

SIEMENS

Ingenuity for life



SCALANCE XM-400 / XR-500 as Static NAT Router

SCALANCE XM-400, SCALANCE XR-500

<https://support.industry.siemens.com/cs/ww/en/view/109762688>

Siemens
Industry
Online
Support



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

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

The customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase the customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <http://www.siemens.com/industrialsecurity>.

Contents

1	Introduction	3
1.1	Network Address Translation	3
1.2	NAT Function in SCALANCE XM-400 / XR-500	5
2	Task and Solution	7
3	Configuration	9
3.1	Preparation	9
3.2	Configuration via the Web Based Management	11
3.2.1	Preparation	11
3.2.2	Create VLANs	11
3.2.3	Define the IP Interface.....	15
3.2.4	Configure Static NAT.....	17
3.3	Configuration via the Command Line Interface.....	21
3.3.1	Preparation.....	21
3.3.2	Create VLANs	23
3.3.3	Define the IP Interface.....	27
3.3.4	Configure Static NAT.....	28
4	Operation	31

1 Introduction

1.1 Network Address Translation

Network Address Translation (abbreviation: NAT) was specified in the 1990s and is described in the RFC 1631 among others.

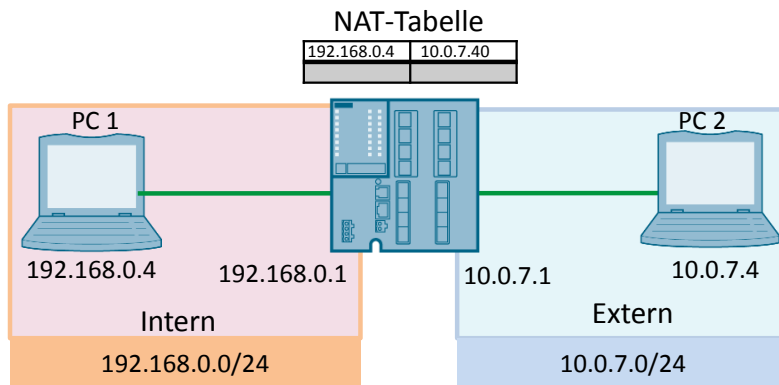
The main motivation for developing NAT was the shortage of public IPv4 addresses and the possibility of using private addressing in distinct network areas. NAT permits you to separate private and public network areas.

Brief description

NAT is a method in IP routers of replacing one IPv4 address in a data packet with another IPv4 address. This permits two different networks (internal and external) to be connected with each other.

If a data packet exceeds the network limit between an inside and an outside network, the router exchanges the IP addresses accordingly. To replace the IP addresses a translation table (NAT table) is stored in the IP router.

Figure 1-1



Translation options

In the context of address translation, the terms NAT and NAPT (Network Address Port Translation) are used in parallel. Technically speaking, the two procedures differ as follows:

- With NAT, an IPv4 address is replaced 1:1 by another IPv4 address. A difference is made between Source NAT, in which the source IP address is translated, and Destination NAT, in which the destination IP address is translated. Both variants can also be used.
- NAPT is an n:1 translation. With NAPT, multiple IPv4 addresses share a single IPv4 address after translation. But port numbers are used here to achieve exact assignment of the data packets.

Note

In this example we use the static, bidirectional NAT procedure.

Advantages

You have the following advantages when using the NAT function:

- You can hide the IP addresses on industrial networks or on the outside.

- The IP address range can be used by multiple connected private networks without any address collisions.
- With Source NAT you can restrict outgoing data packets to specific IP addresses, IP address ranges and specific interfaces. These rules can also be used on VPN connections.
- Despite cross-subnet communication you do not have to enter a router IP address in the terminal devices.

1.2 NAT Function in SCALANCE XM-400 / XR-500

The SCALANCE XM-400 and SCALANCE XR-500 are IP routers and support the NAT mechanism.

Network separation

With the NAT function, the IP addresses of one subnetwork are translated into IP addresses of another subnetwork.

For this, in SCALANCE, IP interfaces are used, each of which has been configured as a virtual IP interface of a VLAN.

Terminology

In the NAT configuration in SCALANCE XM-400 or SCALANCE XR-500, the subnetworks are divided into "Inside" and "Outside". The division is done from the perspective of a NAT interface.

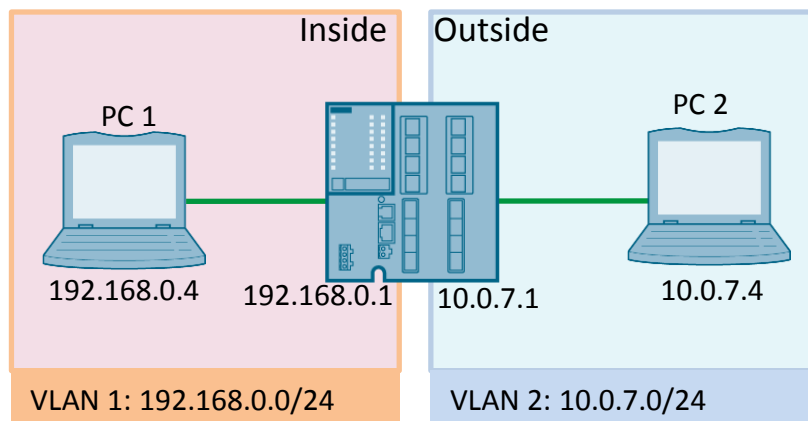
All networks that can be accessed themselves via the NAT interface are considered to be "Outside" for this interface.

All networks that can be accessed via other IP interfaces of the same device are considered to be "Inside" for this NAT interface.

In the following example we have two IP subnetworks connected together via a SCALANCE XM-400. PC 1 is to communicate via NAT with PC 2. The IP networks are divided as follows from the perspective of the NAT interface "10.0.7.1":

- VLAN 2: Outside
- VLAN 1: Inside

Figure 1-2



If routing takes place via a NAT interface, the source or destination IP addresses of the transferred data packets are changed at the transition between "Inside" and "Outside".

The direction of the communication determines whether the source or the destination IP address is changed. It is always the IP address of the communications user on the "Inside" that is changed.

Perspective

Depending on the perspective, the IP address of a communications user is designated "Local" or "Global".

Table 1-1

		Perspective	
		Local	Global
Position	Inside	A real IP address that is assigned to a device in the internal network. This address cannot be accessed from the external network.	An IP address via which an internal device can be accessed from the external network.
	Outside	A real IP address that is assigned to a device in the external network. Since only "Inside" addresses are translated, no difference is made between Outside Local and Outside Global.	

Note

The NAT function is implemented as a software function in the SCALANCE XM-400 and SCALANCE XR-500 and has a restricted bandwidth of 1.2 Mbit. Therefore the entire NAT communication runs via the CPU in the SCALANCE XM-400 and SCALANCE XR-500 and is in competition with the IP communication that goes to the CPU, WBM and Telnet, for example.

Be aware that a large part of the computing capacity is occupied when you use NAT. This means that access via Telnet or WBM might be slower.

It is for this reason that the NAT function is best suited for just a few addresses and small volumes of data. It is recommended to use a SCALANCE S615 or SC-600 for high-performance applications.

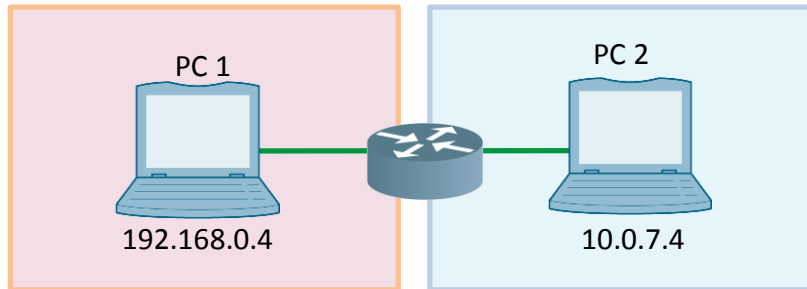
2 Task and Solution

Outset

The outset for the configuration described in [chapter 3](#) is defined as follows:

Two PCs are to communicate bidirectionally. The PCs are in different IP subnetworks.

Figure 2-1



The NAT procedure is to be used instead of routing to enable communication between the PCs.

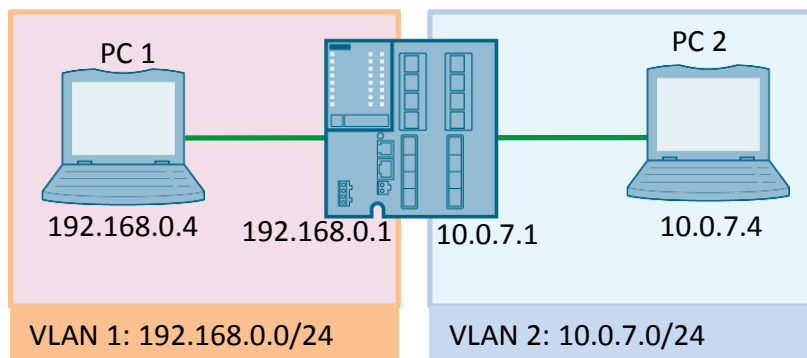
Solution

To connect the two different IP subnetworks with each other, a SCALANCE XM408-8C (article number: 6GK5408-8GR00-2AM2) is placed between the PCs and the NAT function is activated in the SCALANCE.

A static, bidirectional IP address translator is used.

Each IP subnetwork is mapped in the SCALANCE XM408-8C as an IP interface that is configured as a virtual IP interface of a VLAN. The ports with which the SCALANCE with each of the IP subnetworks is connected are assigned to the corresponding VLAN.

Figure 2-2



To enable bidirectional communication both IP interfaces in the SCALANCE (192.168.0.1 and 10.0.7.1) are configured as a NAT interface.

From the perspective of the NAT interface "10.0.7.1" on the SCALANCE XM408-8C, PC 1 is in the "Inside" position and PC 2 in the "Outside" position.

From the perspective of the NAT interface "192.168.0.1" on the SCALANCE XM408-8C, PC 2 is in the "Inside" position and PC 1 in the "Outside" position.

A NAT table in the SCALANCE XM408-8C ensures that

- The IP address of PC 1 is translated into an IP address from the network of PC 2 in VLAN 2.
- The IP address of PC 2 is translated into an IP address from the network of PC 1 in VLAN 1.

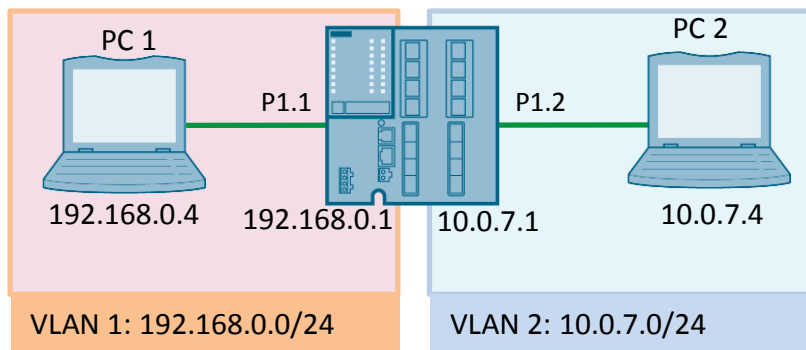
3 Configuration

3.1 Preparation

Overview

The following figure shows the IP addresses, VLANs and virtual IP interfaces used for this configuration.

Figure 3-1



NAT-Tabelle

Inside Local	Inside Global
192.168.0.4	10.0.7.44
10.0.7.4	192.168.0.44

Install and connect the PCs

A PC is placed in each subnetwork to demonstrate the NAT functionality.

Assign the following IP addresses to the PCs:

- PC 1: 192.168.0.4
- PC 2: 10.0.7.4

Connect the PCs with the SCALANCE XM408-8C as follows:

- PC 1 with Port 1.1 of the SCALANCE
- PC 2 with Port 1.2 of the SCALANCE

Factory settings

Reset the SCALANCE to the factory settings to make sure that the function of the example is not impaired by older configurations or settings.

Refer to the manual of the module for instructions about resetting to factory settings.

Note

When you reset the SCALANCE to factory settings, all the settings and IP addresses are lost.

IP address

In order to configure the SCALANCE via the Web Based Management (abbreviation: WBM) or via the Command Line Interface (abbreviation: CLI) the module needs an IP address.

Assign the management IP address "192.168.0.1" to the SCALANCE.

Since PC 1 is in the same IP subnetwork as the management IP address of the SCALANCE, you use PC 1 for assigning the IP address.

You can use the STEP 7 function "Edit Ethernet Node..." or the Primary Setup Tool (PST), for example, to assign an IP address.

Configuration options

This example shows you two options for configuring the SCALANCE XM408-8C:

- Web Based Management
- Command Line Interface

Follow the instructions in [section 3.2](#) to configure the SCALANCE using the Web Based Management.

Follow the instructions in [section 3.3](#) to configure the SCALANCE using the Command Line Interface.

Configuration steps

Proceed as follows to configure the SCALANCE XM408-8C for operation as a NAT router:

- Create VLANs
- Define virtual IP interface
- Activate NAT
- Install static NAT

These configuration steps apply to configuration via the WBM and via the CLI.

3.2 Configuration via the Web Based Management

3.2.1 Preparation

To configure the SCALANCE via the Web Based Management you open an internet browser on PC 1 and in the address line you enter the IP address of the SCALANCE: <https://192.168.0.1>.

If you have reset the SCALANCE to factory settings, you log on with the following data:

- User: admin
- Password: admin

You are requested to assign a new password. Follow the instructions and create a new password.

When you have changed the password, then the home page of the Web Based Management is displayed.

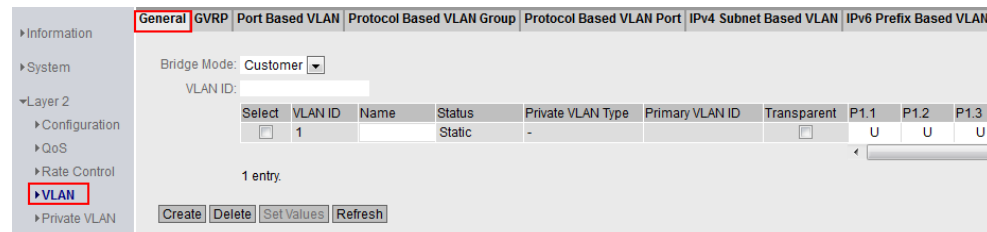
3.2.2 Create VLANs

At least two IP interfaces are needed for the NAT function, each of which is configured as a virtual IP interface of a VLAN. The management VLAN (VLAN 1) and the associated virtual IP interface are present by default, you have to create a second VLAN and also create a new virtual IP interface for that VLAN. The new VLAN becomes VLAN 2.

Open the VLAN menu

In the navigation area you go to the menu "Layer 2 > VLAN" to enter a new VLAN. You make all the settings in the "General" tab.

Figure 3-2

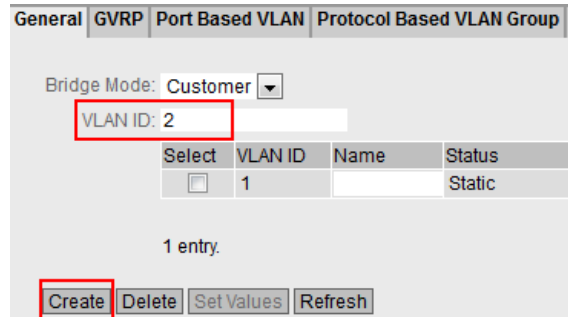


Add a new VLAN

Proceed as follows to add a new VLAN:

1. Enter an ID in the "VLAN ID" input field. Use the number "2" as ID for the VLAN 2. Click the "Create" button.

Figure 3-3



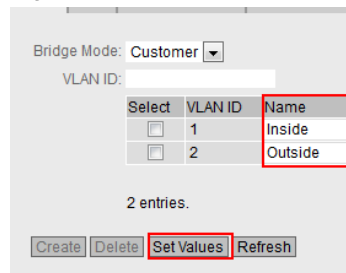
2. A new entry is created in the table. The port fields are occupied by default with "-" so that no port is assigned to the new VLAN.

Figure 3-4

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Transparent	P1.1	P1.2	P1.3
<input type="checkbox"/>	1		Static	-		<input type="checkbox"/>	U	U	U
<input type="checkbox"/>	2		Static	-		<input type="checkbox"/>	-	-	-

3. You can enter a name for the VLANs in the "Name" column if you wish. Click the "Set Values" button.

Figure 3-5



Define port properties

In the default setting, all the ports are always assigned to VLAN 1 (management VLAN) and have PVID 1. Therefore these ports have the ID "U".

In the next step you define how the properties of the two ports P1.1 and P1.2 are to be configured in the VLANs.

To change the properties of a port you click in the corresponding table cell and select the desired item from the drop-down list box. Refer here to the screenshot:

Figure 3-6

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Transparent	P1.1	P1.2	P1.3	P1.4	P1.5	P1.6	P1.7	P1.8
<input type="checkbox"/>	1	Inside	Static	-		<input type="checkbox"/>	U	-	-	-	-	-	-	-
<input type="checkbox"/>	2	Outside	Static	-		<input type="checkbox"/>	-	u	-	-	-	-	-	-

The following options are used in this example:

- "-": The port is not a member of the specified VLAN.
- "U" (uppercase letter): The port is an untagged member of the VLAN and has the corresponding PVID. Messages are sent from this port without VLAN tag and incoming packets are tagged with the VLAN ID.
- "u" (lowercase letter): The port is an untagged member of the VLAN. Messages are sent from this port without VLAN tag. The PVID has not yet been set for this port.

Set port VID

The messages sent from the normal PCs reach the SCALANCE XM408-8C without VLAN tag.

With the Port VID (abbreviation: PVID) settings you define per port which VLAN ID is to be assigned to these messages. Because the default setting is already set to VLAN 1, in this example you only have to make the PVID setting for port P1.2.

Proceed as follows to make the PVID setting for port P1.2:

1. Switch to the "Port Based VLAN" tab.
To assign a VLAN ID to port P1.2 you click in the corresponding table cell and select "VLAN 2" from the drop-down list box.

Figure 3-7

General		GVRP	Port Based VLAN	Protocol Based VLAN Group	Protocol Based VLAN Port	IPv4 Subnet Base
All ports		Priority	Port VID	Acceptable Frames	Ingress Filtering	
		No Change	No Change	No Change	No Change	
Port	Priority	Port VID	Acceptable Frames	Ingress Filtering		
P1.1	0	VLAN1	All			
P1.2	0	VLAN1	All			
P1.3	0	VLAN1	All			
P1.4	0	VLAN2	All			
P1.5	0	VLAN1	All			

2. Then click the "Set Values" button.

Figure 3-8

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering	
P1.1	0	VLAN1	All		<input type="checkbox"/>
P1.2	0	VLAN2	All		<input type="checkbox"/>
P1.3	0	VLAN1	All		<input type="checkbox"/>
P1.4	0	VLAN1	All		<input type="checkbox"/>
P1.5	0	VLAN1	All		<input type="checkbox"/>
P1.6	0	VLAN1	All		<input type="checkbox"/>
P1.7	0	VLAN1	All		<input type="checkbox"/>
P1.8	0	VLAN1	All		<input type="checkbox"/>
P2.1	0	VLAN1	All		<input type="checkbox"/>
P2.2	0	VLAN1	All		<input type="checkbox"/>
P2.3	0	VLAN1	All		<input type="checkbox"/>
P2.4	0	VLAN1	All		<input type="checkbox"/>
P2.5	0	VLAN1	All		<input type="checkbox"/>
P2.6	0	VLAN1	All		<input type="checkbox"/>
P2.7	0	VLAN1	All		<input type="checkbox"/>
P2.8	0	VLAN1	All		<input type="checkbox"/>
P3.1	0	VLAN1	All		<input type="checkbox"/>
P3.2	0	VLAN1	All		<input type="checkbox"/>
P3.3	0	VLAN1	All		<input type="checkbox"/>
P3.4	0	VLAN1	All		<input type="checkbox"/>
P3.5	0	VLAN1	All		<input type="checkbox"/>
P3.6	0	VLAN1	All		<input type="checkbox"/>
P3.7	0	VLAN1	All		<input type="checkbox"/>
P3.8	0	VLAN1	All		<input type="checkbox"/>

Set Values Refresh

3.2.3 Define the IP Interface

The SCALANCE has a virtual IP interface of a VLAN for each adjacent subnetwork. Two subnetworks are needed in this example (Inside and Outside). Therefore the SCALANCE needs two IP interfaces.

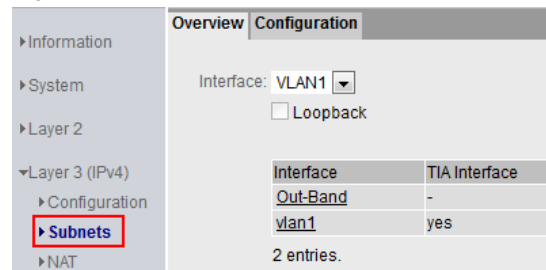
In [section 3.2.2](#) you have created the basis for another subnetwork by creating another VLAN (VLAN 2).

Since the management VLAN (VLAN 1) and the associated virtual IP interface are present by default, you have to create a new virtual IP interface for VLAN 2.

Open the Subnets menu

In the navigation area you switch to the menu "Layer 3 (IPv4) > Subnets" to create a virtual IP interface and assign it an IP address of a subnetwork.

Figure 3-9

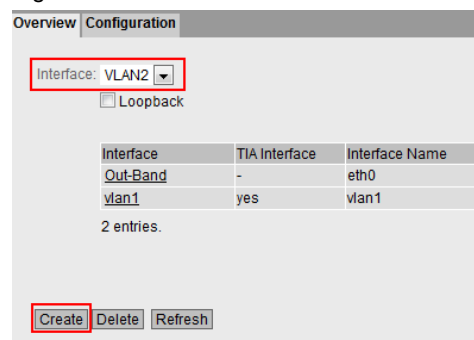


Create an IP interface for a VLAN

You can add a new virtual IP interface in the "Overview" tab.

To create another virtual IP interface you open the "Interface" drop-down list box and select "VLAN 2". Then you click the "Create" button.

Figure 3-10



Another item is added to the interface table and shows the newly created IP interface with the subnetwork that has not yet been configured.

Figure 3-11

Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type
	Out-Band	-	eth0	20-87-56-0c-4c-3d	0.0.0.0	0.0.0.0	Primary
	vlan1	yes	vlan1	20-87-56-0c-4c-00	192.168.0.1	255.255.255.0	Primary
<input type="checkbox"/>	vlan2	-	vlan2	20-87-56-0c-4c-00	0.0.0.0	0.0.0.0	Primary

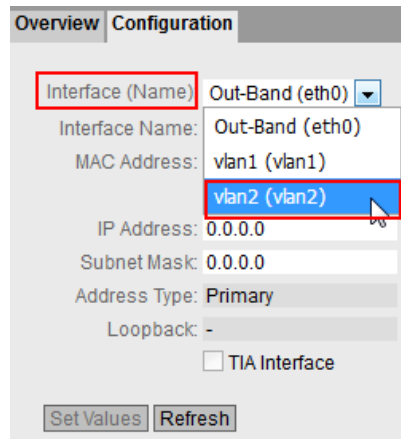
Configure the IP address of the virtual IP interface

You configure the IP address for the new virtual IP interface in the "Configuration" tab.

Proceed as follows to configure the IP address.

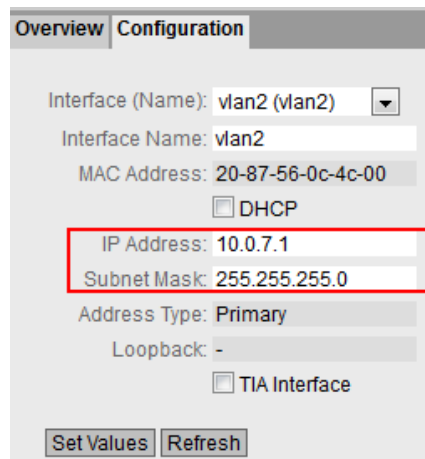
1. Open the "Interface (Name)" drop-down list box and select "VLAN 2".

Figure 3-12



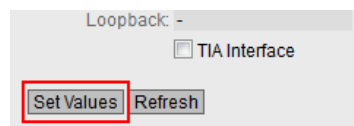
2. In the "IP Address" input field you enter the IP address "10.0.7.1" and in the "Subnet Mask" input field you enter the subnet mask "255.255.255.0".

Figure 3-13



3. Then click the "Set Values" button.

Figure 3-14

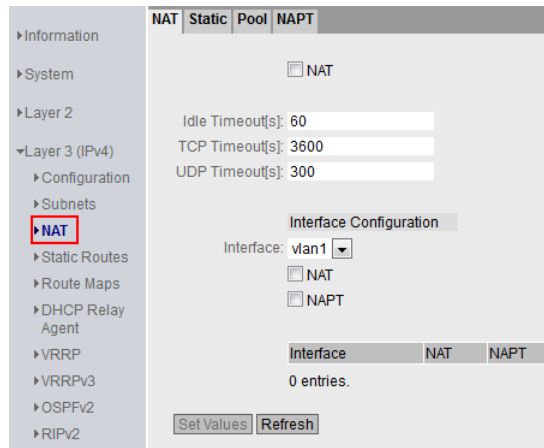


3.2.4 Configure Static NAT

Open the NAT menu

In the navigation area you go to the menu "Layer 3 > (IPv4) > NAT" to use the NAT function.

Figure 3-15



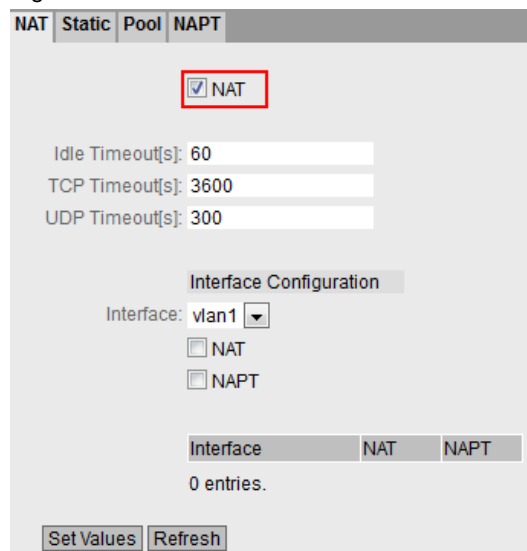
Activate NAT

In the "NAT" tab you can activate the NAT function globally for the device and define the NAT interfaces. When the NAT function has been activated globally for the device and the NAT interfaces have been defined, the device operates as a NAT router.

Proceed as follows to activate the NAT function.

1. Enable the "NAT" option to operate SCALANCE as a NAT router:

Figure 3-16



- To define the interface "192.168.0.1" (VLAN 1) as NAT interface you open the "Interface" drop-down list box and select "VLAN 1".
Activate NAT for the interface "192.168.0.1" (VLAN 1) by enabling the "NAT" option.

Then click the "Set Values" button.

Figure 3-17

The screenshot shows the NAT configuration page with tabs for NAT, Static, Pool, and NAPT. The NAT tab is active. There are input fields for Idle Timeout (60s), TCP Timeout (3600s), and UDP Timeout (300s). Under 'Interface Configuration', the 'Interface' dropdown is set to 'vlan1'. The 'NAT' checkbox is checked, and the 'NAPT' checkbox is unchecked. Below this is a table with columns 'Interface', 'NAT', and 'NAPT', currently showing '0 entries'. At the bottom, the 'Set Values' button is highlighted with a red box.

- An item is added to the table.
To operate the interface "10.0.7.1" (VLAN 2) as NAT interface you open the "Interface" drop-down list box and select "VLAN 2".
Activate NAT for the interface "10.0.7.1" (VLAN 2) by enabling the "NAT" option.

Then click the "Set Values" button.

Figure 3-18

The screenshot shows the NAT configuration page. The 'Interface' dropdown is now set to 'vlan2'. The 'NAT' checkbox is checked, and the 'NAPT' checkbox is unchecked. The table below now shows '1 entry' for 'vlan1' with 'NAT' checked and 'NAPT' unchecked. At the bottom, the 'Set Values' button is highlighted with a red box.

- Another item is added to the table.

Figure 3-19

Interface	NAT	NAPT
vlan1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
vlan2	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Note

If you have configured multiple NAT interfaces on a device, a network is "Outside" from the perspective of one NAT interface and "Inside" from the perspective of another NAT interface.

Install static NAT

To enable bidirectional communication across subnetwork boundaries the SCALANCE needs a translation table (NAT table) for the IP addresses.

In the "Static" tab you configure the static 1:1 address translations. You define the Inside Global address into which the Inside Local address of a device is to be translated and vice versa.

In this example the NAT table is filled in as follows:

Table 3-1

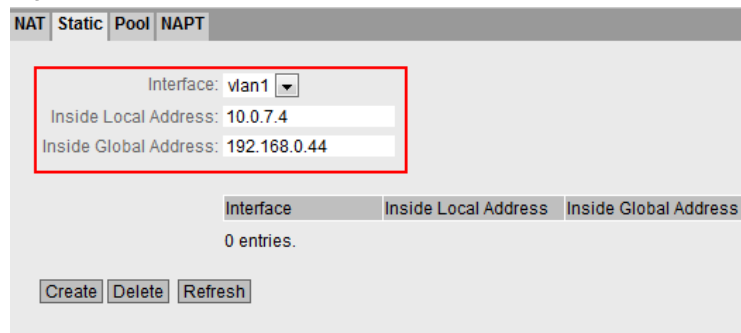
	Inside Local	Inside Global
PC 1	192.168.0.4	10.0.7.44
PC 2	10.0.7.4	192.168.0.44

Proceed as follows to define the static address translation for the NAT interface "192.168.0.1":

1. Open the "Interface" drop-down list box and select the NAT interface "VLAN 1". VLAN 2 is "Inside" from the perspective of this NAT interface. In the "Inside Local Address" input field you enter the real IP address of PC 2 ("10.0.7.4").

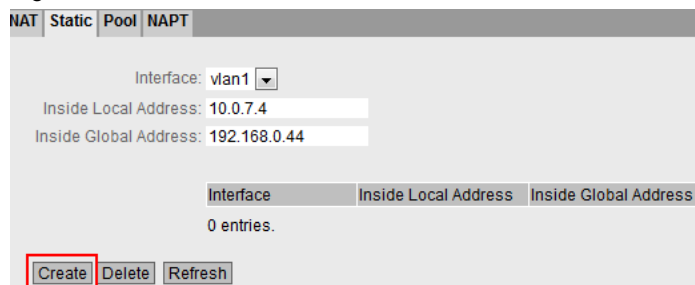
In the "Inside Global Address" input field you enter the IP address of PC 2 under which PC 2 is to be accessible from outside ("192.168.0.44").

Figure 3-20



2. Click the "Create" button.

Figure 3-21



3. A new entry is created in the table.

Figure 3-22

	Interface	Inside Local Address	Inside Global Address
<input type="checkbox"/>	vlan1	10.0.7.4	192.168.0.44

Proceed as follows to define the static address translation for the NAT interface "10.0.7.1":

1. Open the "Interface" drop-down list box and select the NAT interface "VLAN 2". VLAN 1 is "Inside" from the perspective of this NAT interface. In the "Inside Local Address" input field you enter the real IP address of PC 1 ("192,168.0.4").

In the "Inside Global Address" input field you enter the IP address of PC 1 under which PC 1 is to be accessible from outside ("10.0.7.44").

Figure 3-23

The screenshot shows the NAT configuration interface with the 'Static' tab selected. The 'Interface' dropdown is set to 'vlan2'. The 'Inside Local Address' field contains '192.168.0.4' and the 'Inside Global Address' field contains '10.0.7.44'. Below the form is a table with one entry for 'vlan1'.

	Interface	Inside Local Address	Inside Global Address
<input type="checkbox"/>	vlan1	10.0.7.4	192.168.0.44

1 entry.

Buttons: Create, Delete, Refresh

2. Click the "Create" button.

Figure 3-24

The screenshot shows the NAT configuration interface with the 'Static' tab selected. The 'Interface' dropdown is set to 'vlan2'. The 'Inside Local Address' field contains '192.168.0.4' and the 'Inside Global Address' field contains '10.0.7.44'. The 'Create' button is highlighted with a red box.

	Interface	Inside Local Address	Inside Global Address
<input type="checkbox"/>	vlan1	10.0.7.4	192.168.0.44

1 entry.

Buttons: Create, Delete, Refresh

3. A new entry is created in the table.

Figure 3-25

	Interface	Inside Local Address	Inside Global Address
<input type="checkbox"/>	vlan1	10.0.7.4	192.168.0.44
<input type="checkbox"/>	vlan2	192.168.0.4	10.0.7.44

Note

You have completed the configuration of the NAT function. An option for testing the NAT function is given in [chapter 4](#).

3.3 Configuration via the Command Line Interface

3.3.1 Preparation

Setting up a connection

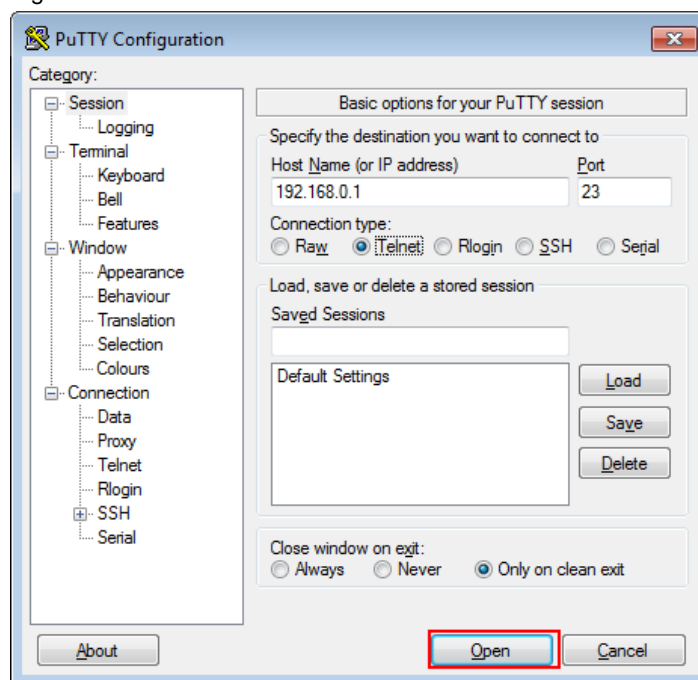
You need a terminal program to configure the SCALANCE using the Command Line Interface. You can use the function integrated in Windows, a different terminal program or the serial console cable.

In this example the free tool PuTTY is used.

Proceed as follows to establish a connection to the SCALANCE XM408-8C:

1. Start PuTTY and enter the IP address of the SCALANCE XM408-8C. Select the required protocol, "SSH", for example.
2. Click the "Open" button to start the connection.

Figure 3-26



If you have reset the SCALANCE to factory settings, you log on with the following data:

- User: admin
- Password: admin

You are requested to assign a new password. Follow the instructions and create a new password.

When you have changed the password and have logged on successfully, you get the following input prompt: "CLI#".

Note

In the following configurations it is assumed that you are logged in as "admin". With that login you are automatically in the "Privileged EXEC mode" and have extended access authorization.

Open the Global Configuration mode

In the Global Configuration mode you can make the basic configuration settings. Furthermore, in this mode you can call other modes for the configuration of special interfaces or functions, for the configuration of a VLAN, for instance.

You get to the Global Configuration mode by entering the following command in the Privileged EXEC mode:

```
CLI# configure terminal
```

The following input prompt is displayed: "CLI(config)#".

Quit the Global Configuration mode

Enter the following command to quit the Global Configuration mode:

```
CLI(config)# end
```

The following input prompt is displayed: "CLI#".

3.3.2 Create VLANs

At least two IP interfaces are needed for the NAT function, each of which is configured as a virtual IP interface of a VLAN. The management VLAN (VLAN 1) and the associated virtual IP interface are present by default, you have to create a second VLAN and also create a new virtual IP interface for that VLAN. The new VLAN becomes VLAN 2.

Outset

You are in the Global Configuration mode.

The following input prompt is displayed: "CLI(config)#".

Add a new VLAN

To add a new VLAN (in this case: VLAN 2), you call the "vlan" command as follows and press the Enter key:

```
CLI(config)# vlan 2
```

The VLAN is created and you are automatically in the VLAN configuration mode.

The following input prompt is displayed: "CLI(config-vlan-2)#".

Assigning a name

To assign the new VLAN a name (in this case: VLAN2), you call the "name" command as follows and press the Enter key:

```
CLI(config-vlan-2)# name VLAN2
```

The name "VLAN2" is assigned to the VLAN.

Define port properties

In the next step you define how the properties of the two ports P1.1 and P1.2 are to be configured in the VLANs.

You define the port properties as follows:

Table 3-2

Port	VLAN	Identifier
P1.1	VLAN 1	Untagged member
P1.2	VLAN 2	Untagged member

Assign port P1.2 to VLAN 2

In order to incorporate port P1.2 as untagged member in VLAN 2 you call the "ports" command as follows and press the Enter key:

```
CLI(config-vlan-2)# ports gi 1/2 untagged gi 1/2
```

Note:

"gi" is the abbreviation for "gigabitethernet" and describes the interface type.

To quit the configuration mode of VLAN 2 you call the following command and press the Enter key:

```
CLI(config-vlan-2)# exit
```

The following input prompt is displayed: "CLI(config)#".

Set port VID settings

The messages sent from the normal PCs reach the SCALANCE XM408-8C without VLAN tag.

With the Port VID (abbreviation: PVID) settings you define per port which VLAN ID is to be assigned to these messages. Because the default setting is already set to VLAN 1, in this example you only have to make the PVID setting for port P1.2.

You open the configuration mode of the P1.2 interface by calling the "interface" command as follows and then pressing the Enter key:

```
CLI(config)# interface gi 1/2
```

The following input prompt is displayed: "CLI(config-if-Gi1-2)#".

To set the PVID setting for port P1.2 you call the "switchport" command as follows and then press the Enter key:

```
CLI(config-if-Gi1-2)# switchport pvid 2
```

To quit the configuration mode of interface P1.2 you call the following command and press the Enter key:

```
CLI(config-if-Gi1-2)# exit
```

The following input prompt is displayed: "CLI(config)#".

View the VLAN configuration

To check the VLAN configuration you can use the "show" command to have the configuration displayed.

To view the VLAN configuration from the Global Configuration mode you call the "do show" command as follows and then press the Enter key:

```
CLI(config)# do show vlan
```

The VLAN configuration is displayed.

Figure 3-27

```
Vlan database
-----
Vlan ID      : 2
Member Ports : Gi1/2
Untagged Ports : Gi1/2
Forbidden Ports : None
Name         : VLAN2
Status      : Permanent
-----
Vlan ID      : 1
Member Ports : Gi1/1
Untagged Ports : Gi1/1
Forbidden Ports : None
Name         :
Status      : Permanent
-----
```

You see the following information:

- Port 1.2 is assigned to VLAN 2 as only member. The port is "untagged" and has the PVID 2.
- Port 1.1 is assigned to VLAN 1 as only member. The port is "untagged" and has the PVID 1.

To view the PVID settings you call the "do show" command as follows and then press the Enter key:

```
CLI(config)# do show vlan port config
```

Figure 3-28

```
Vlan Port configuration table
-----
Port Gi1/1
Port Vlan ID           : 1
Port Acceptable Frame Type : Admit All
Port Ingress Filtering  : Disabled
Port Mode               : Hybrid
Port Gvrp Status        : Enabled
Port Gmrp Status        : Enabled
Port Gvrp Failed Registrations : 0
Gvrp last pdu origin    : 00:00:00:00:00:00
Port Restricted Vlan Registration : Disabled
Port Restricted Group Registration : Disabled
Mac Based Support       : Disabled
Subnet Based Support    : Enabled
Port-and-Protocol Based Support : Enabled
Default Priority        : 0
Dot1x Protocol Tunnel Status : Peer
LACP Protocol Tunnel Status : Peer
Spanning Tree Tunnel Status : Peer
GVRP Protocol Tunnel Status : Peer
GMRP Protocol Tunnel Status : Peer
IGMP Protocol Tunnel Status : Peer
Filtering Utility Criteria : Default
Port Protected Status   : Disabled
-----
Port Gi1/2
Port Vlan ID           : 2
Port Acceptable Frame Type : Admit All
Port Ingress Filtering  : Disabled
Port Mode               : Hybrid
Port Gvrp Status        : Enabled
Port Gmrp Status        : Enabled
Port Gvrp Failed Registrations : 0
Gvrp last pdu origin    : 00:00:00:00:00:00
Port Restricted Vlan Registration : Disabled
```

You see that the PVID setting for port P1.2 is configured on VLAN ID 2. All incoming packets at port P1.2 are tagged with the VLAN ID 2.

3.3.3 Define the IP Interface

The SCALANCE has a virtual IP interface of a VLAN for each adjacent subnetwork. Two subnetworks are needed in this example (Inside and Outside). Therefore the SCALANCE needs two IP interfaces.

In [section 3.3.2](#) you have created the basis for another subnetwork by creating another VLAN (VLAN 2).

Since the management VLAN (VLAN 1) and the associated virtual IP interface are present by default, you have to create a new virtual IP interface for VLAN 2.

Outset

You are in the Global Configuration mode.

The following input prompt is displayed: "CLI(config)#".

Create an IP interface for a VLAN

To create another virtual IP interface for VLAN 2 you have to switch to the configuration mode of the VLAN 2 interface.

You open the configuration mode of the VLAN 2 interface by calling the "interface" command as follows and then pressing the Enter key:

```
CLI(config)# interface vlan 2
```

The following input prompt is displayed: "CLI(config-if-vlan-2)#".

To configure an IP address for the new virtual IP interface you call the "ip address" command as follows and then press the Enter key:

```
CLI(config-if-vlan-2)# ip address 10.0.7.1 255.255.255.0
```

To quit the configuration mode of VLAN interface you call the following command and press the Enter key:

```
CLI(config-if-vlan-2)# exit
```

The following input prompt is displayed: "CLI(config)#".

3.3.4 Configure Static NAT

Outset

You are in the Global Configuration mode.

The following input prompt is displayed: "CLI(config)#".

Activate NAT

You can use the "ip nat" command to activate the NAT function globally for the device. When the NAT function has been activated globally for the device and the NAT interfaces have been defined, the device operates as a NAT router.

To activate the NAT function you call the "ip nat" command as follows and then press the Enter key:

```
CLI(config)# ip nat
```

If you want to operate the interface "192.168.0.1" (VLAN 1) as NAT interface you have to switch to the configuration mode of the VLAN 1 interface.

You open the configuration mode of the VLAN 1 interface by calling the "interface" command as follows and then pressing the Enter key:

```
CLI(config)# interface vlan 1
```

The following input prompt is displayed: "CLI(config-if-vlan-1)#".

To activate NAT for this VLAN interface you call the "ip nat" command as follows and then press the Enter key:

```
CLI(config-if-vlan-1)# ip nat
```

To quit the configuration mode of the VLAN interface you call the following command and press the Enter key:

```
CLI(config-if-vlan-1)# exit
```

The following input prompt is displayed: "CLI(config)#".

If you want to operate the interface "10.0.7.1" (VLAN 2) as NAT interface you have to switch to the configuration mode of the VLAN 2 interface.

You open the configuration mode of the VLAN 2 interface by calling the "interface" command as follows and then pressing the Enter key:

```
CLI(config)# interface vlan 2
```

The following input prompt is displayed: "CLI(config-if-vlan-2)#".

To activate NAT for this VLAN interface you call the "ip nat" command as follows and then press the Enter key:

```
CLI(config-if-vlan-2)# ip nat
```

To quit the configuration mode of the VLAN interface you call the following command and press the Enter key:

```
CLI(config-if-vlan-2)# exit
```

The following input prompt is displayed: "CLI(config)#".

Note

If you have configured multiple NAT interfaces on a device, a network is "Outside" from the perspective of one NAT interface and "Inside" from the perspective of another NAT interface.

Install static NAT

To enable bidirectional communication across subnetwork boundaries the SCALANCE needs a translation table (NAT table) for the IP addresses.

You configure the static 1:1 address translation in the corresponding configuration mode of the NAT interface. You define the Inside Global address into which the Inside Local address of a device is to be translated and vice versa.

In this example the NAT table is filled in as follows:

Table 3-3

	Inside Local	Inside Global
PC 1	192.168.0.4	10.0.7.44
PC 2	10.0.7.4	192.168.0.44

If you want to define static address translation for the NAT interface "192.168.0.1"

(VLAN 1) you have to switch to the configuration mode of the VLAN 1 interface.

You open the configuration mode of the VLAN 1 interface by calling the "interface" command as follows and then pressing the Enter key:

```
CLI(config)# interface vlan 1
```

The following input prompt is displayed: "CLI(config-if-vlan-1)#".

If you want to define static address translation for the IP interface "192.168.0.1" you call the "ip nat static" command as follows and then press the Enter key:

```
CLI(config-if-vlan-1)# ip nat static 10.0.7.4 192.168.0.44
```

To quit the configuration mode of the VLAN interface you call the following command and press the Enter key:

```
CLI(config-if-vlan-1)# exit
```

The following input prompt is displayed: "CLI(config)#".

If you want to operate the interface "10.0.7.1" (VLAN 2) as NAT interface you have to switch to the configuration mode of the VLAN 2 interface.

You open the configuration mode of the VLAN 2 interface by calling the "interface" command as follows and then pressing the Enter key:

```
CLI(config)# interface vlan 2
```

The following input prompt is displayed: "CLI(config-if-vlan-2)#".

If you want to define static address translation for the IP interface "10.0.7.1" you call the "ip nat static" command as follows and then press the Enter key:

```
CLI(config-if-vlan-2)# ip nat static 192,168.0.4 10.0.7.44
```

To quit the configuration mode of the VLAN interface you call the following command and press the Enter key:

```
CLI(config-if-vlan-2)# exit
```

The following input prompt is displayed: "CLI(config)#".

View the NAT configuration

To check the global NAT configuration and the static address translation you can use the "show" command to have the configurations displayed.

To view the global NAT configuration from the Global Configuration mode you call the "do show" command as follows and then press the Enter key:

```
CLI(config)# do show ip nat config
```

The global NAT configuration is displayed.

Figure 3-29

```
NAT Configuration
-----
NAT Status           : Enabled
Maximum Translation Entries : 1000
Start Free Port      : 6001
Idle Timeout         : 60 seconds
TCP Timeout          : 3600 seconds
UDP Timeout          : 300 seconds
```

To view the address translation you call the "do show" command as follows and then press the Enter key:

```
CLI(config)# do show ip nat static
```

The static address translation table is displayed.

Figure 3-30

```
Static Address Mapping
-----
Outside   Inside   Inside
Interface Local IP   Global IP
-----
vlan1     10.0.7.4   192.168.0.44
vlan2     192.168.0.4 10.0.7.44
```

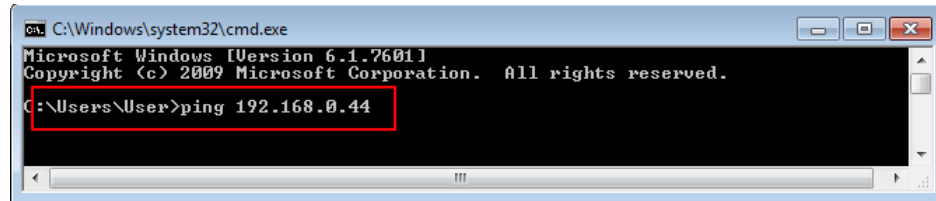
4 Operation

The simplest way of testing the NAT function is the PING command.

Proceed as follows to test the communication between PC 1 and PC 2:

1. Open the console window on PC 1.
2. From the PC 1 perspective PC 2 is accessible via the IP address "192.168.0.44". Enter the command "ping 192.168.0.44" and press the Enter key.

Figure 4-1

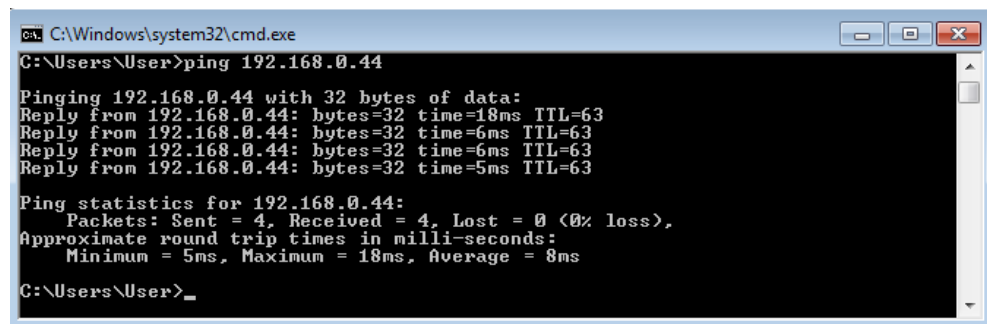


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>ping 192.168.0.44
```

3. You see the result of the PING command in plain text. If PC 2 is accessible, PC 2 responds to the PING command and the statistics show no lost packet.

Figure 4-2



```
C:\Windows\system32\cmd.exe
G:\Users\User>ping 192.168.0.44

Pinging 192.168.0.44 with 32 bytes of data:
Reply from 192.168.0.44: bytes=32 time=18ms TTL=63
Reply from 192.168.0.44: bytes=32 time=6ms TTL=63
Reply from 192.168.0.44: bytes=32 time=6ms TTL=63
Reply from 192.168.0.44: bytes=32 time=5ms TTL=63

Ping statistics for 192.168.0.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 18ms, Average = 8ms

C:\Users\User>_
```

Note

To test the communication from PC 2 to PC 1, you open the console window on PC 2 and enter the command "ping 10.0.7.44".