ConneXium
Ethernet Cabling System Switch Management Manual

Version 4.0

31005844 00

a brand of Schneider Electric

Telemecanique

Table of Contents

Safety Information

Important Information

Notice

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

⚠ The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

⚠ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER
DANGER indicates an imminently hazardous situation, which, if not avoided, **will result** in death, serious injury, or equipment damage.

⚠ WARNING
WARNING indicates a potentially hazardous situation, which, if not avoided, **can result** in death, serious injury, or equipment damage.

⚠ CAUTION
CAUTION indicates a potentially hazardous situation, which, if not avoided, **can result** in injury or equipment damage.

Please Note

Electrical equipment should be serviced only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material. This document is not intended as an instruction manual for untrained persons.

About the Book

At a Glance

Document Scope

Schneider Electric provides a complete family of products with uniform management from Fiber/Electrical interfaces for fieldbus systems through Ethernet transceivers, hubs, switches, and Fast Ethernet ConneXium switches. This manual covers firmware SV:5.2 for the 499NES17100 and 499NOS17100 ConneXium managed switches.

Validity Note

The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

Product Related Warnings

Schneider Electric assumes no responsibility for any errors that may appear in this document. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric. All rights reserved. Copyright 2004.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When controllers are used for applications with technical safety requirements, please follow the relevant instructions.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this product related warning can result in injury or equipment damage.

User Comments

We welcome your comments about this document. You can reach us by e-mail at TECHCOMM@modicon.com

Introduction

1

At a Glance

Overview

Schneider Electric provides a complete line of innovative Ethernet products to support real-time and high availability Ethernet architectures. ConneXium is a family of products with uniform management from fiber/electrical interfaces for fieldbus systems through Ethernet transceivers, hubs, and switches through ConneXium fast Ethernet switches.

This manual covers firmware SV:5.2 for the 499NES17100 and 499NOS17100 ConneXium managed switches.

What's in this Chapter?

This chapter contains the following topics:

Industrial Networking Solutions with a Future

Overview

Underpinning trends in automation technology and process control is a move toward open, transparent system solutions. These rely increasingly on Open PLC control with either Ethernet or Intranet access. The most important standards are TCP/IP communications protocols, Ethernet network structures and Modbus as the industrial application protocol standard. Schneider Electric currently provides these solutions through its Transparent Ready products targeted at the industrial automation and electrical distribution markets.

Although the Ethernet standard used in automation technology is the same as that used in offices, the requirements for network products are considerably different. In day-to-day industrial applications, networks are expected to work reliably under extreme conditions, such as electromagnetic interference, high operating temperatures and mechanical loads.

Availability

This ConneXium fast Ethernet switch family was specifically designed for use in industrial automation applications taking all these requirements into consideration. In order to meet these challenges, Schneider Electric provides the redundant "Ethernet Ring," which ensures continual production operation even while the network is being reconfigured. The "Ethernet Ring" also allows networks to be maintained and expanded while still in operation. Since the system is reconfigured in a matter of milliseconds, the "Ethernet Ring" is considerably faster than the 'spanning tree' algorithm, which only meets the needs of office systems.

The "Ethernet Ring" and other concepts ensure ultimate network and production system reliability. Our highly integrated family of Ethernet products allow you to adapt your network to the specific geographical layout and security-related considerations at any time. This scalability also ensures the network will meet all future requirements.

Features

General features include:

- High temperature range, permitting new fields of application
- Quick assembly (the rugged devices are simply mounted on a standard DIN Rail)
- Easy access plug connections, together with extensive status displays help save time during installation.

The ConneXium Fast Ethernet Switches

Overview

Created from the start as mission-critical switches, Schneider Electric's Fast Ethernet ConneXium switches benefit from no single point of network failure, either physically or logically, when configured in a "single ring" topology. Incorporating high levels of resilience as standard, the switches create an inherently "bulletproof" Ethernet network.

Depending on how important the process application is, the level of resilience in the overall network can be matched to meet further continuity requirements. For example, where a controller has dual redundant network interface cards, each card could connect to separate switches on the same resilient fiber ring or, if double redundancy is needed, a second ring could be added.

The Fast Ethernet ConneXium NxS switches allow you to configure medium to large sized deterministic Ethernet/Fast Ethernet networks easily and cost-effectively. An important feature of these NxS switches is the fast media redundancy. The failure of a transmission path will be recognized in less than 500 ms and the switch will divert data to a redundant path. You can activate this function via dip switches on any switch. This Schneider Electric NxS switch ensures ultimate network and system reliability. This function can also be used, for example, to expand existing networks while they are still in operation.

NxS switches also contain an SNMP management agent and integrated web-based management. These features provide you with simple, easy-to-use configuration functions for fast installation and setup. Extensive network and device information also contribute to ultimate system reliability.

An NxS switch is a compact, heavy-duty device suitable for industrial applications which can be installed on a standard DIN Rail. It has five twisted pair ports (10/100 Mbps auto-negotiation) and two ports (100 Mbps) available as twisted pair, or multi-mode fiber optic.

The 24 V operating voltage is supplied via a plug-in terminal block and can also be configured for redundancy. An additional contact in the terminal block allows you to read in status messages directly. Integrated LEDs allow fast on-site installation and troubleshooting.

Hardware

2

At a Glance

Overview

The ConneXium Fast Ethernet switch NxS family consists of two devices. These devices can be managed and have the same functions. They are differentiated by their interfaces for connecting segments:

- 499NES17100 - Electrical ConneXium switch
- 499NOS17100 - Optical ConneXium switch

For the sake of simplicity, these two devices have been designated as NxS in this manual.

What's in this Chapter?

This chapter contains the following topics:

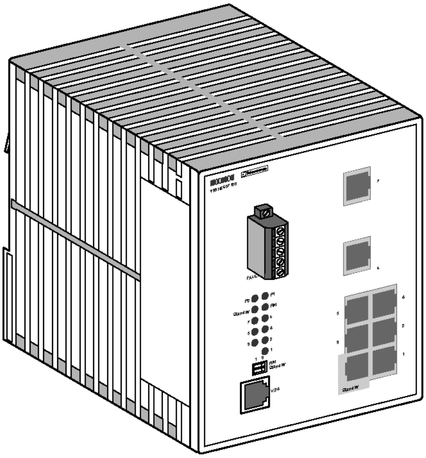
ConneXium Switch 499NES17100

Description

The ConneXium 499NES17100 dual-speed switch provides seven shielded twisted pair interfaces. It allows you to connect up to five independent shielded-and-foiled twisted-pair (SFTP) segments (10BASE-T/100BASE-TX) and up to two independent SFTP segments (100 BASE-TX).

Front View of 499NES17100

The figure below shows the front view of the 499NES17100.



499NES17100 Basics

The 499NES17100 operates in store-and-forward mode. When a data packet is being received, the 499NES17100 analyzes the source and target address. It can store up to 2000 addresses with port allocations in its address table.
The 499NES17100 conforms to the specifications of the standards ISO/IEC 8802-3 (10BASE-T) and ISO/IEC 8802-3u (100BASE-TX).
The LED indicates data reception, connection status and processor status.

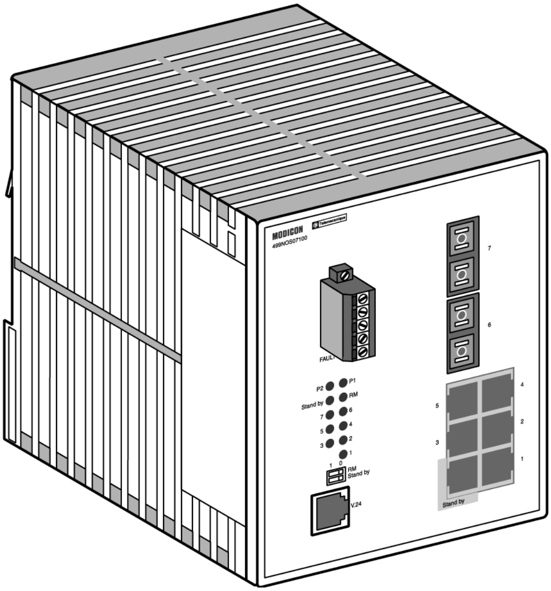
ConneXium Switch 499NOS17100

Description

The ConneXium fast Ethernet switch 499NOS17100 is a switch with five shielded twisted pair interfaces and two F/O interfaces. It makes it possible to connect up to five independent shielded-and-foiled twisted-pair (STP) segments (10BASE-T/ 100BASE-TX) and up to two independent fiber optic segments (100BASE-FX).

Front View of 499NOS17100

The figure below shows the front view of the 499NOS17100.



499NOS17100 Basics

The 499NOS17100 operates in the store-and-forward mode. When a data packet is being received, the 499NOS17100 analyzes the source and target address. It can store up to 2000 addresses with port allocations in its address table.
The 499NOS17100 conforms to the specifications of ISO/IEC 8802-3 100BASE-FX and ISO/IEC 8802-3 (10BASE-T) and ISO/IEC 8802-3u (100BASE-TX).
The LED indicate data reception, connection status and processor status.

Installation and Startup Procedure

3

At a Glance

Overview

The ConneXium fast Ethernet switch NxS family has been developed for practical application in a harsh industrial environment. Accordingly, the installation process has been kept simple. The few configuration settings required for operation are described in this chapter.

What's in this Chapter?

This chapter contains the following topics:

Security Instructions

Supply Voltage

The devices are designed for operation with a safety extra-low voltage. Thus, they may only be connected to the supply voltage connections and to the signal contact with the safety extra-low voltages (SELV) in compliance with IEC950/ EN60950/ VDE0805.
The supply voltage is electrically isolated from the housing.

⚠ **WARNING**

Potential injury or damage to equipment

Never start operation with damaged components!

Failure to follow this precaution can result in death, serious injury, or equipment damage.

Shielding Ground

The shielding ground of the connectable twisted pairs lines is connected to the front panel as a conductor.

⚠ **CAUTION**

Potential injury or damage to equipment

Beware of possible short circuits when connecting a cable section with conductive shielding braiding.

Failure to follow this precaution can result in injury or equipment damage.

Housing

Only technicians authorized by Schneider Electric are permitted to open the housing.
The device is grounded via the separated ground screw. It is located on the left under the front panel.

- Make sure that the electrical installation meets local or nationally applicable safety regulations.
- The ventilation slits must not be covered to ensure free air circulation.
- The device may be operated exclusively in switchgear cabinets with energy-limited power sources.

Ambient Conditions

The device may only be operated in an ambient temperature of 0°C to +55°C at a relative air humidity of 10% to 90% (non-condensing).

Qualification Requirements for Personnel

Qualified personnel as understood in this manual and the warning signs, are persons who are familiar with the setup, assembly, startup, and operation of this product and are appropriately qualified for their job. This includes, for example, people who have been

- trained, directed, or authorized to switch on and off and ground and label power circuits and devices or systems in accordance with current safety engineering standards;
- trained or directed in the care and use of appropriate safety equipment in accordance with the current standards of safety engineering; and
- trained in providing first aid.

Device Installation

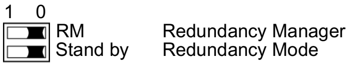
Controls

The standby function can be switched on and off with the two-pin DIP switch on the front panel of the NxS.
State on delivery: switch position 0 (Off), i.e., normal operation. For redundant coupling of 10/100 Mbit/s segments, the NxS is operated in the redundant sections in standby mode.
The RM functionality (Redundancy Manager) can be switched on or off with the RM switch. State on delivery: Switch position 0 (Off), i.e., RM function not active.

Note: Activate just one of the two functions: standby or RM. Activating both functions simultaneously causes the device to be reset.

Two-Pin DIP Switch

The figure below shows the two-pin DIP switch.



Matching RM Requirements

Check the RM/Standby requirements.

Step	Action
1	Check whether the switch setting matches your requirements.

Five-Pin Terminal Block

The supply voltage and the fault contact are connected via a five-pin terminal block with screw locking.

⚠ **WARNING**

SELV must be observed.

The NxS devices are designed for operation with safety extra-low voltage. Correspondingly, they may only be connected to the supply voltage connections and to the signal contact with the safety extra-low voltages (SELV) in compliance with IEC950/ EN60950/ VDE0805.

Failure to follow this precaution can result in death, serious injury, or equipment damage.

Supply Voltage

The supply voltage can be connected redundantly. Both inputs are decoupled. There is no distributed load. With redundant supply, the transformer supplies the NxS alone with the higher output voltage. The supply voltage is electrically isolated from the housing.

Fault Contact

The fault contact monitors proper functioning of the NxS, thus enabling remote diagnostics. A break in contact is reported via the zero-potential fault contact (relay contact, closed circuit). A break may be caused by:

- the failure of at least one of the two supply voltages;
- a continuous malfunction in the NxS (internal 3.3 VDC voltage, supply voltage 1 or 2 < 18 V, ...);
- the defective link status of at least one port. With the NxS, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition;
- error during self-test.

The following conditions are reported in standby mode:

- Control cable disrupted
- Control cable short-circuited
- Partner device is in standby mode

The following conditions are reported in normal mode:

- Control cable short-circuited
- Partner device is in normal mode

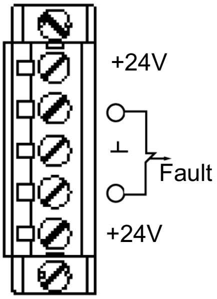
The following conditions are reported in RM mode:

- Ring monitoring is not possible, e.g. during software initialization.

Note: With non-redundant supply of the mains voltage, the NxS reports a power failure. You can prevent this message by applying the supply voltage over the two inputs.

Pin Assignments

The figure below describes the pin assignment of the five-pin terminal block.



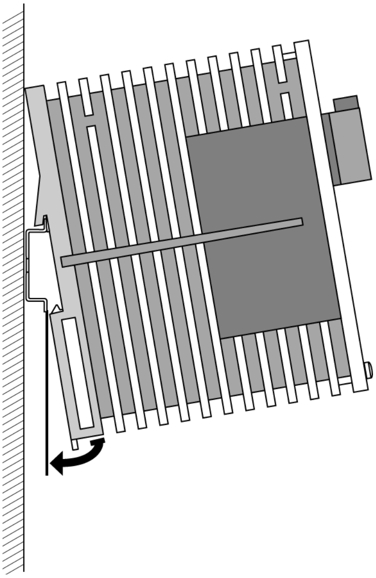
Connecting the Lines

Connect the power supply and signal lines.

Step	Action
1	Pull the terminal block off the NxS and connect the power supply and signal lines.

Assembly

On delivery, the device is ready for operation.
Slide the upper snap-in guide of the NxS into the top hat rail and press the guide down against the rail until it snaps in place.



Note: The front panel of the housing of the NxS is grounded via a ground connection.

Note: The housing must not be opened.

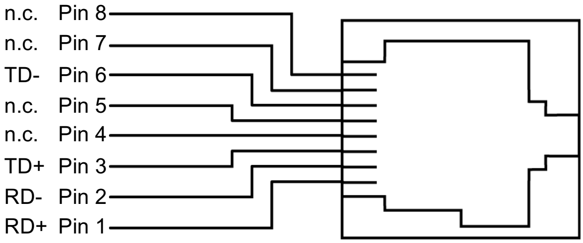
Note: The shielding ground of the industrial connectable twisted pairs lines is connected to the front panel as a conductor.

10/100 Mbps Connection

Five 10/100 Mbit Ports (Port 1 to Port 5, 8 pin RJ45 sockets) with NxS make it possible to connect terminal devices or five independent network segments in compliance with the standards ISO/IEC 8802-3 (10BASE-T) and ISO/IEC 8802-3u (100BASE-TX). The ports support autonegotiation and the autopolarity function.
State on delivery: Autonegotiation is activated for Port 1 to Port 5.
The socket housing are electrically connected to the front panel. The pin assignment corresponds to MDI-X.
Port 1 is used for linking redundant rings.

Pin Assignments

The figure below describes the pin assignment of a TP/TX interface.



100 Mbps Connection (Backbone Port)

Two 100 Mbps ports (Port 6 and 7) make it possible to set up a backbone.

- 499NES17100: two ports in compliance with 10/100BASE-TX (RJ45 sockets)
- 499NOS17100: two ports in compliance with 100BASE-FX (SC-sockets, multimode)

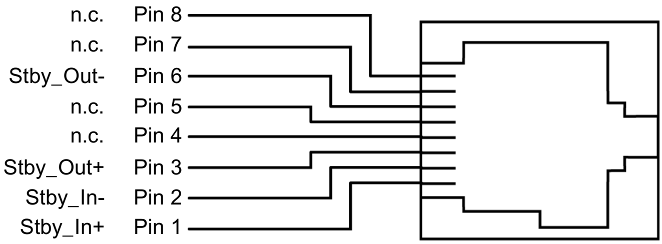
Delivery condition: The backbone ports are preconfigured to 100 Mbit/s full duplex. This configuration is required for setting up redundant structures.
The backbone ports support the full-duplex and half-duplex mode. The TX ports in addition support autonegotiation and the autopolarity function.

Standby Port

The control cable is connected via an eight-pin RJ45 socket (standby) for the redundant operating mode for redundantly coupling rings (See *Redundant Ring Structure, p. 58*). The socket housing is electrically connected to the front panel of the NxS. The outputs Stby_Out+ and Stby_Out- are electrically isolated from the supply voltage and the chassis (relay contact).

Pin Assignment

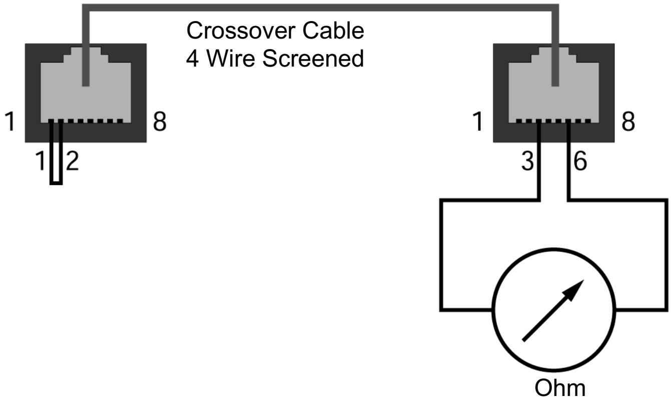
The figure below describes the pin assignment of the standby interface.



Control Cable Length

To determine the maximum length of the control cable, measure the line resistance in the upstream and downstream directions. The DC current resistance must not exceed 10 Ω.

The following figure shows the maximum length of the control cable.



V.24 Connection (External Management)

A serial interface is provided on the RJ11 socket (V.24 interface) for the local connection of an external management station (VT100 terminal or PC with appropriate terminal emulation). (The serial cable that allows external management is part number 490NTRJ11.) This makes it possible to establish a connection to the user interface UI.
Settings VT-100 Terminal:

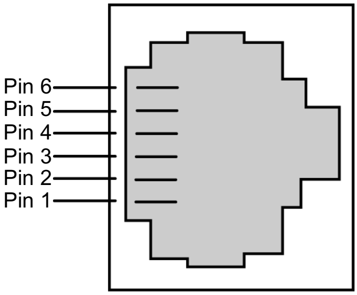
Speed:	9600 Baud (NxS17100)
Data:	8 bit
Stopbit:	1 bit
Handshake:	off
Parity:	none

The V.24 connection can be activated with Baud rate 9600. The setting at system start is 19200 Baud. The Xon/Xoff protocol is used.
The socket housing is electrically connected to the front panel of the device.
The signal lines are electrically isolated from the supply voltage (60 V insulation voltage) and the front panel.

Note: If a connection has been established, data cannot be transferred via the console as long as Telnet makes use of the UI. The input of the exit command via the Telnet connection enables the UI.

Pin Assignment

The figure below describes the pin assignment of the V24 interface.



Pin Number	V.24 Interface
Pin 1	CTS
Pin 2	not connected
Pin 3	TX
Pin 4	GND
Pin 5	RX
Pin 6	RTS

CTS	Clear to Send
RTS	Request to Send
RX	Receive Data
TX	Transmit Data

Line Installation

The following table shows how to install the lines.

Step	Action
1	Install the signal lines and if necessary, the control line and terminal cable.
2	Attach the ground cable to the ground screw.

Disassembly

The following table shows how to remove the NxS from the tophat rail.

Step	Action
1	Move the screwdriver horizontally under the chassis in the locking gate.
2	Pull this down — without tilting the screwdriver.
3	Fold the NxS up.

Startup Operation

Starting the NxS

Start the NxS when the supply voltage is connected via the five-pin terminal.

Step	Action
1	Start up the NxS.
2	Lock the terminal block with the side locking screw.

Basic Settings

NxS Settings

Although the NxS is designed for ease of use and complies as far as possible with the "plug and play" principle, certain settings are still necessary for correct operation of the management.To enable network management, IP address(es) must be entered when the NxS is installed for the first time.

The NxS offers 3 possibilities to configure IP addresses:

- configuration via BOOTP
- configuration via DHCP
- entry via V.24 connection

BOOTP (BOOTstrap Protocol)

During startup operation, the NxS receives its configuration data according to the flowchart "BOOTP process" (See the figure "BOOTP/DHCP Process" below.).

For the NxS, a BOOTP server should make available the following data:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateways
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template
```

Enabling/ Disabling BOOTP

To enable/disable BOOTP, see *System Parameter, p. 117* and *System Data, p. 71*.

Note: ConneXium switch management agent does not support IEEE 802.3 frame type.

DHCP

The DHCP (dynamic host configuration protocol) responds similar to the BOOTP and offers in addition the configuration of a DHCP client with a name instead of the MAC address. For the DHCP, this name is known as the "client identifier" in accordance with rfc 2131.

The NxS uses the name entered under `sysName` as the client identifier in the system group of the MIB II (see *System Group (1.3.6.1.2.1.1), p. 97*). You can enter the system name directly via SNMP, the Web-based management (see *System Data, p. 71*) or the user interface (see *System Parameter, p. 117*).

On startup, an NxS receives its configuration data according to the flow chart "BOOTP/DHCP process." (See the figure "BOOTP/DHCP Process" below.)

The NxS sends its system name to the DHCP server. The DHCP server can then assign an IP address as an alternative to the MAC address by using the system name.

In addition to the IP address, the DHCP server sends

- the tftp server name (if present) and
- the name of the configuration file (if present).

The NxS accepts this data as configuration parameters (see *Set Network Parameters, p. 77*). If an IP address was assigned by a DHCP server, it will be permanently saved locally.

The special feature of DHCP in contrast to BOOTP is that the server can only provide the configuration parameters for a certain period of time ("lease"). When the time period expires ("lease duration"), the DHCP client must attempt to renew the lease or negotiate a new one. A BOOTP-similar response can be set on the server (i.e., the same IP address is always assigned to a particular client using the MAC address), but this requires the explicit configuration of a DHCP server in the network. If this configuration was not performed, a random IP address (whichever one happens to be available) is assigned.

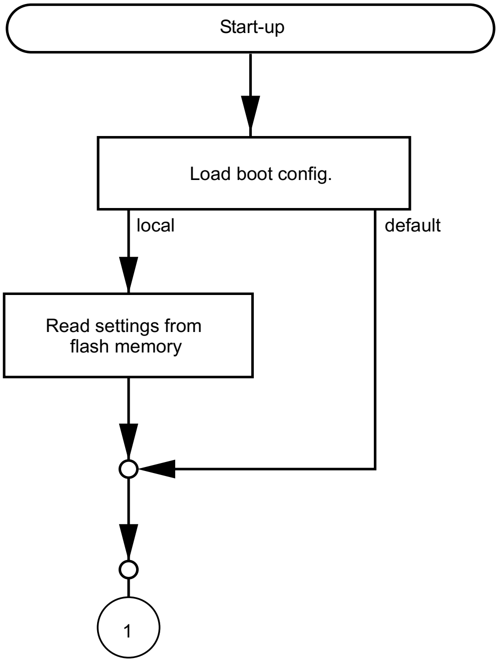
As long as DHCP is activated, NxS attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.

To activate/deactivate DHCP, see *Set Network Parameters, p. 77*.

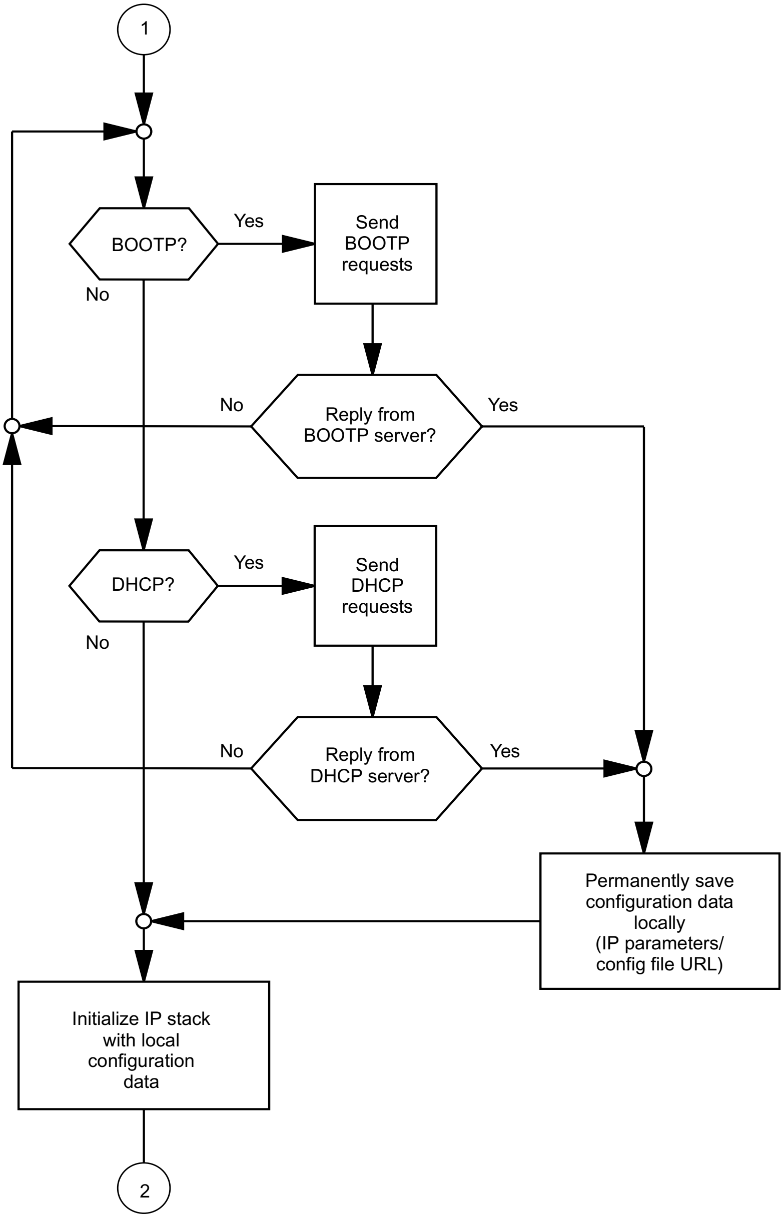
Note: ConneXium switch management agent does not support IEEE 802.3 frame type.

BOOTP/DHCP Process

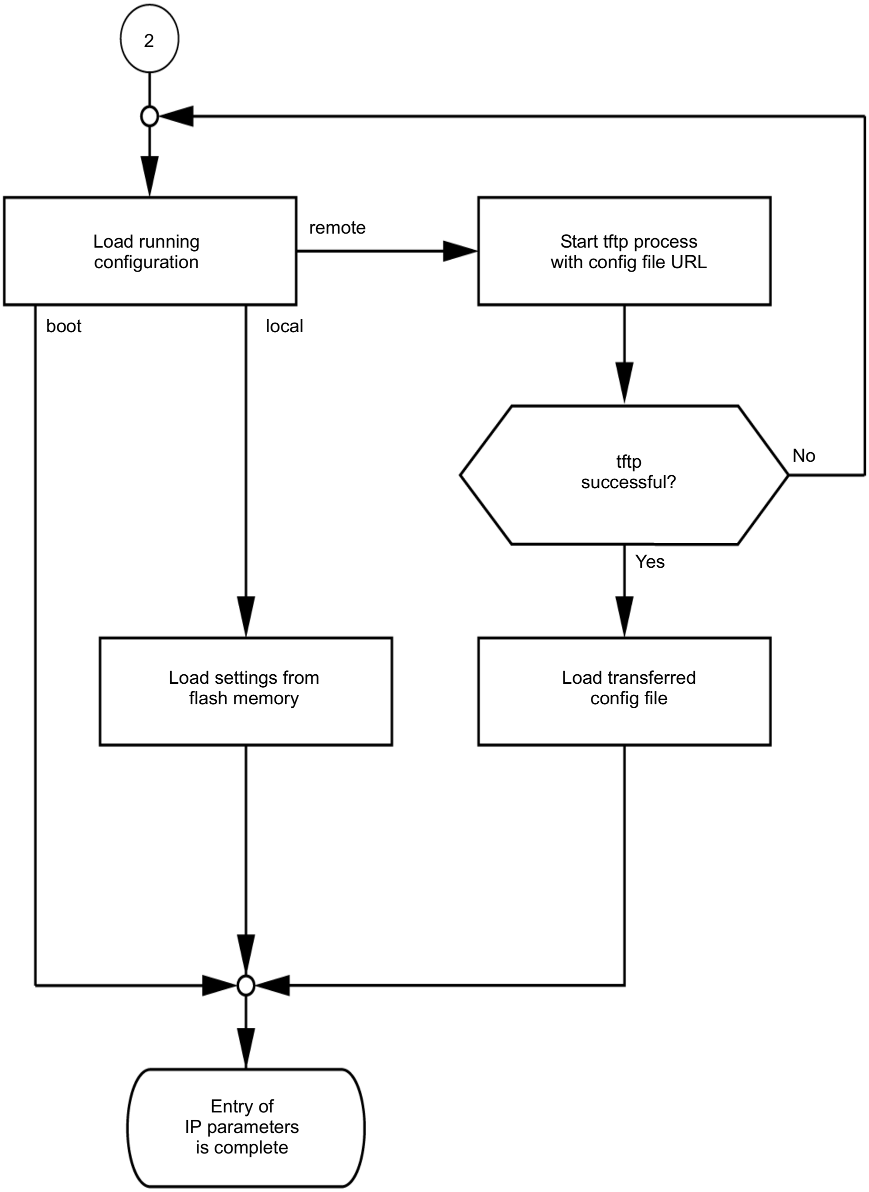
The following flow chart describes Part 1 of the BOOTP/DHCP process.



The following flow chart describes Part 2 of the BOOTP/DHCP process.

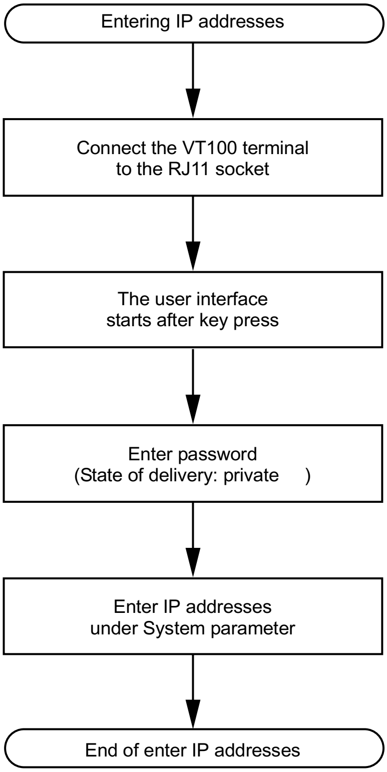

1
BOOTP?
Yes
No
Send BOOTP requests
Reply from BOOTP server?
No
Yes
DHCP?
Yes
No
Send DHCP requests
Reply from DHCP server?
No
Yes
Permanently save configuration data locally (IP parameters/ config file URL)
Initialize IP stack with local configuration data
2

The following flow chart describes Part 3 of the BOOTP/DHCP process.


2
Load running configuration
remote
Start tftp process with config file URL
boot
local
tftp successful?
No
Yes
Load settings from flash memory
Load transferred config file
Entry of IP parameters is complete

V. 24

The following figure describes the sequence for entering IP addresses.


Entering IP addresses
Connect the VT100 terminal to the RJ11 socket
The user interface starts after key press
Enter password (State of delivery: private)
Enter IP addresses under System parameter
End of enter IP addresses

If there is no VT 100 terminal available in the vicinity of the installation location, the IP addresses can be entered prior to ultimate installation. A VT100 terminal or suitable emulation (e.g. MS Windows terminal) is required for this purpose.

IP Address Entry Via Terminal

> **Note:** The installation of NxS is easier if you enter the appropriate IP addresses for each NxS at your workstation. Even if only one NxS is to be installed, it may be more convenient to enter the IP addresses at your own workstation.

The NxS should be labelled to prevent confusion during subsequent installation.
The addresses are stored in a non-volatile memory.
Connect a VT 100 terminal or a PC with terminal emulation to the RJ11 socket (V.24).
Data transfer parameters

Speed:	9600 Baud (NxS17100)
Data:	8 bit
Parity:	none
Stopbit:	1 bit
Handshake:	off

System Configuration

After installation, follow the steps below.

Step	Action
1	Once the NxS has been installed, start it by connecting the power supply. The operating system is loaded after a key press (See).
2	Enter the password you assigned (the password is case sensitive) and then press the enter key. The factory default for the password is: private.
3	Enter the IP address, the subnet mask, and the gateway IP address. (See).

Local IP Address

The factory default local IP address is: 0.0.0.0.

Gateway IP Address

This entry is only needed if the NxS and management station/tftp server are located in different subnetworks (See *Network Mask, p. 34*). Enter the IP address of the gateway between the subnetwork with the NxS and the path to the management station. The factory default local IP address is: 0.0.0.0.

Network Mask

If your network has been divided up into subnetworks and if these are identified with a network mask, then this is to be entered here. On leaving the factory, the mask address entered is 0.0.0.0.

IP Address

The IP addresses consist of four bytes. These four bytes are written in decimal notation, each separated by a dot.

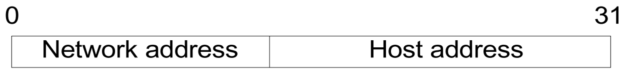
Since 1992, there are five classes of IP addresses defined in RFC 1340. The most frequently used address classes are A, B and C.

The following table describes IP address classification.

Class	Net Address	Host Address
A	1 Byte	3 Bytes
B	2 Bytes	2 Bytes
C	3 Bytes	1 Byte

The network address represents the fixed part of the IP address. It is assigned by the DOD (Department of Defense) Network Information Center.

The following figure shows the bit notation of the IP address.



All IP addresses belong to class A when their first bit is a zero, i.e., the first decimal number is less than 128.

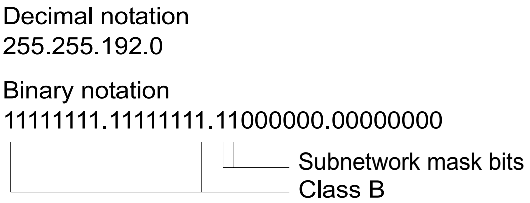
The IP address belongs to class B if the first bit is a one and the second bit is a zero, i.e., the first decimal number is between 128 and 191.

The IP address belongs to class C if the first two bits are a one, i.e., the first decimal number is higher than 191.

Assigning the host address (host id) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

Network Mask

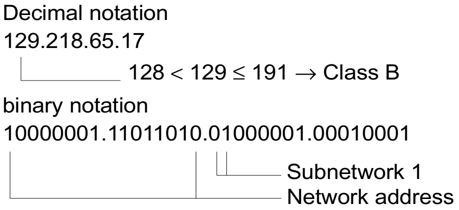
Routers and gateways subdivide large networks into subnetworks. The network mask assigns the individual devices to particular subnetworks.
The subdivision of the network into subnetworks is performed in much the same was as IP addresses are divided into classes A to C (net id).
The bits of the host address (host id) that are to be shown by the mask are set to one. The other host address bits are set to zero in the network mask (see the following example).
The following figure shows an example of a network mask.



Decimal notation
255.255.192.0

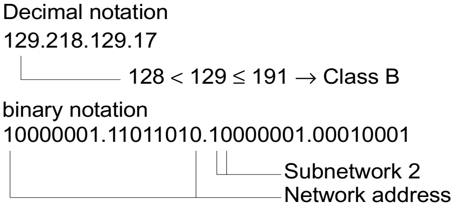
Binary notation
11111111.11111111.11000000.00000000

The following figure shows an example of IP addresses with subnetwork allocation in accordance with the network mask from the above example.



Decimal notation
129.218.65.17

binary notation
10000001.11011010.01000001.00010001

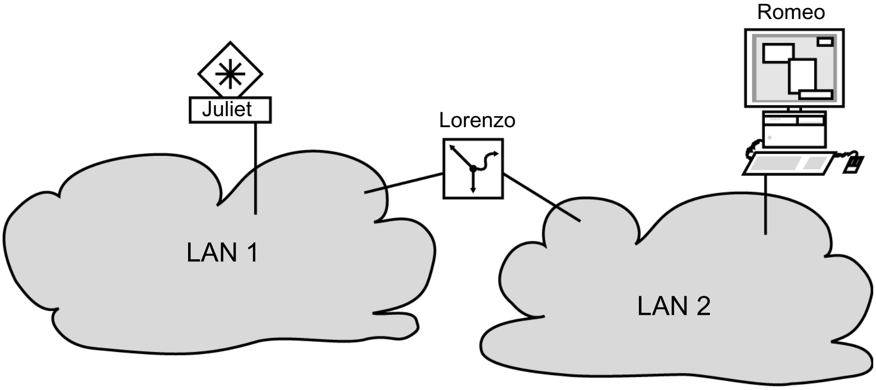


Decimal notation
129.218.129.17

binary notation
10000001.11011010.10000001.00010001

Example of Network Mask Usage

In a large network it is possible that gateways and routers separate the management card from its management station. How does addressing work in such a case? The figure below shows a management agent that is separated from its management station by a router.



Sending Data

The management station "Romeo" wants to send data to the management agent "Juliet." Romeo knows Juliet's IP address and also knows that the router "Lorenzo" knows the way to Juliet.

Example

Romeo therefore puts his message in an envelope and writes Juliet's IP address on the outside as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer three to layer two of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer two to layer one, i.e., to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope, exposing the inner envelope with Romeo's IP address. Opening the letter and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. The question then arises, where should she send the letter, since she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable saNetGatewayIPAddr as a means of communicating with Romeo. The envelope with the IP addresses is therefore placed in a further envelope with the MAC destination address of Lorenzo.

The letter then travels back to Romeo via Lorenzo, in the same manner that the first letter traveled from Romeo to Juliet.

TFTP Server for Software Updates

Switch Software

The switch software is in the flash memory in the as delivered condition. The NxS boots the software from the flash memory.

Software updates can be realized via a tftp server. This presupposes that a tftp server has been installed in the connected network and that it is active.

The NxS requires the following information to be able to make a software update from the tftp server:

- Own IP address (permanently entered),
- IP address of tftp server or gateway to tftp server,
- Path in which operating system of tftp server is located.

File transfer between NxS and tftp server is handled by way of the Trivial File Transfer Protocol (tftp).

Management station and tftp server may be made up of one or more computers.

Preparation of the tftp server for the NxS software involves the following:

- Setting up of NxS directories and copying of NxS software
- Setting up of tftp process

Note: You cannot upgrade from NxS07100 to NxS17100.

Setting Up the Tftp Process

This segment contains information on setting up the tftp process with a breakdown according to operating systems and applications.

General prerequisites:

- NxS familiar with local IP address of NxS IP address of tftp server/gateway.
- TCP/IP stack with tftp installed on tftp server.

SunOS and HP

The following table shows the steps for setting up the tftp process, with subsequent tables providing a breakdown according to operating systems and applications.

Step	Action	Comment
1	Check to see if the tftp daemon (background process) is running.	See the tables that follow to find out how to determine if the process is running.
2	Check whether the status of this process is "IW."	The status should be "IW."
3	Test the tftp process.	See the table below to find out how to test the process.

Testing the Tftp Process

The following step is used to test the tftp process.

Step	Action
1	cd /tftpboot/NxS tftp <tftp-Servername> get NxS/NxS.bin rm NxS.bin

Tftp Installation on HP Workstations

The following table describes a special step for tftp installation on HP workstations.

Step	Action	Comment
1	Enter the user tftp in the file /etc/passwd.	For Example: tftp:*:510:20:tftp server:/usr/tftpdir:/bin/false Where: tftp = user ID * = in the password field 510 = sample user ID 20 = sample group ID tftp server = reely selectable designation /bin/false = mandatory entry (login shell)

Status of SunOS Tftp Process

The following table shows how to determine if the tftp process is running under SunOS.

If...	Then ...	Comment
the file /etc/inetd.conf contains the line tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -s /tftpboot	The tftp daemon (background process) is running.	The process must be running.
the process is not in the file, or if the related line is commented out (#)	modify /etc/inetd.conf accordingly and then re-initialize the INET daemon.	See the table below to find out how to re-initialize the INET daemon.

Status of HP Tftp Process

The following table explains how to determine if the tftp process is running under HP.

If...	Then ...	Comment
the file /etc/inetd.conf contains the line `tftp dgram udp wait root /usr/etc/in.tftpd tftpd`	The tftp daemon (background process) is running.	The process must be running.
the process is not in the file, or if the related line is commented out (#)	modify /etc/inetd.conf accordingly and then re-initialize the INET daemon.	See the following table to find out how to re-initialize the INET daemon.

Re-initializing the INET Daemon Under SunOS

The following table shows how to re-initialize the INET daemon under SunOS.

If...	Then ...
you want to re-initialize manually	Use the command `kill -1 PID`, where PID is the process ID of inetd.
you want to re-initialize automatically	Use the command `ps -ax grep inetd head -1 awk -e {print $1} kill -1`

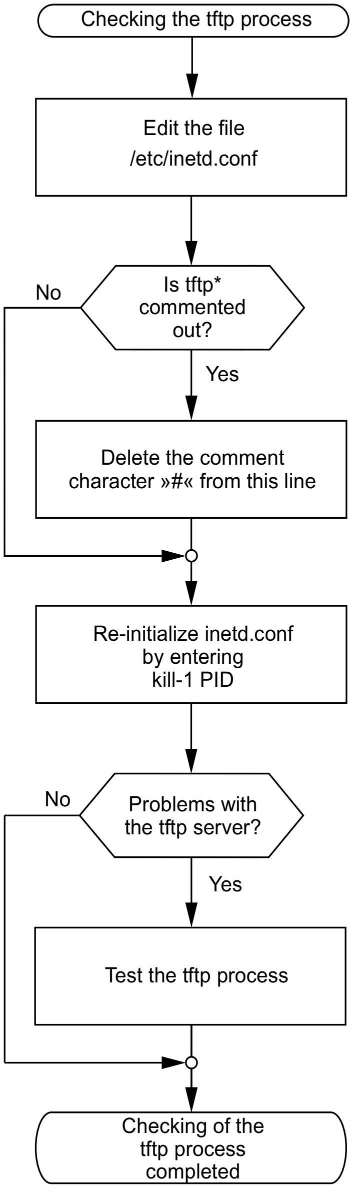
Re-initializing the INET Daemon Under HP

The following table shows how to re-initialize the INET daemon under HP.

If...	Then ...
you want to re-initialize manually	Use the command `kill -1 PID`, where PID is the process ID of inetd.
you want to re-initialize automatically	Use the command `/etc/inetd -c`

Flowchart

The following flowchart summarizes setting up the tftp server with SunOS and HP.



e.g.

```
cd /tftpboot/NxS
tftp <tftp-Servername>
get NxS/NxS.bin
```

Response if the process is running: Received ...

```
rm NxS.bin
```

* tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot

Directory Structure of the Software

The following table shows the directory structure of the tftp server with stated access rights, once NxS software has been installed.

Filename	Access
NxS.bin	444-r--r--r-

d = directory; r = read; w = write; x = execute
1st position designates d (directory)
2nd-4th positions designate access rights of user
5th-7th positions designate access rights of user groups
8th-10th positions designate access rights of all others.

System Monitor 1

Overview

System monitors facilitate the implementation of an update of the operating system. The software update can be implemented via v.24 or tftp. The V.24 interface of NxS supports the baud rates 9600 and 19200. (For information on VT100 terminal emulation, see *V.24 Connection (External Management), p. 25*.)

Update of the Operating System

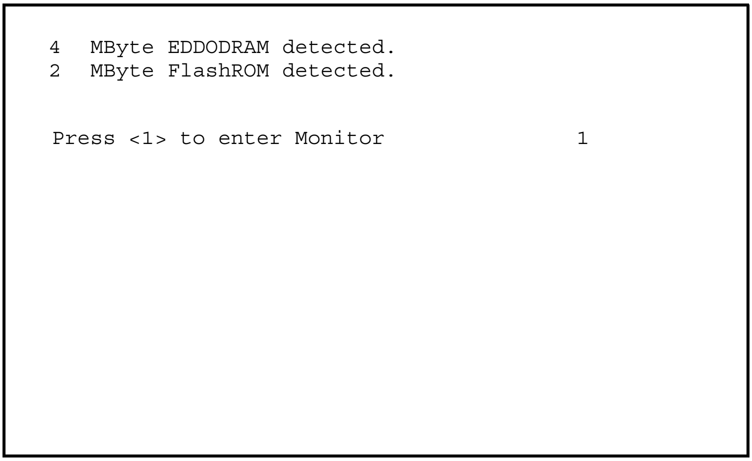
System Monitor 1 facilitates an update of the operating system of the NxS via V.24.

Note: System Monitor 2 is preferred for updating the operation system.

If you boot NxS with 9600 baud, the message "Press <1> to enter Monitor 1" appears.

Boot Phase

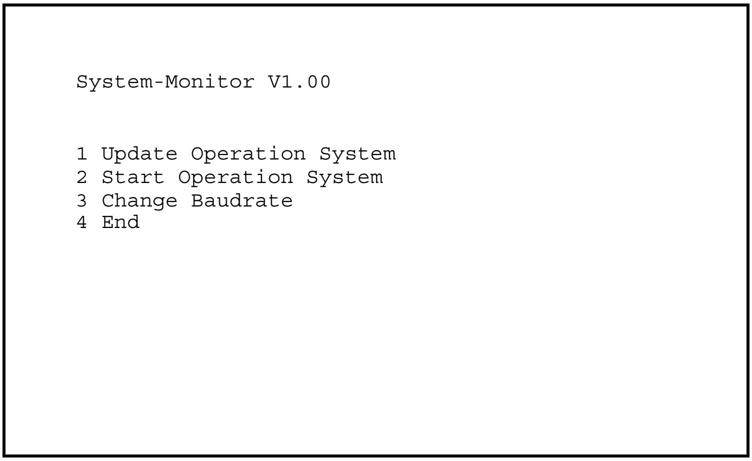
The figure below shows the screen display during the boot phase.



```
4   MByte EDDODRAM detected.
2   MByte FlashROM detected.


Press <1> to enter Monitor              1
```

System Monitor 1 Main Menu

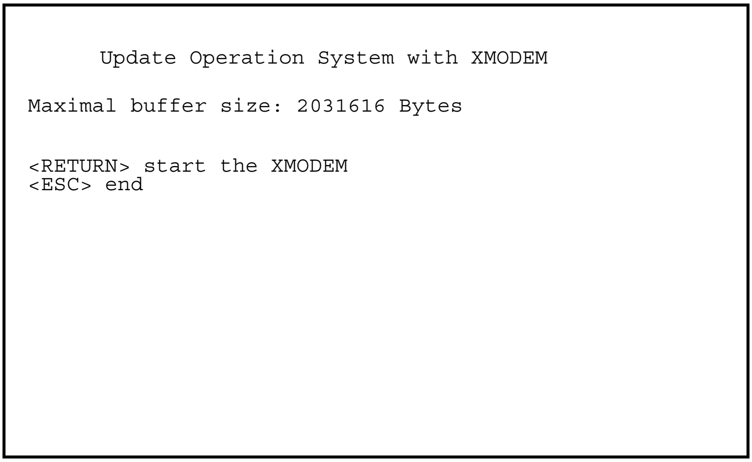
Press the <1> key within one second to start system monitor 1. System Monitor 1 displays the following selections.



```
System-Monitor V1.00


1 Update Operation System
2 Start Operation System
3 Change Baudrate
4 End
```

Update the Operating System

Choose the first option to run an update of the operating system.
The **Update Operation System** screen appears.

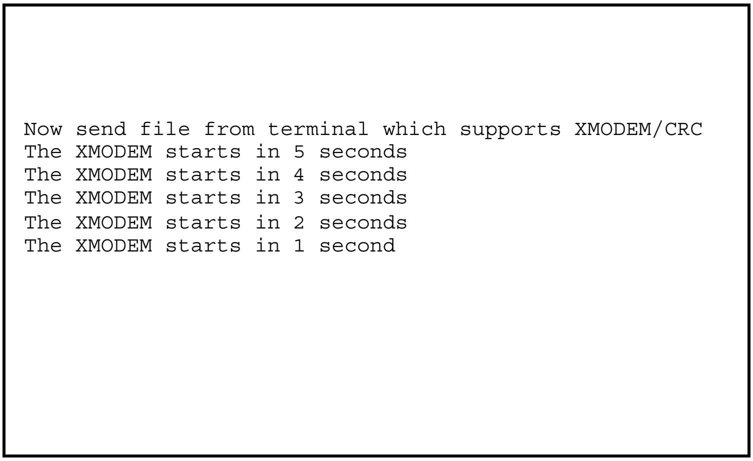


```
      Update Operation System with XMODEM

Maximal buffer size: 2031616 Bytes


<RETURN> start the XMODEM
<ESC> end
```

To return to the main menu of system monitor 1, press the **<ESC>** key. Press **<RETURN>** to start the update with XMODEM.

Confirm Operation System Update

Press **<RETURN>**, and the following window appears on the screen.



```
Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 second
```

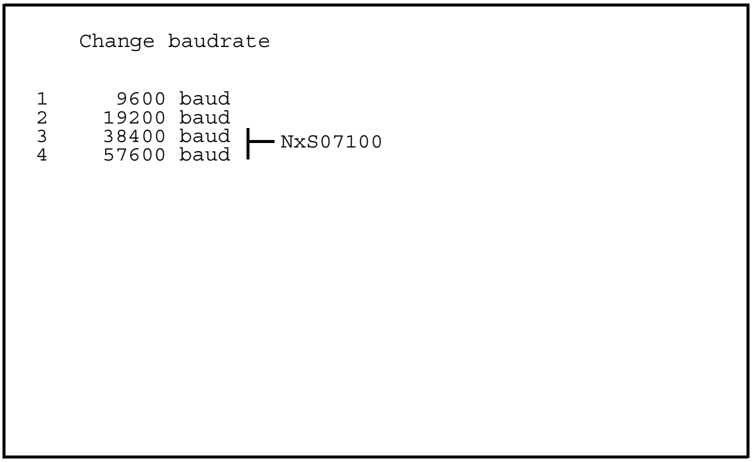
Enter the name of the path where the operating system is to be loaded. Enter the path name via the terminal program, e.g. under Transmission Binary File. The transmission starts. When the transmission has finished, the operating system restarts.

Start Operation System

Choose the second option to start the operating system.
System monitor 1 will be terminated. The operating system will be started with 19200 baud.

Change Baudrate

Choose the third option to modify the baud rate.
The **Change Baudrate** screen appears.

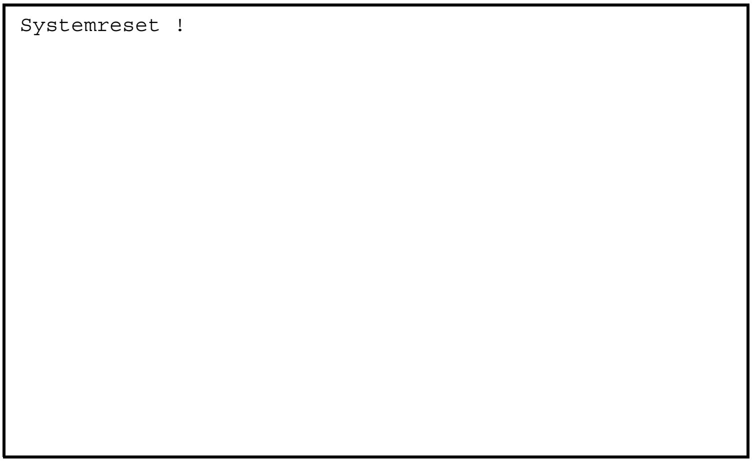


```
     Change baudrate


 1      9600 baud
 2     19200 baud
 3     38400 baud  ├─ NxS07100
 4     57600 baud
```

For an update of your operating system, (ref. menu 1) you should choose the maximum speed for the baud rate.
Then, adapt the speed of your terminal program to this baud rate.

End

Choose the fourth option to terminate system monitor 1.
The following window appears on the screen.



```
Systemreset !
```

Then, execute a hardware reset.

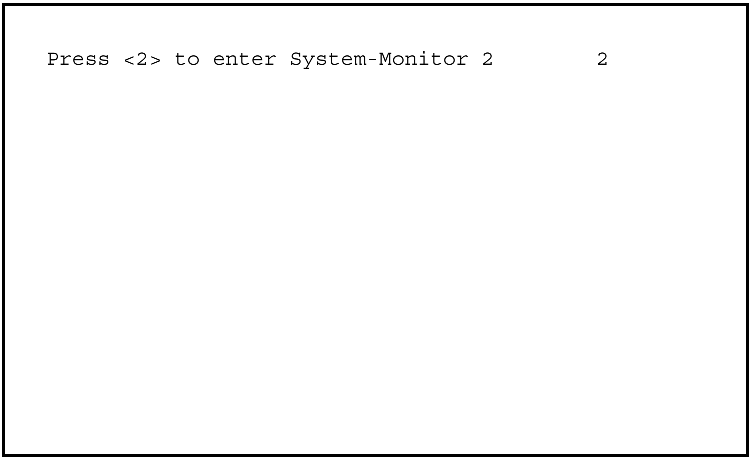
System Monitor 2

Overview

System monitor 2 facilitates an update of the NxS operation system via V.24 as well as via tftp. (For information on VT100 terminal emulation, see *V.24 Connection (External Management), p. 25*.)

Boot Phase

If you boot NxS with 9600 baud, the following window appears on the screen.

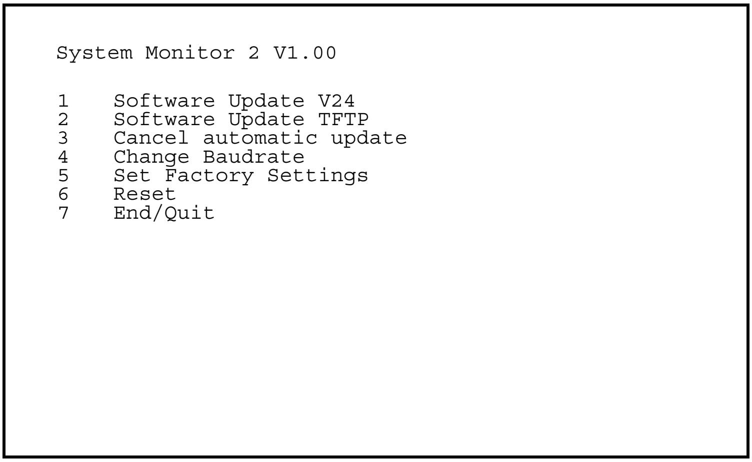


```
Press <2> to enter System-Monitor 2        2
```

Press the <2> key within three seconds to start system monitor 2.

System Monitor 2 Main Menu

System monitor 2 displays the following selections.



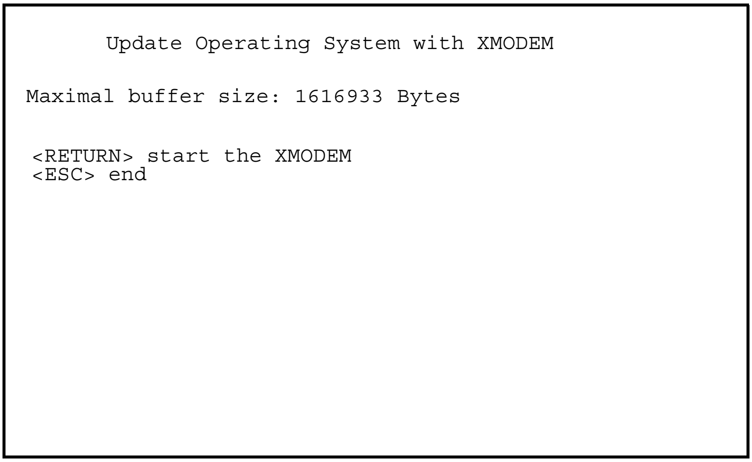
```
System Monitor 2 V1.00

1    Software Update V24
2    Software Update TFTP
3    Cancel automatic update
4    Change Baudrate
5    Set Factory Settings
6    Reset
7    End/Quit
```

Software Update V24

Choose the first option to execute an update of the operation system in the flash memory of the NxS. The Update runs via V.24.

> **Note:** tftp transfer is preferred for update of the operation system (See). It is more than three times faster than the fastest V.24 transfer.

The **Update Operation System** screen appears.

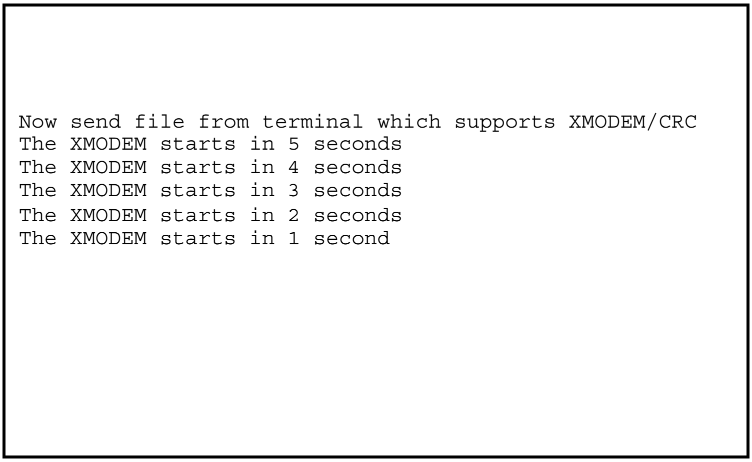


```
      Update Operating System with XMODEM

Maximal buffer size: 1616933 Bytes


 <RETURN> start the XMODEM
 <ESC> end
```

To return to the main menu of system monitor 2, press the **<ESC>** key.

Confirm Operation System Update

Press **<RETURN>** to start XMODEM; the following window appears on the screen.



```
Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 second
```

Then, enter the name of the path in which the operating system that is to be loaded is located. Enter the path name via the terminal program, e.g. under Transmission Binary File. The transmission starts. When the transmission has finished, the operating system is restarted.

Software Update tftp

Choose the second option to execute an update of the operation system in the flash memory of the NxS. The Update runs via tftp.

Cancel Automatic Update

Choose the third option to terminate the running automatic software update.

Change Baudrate

Choose the fourth option to modify the baud rate.

Set Factory Setting

Choose the fifth option to restore the original settings. With the exception of the IP parameters, all SNMP-MIB variables are reset to their default values.

Reset

Choose the sixth option to perform a device reset.

End/Quit

Choose the seventh option to terminate system monitor 2. The management software is started.

Functions

4

At a Glance

Overview

The devices of the Ethernet ConneXium switch NxS family contain a wide variety of functions. They are presented in this chapter.

What's in this Chapter?

This chapter contains the following topics:

Hardware Functions

Diagnostics

When restarting, the NxS performs a hardware self-test.
During operation, an integrated watchdog (monitoring unit) monitors the function of the software.

Autonegotiation

Autonegotiation is a procedure in which the switch automatically selects the operating mode of its 10/100 RJ-45 ports. When a connection is set up for the first time, the switch detects the speed (10 or 100 Mbps) and the transmission mode of the connected network (half duplex or full duplex). The automatic setting of the ports eliminates the need for manual intervention on the part of the user. The autonegotiation function is activated/deactivated by the web management tool.

Autopolarity Exchange

If the receive line pair of a twisted-pair cable is incorrectly connected (RD+ and RD- are reversed), polarity is reversed automatically.

Line Supervision with Twisted Pair

Using regular link-test pulses in accordance with the ISO/IEC 8802-3 (10BASE-T) and ISO/IEC 8802-3u (100BASE-TX) standard, the NxS monitors the connected TP/TX line segments for short circuiting or interruptions. The NxS does not send any data to a TP/TX segment from which it does not receive a link-test pulse.

Note: An unassigned interface is interpreted as a line interruption. The TP/TX line to a deactivated terminal device is also interpreted as a line interruption, since the current-free connected device is unable to send link-test pulses.

Line Supervision with F/O

A NxS monitors the connected fiber optic lines for breaks in accordance with the ISO/IEC 8802-3u (100BASE-FX) standard.

Reset

The NxS is reset by the following events:

- management
- insufficient level of both input voltages
- watchdog

The following actions are carried out after a reset:

- self-test
- initialization

Display Indicators

Device Status

These LEDs provide information about conditions that affect the operation of the whole NxS.

LED	Lit	Not Lit
P1 - Power 1 (green)	supply voltage 1 is supplied.	supply voltage 1 is less than 18 V
P1 - Power 2 (green)	supply voltage 2 is supplied.	supply voltage 2 is less than 18 V
FAULT - Error (red)	The signal contact is open, i.e. it reports an error.	The signal contact is closed, i.e. it does not report an error.
Standby (green)	The standby function is switched on.	The standby function is switched off.
RM - Redundancy Manager (green/yellow)	**green:** RM function active, redundant port not active. **yellow:** RM function active, redundant port active.	RM function not active.

Port Status

These LEDs display port-related information.

1 to 7 - (green/yellow LED)	Data, link status
Not lit	No valid connection
Green	Valid connection
Blinks green (once a period)	Port is switched to standby (Port 1)
Blinks green (three times a period	Port is disabled
Blinks yellow	Data reception
Blinking in sequence	Initialization phase after restart

Frame Switching

Store and Forward

All data received by a NxS are stored, and their validity is checked. Invalid and defective data packets (> 1522 bytes or CRC errors, >1518 bytes in NxS07100) as well as fragments (< 64 Bytes) are discarded. Valid data packets are forward by the NxS.

Multi-Address Capability

An NxS learns all the source addresses for a port. Only packets with

- unknown addresses
- these addresses or
- a multi/broadcast address

in the target address field are sent to this port.
An NxS can learn up to 2000 addresses. This becomes necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to an NxS.

Learning Addresses

An NxS monitors the age of the learned addresses. Address entries which exceed a certain age (30 seconds, aging time), are deleted by the NxS from its address table.

Note: A reboot deletes the learned address entries.

Prioritization

The NxS supports two priority queues (traffic classes in compliance with IEEE 802.1D). The received data packets are assigned to these classes by

- the predefined assignment in static address entries.
- the priority of the data packet contained in the VLAN tag.

This function prevents high priority data traffic being disrupted by other traffic during busy periods. The traffic of lower priority will be discarded when the memory or transmission channel is overloaded.

Tagging

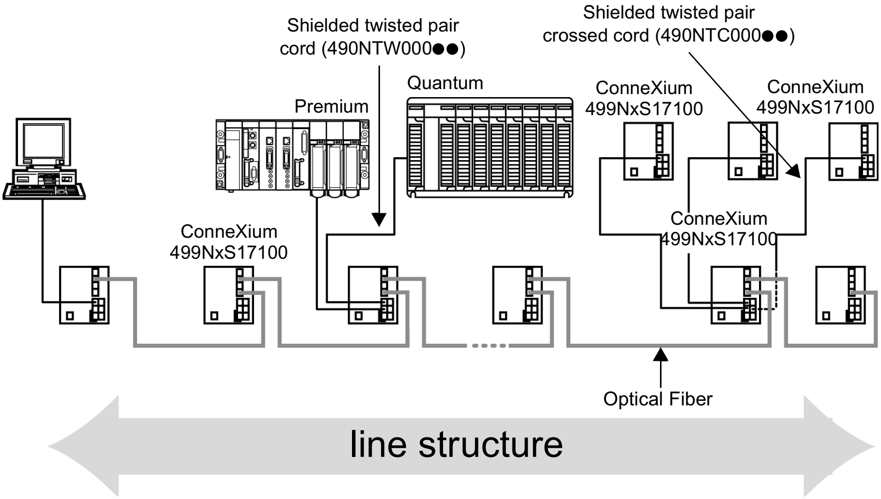
According to the IEEE 802.1 Q standard, the VLAN tag is integrated into the MAC data frame for the functions VLAN and prioritization. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.
With data packets with VLAN tag, the NxS evaluates the 3 Bit priority field within the VLAN tag.
The MAC data frame is transferred unchanged by the NxS.

Redundancy

Bus Type Configuration

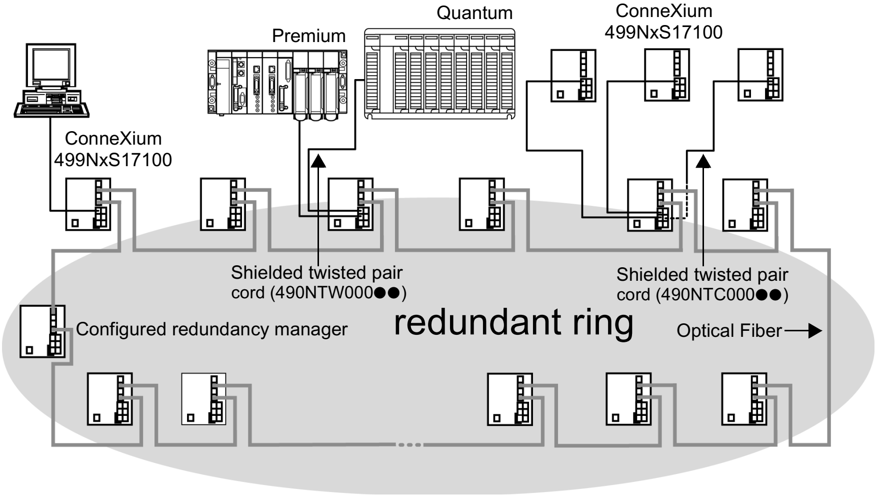
The NxS enables the setup of backbones in the Bus type configuration. Cascading takes place via the backbone ports.

The figure below shows how backbones may be set up in a Bus type configuration.



Redundant Ring Structure

The two ends of a backbone in a Bus type configuration can be closed to form a redundant ring by using the RM function (**R**edundancy **M**anager) of the NxS.
The figure below shows an example of a redundant optical ring structure.

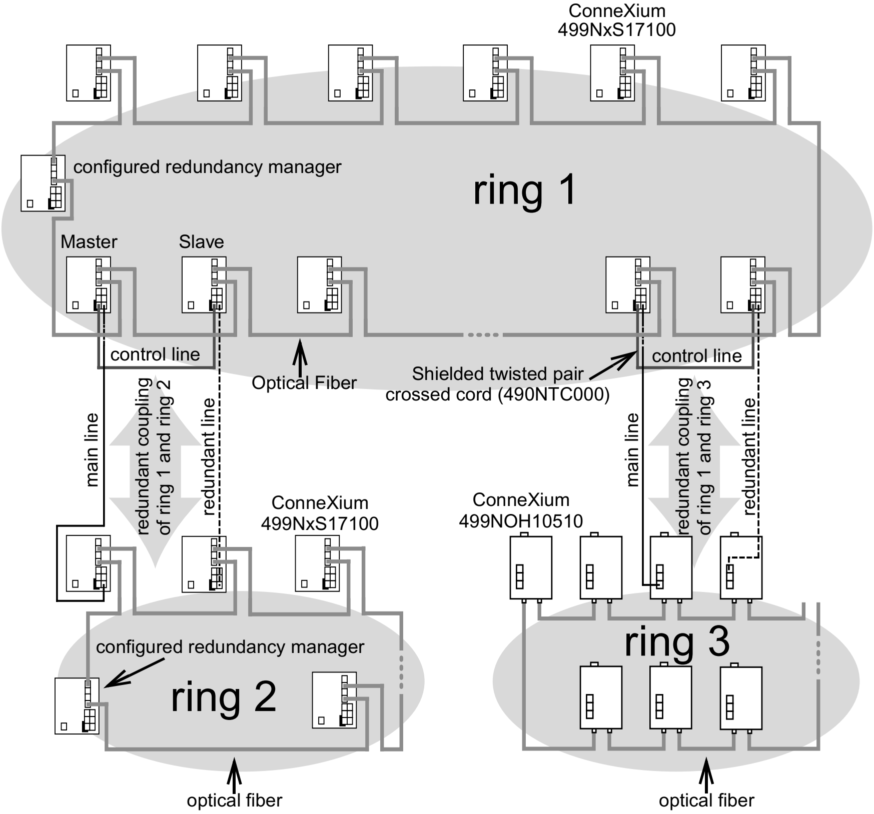


The NxS is integrated into the ring via the backbone ports (ports 6 and 7). If a line section fails, the ring structure of up to 50 NxS switches transforms back to a Bus type configuration within 0.5 seconds.

Note: The function "Redundant ring" requires the following setting for ports 6 and 7: 100 Mbps, full duplex and autonegotiation off (which is the factory default setting).

Redundant Coupling of Network Segments

The control intelligence built into the NxS allows the coupling of network segments. The figure below shows how network segments may be joined in a redundant coupling of rings configuration.



Two network segments are connected over two separate paths with one NxS each. The redundancy function is assigned to the NxS in the redundant link via the Standby DIP switch setting.

The NxS in the redundant line and the NxS in the main line inform each other about their operating states via the control line (crossed twisted-pair cable).

Note: The main and redundant lines must be connected to port 1 of the respective NxS switches.

Immediately after the main line fails, the redundant NxS line releases the redundant line. As soon as the main line is restored to normal operation, the NxS in the main line informs the redundant NxS. The main line is released, and the redundant line is re-blocked.

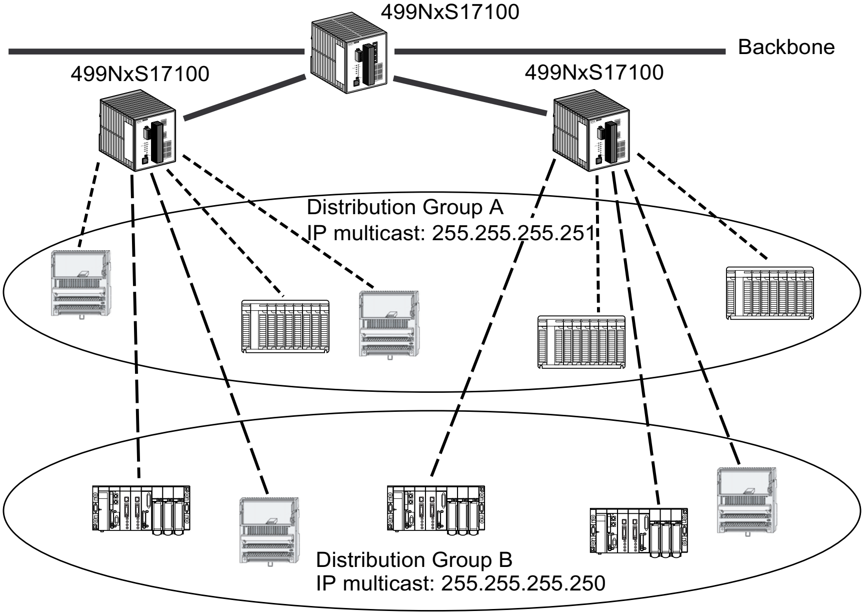
An error is detected and eliminated within 0.5 seconds.

GMRP

Using GMRP in an Automation Setting

The GARP Multicast Registration Protocol (GMRP) describes how multicast information is distributed to other switches. This makes it possible for switches to learn multicast addresses.

The following figure shows GMRP as used in an automation setting.



GMRP is useful in an automation setting where switches connect several groups of modules using Global Data Service.

> **Note:** Global Data Service exchanges variables on the network in order to synchronize automation applications.

ConneXium switches (499NxS17100, V 5.2), Telemecanique Quantum Ethernet modules (140NOE771x1), and Telemecanique Premium Ethernet modules (TSXETYx103xx) prevent network congestion using GMRP, sending data only to the multicast address of the local distribution group. Ethernet modules send their multicast addresses to the switches. The switches learn the addresses, thus propogating multicast frames only to ports that are members of the same group. The multicast tree is set up within 5 seconds in a network of up to 20 NxS modules, after the multicast address has been entered for the first time at an NxS port. Devices that do not support GMRP can be integrated into the multicast addressing scheme by means of a static filter address entry on the connector port.

Activating GMRP Using SNMP

On delivery, GMRP is deactivated at all ports.
Multicast filtering can be enabled by modifying one of the switch parameters using SNMP (Simple Network Management Protocol).
To modify the parameter will require a SNMP MIB Browser or SNMP Manager program.
The parameter can be modified in two ways:

- Direct access to the parameter - To access the object directly the user can directly request the browser to read the object ID : 1.3.6.1.2.1.17.6.1.1.3.0
- Browsing the MIB objects in the device – to browse the objects the user must obtain and install the following MIBs into the browser:
  - Definitions of Managed Objects for Bridges (rfc1493)
  - Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions (rfc2674)

Once the object is accessed, you should set the value to ‘1’ for Multicast filtering enabled or ‘2’ for Multicast filtering disabled.
A full description of the object to be modified is provided below:

```
dot1dGmrpStatus OBJECT-TYPE
SYNTAX : EnabledStatus
MAX-ACCESS : read-write
STATUS : current
DESCRIPTION
```

"The administrative status requested by management for GMRP. The value enabled(1) indicates that GMRP should be enabled on this device, in all VLANs, on all ports for which it has not been specifically disabled. When disabled(2), GMRP is disabled, in all VLANs, on all ports and all GMRP packets will be forwarded transparently. This object affects both Applicant and Registrar state machines. A transition from disabled(2) to enabled(1) will cause a reset of all GMRP state machines on all ports."

```
::= { dot1dExtBase 3 }
```

Activating GMRP Using Web Configuration

You can also activate GMRP using Web configuration.

Step	Action
1	At the NxS Web site home page, find the global setting for the GMRP in **Switching General Settings**.
2	Within the **Switching General Settings** window, find the setting for this port in **Configuration: GMRP**.

Security and SNMP Traps

Port Security

An NxS protects every port from unauthorized access. The following functions are available for monitoring every individual port:

Access: The NxS recognizes 2 classes of access control.

- **Every:** no access restriction.
- **User:** only an assigned user has access.

Unauthorized Access: The NxS can respond in three selectable ways to an unauthorized access attempt.

- **non:** no response
- **trapOnly:** message by sending a trap
- **portDisable:** message by sending a trap and disabling a port

The settings for port security are made via an SNMP network manager. Proceed by selecting the agent icon `Security` in the device window with the right mouse button. In the agent window that then appears, you will find the table with the respective MIB variables under `Port Security`.

SNMP

The agent communicates with the network management station via the Simple Network Management Protocol (SNMP). Therefore the network management station uses a network management software or the web based interface. Every SNMP packet contains the IP address of the sending computer and the community under which the sender of the packet will access the switch MIB.

The switch receives the SNMP packet and compares the IP address of the sending computer and the community with the entries in the `saAuthCommTable` and the `saAuthHostTable` of its MIB. If the community has the appropriate access right, and if the IP address of the sending computer has been entered, then the switch will allow access. In the delivery state, the switch is accessible via the community "public" (read only) and "private" (read and write) from every computer.

Preventing Unauthorized Switch Access

The following steps will secure the NxS.

Step	Action	Comment
1	Define a new community which you can access from your computer with all rights.	Make a note of the community name and the associated index. For reasons of security, the community name cannot be read later. Treat this community with discretion since everyone who knows the community can access the switch MIB with the IP address of your computer.
2	Limit the access rights of the known communities or delete their entries.	Access to the community access, trap destination and trap configuration table is made via the community index.

SNMP Traps

If unusual events occur during normal operation of the NxS, they are reported immediately to the management station. This is done by means of so-called traps-alarms - that bypass the polling procedure ("Polling" means to query the data stations in regular intervals). Traps make it possible to react quickly to critical situations.
Examples for such events are:

- hardware reset
- changing the basic device configuration
- segmentation of a port

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.
The management agent sends traps to those hosts that are entered in the target table (trap destination table). The trap destination table can be configured with the management station via SNMP.

SNMP Trap Listing

All possible traps that can occur are listed in the following table.

Trap	**Is sent**
authenticationFailure	if a station attempts to access an agent without permission.
coldStart	for a cold and warm start during the boot process after successful management initialization. The trap coldStart is sent during every boot procedure.
saPowerSupply	if the status of the voltage supply changes.
saSignallingRelay	if the status of the signal contact changes.
saStandby	if the operating state of the NxS changes.
linkDown	if the link to a port breaks.
linkUp	if the link to a port is re-established.
risingAlarm	if an alarm input exceeds the upper threshold.
fallingAlarm	if an alarm input falls below the lower threshold.

saPortSecurityTrap	if a MAC address is detected at the port that does not correspond to the current settings of:
	`saPortSecPermission`
	and
	`saPorSecAction` set either to `trapOnly` (2) or `portDisable` (3).

Web-Based Management

5

At a Glance

Overview

The NxS supports both SNMP management and Web-based management and can thus offer extensive diagnostic and configuration functions for fast startup and extensive network and device information.
The NxS supports the TCP/IP protocol family.
The user-friendly web-based (hypertext) interface gives you the option of managing the NxS from any location in the network via a standard browser such as the Netscape Navigator/Communicator or the Microsoft Internet Explorer version 4.x or higher. As a universal access tool, the Web browser can then directly communicate with the NxS via the HTTP protocol. The Web-based interface allows you to graphically configure the NxS.

What's in this Chapter?

This chapter contains the following sections:

5.1 Starting the Web-Based Interface

Starting the Web-Based Interface

Requirements

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example, Netscape Navigator/Communicator or Microsoft Internet Explorer version 4.x or later.

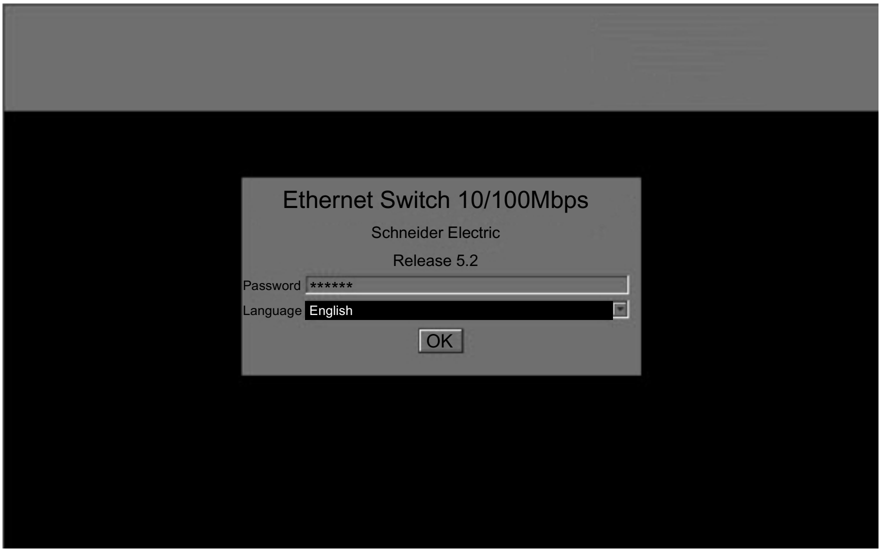
Enabling the Web-Based Interface

The following table shows the steps to enable the Web-based interface.

Step	Action	Comment
1	Start your Web browser.	
2	Make sure that you have activated JavaScript in your browser.	
3	Establish the connection by entering the IP address of the NxS, with which you want to administer the Web-based network management in the address field of the Web browser. Enter the address in the following form: `http://xxx.xxx.xxx.xxx`	The Web-based interface uses the "Java(tm) Runtime Environment Version 1.4" plug-in. If it is not yet installed on your computer, it will be installed automatically via the Internet when you start the Web-based interface. This installation is very time consuming. **For Windows NT users:** Cancel the installation. Install the plug-in from the enclosed CD-ROM. Proceed by starting the program file **j2re1_4_0-win-i.exe** in the Java directory on the CD-ROM.

Logging In to the NxS

The NxS login window will appear on the screen.



Ethernet Switch 10/100Mbps

Schneider Electric

Release 5.2

Password ******

Language English

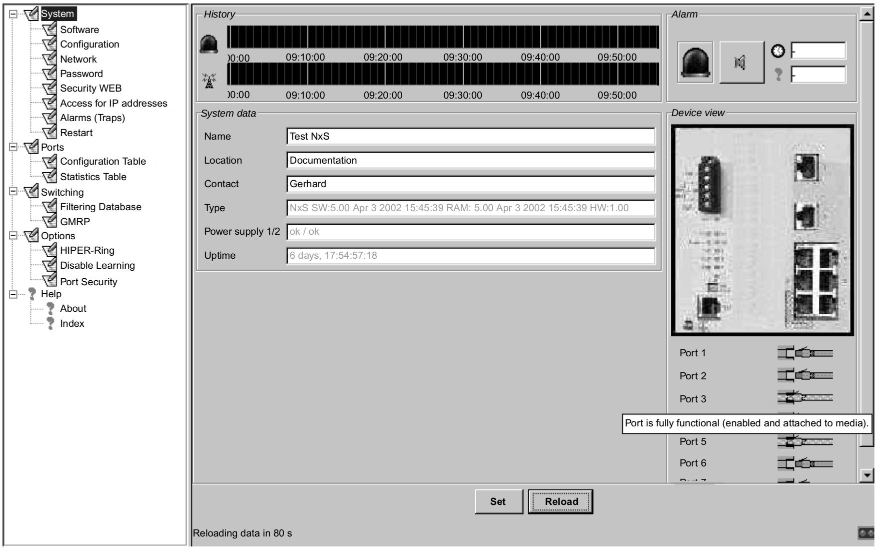
Completing the Login

The following table shows the steps to complete the NxS login.

Step	Action	Comment
1	Select the desired language.	
2	Enter password.	The password "public" appears in the password field, which logs in with read permission. If you wish to access the NxS with write permission, then highlight the contents of the password field and overwrite it with the password "private" (Factory default setting). Changing the password protects NxS against unauthorized access.
3	Click OK.	The home page of the NxS appears on the screen.

The NxS Home Page

The home page of the NxS Web site appears.



Name	Test NxS
Location	Documentation
Contact	Gerhard
Type	NxS SW:5.00 Apr 3 2002 15:45:39 RAM: 5.00 Apr 3 2002 15:45:39 HW:1.00
Power supply 1/2	ok / ok
Uptime	6 days, 17:54:57:18

Port is fully functional (enabled and attached to media).

Reloading data in 80 s

5.2 Operating the Web-Based Interface

Operating the Web-Based Interface

Information

The information section of the NxS home page (right side) is divided into the following items.

- history
- alarm
- system data
- device view
- port status
- updating

Configuration

The configuration section of the NxS home page (left side) displays the following menu items.

System

- software update
- configuration
- network parameters
- password
- Web access
- IP address access
- alarm (traps)
- restart

Ports

- configuration table
- statistics table

Switching

- filtering database
- GMRP

Options

- HIPER-Ring
- disable learning
- port security

Help

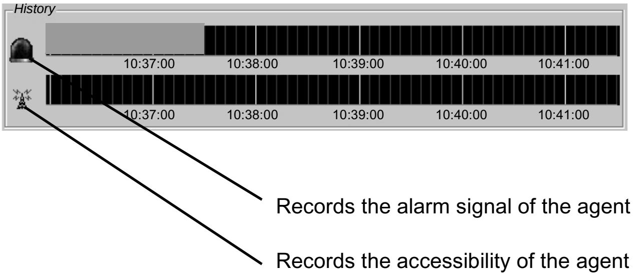
- about
- index

5.3 NxS Home Page -- Information

Information

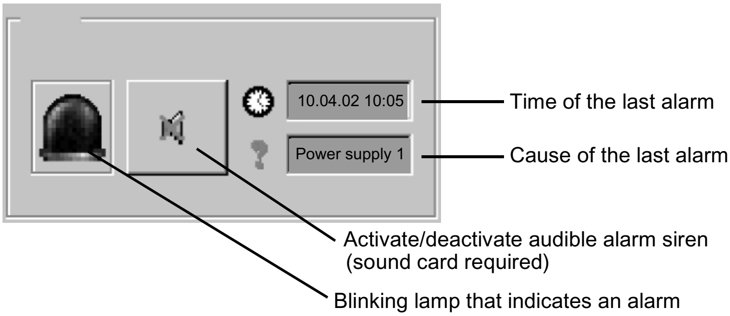
History

This portion of the home page shows the history of the NxS. Since the history is maintained by the Web browser applet, the history is available only while the applet is running.



Alarm

This portion of the home page provides information on the alarm state of the NxS.



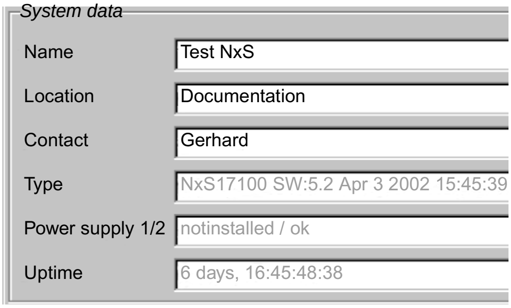
10.04.02 10:05

Power supply 1

Time of the last alarm
Cause of the last alarm
Activate/deactivate audible alarm siren
(sound card required)
Blinking lamp that indicates an alarm

System Data

This portion of the home page displays the system history of the agent.

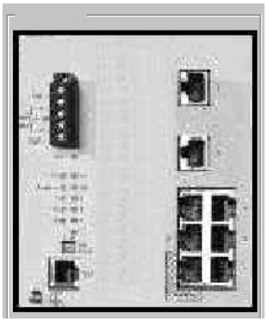


System data

Name	Test NxS	- System name of the switch
Location	Documentation	- Location of the switch
Contact	Gerhard	- Contact person for the switch
Type	NxS17100 SW:5.2 Apr 3 2002 15:45:39	- Software and hardware version
Power supply 1/2	notinstalled / ok	- Status of the power supply units
Uptime	6 days, 16:45:48:38	- Time that has elapsed since the switch was last restarted

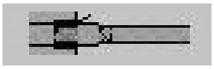
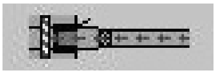
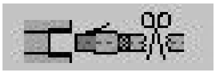
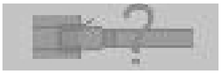
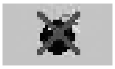
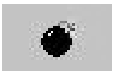
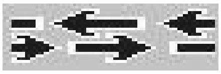
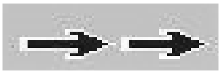
Device View

This portion of the home page displays the switch basic module with the current configuration. The symbols underneath the device view represent the status of the individual ports.



Port Status

The following table describes the meaning of the port symbols.

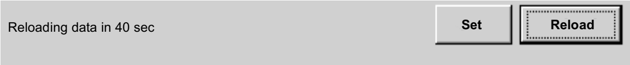
Symbol	Meaning
	The port is enabled, and the connection is OK.
	The port is locked by management.
	The port is enabled, and the connection is interrupted.
	The NxS cannot be reached. A false password may have been entered.
	The trap, triggered by a connection error, is deactivated.
	The trap, triggered by a connection error, is activated.
	Port is in full-duplex operation.
	Port is in half-duplex operation.

The following settings are required on ports 6 and 7 for the ring redundancy (See *Redundant Coupling of Network Segments, p. 59*).

- 100 Mbps
- full duplex
- autonegotiation off
- operation on

Updating

This area displays the countdown time until the applet requests the current data of this dialog again. Click **Reload** to refresh this data immediately. By default, the data is refreshed automatically every 100 seconds.



Reloading data in 40 sec

5.4 NxS Home Page -- Configuration

At a Glance

Overview

This section provides information on the following menu functions.

System
- software update
- configuration
- network parameters
- password
- Web access
- IP address access
- alarm (traps)
- restart

Ports
- configuration table
- statistics table

Switching
- filtering database
- GMRP

Options
- HIPER-Ring
- disable learning
- port security

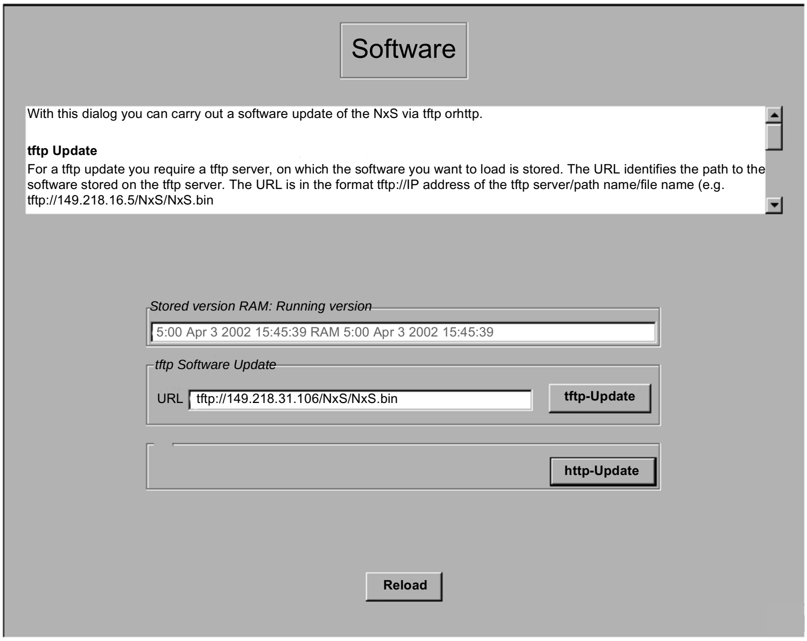
What's in this Section?

This section contains the following topics:

System Menu

Update the Software

You can update the software for the NxS via **tftp** or **http**. Before you update, you need to know the correct location (pathname) of the update file. The following figure shows the **Software** update screen.



Software

With this dialog you can carry out a software update of the NxS via tftp orhttp.

tftp Update

For a tftp update you require a tftp server, on which the software you want to load is stored. The URL identifies the path to the software stored on the tftp server. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. tftp://149.218.16.5/NxS/NxS.bin

Stored version RAM: Running version

5:00 Apr 3 2002 15:45:39 RAM 5:00 Apr 3 2002 15:45:39

tftp Software Update

URL tftp://149.218.31.106/NxS/NxS.bin

Follow these steps to update the software.

Type of Update	Action	Comments
tftp	Enter the correct pathname in the field URL, and click **tftp Update**.	Example of a pathname: tftp://149.218.16.5/NxS/NxS.bin
http	● Enter the correct pathname in the field URL, and click **http Update**.	A second browser window opens.
	● Click **Search** to select the software to update. ● Click **Update** to transfer the software to the switch.	One of the following messages will appear on screen when the update is complete. ● Update completed successfully. ● Update failed. Reason: incorrect file. ● Update failed. Reason: file damaged. ● Update failed. Reason: flash error.
	● Click **File: close**.	You will return to the software window.

After a restart, your browser is able to load the new release of the Web-based interface.

Note: Delete the browser's cache after the software update and before restarting the switch.

Load/Store the Configuration

This window offers the option of storing a user-defined configuration. This configuration can be reloaded

- automatically during a reboot or
- after a reboot with the default settings.

The configuration can be either saved or loaded in flash memory or to a tftp server. The path for storing the configuration data is displayed in the line **URL**.
tftp is not able to create a new file. Therefore, create an empty file on the tftp server before you click **Save to URL**.

Auto Configuration Adapter (ACA)

The Auto Configuration Adapter (ACA) is a device for storing the configuration data of an NxS switch. In the case of a switch failure, the ACA enables a very simple configuration data transfer by means of a substitute switch of the same type.

Storing the Configuration Data in the ACA

You can transfer the current switch configuration onto the ACA by clicking **Save local configuration**.

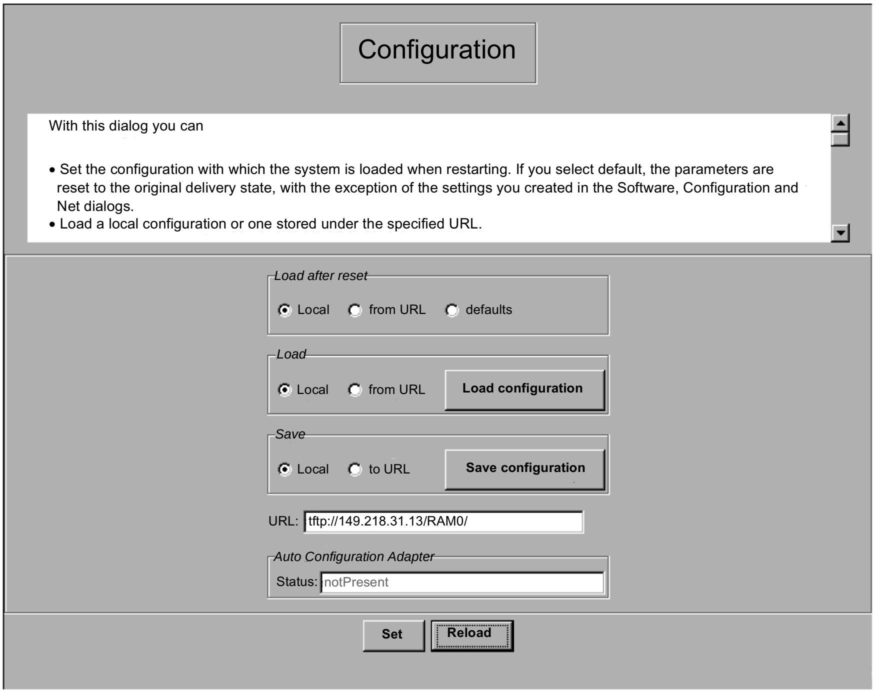
Transferring the Configuration Data from the ACA

When you restart, the switch compares the content of the ACA with its own configuration data. If the data is not consistent, the switch assumes the configuration data of the ACA. After the restart, you can permanently transfer the configuration data of the ACA into the local memory of the switch by clicking **Save local configuration**. The following table outlines the ACA status.

Status	Meaning
notPresent	No ACA present.
ok	The configuration data from the ACA and the switch are consistent.
removed	The ACA has been removed after rebooting.
notInSync	The configuration data from the ACA and the switch are not consistent.
outOfMemory	The local configuration data is too extensive to be stored on the ACA.
wrongMachine	The configuration data in the ACA comes from another device type.
checksumErr	The configuration data is damaged.

Save to a tftp Server

The following figure shows the **Configuration** screen.



Configuration

With this dialog you can

- Set the configuration with which the system is loaded when restarting. If you select default, the parameters are reset to the original delivery state, with the exception of the settings you created in the Software, Configuration and Net dialogs.
- Load a local configuration or one stored under the specified URL.

Load after reset

● Local ○ from URL ○ defaults

Load

● Local ○ from URL [Load configuration]

Save

● Local ○ to URL [Save configuration]

URL: tftp://149.218.31.13/RAM0/

Auto Configuration Adapter

Status: notPresent

Use the following steps to save to a tftp server.

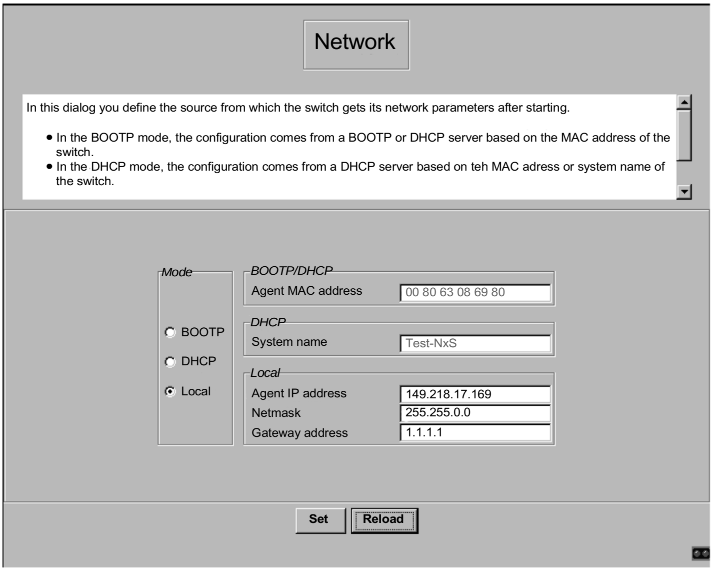
Step	Action
1	Open a new file with any editor.
2	Save the empty file to the appropriate path of the tftp server, including the file name, e.g. **RAM0/Switch_Role_Name.prm**
3	In the **URL** line, enter the path of the tftp server, e.g. **tftp://149.218.076.214//RAM0/Switch_Role_Name.prm**.
4	View the status of the Auto Configuration Adapter.

tftp Server Security

The configuration file includes all configuration data including the password, so set the access rights on the tftp server appropriately.

Set Network Parameters

The following figure shows the **Network** parameters page.



Network

In this dialog you define the source from which the switch gets its network parameters after starting.

- In the BOOTP mode, the configuration comes from a BOOTP or DHCP server based on the MAC address of the switch.
- In the DHCP mode, the configuration comes from a DHCP server based on teh MAC adress or system name of the switch.

Mode

○ BOOTP
○ DHCP
● Local

BOOTP/DHCP

Agent MAC address: 00 80 63 08 69 80

DHCP

System name: Test-NxS

Local

Agent IP address: 149.218.17.169
Netmask: 255.255.0.0
Gateway address: 1.1.1.1

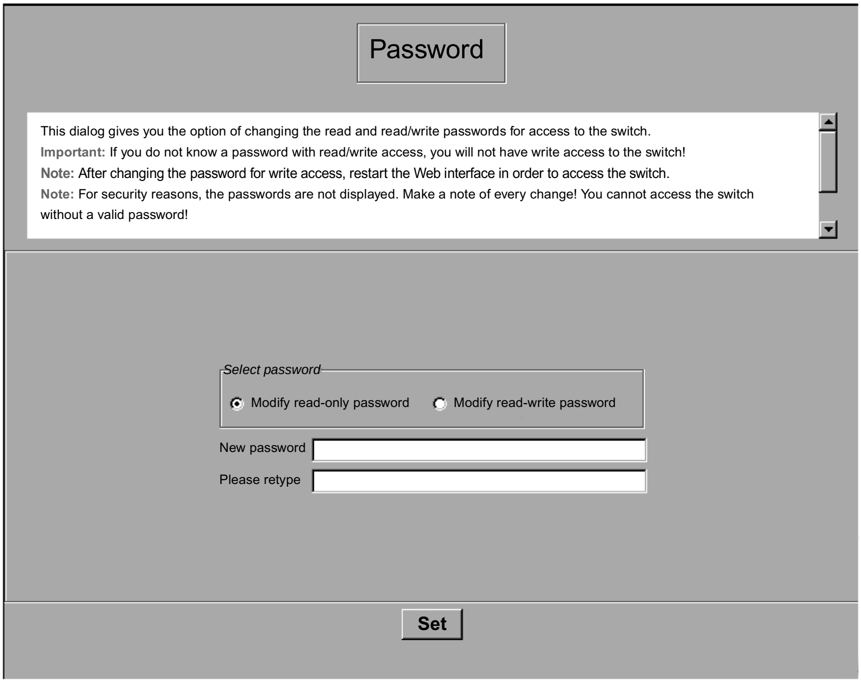
Follow the steps below to assign the network parameters.

Step	Action
1	Under **Mode**, enter where the NxS will obtain its IP parameters. ● BOOTP (see *BOOTP (BOOTstrap Protocol), p. 28*) ● DHCP (see *DHCP, p. 29*) ● Local
2	Enter the parameters according to the selected mode at the right.

Change the Password

Use the following steps to change the password.

Step	Action
1	Enter the new password in the **New password** line.
2	Repeat the new password in the **Please re-enter** line. (Please note that passwords are case-sensitive.)
3	Click **Set**.



This dialog gives you the option of changing the read and read/write passwords for access to the switch.

Important: If you do not know a password with read/write access, you will not have write access to the switch!

Note: After changing the password for write access, restart the Web interface in order to access the switch.

Note: For security reasons, the passwords are not displayed. Make a note of every change! You cannot access the switch without a valid password!

Select password

● Modify read-only password ○ Modify read-write password

New password

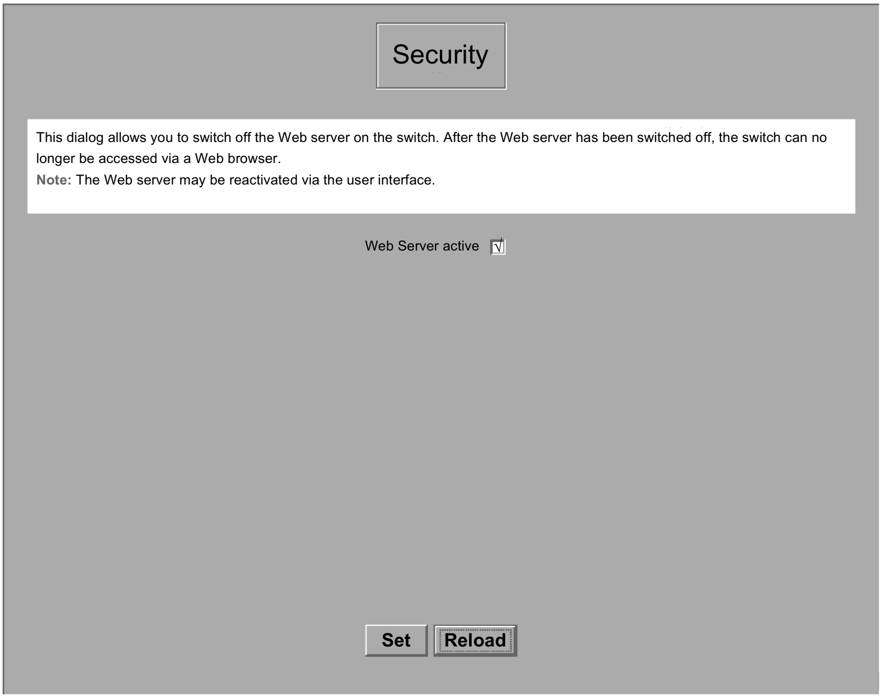
Please retype

Note:

- After you change the password for write access, restart the Web interface in order to access the switch.
- For security reasons, the passwords are not displayed. Make a note of every change because you cannot access the switch without a valid password.

Web Access

This window allows you to turn off the Web server on the switch. After the Web server has been turned off, the switch can no longer be accessed via a Web browser.



Security

This dialog allows you to switch off the Web server on the switch. After the Web server has been switched off, the switch can no longer be accessed via a Web browser.
Note: The Web server may be reactivated via the user interface.

Web Server active ☑

Note: You can reactivate the Web server through the user interface.

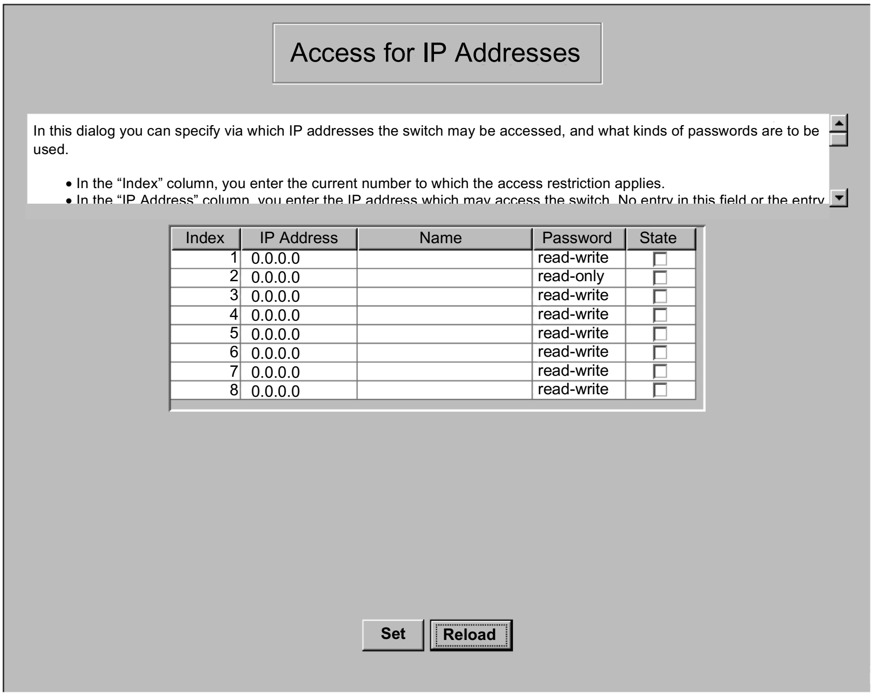
IP Address Access

You can specify which IP addresses may access the switch and what kinds of passwords may be used.

Column	Action
Index	Enter the current number to which the access restriction applies.
IP Address	Enter the IP address that may access the switch.
Name	Enter a name of your choice for the computer with this IP address.
Password	Specify whether this computer can access the switch withthe read or the read/ write password.
State	Mark the entries to which access control applies.

Note:

- If you leave any of the entries blank, there will be no access restrictions. Any computer with any IP address may access the switch.
- Make sure that at least one of the fields has a read/write password, so that you ensure yourself write access to the switch.



Access for IP Addresses

In this dialog you can specify via which IP addresses the switch may be accessed, and what kinds of passwords are to be used.

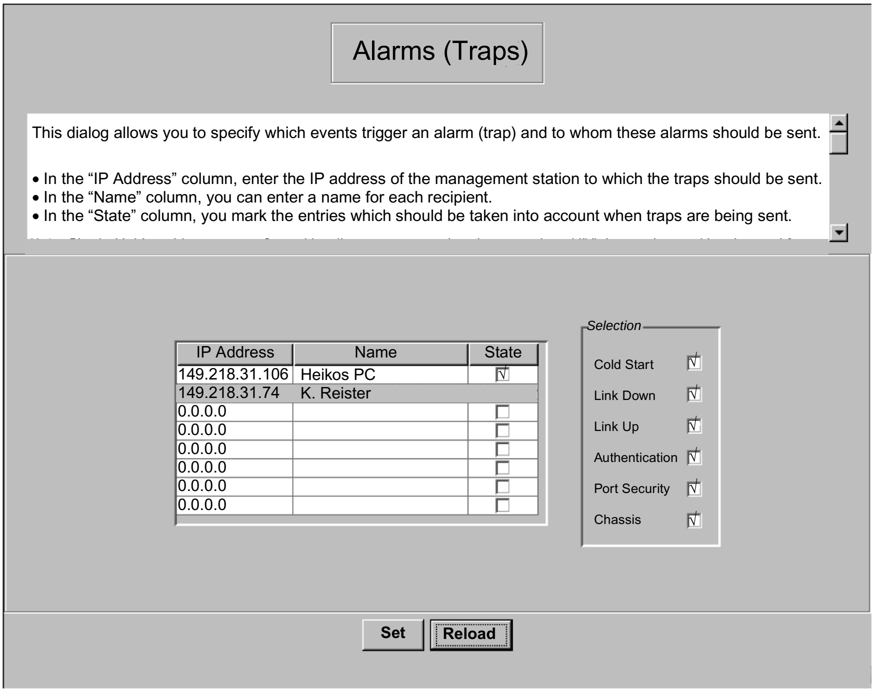
- In the “Index” column, you enter the current number to which the access restriction applies.
- In the “IP Address” column, you enter the IP address which may access the switch. No entry in this field or the entry

Index	IP Address	Name	Password	State
1	0.0.0.0		read-write	□
2	0.0.0.0		read-only	□
3	0.0.0.0		read-write	□
4	0.0.0.0		read-write	□
5	0.0.0.0		read-write	□
6	0.0.0.0		read-write	□
7	0.0.0.0		read-write	□
8	0.0.0.0		read-write	□

Configure Alarms (Traps)

This window allows you to specify which actions trigger an alarm (trap) and who is notified about these alarms.

Column	Action
IP Address	Enter the IP address of the management station where the alarms should be sent.
Name	Enter a name for each recipient.
State	Mark the entries that should be considered when alarms are sent.



Alarms (Traps)

This dialog allows you to specify which events trigger an alarm (trap) and to whom these alarms should be sent.

- In the “IP Address” column, enter the IP address of the management station to which the traps should be sent.
- In the “Name” column, you can enter a name for each recipient.
- In the “State” column, you mark the entries which should be taken into account when traps are being sent.

IP Address	Name	State
149.218.31.106	Heikos PC	☑
149.218.31.74	K. Reister	
0.0.0.0		□
0.0.0.0		□
0.0.0.0		□
0.0.0.0		□
0.0.0.0		□
0.0.0.0		□

Selection

Cold Start ☑

Link Down ☑

Link Up ☑

Authentication ☑

Port Security ☑

Chassis ☑

You can select the following events to trigger an alarm.

Event	Description
Cold Start	The switch has been turned on.
Link Down	The link to the device at one port of the switch has been interrupted.
Link Up	The link to the device at one port of the switch has been established.
Authentication	The switch has rejected an unauthorized access attempt. (See *IP Address Access, p. 80*.
Port Security	A data packet has been received on one port from an unauthorized terminal device.
Chassis	● **Power supply:** The status of a supply voltage has changed. ● **Signaling Relay:** The status of the signal contact has changed. ● **Standby:** The status of the redundancy manager has changed. ● **AutoConfigAdapter:** The AutoConfiguration Adapter (ACA) has been inserted or removed.

Restart the Switch

This window allows you to restart the switch.

Note: During the restart, the switch temporarily does not transfer any data, and it cannot be accessed via the Web-based interface or other management systems.

Ports Menu

Overview

The ports menu includes

- a configuration table and
- a statistics table.

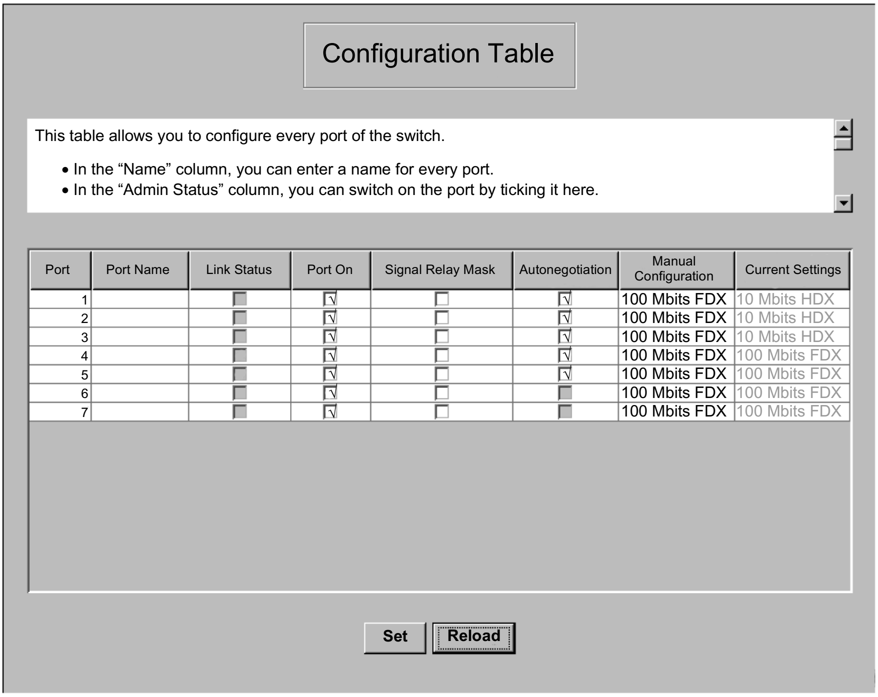
Configuration Table

The configuration table allows you to configure every port of the switch.

Column	**Action**
Name	Enter a name for every port.
Port On	Switch on the port by marking it in this column.
Signal Relay Mask	Specify whether the signal contact should be opened when a link alarm occurs.
Autonegotiation	Activate the automatic selection of a port's operating mode by marking the appropriate field. After the autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.
Manual Configuration	Set the operating mode for this port. The choice of operating modes, listed below, depends on the media module. ● 10 Mbits half duplex (HDX) ● 10 Mbits full duplex (FDX) ● 100 Mbits HDX ● 100 Mbits FDX **Note:** The active automatic configuration has priority over the manual configuration.

Note: The following settings are required for the ring ports. (See *Redundant Ring Structure, p. 58*.)

- 100 Mbits
- full duplex
- autonegotiaion off
- port on



Configuration Table

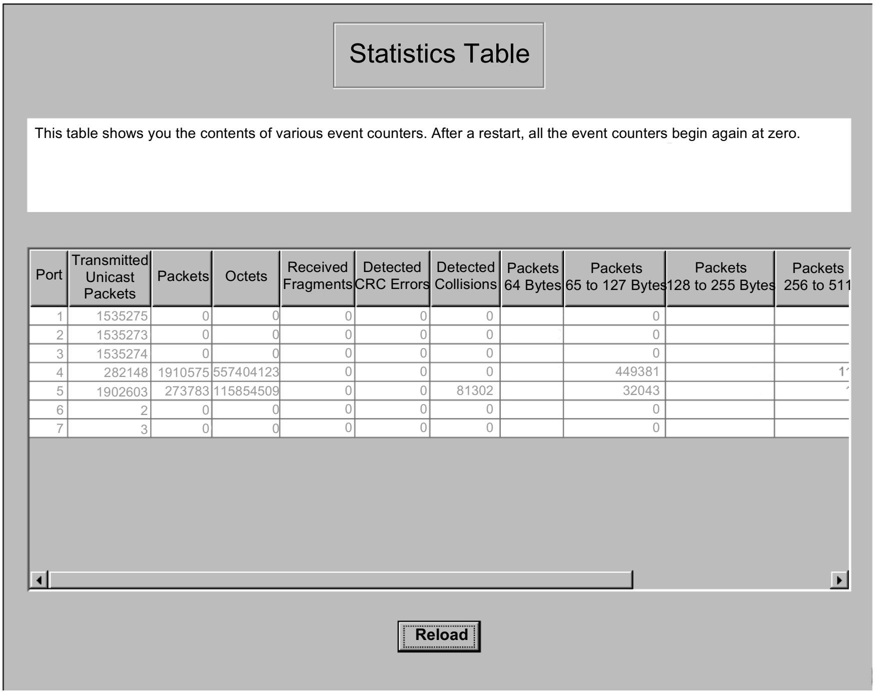
This table allows you to configure every port of the switch.

- In the “Name” column, you can enter a name for every port.
- In the “Admin Status” column, you can switch on the port by ticking it here.

Port	Port Name	Link Status	Port On	Signal Relay Mask	Autonegotiation	Manual Configuration	Current Settings
1		□	☑	□	☑	100 Mbits FDX	10 Mbits HDX
2		□	☑	□	☑	100 Mbits FDX	10 Mbits HDX
3		□	☑	□	☑	100 Mbits FDX	10 Mbits HDX
4		□	☑	□	☑	100 Mbits FDX	100 Mbits FDX
5		□	☑	□	☑	100 Mbits FDX	100 Mbits FDX
6		□	☑	□	□	100 Mbits FDX	100 Mbits FDX
7		□	☑	□	□	100 Mbits FDX	100 Mbits FDX

Statistics Table

The statistics table shows you the contents of various event counters. After a restart, all event counters begin again at zero.



Statistics Table

This table shows you the contents of various event counters. After a restart, all the event counters begin again at zero.

Port	Transmitted Unicast Packets	Packets	Octets	Received Fragments	Detected CRC Errors	Detected Collisions	Packets 64 Bytes	Packets 65 to 127 Bytes	Packets 128 to 255 Bytes	Packets 256 to 511
1	1535275	0	0	0	0	0		0		
2	1535273	0	0	0	0	0		0		
3	1535274	0	0	0	0	0		0		
4	282148	1910575	557404123	0	0	0		449381		1
5	1902603	273783	115854509	0	0	81302		32043		
6	2	0	0	0	0	0		0		
7	3	0	0	0	0	0		0		

Switching Menu

Overview

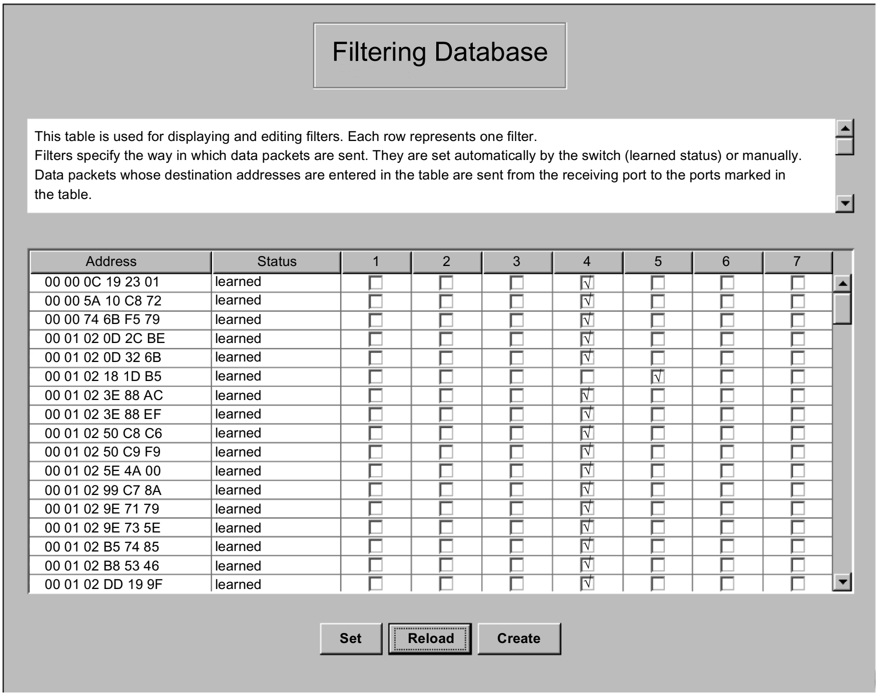
The switching menu includes
- the filter table and
- the GMRP configuration.

Filter Table

The filter table is used for displaying and editing filters. Each row represents one filter. Filters specify the way data packets are sent. They are set automatically by the switch (learned status) or manually. Data packets whose destination addresses are entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination addresses are not in the table are sent from the receiving port to all other ports. The following status settings are possible.

Status	Description
Learned	The switch automatically created the filter.
Invalid	Delete a manually created filter.
Permanent	Filter is stored permanently in the switch or on the URL (see *Load/ Store the Configuration, p. 75*).
DeleteOnReset	Filter is deleted when the switch is reset.
GMRP	Filter was created by GMRP.
GMRP/Permanent	GRMRP added port markings to the filter after the administrator created it. The port markings added by the GMRP are deleted by a restart.
GMRP/DeleteOnReset	Filter was created by the administrator and extended by the GMRP with further port markings. The filter is deleted when the switch is reset.

Note: You can set up new filters by clicking **Create**.



Filtering Database

This table is used for displaying and editing filters. Each row represents one filter.
Filters specify the way in which data packets are sent. They are set automatically by the switch (learned status) or manually.
Data packets whose destination addresses are entered in the table are sent from the receiving port to the ports marked in the table.

Address	Status	1	2	3	4	5	6	7
00 00 0C 19 23 01	learned	☐	☐	☐	☑	☐	☐	☐
00 00 5A 10 C8 72	learned	☐	☐	☐	☑	☐	☐	☐
00 00 74 6B F5 79	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 0D 2C BE	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 0D 32 6B	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 18 1D B5	learned	☐	☐	☐	☐	☑	☐	☐
00 01 02 3E 88 AC	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 3E 88 EF	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 50 C8 C6	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 50 C9 F9	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 5E 4A 00	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 99 C7 8A	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 9E 71 79	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 9E 73 5E	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 B5 74 85	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 B8 53 46	learned	☐	☐	☐	☑	☐	☐	☐
00 01 02 DD 19 9F	learned	☐	☐	☐	☑	☐	☐	☐

Note: If the redundancy manager is active (see *Redundant Ring Structure, p. 58*), it is not possible to make permanent unicast entries.

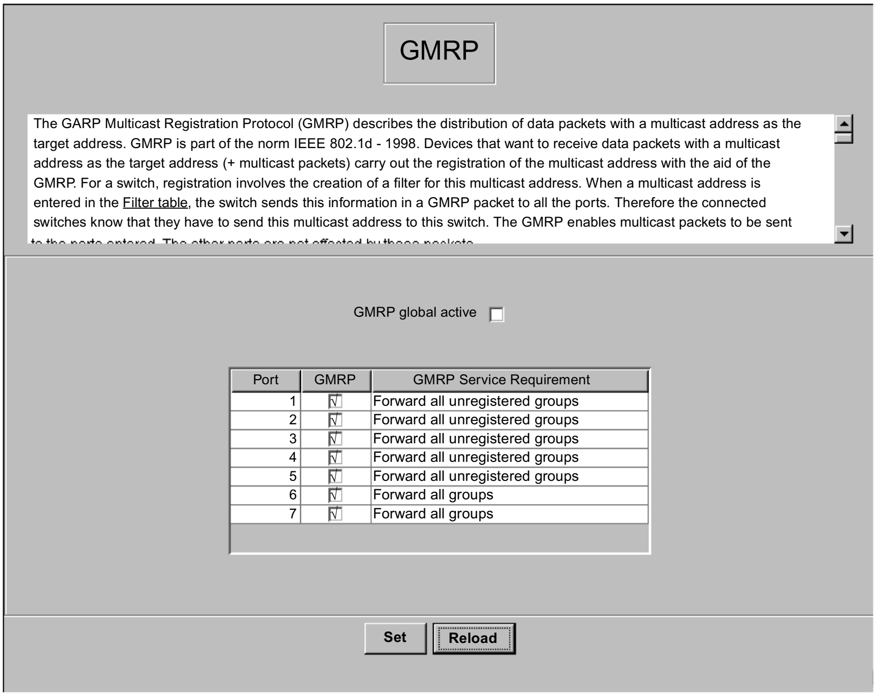
GMRP

The GARP Multicast Registration Protocol (GMRP) describes the distribution of data packets with a multicast address as the target address. Devices that want to receive data packets with a multicast address as the target address carry out the registration of the multicast address with the help of GMRP. For a switch, registration involves entering the multicast address in the filter table. When this is done, the switch sends the information in a GMRP packet to all ports. Therefore, the connected switches know that they have to send this multicast address to the respective switch. The GMRP enables packets with a multicast address in the target address field to be sent to the ports entered. The remaining ports are not affected by these packets. Data packets with unregistered multicast addresses are sent to all ports by the switch.
Below are the basic settings of the GMRP.

Field	Description
Global GMRP	You can switch the GMRP on/off globally for the entire switch. If the GMRP is switched off, then ● the switch does not generate any GMRP [packets, ● it does not evaluate any GMRP packets received, discards them, and ● it sends (streams) received data packets with a multicast address as the target address to all ports.
GMRP per port	You can switch on/off the GMRP for each port. When you switch off the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be sent from this port.
Transmission per port	This field describes the **GMRP service requirements** of the terminal device on the entire network. ● With the **selective** setting (GMRP default setting: forward all unregistered groups), the switch sends all data packets with a multicast address in the target address field, which 1) is entered into the filter table for the port OR 2) for which no entry exists in the filter table. ● With the **all** setting (GMRP default setting: forward all groups), the switch sends all data packets with a multicast address in the target address field.

Note: In the event of a ring interruption, if the switch is connected to a HIPER-Ring, you can quickly reconfigure the network for data packets with registered multicast target addresses by

- switching on the GMRP globally and on the ring ports and
- selecting the **all** transmission type per port on the ring ports.



GMRP

The GARP Multicast Registration Protocol (GMRP) describes the distribution of data packets with a multicast address as the target address. GMRP is part of the norm IEEE 802.1d - 1998. Devices that want to receive data packets with a multicast address as the target address (+ multicast packets) carry out the registration of the multicast address with the aid of the GMRP. For a switch, registration involves the creation of a filter for this multicast address. When a multicast address is entered in the Filter table, the switch sends this information in a GMRP packet to all the ports. Therefore the connected switches know that they have to send this multicast address to this switch. The GMRP enables multicast packets to be sent to the ports entered. The other ports are not affected by these packets.

GMRP global active □

Port	GMRP	GMRP Service Requirement
1	☑	Forward all unregistered groups
2	☑	Forward all unregistered groups
3	☑	Forward all unregistered groups
4	☑	Forward all unregistered groups
5	☑	Forward all unregistered groups
6	☑	Forward all groups
7	☑	Forward all groups

Options Menu

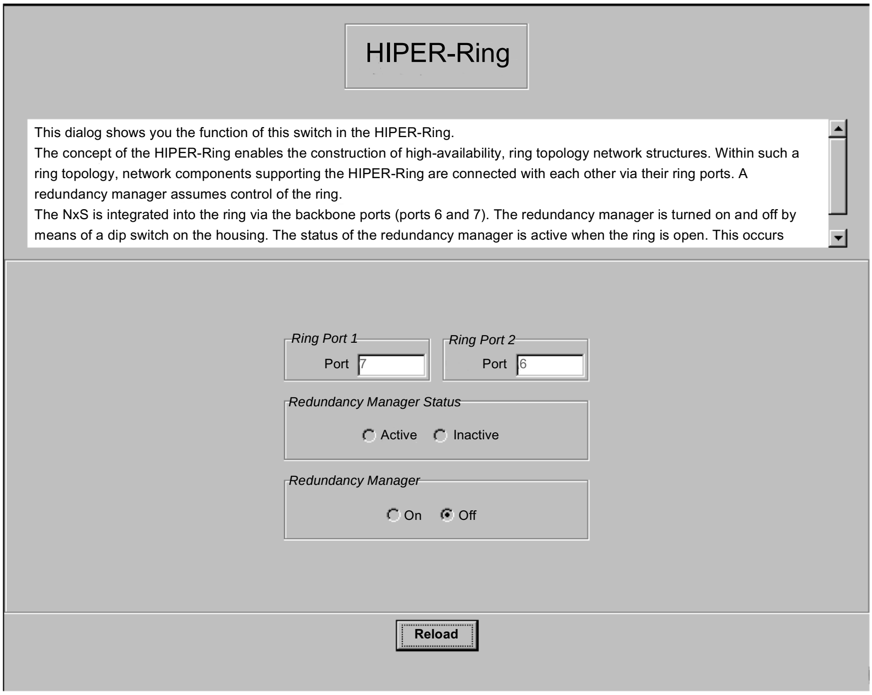
Overview

The options menu includes

- configuring the HIPER-Ring function,
- switching the learn function on and off, and
- setting port security.

Configuring the HIPER-Ring Function

This window shows you the function of the switch in the HIPER-Ring. The concept of the HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring. The NxS is integrated into the ring via the backbone ports (ports 6 and 7). The redundancy manager is turned on and off by means of a dip switch on the housing. The status of the redundancy manager is active when the ring is open. This occurs, for example, when a data cable or a network component within the ring is down.



HIPER-Ring

This dialog shows you the function of this switch in the HIPER-Ring.
The concept of the HIPER-Ring enables the construction of high-availability, ring topology network structures. Within such a ring topology, network components supporting the HIPER-Ring are connected with each other via their ring ports. A redundancy manager assumes control of the ring.
The NxS is integrated into the ring via the backbone ports (ports 6 and 7). The redundancy manager is turned on and off by means of a dip switch on the housing. The status of the redundancy manager is active when the ring is open. This occurs

Ring Port 1: Port 7

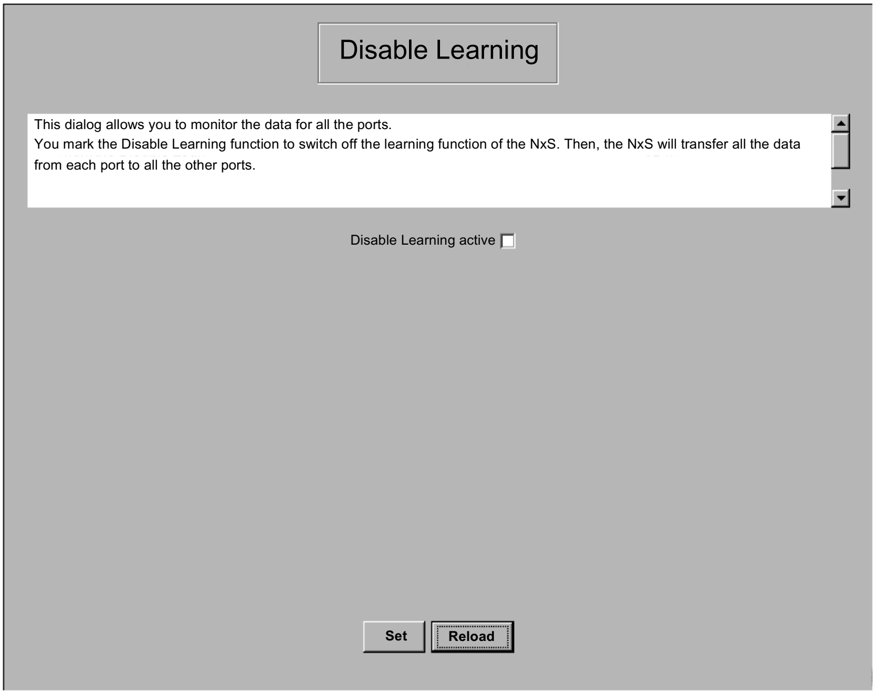
Ring Port 2: Port 6

Redundancy Manager Status: ○ Active ○ Inactive

Redundancy Manager: ○ On ● Off

Disable Learning

This window allows you to monitor the data for all ports. You mark the Disable Learning function to switch off the learning function of the NxS. Then, the NxS will transfer all data from each port to all other ports.



Disable Learning

This dialog allows you to monitor the data for all the ports.
You mark the Disable Learning function to switch off the learning function of the NxS. Then, the NxS will transfer all the data from each port to all the other ports.

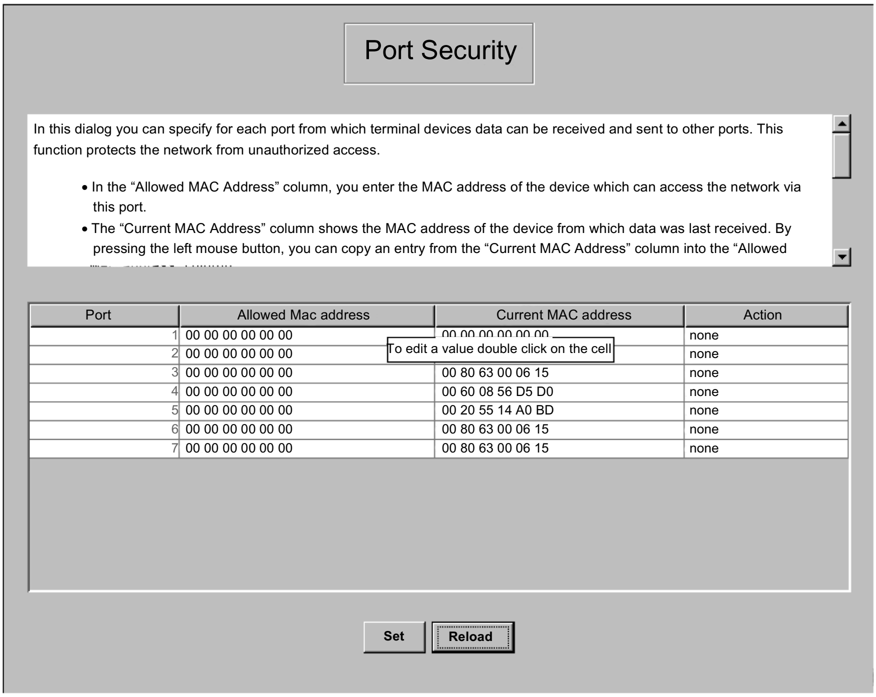
Disable Learning active □

Set the Port Security

In this window you can specify for each port which terminal devices receive and send data. This function protects the network from unauthorized access.

Column	Action
Allowed MAC Address	Enter the MAC address of the device with which a data exchange at this port is permitted.
Current MAC Address	Displays the MAC address of the device that last received data. By clicking the left mouse button, you can copy an entry from the **Current MAC address** column into the **Allowed MAC address** column.
Action	Select whether an unauthorized access attempt should be followed by ● no action (none), ● sending an alarm (trapOnly), or ● switching off the port and sending an alarm (portDisable).

Note: You can only send an alarm (trap) if at least one recipient is entered under Alarms (Traps), and both the appropriate status and **Authentication** are marked.



Port Security

In this dialog you can specify for each port from which terminal devices data can be received and sent to other ports. This function protects the network from unauthorized access.

- In the “Allowed MAC Address” column, you enter the MAC address of the device which can access the network via this port.
- The “Current MAC Address” column shows the MAC address of the device from which data was last received. By pressing the left mouse button, you can copy an entry from the “Current MAC Address” column into the “Allowed

Port	Allowed Mac address	Current MAC address	Action
1	00 00 00 00 00 00	00 00 00 00 00 00	none
2	00 00 00 00 00 00		none
3	00 00 00 00 00 00	00 80 63 00 06 15	none
4	00 00 00 00 00 00	00 60 08 56 D5 D0	none
5	00 00 00 00 00 00	00 20 55 14 A0 BD	none
6	00 00 00 00 00 00	00 80 63 00 06 15	none
7	00 00 00 00 00 00	00 80 63 00 06 15	none

To edit a value double click on the cell

Management Information Base (MIB)

6

At a Glance

Overview

This chapter provides information on the design, structure, abbreviations, terms, object groups, and property configuration of the Management Information Base (MIB).

What's in this Chapter?

This chapter contains the following topics:

Management Information Base (MIB)

Overview

The **M**anagement **I**nformation **B**ase (MIB) is designed in the form of an abstract tree structure.

The branching points are the **object classes**. The "leaves" of the MIB are called **generic object classes**. Wherever necessary for unambiguous identification, the generic object classes are **instantiated**, i.e. the abstract structure is imaged on the reality, by specifying the port address or the source address.

Values (integers, timeticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The **object description** or **object ID** (OID) identifies the object class. The subidentifier (SID) is used for instantiation.

Example:

The generic object class

```
saPSState (OID = 1.3.6.1.4.1.3833.1.1.14.1.2.1.3)
```

is the description of the abstract information "power supply state". It is, however, not possible to read any information from this, as the system does not know which power supply is meant.

Specification of the subidentifier (2) images this abstract information on the reality (instantiates it), which means that it refers to power supply 2. A value is assigned to this instance and can then be read. The instance "get 1.3.6.1.4.1.3833.1.1.14.1.2.1.3" for example, returns the response "1", which means that the power supply is running correctly.

MIB Abbreviations

The following table defines the abbreviations used in the MIB.

Abbreviation	Meaning
Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold)
PS	Power supply
Pwr	Supply voltage
sys	System
UI	User Interface
Upr	Upper (e.g. threshold)
ven	Vendor (Schneider Automation)

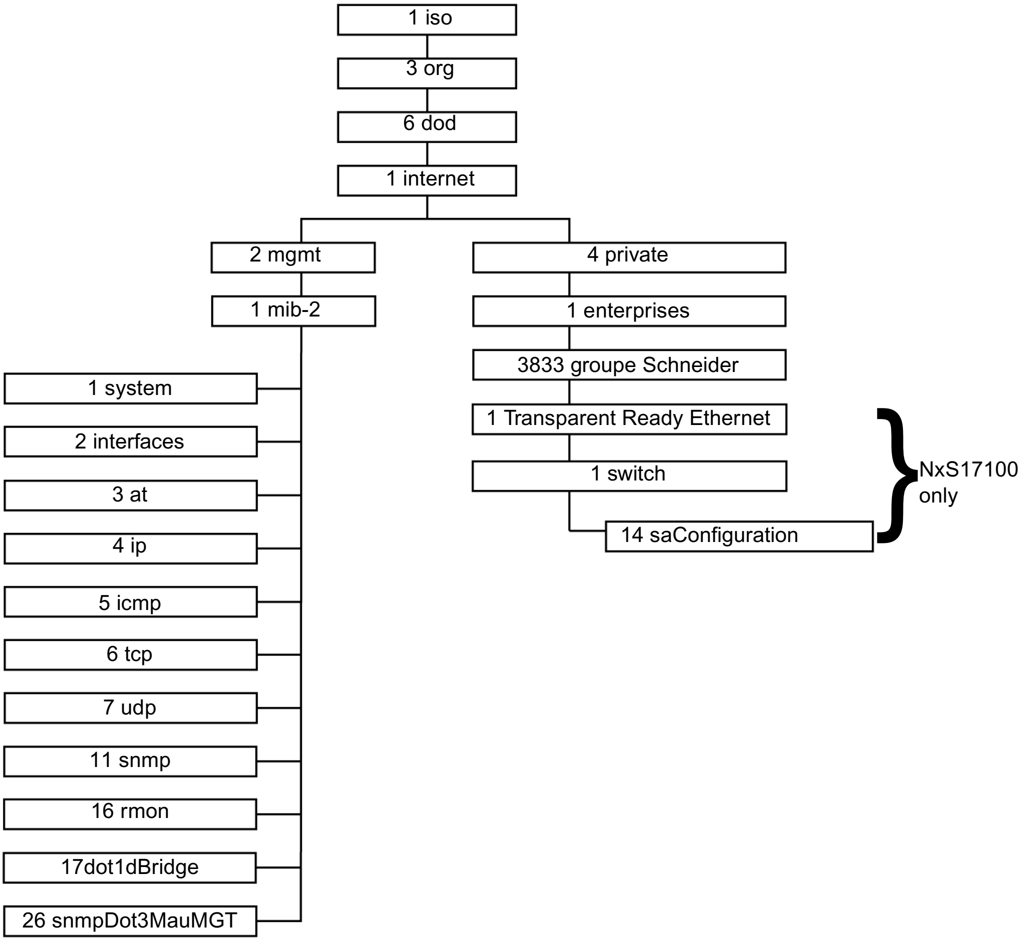
Syntax Definitions

The following table defines the syntax terms used in the MIB.

Term	Definition
Integer	An integer in the range 0-2^{32}
IP address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC address	12-digit hexadecimal number in accordance with ISO / IEC 8802-3
Object Identifier	x.x.x.x... (e.g. 1.3.6.1.1.4.1.3833...)
Octet String	ASCII character string
PSID	Power supply identifier (power supply number)
TimeTicks	Stopwatch Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in the range 0-2^{32}
Timeout	Time value in hundredths of a second Time value = integer in the range 0-2^{32}
Typefield	4-digit hexadecimal number in accordance with ISO / IEC 8802-3
Counter	Integer (0-2^{32}) whose value is incremented by 1 when certain events occur.

MIB Tree Structure

The following flowchart describes the tree structure of the switch MIB.



Note: Not all devices support all object classes. The value "not supported" is given in response to a non-supported object class request. Any attempt to alter a non-supported object class produces the message "badValue".

MIB II

System Group (1.3.6.1.2.1.1)

The system group is a required group for all systems. It contains system-related objects. If an agent has no value for a variable, then the response returned includes a string of length 0.

```
(1) system
     |-- (1) sysDescr
     |-- (2) sysObjectID
     |-- (3) sysUpTime
     |-- (4) sysContact
     |-- (5) sysName
     |-- (6) sysLocation
     |-- (7) sysServices
```

System Group Objects

The following table describes the member objects of the system group.

Object	OID	Syntax	Access	Description
sysDescr	1.3.6.1.2.1.1.1.0	ASCII String (Size: 0-255)	Read	A verbal description of the entry. This value should contain the full name and version number of type of system hardware, operating system software, and network software. The description must consist only of printable ASCII characters.
sysObjectID	1.3.6.1.2.1.1.2.0	Object identifier	Read	The authorization identification of the manufacturer of the network management system that is integrated in this device. This value is placed in the SMI enterprises subtree (1.3.6.1.4.1) and describes which type of device is being managed. For example: if the manufacturer "Schneider Electric" is assigned the subtree 1.3.6.1.4.1.3833, then he can assign his switch the identifier 1.3.6.1.4.1.3833.1.1.
sysUpTime	1.3.6.1.2.1.1.3.0	Time ticks	Read	The time in 1/100 seconds since the last reset of the network management unit.
sysContact	1.3.6.1.2.1.1.4.0	ASCII string (size: 0-255)	Read and write	The clear-text identification of the contact person for this managed node along with the information about how that person is to be contacted.
sysName	1.3.6.1.2.1.1.5.0	ASCII string (size: 0-255)	Read and write	A name for this node for identifying it for administration. By convention, this is the fully qualified name in the domain.
sysLocation	1.3.6.1.2.1.1.6.0	ASCII string (size: 0-255)	Read and write	The physical location of this node (e.g. "staircase, 3rd floor")
sysServices	1.3.6.1.2.1.1.7.0	Integer (0-127)	Read	This value indicates the services offered by the node. It is an integral value calculated by summing $2^{(layer - 1)}$ for each ISO layer for which the node provides service. For example: A node primarily provides routing functions (OSI layer 3): sysServices = $2^{(3-1)}$ = 4 A node is a host and offers application and network services (OSI layers 4 and 7): sysServices = $2^{(4-1)} + 2^{(7-1)}$ = 72

Interface Group (1.3.6.1.2.1.2)

The interface group contains information about the device interfaces.

```
(2) interfaces
    |-- (1) ifNumber
    |-- (2) ifTable
        |-- (1) ifEntry
            |-- (1) ifIndex
            |-- (2) ifDescr
            |-- (3) ifType
            |-- (4) ifMtu
            |-- (5) ifSpeed
            |-- (6) ifPhysAddress
            |-- (7) ifAdminStatus
            |-- (8) ifOperStatus
            |-- (9) ifLastChange
            |-- (10) ifInOctets
            |-- (11) ifInUcastPkts
            |-- (12) ifInNUcastPkts
            |-- (13) ifInDiscards
            |-- (14) ifInErrors
            |-- (15) ifInUnknownProtos
            |-- (16) ifOutOctets
            |-- (17) ifOutUcastPkts
            |-- (18) ifOutNUcastPkts
            |-- (19) ifOutDiscards
            |-- (20) ifOutErrors
            |-- (21) ifOutQLen
            |-- (22) ifSpecific
```

Address Translation Group (1.3.6.1.2.1.3)

The address translation group is required for all systems. It contains information about the assignment of addresses.

```
(3) at
    |-- (1) atTable
        |-- (1) atEntry
            |-- (1) atIfIndex
            |-- (2) atPhysAddress
            |-- (3) atNetAddress
```

Internet Protocol Group (1.3.6.1.2.1.4)

The internet protocol group is required for all systems. It contains information affecting IP switching.

```
(4) ip
    |-- (1) ipForwarding
    |-- (2) ipDefaultTTL
    |-- (3) ipInReceives
    |-- (4) ipInHdrErrors
    |-- (5) ipInAddrErrors
    |-- (6) ipForwDatagrams
    |-- (7) ipInUnknownProtos
    |-- (8) ipInDiscards
    |-- (9) ipInDelivers
    |-- (10) ipOutRequests
    |-- (11) ipOutDiscards
    |-- (12) ipOutNoRoutes
    |-- (13) ipReasmTimeout
    |-- (14) ipReasmReqds
    |-- (15) ipReasmOKs
    |-- (16) ipReasmFails
    |-- (17) ipFragOKs
    |-- (18) ipFragFails
    |-- (19) ipFragCreates
    |-- (20) ipAddrTable
    |    |-- (1) ipAddrEntry
    |        |-- (1) ipAdEntAddr
    |        |-- (2) ipAdEntIfIndex
    |        |-- (3) ipAdEntNetMask
    |        |-- (4) ipAdEntBcastAddr
    |        |-- (5) ipAdEntReasmMaxSize
    |-- (21) ipRouteTable
    |    |-- (1) ipRouteEntry
    |        |-- (1) ipRouteDest
    |        |-- (2) ipRouteIfIndex
    |        |-- (3) ipRouteMetric1
    |        |-- (4) ipRouteMetric2
    |        |-- (5) ipRouteMetric3
    |        |-- (6) ipRouteMetric4
    |        |-- (7) ipRouteNextHop
    |        |-- (8) ipRouteType
    |        |-- (9) ipRouteProto
    |        |-- (10) ipRouteAge
    |        |-- (11) ipRouteMask
    |        |-- (12) ipRouteMetric5
    |        |-- (13) ipRouteInfo
    |-- (22) ipNetToMediaTable
```

```
|    |-- (1) ipNetToMediaEntry
|        |-- (1) ipNetToMediaIfIndex
|        |-- (2) ipNetToMediaPhysAddress
|        |-- (3) ipNetToMediaNetAddress
|        |-- (4) ipNetToMediaType
|-- (23) ipRoutingDiscards
```

ICMP Group (1.3.6.1.2.1.5)

The internet control message protocol group is obligatory for all systems. It contains all the information on error handling and control for data exchange in the Internet.

```
(5) icmp
    |-- (1) icmpInMsgs
    |-- (2) icmpInMsgs
    |-- (3) icmpInDestUnreachs
    |-- (4) icmpInTimeExcds
    |-- (5) icmpInParmProbs
    |-- (6) icmpInSrcQuenchs
    |-- (7) icmpInRedirects
    |-- (8) icmpInEchos
    |-- (9) icmpInEchoReps
    |-- (10) icmpInTimestamps
    |-- (11) icmpInTimestampReps
    |-- (12) icmpInAddrMasks
    |-- (13) icmpInAddrMaskReps
    |-- (14) icmpOutMsgs
    |-- (15) icmpOutErrors
    |-- (16) icmpOutDestUnreachs
    |-- (17) icmpOutTimeExcds
    |-- (18) icmpOutParmProbs
    |-- (19) icmpOutSrcQuenchs
    |-- (20) icmpOutRedirects
    |-- (21) icmpOutEchos
    |-- (22) icmpOutEchoReps
    |-- (23) icmpOutTimestamps
    |-- (24) icmpOutTimestampReps
    |-- (25) icmpOutAddrMasks
    |-- (26) icmpOutAddrMaskReps
```

Transfer Control Protocol Group (1.3.6.1.2.1.6)

The transfer control protocol group is required for all systems that have implemented TCP. Instances of objects that describe information about a particular TCP connection exist only as long as the connection exists.

```
(6) tcp
    |-- (1) tcpRtoAlgorithm
    |-- (2) tcpRtoMin
    |-- (3) tcpRtoMax
    |-- (4) tcpMaxConn
    |-- (5) tcpActiveOpens
    |-- (6) tcpPassiveOpens
    |-- (7) tcpAttemptFails
    |-- (8) tcpEstabResets
    |-- (9) tcpCurrEstab
    |-- (10) tcpInSegs
    |-- (11) tcpOutSegs
    |-- (12) tcpRetransSegs
    |-- (13) tcpConnTable
    |   |-- (1) tcpConnEntry
    |       |-- (1) tcpConnState
    |       |-- (2) tcpConnLocalAddress
    |       |-- (3) tcpConnLocalPort
    |       |-- (4) tcpConnRemAddress
    |       |-- (5) tcpConnRemPort
    |-- (14) tcpInErrs
    |-- (15) tcpOutRsts
```

User Datagram Protocol Group (1.3.6.1.2.1.7)

The user datagram protocol group is required for all systems that have implemented UDP.

```
(7) udp
    |-- (1) udpInDatagrams
    |-- (2) udpNoPorts
    |-- (3) udpInErrors
    |-- (4) udpOutDatagrams
    |-- (5) udpTable
    |   |-- (1) udpEntry
    |       |-- (1) udpLocalAddress
    |       |-- (2) udpLocalPort
```

Simple Network Management Protocol Group (1.3.6.1.2.1.11)

The simple network management protocol group is required for all systems. In SNMP installations that have been optimized to support either just one agent or one management station, some of the listed objects will contain the value "0."

```
(11) snmp
    |-- (1) snmpInPkts
    |-- (2) snmpOutPkts
    |-- (3) snmpInBadVersions
    |-- (4) snmpInBadCommunityNames
    |-- (5) snmpInBadCommunityUses
    |-- (6) snmpInASNParseErrs
    |-- (7) not used
    |-- (8) snmpInTooBigs
    |-- (9) snmpInNoSuchNames
    |-- (10) snmpInBadValues
    |-- (11) snmpInReadOnlys
    |-- (12) snmpInGenErrs
    |-- (13) snmpInTotalReqVars
    |-- (14) snmpInTotalSetVars
    |-- (15) snmpInGetRequests
    |-- (16) snmpInGetNexts
    |-- (17) snmpInSetRequests
    |-- (18) snmpInGetResponses
    |-- (19) snmpInTraps
    |-- (20) snmpOutTooBigs
    |-- (21) snmpOutNoSuchNames
    |-- (22) snmpOutBadValues
    |-- (23) not used
    |-- (24) snmpOutGenErrs
    |-- (25) snmpOutGetRequests
    |-- (26) snmpOutGetNexts
    |-- (27) snmpOutSetRequests
    |-- (28) snmpOutGetResponses
    |-- (29) snmpOutTraps
    |-- (30) snmpEnableAuthenTraps
```

RMON Group (1.3.6.1.2.1.16)

This part of the MIB provides a continuous flow of current and historical network component data to the network management. The configuration of alarms and events controls the evaluation of network component counters. The agents inform the management station of the evaluation result by means of traps depending on the configuration.

```
(16 rmon
    |--(1) statistics
        |--(1) etherStatsTable
            |--(1) etherStatsEntry
                |--(1) etherStatsIndex
                |--(2) etherStatsDataSource
                |--(3) etherStatsDropEvents
                |--(4) etherStatsOctets
                |--(5) etherStatsPkts
                |--(6) etherStatsBroadcastPkts
                |--(7) etherStatsMulticastPkts
                |--(8) etherStatsCRCAlignErrors
                |--(9) etherStatsUndersizePkts
                |--(10) etherStatsOversizePkts
                |--(11) etherStatsFragments
                |--(12) etherStatsJabbers
                |--(13) etherStatsCollisions
                |--(14) etherStatsPkts64Octets
                |--(15) etherStatsPkts65to127Octets
                |--(16) etherStatsPkts128to255Octets
                |--(17) etherStatsPkts256to511Octets
                |--(18) etherStatsPkts512to1023Octets
                |--(19) etherStatsPkts1024to1518Octets
                |--(20) etherStatsOwner
                |--(21) etherStatsStatus
    |--(2) history
        |--(1) historyControlTable
            |--(1) historyControlEntry
                |--(1) historyControlIndex
                |--(2) historyControlDataSource
                |--(3) historyControlBucketsRequested
                |--(4) historyControlBucketsGranted
                |--(5) historyControlInterval
                |--(6) historyControlOwner
                |--(7) historyControlStatus
        |--(2) etherHistoryTable
            |--(1) etherHistoryEntry
                |--(1) etherHistoryIndex
                |--(2) etherHistorySampleIndex
                |--(3) etherHistoryIntervalStart
```

```
                    |--(4) etherHistoryDropEvents
                    |--(5) etherHistoryOctets
                    |--(6) etherHistoryPkts
                    |--(7) etherHistoryBroadcastPkts
                    |--(8) etherHistoryMulticastPkts
                    |--(9) etherHistoryCRCAlignErrors
                    |--(10) etherHistoryUndersizePkts
                    |--(11) etherHistoryOversizePkts
                    |--(12) etherHistoryFragments
                    |--(13) etherHistoryJabbers
                    |--(14) etherHistoryCollisions
                    |--(15) etherHistoryUtilization
        |--(3) alarm
            |--(1) alarmTable
                |--(1) alarmEntry
                    |--(1) alarmIndex
                    |--(2) alarmInterval
                    |--(3) alarmVariable
                    |--(4) alarmSampleType
                    |--(5) alarmValue
                    |--(6) alarmStartupAlarm
                    |--(7) alarmRisingThreshold
                    |--(8) alarmFallingThreshold
                    |--(9) alarmRisingEventIndex
                    |--(10) alarmFallingEventIndex
                    |--(11) alarmOwner
                    |--(12) alarmStatus
        |--(9) event
            |--(1) eventTable
                |--(1) eventEntry
                    |--(1) eventIndex
                    |--(2) eventDescription
                    |--(3) eventType
                    |--(4) eventCommunity
                    |--(5) eventLastTimeSent
                    |--(6) eventOwner
                    |--(7) eventStatus
            |--(2) logTable
                |--(1) logEntry(1)
                    |--(1) logEventIndex
                    |--(2) logIndex
                    |--(3) logTime
                    |--(4) logDescription
```

dot1dBridge (1.3.6.1.2.1.17)

This part of the MIB contains bridge-specific objects.

```
(17) dot1dBridge
    |--(1) dot1dBase
        |--(1) dot1dBaseBridgeAddress
        |--(2) dot1dBaseNumPorts
        |--(3) dot1dBaseType
        |--(4) dot1dBasePortTable
            |--(1) dot1dBasePortEntry
                |--(1) dot1dBasePort
                |--(2) dot1dBasePortIfIndex
                |--(3) dot1dBasePortCircuit
                |--(4) dot1dBasePortDelayExceededDiscards
                |--(5) dot1dBasePortMtuExceededDiscards
    |--(2) dot1dStp
    |--(3) dot1dSr
    |--(4) dot1dTp
        |--(1) dot1dTpLearnedEntryDiscards
        |--(2) dot1dTpAgingTime
        |--(3) dot1dTpFdbTable
            |--(1) dot1dTpFdbEntry
                |--(1) dot1dTpFdbAddress
                |--(2) dot1dTpFdbPort
                |--(3) dot1dTpFdbStatus
        |--(4) dot1dTpPortTable
            |--(1) dot1dTpPortEntry
                |--(1) dot1dTpPort
                |--(2) dot1dTpPortMaxInfo
                |--(3) dot1dTpPortInFrames
                |--(4) dot1dTpPortOutFrames
                |--(5) dot1dTpPortInDiscards
    |--(5) dot1dStatic
        |--(1) dot1dStaticTable
            |--(1) dot1dStaticEntry
                |--(1) dot1dStaticAddress
                |--(2) dot1dStaticReceivePort
                |--(3) dot1dStaticAllowedToGoTo
                |--(4)  dot1dStaticStatus
    |--(6) pBridgeMIB
        |--(1) pBridgeMIBObjects
            |--(1) dot1dExtBase
                |--(1) dot1dDeviceCapabilities
                |--(2) dot1dTrafficClassesEnabled
                |--(3) dot1dGmrpStatus
                |--(4) dot1dPortCapabilitiesTable
                    |--(1) dot1dPortCapabilitiesEntry
```

```
                        |--(1) dot1dPortCapabilities
            |--(3) dot1dGarp
                |--(1) dot1dPortGarpTable
                    |--(1) dot1dPortGarpEntry
                        |--(1) dot1dPortGarpJoinTime
                        |--(2) dot1dPortGarpLeaveTime
                        |--(3) dot1dPortGarpLeaveAllTime
            |--(4) dot1dGmrp
                |--(1) dot1dPortGmrpTable
                    |--(1) dot1dPortGmrpEntry
                        |--(1) dot1dPortGmrpStatus
                      |--(2) dot1dPortGmrpFailedRegistrations
                        |--(3) dot1dPortGmrpLastPduOrigin
    |--(7) qBridgeMIB
        |--(1) qBridgeMIBObjects
            |--(2) dot1qTp
                |--(3) dot1qTpGroupTable
                    |--(1) dot1qTpGroupEntry
                        |--(1) dot1qTpGroupAddress
                        |--(2) dot1qTpGroupEgressPorts
                        |--(3) dot1qTpGroupLearnt
                |--(4) dot1qForwardAllTable
                    |--(1) dot1qForwardAllEntry
                        |--(1) dot1qForwardAllPorts
                        |--(2) dot1qForwardAllStaticPorts
                        |--(3) dot1qForwardAllForbiddenPorts
                |--(5) dot1qForwardUnregisteredTable
                    |--(1) dot1qForwardUnregisteredEntry
                        |--(1) dot1qForwardUnregisteredPorts
                    |--(2)dot1qForwardUnregisteredStaticPorts
                        |--(3)
dot1qForwardUnregisteredForbiddenPorts
```

MAU Management Group (1.3.6.1.2.1.26)

The MAU management group is responsible for setting the autonegotiation parameters.

```
(26) snmpDot3MauMgt
    |-- (2) dot3IfMauBasicGroup
    |    |-- (1) ifMauTable
    |        |-- (1) ifMauEntry
    |             |-- (1) ifMauIfIndex
    |             |-- (2) ifMauIndex
    |             |-- (3) ifMauType
    |             |-- (4) ifMauStatus
    |             |-- (5) ifMauMediaAvailable
    |             |-- (6) ifMauMediaAvailableStateExits
    |             |-- (7) ifMauJabberState
    |             |-- (8) ifMauJabberingStateEnters
    |             |-- (9) ifMauFalseCarriers
    |             |-- (10)ifMauTypeList
    |             |-- (11)ifMauDefaultType
    |             |-- (12)ifMauAutoNegSupported
    |-- (5) dot3IfMauAutoNegGroup
    |    |-- (1) ifMauAutoNegTable
    |        |-- (1) ifMauAutoNegEntry
    |             |-- (1) ifMauAutoNegAdminStatus
    |             |-- (2) ifMauAutoNegRemoteSignaling
    |             |-- (4) ifMauAutoNegConfig
    |             |-- (5) ifMauAutoNegCapability
    |             |-- (6) ifMauAutoNegCapAdvertised
    |             |-- (7) ifMauAutoNegCapReceived
    |             |-- (8) ifMauAutoNegRestart
```

Private MIB

Overview

The private MIB is for configuring the device-specific properties of the NxS. The groups below are implemented in the NxS from the private MIB saConfiguration (OID = 1.3.6.1.4.1.3833.1.1.14).

- saChassis (OID = 1.3.6.1.4.1.3833.1.1.14.1)
- saAgent (OID = 1.3.6.1.4.1.3833.1.1.14.2)
- saUserGroup (OID = 1.3.6.1.4.1.3833.1.1.14.3
- saRingRedundancy (OID = 1.3.6.1.4.1.3833.1.1.14.5

Device Group

The device group contains information on the status of the NxS hardware.

```
(14) saConfiguration
    |-- (1) saChassis
    |   |-- (1) saSystemTable
    |       |-- (1) saSysProduct
    |       |-- (2) saSysVersion
    |       |-- (3) saSysGroupCapacity
    |       |-- (4) saSysGroupMap
    |       |-- (5) saSysMaxPowerSupply
    |       |-- (6) saSysMaxFan
    |       |-- (7) saSysGroupModuleCapacity
    |       |-- (8) saSysModulePortCapacity
            |-- (9) saSysGroupTable
                |-- (1) saSysGroupEntry
                    |-- (1) saSysGroupID
                    |-- (2) saSysGroupType
                    |-- (3) saSysGroupDescription
                    |-- (4) saSysGroupHwVersion
                    |-- (5) saSysGroupSwVersion
                    |-- (6) saSysGroupModuleMap
                    |-- (7) saSysGroupAction
                    |-- (8) saSysGroupActionResult
            |-- (11) saInterfaceTable
                |-- (1) saIfEntry
                    |-- (1) saIfaceGroupID
                    |-- (2) saIfaceID
                    |-- (3) saIfaceStpEnable
                    |-- (4) saIfaceLinkType
                    |-- (5) saIfaceAction
                    |-- (6) saIfaceNextHopMacAddress
                    |-- (7) saIfaceFlowControl
                    |-- (8) saIfacePriorityThreshold
                    |-- (9) saIfaceName
                    |-- (10) saIfaceTrunkID
                    |-- (11) saIfacePrioTOSEnable
                    |-- (12) saIfBcastLimit
                    |-- (13) saIfaceUtilization
                   |-- (14) saIfaceUtilizationControlInterval
            |-- (20) saSysChassisName
            |-- (21) saSysStpEnable
            |-- (22) saSysFlowControl
            |-- (23) saSysBOOTPEnable
            |-- (24) saSysDHCPEnable
            |-- (25) saSysTelnetEnable
            |-- (26) saSysHTTPEnable
```

```
|   |-- (2) saPSTable
|       |-- (1) saPSEntry
|           |-- (1) saPSSysID
|           |-- (2) saPSID
|           |-- (3) saPSState
    |-- (5) saCurrentAddressTable
        |-- (1) saCurrentAddressEntry
            |-- (1) saCurrentAddress
            |-- (2) saCurrentAddressReceivePort
            |-- (3) saCurrentAddressStaticEgressPorts
            |-- (4) saCurrentAddressEgressPorts
            |-- (5) saCurrentAddressStatus
|   |-- (10) saNxSext
|       |-- (1) saNxSOperMode
|       |-- (2) saNxSConfigError
|       |-- (3) saNxSSigRelayState
|       |-- (4) saSigLinkTable
|           |-- (1) saSigLinkEntry
|               |-- (1) saSigLinkID
|               |-- (2) saSigLinkAlarm
        |-- (5) saSigTrapReason
        |-- (6) saSigReasonIndex
        |-- (7) saNxSTopologyGroup
            |-- (1) saNxSPartnerIpAddress
            |-- (2) saNxSTopologyTable
                |-- (1) saNxSTopologyEntry
                    |-- (1) saNxSTopologyLinkID
                    |-- (2) saNxSTopologyIpAddress
        |-- (8) saNxSConnectionMirroringGroup
            |-- (1) saNxSConnectionMirroringStatus
            |-- (2) saNxSConnectionMirroringPortOne
            |-- (3) saNxSConnectionMirroringPortTwo
        |-- (9) saNxSDisableLearningGroup
            |-- (1) saNxSDisableLearningStatus
        |-- (10) saNxSSigRelayGroup
            |-- (1) saNxSSigRelayMode
            |-- (2) saNxSSigRelayManualState
        |-- (11) saNxSSelftestGroup
            |-- (1) saNxSSelftestResult
            |-- (2) saNxSSelftestMode
```

Management Group

The management group contains parameters for configuring the management agent.

```
(14)saConfiguration
    |-- (2) saAgent
    |   |-- (1) saAction
    |   |-- (2) saActionResult
    |   |-- (3) saNetwork
    |       |-- (1) saNetLocalIPAddr
    |       |-- (2) saNetLocalPhysAddr
    |       |-- (3) saNetGatewayIPAddr
    |       |-- (4) saNetMask
            |-- (7) saNetAction
    |   |-- (4) saFSTable
    |       |-- (1) saFSUpdFileName
    |       |-- (2) saFSConfFileName
    |       |-- (3) saFSLogFileName
    |       |-- (4) saFSUserName
    |       |-- (5) saFSTPPassword
    |       |-- (6) saFSAction
    |       |-- (8) saFSActionResult
            |-- (9) saFSBootConfiguration
            |-- (10) saFSRunningConfiguration
            |-- (200) saAutoconfigGroup
    |           |-- (1) saAutoconfigAdapterStatus
    |   |-- (7) saAuthGroup
    |       |-- (1) saAuthHostTableEntriesMax
    |       |-- (2) saAuthCommTableEntriesMax
    |       |-- (3) saAuthCommTable
    |           |-- (1) saAuthCommEntry
    |               |-- (1) saAuthCommIndex
    |               |-- (2) saAuthCommName
    |               |-- (3) saAuthCommPerm
    |               |-- (4) saAuthCommState
    |       |-- (4) saAuthHostTable
    |           |-- (1) saAuthHostEntry
    |               |-- (1) saAuthHostIndex
    |               |-- (2) saAuthHostName
    |               |-- (3) saAuthHostCommIndex
    |               |-- (4) saAuthHostIpAddress
    |               |-- (5) saAuthHostIpMask
    |               |-- (6) saAuthHostState
    |   |-- (8) saTrapGroup
    |       |-- (1) saTrapCommTableEntriesMax
    |       |-- (2) saTrapDestTableEntriesMax
    |       |-- (3) saTrapCommTable
|           |-- (1) saTrapCommEntry
|               |-- (1) saTrapCommIndex
|               |-- (2) saTrapCommCommIndex
|               |-- (3) saTrapCommColdStart
|               |-- (4) saTrapCommLinkDown
|               |-- (5) saTrapCommLinkUp
|               |-- (6) saTrapCommAuthentication
|               |-- (7) saTrapCommBridge
|               |-- (8) saTrapCommRMON
|               |-- (9) saTrapCommUsergroup
|               |-- (10)saTrapCommDualHoming
|               |-- (11)saTrapCommChassis
|               |-- (12)saTrapCommState
|       |-- (4) saTrapDestTable
|           |-- (1) saTrapDestEntry
|               |-- (1) saTrapDestIndex
|               |-- (2) saTrapDestName
|               |-- (3) saTrapDestCommIndex
|               |-- (4) saTrapDestIpAddress
|               |-- (5) saTrapDestIpMask
|               |-- (6) saTrapDestState
|   |-- (9) saLastAccessGroup
|       |-- (1) saLastIpAddr
|       |-- (2) saLastPort
|       |-- (3) saLastCommunity
```

User Groups Group

The user groups group contains parameters for configuring the user group functions.

```
(14) saConfiguration
    |-- (3) saUserGroup
        |-- (4) saPortSecurityTable
            |-- (1) saPortSecurityEntry
                |-- (1) saPortSecSlotID
                |-- (2) saPortSecPortID
                |-- (3) saPortSecPermission
                |-- (4) saPortSecAllowedUserID
                |-- (5) saPortSecAllowedGroupIDs
                |-- (6) saPortSecConnectedUserID
                |-- (7) saPortSecAction
                |-- (8) saPortSecAutoReconfigure
```

Redundancy Group

The redundancy group contains parameters for configuring the redundancy functions.

```
(14) saConfiguration
    |-- (5) saRingRedundancy
        |-- (1) saRingRedTable
            |-- (1) saRingRedEntry
                |-- (1) saRingRedPrimGroupID
                |-- (2) saRingRedPrimIfIndex
                |-- (3) saRingRedPrimIfOpState
                |-- (4) saRingRedRedGroupID
                |-- (5) saRingRedRedIfIndex
                |-- (6) saRingRedRedIfOpState
                |-- (7) saRingRedOperState
                |-- (8) saRingRedMode
    |-- (10) saProducts
        |-- (2) nxsx7100
```

User Interface

7

Working with the User Interface

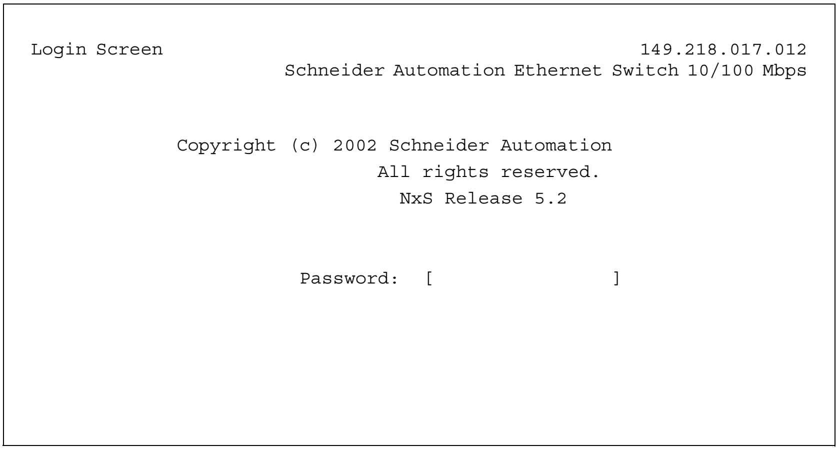
Overview

Follow these steps to open the user interface and enter the password.

Step	Action	Comment
1	After connecting the management agent with a VT100 terminal via V.24, press a key.	A window will appear on the screen for entering the password. Only one user can access the user interface.
2	Type the password.	The default value for the password is **private**. You can change the password via the WWW interface or later in the user interface (see *Password, p. 124*). Please note that passwords are case-sensitive.
3	Press **<ENTER>**.	The main menu screen appears.

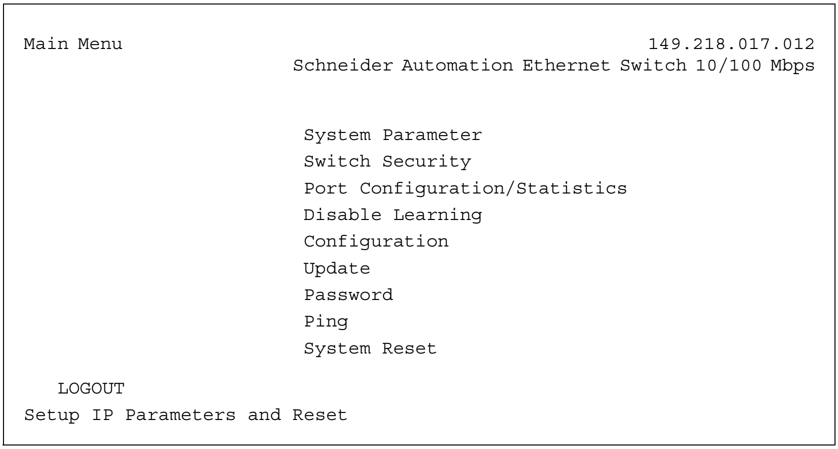
User Interface Login

The following figure shows the user interface login screen.



```
Login Screen                                               149.218.017.012
                       Schneider Automation Ethernet Switch 10/100 Mbps


             Copyright (c) 2002 Schneider Automation
                              All rights reserved.
                                NxS Release 5.2


                        Password:  [                ]
```

The following figure shows the main menu.



```
Main Menu                                                      149.218.017.012
                        Schneider Automation Ethernet Switch 10/100 Mbps


                         System Parameter
                         Switch Security
                         Port Configuration/Statistics
                         Disable Learning
                         Configuration
                         Update
                         Password
                         Ping
                         System Reset

   LOGOUT
Setup IP Parameters and Reset
```

User Interface Basics

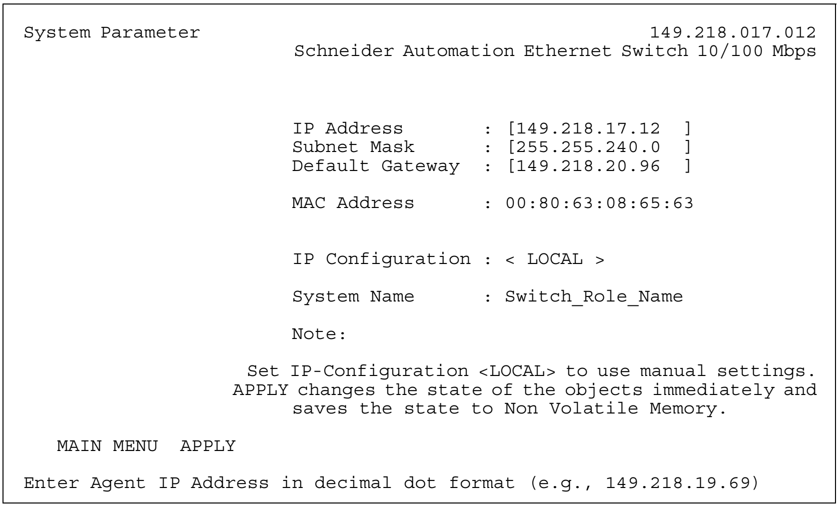
- Use the arrow keys or the tab key to move the cursor.
- To change the specified values in a selection field, press the **space bar**.
- The new settings are accepted if the cursor is in the **APPLY** field, and the enter key is pressed.
- The bottom line contains a help text for the selected item.
- To exit the user interface, select **LOGOUT** in the main menu and press the enter key.

System Parameter

This menu is for

- entering the IP address,
- entering the subnet mask,
- entering the gateway IP address,
- displaying the MAC address of the NxS, and
- enabling/disabling the BOOTP/DHCP.

The following figure shows the system parameter screen.



```
System Parameter                                                149.218.017.012
                            Schneider Automation Ethernet Switch 10/100 Mbps



                            IP Address       : [149.218.17.12  ]
                            Subnet Mask      : [255.255.240.0  ]
                            Default Gateway  : [149.218.20.96  ]

                            MAC Address      : 00:80:63:08:65:63


                            IP Configuration : < LOCAL >

                            System Name      : Switch_Role_Name

                            Note:

                       Set IP-Configuration <LOCAL> to use manual settings.
                     APPLY changes the state of the objects immediately and
                            saves the state to Non Volatile Memory.

   MAIN MENU  APPLY

Enter Agent IP Address in decimal dot format (e.g., 149.218.19.69)
```

The following table outlines the fields of the system parameter screen.

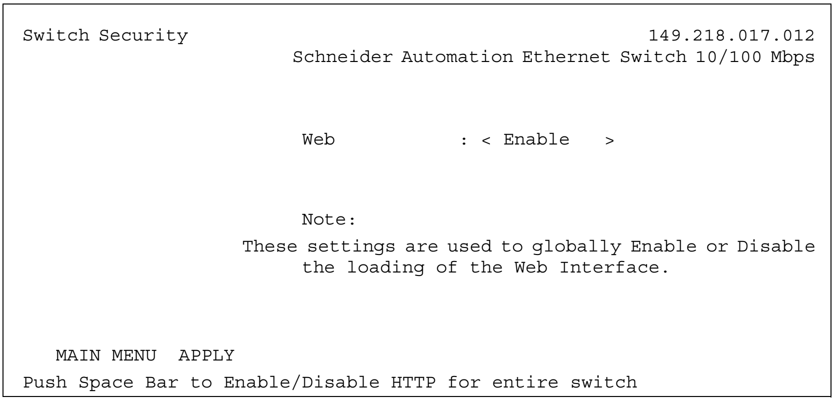
Field	Action
IP Address	Enter the IP address of the management agent here. The default setting of the address is 0.0.0.0.
Subnet Mask	In the event you are working in a large network and are using subnet masks, you can specify here the mask of the subnet to which your management agent is connected. The default setting of the IP address is 0.0.0.0.
Default Gateway	Enter the IP address of the gateway here. If there is no such gateway, you can omit this entry. The default setting of the IP address is 0.0.0.0.
MAC Address	This field displays the MAC address of the device.
IP Configuration	Select the desired IP configuration mode. When you press the **space bar**, the following options are available: ● Local ● BOOTP ● DHCP The mode is activated when you select **APPLY**.
System Name	Assign your NxS the name of your choice (see *DHCP, p. 29*.

Switch Security

This menu configures access to the web-based management.

- **Disable** does not allow any access to the web-based management.
- **Enable** allows access to the web-based management.

The following figure shows the switch security menu.



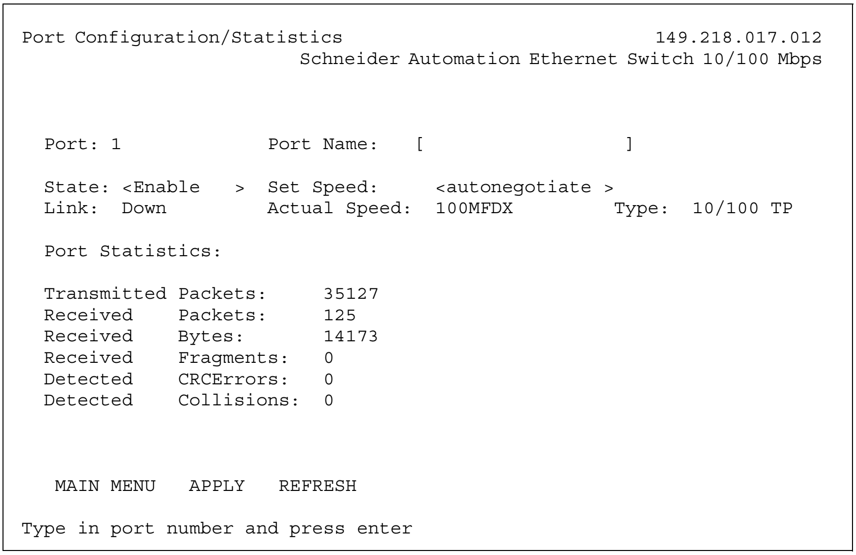
```
Switch Security                                            149.218.017.012
                            Schneider Automation Ethernet Switch 10/100 Mbps



                             Web           : < Enable   >



                             Note:
                       These settings are used to globally Enable or Disable
                             the loading of the Web Interface.



   MAIN MENU  APPLY
Push Space Bar to Enable/Disable HTTP for entire switch
```

Port Configuration/ Statistics

This window sets port configuration and displays port statistics. Follow the steps below to set the port configuration.

Step	Action	Comment
1	Enter the port number and press **Return**.	
2	Set the State.	State options: ● **Disable** turns off the port. ● **Enable** turns on the port.
3	Set the Speed.	Speed options: ● **Autonegotiate** activates the autonegotiation function. ● **10MHDX** 10 Mbps, half duplex ● **10MFDX** 10 Mbps, full duplex ● **100MHDX** 100Mbps, half duplex ● **100MFDX** 100 Mbps, full duplex

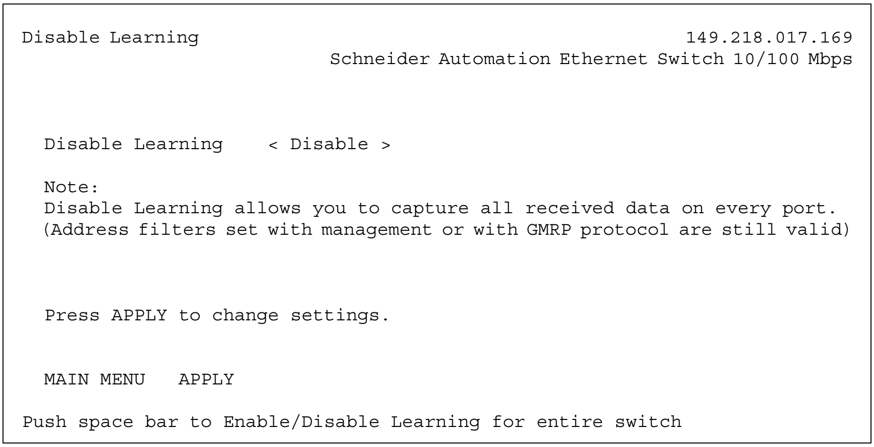
The following figure shows the port configuration menu.



```
Port Configuration/Statistics                                149.218.017.012
                         Schneider Automation Ethernet Switch 10/100 Mbps



  Port: 1             Port Name:   [                  ]

  State: <Enable    >  Set Speed:     <autonegotiate >
  Link:  Down         Actual Speed:  100MFDX        Type:  10/100 TP

  Port Statistics:

  Transmitted Packets:     35127
  Received    Packets:     125
  Received    Bytes:       14173
  Received    Fragments:   0
  Detected    CRCErrors:   0
  Detected    Collisions:  0



   MAIN MENU   APPLY   REFRESH

Type in port number and press enter
```

Disable Learning

This window allows you to monitor the data for all ports. Select **disable** to switch off the learning function of the NxS. Then, the NxS will transfer all data from each port to all other ports. The following figure shows the disable learning menu.



```
Disable Learning                                               149.218.017.169
                            Schneider Automation Ethernet Switch 10/100 Mbps



  Disable Learning    < Disable >

  Note:
  Disable Learning allows you to capture all received data on every port.
  (Address filters set with management or with GMRP protocol are still valid)



  Press APPLY to change settings.


  MAIN MENU   APPLY

Push space bar to Enable/Disable Learning for entire switch
```

Configuration

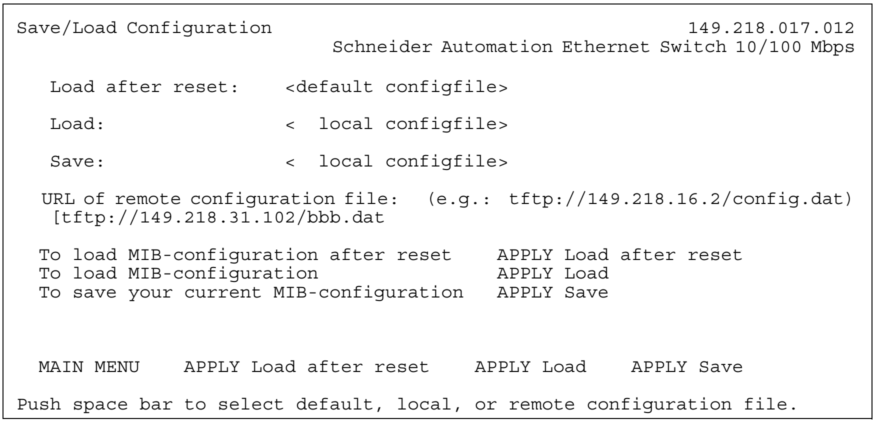
The NxS has two configuration settings:

- default setting
- user-defined setting

This submenu offers the option of storing a user-defined configuration. This configuration can be loaded automatically when restarting or after restarting with the default settings loaded.

Configuration Option	Result
Load after reset	Determines which configuration setting will be active after a restart. ● **Default** loads the default configuration. ● **Local** loads the user-defined configuration from flash memory. ● **Remote** loads the user-defined configuration from the configuration file on the tftp server.
Load	Determines which configuration setting will be loaded. ● **Local** loads the user-defined configuration from flash memory. ● **Remote** loads the user-defined configuration from the configuration file on the tftp server. ● **configadapter** loads the user-defined configuration from the AutoConfiguration Adapter.
Save	Determines where the configuration setting is saved. ● **Local** saves the user-defined configuration in flash memory. ● **Remote** saves the user-defined configuration as a configuration file on the tftp server. ● **configadapter** saves the user-defined configuration in the AutoConfiguration Adapter and in flash memory.

Click **APPLY** to accept the changes.
The path for storing the configuration data is displayed in the line **URL**. Create an empty file on the tftp server before you click **Save to URL** because tftp is not able to create a new file.
The following figure shows the save/load configuration screen.



```
Save/Load Configuration                                       149.218.017.012
                             Schneider Automation Ethernet Switch 10/100 Mbps

   Load after reset:    <default configfile>

   Load:                <  local configfile>

   Save:                <  local configfile>

  URL of remote configuration file:  (e.g.: tftp://149.218.16.2/config.dat)
   [tftp://149.218.31.102/bbb.dat

  To load MIB-configuration after reset    APPLY Load after reset
  To load MIB-configuration                APPLY Load
  To save your current MIB-configuration   APPLY Save



  MAIN MENU    APPLY Load after reset    APPLY Load    APPLY Save

Push space bar to select default, local, or remote configuration file.
```

Note: You must reboot the NxS twice when you change its IP address via the web interface.

Save to a tftp Server

Use the following steps to save to a tftp server.

Step	Action
1	Open a new file with any editor.
2	Save the empty file to the appropriate path of the tftp server including the file name, e.g. **RAM0/Switch_Role_Name.prm**.
3	In the **URL** line, enter the path of the tftp server, e.g. **tftp://149.218.076.214/RAM0/Switch_Role_Name.prm**.

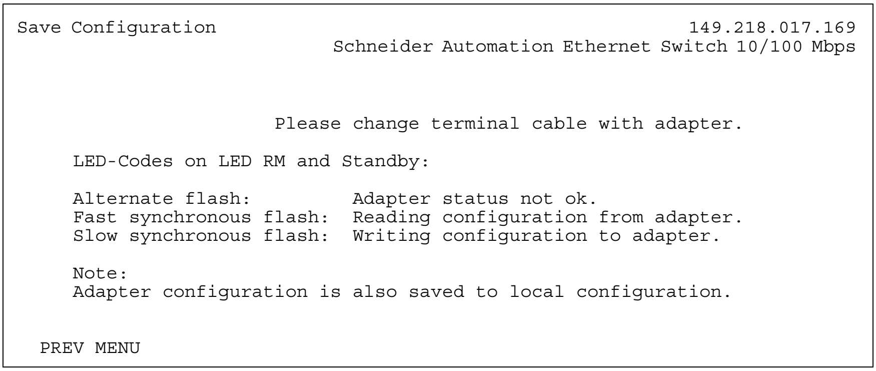
Note: The configuration file includes all configuration data, including the password, so be sure to set the access rights on the tftp server appropriately.

Auto-Configuration Adapter (ACA) Memory Operation

To select AutoConfiguration Adapter (ACA) for a memory operation, click **APPLY**, and a new window opens with the following request: (**Pull the terminal block off the NxS, and connect the ACA to the V.24 connection of the NxS**.) Then, the NxS performs the memory operation. The following table shows the status of the memory operation.

Display	Meaning
LEDs flash alternately	error in the memory operation
LEDs flash synchronously, two times a second	loading the configuration from the ACA
LEDs flash synchronously, once a second	saving the configuration in the ACA

The transition of the LEDs from a flashing to a static state indicates the end of the memory operation. To go back to the user interface, pull the ACA from the NxS and connect the terminal block to the V.24 connection of the NxS. The following figure shows the ACA memory operation menu.



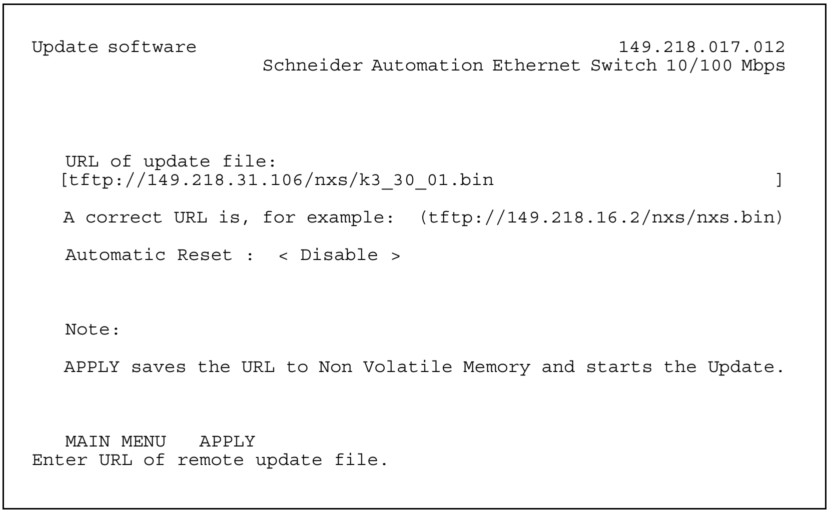
```
Save Configuration                                                          149.218.017.169
                                          Schneider Automation Ethernet Switch 10/100 Mbps



                        Please change terminal cable with adapter.

     LED-Codes on LED RM and Standby:

     Alternate flash:         Adapter status not ok.
     Fast synchronous flash:  Reading configuration from adapter.
     Slow synchronous flash:  Writing configuration to adapter.

     Note:
     Adapter configuration is also saved to local configuration.


  PREV MENU
```

Update

Before you can update the software, you need to know the correct location (pathname) of the update file.

Step	Action
1	Enter the correct pathname in the field **URL of update file** and press **Enter**.
2	In the line **Reset**, decide whether the NxS should be restarted immediately after loading an update or at a later time.
3	Choose **Apply** to load the update. It is active after a restart.

The following figure shows the update software menu.



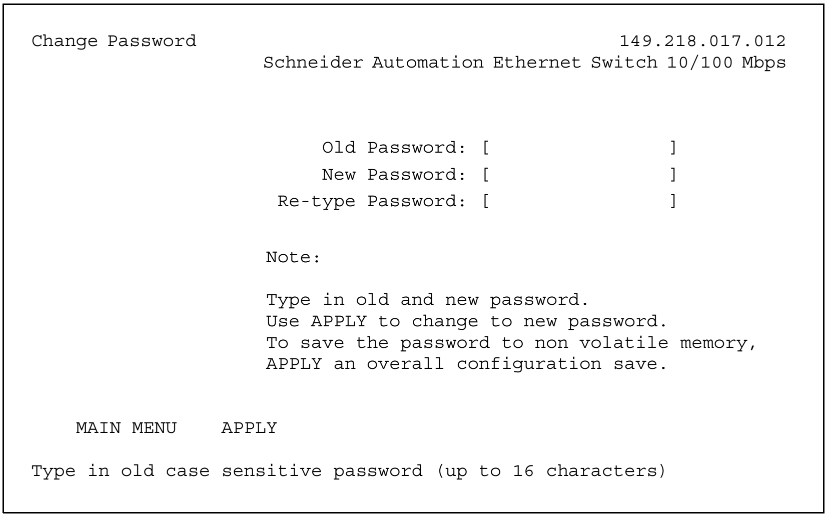
```
Update software                                      149.218.017.012
                    Schneider Automation Ethernet Switch 10/100 Mbps



   URL of update file:
  [tftp://149.218.31.106/nxs/k3_30_01.bin                          ]

   A correct URL is, for example:  (tftp://149.218.16.2/nxs/nxs.bin)

   Automatic Reset :  < Disable >


   Note:

   APPLY saves the URL to Non Volatile Memory and starts the Update.


   MAIN MENU   APPLY
Enter URL of remote update file.
```

Password

Change the password in this submenu to protect the NxS from unauthorized access.

Step	Action
1	Enter your old password in the **Old Password** field and press **Enter**.
2	Enter your new password in the **New Password** field and press **Enter**.
3	Repeat your new password in the **Retype password** field and press **Enter**.
4	Choose **APPLY** to accept the new password and press **Enter**.
5	Save the configuration to ensure that the new password is available after a restart (see *Configuration, p. 120*).

The following figure shows the change password menu.



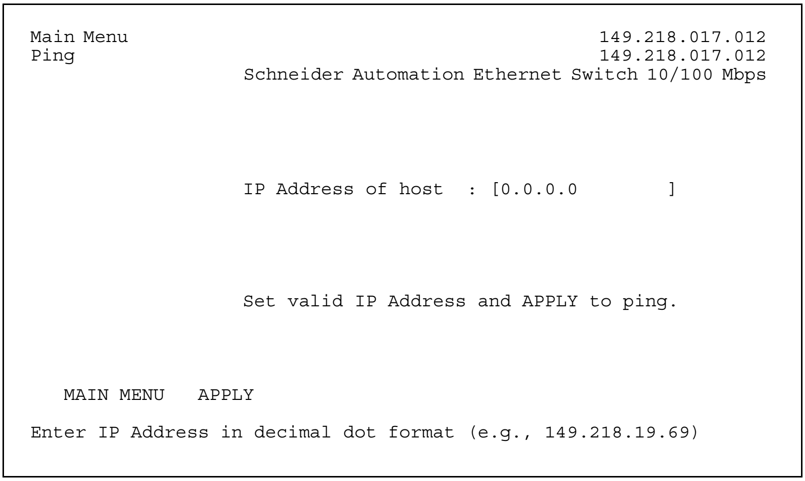
```
Change Password                                          149.218.017.012
                    Schneider Automation Ethernet Switch 10/100 Mbps



                         Old Password: [                ]
                         New Password: [                ]
                     Re-type Password: [                ]

                     Note:

                     Type in old and new password.
                     Use APPLY to change to new password.
                     To save the password to non volatile memory,
                     APPLY an overall configuration save.


    MAIN MENU    APPLY

Type in old case sensitive password (up to 16 characters)
```

Ping

In the ping menu you can test the accessibility of another network station.

Step	Action	Comment
1	Type the IP address of the desired station in the **IP address of the host** field, and press **Enter**.	
2	Choose **Apply** to ping the desired station.	Depending on the accessibility of the station, you will receive one of two responses. ● **Host alive** ● **Host not alive**

The following figure shows the ping menu.



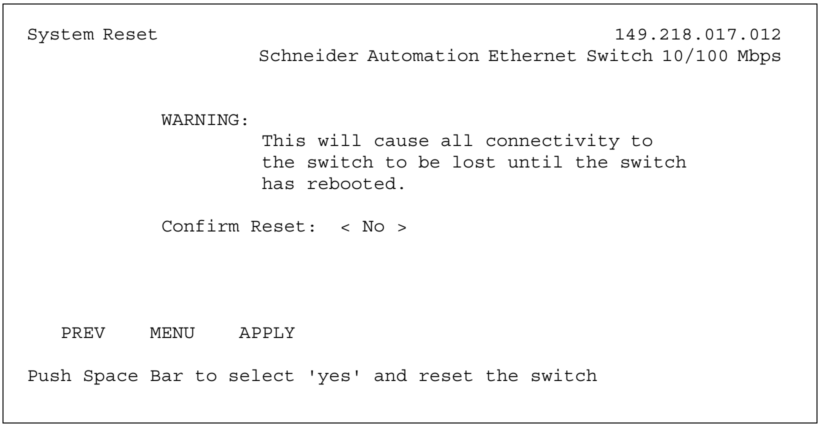
```
Main Menu                                                     149.218.017.012
Ping                                                          149.218.017.012
                   Schneider Automation Ethernet Switch 10/100 Mbps



                   IP Address of host   : [0.0.0.0        ]



                   Set valid IP Address and APPLY to ping.



   MAIN MENU   APPLY

Enter IP Address in decimal dot format (e.g., 149.218.19.69)
```

System Reset

Use the following steps to reset the NxS.

Step	Action
1	Select the **Confirm Reset** line.
2	Press the **space bar** to change the setting from **No** to **Yes**.
3	Choose **APPLY** to reset the NxS.

The following figure shows the system reset menu.



```
System Reset                                               149.218.017.012
                    Schneider Automation Ethernet Switch 10/100 Mbps


            WARNING:
                     This will cause all connectivity to
                     the switch to be lost until the switch
                     has rebooted.

            Confirm Reset:  < No >




   PREV    MENU    APPLY

Push Space Bar to select 'yes' and reset the switch
```

Index