SubMenu

BATM Advanced Communications

ESB20 10/100 Mbit Ethernet Switch

User Guide

SubMenu

Preface

This guide provides the required information to setup and configure the ESB20 switch, *firmware version 1.28*. It is intended for network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of the following:

- Local area networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- Internet Protocol (IP) concepts

If the information in the Release Notes that are shipped with your unit differs from the information in this guide, follow the Release Notes.

Manual Organization

Chapter 1 –. **Introduction.** Describes the unit, its features, and specifications

Chapter 2 – **Getting Started.** Describes how to unpack and install the unit, perform the initial setup procedure, navigate the management applications, and unit operation commands.

Chapter 3 – **Configuration Procedures.** Describes all the unit and the port configuration procedures, except for the VLAN related procedures. The latter are described in Chapter 4.

Chapter 4 – **VLAN Configuration.** Describes the VLAN related configuration procedures.

Chapter 5 – **Statistics and Status Reports.** Describes the statistics and status reports.

Chapter 6 – **TFTP Procedures.** Describes how to perform remote software upgrades, uploads, and download using TFTP.

Chapter 7 – **Troubleshooting.** Describes common problems and provides solutions.

SubMenu

Table of Contents

Document History

ISSUE	DATE ISSUED	COMMENTS
0-1	May 1, 2002	Initial issue. Firmware version 1.28
0-2	July 17, 2002	Updated according to review.
1-0	August 18, 2002	Final editing to version 1.28

SubMenu

Chapter 1 Introduction

General

Nokia ESB20 switch is a 20 port 10/100BaseT/Tx switch board which is integrated into the DX200 M98 system. Interface to two ports is provided on the front panel via standard RJ-45 connectors, and to eighteen additional ports via the backplane.

Two management applications are integrated into the switch: Terminal Interface management for initial setup and troubleshooting, and Web Management application for remote management and monitoring.

Main Features

- Store and Forward operation.
- Half and full duplex on all ports.
- IEEE802.3X Full Duplex flow control on all ports
- Back pressure in Half Duplex mode on all ports
- Priority queuing based on Port or 802.1p.
- Complies with IEEE802.1d Spanning Tree protocol.
- None blocking operation.
- VLAN per 802.1q
- Address table contains 4000 entries.
- Port Trunking
- Hot-swap

Specifications

Compliance	IEEE802.3 IEEE802.1D IEEE802.3X IEEE802.1q IEEE802.1.	
Switching characteristics	Bridging	Per IEEE 802.1d spanning tree.
	Address table:	4,000 MAC address per switch.
	Forwarding Rate:	More than 2Mpps max.
	Internal Bandwidth (max.):	5.3 Gbit per second (F.D.).
	Buffers Memory:	737,280 bytes total 24,576 bytes per 10/100Mbps port
	Priority Queuing:	2 Queues per port, provides CoS per 802.1p
	Virtual LAN:	Port Based VLAN per 802.1q. Up to 32 VLAN groups can be defined. 4096 VLAN ID's are supported.
	Port Trunking:	Up to three trunks can be defined: two trunks consisting of up to 8 rear panel ports, and an additional trunk consisting of either the two front-panel ports or the remaining two rear panel ports.
Management	In-Band:	SNMP, TELNET, Java Based WEB application
	Supported MIBs:	MIB-II, BRIDGE MIB (RFC-1493) , PRIVATE MIB, RMON MIB (Group I,2,3,9)
	Local:	For initial configuration, EIA-232 protocol, RJ-45 console connector on the front panel, VT100 compatible
	Software download:	Via TFTP (Server application)
	Monitoring	Port mirroring for sniffer connection
Indicators:	General:	A single two-color LED (Green/Red) Green – Unit is operational Red – Unit is not operational or faulty. During reset the LED should lit in RED till unit is finalizing the restart procedure. Blinking – while firmware is being updated. Off – powered off (during Hotswap process).
Physical Characteristics	Dimension:	233.4*220 mm with PCB thickness of 1.6mm and spacing of 20.34mm (4T)
Environmental Characteristics	Operating Temp:	According to Nokia Environmental Specification (Commercial range 0-70C)
	Humidity:	According to Nokia Environmental Specification
Power Characteristics	Voltage:	3.3V and 5V
	Power Consumption:	<30w
Hot-swap:	The card can be inserted and removed when power is applied to the DX200 chassis. Before removing the card it is necessary to push the Reset button twice within two seconds. Doing so, will remove the power (the LED will go off) from the card for 20 seconds. During those 20 seconds the card can be removed safely.	

Chapter 2 Getting Started

Overview

ESB20 installation consists of inserting the card into the appropriate slot in the system, powering on the unit, and setting the IP Address in order to enable remote management. All other management procedures may be performed remotely via the Web or Terminal Interface management applications that are integrated into the unit.

This chapter describes how to install the unit, perform initial setup, navigate the Web and the Terminal Interface management applications, and how to perform basic switch operations.

Unpacking

After unpacking:

- Verify that the ESB20 unit is not damaged during shipment.
- It is recommended that you keep the shipping package until the unit has been installed and verified as being fully operational. As all electronic devices with static sensitive components, ESB20 should be handled with care.

ESB20 Front Panel

ESB20 front panel is illustrated below.

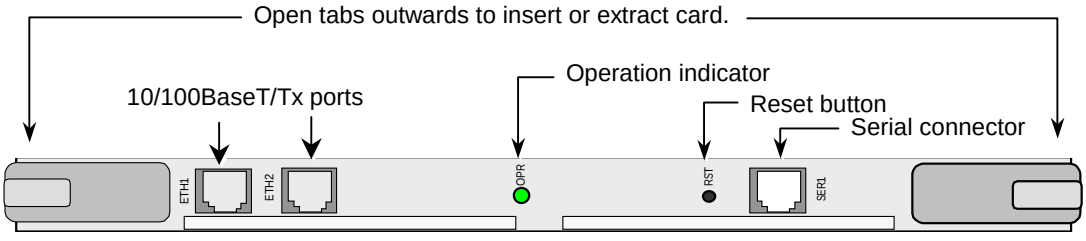


Figure 2-1. ESB20 Front Panel

1.

ETH1, ETH2	Two 10/100BaseT/Tx ports interface connectors
OPR	Operation Indicator. A single two-color LED (Green/Red) Green – Unit is operational Red – Unit is not operational or faulty. During reset the LED turns RED until the restart procedure has been completed. Blinking – while the firmware is updated, the LED blinks. Off – powered off (during the Hotswap process).

RST	Local Reset and Hotswap button. To perform Hotswap, press twice within two seconds before removing the card. Power will be turned off for 20 seconds during which the card may be removed safely.
SER1	RJ45 console connector used for initial configuration.

Initial Setup

In order to manage the card remotely, it is first required to *locally* connect to the card via a VT100 compatible console and set the card IP Address definitions. By default, ESB20 is setup with the static IP-address **192.168.0.5.**

During the initial setup procedure, you may configure the unit with a user defined IP Address and change the IP Address acquisition source (changes are implemented after the unit has been reset). All other configuration, management and monitoring operations may be performed remotely after logging in using the IP Address assigned to the unit.

Card Installation and Initial Login

1. Insert ESB20 into its chassis slot.
2. Connect the supplied **console** cable between the **card RJ-45** (**Console**) connector and the PC.
3. Open the terminal-emulation application on the PC and verify that it is set up as follows:
   - Emulation mode: VT-100 mode (default mode).
   - Communication parameters: 9600, 8 bits, No parity, 1 stop bit
4. Reset ESB20 by using front panel reset switch. Self-test will be performed and the corresponding messages indicating the various stages in the test will be displayed on the screen.
5. Enter the default **User Name** followed by the **Password**.
6. Set the IP Address definitions according to the following section, referring to the basic editing instructions given below:

Basic Editing Instructions for the Terminal Interface Menus

- Access the next menu by *typing* the item number.
- Re-access previous menus by pressing **Esc.**
- Access the **Main** menu by typing the number **9** from any menu.
- Edit an option by typing the number of the option, entering the new value at the prompt, and pressing **Enter.** The change is *automatically saved* and displayed either immediately or after a short waiting period on the screen.

IP Address Definitions

User Assigned IP Address

In the **Main** menu, type **1** (option **1. General Configuration**.) The General Configuration menu appears.

```
General Configuration

    MAC address                    00 A0 12 07 14 58
1.  Agent IP Address              : 010.002.005.250
2.  Agent Netmask                 : 255.255.000.000
3.  Default Gateway               : 010.002.001.001
4.  Supervisor/Terminal Password  :
5.  System Name                   :
6.  Advanced Features
9.  Main Menu
```

Figure 2-2. General Configuration Menu

The assigned IP Address definitions (in addition to other options) are displayed.

Define the following parameters as necessary and upon concluding the definitions, press **Esc** to return to the Terminal Interface Main menu:

- **Agent IP Address.** A unique address in the network that is assigned to the unit. The address is in standard dot notation; for example: 192.115.16.131.
- **Agent Netmask.** Thirty-two bit number that determines the network size and the IP of the unit subnet.
- **Default Gateway.** The gateway to which packets with unknown addresses are sent, to be forwarded to their destination on other subnets.

Setting-up and Navigating the Management Applications

Two management applications are integrated into the ESB20:

- **WEB Management**. Remotely accessible via Internet Explorer or WEB Browser applications. This management application is used to configure, monitor, and manage the switch after the initial setup procedure, executed via Terminal Interface, has been completed.
- **Terminal Interface Management.** Accessible either locally via direct connection, or remotely via Telnet. This application is used to perform the initial setup (as described in the previous section). It also provides basic monitoring and configuration options.

In order to use either management applications, some configuration of the management station is required. The management applications and the corresponding configuration procedures are described in the following sections.

Web Management Application

Network Management Station *Minimum* Requirements

- Pentium 90 MHz PC Minimum
- 32 Mbytes of memory
- Windows 95
- Internet Browser or Internet Explorer 4.X installed.
- Microsoft Java Virtual Machine™. This application may have been automatically installed after installing Microsoft Internet Explorer (depending on the chosen options).

  If necessary, Microsoft Java Virtual Machine™ may be downloaded from the URL: http://www.microsoft.com/java/ (go to: get components. Castle Rock SNMPc™ for Windows).

NOTE: *Linux, Unix etc. operating systems can be used as well; however, it is required that the Web Browser used support Java (version x.x or later).*

Working with a DNS Server

If you have a DNS Server, you can register the unit's IP Address and logical name on the DNS Server.

Setting Up the Web Browser to Connect to the Web Application

In order to access the switch management Web application, the Web browser on the management station must first be setup to allow communication with the unit.

Note: *The setup description is applicable to the Internet Explorer versions* ***5.x****. The procedure slightly differs for 4.x. Browsers than Internet Explorer can be use as well, however it is required that they support Java. Internet explorer is used through this document for example.*

To setup the Internet Explorer:

1. From the **Tools** (**View** in Version 4.x)] menu, depending on the Internet Explorer version, choose **Internet Options.** The Internet Options menu appears.
2. Select the **Security** tab. The following dialog appears.

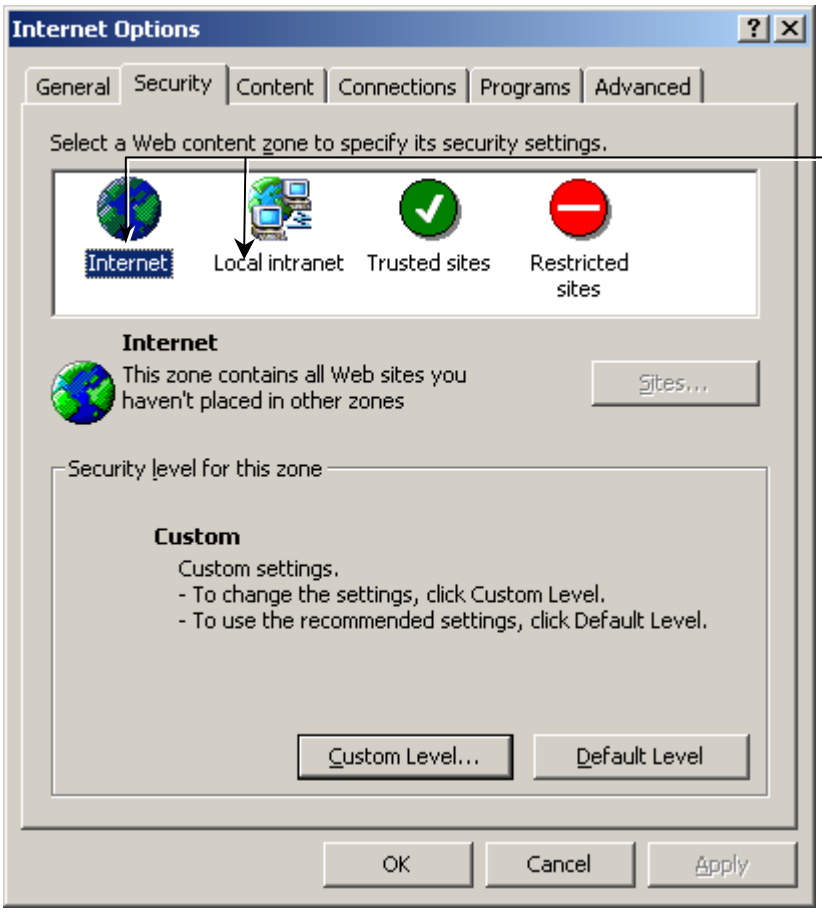


Figure 2-3. Security Options

3. Select the **Internet/Local Intranet** icon. (Perform the configuration procedure first for the **Internet** zone and then for the **Local Intranet).**
4. Click the **Custom Level** button. The **Security Settings** dialog appears.

5. Click the **Security Settings** button. The Security Settings dialog appears.

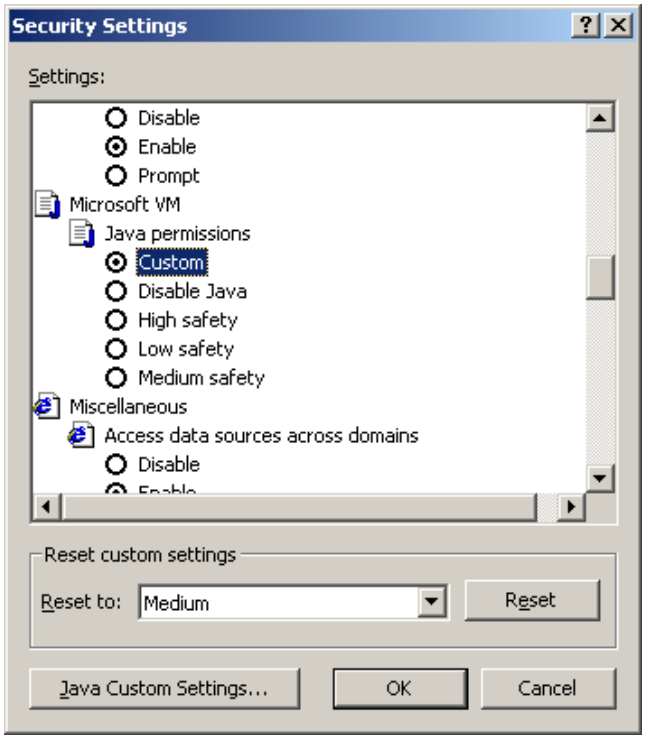


Figure 2-4. Java Custom Settings

6. Under **Java Permissions** select **Custom.** The Java Customs button becomes available.
7. Click the **Java Customs** Button. The Internet dialog appears.

8. Click the **Edit Permissions** tab. The following dialog appears.

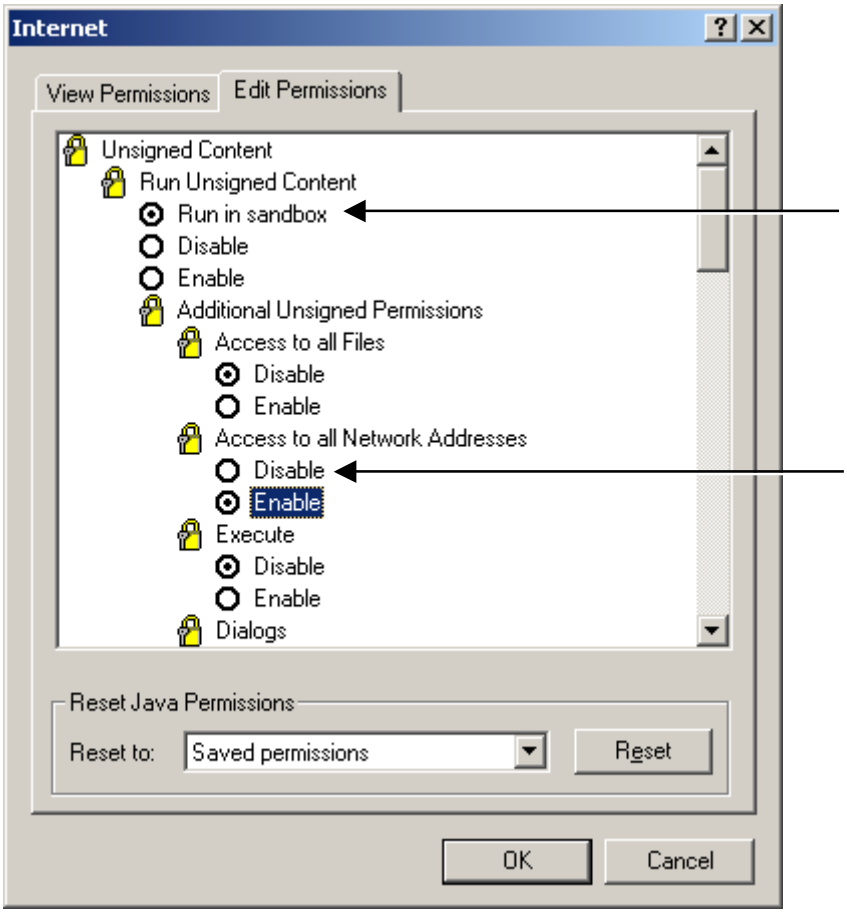


Figure 2-5. Internet Explorer Configuration window

9. Under Run Unsigned Content, enable Run in Sandbox.
10. Under Access to all Network Addresses, Click Enable.
11. Click **OK** for each consecutive dialog to save all changes.
12. Repeat steps 3 to 11 for **Intranet Options**.

Opening the Web Management Application

It is assumed that the *Explorer* on the management station is configured according to the previous section.

1. Open your Web Browser application.
2. Enter the unit **IP Address** in the Web Browser address field. After connection has been established you will be prompted to enter the **User Name**.
3. Enter the switch **User Name (**default is **nokia)** followed by the password (press **Enter** if none has been assigned).

The **Welcome** dialog appears together with the switch view dialog from which all configuration and monitoring options can be accessed.

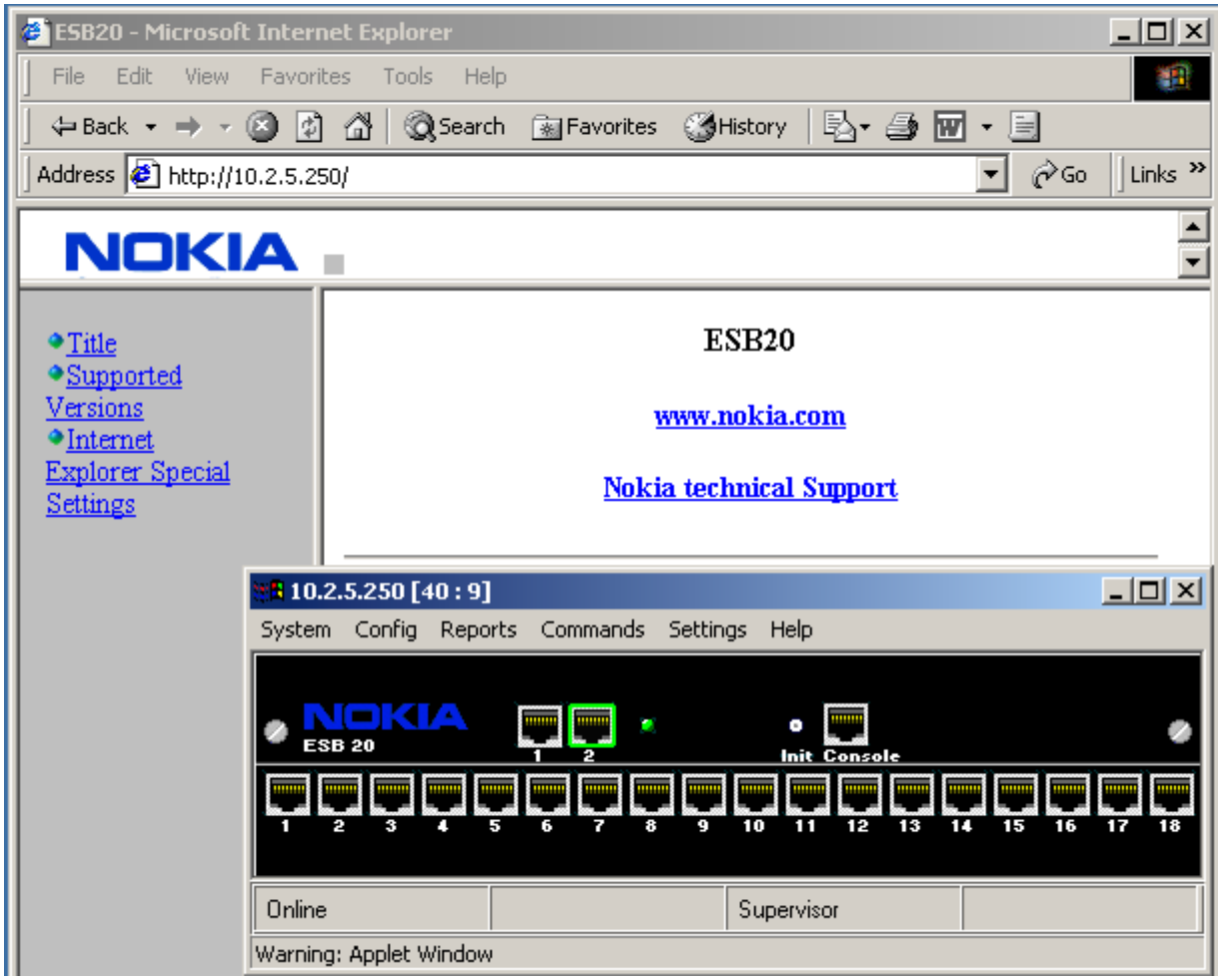


Figure 2-6. Web Management application Welcome screen and switch view dialog

4. You may now start working with the Web Management application according to the description given in the following section.

Navigating the ESB20 Web Management Dialog

The switch view provides a real-time display of the ESB20 interfaces, showing the currently active connections (green). The *menu* options provide access to *unit* configuration and monitoring options. *Port specific* configuration and monitoring options are invoked by right-clicking the port of interest.

If the unit generates traps while switch view is open, a Trap window will appear.

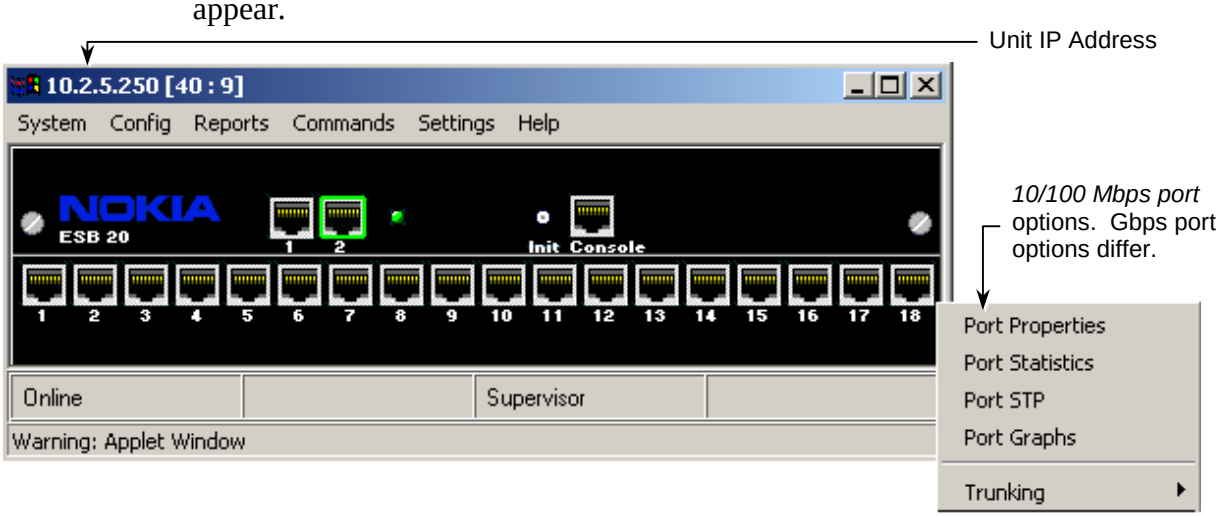


Figure 2-7. Web Management Application Main dialog

Standard Dialog Buttons

Below is a standard dialog showing the **Refresh**, **Set**, and **Abort** buttons.

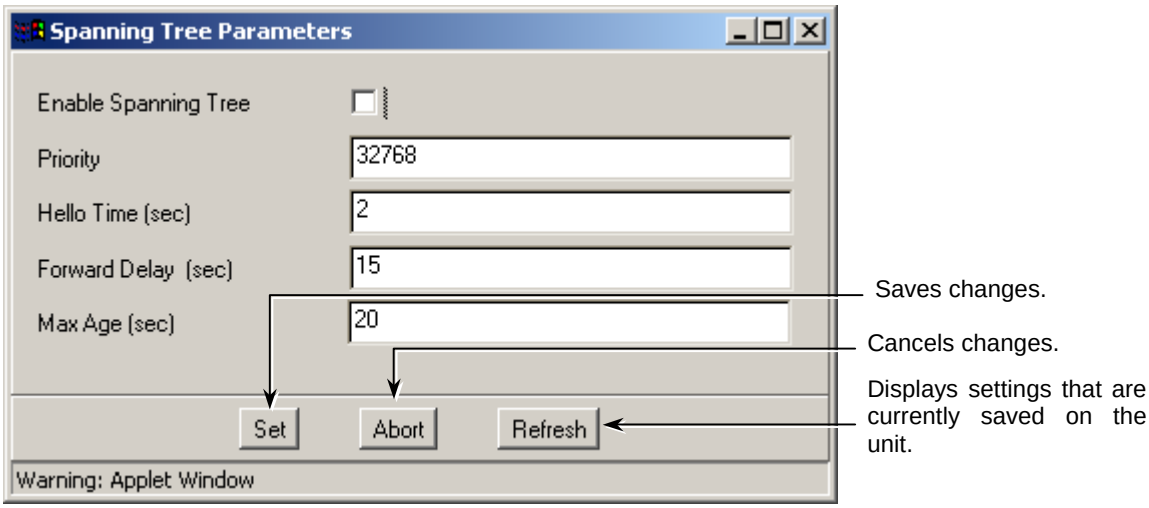
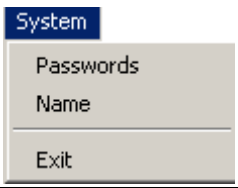
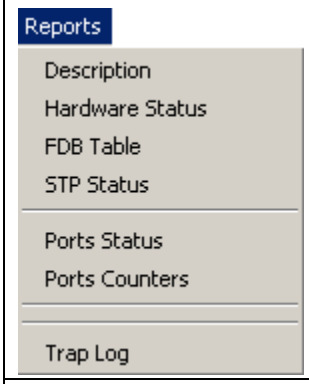
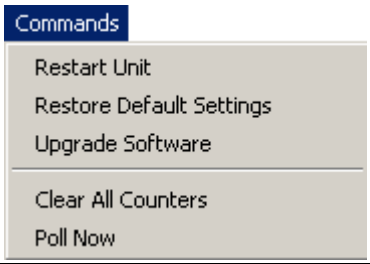


Figure 2-8. Standard ESB20 Web Management dialog

The menu options are described below:

Note: *The menu options provide unit related functionality. All port related options such as port configuration, statistics, STP, Trunking, etc., are accessible by right-clicking the relevant port and selecting the function from the displayed pull-down menu.*

	Password and unit identification options (in addition to application Exit function).

	All unit configuration options.
	Invokes version information, as well as displays of various types of status and log reports.
	Executes the displayed commands.
	Global Polling settings.

Terminal Interface Management Application

About the Terminal Interface Application

The Terminal Interface application provides simple menu driven operator interface that is to be used for system initialization and diagnostics. The terminal interface is VT-100 compatible and as such, can be viewed via a Telnet session. The primary purpose of the terminal interface is to set only the basic operational parameters.

The communication parameters are: 9600, 8 bits, No parity, 1 stop bit

Accessing the Terminal Interface Menu

Remotely

1. Open the **Telnet** application on the management station by clicking the **Start** button and choosing **Run**. The Run dialog appears.

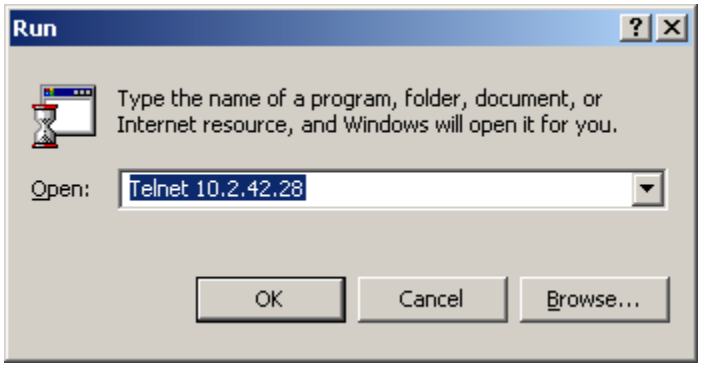


Figure 2-9. Opening a Telnet session

2. Type **Telnet** and the IP Address of the unit.
3. The Telnet window appears. If a connection is established, you will be prompted to enter the **User Name**.
4. Enter the **User Name** (default is **nokia**). You will be prompted for the Password.
5. Enter the **Password** (default is none; press **Enter**). The Setup menu appears.
6. You may start working with the Terminal Interface application according to the instructions given in the following section.

Terminal Interface Navigation Commands

- Previous menus are accessed by pressing **Esc.**
- The **Main** menu is accessed by typing the number **9** from any menu.
- Options are edited by typing the number of the corresponding item, entering the new value at the prompt, and pressing **Enter.** The change is *automatically saved* and may be displayed immediately on the screen, or after a short waiting period.
- You may now type the next number corresponding to another item to be modified.

Terminal Interface Application Main Menu

All Terminal Interface management application options are accessible from the Main menu.

```
ESB20 1.28 Aug 17 2000
Main Menu

1.  General Configuration
2.  SNMP Configuration
3.  Ports Configuration
4.  Ports Status
5.  Load Factory Defaults
6.  Software Upgrade
7.  Reset
8.  Logout
```

Figure 2-10. Terminal Interface Menus

Main Menu Options

- **General Configuration.** Access to remote access IP Address definitions and passwords. Provides access to the Advanced Menu via which DHCP, and VLAN settings are defined, in addition to other functions and protocol settings.
- **SNMP Configuration.** Access to SNMP community and management station definitions.
- **Ports Configuration.** Accesses port configuration screens, where each port is defined separately.
- **Port Status.** Accesses a screen summarizing the status of the ports and their configurations.
- **Factory Defaults.** Loads (after a verification message) the factory defaults.
- **Software Upgrade.** Performs (after a verification message) software upgrade.
- **Reset.** Resets the switch.
- **Logout.** Session logout.
- Subsequent submenus are accessed by *typing* the item number (it is not necessary to press **Enter**).

General Configuration

The General Configuration Menu provides access to the SNMP agent address definitions, and via the Advanced Features, to unit identification defintiions, Watchdog Timer Test, and DHCP address assignment mode setting.

Watchdog and DHCP definitions are only available via the Terminal Interface menus (not via Web Management).

To access the General Configuration Menu:

From the **Main Setup Menu**, enter **1** (**General Configuration.)** The Genreal Configuration menu appears.

```
General Configuration

     MAC address                     00 A0 12 07 14 58
 1.  Agent IP Address               : 010.002.005.250
 2.  Agent Netmask                  : 255.255.000.000
 3.  Default Gateway                : 010.002.001.001
 4.  Supervisor/Terminal Password   :
 5.  System Name                    :
 6.  Advanced Features
 9.  Main Menu
```

Figure 2-11. General Configuration Menu

- **Mac Address.** This is a unique address identifying each unit. The MAC address cannot be modified.
- **Agent IP Address.** This is either the user assigned or the DHCP assigned SNMP address that is used to access the unit remotely. The Agent IP Address is unique in the network.
- **Agent Netmask.** Thirty-two bit number that determines the network size and the IP of the unit subnet.
- **Default Gateway.** This is the gateway to which all packets with unknown IP addresses are sent.
- **Supervisor/Terminal Password.** Password that enables editing access to the unit (the default was blank).
- **System Name.** Name assigned by the user to the switch.
- **Advanced Features.** Accesses menu for enabling VLAN mode, Spanning Tree mode, and Watchdog timer test.

Advanced Features

To access the Advanced Features Menu:

From the **Main Menu**, enter **1** (**General Configuration**), and choose **6. Advanced Features**. The Advanced Features menu appears.

```
Advanced Features

1.  Enable VLAN mode                : No
2.  Enable Spanning Tree mode       : No
3.  Watchdog timer test             : No
9.  General Configuration
```

Figure 2-12. Advanced Features Menu

- **Enable VLAN mode.** Enables the unit to support VLAN configuration mode. VLAN options may only be configured via the Web Management applications.
- **Enable Spanning Tree Mode.** Enables the unit to support Spanning Tree mode.
- **Watchdog Timer Test. Terminal Interface option only.** Tests the Watch Dog time out value.

SNMP Configuration

Defines the manager to which the unit will send Traps, enables the Alerts, and sets the Read and the Write Community names.

To access the SNMP Configuration Menu:

From the **Main Setup Menu**, enter **2. SNMP Configuration.** The SNMP Configuration menu appears.

```
SNMP Configuration

 1.  IP Address of Manager          : 000.000.000.000
 2.  Read Community Name            : public
 3.  Write Community Name           : private
 4.  Trap Community Name            : public
 5.  Send Alert Traps               : No
 6.  Advanced Mode                  : No
 9.  Main Menu
```

Figure 2-13. SNMP Configuration Menu

- **IP Address of Manager.** The address to which Traps (notification of specific events) are sent.
- **Read Community Name.** In order to *view* management information for this switch, the manager must access the switch using the Community name defined in this field. The default name is **public.**
- **Write Community Name.** In order to *set* management definitions for this switch, the manager must access the switch using the Community name defined in this field. The default name is **private.**
- **Trap Community Name.** This is the Community name used by the switch when sending traps to the management station. The default value is **public.**
- **Send Alert Traps.** Setting this option to **No**, prevents Traps from being sent by the unit. Setting this option to **Yes**, causes Traps to be sent by the unit upon the following conditions:
  - if it receives SNMP queries with the wrong community name;
  - if a link goes up or goes down;
  - if there is a Cold Start or a Remote Fault.
- **Advanced Mode.** When this option is enabled, the unit can *only* be managed by the designated manager and not by any other stations that may have been defined via the Web Management application.

Ports Configuration

To access the Ports Configuration Menu:

From the **Main Setup Menu**, enter **3. Ports Configuration.** The Ports Configuration menu appears.

```
Ports Configuration

     Type                                10/100BaseTx Ports
 1.  Select Panel (F=Front,R=Rear)  : F
 2.  Select Port [1:2]              : 1
 3.  Enable                         : Yes
 4.  Auto Negotiation               : Yes
 5.  Speed 0=10M 1=100M             : 0
 6.  Full Duplex                    : Yes
 7.  Flow Control                   : No
 8.  Back Pressure                  : No
 9.  Main Menu
```

Figure 2-14. 1Gbps module Configuration Menu

To access the desired port

1. In the **Select Panel** field, enter the letter corresponding to the location of the number of the port to be defined: **F** (front panel), or **R** (rear panel or backplane).
2. In the **Select Port** field, enter the number of the port to be defined: 1..2 if **F** was previously selected, or 1..18 if **R** was previously selected.
3. Make the desired modifications according to the parameter definitions given in the **Port Configuration** section.
4. If no other ports are to be configured, press **Esc** until the **Main** menu is accessed.

Basic Unit Operation Commands

Reset Options

The switch can be restarted using the following methods:

- From the **Front Panel:** by pressing the **Reset** button on the front panel.
- Via the **Web Management application**: by selecting **Reset** from the **Commands** menu.
- Via the **Terminal Interface Management application**: by selecting **7** (**Reset**) from the **Main** menu.

Restore Default Settings

The factory defined default settings can be reloaded to the switch using the following methods:

- Via the **Web Management application**: by selecting **Restore Default Settings** from the **Commands** menu.
- Via the **Terminal Interface Management application**: by selecting **5** (**Load Factory Defaults**) from the **Main** menu.

For additional information on Default Settings, refer to section **XX.**

Clearing Counters

To clear all counters

In the **Web Management application,** select **Clear All Counters** from the **Commands** menu.

Executing a Polling Command and Setting the Timing Values

Enabling Polling and Setting Polling Timing Values

1. In the **Web Management application,** choose **Setting**, and select **Polling.** The following dialog appears.

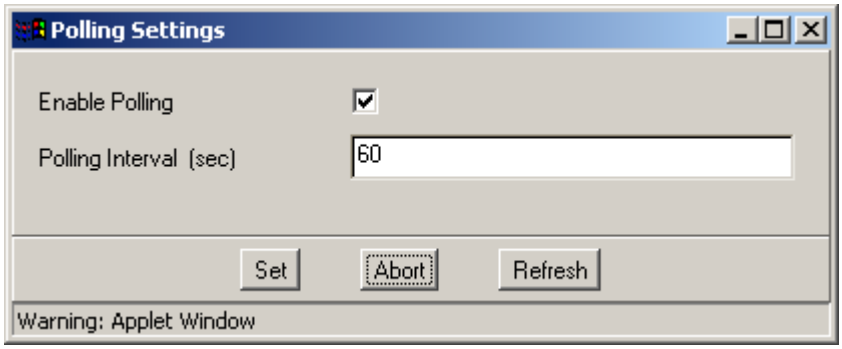


Figure 2-15. Polling Setting dialog

2. Set the **Polling Interval** to the desired value: 1..60 seconds (Default = 60).
3. Click **Set**.

Executing a Polling Operation

In the **Web Management application,** select **Poll Now** from the **Commands** menu.

Chapter 3 Configuration Procedures

ESB20 may be remotely configured by opening a sessions using the IP Address and passwords assigned to the unit. The Web Management application is most commonly used for configuring and monitoring the unit. The Terminal Interface Management application also provides basic functions necessary for unit configuration and management and is usually used only for the initial setup. Consequently, this chapter describes in detail the configuration procedures as performed via the Web Management application, followed by a short description of the same procedures that may be executed via the Terminal Interface application.

The unit is supplied with pre-configured factory default values. The default values can be reloaded anytime by executing the appropriate command.

Factory Defaults

The unit is supplied with pre-configured factory default values which can be reloaded anytime by executing the appropriate command. It is recommended to peruse the default definitions and determine which require modification. This section describes the default configuration values, and how to reload them if necessary.

Default Configuration Values

ITEM	DEFAULT DEFINITIONS	
Global Setting	User Name Password Aging Time Long Frames Mode	**nokia** none (press **Enter**) 300 sec Disabled
SNMP Settings	Read Community Write Community Trap Community Send Alert Trap Advanced Mode	public private public Disabled Disabled
Spanning Tree	Disabled	
	Priority Hello Time Forward Delay Max Age	32768 2 sec 15 sec 20 sec
Sniffer Setting	Disabled	
VLAN Setting	Disabled	

ITEM	DEFAULT DEFINITIONS	
10/100 Mbps Port settings	Auto-negotiation	Enabled
	Duplex Mode	Half Duplex
	Class of Service	Low
	Flow control options	Disabled

Reloading Factory Defaults

Factory defaults may be reloaded either from the Web Browser or via the Telnet Setup menu.

Reloading Factory Settings via the Web Management Application

From the **Command** menu, select **Restore Default Settings** and respond with **Yes** to the displayed verification prompt**.** The factory settings will be restored to the unit.

Reloading Factory Settings via the Terminal Interface Menu

In the **Terminal Interface Main Menu**, type **5** (**Reload Factory Default**s), and enter **Yes** in response to the verification prompt. The factory settings will be restored to the unit.

System Information

These parameters include two passwords for different access levels, system access information, and global parameters such as IP Address definitions, Aging Time, and enabling Long Frames mode.

System Passwords

Two different password definitions options are provided for the unit: **Web** and **Supervisor**. The *Web* password secures Web Management session *entry* and *Read Only* access to parameters that affect switch operation. The *Supervisor* password provides access to editing functions. Both passwords are undefined by default, enabling access to a Web session and to editing functionality.

The Supervisor password may be modified via the Terminal Interface Menu or via the Web and is enabled after the unit is reset. The Web password is only modifiable via the Web and is enabled for the next time that the Web application is opened.

Changing Passwords via the Web Management Application

To set the passwords

1. From the switch view **System** menu, choose **Password.** The following dialog appears.

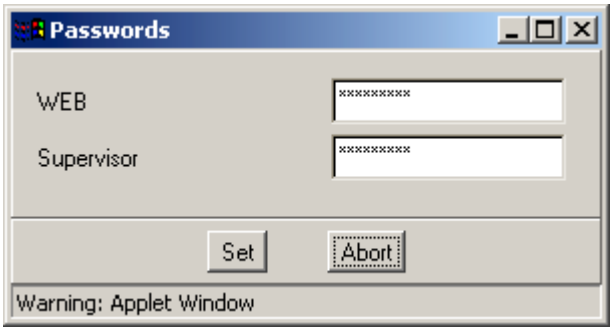


Figure 3-1. Password Definitions dialog

2. To secure all access (including Read Only) to the unit via the Web application, redefine the WEB password. You will be prompted to enter the new Web password each time you attempt to open the Web application for this unit.
3. To limit Write access to the unit, redefine the **Supervisor** password. This password will be a conditional entry in order to edit the unit parameters. The Supervisor password will be enable-ed after the next Reset operation.

Password Modifications via the Terminal Interface Menu

To set the Supervisor password

1. In the **Terminal Interface Main Menu**, type **1** (**General Configuration**). The General Configuration menu appears.
2. Type **4** (**Supervisor / Terminal Password**). You will be prompted to enter the new Supervisor password.

System Location and Contact Information

Web Management enables defining the unit name, its location, and contact information, while via Terminal Interface Management only the system name may be assigned.

Setting System Contact Information via the Web Manager

1. From the **System** menu, choose **Names**. The following dialog appears.

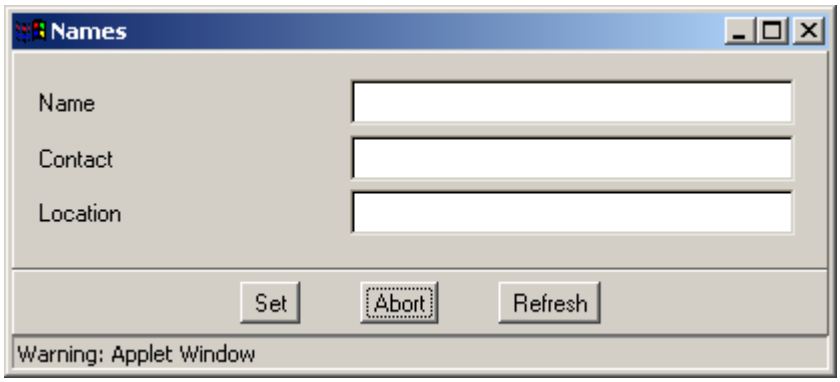


Figure 3-2. Password Definitions dialog

2. In each field, enter the appropriate information according to the following descriptions and click **Set** to apply:
   - **Name**. Unit name appearing in the application window. If none is assigned, then the unit IP Address (e.g. 10.2.42.28) is displayed.
   - **Contact**. Enter the name of the person or organization responsible for administering the system.
   - **Location**. Physical location of the system.

Setting System Name via the Terminal Interface Menu

Only the System Name can be defined via the Terminal Interface Menu.

1. In the **Terminal Interface Main Menu**, type **1** (**General Configuration**). The General Configuration menu appears.
2. Type **5** (**System Name**), and enter the designated name for the unit.

IP Address, Aging Time, and Long Frames Mode

This group includes the IP Address settings and additional parameters.

Defining Global Settings via the Web Manager

1. From the **Config** menu, choose **Global**. The following dialog appears.

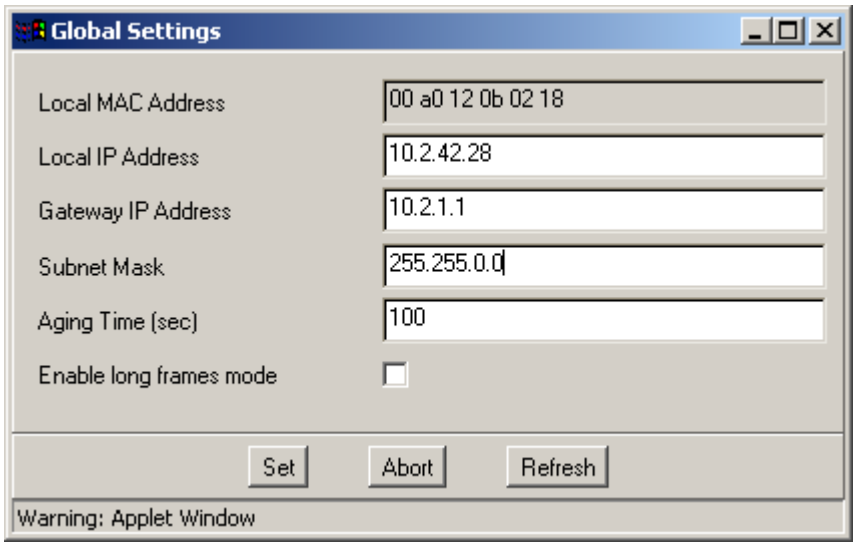


Figure 3-3. Password Definitions dialog

2. To update the currently displayed unit values, Click **Refresh.**
3. Modify the settings according to the following definitions, and click **Set** to enable:
   - **Local MAC Address.** Unique address specifically assigned to the unit during the manufacturing stage. This address cannot be modified.
   - **Local IP Address.** Identifies the device on the network. The value of an IP Address should be unique in the network.
   - **Gateway IP Address.** IP Address of the Gateway device. The device is on the same network as the unit.
   - **Subnet Mask.** Designates the subnet to which the IP Address belongs.
   - **Aging Time.** Maximum duration (in seconds) for which the address of a learned network device remains on the list of stations bridged by the unit. The address is removed from the list of stations if no frame is received within the specified Aging Time.
   - **Enable Long Frames Mode.** Enables the module to transfer non-standard packets up to 6K bytes long.

SubMenu

Defining Global Settings via the Terminal Interface Menu

1. In the **Terminal Interface Main Menu**, type **1** (**General Configuration**)**.** The General Configuration menu appears.
2. Define the **Agent IP Address**, **Agent Netmask,** and **Default Gateway** by selecting the corresponding menu numbers and entering the values.

Port Configuration

Each of the ports is configured by default according to *Factory Defaults* page *3-1*. The configuration of each port may be viewed or modified via the Web Management application or the Terminal Interface.

Configuring Ports via the Web Manager

The port configuration dialog is invoked separately for each port. The port dialog includes the option **Use Port Properties for All Ports** that enables you to automatically assign a selected port configuration to all other ports in the same group (group of two, or group of eighteen)..

To configure an ESB20 port

1. In the **Switch View** dialog, right-click on the port of interest. A pull down menu appears.
2. Choose **Port Properties.** The following dialog appears.

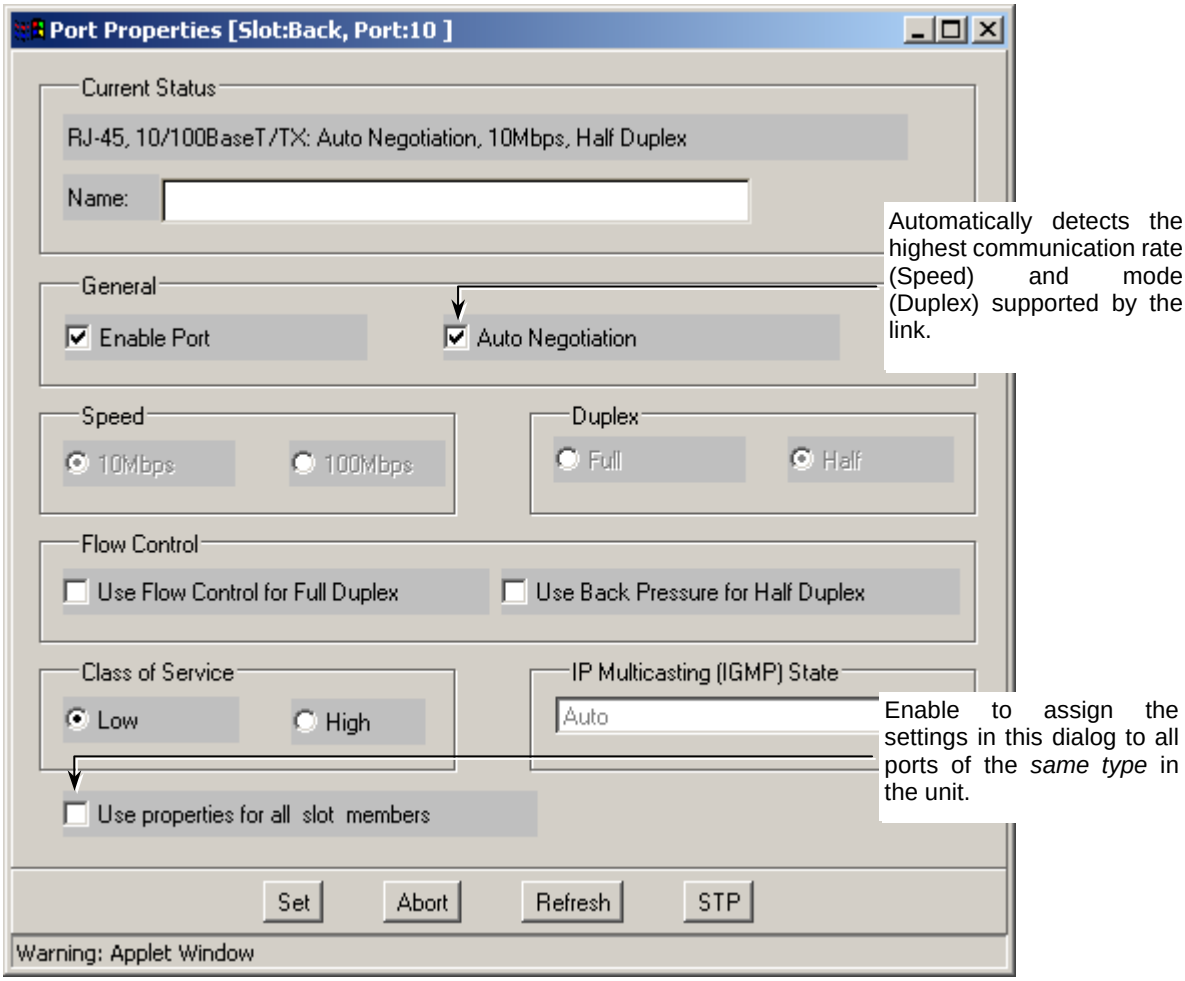


Figure 3-4. Port Configuration

3. Set the parameters according to the following definitions:
   - **Name.** User assigned name to the port.
   - **Enable Port**. Used to enable (or disable) the port.
   - **Auto Negotiation**. When check-marked, it automatically sets the *Speed* and *Duplex Mode* (Half or Full Duplex) of the port to correspond to the connected device. Default = enabled.
   - **Speed.** If Auto Negotiation mode is *disabled*, the port communication rate is determined by the assigned value (10Mbps, or 100Mbps). Default = 100Mbps.
   - **Duplex (Mode).** If Auto Negotiation mode is *disabled*, the port Duplex Mode is determined by the assigned value (Full, Half). Default = Half

- **Flow Control.** Enables controlling the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it:
  - **Flow Control for Full Duplex.** Generates Flow Control packets and processes received flow control packets.
  - **Back Pressure for Half Duplex.** When enabled, it ensures that the transmitting port does not overwhelm a receiving port with data. When the buffers allocated to a port exceed a certain size, a "Jam" message will be sent to the transmitting port to stop its transmission.
- **Class of Service (CoS).** The priority flag of an input port may be set to High to Low. All frames received from that port would be assigned with the port priority to the output queues. The Priority weight between the low and high priority queues is defined as 8 to 2, means that 8 frames from the high queue will be transmitted and two from the low queue.
- **Use Properties for all slot members.** Copies the configuration values of this port to other ports of the same group (all front-panel ports and all rear-panel ports).

Configuring the Ports via the Terminal Interface Menu

1. In the **Terminal Interface Main Menu**, type **3** (**Port Configuration**). The Port Configuration screen appears.

```
Ports Configuration

    Type                              10/100BaseTx Ports
1.  Select Panel (F=Front,R=Rear)   : F
2.  Select Port [1:2]               : 1
3.  Enable                          : Yes
4.  Auto Negotiation                : No
5.  Speed 0=10M 1=100M              : 1
6.  Full Duplex                     : No
7.  Flow Control                    : No
8.  Back Pressure                   : No
9.  Main Menu
```

2. Select the location of the port to be modified as follows:
   - Type **1 (Select Panel).**
   - Enter **R** for Rear Panel, or **F** for Front Panel (Gbps ports).
3. Select the port to be configured as follows:
   - Type **2 (Select Port).**
   - Enter the port number. The number of the port corresponding to the current configuration screen will appear in the **Select Port** line.

4. For each parameter to be modified:
   - Enter the number corresponding to the option.
   - Enter the value.
5. Press the **Esc** key to save the changes and return to the previous screen.

SNMP Agent Configuration

The SNMP protocol provides a mechanism for management entities, or stations, to extract information from the *Management Information Base* (MIB) of a managed device. The Network Management Station (NMS) accesses this information by using the SNMP protocol to send commands to the managed device.

The NMS polls the managed device for information as and when it is required. A managed device may initiate an exchange of information by generating various types of traps to notify the NMS of critical events that may affect the ability of the NMS to communicate with the managed device or other managed devices on the network, and therefore to "manage" the network. Such events include the restarting or re-initialization of a device, a change in the status of a network link (up or down), or an authentication failure.

A *community* is a relationship between an NMS and an agent. The community name is used like a password for a trivial authentication scheme. A pairing of an SNMP community and an SNMP community profile determines the level of access that the agent affords to an NMS that is a member of the specified community

The SNMP Settings dialog designates the NMS address and the Community names for various access levels. In *standard* mode, the unit sends traps to a single designated station, and other network stations with the appropriate Community names can *read* and *write* unit parameters. In *Advanced* mode, the unit can send traps to more than one designated manager; however, non-designated stations have no management access. The traps sent by the unit to the NMS are displayed in the Traps Log dialog. The Advanced mode may be enabled or disabled from the Terminal Interface Menu and the WEB Management applications; however, additional management stations can only be *defined* via the WEB Management Applications.

Note: *The Web Management application may also be configured to send e-mail notification messages when specific types of Traps occur.*

SNMP Agent Configuration via Web Management

The SNMP Settings dialog designates management profile for a single management station (standard mode). If *Advanced Mode* is enabled, a dialog enabling the definitions of eight management profiles is opened and the definitions for the *single* profile are *irrelevant.*

Note: *The* ***Trap Community*** *name is relevant to both standard and Advanced modes. Only management stations accessing the unit with the defined Trap Community name will receive Traps.*

Configuring SNMP Parameters for a Single Manager

1. From the **Config** menu, choose **SNMP**. The following dialog appears.

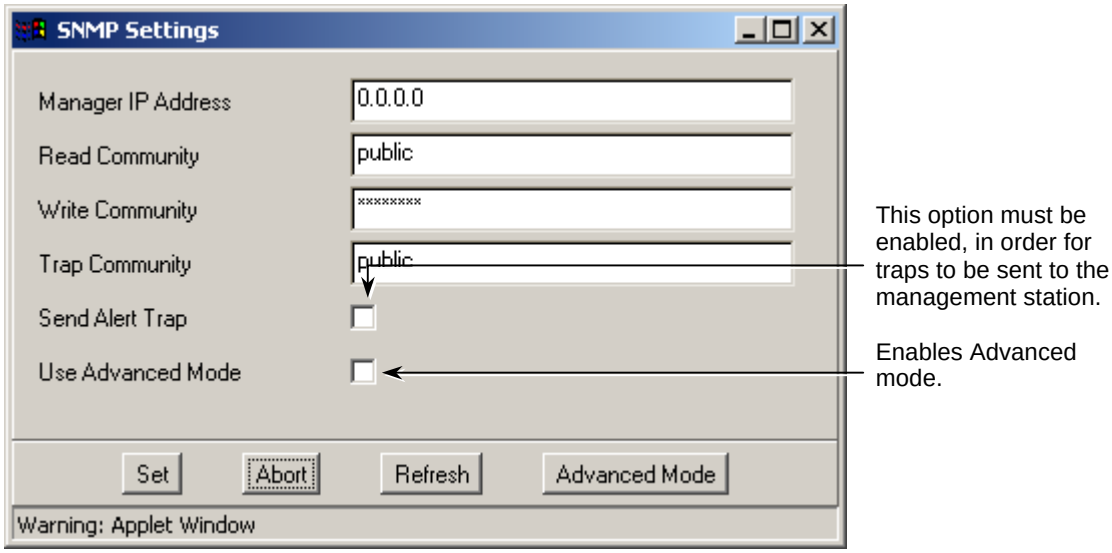


Figure 3-5. SNMP Configuration Settings

2. To update the display of the switch definitions, Click **Refresh.**
3. Define the parameters according to the following definitions, and Click **Set** to save:
   - **Manager IP Address.** The address of the NMS to which the unit sends traps in *standard* mode (Advanced mode is disabled).

     Note: *In order for Traps to be sent, verify that* ***Send Alert Traps*** *is check marked.*
   - **Read Community.** Enables *get* types of operations to be performed on the unit if it is accessed with this Community name. Default = **public**
   - **Write Community.** Enables *set* types of operations to be performed on the unit if it is accessed with this Community name.. Default = **private**
   - **Trap Community.** An additional security measure that limits the stations to which Traps are sent (even if they are defined to receive

Traps), to those that access the unit using this Community name. Default = **public**

Configuring SNMP Parameters for Up To Eight Managers

To configure the unit to send traps to up to eight stations

1. From the **Config** menu, choose **SNMP**. The SNMP Setting dialog appears.
2. Click the **Advanced Mode** button. The SNMP Advance Setting dialog appears.

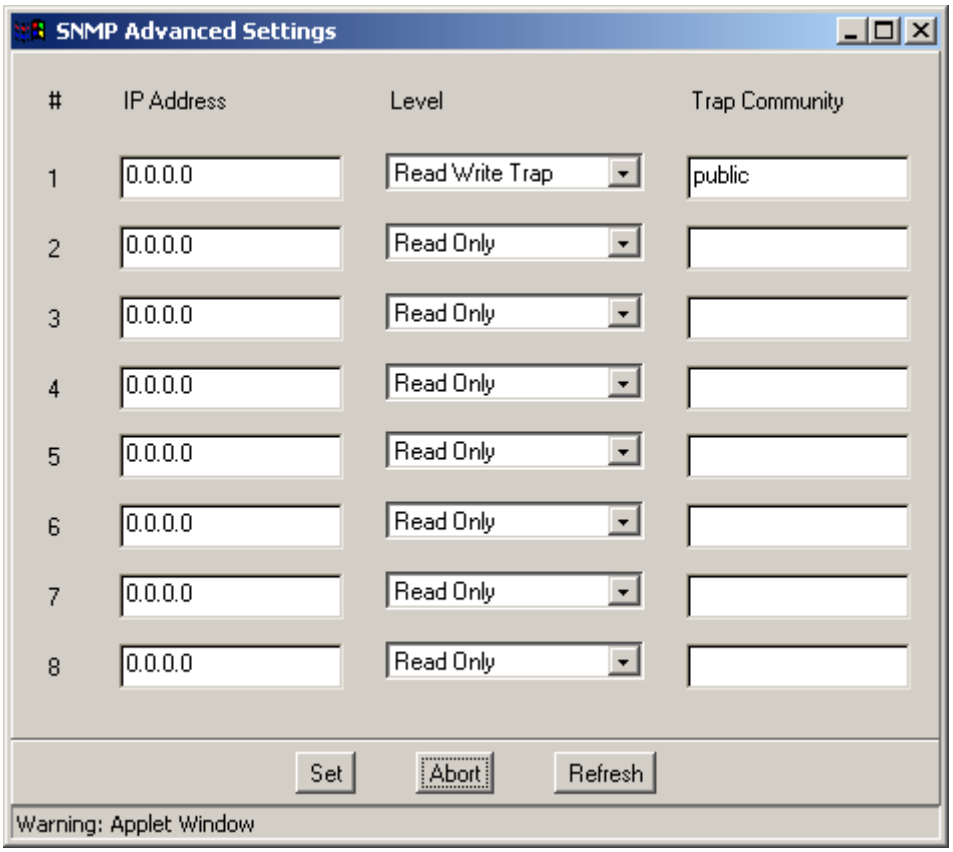


Figure 3-6. Defining up to Eight Management Stations

3. To view the currently Trap management definitions, Click the **Refresh** button.

   Note: *The single manager definitions (standard mode) are automatically assigned to the first profile.*

4. For each management profile:
   - Enter the NMS **IP Address**
   - Select the access mode (Read/Write/Trap, Read Only).

     Note: *Trap access mode may be limited by the **Trap Community** name defined in the **SNMP Setting** dialog.*

- Define the **Community Name.**

5. Click the **Set** button to save.

Note: *Enable or disable the Advanced Mode by checking the* ***Use Advanced Mode*** *button in the SNMP Settings dialog.*

Configuring E-Mail Trap Notifications

You may configure up to four different e-mails to which specified Traps are sent from selected ports. Two types of Trap Notifications may be sent:

- **Control Traps**, include Cold Start, and Authentication Failure.
- **Link Traps**, consist of the link status (link up or down).

To configure the E-mail Trap Notifications

1. From the **Config** menu, select **Mail Notification.** The following dialog appears.

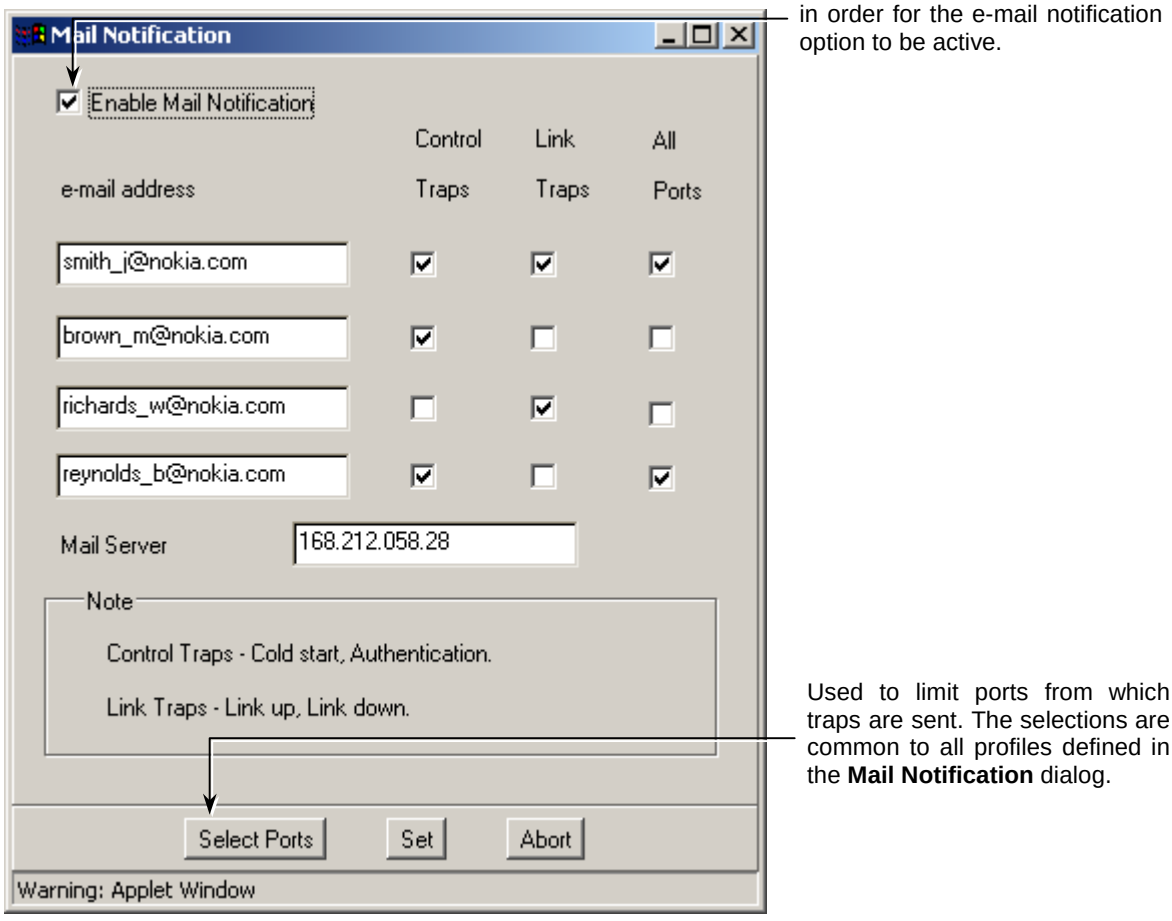


Figure 3-7. Configuring Alert E-mail Notifications

2. Verify that **Enable Mail Notification** is check-marked.
3. Type the **Mail Server** IP Address.

4. For each e-mail trap notification profile, do the following:
   - In the **E-mail Address** fields, enter the e-mail addresses to which Traps will be sent.
   - Check-mark **Control Traps** and/or **Link Traps** according to the type of traps to be sent to the specified e-mail address.
   - For the e-mail addresses to which Traps will be sent from all the ports, check the **All Ports** checkbox. Unchecked e-mail addresses will receive traps from ports defined by via the dialog invoked by clicking **Select Ports** button (step 5).
5. To choose the ports from which Traps will be sent:
   - Click the **Select Ports** button. The following dialog appears.

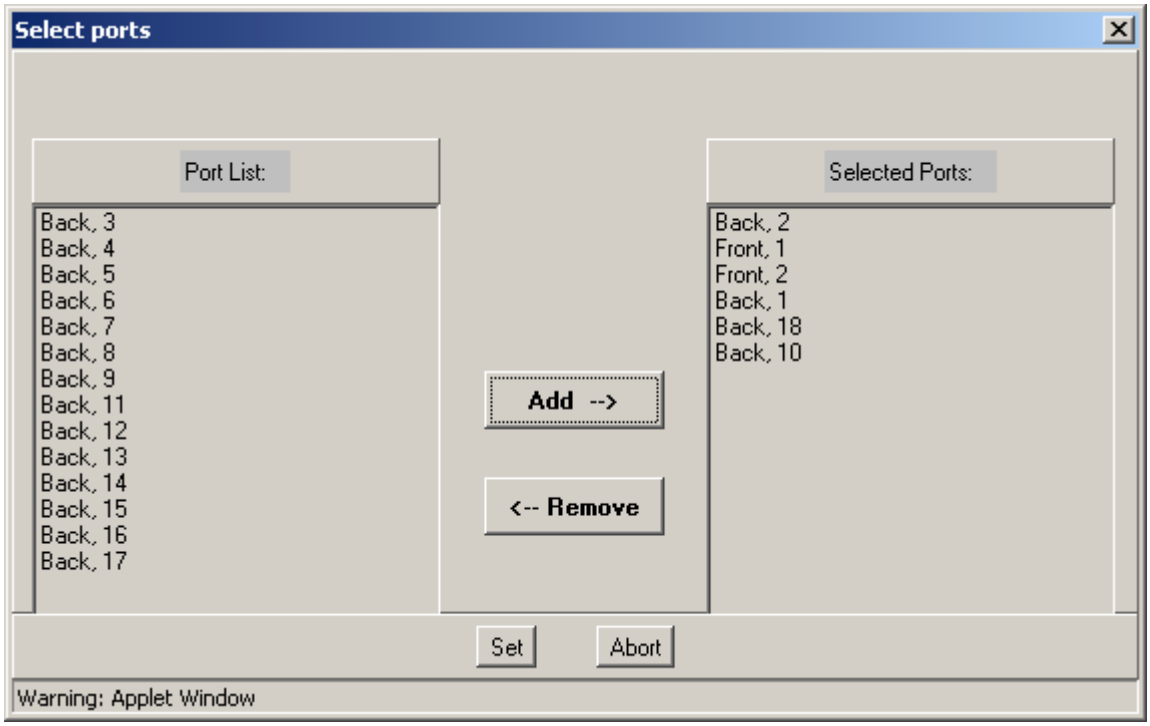


Figure 3-8. Selecting the Ports From which Trap Notifications will be sent

   - Select each port from the **Port List** and Click **Add** to add it to the **Selected Ports.**
   - To remove a selected port, highlight the port in the **Selected Ports** and Click **Remove.**
   - Click **Set** to save the settings. The previous (Mail Notification) dialog will be re-accessed.
6. In the **Mail Notification** dialog, click **Set** to save the changes.

SNMP Configuration via the Terminal Interface Menu

The Terminal Interface Menu provides capabilities for *defining* only a *single* manager; however, *Advanced Mode* may be *controlled* from this menu. This allows enabling or disabling access of additional manager profiles that were defined via Web Management.

To access the SNMP Configuration Menu

From the **Main Setup Menu**, enter **2. SNMP Configuration.** The SNMP Configuration menu appears.

```
SNMP Configuration
 1.  IP Address of Manager          : 000.000.000.000
 2.  Read Community Name            : public
 3.  Write Community Name           : private
 4.  Trap Community Name            : public
 5.  Send Alert Traps               : No
 6.  Advanced Mode
 9.  Main Menu
```

Figure 3-9. SNMP Configuration Menu

Spanning Tree Configuration

Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. The logical tree computed by the spanning tree algorithm has the following properties:

- A single switch, called the *root* switch, forms a unique root to the tree. The switch with the lowest switch ID is designated as the *root switch*
- Each switch in the tree, except the root switch, has a unique parent. This is the *designated* switch for the LAN that logically connects the LAN to the next LAN closer to the root switch.
- Each port connecting a switch to a LAN has an associated *root path cost* (link cost) which is the sum of the costs for each port between the switch and the root switch.

The spanning tree algorithm is implemented by communication using the Spanning Tree Protocol. The primary protocol data unit (PDU) is the *Hello message* which includes information on the previously mentioned spanning tree properties (root switch ID, designated switch ID, and link cost).

Hello messages are initiated a regular intervals by the root switch and propagated throughout the extended LAN.

ESB20 Spanning Tree Parameters are *set* via the Web Manager, where Spanning Tree Parameters are set for the *unit* and for *individual ports*. These

designate the priority of the unit, and Hello message timing parameters. However, support for Spanning Tree Protocol may be enabled or disabled from the Terminal Interface application as well.

Configuring the Spanning Tree Unit Parameters

Note: *Changes in Spanning Tree parameters are enabled only after the unit has been reset.*

To configure the Spanning Tree unit parameters

1. From the **Config** menu, choose **Spanning Tree**. The following dialog appears.

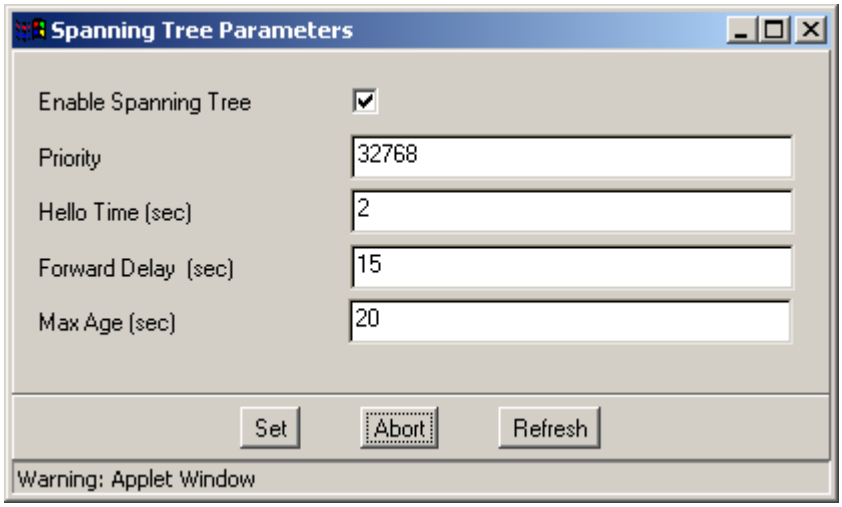


*Figure 3-10. Spanning Tree Protocol **Unit** Configuration dialog*

2. Define the parameters according to the following definitions and Terminal click **Set** to save:
   - **Enable Spanning Tree Protocol.** Enables the unit to support Spanning Tree Protocol.
   - **Priority.** If all switches are enabled with default settings, the switch with the lowest MAC address in the network becomes the root switch. However, due to traffic patterns, number of forwarding ports, or line types, that switch might not be the ideal root switch. By increasing the priority (lowering the numerical priority number) of the ideal switch so that it then becomes the root switch, you force a Spanning-Tree Protocol recalculation to form a new, stable topology.
   - **Hello Time.** Time (in seconds) that determines how often the switch broadcasts its Hello message to other switches.

     Value: 1..10 sec Default = 2.
   - **Maximum Age Timer.** Measures the age of the received protocol information recorded for a port and ensures that this information is discarded when its age limit exceeds the value to the maximum age

parameter recorded by the switch. The timeout value for this timer is the maximum age parameter of the switches.

- **Forward Delay Timer.** Monitors the time spent by a port in the learning and listening states. The timeout value is the forward delay parameter of the switches.

Configuring the Spanning Tree Port Parameters

The Port STP Properties dialog contains the port relevant STP configuration parameters and the displays the status of other port relevant STP parameters that are not configurable.

Note: *Spanning Tree is activated only after the unit has been reset.*

To configure a port's Spanning Tree parameters

1. In the switch view, right-click on the port of interest and select **Port STP** (Spanning Tree Protocol). The following dialog appears.

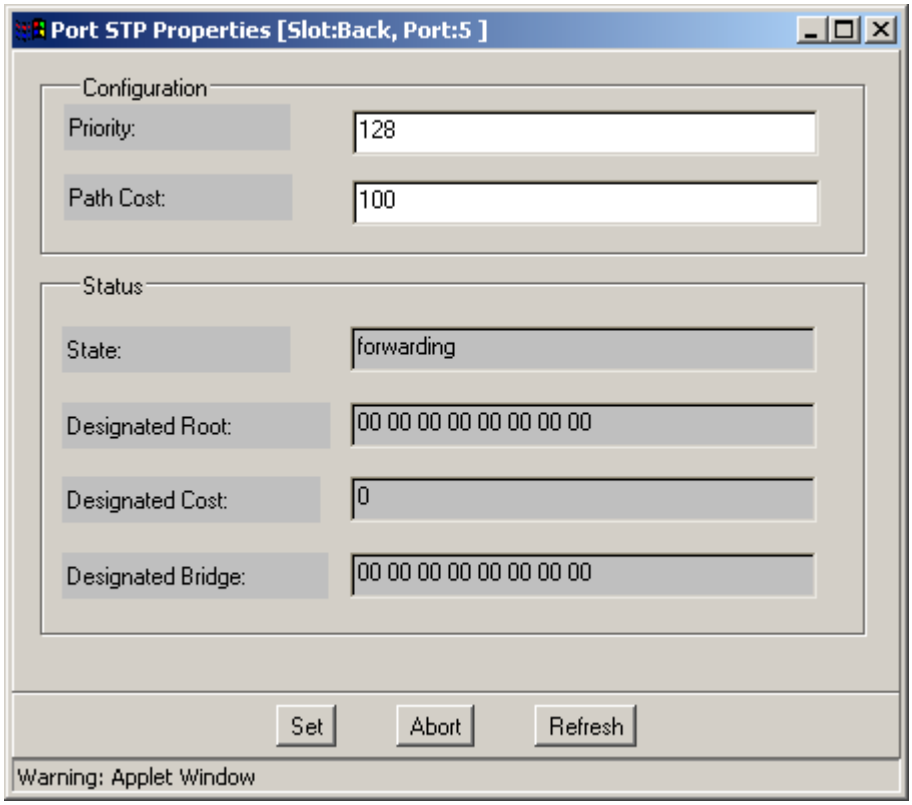


*Figure 3-11. Spanning Tree Protocol **Port** Configuration dialog*

2. Define the parameters according to the following definitions and Terminal click **Set** to save:

   - **Priority.** Priority of the current port (see RFC 1493 for detailed explanation).
     The Priority and the Port number compose the STP port id to be encoded in BPDU.

- **Path Cost.** This port's share of the cost of the paths, heading towards the Spanning Tree root, that include this port; in other words, the Spanning Tree "cost" of going through this port.
- **State.** The port's current state as defined by the Spanning Tree Protocol. Possible states include Disabled, Blocking, Listening, Learning, Forwarding, and Broken.
- **Designated Root.** The MAC address of the network device that functions as the root of the Spanning Tree.
- **Designated Cost.** The path cost of the designated port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
- **Designated Bridge.** The identifier of the designated bridge for this port's segment.

Enabling Spanning Tree Mode via the Terminal Interface Menu

To enable the Spanning Tree Protocol

1. From the **Main Menu**, enter **1. General Configuration**, and choose **6. Advanced Features**. The Advanced Features menu appears.

```
Advanced Features

1.  Enable VLAN mode                : No
2.  Enable Spanning Tree mode       : No
3.  Watchdog timer test             : No
9.  General Configuration

New  Enable Spanning Tree mode       : Yes
```

Figure 3-12. Advanced Features Menu

2. Type 2 (Enable Spanning Tree mode) and type Yes.

Port Trunking

The Link Aggregation Group (**LAG** or Trunk) feature is used to create Fast Ethernet port groups. These LAGs act as single logical ports for high-bandwidth connections between switches or between switches and servers.

Link properties and trunk properties. Properties of a trunk are configured in the same way that the properties of an individual link are configured. Properties for both a trunk and for the individual links of the trunk can be configured, where the properties of an individual link can be different from the properties of the trunk to which it belongs. When a link is a member of a trunk, it takes on the properties of the trunk; when removed from the trunk, it reverts to its own configured properties. For example, a link is configured to half-duplex and the trunk is configured to full duplex. When the link belongs to the trunk, it will transmit full duplex; when the link does not belong to the trunk it will transmit half duplex.

Port groups. Up to three port groups can be defined on each ESB20 switch: two each consisting of up to eight 10/100T/TxBase ports of the same octate (1 to 8, and 9 to 16), and an additional Trunk consisting of the two remaining ports.

The lowest port in the group is the master. It is used as the group communication port for broadcasts, spanning tree and routing. If the lowest port link goes down, the next lowest port in the trunk becomes the master.

Communication rate and connection continuity. A port trunk can be defined to operate at full duplex or at half duplex. Full duplex is recommended in order to achieve the higher bandwidth. If one of the links in the trunk fails, the traffic on that link is automatically divided among the other links in the trunk—assuring continuity of the connection.

Trunking method. ESB20 switch port trunk operates by the method of Source Address Distribution (SA). With this method, the switch distributes traffic in a sequential manner to the links within the trunk on the basis of the source address. Thus, traffic from the same source address is transmitted over the same trunked link regardless of its destination address.

For example, for a trunk of three links that is handling traffic from four nodes A, B, C, and D, distribution would be as follows:

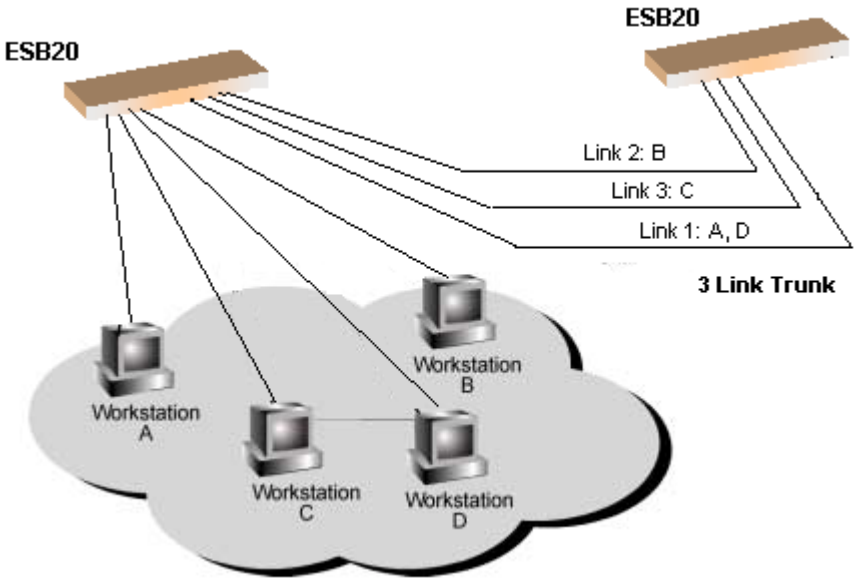


Figure 3-13. Source Address Distribution in Port Trunking

The sequence of learning the addresses of the PCs on the Trunk ports of the ESB20 on the right are:

Mac #1 will be learned on Link1

Mac #2 will be learned on Link 2

Mac #3 will be learned Link 3

Mac #4 will be learned Link 1

Next Mac will be learned on Link 2

Trunks in a Spanning Tree – Port Connection Order

A port trunk acts in a spanning tree just like an individual link. When the trunk is unblocked in the spanning tree, all its links are unblocked; when the trunk is blocked, all its links are blocked.

When a port trunk between two ESB20 switches is to be used in a spanning tree, you need to connect the trunk's links between the switches in *ascending* order. If, for example, ports 1, 2, and 3 of the first switch are to be connected to ports 4, 5, and 6 of the second switch, then they must be connected as follows: 1–4, 2–5, 3–6.

Note: *It is recommended that the ports of each trunk be defined to begin with port 1 so that the port connections between switches will be 1–1, 2–2, 3–3, etc.*

Trunk Configuration

ESB20 provides two predefined empty trunks; one for each octate. To activate a trunk a port from that octate is added to the trunk.

To add a port to the predefined trunk

1. In the switch view, right-click on the port to be added to the trunk. The port menu appears.
2. Select **Add to Trunk**. The port will be added to the trunk of that octate.
3. Repeat the process for any other ports to be added to that trunk.

To remote a port from the predefined trunk

1. In the switch view, right-click on the port to be added to the trunk. The port menu appears.
2. Select **Remove from Trunk**. The port will be removed from the trunk of that octate.
3. Repeat the process for any other ports to be removed from that trunk.

Port Mirroring

The Web Management application provides a function that enables analyzing the traffic on a port without disturbing the connections. This is done by copying the traffic from the port designated as the 'Monitored' port to the one designated as the 'Sniffer' port where it will be analyzed. Each port of the Switch can be mirrored to a Sniffer port under the following conditions:

- Only a single Sniffer port and the corresponding mirrored port can be defined at any one time the same time
- If the mirroring is full duplex, all receive and transmit frames are mirrored to the sniffer port.
- The Sniffer port can be any of the switch ports.

Note: *Port mirroring settings are cleared when the unit is reset.*

To configure and use the Sniffer function

1. From the **Config** menu, select **Sniffer**. The following dialog appears.

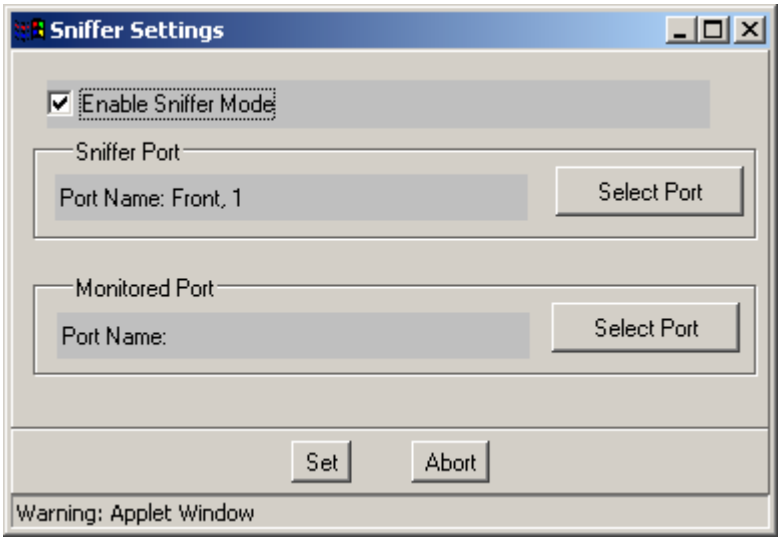


Figure 3-14. Port monitoring Sniffer configuration options

2. Select the **Sniffer Port** by doing the following:
   - In the **Sniffer Port** area, click on **Select Port**. The following dialog appears.

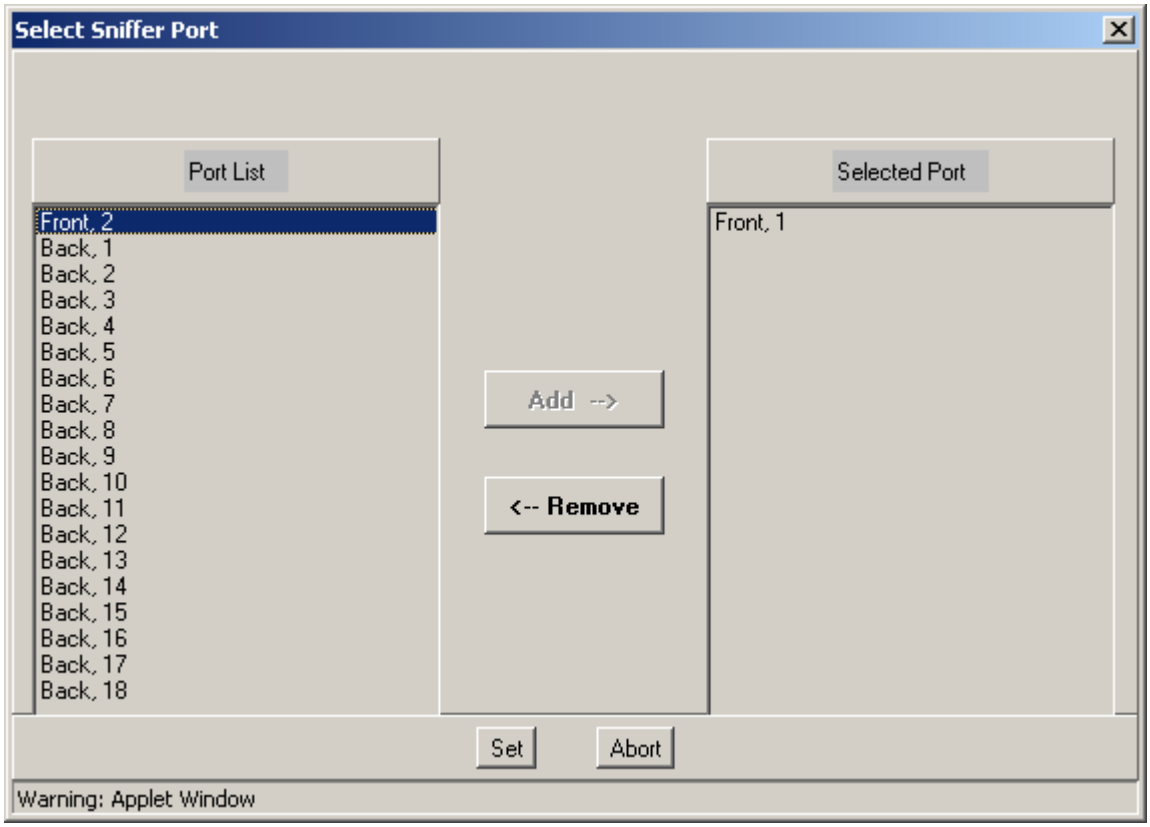


Figure 3-15. Selecting the Sniffer port

- Under **Ports List,** click on the port designated as the Sniffer.
- Click **Add**. The port appears in the **Selected Port** list.
- Click **Set** to save the changes. The Sniffer Settings dialog is reaccessed.

3. From the **Sniffer Settings** dialog, select the **Monitored Port** window area by doing the following:
   - In the **Sniffer Setting** dialog, **Monitored Port** area, click on **Select Port**. The following dialog appears.

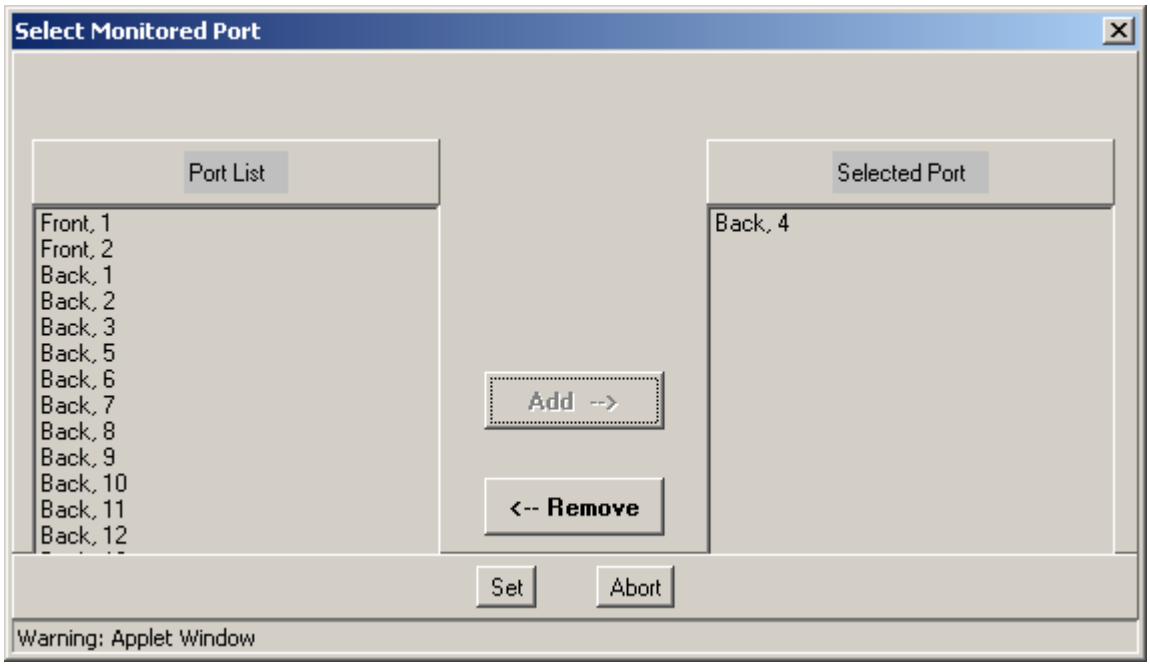


Figure 3-16. Selecting the Monitored port

- Under **Ports List,** click on the port designated as the Monitored Port.
- Click **Add**. The port appears in the **Selected Port** list.
- Click **Set** to save the changes. The Sniffer Settings dialog will be reaccessed.

4. Check-mark the **Enable Sniffer Mode** option in the **Sniffer** dialog.

Chapter 4 VLAN Configuration

General

VLANs enable segmenting a network into related groups by limiting the propagation of *multicast* and *broadcast* messages to members of a specific VLAN. VLANs provide the following advantages for the network:

- Users can be grouped according to logical function rather than physical location.
- Reduction of broadcast traffic.
- Network security since transmissions do not cross from one VLAN to another.
- Software station management.
- Bandwidth usage control by grouping high-bandwidth users on low-traffic segments.

There are several methods for creating VLANS. **ESB20** supports up to 32 *port-based*, 802.1Q-compatible virtual LANs (VLANs). A port-based VLAN is a group of switch ports designated by the switch as belonging to the same broadcast domain. Compatibility with the 802.1Q standard enables assigning a single switch port to two or more VLANs, while still allowing for interfacing with older switches that require a separate port for each VLAN. VLANs may be *statically* configured by manually assigning the ports of each switch in the network to the corresponding VLAN or VLANs.

ESB20 provides an option for enabling or disabling VLAN mode on the switch.

Enabling VLAN Mode

The switch can be made VLAN compliable by simply enabling or disabling VLAN mode.

Note: *VLANs are activated after the module is reset.*

To enable VLAN mode

1. From the **Config** menu, choose **VLANs,** and select **Global Setting**. The following dialog appears.

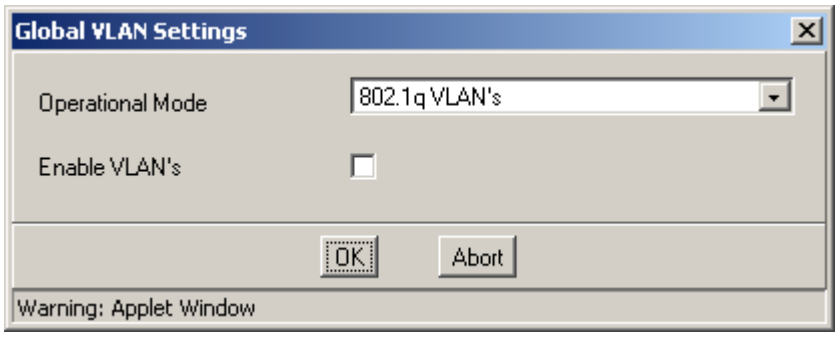


Figure 4-1. Selecting the VLAN operation mode.

2. Select the operation mode.
3. Checkmark the **Enable VLANs** field.
4. Click **OK** to save the changes and close the dialog (VLANs are activated after the switch is reset).

VLAN Configuration

Since an ESB20 port may be assigned to more than one VLAN at the same time, VLAN Tagging is used in order to distinguish between frames *sourced* from this port. The tag contains a unique VLAN identification number between 1 and 4095 that is inserted in packets forwarded between two VLAN-aware devices. A *VLAN-aware* device is a device that complies with the 802.1Q standard; it is a switch, server or station that is able to handle traffic from more than one VLAN on a port.

If the data is to go to a VLAN-aware device, the VLAN identifier is added to the data. If it is to go to a VLAN-unaware device, the switch sends the data without the VLAN identifier.

Note: *VLAN configuration changes are activated after the module is reset.*

Configuring the Switch for VLAN Tagging

ESB20 is configured for VLANs by defining the VLANs, assigning the ports to the corresponding VLANs, identifying the ports connected to VLAN-aware devices and configuring the switch to *tag* the VLAN frames forwarded through these ports. Accordingly, ports to which VLAN-unaware device *assigned to a VLAN* are connected, will be configured to *untag* frames that are forwarded by that port as an *egress* port, and to tag frames forwarded by that port as an *ingress* port with the Default VLAN value. A *default* VLAN is a VID automatically attached to a frame that is to be forwarded from a VLAN-unaware device attached to the port, to a VLAN-aware device.

Trunking and VLANs

ESB20 enables the configuration of up to three Trunks: two consisting of up to eight ports for each octate in the back panel connection, and an additional Trunk consisting either of the two front panel ports or ports 17 and 18 on the back panel.

By assigning a trunk to one VLAN, all of its links are automatically assigned to that VLAN. If a trunk is moved to a different VLAN, all the links moved with it.

Any link that is added to the trunk after the trunk's creation is automatically assigned to the trunk's VLAN. After a link is removed from a trunk, it remains in the trunk's VLAN until it is assigned to a different VLAN.

Defining and Editing VLAN Definitions

Up to 32 VLANs may be created on the ESB20. Each VLAN may be defined according to a VLAN Name which may be a recognizable name such as *Accounting, Production, Red,* etc., and a VLAN ID which is the Tag assigned to the VLAN.

1. From the **Config** menu, choose **Vlans,** and select **Create and Edit**. The following dialog listing the currently defined VLANs appears.

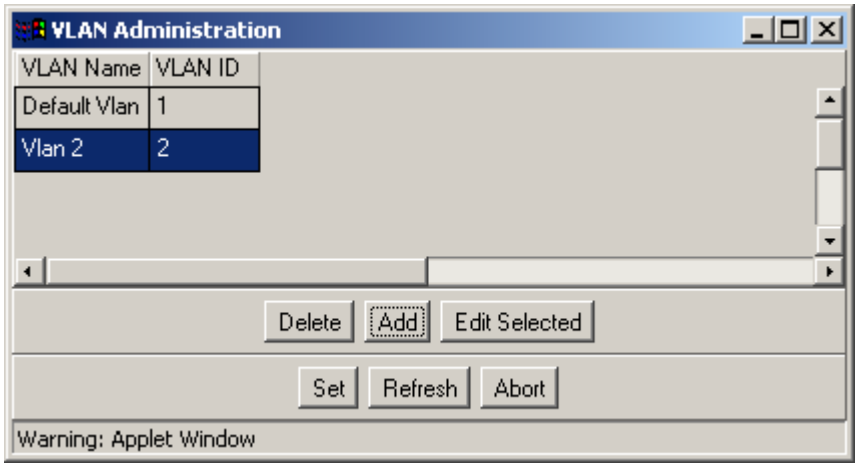


Figure 4-2. VLAN Administration

2. To **Add** a VLAN definition:
   - Click **Add.** The Edit VLAN dialog appears.

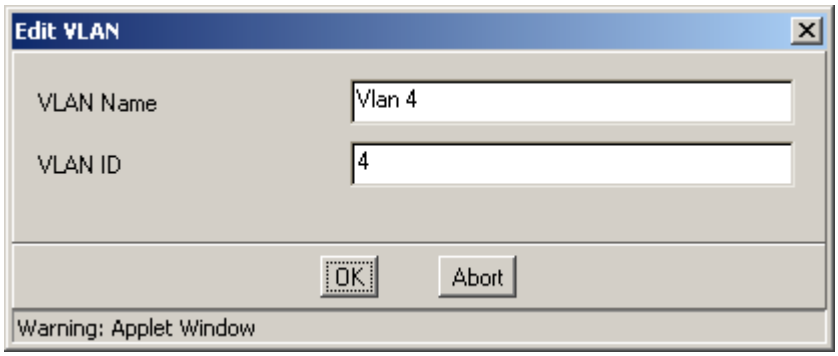


Figure 4-3. Edit VLAN dialog

   - By default, the VLAN Name and VLAN ID are assigned progressively ascending numbers. Make any necessary changes according to the following criteria:
     - **VLAN Name.** A recognizable name that will identify the VLAN.
     - **VLAN ID.** The Tag assigned to the VLAN. Range = 1 to 4095
   - Click **OK.** The newly defined VLAN will be added to the VLAN list in the VLAN Administration dialog.

3. To **Delete** a VLAN: In the **VLAN Administration** dialog, select the VLAN to be deleted and click **Delete.** The VLAN will be deleted immediately, without a verification prompt.

4. To **Edit** VLAN Definitions:
   - Click the VLAN of interest and click **Edit**. The **VLAN Edit** dialog appears.
   - Make the necessary changes and click **Set.**

Assigning Switch Ports to VLANs

By default all ports are configured to the VLAN 1, referred to as the *Default VLAN* (VLAN 1). Each port may be mapped to one or more VLANs. Each VLAN port association is defined as *Tagged, Untagged,* or *No*:

- **No –** assign this value to VLANs to which the corresponding port will *not* be mapped.
- **Tagged –** assign this value to all VLANs to which the corresponding port will be mapped. Incoming frames tagged with the IDs corresponding to the VLANs to which this port is mapped, will access the port device.
- **Untagged –** assign this value to the default VLAN to which the port is mapped. All VLAN frames will have access to this port device. Usually used for devices such as printers that may be shared by several VLANs.

To assign ports to VLANs

1. From the **Config** menu, choose **802.q Vlans,** and select **Members**. The following dialog appears.

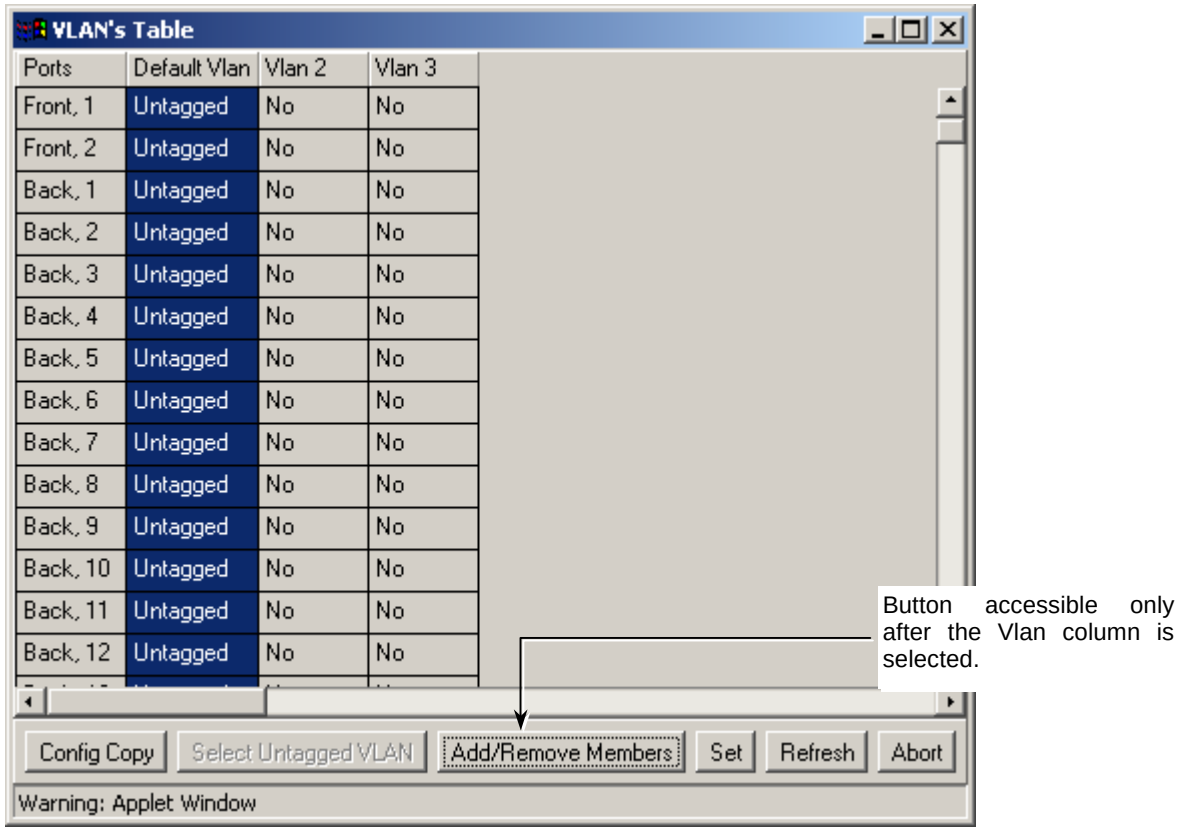


Figure 4-4. Defining VLAN Member

***Note:** The Default Vlan is Vlan1.*

2. Click on the *column* corresponding to the VLAN to be configured. The **Add/Remove Members** button will become accessible.

3. Click the **Add/Remove Members** button. The following dialog appears.

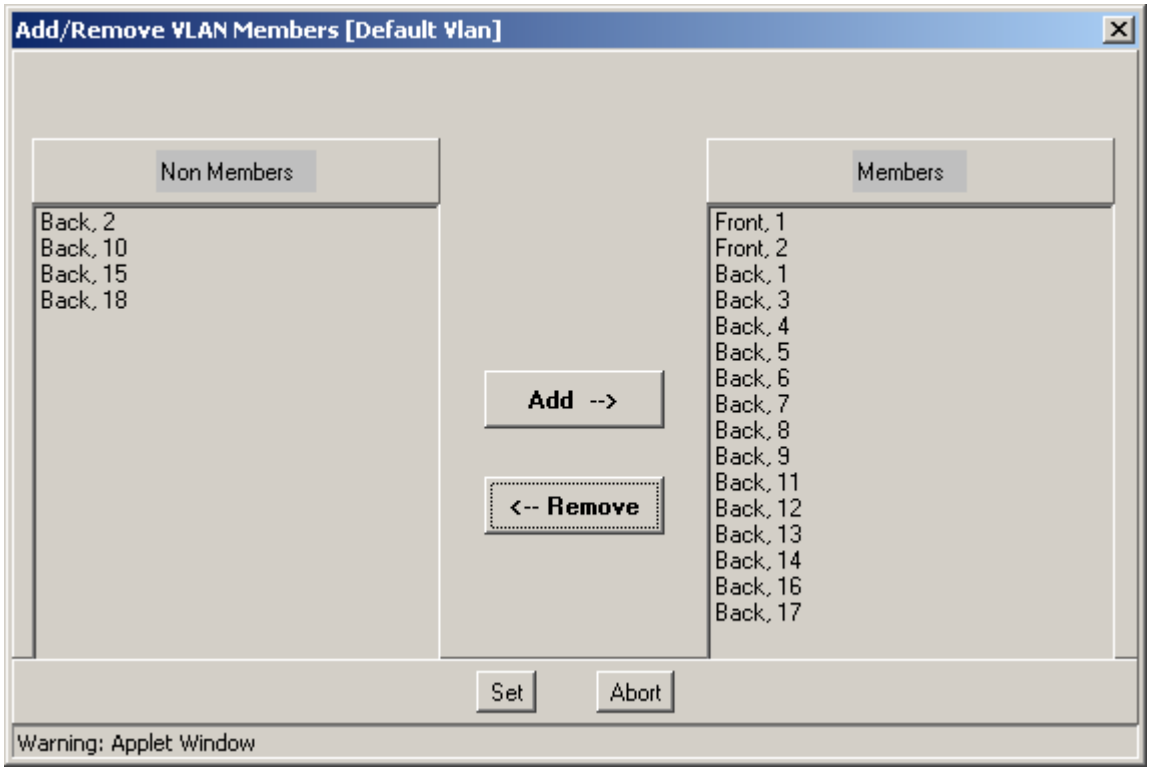


Figure 4-5. Adding Removing Members of a VLAN

4. Select each member to be added to the VLAN and click **Add.**
5. Click **Set.** The VLAN table showing the changes will be displayed, showing membership of each VLAN as Tagged.
6. Repeat the process for each VLAN.

Specifying a VLAN to be Untagged on a Port

Ports to be accessed by all defined VLANs in the switch, are mapped to a *Default VLAN*. The Default VLAN is factory defined as Vlan 1. However the definition may be changed according to the procedure described in this section.

Note: *If the port is a member of more then one VLAN, then only one of the VLANs can be in "Untagged" mode; all others VLAN port modes must be "tagged".*

To change the default VLAN

1. From the **Config** menu, choose **Vlans** and select **Members**. The following dialog appears.

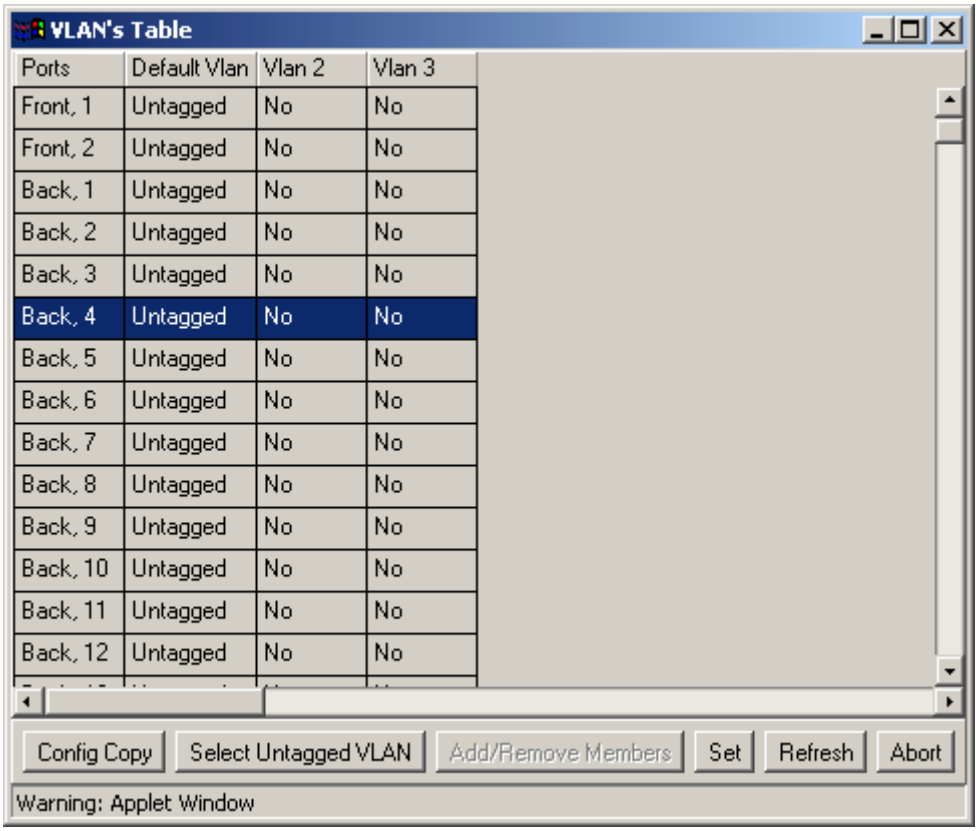


Figure 4-6. Defining the Untagged (Default VLAN)

2. Select the *row* of the port whose Untagged VLAN assignment is to be modified. The **Select Untagged VLAN** button is accessible.
3. Click the Untagged VLAN button. The following dialog appears.

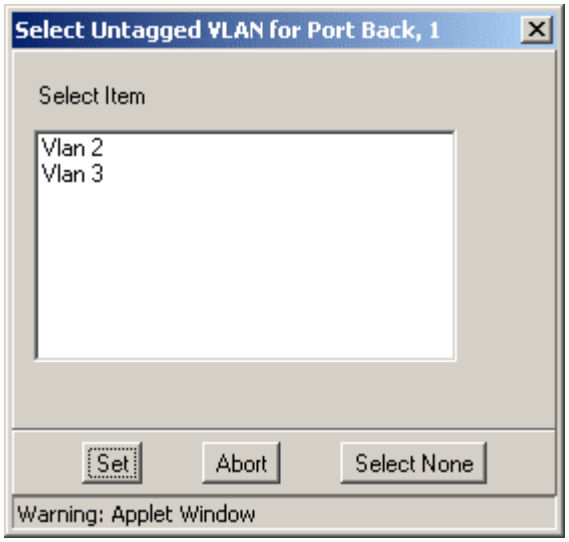


Figure 4-7. Defining the Untagged (Default VLAN)

4. Select the VLAN to be defined as Untagged and click **Set**. The selected VLAN will be configured as Untagged.

Chapter 5 Statistics and Status Reports

ESB20 provides windows for viewing versions, status parameters, configurations, and monitoring statistics. Windows are provided on the unit level and on the port level.

Unit level windows are invoked from the switch view **Reports** menu, while port level windows are invoked by right-clicking on the relevant port and selecting the appropriate option.

This chapter describes the unit level and the port level windows.

Unit Level Reports

Unit level status windows include Description (versions and time from last reset), Hardware Status, FDB Table, Multicast, VLANs, STP status, ports status, ports counters, and Trap Log.

To invoke unit level status and statistics windows

From the switch view **Reports** menu, choose the appropriate option.

Description (Versions)

This window shows the unit type, currently installed software version, and time since the last reset.

To display the Unit Description window

From the switch view **Reports** menu, choose **Unit Description.**

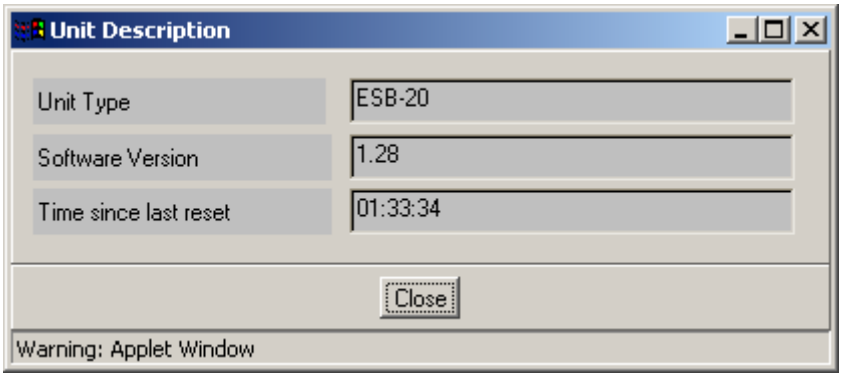


Figure 5-1 Unit Description window

Hardware Status

This dialog shows the currently installed Boot version and the status (Pass/fail) of the self test performed during the last boot procedure.

To display the Hardware Status window

From the switch view **Reports** menu, choose **Hardware Status.**

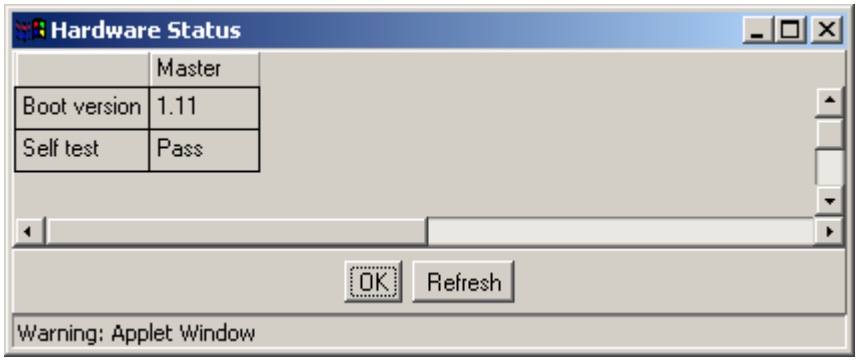


Figure 5-2. Hardware Status window

Viewing the Forwarding Database (FDB) Table

The *Forwarding Database* shows the *source* MAC addresses and the corresponding ports that have received the data on the unit. The Forwarding Database can hold up to 8000 entries. That is 8000 individual stations. When the Forwarding Database table is full, no new MAC address information will be stored in the Forwarding Database. If a packet comes from a device whose MAC Address is not in the Forwarding Database table and the table is full, the unknown address is broadcast to all devices connected to the ESB20 unit.

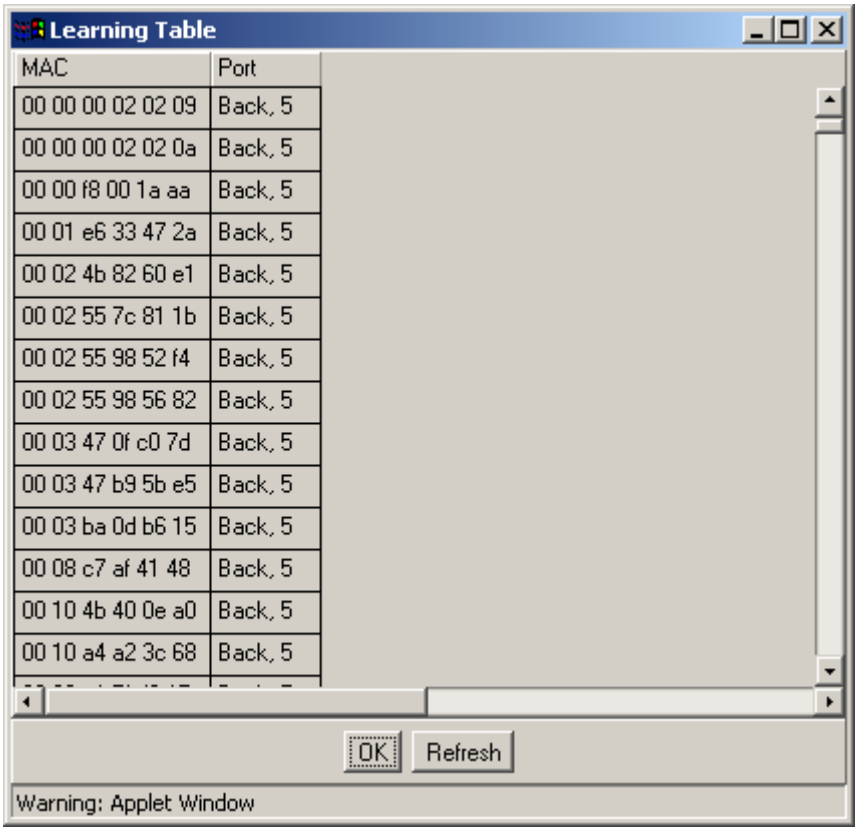


Figure 5-3. FDB Learning Table

The ESB20 automatically generates and updates all the FDB Table information. The table contains two columns:

- **MAC Address.** MAC Address of the ports that have *sent* information to the unit.
- **Ports.** These are the corresponding unit ports that have *received* this information.

STP Status

This window displays STP status and timing parameters. The timing parameters values are configurable via the **Spanning Tree** configuration dialog that is invoked from the switch view **Config** menu.

To display the Spanning Tree Report window

From the switch view **Reports** menu, choose **STP Status.**

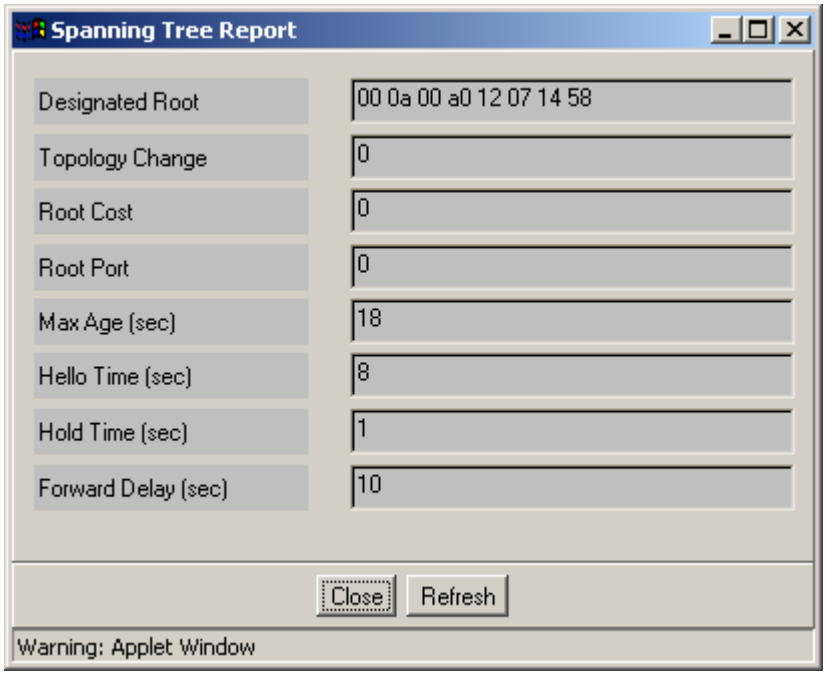


Figure 5-4. Spanning Tree Report

- **Topology Change.** Shows the number of times the Spanning Tree has been reconfigured since the unit was last reset. The “tree” reconfigures itself automatically in response to network changes.
- **Root Cost.** “Cost” of getting from this unit to the designated root. The lower the cost, the more preferred this path.
- **Root Port.** The unit port with the lowest travel “cost” to the designated root.
- **Max Age.** Number of seconds learned Spanning Tree information is kept before being discarded.
- **Hello Time.** Number of seconds between configuration bridge PDU transmissions by the ports of this unit when it is the root of the Spanning Tree or trying to become so.

- **Hold Time.** Number of seconds during which no more than two configuration bridge PDUs are transmitted by the unit.
- **Forward Delay.** Length of time that the unit stays in each of the Listening and Learning states that precede the Forwarding state. In addition, when a topology change has been detected and is underway, this parameter is used to age all dynamic entries in the Forwarding Database.

Ports Status

This window shows the current link status for all the ports and a summary of the port definitions.

To display the Ports Status window

From the switch view **Reports** menu, choose **Ports Status.**

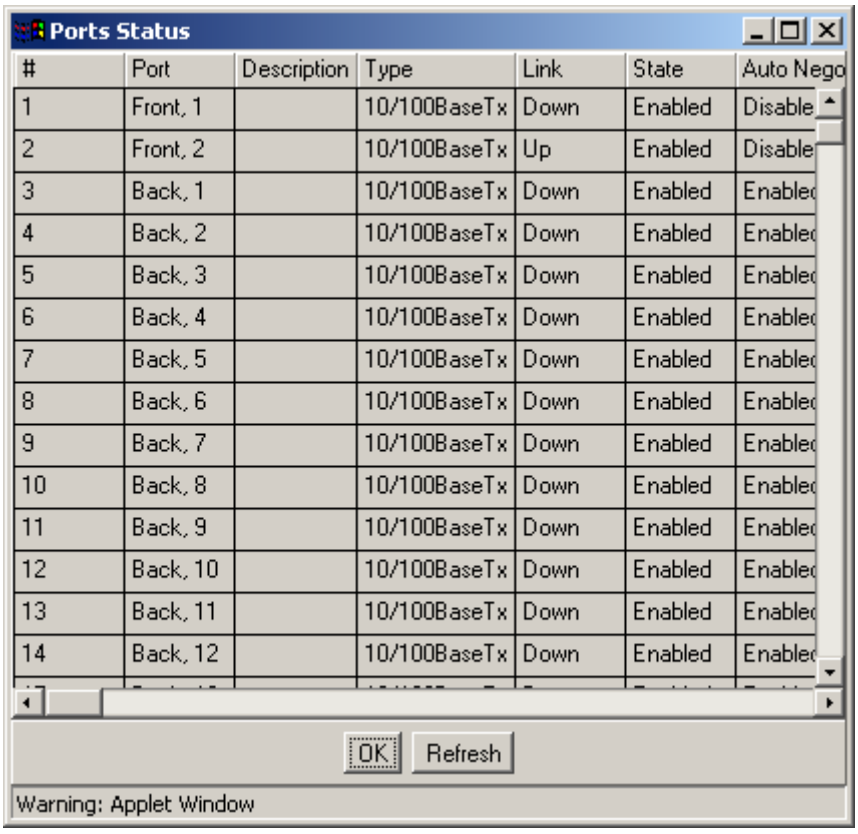


Figure 5-5. Window summarizing the status and definitions of all the ports

Port Counters

This window summarizes various types of data transmitted and received data on each of the unit ports.

To display the Ports Status window

From the switch view **Reports** menu, choose **Ports Status.**

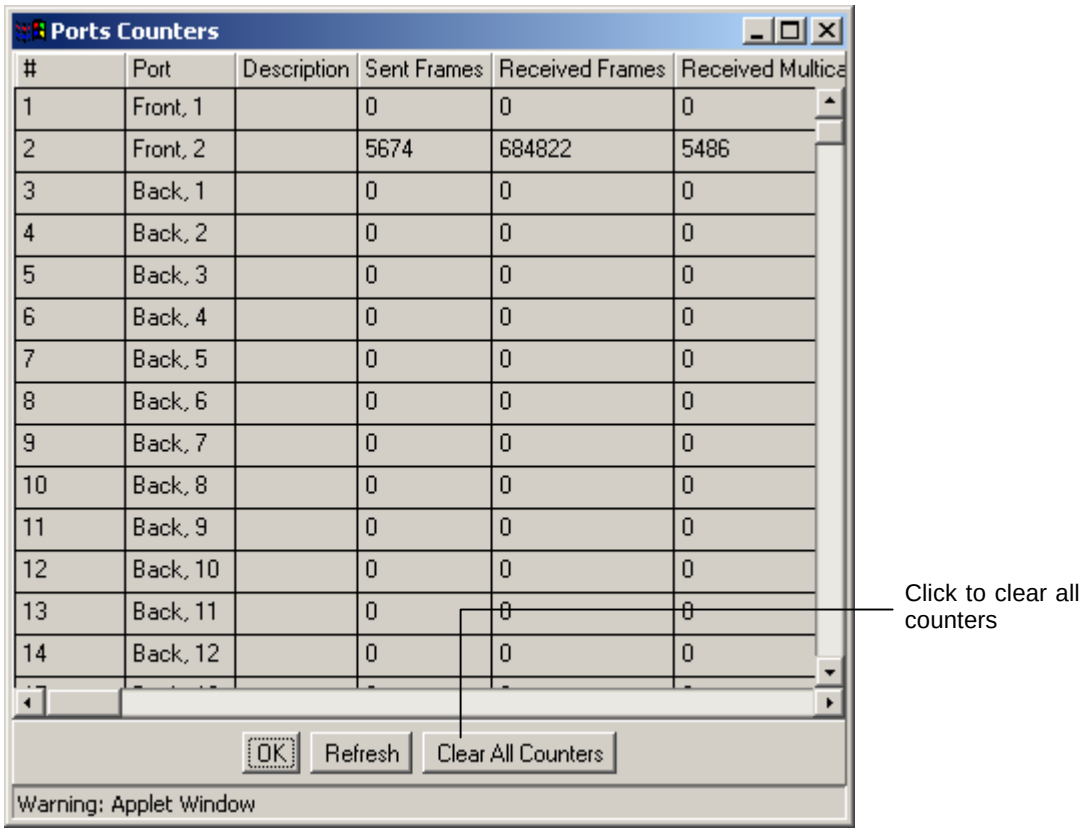


Figure 5-6. Summary of the statistics on all the ports

Trap Log

This window shows the traps sent by this unit and the corresponding information for each trap. This includes time the trap was sent, the severity, and the type of trap.

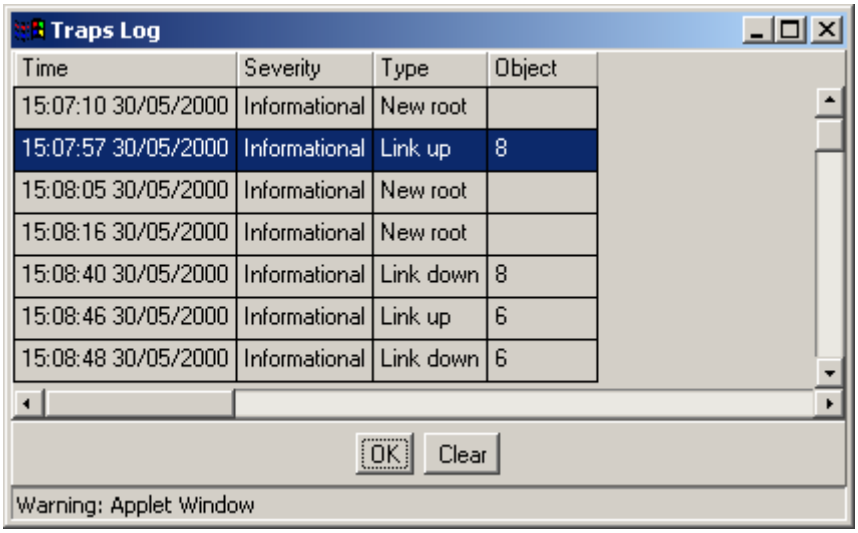


Figure 5-7. Trap Logs

Port Statistics

Detailed statistics accumulated on each port can be displayed separately for each port. For each display, the corresponding graph showing frames, frame size, and total errors can be invoked.

To display statistic of a specific port

In the switch view dialog, right-click on the port of interest and select **Statistics.** The statistics window for that port appears.

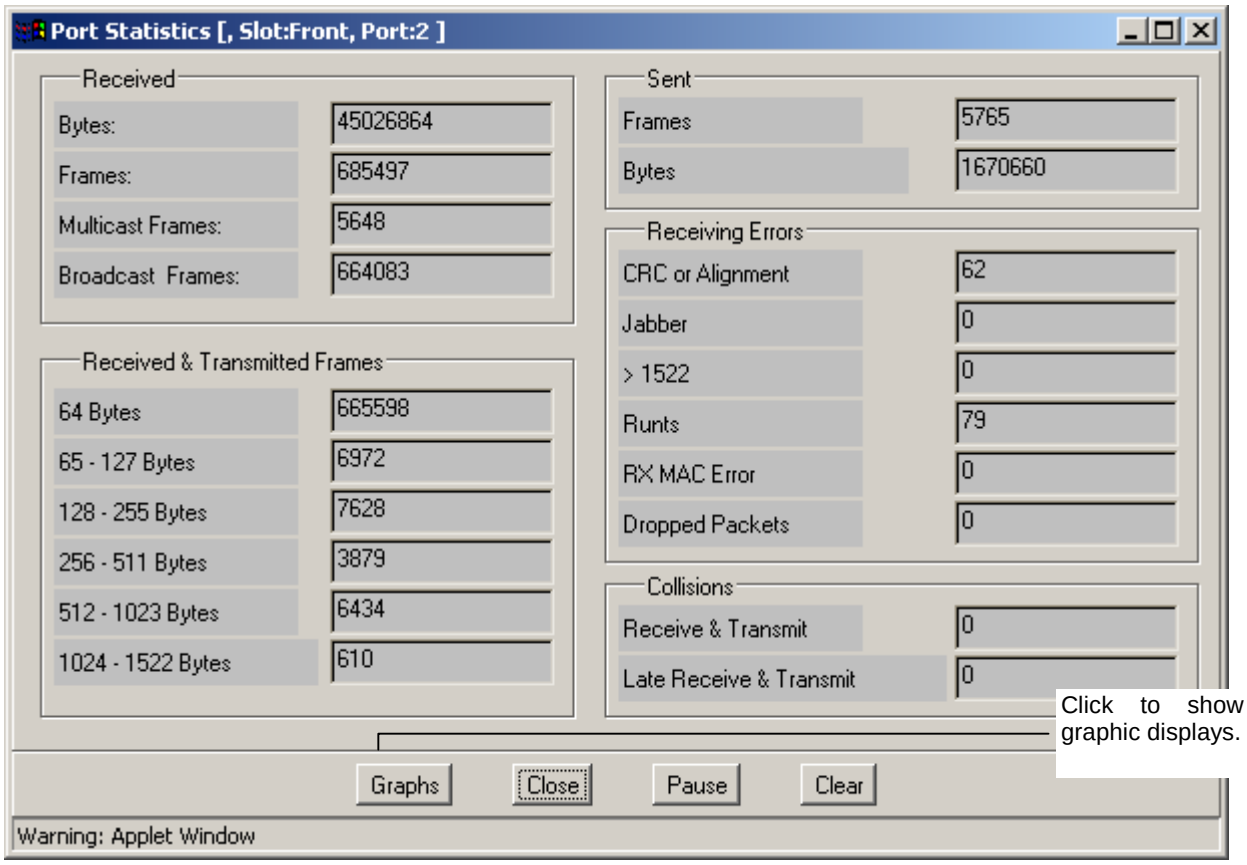


Figure 5-8. Statistics for the selected port of interest

To invoke graphic display

Click on the **Graphs** button to show the graph.

The example illustrated below shows the Frame Size graph, where the **Y-axis** shows the number of frames. You may view the following types of graphs, by double-clicking on the appropriate option: Frames Size, Frames, or Errors. The **Show Delta** option enables you to view only the difference between the last poll.

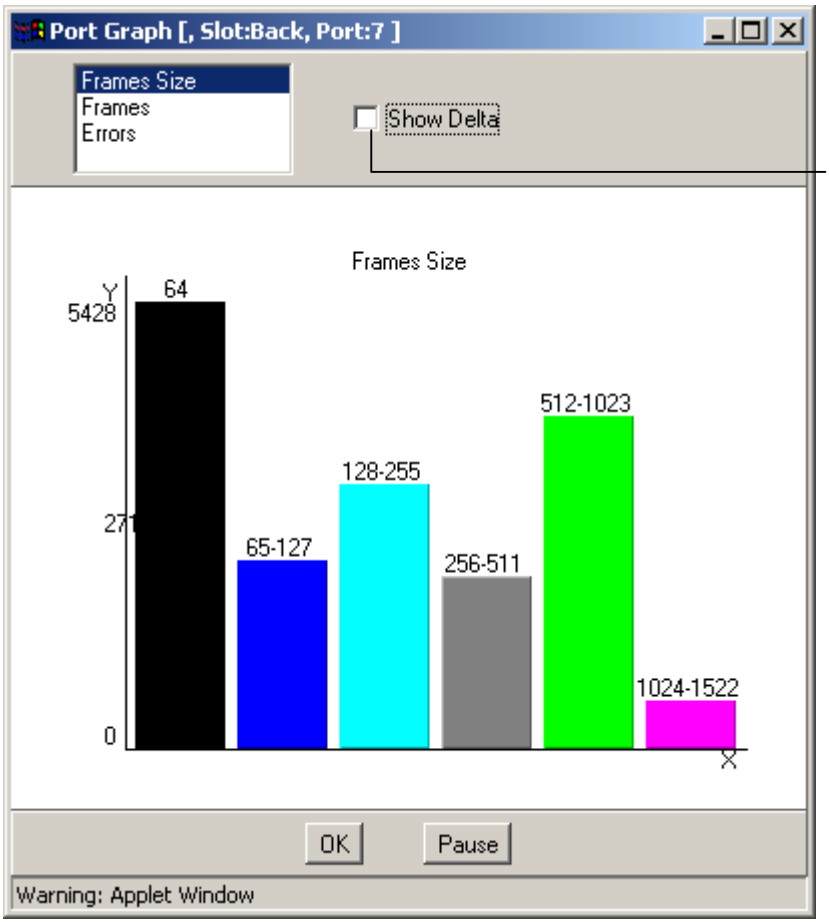


Figure 5-9. Graph showing number of frames of various sizes

Port STP

The Port STP Properties dialog is divided into to separate areas containing the STP *configuration* and *status* parameters for the selected port.

To display STP parameters for a specific port

In the switch view dialog, right-click on the port of interest and select **STP.** The STP window for that port appears.

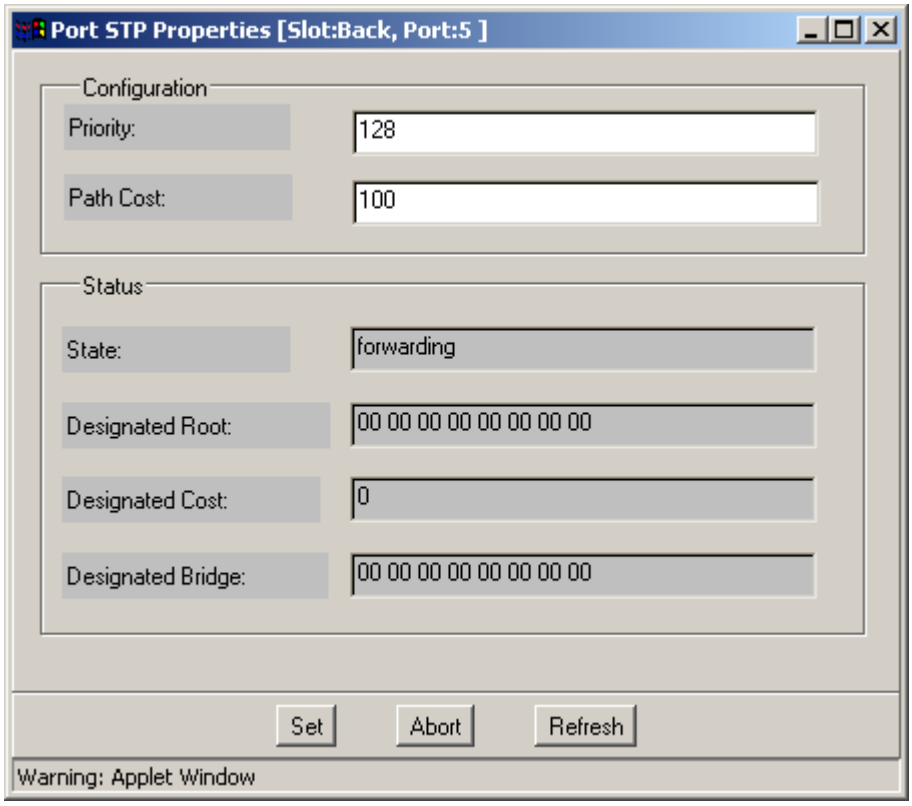


Figure 5-10. Port STP Properties

Chapter 6 Software Update Procedures

Overview

This chapter describes how to update the ESB20 software image and how to transfer configuration parameters to/from the ESB20 Ethernet switch.

In the given instructions the following configuration is assumed that:

A. IP-address of the updated switch = 192.168.0.5.

B. IP Address of the TFTP client PC is on the same subnet as the switch.

The IP-address of the PC must be on the same subnet as the switch; otherwise, TFTP transfer cannot be performed properly (unless there is a router between the subnets directing the IP packets to the correct subnet).

ESB20 has two different Flash memories: one containing the ESB20 operating software (Firmware), and the other containing the Boot code. Only the Firmware may be updated using the instructions given in this chapter. The Boot code Flash is write-protected so that it cannot be mistakenly overwritten during the software upgrade.

Required Equipment for Firmware Upgrade

Upgrade may be performed either using only an Ethernet connection, or using an Ethernet connection and a session.

- ESB20 Unit to be updated
- A PC or laptop on which the following are installed:
  - Ethernet card
  - TFTP-program. Walusoft TFTP client is used in these instructions for example.
  - Telnet program
- One straight through Ethernet cable (RJ-45)
- Software image to be uploaded (provided e.g. on CD-ROM)
- If the upgrade performed via an Ethernet connection and a session, a serial cable with RJ-45 connector in other end is required as well.

-

Software Update via Ethernet Connection

To update the new software image to the unit Flash memory:

1. Connect a PC or Laptop to one of the Ethernet ports of the switch via an Ethernet cable.
2. Insert media (e.g. CD-ROM) containing the new software image version into the PC and copy the software image to your hard disk.
3. Verify that the Ethernet switch is powered up.
4. Start a Telnet session session and connect to the IP-address of the switch. On a Windows system this can be done by entering (**Start → Run → Telnet** *switch IP Addresss i.e.* 192.168.0.5).
5. Login to the switch:
   - Username: **nokia** (by default)
   - Password: **<Press enter>** (by default) or if the password is set, give correct password and then press enter.
6. From the **Main Menu**, select **6. Software Upgrade**. You will be prompted by **Software Upgrade (Y/N)?**.
7. Enter **Y.** The Telnet session should now automatically terminate and the front panel LED should blink in red indicating that the unit is in TFTP mode and is waiting for the new software to be uploaded.

   Note: *If a TFTP call is not received within 10 minutes, or if the unit was booted while waiting for it, it will restart using the last image file.*
8. Start TFTP-program located on the PC.

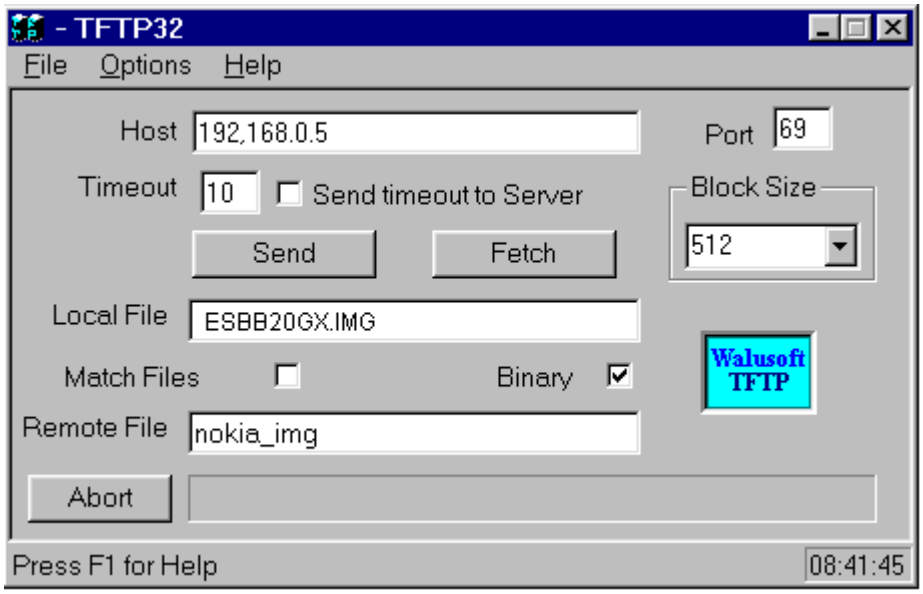


Figure 6-1. TFTP settings for software image transfer on Walusoft TFTP client

9. Set the TFTP according to the following settings:
   - Host IP-address: *IP Address of the switch* e.g. **192.168.0.5**
   - Port: **69**
   - Local filename: **ESBB20GX.img**. *This is the file you copied to the hard drive (filename might differ). You may have to change some path settings of the TFTP-program so the program can find the appropriate file.*
   - Remote file name: ***nokia_img***. *This is the filename to be written to the unit Flash. The destination filename must always be the '**nokia_img**' and the file extension must be extended by using underscore not period. Otherwise the unit will not accept the file and the transfer will be terminated. This is indicated by the error message e.g.* `"MSG from Server >file not writable"` *or similar*
   - Transfer type: **Binary**

   Note: *Some of these settings may not be available on all TFTP-programs. In some TFTP-programs it may be nessessary to change the local filename to **nokia_img** if the remote filename field is not available.*

10. Start the file transfer from TFTP-program by doing one of the following depending on the program:
    - Either click **Send** or,
    - open the **File** menu and choose **Put,** select **binary mode**, type **nokia_img** and press **Enter**.

    The TFTP program should now indicate that software transfer is in progress. If the appropriate response is not displayed, verify that:
    - The settings of the TFTP program are correct.
    - The remote filename is **nokia_img** (note that the file extension is underscore not period).
    - Connection is established to the unit. this is done by using Ping (**Start → Run → ping** *switch IP Addresss i.e.* 192.168.0.5).

When the software is uploaded the switch will begin to program the Flash memories. This will take a while. All the previous SNMP-interface settings will be copied to the new software version. When the programming of the Flashes is completed, the switch will reboot itself automatically to the operating state.

If a problem is encountered during the update phase and the Flash banks are not thoroughly reprogrammed, the unit will automatically reboot to the TFTP state. From this state, the unit may be reprogrammed following the instructions in steps 8 to 10.

Software Update via an Ethernet Connection and a Terminal Session

To transfer the new software image to the unit Flash memory:

1. Connect PC or Laptop to one of the Ethernet ports of the switch by using Ethernet cable.
2. Insert media (e.g. CD-ROM) containing the new software image version to PC and copy the software image to your hard disk.
3. Use a serial cable to connect the service terminal to the switch.
4. Check that the Ethernet switch is powered up
5. Start a terminal session. Service terminal settings are:
   - Bitrate: **9600 bit/s**
   - Parity: **None**
   - Data bits: **8**
   - Stop bits: **1**
   - Flow control: **Xon/Xoff**
6. Login to the switch via the service terminal:
   Username: **nokia** (by default)
   Password: **<Press enter>** (by default) or if the password is set, give correct password and then press enter.
7. Select **Software Upgrade** from main menu by pressing number **6** and entering **Y** in response to the prompt **Software Upgrade (Y/N)**?
8. The boot procedure should now be printed on the service terminal screen. Upon the completion of the boot procedure, a message indicating that the unit is waiting for the external TFTP load should be displayed. Also, the front panel LED should blink in red indicating that the unit is in TFTP mode and waiting for the new software to be uploaded.

   Note: *If after 10 minutes the unit does not receive a TFTP call, or if the unit was booted while waiting for a TFTP call, it will restart using the last image file.*
9. Start TFTP-program located on the PC.

   Note: T*FTP-program is not included to all Windows operating systems thus it might have to be installed separately prior to use.*

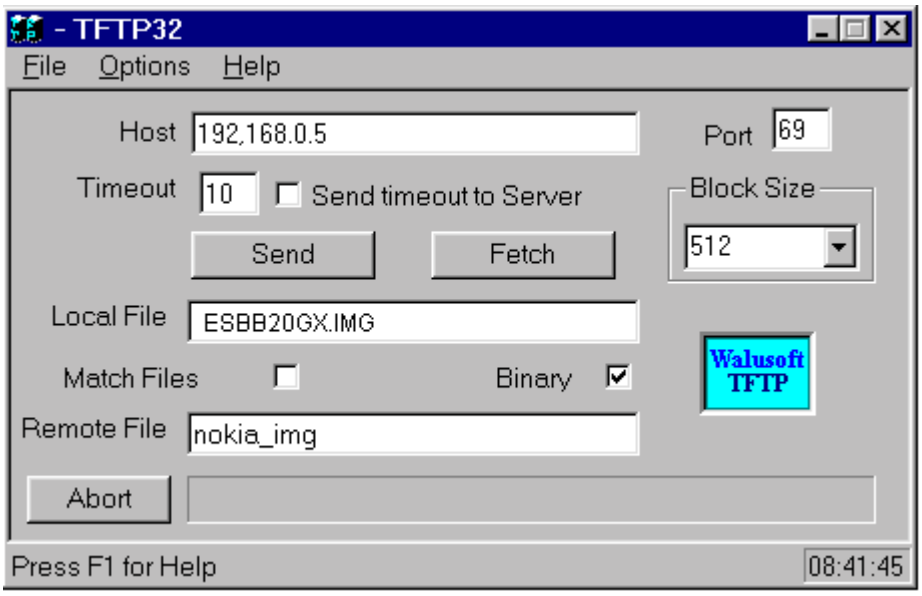


Figure 6-2. TFTP settings for software image transfer on Walusoft TFTP client

10. Set the TFTP-program according to the following settings:
    - Host IP-address: IP Address of the switch e.g. **192.168.0.5**
    - Port: **69**
    - Local filename: e.g. ESBB20GX.img . *This is the file you copied to the hard drive (filename might differ). You may have to change some path settings of the TFTP-program so the program can find the appropriate file.*
    - Remote file name: **nokia_img** . *This is the filename to be written to the unit Flash. The destination filename must always be the '**nokia_img**' and the file extension must be extended by using underscore not period. Otherwise the unit will not accept the file and the transfer will be terminated. This is indicated by the error message e.g. "MSG from Server >file not writable" or similar.*
    - Transfer type: **Binary**

***Note:** Some of these settings may not be available on all TFTP-programs. In some TFTP-programs it may be nessessary to change the local filename to **nokia_img** if the remote filename field is not available.*

11. Start the file transfer from TFTP-program by doing one of the following depending on the program:
    - Either click **Send** or,
    - open the **File** menu and choose **Put,** select **binary mode**, type **nokia_img** and press **Enter**.

    Information on the update procedure should now be printed on the Service Terminal. The procedure is as follows:

- New image is transferred to the DRAM of the switch
- flash bank 1 is erased
- flash bank 2 is erased
- flash bank 1 is reprogrammed
- flash bank 2 is reprogrammed
- unit is booted up.

The TFTP program should also indicate that the software transfer is in progress. If nothing happends check the connection to the switch by using PING (**Start → Run → ping** *switch IP Addresss i.e.* 192.168.0.5).

If the connection is working, the PING should indicate this by printing corresponding reply-messages to the screen. Check also that the settings of the TFTP program are correct and the remote filename is nokia_img (note that the file extension is underscore not period).

All the previous SNMP-interface settings will be copied to the new software version. When the programming of the Flashes is completed the switch will reboot itself automatically to the operating state.

If a problem detected during the update phase and the Flash banks are not thoroughly reprogrammed, the unit will automatically reboot to the TFTP state. From this state the programming can be retried by following instructions 9 - 11.

Update Procedure Using Linux OS

Note: *TFTP-clients might differ from following procedure depending on Linux distribution.*

1. Connect a PC or Laptop with Linux operating system to one of the Ethernet ports of the switch using Ethernet cable.Insert the floppy-disk or CD-ROM containing the new software image version to the PC and copy the software image to your hard disk. It is recommended to copy the image to the TFTP-client's default directory. Otherwise the TFTP-client may not find the image.
2. Verify that the Ethernet switch is powered up.
3. Start a Telnet session and connect to the IP-address of the switch (e.g 192.168.0.5). On Linux this can be done from terminal console by writing telnet 192.168.0.5.
4. Login to the switch by entering:

   Username: **nokia**

   Password: <Press enter or if the password is set, give correct password and then press enter>
5. Check the current software version and date from upper part of the main menu to avoid unnecessary update procedure.

6. Select the 'Software Upgrade' from main menu by pressing number **6** and answer **Y** <enter> to the question "Software Upgrade (Y/N)?"
7. Now the telnet session shoud be automatically terminated and the front panel LED should blink on red. This indicates that the unit is on TFTP mode and is waiting for the new software to be uploaded.

Note: *If after 10 minutes the unit does not receive a TFTP call, or if the unit was booted while waiting for a TFTP call, it will restart using the last image file.*

8. Start TFTP-program located on the Linux by entering the command **tftp** at the prompt. The `tftp>` prompt indictes that the tftp program is enabled.
9. Connect to the switch to be updated by typing the command: **tftp> connect 192.168.0.5**.
10. Set the binary transfer mode by typing the following command at the prompt: `tftp>` **`mode binary`** `transfer mode set to I`
11. Send the new software image to switch to be updated by using command **put** and give local file name and remote file name. For example if the local file "ESBB20GX.img" is stored to directory /usr/root/ use following commands:

    tftp> **put**

    (local-file):/usr/root/ESBB20GX.img

    (remote-file):**nokia_img**

    If software transfer does not begin at this point, check the connection to the switch using the **ping** command (**ping 192.168.0.5)** at the command prompt.

    If the connection is working, the PING should indicate this by printing corresponding Reply-messages to the screen. Check also that the settings of the TFTP program are correct and the remote filename is **nokia_img** (note that the file extension is underscore not period).

    When the sotware is uploaded the switch will begin to program the Flash memories. This will take a while. All the previous SNMP-interface settings will be copied to the new software version. When the programming of the Flashes is completed, the switch will reboot itself automatically to the operating state.

    If something goes wrong during the update phase and the Flash banks are not thoroughly reprogrammed, the unit will automatically reboot to the TFTP state. From this state the programming can be retried by following the instructions 8 - 12.

SubMenu

Chapter 7 Troubleshooting

This chapter presents common problems and describes their solutions. The problems begin with a **P**, and the solutions begin with an **S**.

P: The Terminal Interface main menu does not appear.

S: Verify that the terminal is set to 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

P: The Web Management application switch view does not appear on the management station.

S1: It may take several seconds for the program to load from the device. If after a reasonable time has elapsed the window still has not appeared, verify that the management station is set up properly, and that the basic IP Parameters are set properly.

Ping the unit to verify that connection can be established (**Start → Run → ping** *switch IP Addresss i.e.* 192.168.0.5).

P: Web Management switch view appears, but I can't view a device.

S: Verify that the device community names are properly set.

P: My password is not working.

S: Remember that there are two passwords; one to access switch view and one to change parameters. If you have forgotten the password, please contact Nokia repair services.

P: A port is not working.

S: Check that:

- The port is not disabled.
- Cabling is correct. Cross connect cable between two ESB20s, Hubs, switches or routers. Straight through cable between CPU units, PCs, NICs etc.
- PING to verify the connection (**Start → Run → ping** *switch IP Addresss i.e.* 192.168.0.5).
- Serially connect to the Terminal Interface application on the unit, and from the **Main Menu** select **Port Status.** A table showing the switch ports and their status will appear.

P: The Network Management Station is not receiving traps.

S: Verify that the Manager IP Address is properly set.
Traps notification must be enabled from ESB20. SNMP Agent Configuration via Web Management (enable **Send Alert Traps).**

P: I messed up the configuration.

S: Reload the default factory values using either the configuration terminal or the Web Management application and then restart the switch.

P: The Port Properties window for my port is different than I expected.

S: The Port Properties window contains different parameters and buttons depending on the communication speed supported by the port.