is not configured, device type and serial number match. See: Changing a router configuration online [➜ 16] See: Configuring router (Node Setup) [➜ 13]
Delete device	Delete network configuration, device configuration, and configuration data in the device (factory setting). See: Changing a router configuration online [➜ 16] See: Configuring router (Node Setup) [➜ 13]
Flashing	Makes the LED on the room automation station flash. See: Changing a router configuration online [➜ 16] See: Configuring router (Node Setup) [➜ 13]
Scan network	Scan the (IP) network to discover all IP devices (room automation stations, routers, etc.) and display them in the **Select device on network** table (Desigo TRA only, no Desigo V5 automation stations). See: Changing a router configuration online [➜ 16] See: Configuring router (Node Setup) [➜ 13]

Log window
Shows the individual steps carried out in the program.

Status display (lower left hand edge of pane).
Shows the connection status between commissioning computer and network (IP).

"Update firmware" window
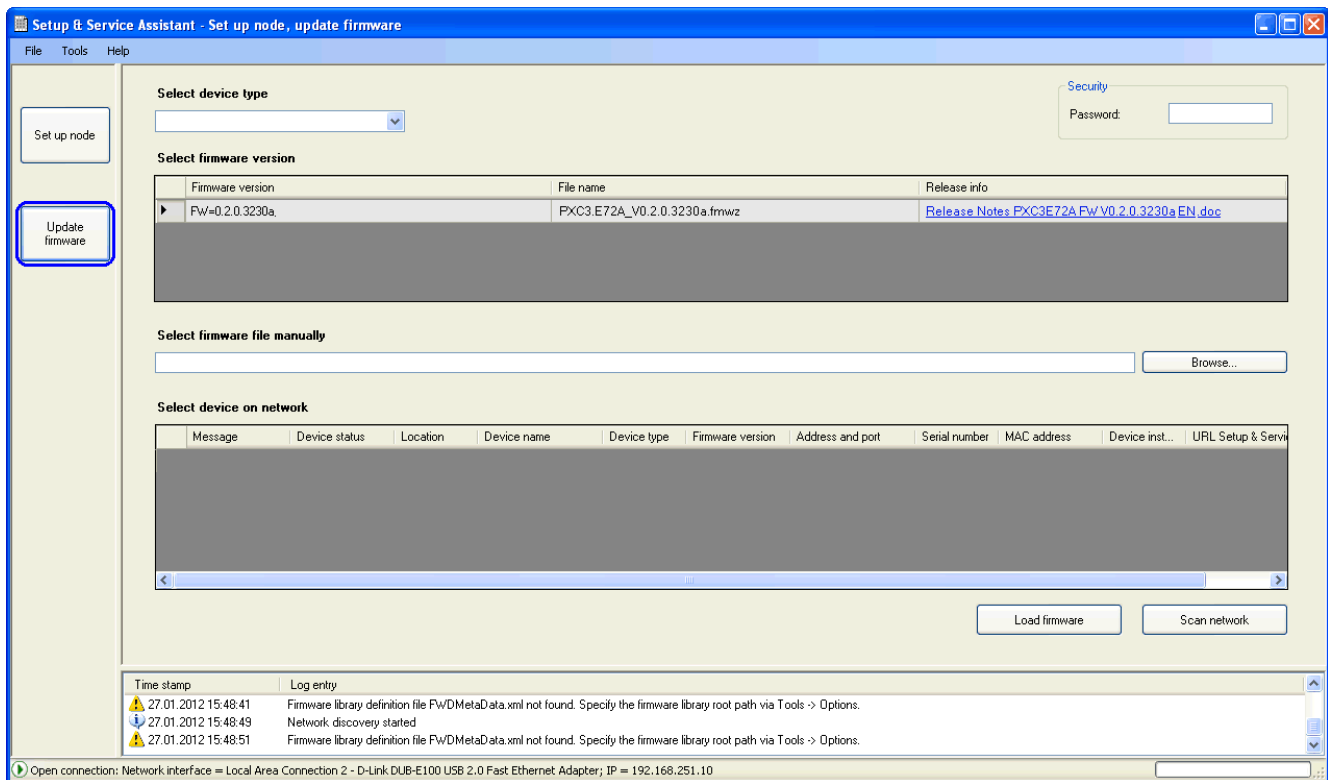
Filter	
Select device type	Searches for the selected device type on the network and lists the devices in the **Select device on network** table. The selectable device types are dependent on whether or not a firmware file exists for the device type. (Tools > Options)

Safety	
Password	Project password to access the IP device. The project password is checked automatically when a connection is established (as project manager).

Select firmware version	
Firmware version	Firmware version in the firmware image.
File name	File name for the firmware image.
Release info	Release information for the firmware image.

The entry field **Select firmware file manually** must be enabled via **Tools > Options: Additional file selection**.

Select firmware file manually	
Entry field	Path for the firmware file.
Browse	Browse button to locate the firmware file.

The **Select device on network** table (Desigo TRA only, no Desigo V5 automation stations) displays all IP devices (room automation stations, routers, etc.) on the (IP) network.

Button	
Loading firmware	Loads the firmware in the selected device. Start and end of loading are logged in the log file. See: Updating firmware
Scan network	Scan the (IP) network to discover all IP devices (room automation stations, routers, etc.) and display them in the **Select device on network** table (Desigo TRA only, no Desigo V5 automation stations).

Log window
Shows the individual steps carried out in the program.

Status display (lower left hand edge of pane).
Shows the connection status between commissioning computer and network (IP).
Shows the connection status between commissioning computer and network (IP).

Remote load window
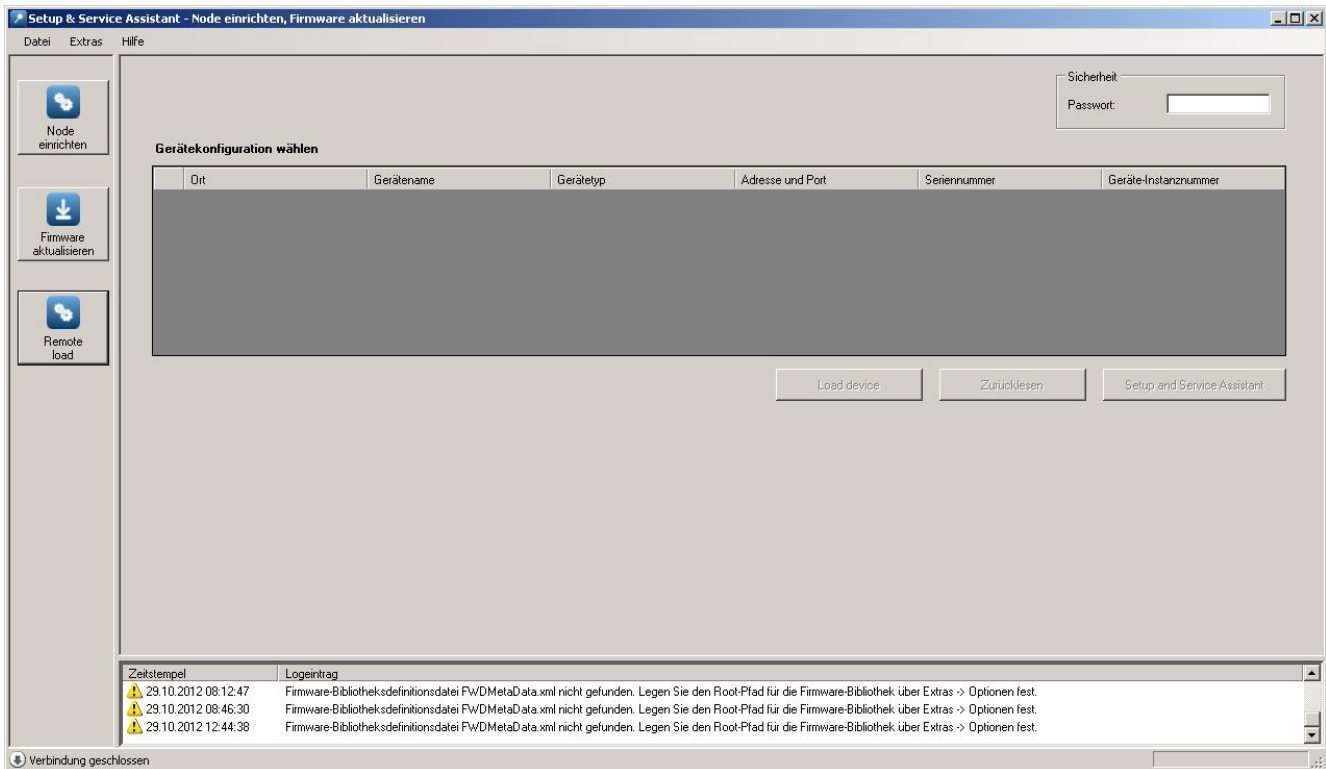
Safety	
Password	Project password to access the IP device.
	The project password is checked automatically when a connection is established (as project manager).

Select device configuration	
Location	Engineered description of the device's mounting location.
Device name	Engineered device name.
Device type	Engineered device type.
Address and port	Engineered IP address and UDP port.
Serial number	Device serial number saved in the project.
Device instance number	Engineered device instance number.

Button	
Loading a device configuration	Starts loading the device configuration in the selected IP device. Start and end of loading are logged in the log file. See: Configuring and reading back via IP connection
Read back	Reads the configuration parameters of the selected IP device and saves them to a file. (Only web interface PXG3 W100 at this time). See: Configuring and reading back via IP connection
Setup & Service Assistant	Opens the homepage of the IP device. See: Configuring and reading back via IP connection

Log window

Shows the individual steps carried out in the program.

Status display (lower left hand edge of pane).

Shows the connection status between commissioning computer and network (IP).

9 Connecting the cable to the IP device

Use a LAN or USB cable to connect the commissioning laptop to the IP device (e.g. room automation station, router, ...).

LAN cable

The LAN cable connects the commissioning laptop with the network (IP) in two ways:

- The LAN cable is plugged in **directly** to the device.
- The LAN cable is plugged in at another location on the network (IP).
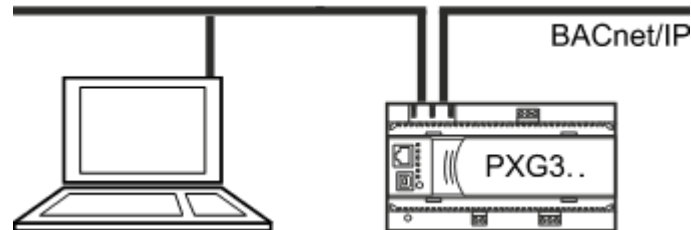
Note: If 24 V power supply to an automation station is interrupted, the switch function of this automation station automatically stops, and IP communication to other automation stations in the communication chain is interrupted.

▷ LAN cable RJ45 is available (Category 5 or higher).

1. Plug in the LAN cable to the commissioning laptop and IP device.

2. Configure the network connection in the SSA DNT.
   See: Configuring a network connection

USB cable

The USB cable **directly** connects the commissioning laptop to the IP device. The IP device establishes the additional connection to the network (IP). This has the following effect: The connection between the commissioning laptop and the network (IP) is interrupted (e.g. during configuration, etc.) if the IP device is restarted.

▷ USB cable is available (type A plug on one end and type B on the other).

▷ USB driver RNDIS is installed or exists locally (load via V5, ACS, BIM tool or Internet).

1. Plug in the USB cable to the commissioning laptop and IP device.
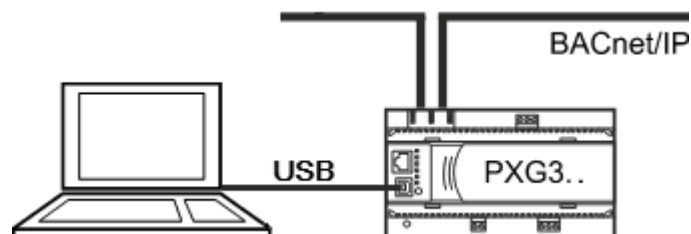
   – If no USB driver is installed and the Internet is connected, locate the right USB driver and install it using the wizard.
   – Enter the storage location in the wizard if the driver is saved locally.
   ⇨ A new USB IP network connection (Siemens USB Remote NDIS Network Device…) is created.

2. Configure the network connection.
   See: Configuring a network connection

10 Configuring a network connection

The commissioning laptop requires a unique IP address in the IP network.
In addition, the commissioning laptop and the IP devices (room automation station, router, etc.) must be located in the same subnet for SSA-DNT to detect a device using UDB Multicast. For example
192.168.251.**10**, **Subnet mask 255.255.255.0**
192.168.251.**20**, **Subnet mask 255.255.255.0**

The network connection of the commissioning laptop must be configured accordingly. Automatic IP address assignment by a DHCP server does not satisfy this requirement.

Note:

• The existing IP address with subnet mask is key for **configured** IP devices.

• The IP address with subnet mask (target address) to be configured is key for **unconfigured** IP devices. This ensures that all devices are located in the same subnet following configuration.

Configuring the commissioning laptop network connection

In the SSA DNT program, network connection settings can be queried directly via the **IP settings** button (same as Start > Control Panel > Network Connections in the Windows operating system).

Prerequisite

• The IP address with subnet mask is known for the commissioning laptop (ask your project manager).

Procedure

1. Start program SSA-DNT:

   – Double-click file SSA DNT.exe.
   or
   – Select **Start > Programs > DESIGO Tools > DESIGO SSA-DNT > SSA-DNT**.

2. In the SSA DNT, click **IP settings**.

   ⇨ The **Network connections** pane opens.
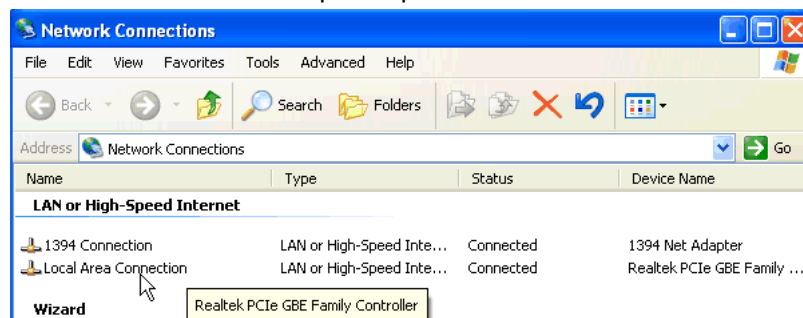
3. Double-click the LAN network interface.
   or
   Double-click the USB network interface (e.g. SBT USB Remote NDIS Network Device…). See: Connecting the cable to the IP device [➜ 37]
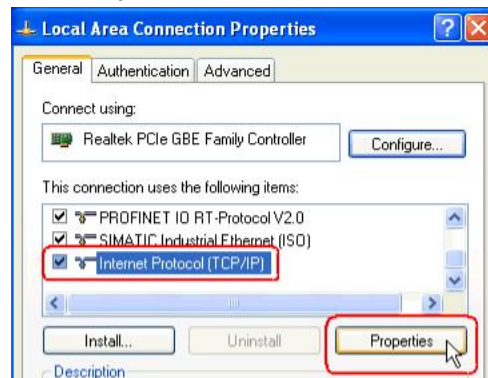
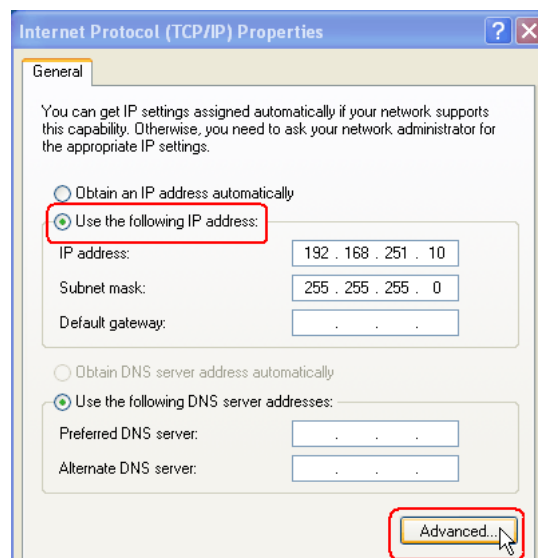   ⇨ The **Status for** dialog box opens.

4. Click **Properties**.
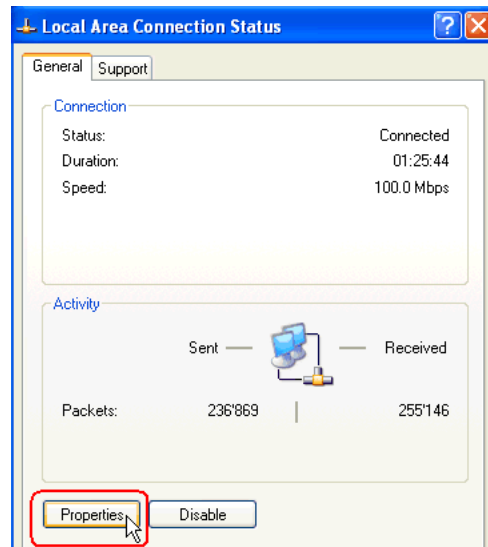
5. Select **Internet Protocol (TCP/IP)**.
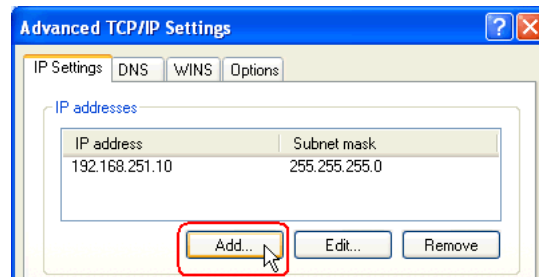
    Click **Properties**.

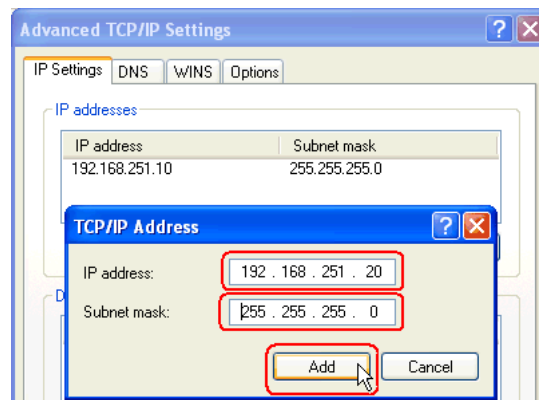6. Select **Use following IP address**.

    Click **Advanced**.

7. Click **Add**.

8. Enter the **IP address** (IP address range for Desigo TRA).

   Enter the **subnet mask** (e.g. 255.255.255.0).

   Click **Add**.

9. Confirm by clicking **OK** and close the dialog box.

⇨ The network connection was assigned another fixed IP address.

11 Defining proxy server settings

Disabling DHCP/APIPA (dynamic addressing) can cause problems when opening a web page, as this disables automatic proxy server configuration. Defining a proxy exception for the APIPA range (e.g. for unconfigured automation station or router 169.254.213.44) can resolve the problem.

Defining the APIPA range (e.g. in Internet Explorer)

1. Open Microsoft Internet Explorer:

2. Select **Tools > Internet Options**.

3. Click the **Connections** tab.

4. Click **LAN settings**.

5. Clear **Use automatic configuration script**.
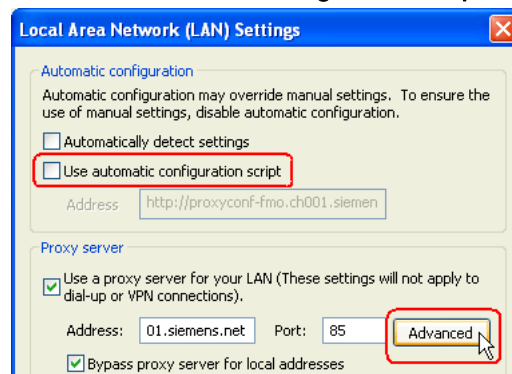
6. Click **Advanced**.

7. Enter **169.***.
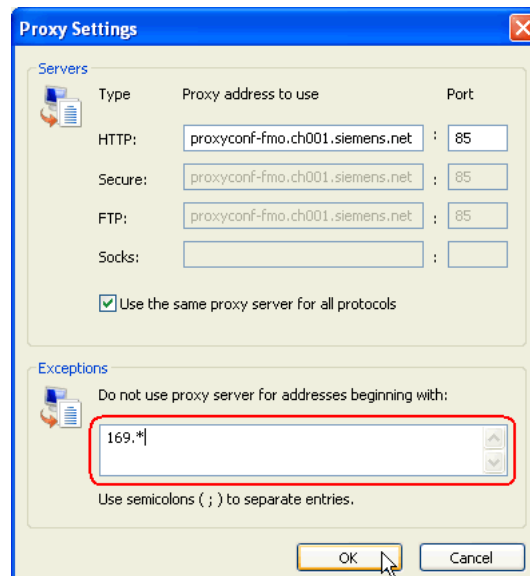
8. Click **OK** several times.

⇨ The browser no longer applies a proxy server to the indicated address range.

Index