FAQ • 11/2013

SCALANCE S – Coupling of company and machine network

SCALANCE S6xx

http://support.automation.siemens.com/WW/view/en/27099462

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

Caution

The functions and solutions described in this article confine themselves to the realization of the automation task predominantly. Please take into account furthermore that corresponding protective measures have to be taken up in the context of Industrial Security when connecting your equipment to other parts of the plant, the enterprise network or the Internet. Further information can be found under the Content-ID 50203404.

http://support.automation.siemens.com/WW/view/en/50203404

Table of contents

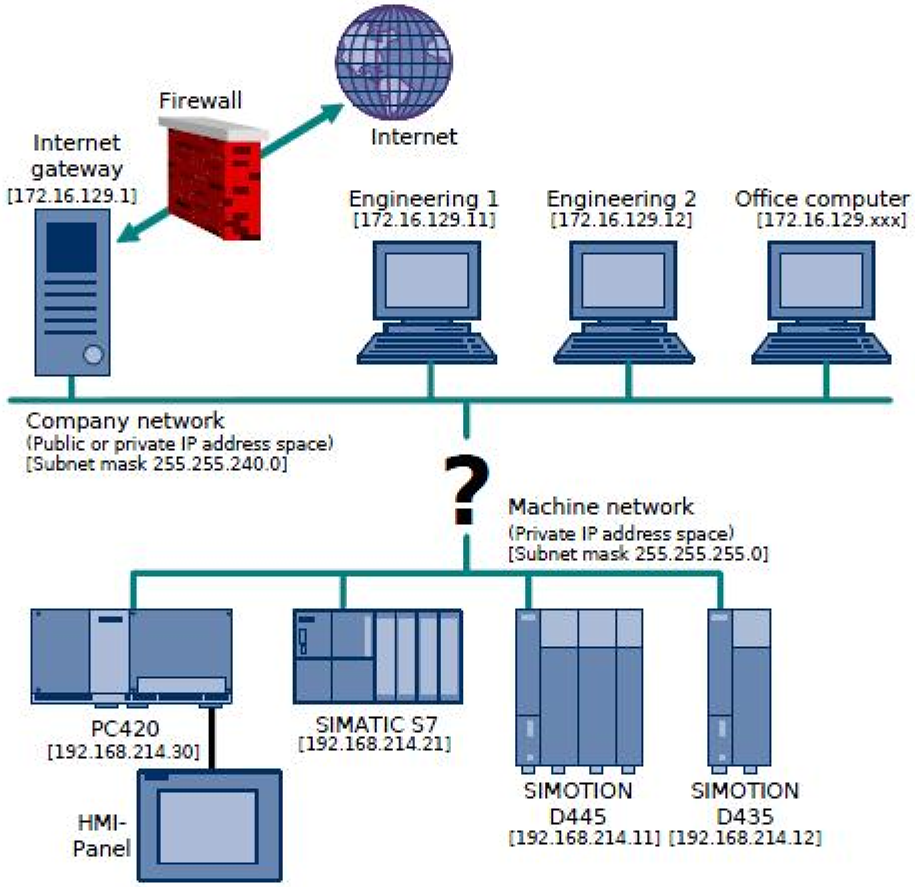
1 Task

1.1 Overview

A production machine is automated with several controllers. It is a combination of SIMATIC and SIMOTION controllers with subordinate SINAMICS drives technology. The operation of the machine is carried out on an industrial PC with Windows operation system.

The individual controllers and the industrial PC are networked to each other by means of Ethernet. The machine network is also used for the engineering.

Figure 1-1 Configuration of the company and machine network



1.2 Requirements

The engineering computers are – amongst other computers – part of a company network (e.g. the machine manufacturer's). For reasons of safety and cost the engineering should…

- …not be carried out in parallel directly on the machine network via a second network card.
- …not be carried out by re-plugging the Ethernet cables from the company network to the machine network and vice versa or by re-parameterization of the Windows network settings.

However the machine should be connected to the company network. The engineering computers should have access up to the machine via the company network.

All services provided by the company network (Email, Intranet, Internet) should work for the engineering computers without any restrictions in parallel to accessing the machine network.

This brings forth the following issues:

- Which components must be used for the connection of the company and machine network?
- How can an engineering computer – linked to the company network – access the machine network?
- How can be guaranteed that influences and errors from the company network do not affect the machine network?
- How is it ascertained that only permitted engineering computers can access the machine network?
- How is it ascertained that devices from the machine network cannot randomly access the company network?
- How is it ascertained that only required services are permitted to pass the boundary between the company and machine network?
- Which settings must be configured on the engineering computers and in the project?
  - For routing up to the drive components?
  - When several machines (with identical IP addresses in the individual machine networks) are connected in parallel to the company network?

2 Solution

2.1 Overview

The solution outlined in this chapter is based on the example described in chapter 1. This applies to both the HW configuration of the machine network and the IP addresses of the company and machine network.

NOTICE **For using the solution described in this chapter the exemplary used IP addresses, subnet masks, etc. must be adapted to the actual conditions.**

2.2 Component selection

In order to connect a machine network to the company network you will need a network component, which can handle routing and also has a firewall.

In this exemplary solution a `SCALANCE S6xx` is used. However, a commercial router with firewall functionality can be used, too. The whole configuration of the SCALANCE S6xx is carried out using the `Security Configuration Tool (SCT)`.

Table 2-1 Used hardware

Component	No.	Order number	Note
SCALANCE S6xx	1	6GK56xx-0BA00-2AA3	V2.3 HF

Table 2-2 Used software

Component	No.	Order number	Note
Security Configuration Tool (SCT)	1	---	V3.0

NOTE All products of the SCALANCE S family support the routing and firewall functionality. Therefore every SCALANCE S is suitable for this solution.

NOTE Referring to following link you will find product information and manuals for the SCALANCE S family in the Siemens Industry Online Support (SIOS) as well as using the keyword “SCALANCE S”:

http://support.automation.siemens.com/WW/view/en/18701555/133400

2.3 Commissioning of the SCALANCE S6xx

Port 1 (P1 – External Network) of the SCALANCE S6xx is connected to the company network and Port 2 (P2 – Internal Network) is connected to the machine network.

Port 1 receives the IP address `172.16.130.30` as well as the subnet mask `255.255.240.0` from the IP address space of the company network. This is carried out in accordance with the responsible IT-department of the company network, which manages the IP addresses.

Port 2 receives the IP address `192.168.214.40` as well as the subnet mask `255.255.255.0` from the IP address space of the machine network.

NOTE When several machines are connected to the company network in parallel please ensure that there is a unique IP address in the company network for each SCALANCE S6xx.

2.3.1 Node initiation

Before the first download to the SCALANCE S6xx it must be ensured that its interface (IP address and subnet mask of port 1) is configured correctly for the `Security Configuration Tool`.

1. Establish the factory settings of the SCALANCE S6xx by using its reset button.

NOTE The reset button is located under the screw cap on the reverse side of the device. It must be pressed for several seconds when the power supply is switched on until the fault LED is flashing yellow-red. The reset to factory settings can last up to two minutes followed by the fault LED lightning continuous yellow.

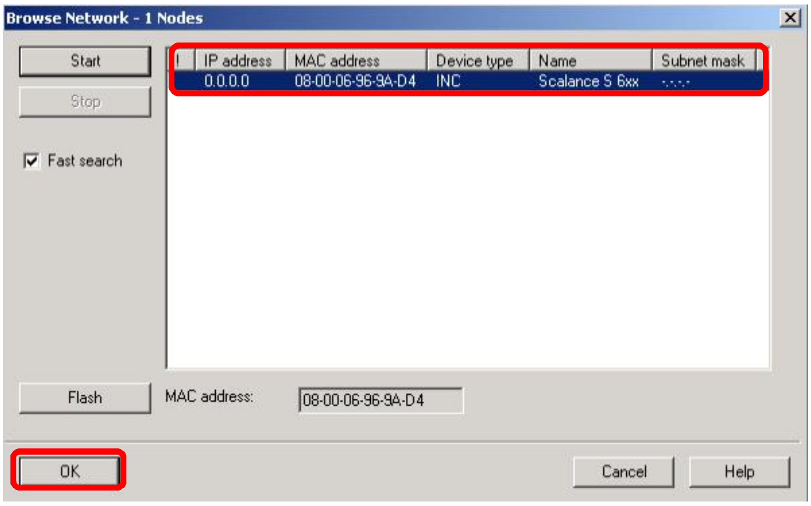
2. Establish a connection between your engineering computer and port 1 of the SCALANCE S6xx using a commercial Ethernet cable.

NOTE The SCALANCE S6xx supports the `auto crossing` functionality, i.e. it is recognized whether the used cable has continuous or crossed send and receive lines. If necessary the send and receive lines are crossed automatically inside of the device.

3. Start the engineering system STEP7 SIMATIC Manager.
   Browse through the network that is connected with the engineering computer via the menu entry `PLC > Edit Ethernet Node… > Browse`.

   Afterwards choose the SCALANCE S6xx (after reset to factory settings it has the IP address 0.0.0.0) and confirm your choice via the button `OK`.

Figure 2-1 Browse for Ethernet nodes



Browse Network - 1 Nodes

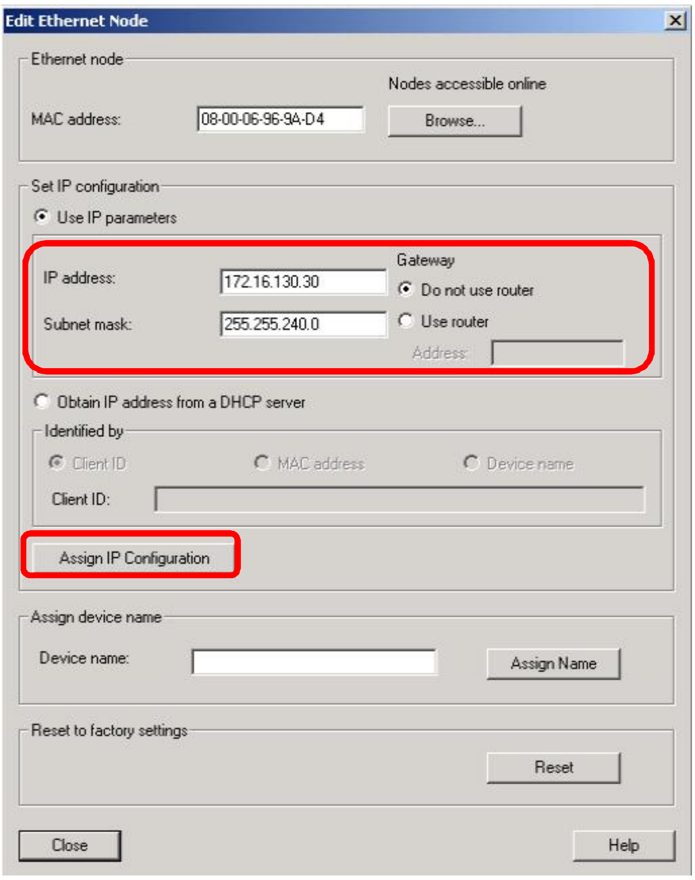
☑ Fast search

IP address	MAC address	Device type	Name	Subnet mask
0.0.0.0	08-00-06-96-9A-D4	INC	Scalance S 6xx	-.-.-.-

MAC address: 08-00-06-96-9A-D4

4. Insert the IP address and subnet mask of port 1 in the provided areas using the option `Set IP configuration` and assign the configuration to the SCALANCE S6xx via the button `Assign IP Configuration`.

Figure 2-2 Edit Ethernet nodes



Edit Ethernet Node

Ethernet node

MAC address: 08-00-06-96-9A-D4

Nodes accessible online

Set IP configuration

● Use IP parameters

IP address: 172.16.130.30

Subnet mask: 255.255.240.0

Gateway

● Do not use router

○ Use router

Address:

○ Obtain IP address from a DHCP server

Identified by

● Client ID ○ MAC address ○ Device name

Client ID:

Assign device name

Device name:

Reset to factory settings

5. The node initiation of the SCALANCE S6xx is now finished.

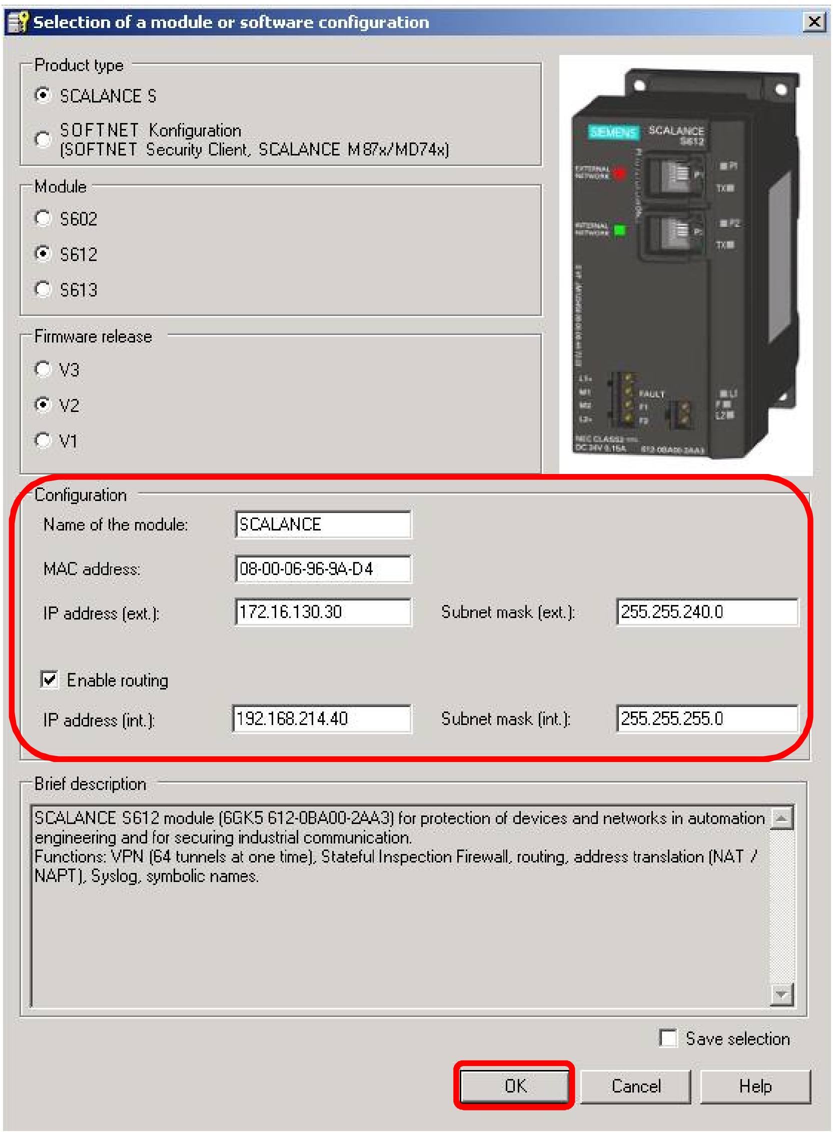
2.3.2 Settings for routing

Open the `Security Configuration Tool` und create a new project. Assign a new username and a password and insert the SCALANCE S6xx (in the example firmware release V2) into the project as a new module.

Carry out following settings:

MAC address	MAC address of the used device
IP address (ext.)	`172.16.130.30`
Subnet mask (ext.)	`255.255.240.0`
Enable routing	Activate the routing functionality
IP address (int.)	`192.168.214.40`
Subnet mask (int.)	`255.255.255.0`

Figure 2-3 Configure SCALANCE S6xx



Selection of a module or software configuration

Product type
● SCALANCE S
○ SOFTNET Konfiguration (SOFTNET Security Client, SCALANCE M87x/MD74x)

Module
○ S602
● S612
○ S613

Firmware release
○ V3
● V2
○ V1

Configuration
Name of the module: SCALANCE
MAC address: 08-00-06-96-9A-D4
IP address (ext.): 172.16.130.30
Subnet mask (ext.): 255.255.240.0
☑ Enable routing
IP address (int.): 192.168.214.40
Subnet mask (int.): 255.255.255.0

Brief description
SCALANCE S612 module (6GK5 612-0BA00-2AA3) for protection of devices and networks in automation engineering and for securing industrial communication.
Functions: VPN (64 tunnels at one time), Stateful Inspection Firewall, routing, address translation (NAT / NAPT), Syslog, symbolic names.

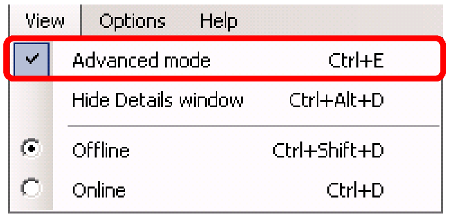
□ Save selection

Afterwards switch to the advanced mode of the project view via the menu entry `View > Advanced`. In this view you can carry out more detailed settings for the SCALANCE S6xx.

NOTE

> If changes in the settings of the SCALANCE S6xx are carried out in the `Advanced Mode` you cannot switch back to the `Standard Mode` afterwards.

Figure 2-4 Advanced Mode



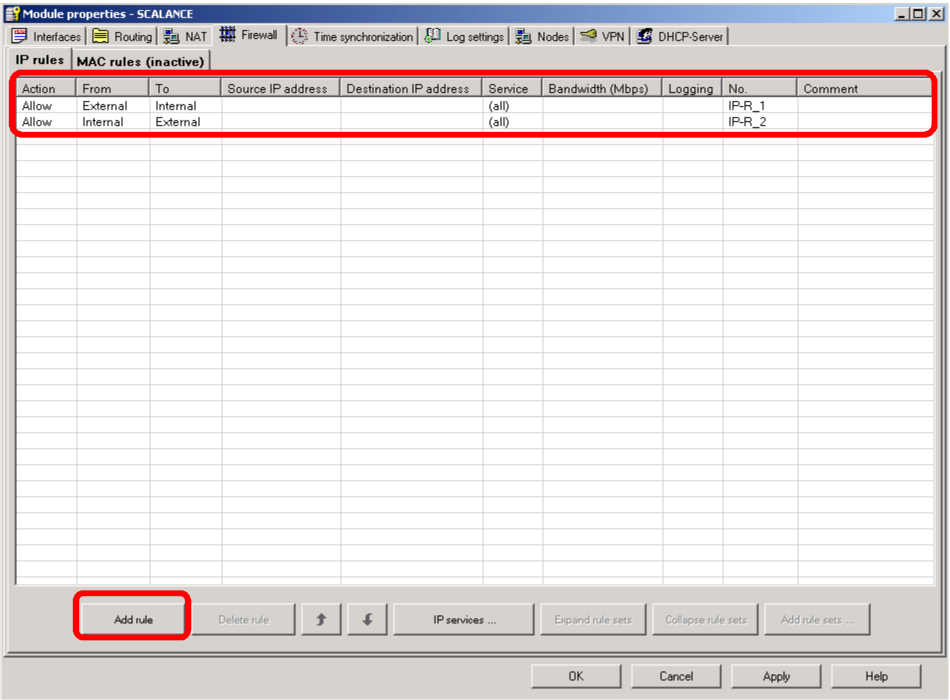
Open the properties of the SCALANCE S6xx by double clicking on it.
Enable all services in the `Firewall` tab for now.

Therefore carry out following settings (new firewall rules can be added via the button `Add rule`):

Table 2-3 Firewall rules to be defined

Action	From	To	Service
Allow	External	Internal	(all)
Allow	Internal	External	(all)

Figure 2-5 Define the firewall rules



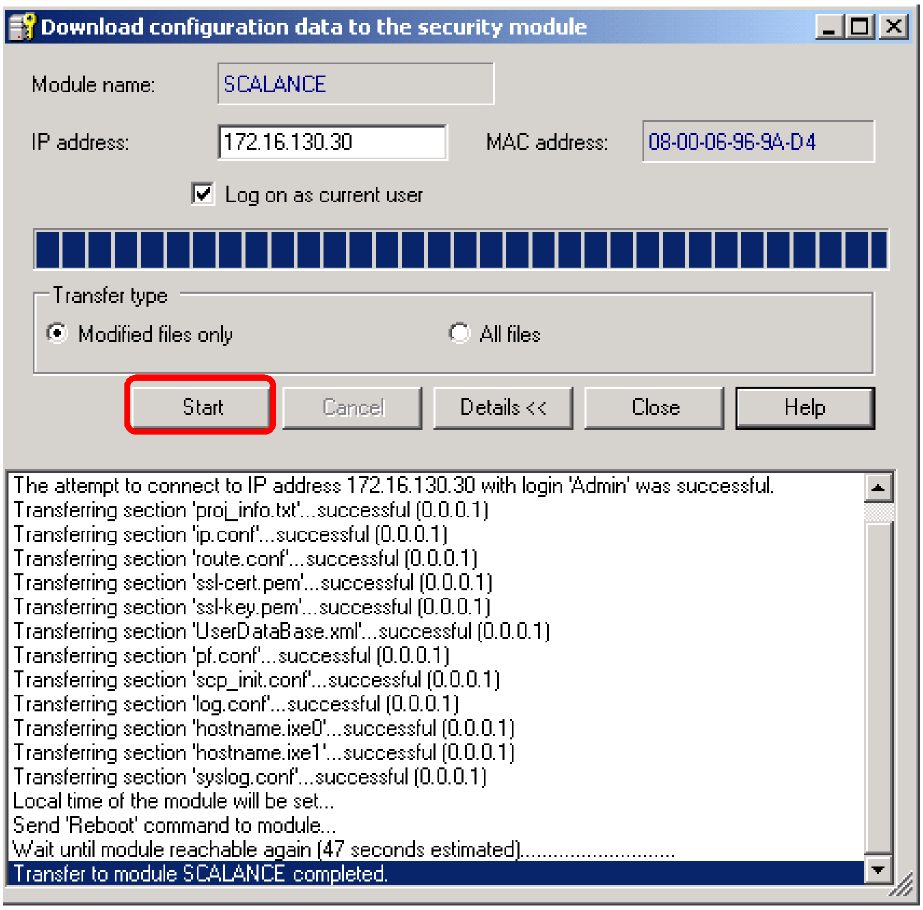
Action	From	To	Source IP address	Destination IP address	Service	Bandwidth (Mbps)	Logging	No.	Comment
Allow	External	Internal			(all)			IP-R_1	
Allow	Internal	External			(all)			IP-R_2	

Save the settings carried out in the project and load the configuration into the SCALANCE S6xx.

Therefore first of all select the device. Afterwards you will arrive at the choice of the used network adapter via the menu entry `Transfer > To module(s)...` Choose the corresponding network adapter and confirm your choice.

Start the download of the configuration via the button `Start`.

Figure 2-6 Download of the configuration



Module name: SCALANCE

IP address: 172.16.130.30

MAC address: 08-00-06-96-9A-D4

☑ Log on as current user

● Modified files only ○ All files

```
The attempt to connect to IP address 172.16.130.30 with login 'Admin' was successful.
Transferring section 'proj_info.txt'...successful (0.0.0.1)
Transferring section 'ip.conf'...successful (0.0.0.1)
Transferring section 'route.conf'...successful (0.0.0.1)
Transferring section 'ssl-cert.pem'...successful (0.0.0.1)
Transferring section 'ssl-key.pem'...successful (0.0.0.1)
Transferring section 'UserDataBase.xml'...successful (0.0.0.1)
Transferring section 'pf.conf'...successful (0.0.0.1)
Transferring section 'scp_init.conf'...successful (0.0.0.1)
Transferring section 'log.conf'...successful (0.0.0.1)
Transferring section 'hostname.ixe0'...successful (0.0.0.1)
Transferring section 'hostname.ixe1'...successful (0.0.0.1)
Transferring section 'syslog.conf'...successful (0.0.0.1)
Local time of the module will be set...
Send 'Reboot' command to module...
Wait until module reachable again (47 seconds estimated)...........................
Transfer to module SCALANCE completed.
```

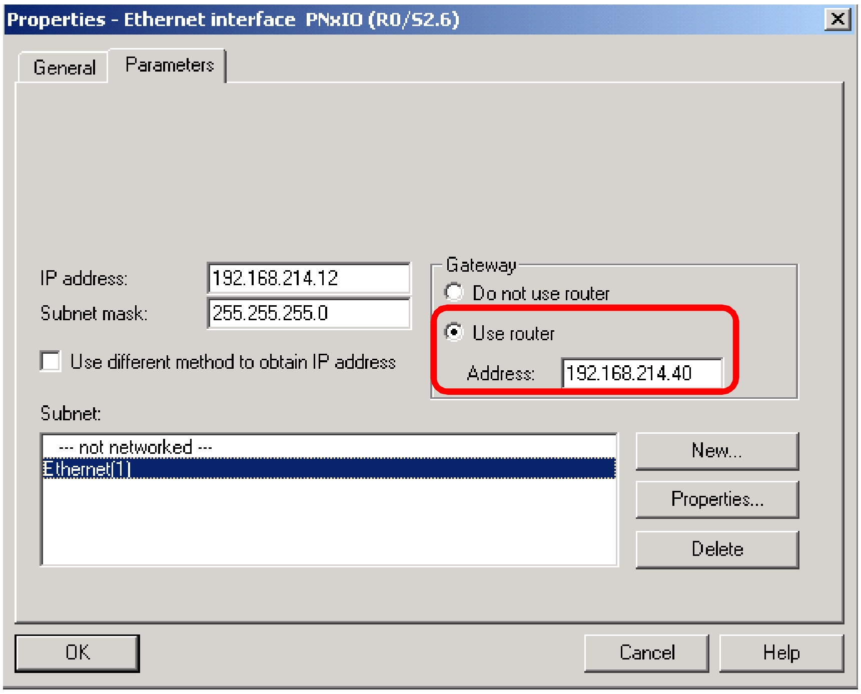
The configuration of the basic routing mechanisms between the company and the machine network is now finished.

2.4 Settings for routing in the STEP7 project

For establishing an online connection from the engineering computers to the individual controllers (SIMATIC, SIMOTION, etc.) in the machine network, the necessary routing information must be added in the HW configuration of the particular controller.

Therefore enter the IP address of the SCALANCE S6xx from the machine networks view (i.e. the IP address of port 2: `192.168.214.40`) in HW configuration for the Ethernet interface of the particular controller, that is connected to the machine network.

Figure 2-7 Settings for routing in HW configuration



Properties - Ethernet interface PNxIO (R0/S2.6)

IP address: 192.168.214.12

Subnet mask: 255.255.255.0

□ Use different method to obtain IP address

Gateway

○ Do not use router

● Use router

Address: 192.168.214.40

Subnet:

--- not networked ---

Ethernet(1)

In addition the PG/PC stations (engineering computers), that shall have access to the controllers in the machine network, must be added in NetPro.

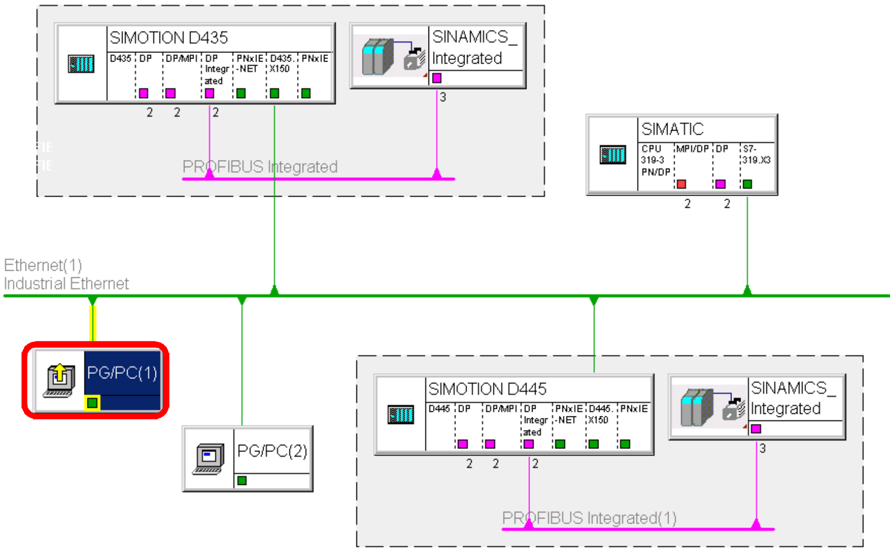
Therefore insert the appropriate number of PG/PC stations in NetPro and enter the PG's IP address from the company networks view for the particular Ethernet interface.

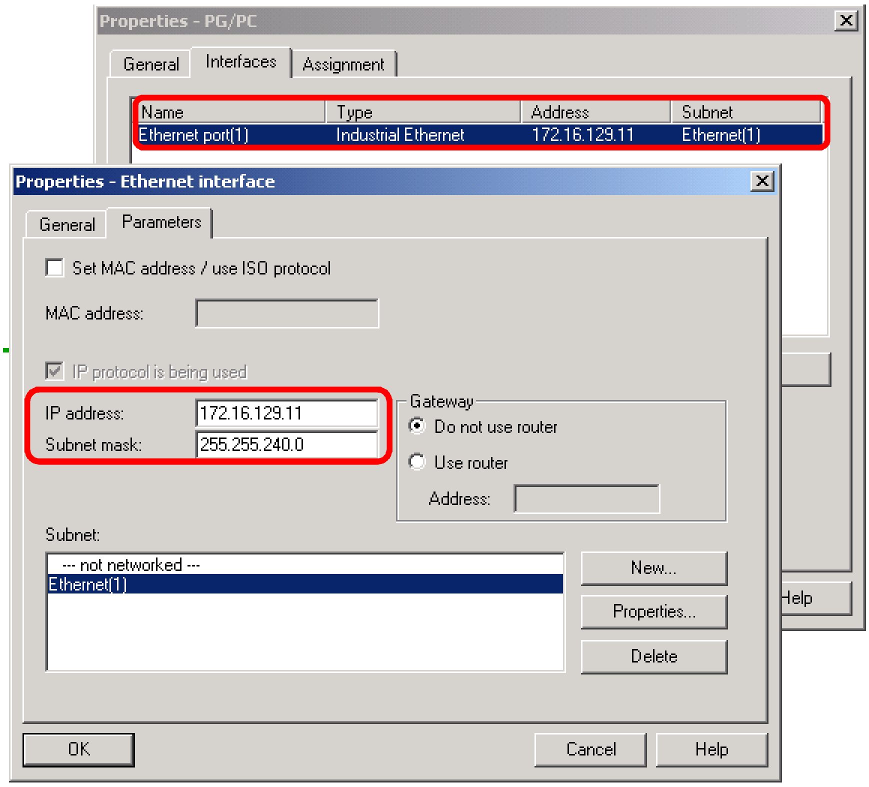
NOTE

In this case the declaration of the IP address of port 1 (`172.16.130.30`) of the SCALANCE S6xx as gateway is not required.

The IP address will be entered afterwards in the Windows routing settings of the particular engineering computer (see also chapter 2.5: "Settings for routing in the engineering computers").

Figure 2-8 Configuration of NetPro




Properties - PG/PC

Name	Type	Address	Subnet
Ethernet port(1)	Industrial Ethernet	172.16.129.11	Ethernet(1)

Properties - Ethernet interface

□ Set MAC address / use ISO protocol

MAC address:

☑ IP protocol is being used

IP address: 172.16.129.11

Subnet mask: 255.255.240.0

Gateway

● Do not use router

○ Use router

Address:

Subnet:

--- not networked ---

Ethernet(1)

NOTE

Pay attention that in the settings of the particular PG/PC interface the option **"Set MAC address / use ISO protocol"** is not used!

The ISO protocol is not supported from SIMOTION controllers.
If this option is activated it is not possible to establish an online connection to this controllers afterwards!

2.5 Settings for routing in the engineering computers

As a rule the entire IP configuration of a computer network is assigned via a DHCP server. The DHCP server usually allocates IP addresses to the computers by means of their MAC addresses based on static allocation tables.

The standard gateway defined in the Windows IP properties defines the contact partner for IP packets, which are not meant for its own subnet.

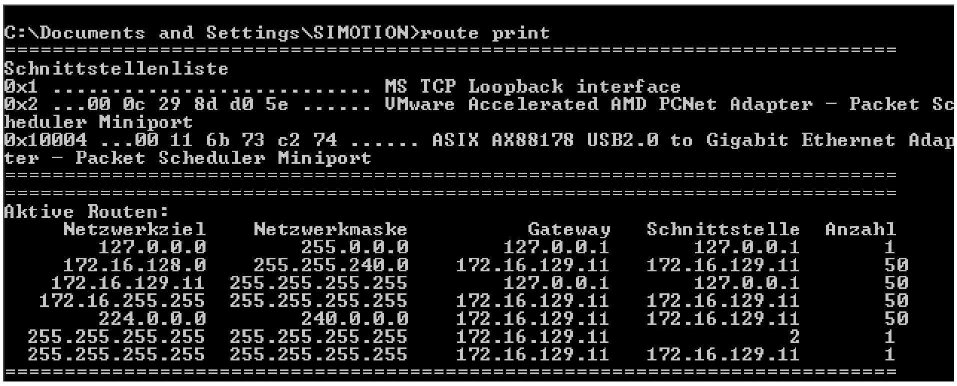
If, however, the new machine network is not announced for the defined standard gateway it cannot do anything with the IP packets that are meant for this network.

So a new route must be defined in the network settings of the engineering computers for IP packets with destination network 192.168.214.0 (net-ID of the machine network). This can be done via two different ways:

6. The defined standard gateway in the company network must receive a new route to the machine network. Therefore the net-ID (`192.168.214.0`) and the IP address of the SCALANCE S6xx (`172.16.130.30`) must be entered in the router from the IT administrator. So a general accepted route is defined.
7. A further gateway is defined in all engineering computers, which shall communicate from the company network to the machine network. This is carried out for example via the prompt (`Start > Execute > cmd`) and the `route` command.

Routes that are already active can be displayed via the `route print` command.

Figure 2-9 Display of the active routes



```
C:\Documents and Settings\SIMOTION>route print
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 8d d0 5e ...... VMware Accelerated AMD PCNet Adapter - Packet Sc
heduler Miniport
0x10004 ...00 11 6b 73 c2 74 ...... ASIX AX88178 USB2.0 to Gigabit Ethernet Adap
ter - Packet Scheduler Miniport
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway   Schnittstelle  Anzahl
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     172.16.128.0    255.255.240.0    172.16.129.11   172.16.129.11      50
    172.16.129.11  255.255.255.255        127.0.0.1       127.0.0.1      50
   172.16.255.255  255.255.255.255    172.16.129.11   172.16.129.11      50
        224.0.0.0        240.0.0.0    172.16.129.11   172.16.129.11      50
  255.255.255.255  255.255.255.255    172.16.129.11               2       1
  255.255.255.255  255.255.255.255    172.16.129.11   172.16.129.11       1
===========================================================================
```

An additional route can be added via the command `route add <net-ID> mask <subnet mask> <router IP address> -p`.

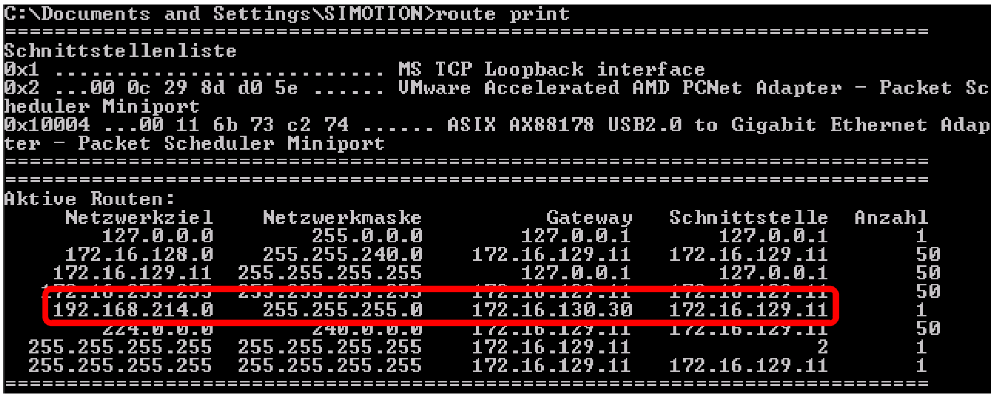
- `<net-ID>` is the net-ID of the machine network (**192.168.214.0**)
- `<subnet mask>` is the subnet mask of the machine network (**255.255.255.0**)
- `<router IP address>` is the IP address of the SCALANCE S6xx from the company networks view (i.e. the IP address of port 1: **172.16.130.30**)
- The addition `-p` causes the route to be used independent from a reboot of the engineering computers. Therefore this route is persistent.

The following command must be carried out to add the new necessary route in the network settings of the engineering computers:

```
route add 192.168.214.0 mask 255.255.255.0 172.16.130.30 -p
```

Via the `route print` command it can be checked afterwards, whether the new route was added successfully.

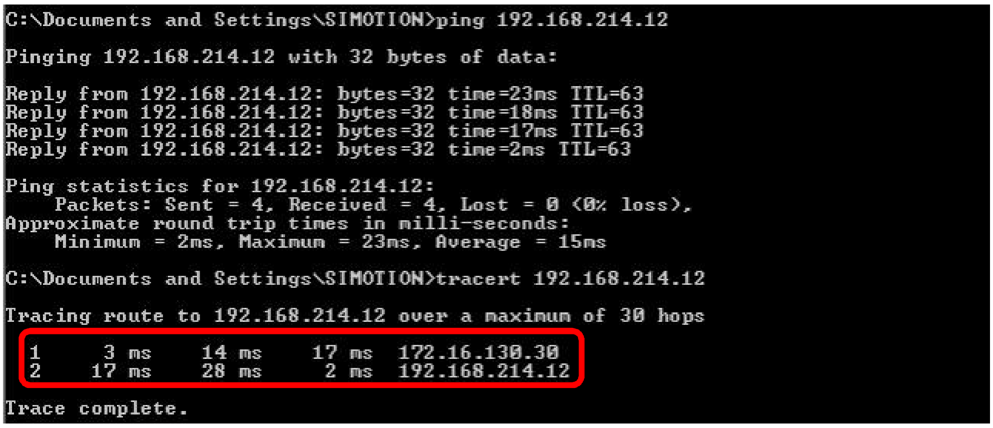
Figure 2-10 Check new added route



```
C:\Documents and Settings\SIMOTION>route print
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 8d d0 5e ...... VMware Accelerated AMD PCNet Adapter - Packet Sc
heduler Miniport
0x10004 ...00 11 6b 73 c2 74 ...... ASIX AX88178 USB2.0 to Gigabit Ethernet Adap
ter - Packet Scheduler Miniport
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway   Schnittstelle  Anzahl
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     172.16.128.0    255.255.240.0    172.16.129.11   172.16.129.11      50
    172.16.129.11  255.255.255.255        127.0.0.1       127.0.0.1      50
   172.16.255.255  255.255.255.255    172.16.129.11   172.16.129.11      50
    192.168.214.0    255.255.255.0    172.16.130.30   172.16.129.11       1
        224.0.0.0        240.0.0.0    172.16.129.11   172.16.129.11      50
  255.255.255.255  255.255.255.255    172.16.129.11               2       1
  255.255.255.255  255.255.255.255    172.16.129.11   172.16.129.11       1
===========================================================================
```

All controllers in the machine network can now be addressed using the command `ping` (e.g. `ping 192.168.214.12`) with the firewall is still deactivated.
The `tracert` (trace route) command shows that the IP packets with destination network `192.168.214.0` take the route via the IP address 172.16.130.30 of the SCALANCE S6xx.

Figure 2-11 Pursuit the route



```
C:\Documents and Settings\SIMOTION>ping 192.168.214.12

Pinging 192.168.214.12 with 32 bytes of data:

Reply from 192.168.214.12: bytes=32 time=23ms TTL=63
Reply from 192.168.214.12: bytes=32 time=18ms TTL=63
Reply from 192.168.214.12: bytes=32 time=17ms TTL=63
Reply from 192.168.214.12: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.214.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 23ms, Average = 15ms

C:\Documents and Settings\SIMOTION>tracert 192.168.214.12

Tracing route to 192.168.214.12 over a maximum of 30 hops

  1     3 ms    14 ms    17 ms  172.16.130.30
  2    17 ms    28 ms     2 ms  192.168.214.12

Trace complete.
```

Now an online connection can be established from the development tools STEP7 SIMATIC Manager and SIMOTION Scout in the company network to the controllers in the machine network without restrictions.

2.5.1 Settings for several machine networks

Several machines with different IP address spaces

When several machines with different IP address spaces shall be reached from an engineering computer in the company network, each route must be individually added in the network settings of the computer via the command `route add` like in the example shown in chapter 2.5.

Several machines with identical IP address spaces

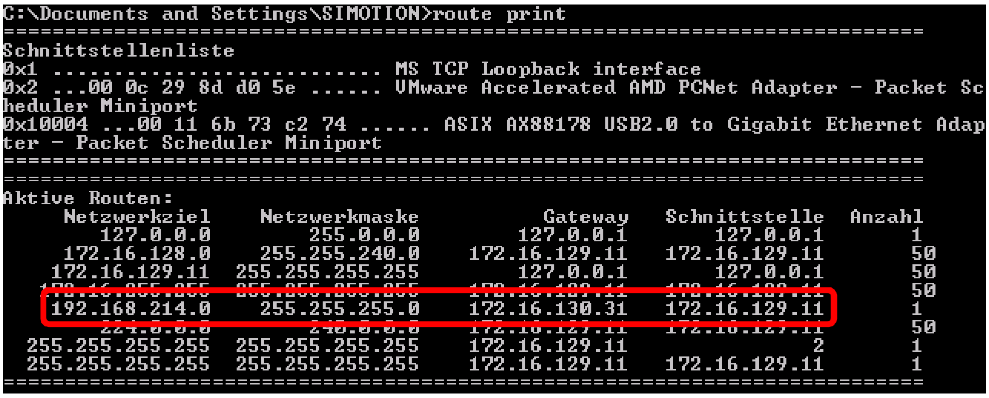
When several machines with identical IP address spaces shall be reached from an engineering computer in the company network, the route must be adapted in accordance with the desired machine.
If a route for the machine network has already been added, it can be changed using the `route change` command.

Example

Command for changing the IP address of the gateway in a route:

```
route change 192.168.214.0 mask 255.255.255.0 172.16.130.31 -
p
```

Figure 2-12 Check changed route



```
C:\Documents and Settings\SIMOTION>route print
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 8d d0 5e ...... VMware Accelerated AMD PCNet Adapter - Packet Sc
heduler Miniport
0x10004 ...00 11 6b 73 c2 74 ...... ASIX AX88178 USB2.0 to Gigabit Ethernet Adap
ter - Packet Scheduler Miniport
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway    Schnittstelle  Anzahl
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
     172.16.128.0    255.255.240.0    172.16.129.11    172.16.129.11       50
    172.16.129.11  255.255.255.255        127.0.0.1        127.0.0.1       50
   172.16.255.255  255.255.255.255    172.16.129.11    172.16.129.11       50
    192.168.214.0    255.255.255.0    172.16.130.31    172.16.129.11       1
        224.0.0.0        240.0.0.0    172.16.129.11    172.16.129.11       50
  255.255.255.255  255.255.255.255    172.16.129.11                2       1
  255.255.255.255  255.255.255.255    172.16.129.11    172.16.129.11       1
===========================================================================
```

NOTE

As an alternative to the shown approach also the NAT (Network Address Translation) functionality of the SCALANCE S6xx can be used.

With this functionality the SCALANCE S6xx has the ability to change over an IP address of the machine network to an IP address of the company network one-to-one.

Further information you will find in chapter 5.1.3: “NAT/NAPT routing” of the manual “SIMATIC NET Industrial Ethernet Security Basics and application” using following link:

http://support.automation.siemens.com/WW/view/en/67437017

NOTE

Please note also the chapter 3.2: “Use the alternative access point (DEVICE)” in this document.

2.6 Firewall settings of the SCALANCE S6xx

Before configuring settings in the firewall of the SCALANCE S6xx you should ask yourself the following question: "Which services will be required?"

The following list shall simply serve you some reference points:

- The `ping` command shall work for all existing devices in the machine network.
- All required services for the development tools from Siemens (i.e. STEP7 SIMATIC Manager, SIMOTION Scout and STARTER) shall be released.
- Enabled devices of the industrial computer in the machine network shall be accessed by the engineering computers in the company network.
- The permitted services may only be initiated by defined computers.
- The different services shall be summarized in service groups for the purpose of clarity in the firewall settings of the SCALANCE S6xx.

Explanation of the most important services:

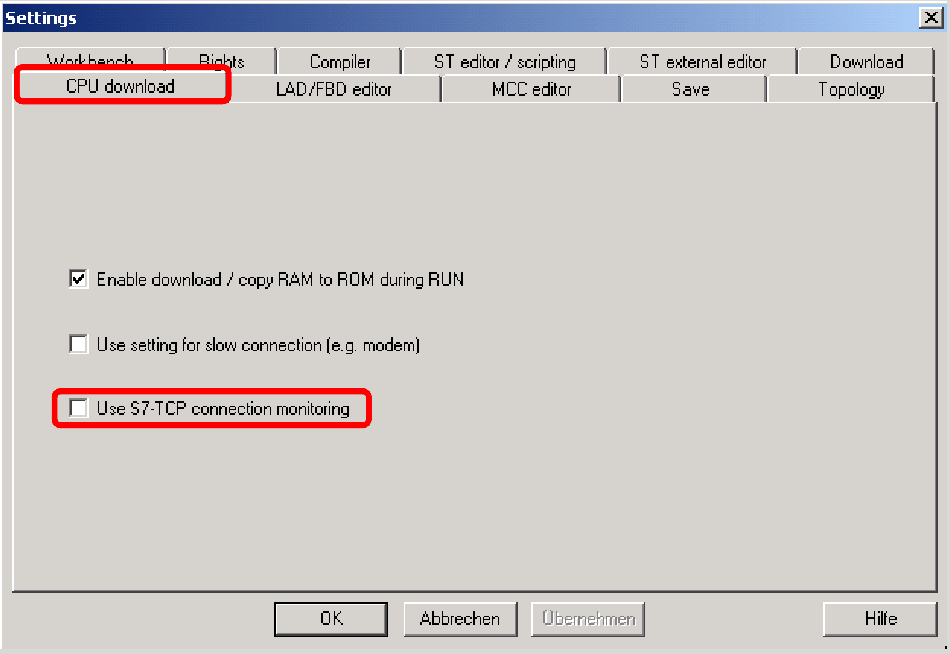
- The development tools from Siemens are using the so called S7 services (S7 communication) for establishing an online connection with SIMATIC CPUs, SIMOTION controllers and also SINAMICS drives. Therefore **TCP port 102** is needed.
- For establishing an online connection with a SIMOTION controller additionally **TCP port 5188** is needed.
- For accessing the web server of a SIMATIC CPU, SIMOTION controller or the web interface of a SCALANCE switch, **TCP port 80** and if necessary **TCP port 8080** is needed for HTTP connections. For secure HTTP connections (HTTPS) **TCP port 443** is needed.
- If the OPC XML DA server of a SIMOTION controller shall be accessed via the firewall, the same ports must be activated as for accessing the web server (**TCP port 80 / 8080 / 443**).
- FTP access requires **TCP port 21** and if necessary **TCP port 20**.
- For establishing an online connection with SINAMICS G120"-2" CUs (as from V4) via Ethernet the following ports must be activated in the firewall of the SCALANCE S6xx:
  - **UDP port 34964**
  - Range of the free **UDP ports from 49152 up to 65535**
  - **TCP port 102** is not needed!
- Access to Windows network share works are transacted over NetBIOS Services (**TCP port 139**) and Microsoft Directory Services (**TCP port 445**).
- For online connection monitoring the ICMP service `Echo request` (PING) is used from the development tools SIMOTION Scout and STARTER.

NOTE

The connection monitoring via the ICMP service `Echo Request` (PING) can be deactivated as from SIMOTION Scout V4.3 and STARTER V4.3.
In this case also the activation of this service in the firewall can be dropped.

For deactivation of the function in SIMOTION Scout respectively STARTER open the project settings using the menu entry `Options > Settings`.
Change to the `CPU download` tab and deactivate the option `Use S7-TCP connection monitoring`.

Figure 2-13 Deactivate connection monitoring



☑ Enable download / copy RAM to ROM during RUN

□ Use setting for slow connection (e.g. modem)

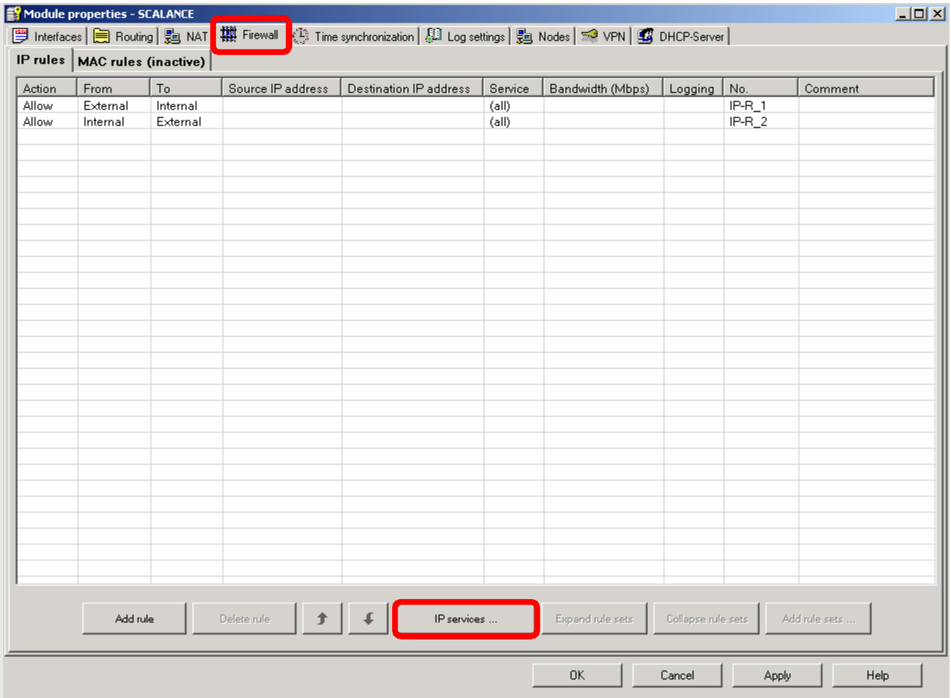
□ Use S7-TCP connection monitoring

2.6.1 Defining IP services

For the definition of the needed IP services open the properties of the SCALANCE S6xx in the project that you have already created in the `Security Configuration Tool (SCT)`.

Change to the `Firewall` tab afterwards.
Open the window for the definition of the IP services via the button `IP services`.

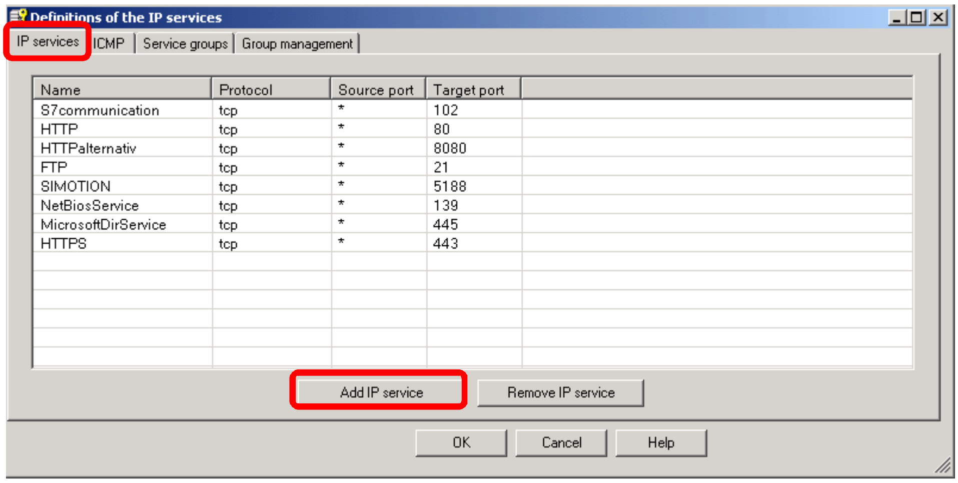
Figure 2-14 Firewall settings



Action	From	To	Source IP address	Destination IP address	Service	Bandwidth (Mbps)	Logging	No.	Comment
Allow	External	Internal			(all)			IP-R_1	
Allow	Internal	External			(all)			IP-R_2	

You can now add the needed IP services via the button `Add IP services` (see following example).

Figure 2-15 Defining IP services

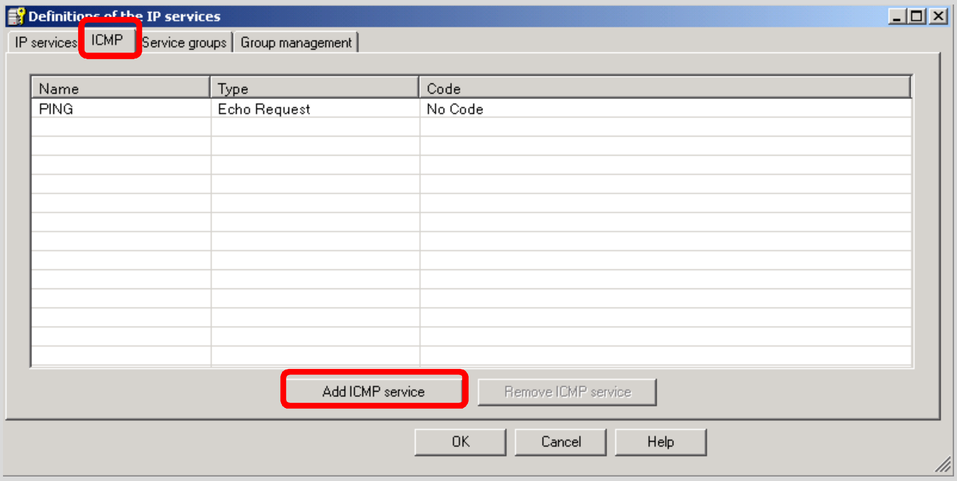


Name	Protocol	Source port	Target port
S7communication	tcp	*	102
HTTP	tcp	*	80
HTTPalternativ	tcp	*	8080
FTP	tcp	*	21
SIMOTION	tcp	*	5188
NetBiosService	tcp	*	139
MicrosoftDirService	tcp	*	445
HTTPS	tcp	*	443

NOTE

If you also want to activate the ICMP service `Echo Request` (PING) in the firewall of the SCALANCE S6xx, you can do this using the button `Add ICMP service` in the `ICMP` tab.

Figure 2-16 Defining ICMP services



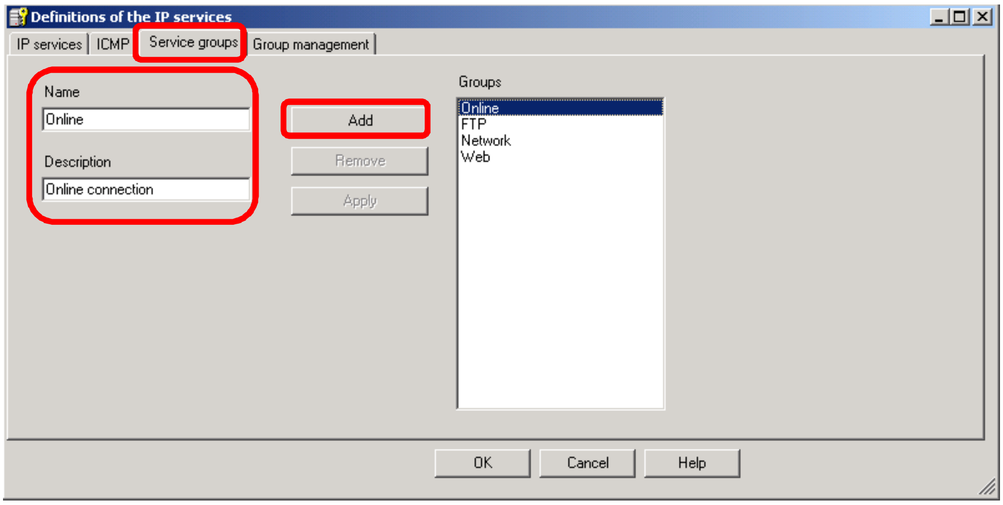
Name	Type	Code
PING	Echo Request	No Code

2.6.2 Creating service groups

For the purpose of clarity it is useful to summarize associated services in so called service groups, if a multiplicity of TCP and UPD ports has to be configured.

Therefore change to the `Service groups` tab and assign a new unique name as well as a description for the new service group.
You can add the service group to the group list via the button `Add`.

Figure 2-17 Creating service groups



Name: Online

Description: Online connection

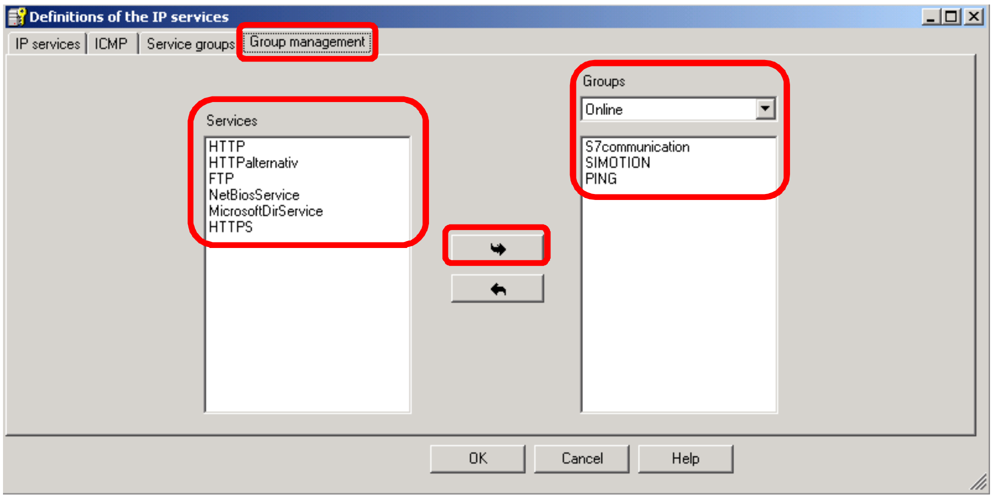
Groups:
Online
FTP
Network
Web

In the `Group management` tab you can afterwards add the IP respectively ICMP services defined before to the particular groups.

Therefore choose the desired service group in the drop-down menu on the right site. Afterwards select the particular service on the left site and add it to the group via the arrow keys.

In the example the services `S7communication` (**TCP port 102**), `SIMOTION` (**TCP port 5188**) as well as `PING` (**Echo Request**) were summarized in the service group named `Online`.

Figure 2-18 Group management



Services
HTTP
HTTPalternativ
FTP
NetBiosService
MicrosoftDirService
HTTPS

Groups
Online
S7communication
SIMOTION
PING

2.6.3 Creating firewall rules

With the IP and ICMP rules as well as the service groups defined before the firewall rules of the SCALANCE S6xx containing the particular source and destination addresses respectively address spaces must be defined.

Therefore open the properties of the SCALANCE S6xx and change to the `Firewall` tab. You can add a new firewall rule via the button `Add rule`.

NOTE

For every rule in the following example the particular IP address of the engineering computer of the company network, which shall have access to the machine network using the defined service, was added as source IP address.

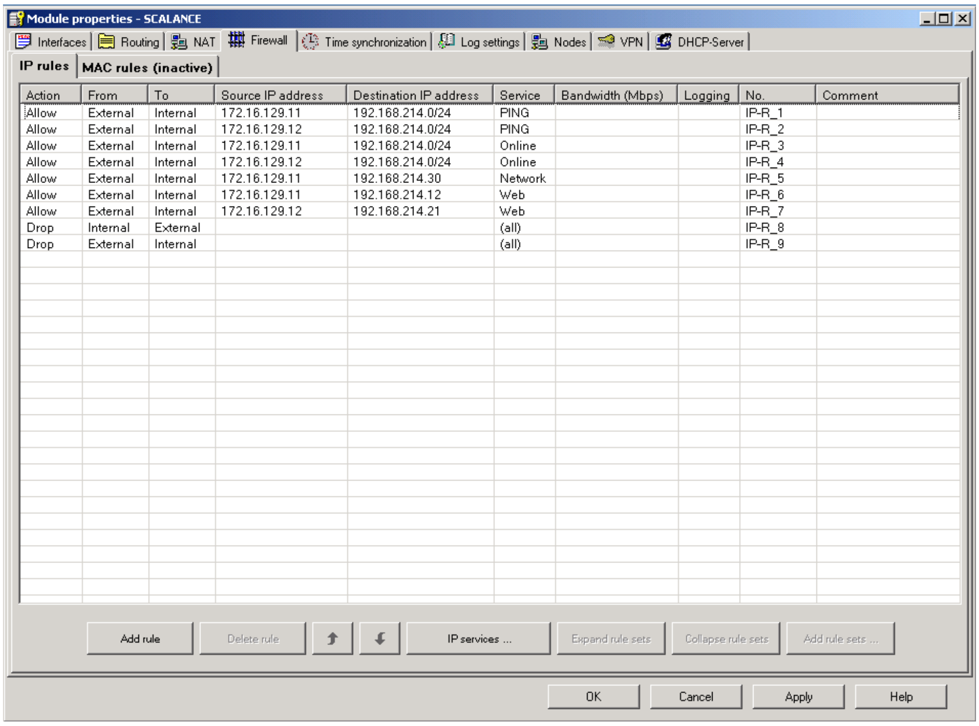
Accessing the machine network with this service will be refused for any other computer.

NOTE

The declaration of the direction **External → Internal** also admits the appropriate reply message in the opposite direction.

Therefore <u>no</u> additional firewall rules with the direction **Internal → External** must be defined!

Figure 2-19 Defined firewall rules



Action	From	To	Source IP address	Destination IP address	Service	Bandwidth (Mbps)	Logging	No.	Comment
Allow	External	Internal	172.16.129.11	192.168.214.0/24	PING			IP-R_1	
Allow	External	Internal	172.16.129.12	192.168.214.0/24	PING			IP-R_2	
Allow	External	Internal	172.16.129.11	192.168.214.0/24	Online			IP-R_3	
Allow	External	Internal	172.16.129.12	192.168.214.0/24	Online			IP-R_4	
Allow	External	Internal	172.16.129.11	192.168.214.30	Network			IP-R_5	
Allow	External	Internal	172.16.129.11	192.168.214.12	Web			IP-R_6	
Allow	External	Internal	172.16.129.12	192.168.214.21	Web			IP-R_7	
Drop	Internal	External			(all)			IP-R_8	
Drop	External	Internal			(all)			IP-R_9	

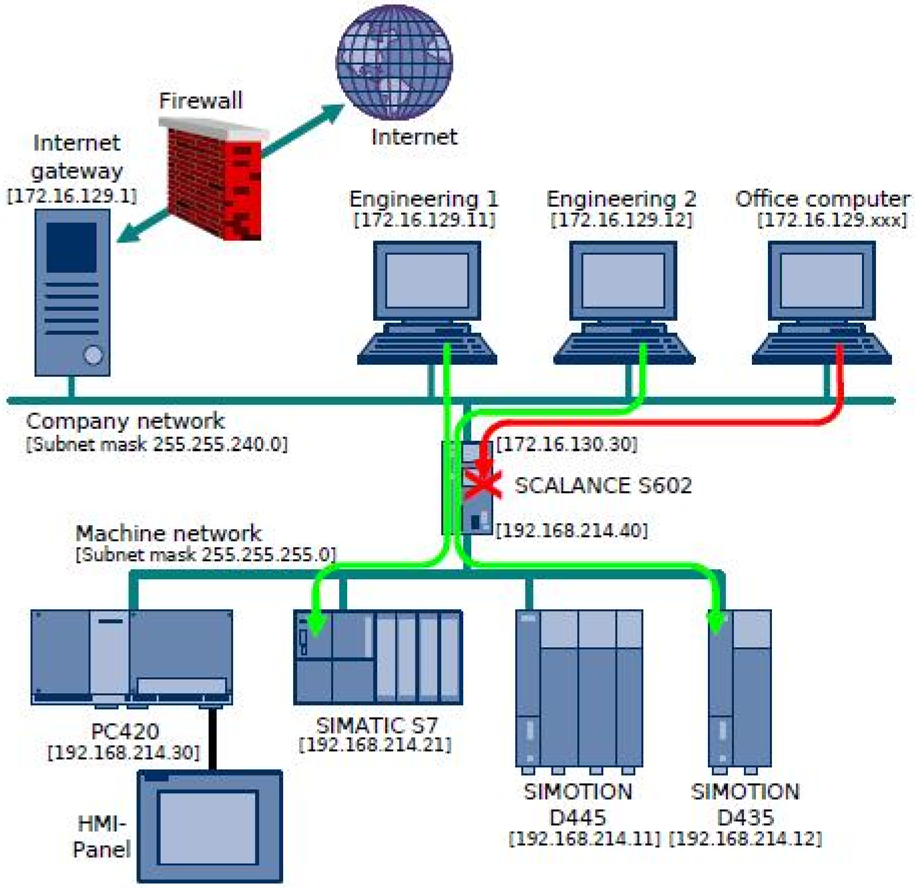
All incoming as well as outgoing telegrams in the SCALANCE S6xx (i.e. telegrams from the company and machine network) will be tested for validation from the firewall because of the defined rules.

Is the telegram applying to a rule of type `Allow` it will be forwarded by the SCALANCE S6xx. Otherwise the telegram will be dropped (rule of type `Drop`).

- The first two rules of the firewall authorize the engineering computers with the IP addresses `172.16.129.11` and `172.16.129.12` to address all stations in the machine network via the `ping` command. Addressing the stations via the `ping` command will be refused for any other computers.
- Rule 3 and 4 authorize the engineering computers with the IP addresses `172.16.129.11` and `172.16.129.12` to establish an online connection with all stations in the machine network. Establishing an online connection will be refused for any other computers.
- Rule 5 authorizes the engineering computer with the IP address `172.16.129.11` to access enabled network drives of the industrial computer in the machine network. Accessing the enabled network drives of the industrial computer will be refused for any other computer.
- Rule 6 authorizes the engineering computer with the IP address `172.16.129.11` to access the web server of the SIMOTION controller in the machine network. Rule 7 secures, that the engineering computer with the IP address `172.16.129.12` is allowed to access the web server of the SIMATIC CPU. Accessing the web server of the controllers will be refused for any other computer.
- The last two rules secure, that every other service, which is not explicit defined in the firewall rules, will be blocked from the SCALANCE S6xx (coming from internal as well as external).

2.7 Final layout with SCALANCE S6xx

Figure 2-20 Coupling of company and machine network with SCALANCE S6xx



The figure shows the coupling of the company and machine network via the SCALANCE S6xx. On the one hand the SCALANCE S6xx is used as firewall, on the other hand as router for the communication between the company and machine network.

The firewall rules defined on the device secure that only permitted engineering computers in the company network can access the stations in the machine network. Only the services needed for this purpose can pass the border between company and machine network, so that influences and errors in the company network cannot affect the machine network in a negative way and vice versa.

3 Further Notes, Tips and Tricks, etc.

3.1 Detection of protocol type and port number

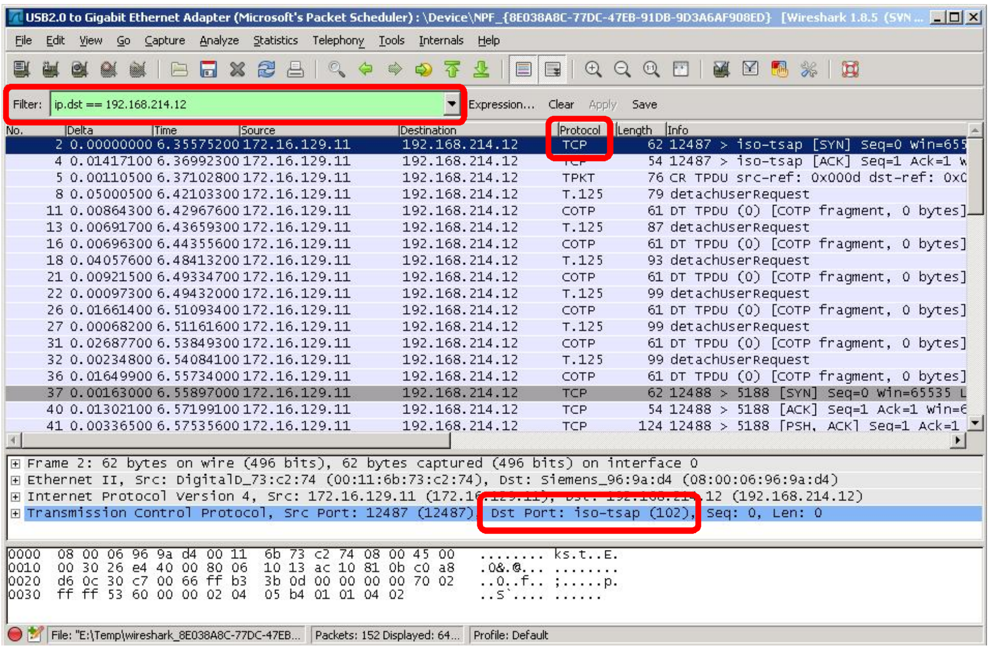
If the protocol type respectively the port number of a needed service is unknown it can be determined by recording the appropriate data communication. The usage of the open source program Wireshark is convenient for this purpose.

NOTE http://www.wireshark.org/download.html

Basic procedure:

8. Configure the SCALANCE S6xx only as router – all services are activated in the firewall.
9. Start the program Wireshark on the computer, where the service is carried out of which you want to determine the protocol type and port number.
   Record the incoming and outgoing data communication for the used Ethernet interface.
10. Carry out the desired service – e.g. addressing a station via the `ping` command or establishing an online connection via the development tools STEP7 SIMATIC Manager, SIMOTION Scout or STARTER.
11. Stop the record of the data communication and filter the recorded data packets, e.g. for the destination IP address of a particular station.
12. Generally the information, which protocol type (e.g. ICMP, UDP, TCP, etc.) and port number must be activated in the firewall of the SCALANCE S6xx for the desired service, can be quickly extracted from the recorded data communication.

Figure 3-1 Filtered data communication to destination IP address 192.168.214.12



USB2.0 to Gigabit Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{8E038A8C-77DC-47EB-91DB-9D3A6AF908ED} [Wireshark 1.8.5 (SVN ...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.dst == 192.168.214.12

No.	Delta	Time	Source	Destination	Protocol	Length	Info
2	0.00000000	6.35575200	172.16.129.11	192.168.214.12	TCP	62	12487 > iso-tsap [SYN] Seq=0 Win=655
4	0.01417100	6.36992300	172.16.129.11	192.168.214.12	TCP	54	12487 > iso-tsap [ACK] Seq=1 Ack=1 W
5	0.00110500	6.37102800	172.16.129.11	192.168.214.12	TPKT	76	CR TPDU src-ref: 0x000d dst-ref: 0x0
8	0.05000500	6.42103300	172.16.129.11	192.168.214.12	T.125	79	detachUserRequest
11	0.00864300	6.42967600	172.16.129.11	192.168.214.12	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
13	0.00691700	6.43659300	172.16.129.11	192.168.214.12	T.125	87	detachUserRequest
16	0.00696300	6.44355600	172.16.129.11	192.168.214.12	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
18	0.04057600	6.48413200	172.16.129.11	192.168.214.12	T.125	93	detachUserRequest
21	0.00921500	6.49334700	172.16.129.11	192.168.214.12	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
22	0.00097300	6.49432000	172.16.129.11	192.168.214.12	T.125	99	detachUserRequest
26	0.01661400	6.51093400	172.16.129.11	192.168.214.12	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
27	0.00068200	6.51161600	172.16.129.11	192.168.214.12	T.125	99	detachUserRequest
31	0.02687700	6.53849300	172.16.129.11	192.168.214.12	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
32	0.00234800	6.54084100	172.16.129.11	192.168.214.12	T.125	99	detachUserRequest
36	0.01649900	6.55734000	172.16.129.11	192.168.214.12	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
37	0.00163000	6.55897000	172.16.129.11	192.168.214.12	TCP	62	12488 > 5188 [SYN] Seq=0 Win=65535 L
40	0.01302100	6.57199100	172.16.129.11	192.168.214.12	TCP	54	12488 > 5188 [ACK] Seq=1 Ack=1 Win=6
41	0.00336500	6.57535600	172.16.129.11	192.168.214.12	TCP	124	12488 > 5188 [PSH, ACK] Seq=1 Ack=1

```
⊞ Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: DigitalD_73:c2:74 (00:11:6b:73:c2:74), Dst: Siemens_96:9a:d4 (08:00:06:96:9a:d4)
⊞ Internet Protocol Version 4, Src: 172.16.129.11 (172.16.129.11), Dst: 192.168.214.12 (192.168.214.12)
⊞ Transmission Control Protocol, Src Port: 12487 (12487), Dst Port: iso-tsap (102), Seq: 0, Len: 0
```

```
0000  08 00 06 96 9a d4 00 11  6b 73 c2 74 08 00 45 00   ........ ks.t..E.
0010  00 30 26 e4 40 00 80 06  10 13 ac 10 81 0b c0 a8   .0&.@... ........
0020  d6 0c 30 c7 00 66 ff b3  3b 0d 00 00 00 00 70 02   ..0..f.. ;.....p.
0030  ff ff 53 60 00 00 02 04  05 b4 01 01 04 02         ..S`.... ......
```

File: "E:\Temp\wireshark_8E038A8C-77DC-47EB... | Packets: 152 Displayed: 64... | Profile: Default

By means of the figure above it can be well realized, that online connections using the development tools STEP7 SIMATIC Manager, SIMOTION Scout or STARTER are always established via the **TCP port 102**.

NOTE

Further information regarding this topic you will find using following links:

- “TCP ports required for access to SIMOTION / SINAMICS”
  http://support.automation.siemens.com/WW/view/en/35680316
- “Which ports are used for the various services for data transfer by means of TCP and UDP and what should you watch out for when using routers and firewalls?”
  http://support.automation.siemens.com/WW/view/en/8970169

NOTE

A list with all usual ports and the appropriate services you will find using following link:

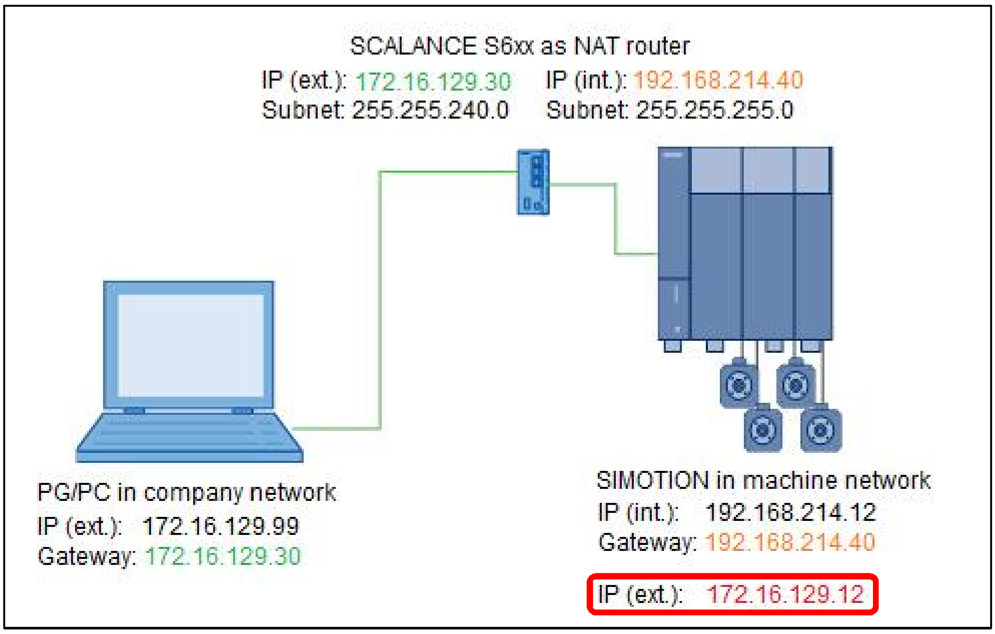
http://www.iana.org/assignment/port-numbers

3.2 Use the alternative access point (DEVICE)

The development tools SIMOTION Scout and STARTER command a second alternative access point named `DEVICE` beside the access point `S7ONLINE`.
The alternative access point opens up the possibility to use an address for the device that is independent from the configured address in the HW configuration for establishing an online connection.

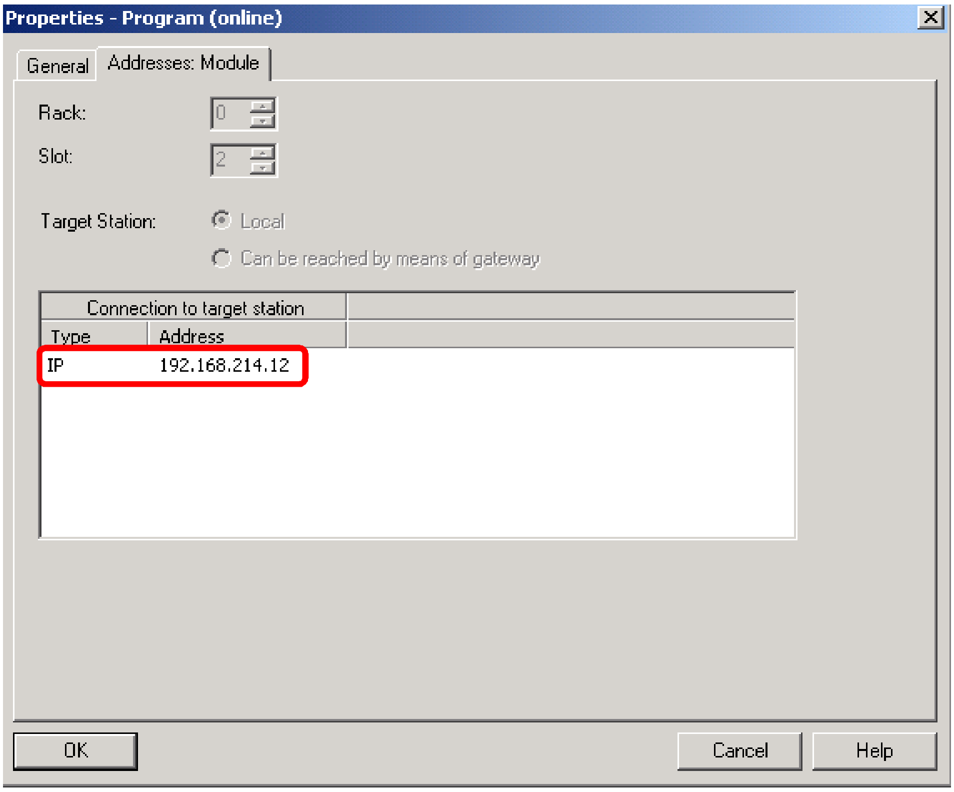
If for example the NAT functionality of a SCALANCE S6xx is used, a free IP address in the internal network (network of port 2) is dedicated to a free IP address in the external network (network of port 1) via which the particular device can be accessed from the external way.

Figure 3-2 Example for 1:1 NAT routing



In case of the previous example the IP address `192.168.214.12` has been configured in the HW configuration of the SIMOTION controller. For the access point `S7ONLINE` this IP address is permanently adjusted and can only be changed via adapting the HW configuration.

Figure 3-3 Properties access point S7ONLINE



Properties - Program (online)

Rack: 0

Slot: 2

Target Station: ● Local
○ Can be reached by means of gateway

Connection to target station	
Type	Address
IP	192.168.214.12

Because of the SCALANCE S6xx is used as NAT router the engineering computer is located in another IP subnet then the SIMOTION controller. Therefore the engineering computer cannot establish an online connection with the controller. This is the reason why the alternative access point `DEVICE` must be used now. For the SIMOTION controller the IP address `172.168.129.12` is adjusted there, which is located in the same IP subnet than the engineering computer. The development tool is using the alternative IP address for establishing an online connection. The necessary IP conversion is done by the SCALANCE S6xx that has been configured in an appropriate way before.

NOTE

Information regarding the configuration of a SCALANCE S6xx as NAT router as well as example configurations for this topic you will find in the manual “SIMATIC NET Industrial Ethernet Security Basics and application” in chapter 5.1.3 ff. using following link:

http://support.automation.siemens.com/WW/view/en/67437017

Setting up access point DEVICE

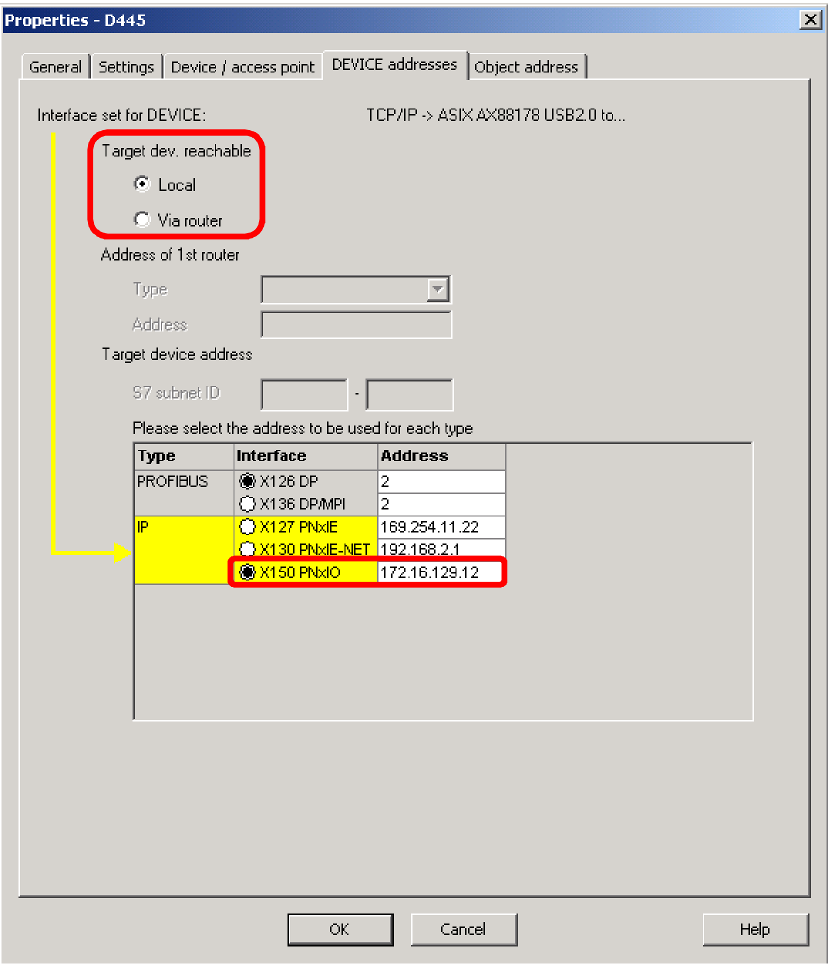
Select the particular device in the project tree of the development tool and open its properties via `right click > Properties` for setting up the access point `DEVICE`. Change to the `Device/access point` tab and choose the access point `DEVICE`.

You will reach the properties of the access point by using the link `Set DEVICE addresses`. Choose the way the device is reachable: local or via router.

NOTE You only have to choose the option `Via router` if the device is connected to another device (except router) and if two different interfaces of the same type (e.g. Ethernet to Ethernet) or two interfaces of different types (e.g. Ethernet to PROFIBUS) are located on the way between the engineering computer and the target device.

For the adjustment `Local` you have to choose the type (e.g. IP) as well as the used interface of the device an online connection shall be established with (e.g. PN interface X150). Assign the external IP address to the array `Address` the device can be reached with.

Figure 3-4 Properties of the access point DEVICE



Interface set for DEVICE: TCP/IP -> ASIX AX88178 USB2.0 to...

Target dev. reachable

● Local

○ Via router

Address of 1st router

Type

Address

Target device address

S7 subnet ID -

Please select the address to be used for each type

Type	Interface	Address
PROFIBUS	● X126 DP	2
	○ X136 DP/MPI	2
IP	○ X127 PNxIE	169.254.11.22
	○ X130 PNxIE-NET	192.168.2.1
	● X150 PNxIO	172.16.129.12