Web Interface

Security Network Access Port Security

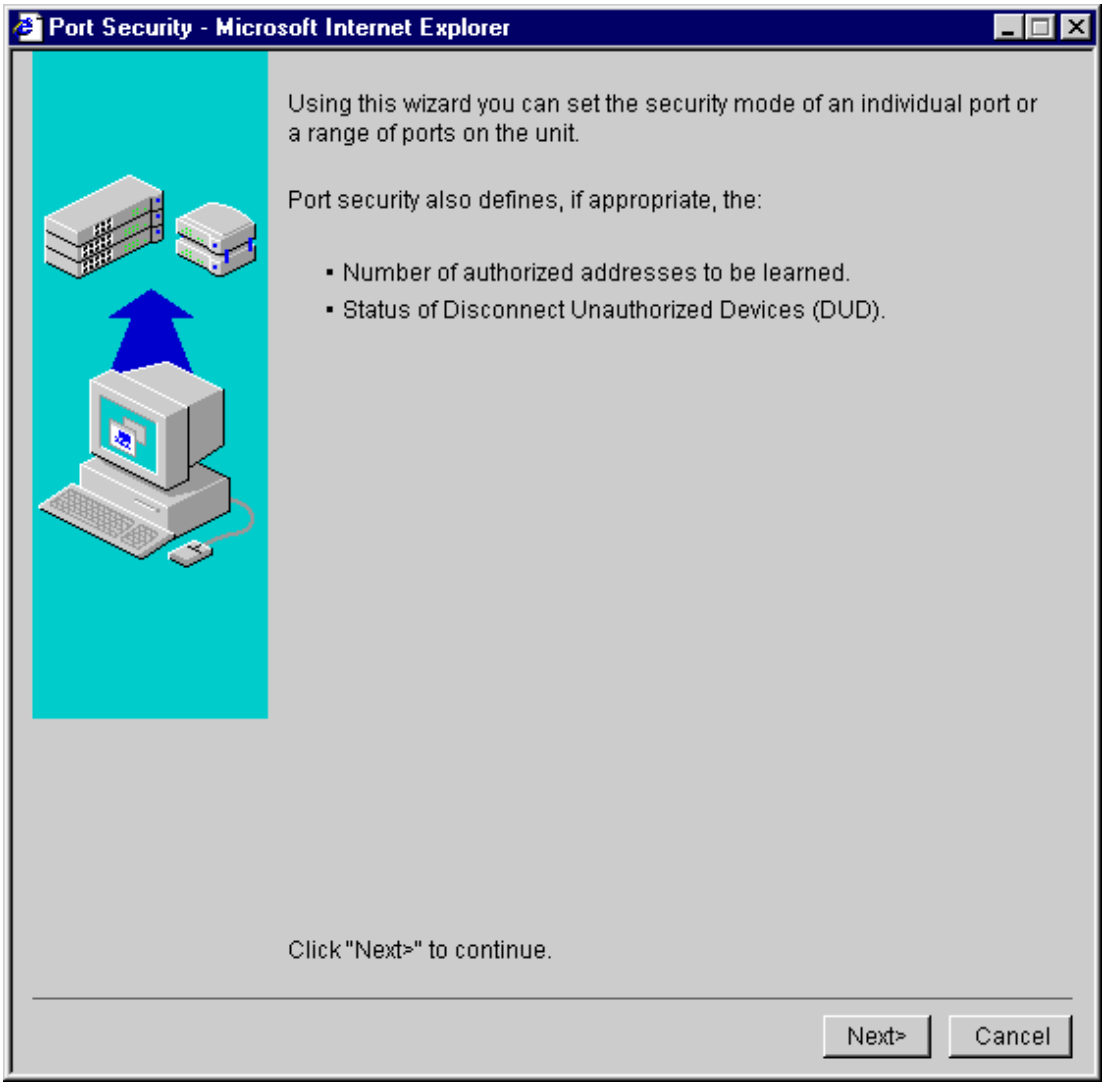
Back
Contents
Search

Enabling and Disabling Port Security

You can enable and disable security and set the mode of operation on a port using the Port Security wizard.

To access the wizard:

1. Click *Device View* on the Toolbar.
2. Select **Security -> Network -> Access -> Port Security** in the Navigation Tree. The first Port Security page is displayed.



As you go through the wizard, you need to:

1. Enter the port number(s), range or label(s) on which you wish to enable or disable port security.
2. Choose a security mode for the ports that you have selected:
   - **No Security** (default)
     Port security is disabled and all network traffic is forwarded through the port without any restrictions.

- **Continuous Learning**
  MAC addresses are learned continuously by the port until the number of authorised addresses specified is reached. When this number is exceeded the first address that was learned by the port is deleted, allowing a new address to be learned.

- **Automatic Learning**
  MAC addresses are learned continuously by the port until the number of authorised addresses specified is reached. When this number is exceeded the port automatically stops learning addresses and Disconnect Unauthorized Device (DUD) is enabled on the port

If you select **No Security**, the final Port Security page is displayed. Click the *Finish* button to assign the security configuration to the selected port(s).

If you select **Continuous Learning** or **Automatic Learning**, the next Port Security page is displayed. Go to Step 3.

3. Enter the number of authorised addresses you wish to have for the port(s).

   This value must be between 0 and 4.

4. If you selected **Automatic Learning**, in step 2, select whether you wish to enable or disable Disconnect Unauthorized Devices (DUD).

Related Operations

Port Setup SummaryDisplaying Ethernet Port Summary Information

---

Back to Top

Bridge Link Aggregation Modify Admin State

Modifying the Administrative State of an Aggregated Link

Aggregated links are connections that allow devices to communicate using up to four links in parallel. Aggregated links provide two benefits:

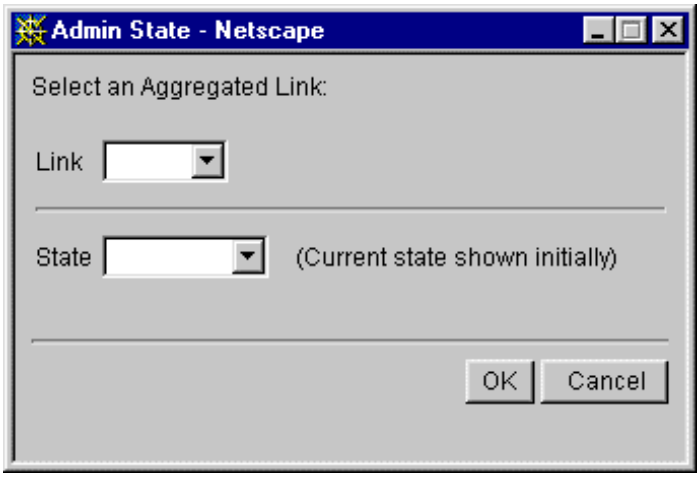
- They can potentially double, treble or quadruple the bandwidth of a connection.
- They can provide redundancy — if one link is broken, the other link shares the traffic for that link.

You can modify the administrative state of an aggregated link using the Admin State window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Link Aggregation -> Modify -> Admin State** in the Navigation Tree.

   The Admin State window is displayed.



The Admin State window contains the following elements:

Link
Allows you to select the aggregated link to modify.

State *Disabled / Enabled*
Allows you to modify the state of the aggregated link.

The current state of the link is intially displayed in the State *listbox.*

Related Operations

Add Port	Setting Up Aggregated Links
Partner ID	Setting or Modifying the Partner ID for an Aggregated Link

LACP State	Enabling or Disabling LACP on a Port
Remove Port	Removing a Port from an Aggregated Link

Back to Top

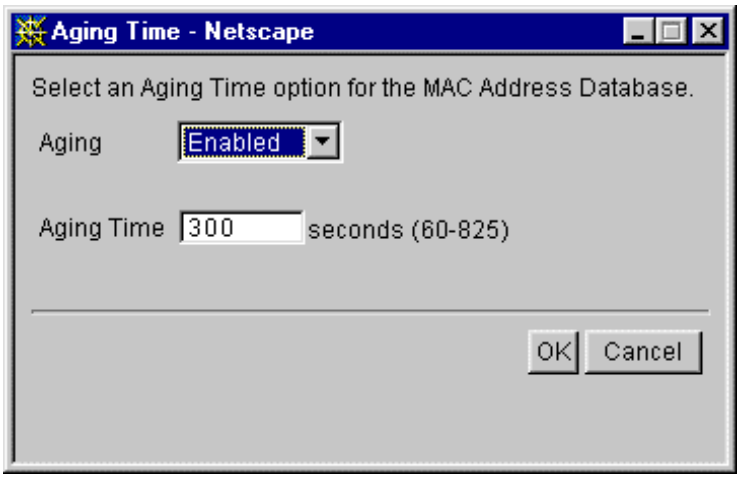
Bridge Address Database Aging Time

Enabling and Disabling Aging Time

You can enable or disable aging time for the Address Database using the Aging Time window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Address Database-> Aging Time** in the Navigation Tree.
3. The Aging Time window is displayed.



The Aging Time window contains the following elements:

Aging *Enabled / Disabled*
Allows you to specify if aging time is enabled or disabled for the Address Database.

Aging Time (seconds) 60-825
Allows you to specify the aging time (in seconds) for all learned entries in the Address Database of the unit; the default time is 300 s (5 min).

Related Operations

Add	Adding a MAC Address
Find	Finding a MAC Address
Remove	Removing a MAC Address
Summary	Displaying Summary Information for MAC Addresses



Back to Top

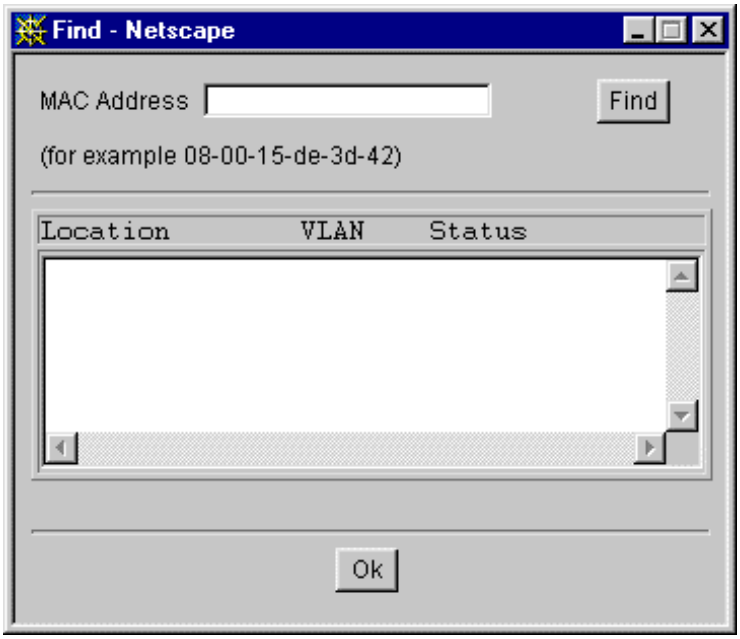
Bridge Address Database Find

Finding a MAC Address

You can find a MAC address within the Address Database using the Find window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Address Database -> Find** in the Navigation Tree.
3. The Find window is displayed.



The Find window contains the following elements:

MAC Address
The address must be entered in the form of hyphen separated bytes, for example 08-00-15-de-3d-42.

Click *Find*.

Location / VLAN / Status
All occurrences of the address within the Address Database and the unit and port number associated with each one are displayed. The VLAN number and status of each occurrence is also shown.

If the address that you have entered is not found in the Address Database then No matches found *is displayed.*

Related Operations

Add	Adding a MAC Address

AgingTime	Enabling and Disabling Aging Time
Remove	Removing a MAC Address
Summary	Displaying Summary Information for MAC Addresses


Back to Top

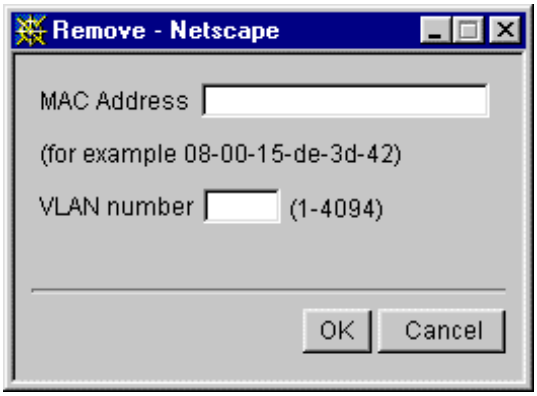
Bridge Address Database Remove

Removing a MAC Address

You can remove a MAC address from the Address Database using the Remove window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Address Database-> Remove** in the Navigation Tree.
3. The Remove window is displayed.



The Remove window contains the following elements:

MAC Address
Allows you to enter the MAC address that you wish to remove. The address must be entered in the form of hyphen separated bytes, for example 08-00-15-de-3d-42.

VLAN number
Allows you to enter the VLAN number for the address that you wish to remove.

The error message No matches found *is displayed if the address that you have entered is not found in the Address Database.*

Related Operations

Add	Adding a MAC Address
AgingTime	Enabling and Disabling Aging Time
Find	Finding a MAC Address
Summary	Displaying Summary Information for MAC Addresses



Back to Top

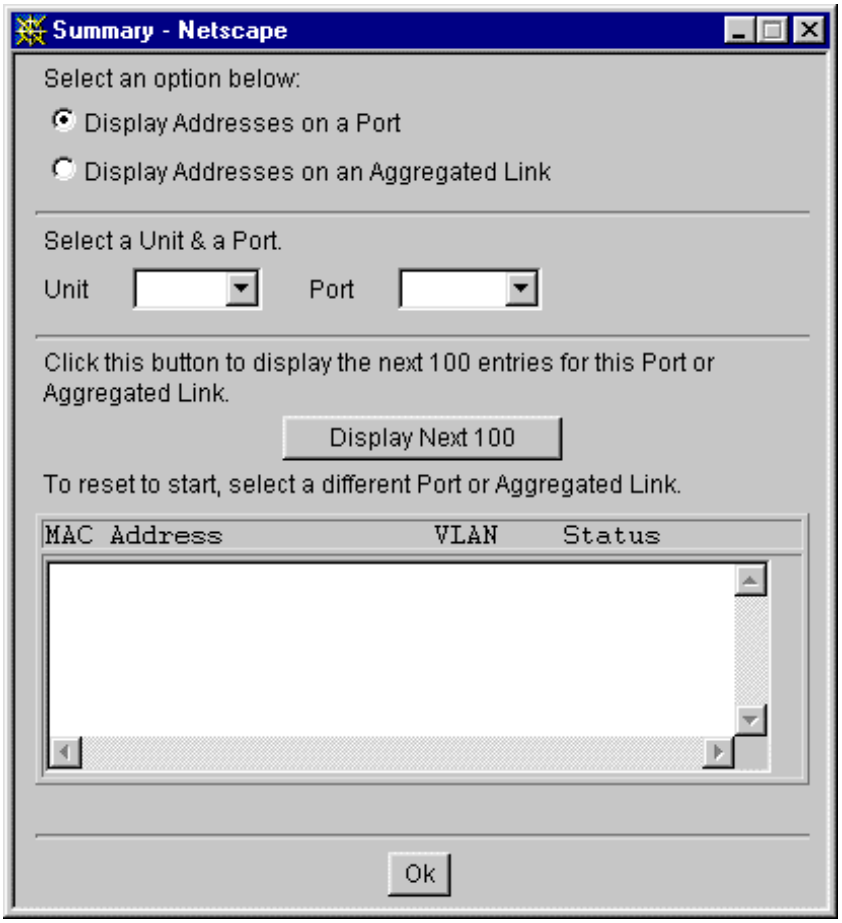
Bridge Address Database Summary

Displaying Summary Information for MAC Addresses

You can display summary information about all MAC addresses that are stored against a particular port or aggregated link in the Address Database using the Summary window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Address Database-> Summary** in the Navigation Tree.
3. The Summary window is displayed.



To display the summary information for an address from the Address Database:

1. From the *Select an option below:* radio buttons, select if the address is to be displayed against a port or an aggregated link.

   If you select *Display Addresses on a Port*, you are prompted to select a unit and a port from the *Unit and Port* listboxes.

   If you select *Display Addresses on an Aggregated Link*, you are prompted to select an aggregated link from the *Link* listbox.

2. Click *Display Next 100*. The Address Database is searched for MAC addresses associated with the port or aggregated link that you have selected. Up to 100 MAC addresses and their VLAN number and status is displayed.

3. If there are more than 100 addresses for the port or aggregated Link, click *Display Next 100* again to display the next set of up to 100 addresses.

 *If the address that you have entered is not found in the Address Database then* No matches found *is displayed.*

 *To reset the list of addresses that is displayed, select a different port or aggregated link and click* Display Next 100 *again.*

Related Operations

Add	Adding a MAC Address
AgingTime	Enabling and Disabling Aging Time
Find	Finding a MAC Address
Remove	Removing a MAC Address

Back to Top

System Management Alert Create

Setting Up an Alert

You can configure the unit to send alerts via email or pager notification if certain events occur.

The events that can generate email or pager notification are:

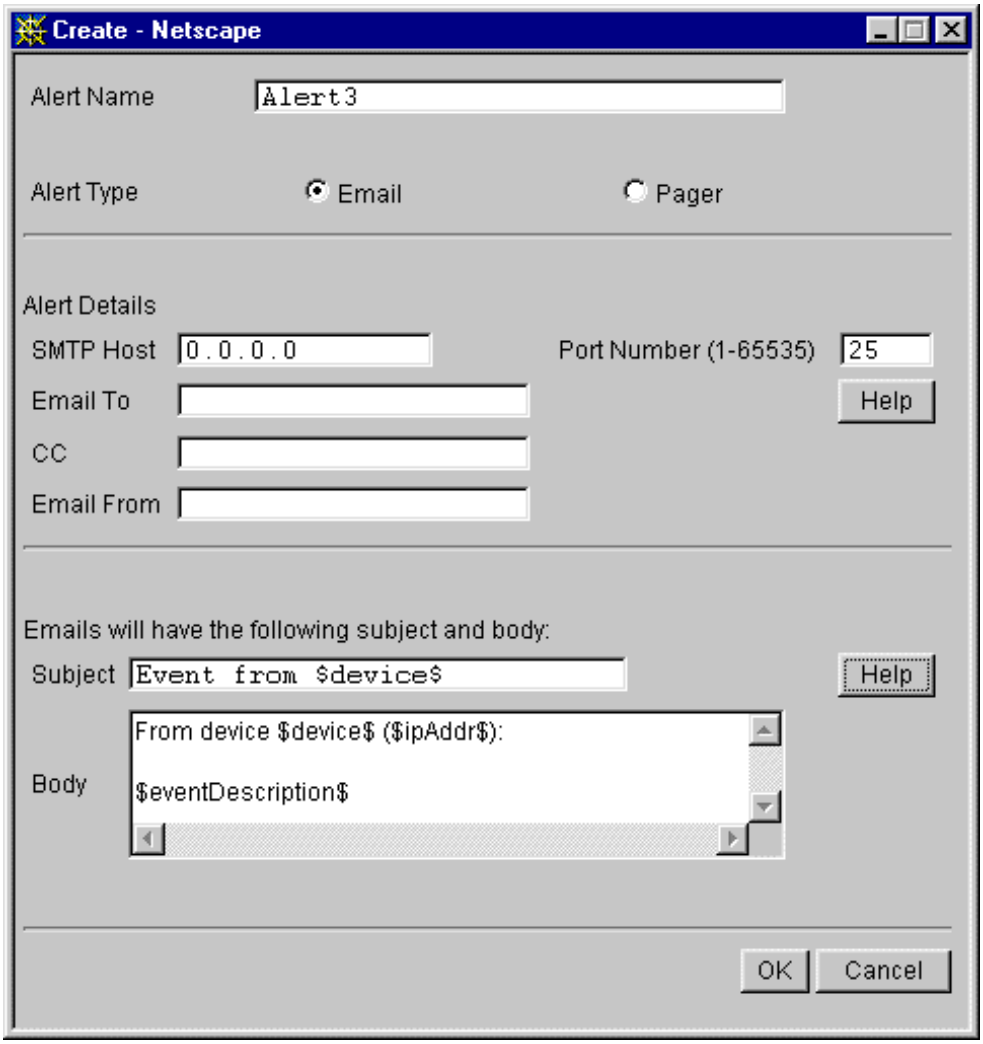
- Unit powers up
- A link fails or returns to service — you can select specific links that you wish to receive messages for, for example, a mission-critical link to a server
- A security violation occurs

You can set up alerts using the Create windows.

To access the windows to set up an alert:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Alert -> Create** in the Navigation Tree.

   The first Create window is displayed.



3. Enter a suitable Alert Name.
4. Click the Alert Type button that you wish to create: email or pager.
5. Enter the Alert Details that you wish to set up. You need to enter the SMTP host IP Address and the port number, EMail To and Email From. The CC list is optional and is not applicable if setting up a pager alert. If no Email To field is entered, the alert feature is disabled.

   The subject and body content of the email notification is not user-configurable.
6. Click *OK*.

Related Operations

Modify	Modifying an Alert
Test	Sending a Test Alert
Delete	Deleting an Alert
Summary	Displaying Summary Information for Alerts

Back to Top

System Management Alert Delete

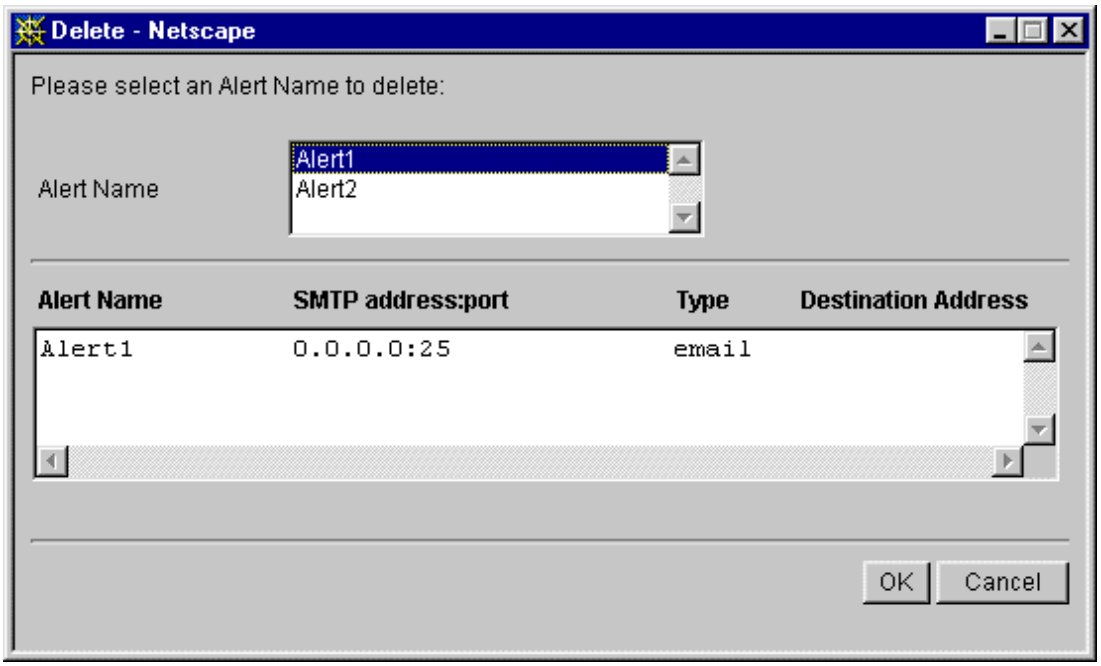
Deleting an Alert

You can delete an alert for the unit using the Delete window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Alert -> Delete** in the Navigation Tree.

   The Delete window is displayed.



3. Select the alert name that you wish to delete.
4. Click *OK*.

Related Operations

Create	Creating an Alert
Modify	Modifying an Alert
Test	Sending a Test Alert
Summary	Displaying Summary Information for Alerts

Back to Top

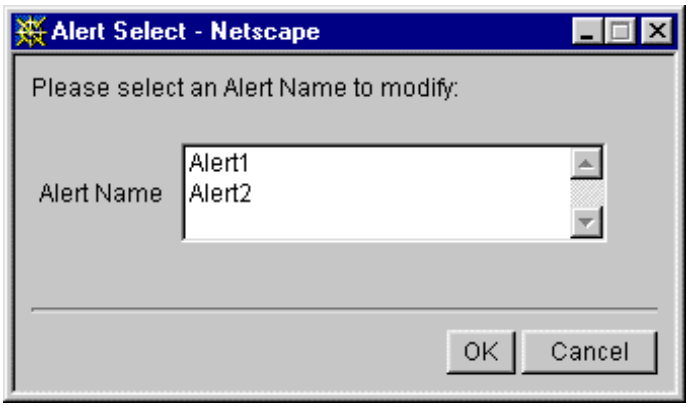
System Management Alert Modify

Modifying an Alert

You can modify an alert for the unit using the Modify pages.

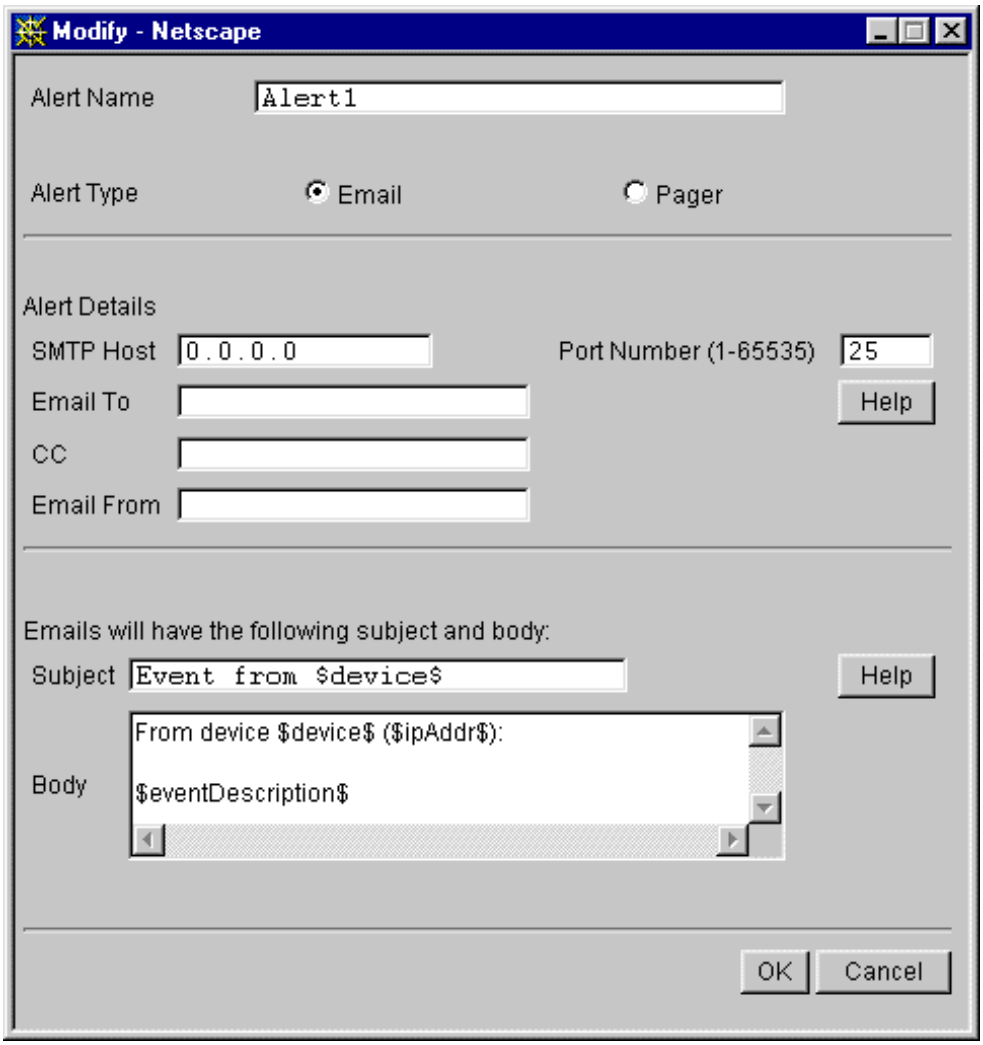
To access the pages:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Alert -> Modify** in the Navigation Tree.
3. The Alert Select page is displayed.



   Select the alert name that you wish to modify and click *OK*.

4. The Modify page is displayed.



5. Enter the new details for the alert that you wish to modify.

   The subject and body content of the email notification is not user-configurable.

6. Click *OK*.

Related Operations

Create	Creating an Alert
Test	Sending a Test Alert
Delete	Deleting an Alert
Summary	Displaying Summary Information for Alerts

Back to Top

System Management Alert Summary

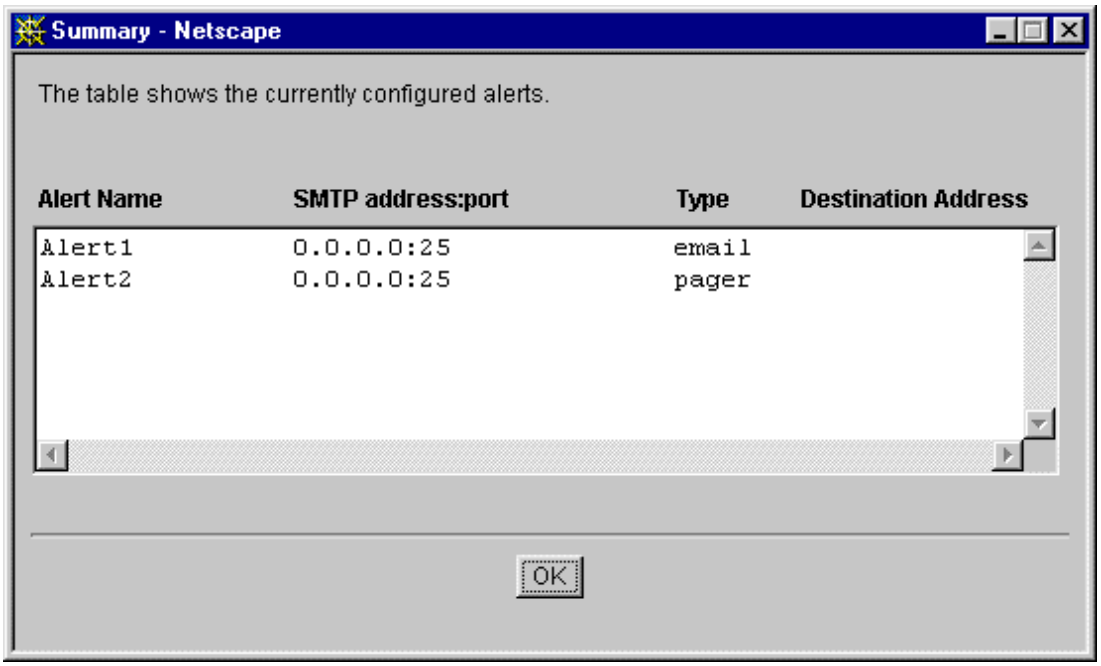
Displaying Alert Summary Information

You can display summary information for all alerts defined for the unit using the Summary window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Alert -> Summary** in the Navigation Tree.

   The Summary window is displayed.



3. Click *OK*.

Related Operations

Create	Creating an Alert
Modify	Modifying an Alert
Test	Sending a Test Alert
Delete	Deleting an Alert

Back to Top

System Management Alert Test

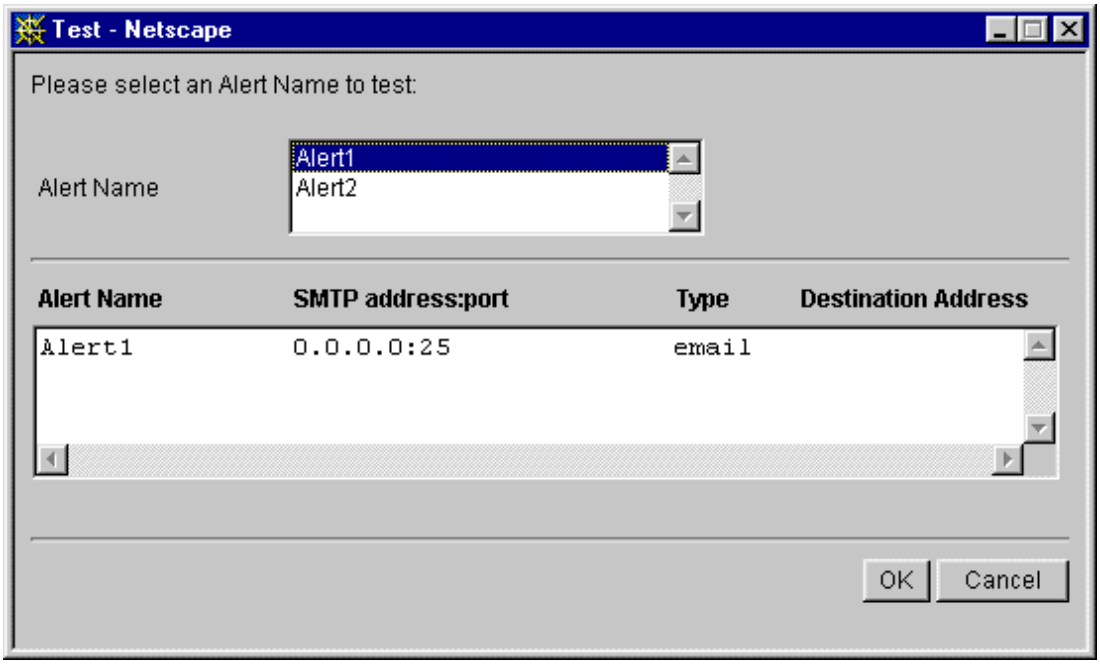
Sending a Test Alert

You can send a test alert for the unit using the Test window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Alert -> Test** in the Navigation Tree.

   The Test window is displayed.



3. Select the alert name for which you wish to send a test alert.
4. Click *OK*.

Related Operations

Create	Creating an Alert
Modify	Modifying an Alert
Delete	Deleting an Alert
Summary	Displaying Summary Information for Alerts

Back to Top

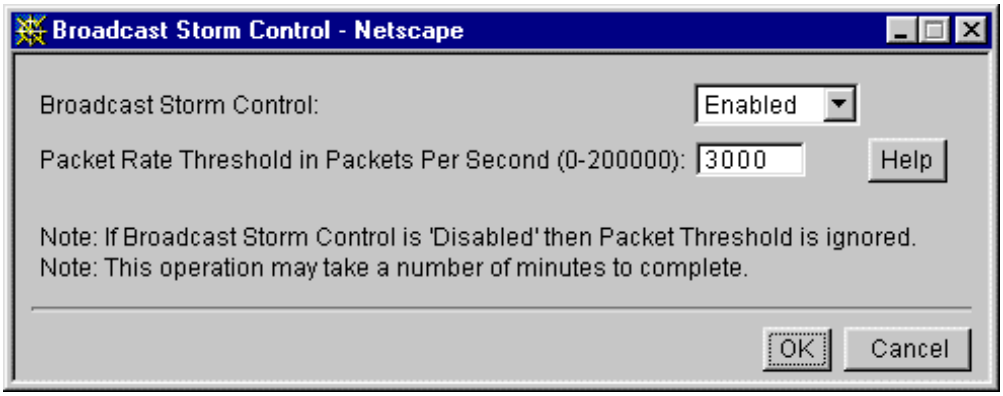
Bridge Broadcast Storm Control Setup

Configuring Broadcast Storm Control

You can enable or disable Broadcast Storm Control using the Setup window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Broadcast Storm Control -> Setup** in the Navigation Tree.
3. The Setup window is displayed.



The Setup window contains the following elements:

Broadcast Storm Control: *Enabled / Disabled*
Allows you to specify whether the unit uses Broadcast Storm Control. This is a system that monitors the level of broadcast traffic on that port. If the broadcast traffic level rises to a pre-defined number of frames per second (threshold), the broadcast traffic on the port is blocked until the broadcast traffic level drops below the threshold. This system prevents the overwhelming broadcast traffic that can result from network equipment which is faulty or configured incorrectly.
Packet Rate Threshold in Packets Per Second (0-200000): *3000*
Allows you to enter the value for the packet rate threshold in packets per second.

If Broadcast Storm Control *is set to disabled, the value that is entered in the* Packet Rate Threshold in Packets Per Second *field is ignored.*

Back to Top

System Console Setup

Configuring the Console Port

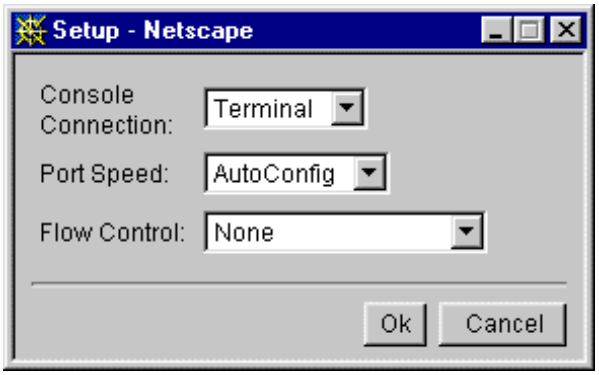
By default, the console port is configured for direct connection to a terminal. You only need to change this configuration if you are connecting a modem to the port. You can configure the console port of the Switch using the Setup window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Console -> Setup** in the Navigation Tree;

   or

   Click the console port on the Switch graphic and select *Setup*.
3. The Setup window is displayed.



The Port Operations - Console Port window contains the following elements:

Console Connection *Terminal / Modem*
Allows you to specify the device that you are connecting to the console port.

Port Speed *AutoConfig / 1200 / 2400 / 4800 / 9600 / 19200*
Allows you to specify the line speed (baud) of the console port. If you select *AutoConfig*, the line speed of the port is automatically set to the line speed of the terminal or modem.

For the Port Speed AutoConfig setting to work, you need to reset the Switch.

Flow Control *None / Hardware RTS/CTS*
Allows you to specify the serial line flow control option suitable for your terminal or modem. See the documentation accompanying your terminal or modem if you are unsure of the correct setting.



Back to Top









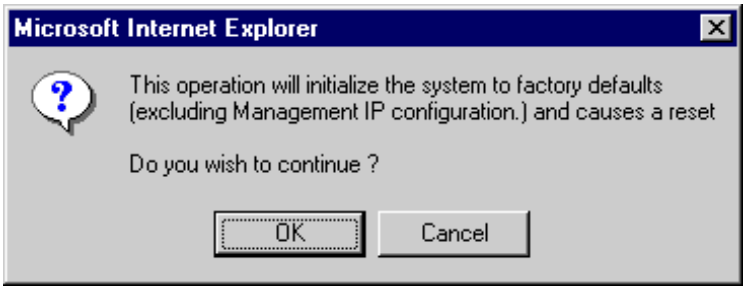
System Control Initialize

Initializing the Unit

You can initialize the Switch using the Initialize window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Control -> Initialize** in the Navigation Tree.
3. The following window is displayed.



4. To initialize the unit, select *OK*.



If the Switch is in a stack with other 4200 series switches the Initialise command will reset the whole stack.

What Happens During Initialization?

Initializing the Switch or stack returns it to its default (factory) settings. The only information that does not return to its default setting is the IP and SLIP information, which is retained to ensure that you can continue managing the unit. You may want to initialize the unit or stack if it has previously been used in a different part of your network, and its settings are incorrect for the new environment.



CAUTION: *Use great care when initializing the unit or stack . It removes all configuration information, including password and security information.*



CAUTION: *When initializing the unit or stack, network loops may occur if you have set up port trunks, VLANs, or the Spanning Tree Protocol. Before initializing the unit, ensure you have disconnected the cabling for all standby or duplicate links.*



The unit takes about 10 seconds to initialize. While the unit is initializing, you cannot communicate with it.

Related Operations

Reboot	Rebooting the Unit
Software Upgrade	Upgrading Management Software


Back to Top

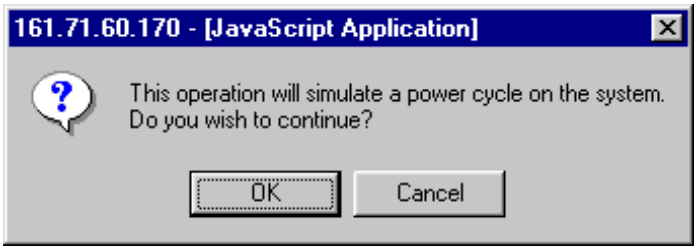
System Control Reboot

Rebooting the Unit

You can reboot the Switch using the Reboot window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Control -> Reboot** in the Navigation Tree.
3. The following window is displayed.



4. To reboot the unit, click *OK*.

If the Switch is in a stack with other 4200 series switches the Reboot command will reboot the whole stack.

What Happens During a Reboot?

Rebooting the Switch simulates a power cycle. You may want to do this if you need to:

- Remove all the learned entries in the Switch Database (SDB).
- Reset the statistic counters on the unit.

CAUTION: *Rebooting the* unit *causes some of the traffic being transmitted over the network to be lost. It also clears all Learned entries from the Switch Database.*

The unit *takes about 10 s to reboot. While the* unit *is rebooting, you cannot communicate with it.*

Related Operations

Initialize	Initializing the Unit
Software Upgrade	Upgrading Management Software



Back to Top









System Control Software Upgrade

Upgrading Management Software

You can upgrade the management software on the Switch using the `softwareUpgrade` command on the Control menu.

Use the method outlined below to upgrade the management software on the Switch, using the Windows 3Com TFTP Server.

Preparing for the Software Upgrade

- Before you begin
- Preparing the management software file
- Setting up your TFTP Server
- Configuring the Switch and TFTP Server IP information

Performing the Software Upgrade

- Performing a TFTP upgrade via the Web Interface

Before you begin

- The 3Com TFTP Server is a Microsoft Windows-only TFTP application. If you are using another operating system (for example Macintosh or Unix), you will require a different TFTP Server application, please refer to the instructions that accompanied your system for further information.
- The management software cannot be upgraded out-of-band over RS232 using the TFTP protocol, because TFTP is not supported over the console port.
- The management software cannot be upgraded using IPX, because TFTP/IPX
  (In-band over Ethernet) protocols are not supported.
- Upgrading the management software of a Switch results in a reset and causes data to temporarily stop passing through the Switch. You should perform an upgrade when your network is inactive, or you should notify users that the network will temporarily be offline. Users should save their work and exit before the upgrade begins.
- Ensure that the Switch that you are upgrading and the workstation which is running the TFTP Server application are on the same IP subnet or have a route between them.
- Downgrading your Switch to an older version of management software is not recommended. It may introduce faults that have been fixed in the latest release of software.
- When the management software is upgraded the Switch will retain all currently configured settings.

Preparing the management software file

1. The executable file containing the management software to upgrade the Switch may be supplied on the CD-ROM that accompanies your Switch.

   3Com recommends that you download the latest publicly available version of management software from the 3Com website:

   http://support.3com.com

   To receive the very latest releases you must purchase a support contract from your reseller.

2. Run the executable file to extract the .bin file to a tftp boot sub-directory e.g. C:\Program Files\3Com\TFTP Server\tftpboot. This file contains the management software.

3. If you have not used the default tftpboot sub-directory, make a note of where you have extracted the .bin file, as you will need to direct your TFTP Server to it.

Setting up your TFTP Server

CAUTION: *These instructions apply to the 3Com TFTP Server, which is a Microsoft Windows TFTP application.*

1. Install the 3Com TFTP Server:

   - From the CD-ROM that accompanies your Switch, or
   - By downloading the 3Com TFTP Server (filename 3ts01_xx.exe) from the 3Com website:

     http://support.3com.com

2. Install the 3Com TFTP Server on a Microsoft Windows 95/98/NT/2000/XP machine.

3. To launch the 3Com TFTP Server, click **Start** -> **Programs** -> **3Com TFTP Server** -> **3Com TFTP Server**.

4. Check that the 3Com TFTP Server is configured to point where the .bin upgrade file is located. To do this:

   - Click the *Options* button on the 3Com TFTP Server menu bar.
   - The *Upload/Download directory* file path should point to the tftp boot sub-directory e.g. C:\Program Files\3Com\TFTP Server\tftpboot. This is the directory where the Switch will look for the file to upgrade the Switch.
   - You may need to change the path to point to the directory containing the .bin upgrade file.
   - Click the *OK* button to close the *Setup* window.

     The IP address of the 3Com TFTP Server is displayed on the Title Bar. You will need this to configure the Switch and TFTP Server with

IP information.

Configuring the Switch and TFTP Server IP information

1. Ensure that you assign an IP address to the Switch that is being upgraded. For further information about setting up an IP address, refer to Setting Up IP Information in the Switch documentation.

2. Ensure that you have connected your Switch to the TFTP Server using an RJ45 cable (the TFTP Server is the workstation containing the 3Com TFTP Server application).

3. The Switch that you are upgrading must:

    - Be in the same subnet as the workstation running your TFTP Server.

      For example, if your workstation's IP address is 192.168.1.40, and a subnet mask of 255.255.255.0, and your Switch unit is configured with an IP address of 192.168.1.x, and a subnet mask of 255.255.255.0, then your upgrade should be successful.

      Or,

    - Have a route between the Switch and the workstation.

CAUTION: *Ensure that the Switch port connected to the TFTP Server belongs to the Default VLAN (VLAN 1). The TFTP Server can only upgrade the management software of the Switch if it is connected to the Switch by the Default VLAN or if an IP route exists between the Default VLAN and the VLAN the TFTP Server belongs to.*

Performing a TFTP upgrade via the Web Interface

1. Open your web browser and enter the Switch IP address in the *Address or Location* field (press *Enter*).

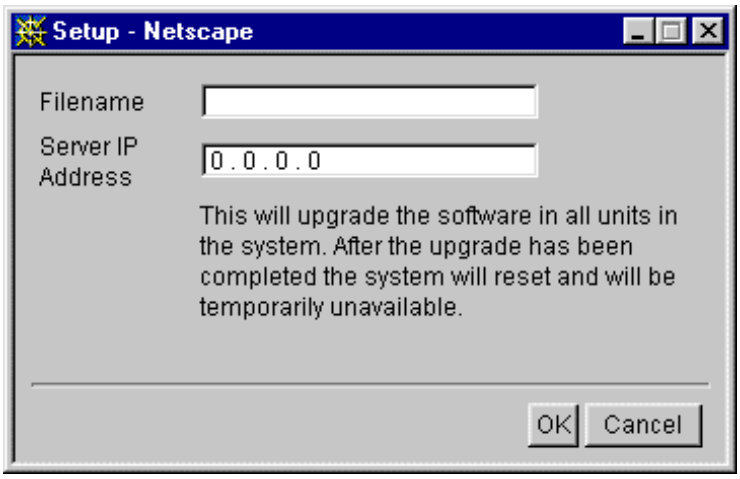
2. Log into the Switch.

   The default user name is **admin** (lower case). There is no default password (press *Enter*).

3. Click *Device View* on the Toolbar.

4. Select **System -> Control -> Software Upgrade** in the Navigation Tree.

5. The Setup window is displayed.



6. Enter the name of the software upgrade file in the *Filename* field. The filename format is:

   nnnxx_yy.bin

   where nnn is the prefix of Switch and xx_yy is the version of management software.

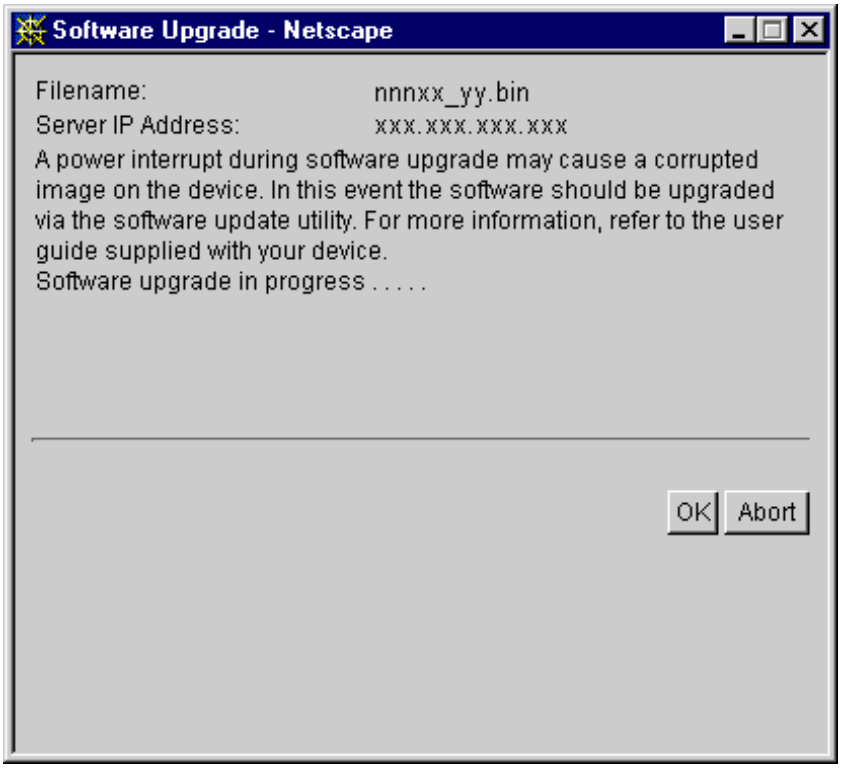
   ⚠ ***CAUTION:*** *You must use the nnnxx_yy.bin format, otherwise the upgrade will fail.*

7. Enter the IP address of the TFTP Server in the *Server IP Address* field. This is the IP address of the workstation running the TFTP Server application.

   ▷ *On the 3Com TFTP Server this IP address is displayed on the title bar.*

8. Click *OK*.

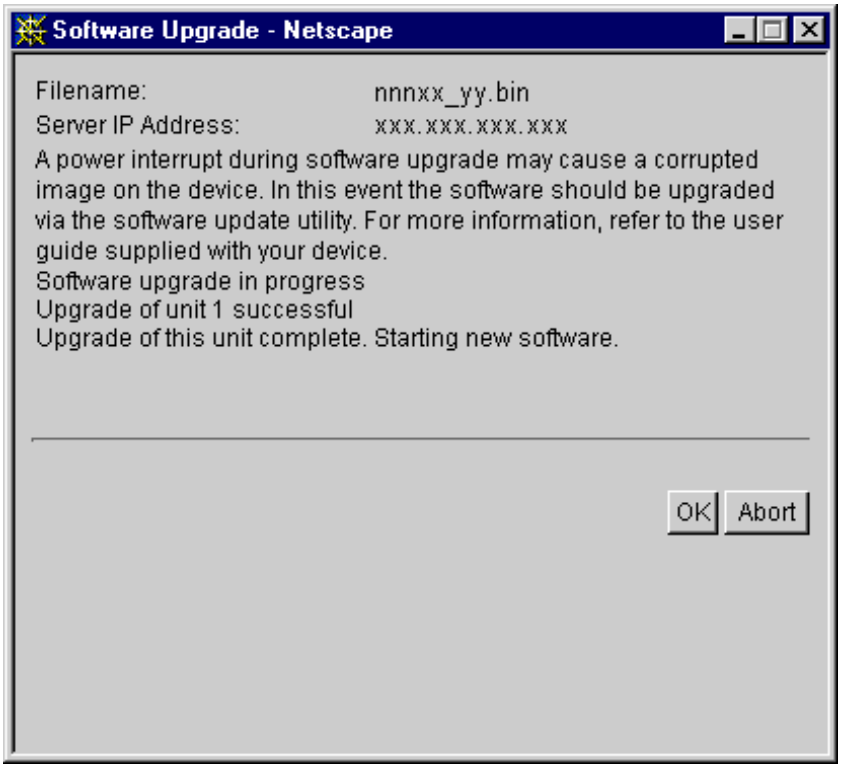
   The following window is displayed:



▷ *The unit will report errors if they occur and abort the file transfer if it*

is unable to complete it. Follow any instructions listed with the errors to resolve the problem.

9. When the software upgrade is complete the following window is displayed (the text will vary depending on the number of units being upgraded):



10. Click the *OK* button to close the Software Upgrade window. The unit will disconnect the Web session and be unavailable for both Telnet and Web access for 1—2 minutes while it overwrites the old software.

    CAUTION: *Do not power down or reset the Switch or attempt to stop the upgrade once it has begun. Interrupting the upgrade will cause the Switch to become unusable.*

11. The Switch will reset when the upgrade is complete, and the Power/Self test LED will change from flashing ON/OFF Green to solid Green.

    Once the LED shows as solid Green the upgrade has been completed and the unit is again ready for Telnet and Web access.

If you are unable to access the Switch through the Web Interface or through the Command Line Interface, then it is possible that you can no longer manage your Switch due to a failure during the software upgrade. Refer to the Solving Management Software Upgrade Problems section of the Management Interface Reference Guide for further assistance.

Related Operations

Initialize	Initializing the Switch
Reboot	Rebooting the Switch



Back to Top

Physical Interface Ethernet Setup

Configuring Ports

You can configure individual and multiple ports on the Switch using the Setup window.

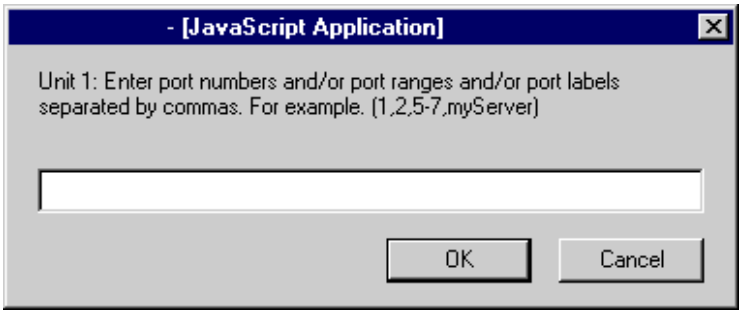
To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Physical Interface -> Ethernet -> Setup** in the Navigation Tree;

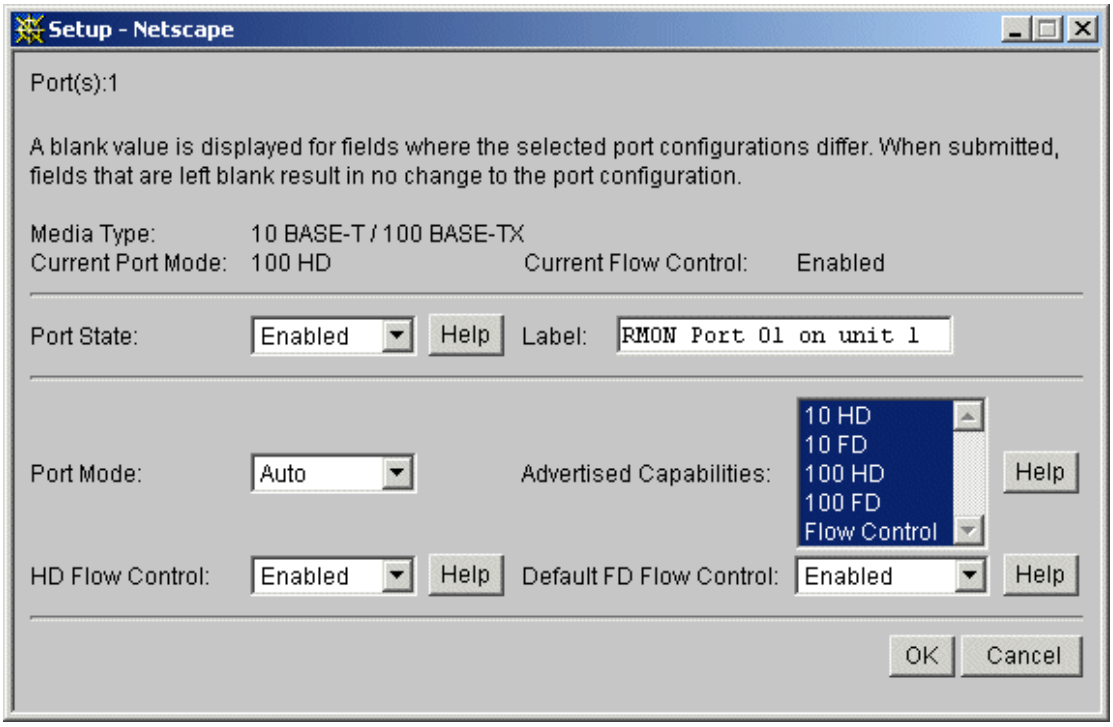
   or

   Click the relevant port on the Switch graphic and select *Setup*.

   If you want to configure several ports at once, you must access the Setup window through the Navigation Tree. Clicking a port on the Switch graphic will only allow you to configure that particular port.
3. If you access the Setup window through the Navigation Tree, you are prompted to enter the port numbers, port ranges and/or port labels that you wish to configure:



   You must separate the values that you enter with commas.
4. Click OK. The Setup window is displayed.



The Setup page contains the following elements:

Port(s):
Displays the number or label of the selected port(s).

Media Type
Displays the media type of the link connected to the port(s).

Current Port Mode:
Displays the speed and duplex mode of the port. If auto-negotiation is enabled, *Auto* is displayed.

Current Flow Control:
Displays the current flow control setting for the port(s).

Port State: *Enabled / Disabled*
Allows you to enable or disable the port(s) (that is, turn the port(s) on or off). The default state is *Enabled*.

Label:
Allows you to assign a name to the port(s).

Port Mode: *Auto / 10HD / 10FD / 100HD / 100FD / 1000FD*
This listbox allows you to specify the speed and duplex mode of the selected ports (*HD* indicates half duplex, *FD* indicates full duplex). The default *Port Mode* is *Auto*. In this mode the port will negotiate speed, duplex and flow control.

⚠ ***CAUTION:*** *To communicate without errors, both ends of a link must use the same duplex mode.*

Ports operating at 1000 Mbps support full duplex mode only.

GBIC ports (if present on the switch) operate at 1000 Mbps only in full duplex mode. They will still autonegotiate flow control.

For auto-negotiation to succeed, ports at both ends of the link must be set to

auto-negotiate.

Advertised Capabilities: *10HD / 10FD / 100HD / 100FD / 1000FD / Flow Control*
Allows you to select the values that are advertised during auto-negotiation, allowing you to restrict the features that the port offers. If you deselect features the port will continue to auto-negotiate, but will only advertise the selected states. To select multiple items from the list, control-click each one with your mouse. The default is that all available items are selected.

HD Flow Control: *Enabled / Disabled*
Allows you to enable or disable the flow control that can be used when the port is operating in half duplex mode. Flow control minimizes packet loss during periods of congestion on the port. The default setting is *Enabled*.

 *The HD Flow Control listbox should be set to disabled if the port is connected to multiple devices using a hub. If it is enabled, local traffic between those multiple devices is inhibited. HD Flow Control is not supported by 1000BASE-LX/SX ports.*

Default FD Flow Control: *Enabled / Disabled / TxOn / RxOn*
If auto-negotiation is disabled, this listbox allows you to enable or disable the IEEE 802.3x flow control that can be used when the port is operating in full duplex. If auto-negotiation is enabled, the listbox displays Auto, and you cannot change the flow control setting for the port manually. Flow control minimizes packet loss during periods of congestion on the port. The default setting is *Enabled*.

 `rxOn` *and* `txOn` *are unidirectional flow control commands that may be set up for fiber Gigabit Ethernet ports. They will only be available on GBIC ports if present on your unit.*

 *For IEEE 802.3x flow control to operate correctly, it must be enabled at both ends of the link.*

 *If you choose to configure more than one port at the same time, only the values that are identical for each port are displayed in the Setup window. If a value is different for one or more ports, then the field in which it is usually displayed is left blank.*

Related Operations

Smart Autosensing	Enabling and Disabling Smart Autosensing
Statistics	Displaying Unit Statistics
Port Setup Summary	Displaying Summary Information for Ports

Back to Top

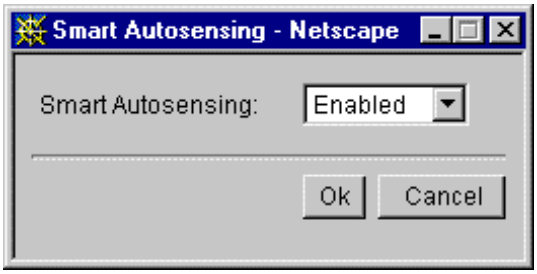
Physical Interface Ethernet Smart Autosensing

Enabling and Disabling Smart Autosensing

You can enable and disable smart autosensing for the unit using the Smart Autosensing window. If smart autosensing is enabled on a 10BASE-T/100BASE-TX or 10BASE-T/100BASE-TX/1000BASE-T port, the port monitors the error rate. If this becomes unacceptably high and the other end of the link also supports auto negotiation, then the error rate is reduced by lowering the speed of the link.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Physical Interface -> Ethernet -> Smart Autosensing** in the Navigation Tree. The Smart Autosensing window is displayed.



3. From the *Smart Autosensing:* listbox, select *Enabled* or *Disabled*.

Smart Autosense will not operate on links that do not support auto-negotiation, or on links where one end is at a fixed speed.

GBIC ports (if present on the switch) will only operate at 1000 Mbps and are unaffected by this setting.

Related Operations

Setup	Configuring Ports
Statistics	Displaying Unit Statistics
Port Setup Summary	Displaying Summary Information for Ports

Back to Top

Physical Interface Ethernet Statistics

Displaying Unit Statistics

You can display a range of statistics for all the ports on the Switch using the Statistics window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Physical Interface -> Ethernet -> Statistics** in the Navigation Tree;

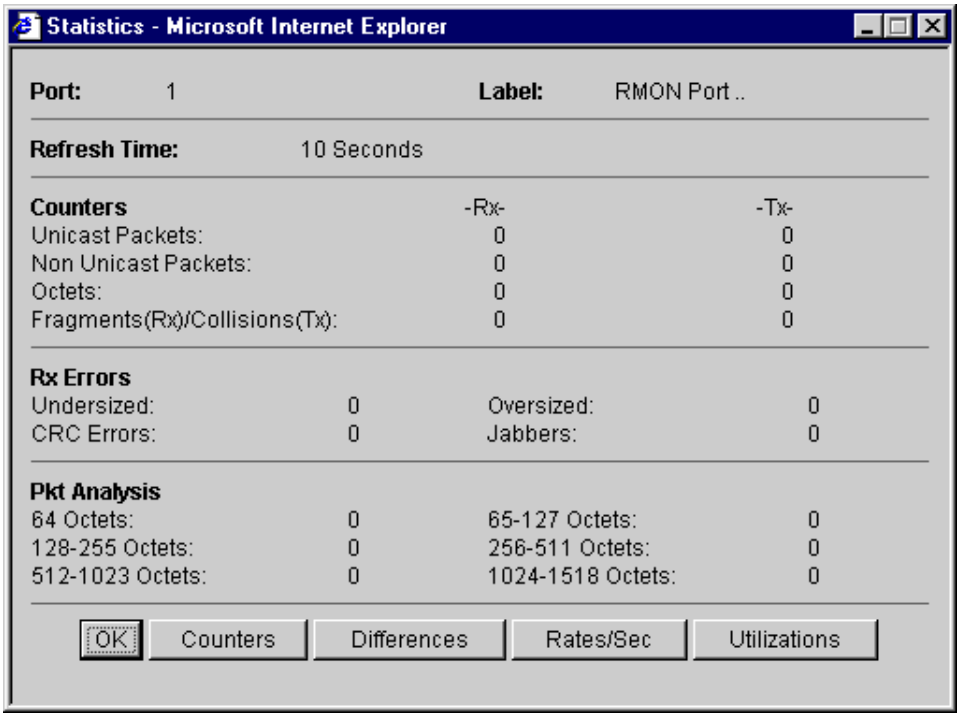
   or

   Click the relevant port on the Switch graphic and select *Statistics*.

   If you want to display the statistics for more than one port at the same time, you must access the Statistics window through the Navigation Tree. Clicking a port on the Switch graphic will only allow you to display the statistics for that particular port.

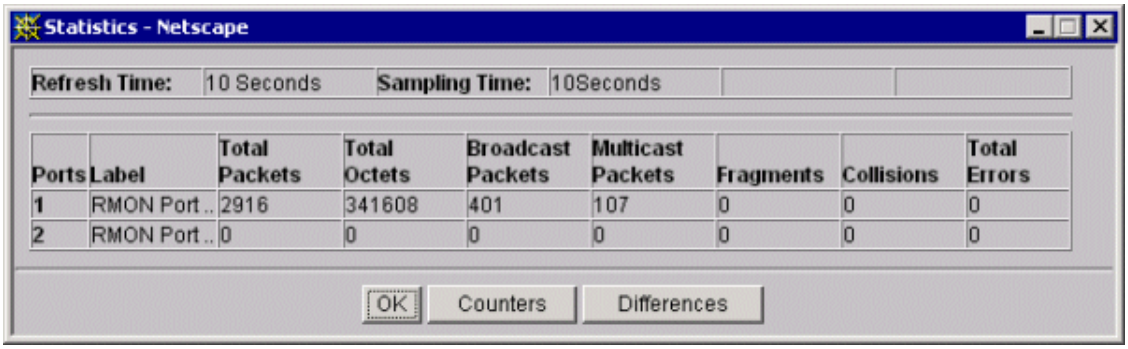
   If you access the Statistics window through the Navigation Tree, you are prompted to enter the port numbers, port ranges and/or port labels that you wish to configure.

   You must separate the values that you enter with commas.
3. The following window is displayed for a single port.



You can click on Counters, Differences, Rates, or Utilitizations to change the type of statistics displayed for the port selected (Counters is the default screen display).

The following window is displayed for multiple ports.



You can click on Counters or Differences to change the type of statistics displayed for the range of ports selected (Counters is the default screen display).

Related Operations

Setup	Configuring Ports
Smart Autosensing	Enabling and Disabling Smart Autosensing
Summary	Displaying Summary Information for Ports

Back to Top

Physical Interface Ethernet Port Setup Summary

Displaying Summary Information for Ports

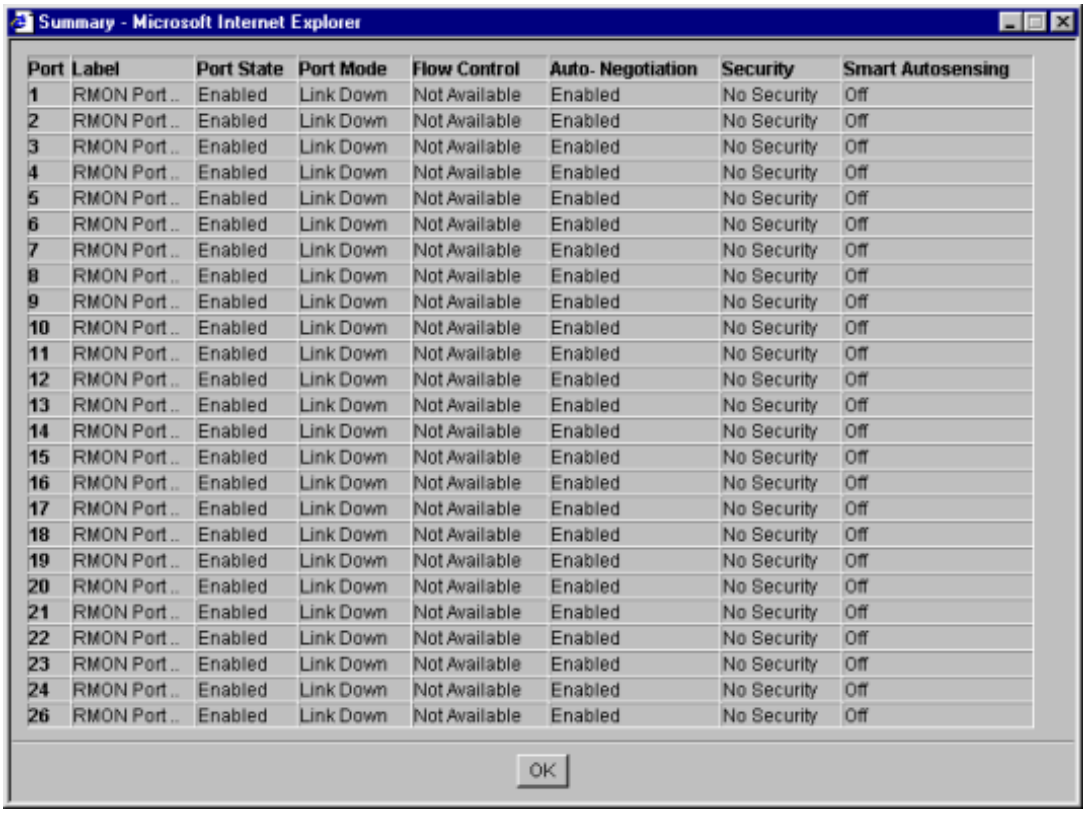
You can display summary information for all the ports on the Switch using the Port Setup Summary window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Physical Interface -> Ethernet -> Port Setup Summary** in the Navigation Tree;

   or

   Click the device body part of the Switch graphic and select *Port Setup Summary*.
3. The Port Setup Summary window is displayed.



Port	Label	Port State	Port Mode	Flow Control	Auto- Negotiation	Security	Smart Autosensing
1	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
2	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
3	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
4	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
5	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
6	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
7	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
8	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
9	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
10	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
11	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
12	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
13	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
14	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
15	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
16	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
17	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
18	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
19	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
20	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
21	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
22	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
23	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
24	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off
26	RMON Port ..	Enabled	Link Down	Not Available	Enabled	No Security	Off

OK

Related Operations

Setup	Configuring Ports
Smart Autosensing	Enabling and Disabling Smart Autosensing
Statistics	Displaying Unit Statistics



Back to Top









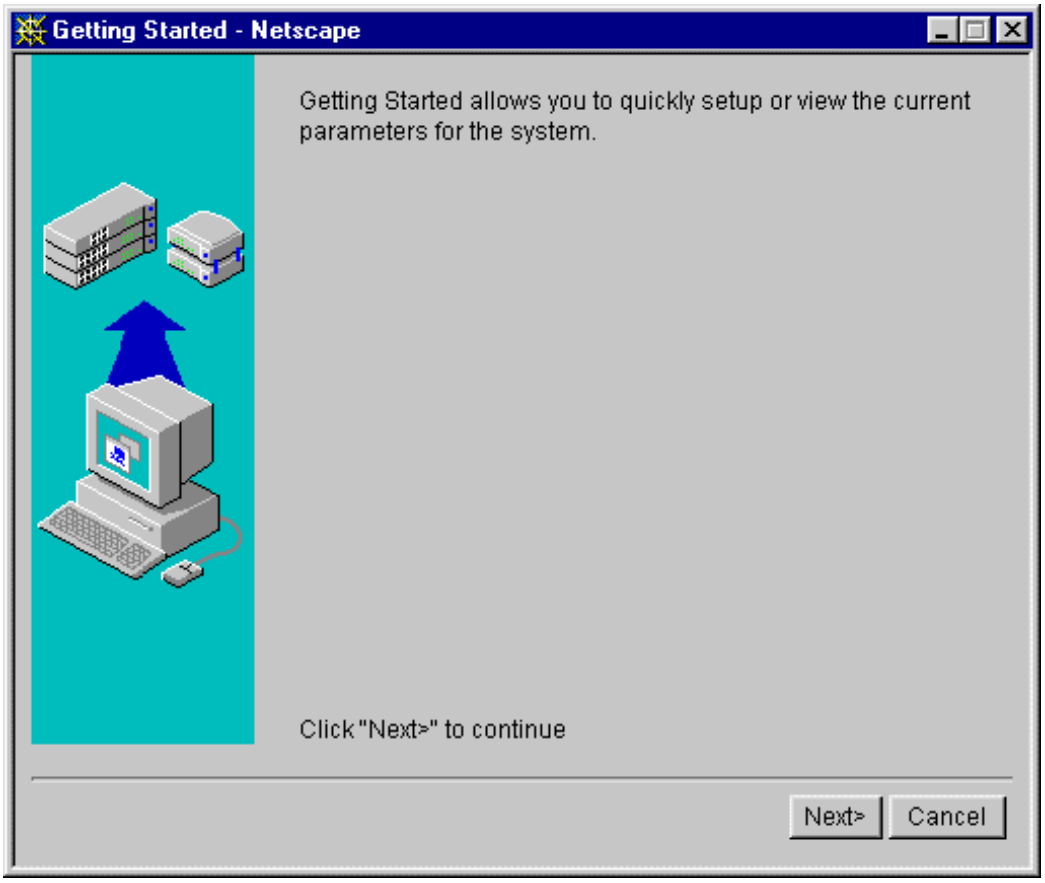
System Getting Started

The Getting Started Pages

When you access the web interface for the first time or after a power-off/on cycle, a set of Getting Started pages are displayed. The Getting Started pages allow you to enter basic setup information for the unit. The Getting Started pages are also available from the main web interface at any time.

To access the Getting Started pages:

1. Click *Device View* on the Toolbar.
2. Select **System -> Getting Started** in the Navigation Tree. The first Getting Started page is displayed.



As you go through the pages, you need to enter:

1. A descriptive name for the unit.
2. The physical location of the unit.
3. The name of a person to contact about the unit.
4. Whether you want to:

   - manually configure IP information for the unit
   - automatically configure IP information for the unit
   - disable the LAN interface

The Switch has three automatic IP configuration methods that it tries in turn, these are: DHCP, Auto-IP and BOOTP. For detailed information on how the automatic IP configuration process works, please refer to the Implementation Guide that accompanies your Switch.

Automatic is the default setting for IP configuration. If you select Automatic IP configuration, no further prompts are displayed.

If you choose to manually configure the IP information, you are prompted to enter the following:

IP Address
Allows you to enter a unique IP address for the Switch.

If you change the IP address of the Switch, you can no longer access the web interface unless you enter the new IP address in the Location Address *field of your browser.*

Subnet Mask
Allows you to enter a subnet mask for the Switch.

Default Gateway (router)
If your network contains one or more gateways, this field allows you to enter the IP address of the default gateway.

5. If you select **None**, no further prompts are displayed.

6. A new password for the current user (enter the existing password if you want to leave the password unchanged).

Back to Top

Physical Interface Ethernet History History-1 Hour

Displaying 1-Hour Unit History

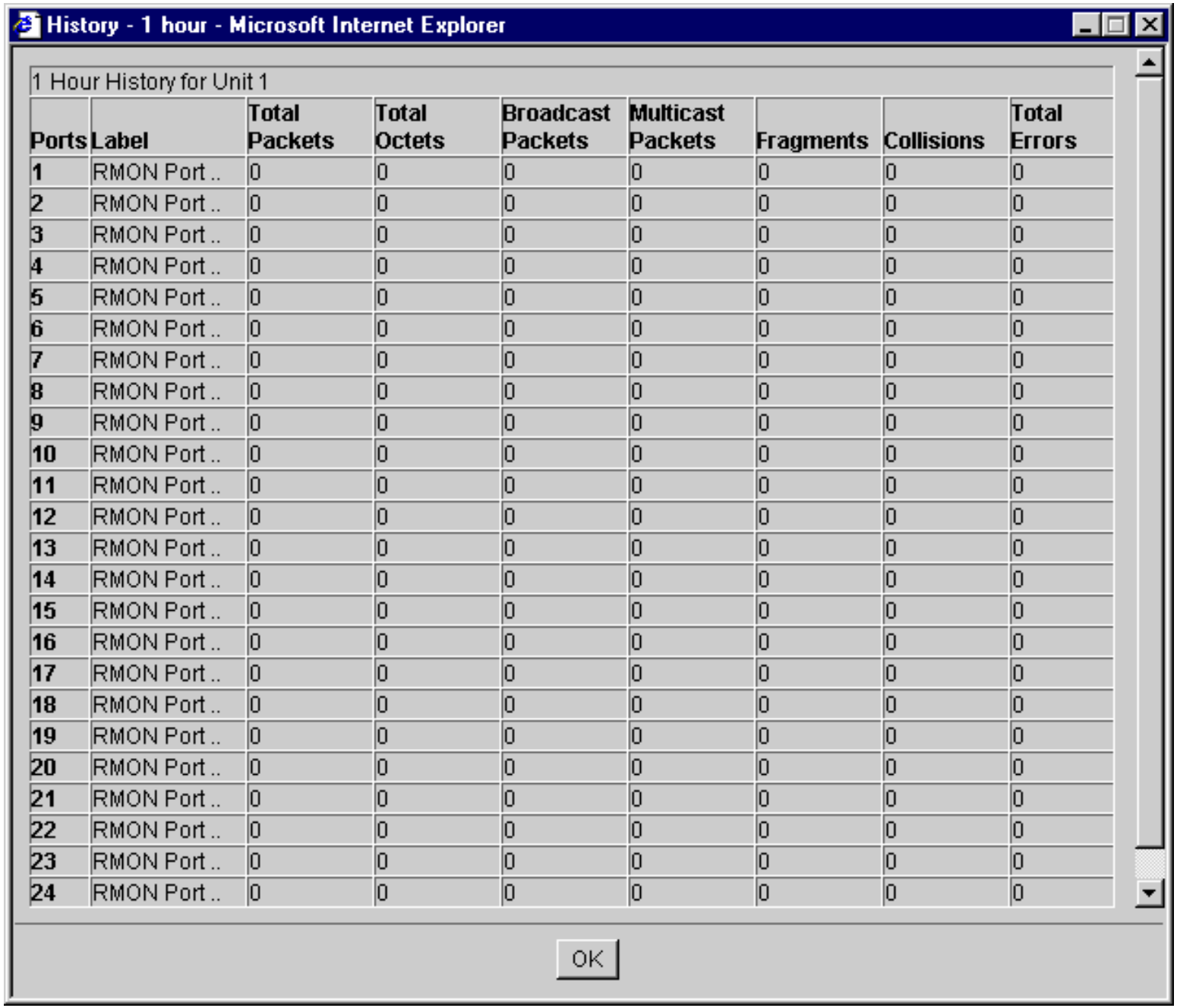
You can display the packet activity for all ports on a unit for the previous hour using the History-1 Hour window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Physical Interface -> Ethernet -> History -> History-1 Hour** in the Navigation Tree;

   or

   Click the device body part on the Switch graphic and select *History-1 Hour*.
3. The History-1 hour window is displayed.



Ports	Label	Total Packets	Total Octets	Broadcast Packets	Multicast Packets	Fragments	Collisions	Total Errors
1	RMON Port ..	0	0	0	0	0	0	0
2	RMON Port ..	0	0	0	0	0	0	0
3	RMON Port ..	0	0	0	0	0	0	0
4	RMON Port ..	0	0	0	0	0	0	0
5	RMON Port ..	0	0	0	0	0	0	0
6	RMON Port ..	0	0	0	0	0	0	0
7	RMON Port ..	0	0	0	0	0	0	0
8	RMON Port ..	0	0	0	0	0	0	0
9	RMON Port ..	0	0	0	0	0	0	0
10	RMON Port ..	0	0	0	0	0	0	0
11	RMON Port ..	0	0	0	0	0	0	0
12	RMON Port ..	0	0	0	0	0	0	0
13	RMON Port ..	0	0	0	0	0	0	0
14	RMON Port ..	0	0	0	0	0	0	0
15	RMON Port ..	0	0	0	0	0	0	0
16	RMON Port ..	0	0	0	0	0	0	0
17	RMON Port ..	0	0	0	0	0	0	0
18	RMON Port ..	0	0	0	0	0	0	0
19	RMON Port ..	0	0	0	0	0	0	0
20	RMON Port ..	0	0	0	0	0	0	0
21	RMON Port ..	0	0	0	0	0	0	0
22	RMON Port ..	0	0	0	0	0	0	0
23	RMON Port ..	0	0	0	0	0	0	0
24	RMON Port ..	0	0	0	0	0	0	0

Related Operations

 Displaying 48-Hour Unit History



Back to Top

Physical Interface Ethernet History History-48 Hours

Displaying 48-Hour Unit History

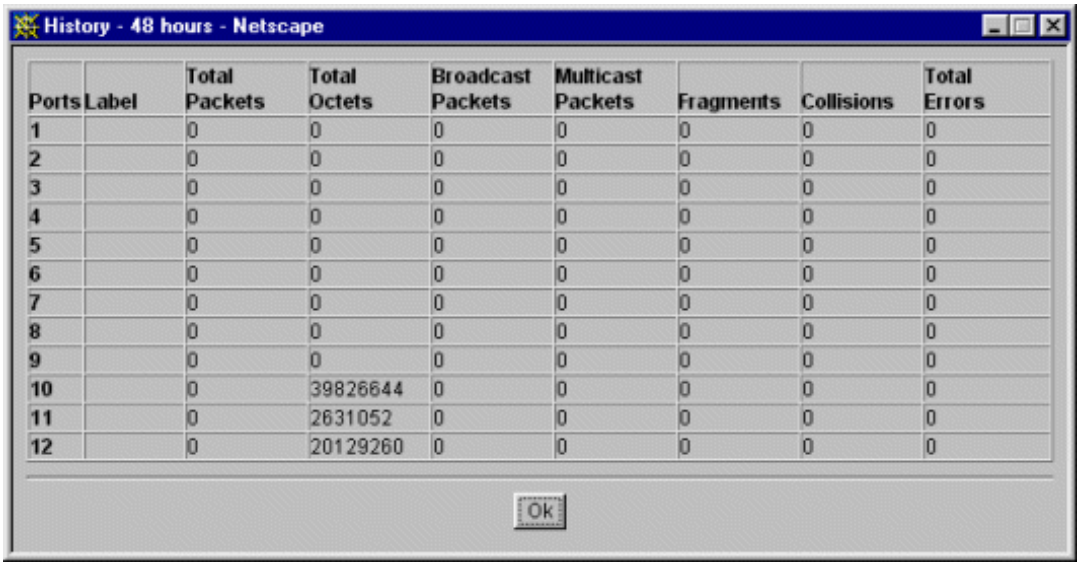
You can display the packet activity for all ports on a unit for the previous 48 hours using the History-48 Hours window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Physical Interface -> Ethernet -> History -> History-48 Hours** in the Navigation Tree;

   or

   Click the device body part on the Switch graphic and select *History-48 Hours*.
3. The History-48 hours window is displayed.



Related Operations

History-1 Hour	Displaying 1-Hour Unit History

Back to Top

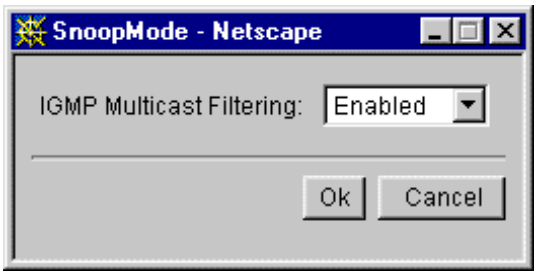
Bridge Multicast Filter IGMP SnoopMode

Enabling or Disabling IGMP Multicast Filtering

You can enable or disable IGMP Multicast Filtering for the unit using the SnoopMode window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Multicast Filter -> IGMP -> SnoopMode** in the Navigation Tree.
3. The SnoopMode window is displayed.



The SnoopMode window contains the following elements:

IGMP Multicast Filtering: *Enabled* / *Disabled*
Allows you to specify whether the ports in the unit use IGMP multicast filtering to filter unknown multicasts automatically.

Back to Top

Protocol IP Setup

Setting Up IP Information

You can set up the IP information for the Switch using the Setup windows.

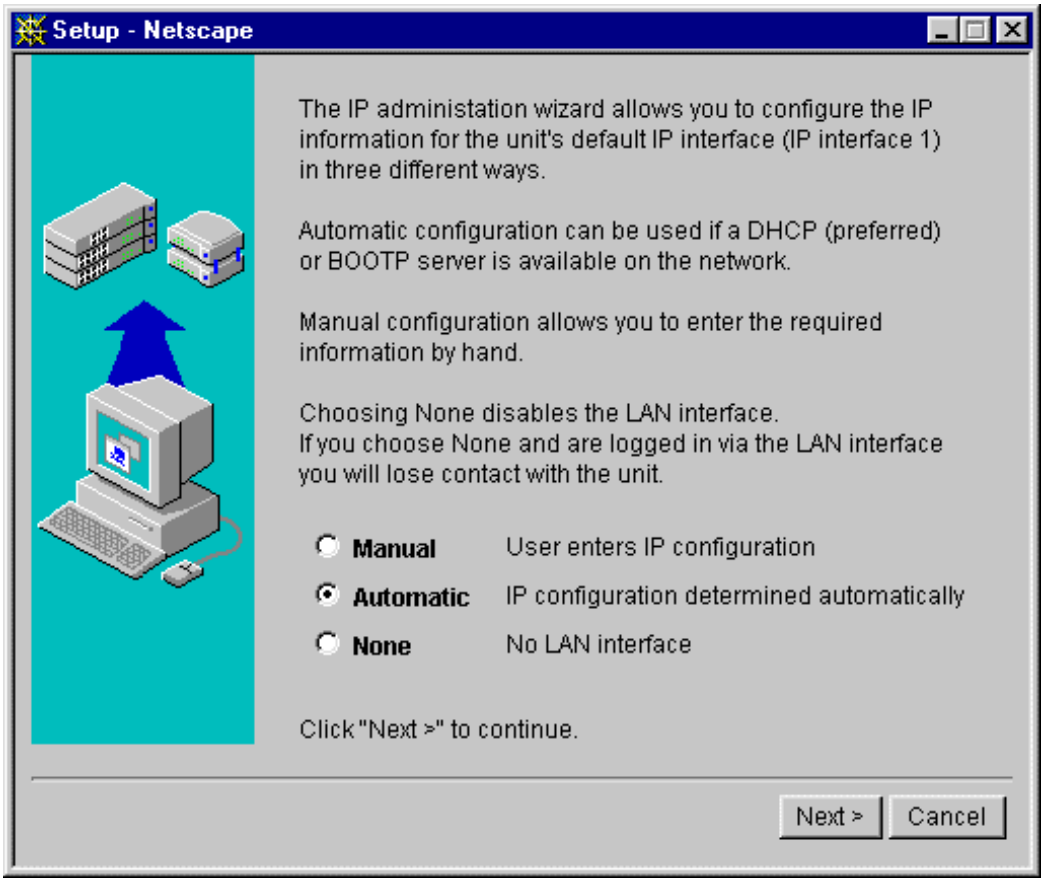
To access the windows:

1. Click *Device View* on the Toolbar.
2. Select **Protocol -> IP -> Setup** in the Navigation Tree;

   or

   Click the device body part of the Switch graphic and select *Setup*.

   The first Setup window is displayed.



3. As you go through the setup windows, you are asked to enter whether you want to:

   - manually configure IP information for the unit
   - automatically configure IP information for the unit
   - disable the LAN interface

The Switch has three automatic IP configuration methods that it tries in turn, these are: DHCP, Auto-IP and BOOTP. For detailed information on how the automatic IP configuration process works, please refer to the Implementation Guide that accompanies your Switch.

Automatic is the default setting for IP configuration. If you select Automatic IP configuration, no further prompts are displayed.

4.

If you choose to manually configure the IP information, you are prompted to enter the following:

IP Address
Allows you to enter a unique IP address for the Switch.

 *If you change the IP address of the Switch, you can no longer access the web interface unless you enter the new IP address in the* Location Address *field of your browser.*

Subnet Mask
Allows you to enter a subnet mask for the Switch.

Default Gateway (router)
If your network contains one or more gateways, this field allows you to enter the IP address of the default gateway.

5. If you select **None**, no further prompts are displayed.

Back to Top

Bridge Link Aggregation Summary

Displaying Summary Information for Aggregated Links

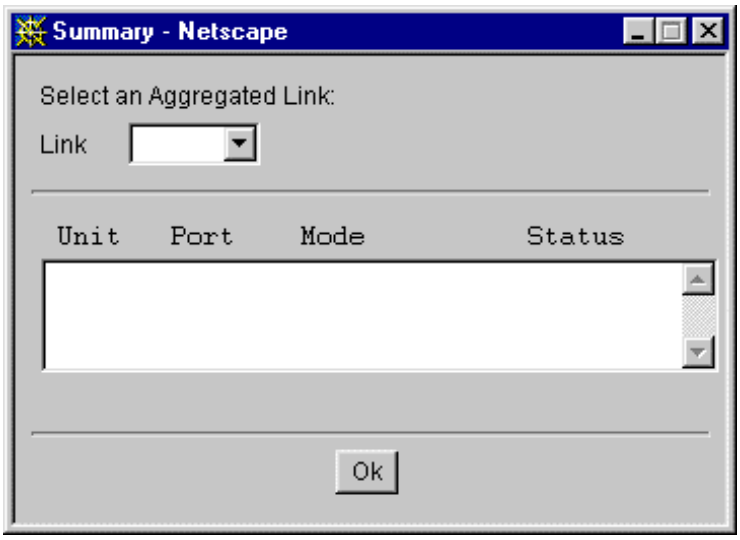
Aggregated links are connections that allow devices to communicate using up to four links in parallel. Aggregated links are supported on the 10/100/1000BASE-T ports and GBIC ports (if present on the unit). These parallel links provide two benefits:

- They can potentially double, treble or quadruple the bandwidth of a connection.
- They can provide redundancy—if one link is broken, the other link can share the traffic for that link.

You can display summary information for an aggregated link using the Summary window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Link Aggregation -> Summary** in the Navigation Tree.
3. The Summary window is displayed.



The Summary window contains the following elements:

Select an Aggregated Link:
Allows you to select the aggregated link for which you want to display summary information.

When an aggregated link is selected, a list of all the ports in the link is displayed. The mode and status of each occurrence is also shown.

If the aggregated link is empty then the message No ports in this Link *is displayed.*



Back to Top

System Management Setup

Changing the Management Settings for the Unit

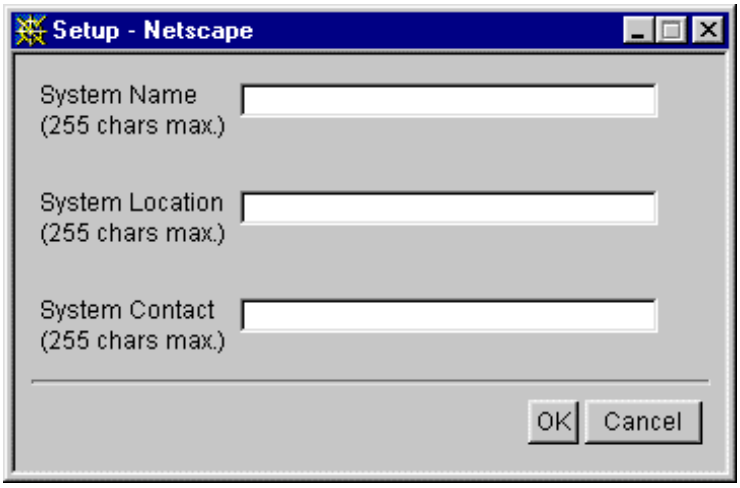
You can change the management settings for the unit using the Setup window.

This window allows you to:

- Specify a descriptive name for the unit.
- Specify the physical location of the unit.
- Specify the details of a person to contact about the unit.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Setup** in the Navigation Tree.
3. The Setup window is displayed.



The window contains the following elements:

System Name
This field allows you to enter a descriptive name for the unit.

System Location
This field allows you to enter the physical location of the unit.

System Contact
This field allows you to enter the name of a person to contact about the unit.

Back to Top

Bridge Link Aggregation Modify Add Port

Setting Up Aggregated Links

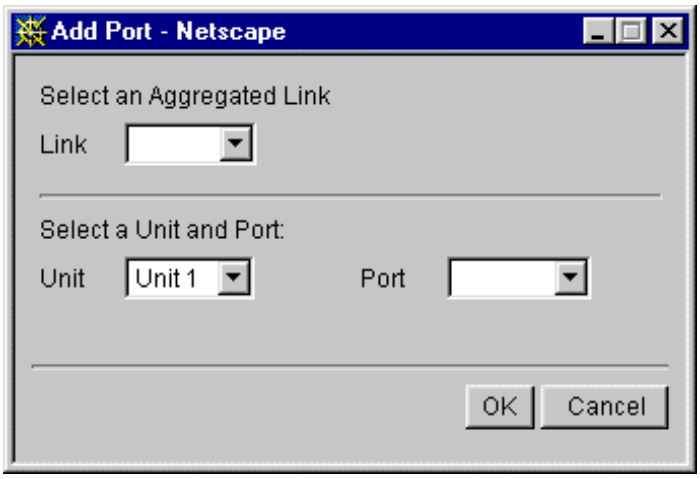
Aggregated links are connections that allow devices to communicate using up to two links in parallel. Aggregated links provide two benefits:

- They can potentially double the bandwidth of a connection.
- They can provide redundancy — if one link is broken, the other link shares the traffic for that link.

You can set up aggregated links for the unit using the Add Port window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Link Aggregation -> Modify -> Add Port** in the Navigation Tree.
3. The Add Port window is displayed.



The Add Port window contains the following elements:

Select an Aggregated Link:
Allows you to select the aggregated link to set up. Only links that are not already full are available for selection.

If all aggregated links are full then the message All Aggregated Links are full. You cannnot add any ports *is displayed when you try to open the Add Port window.*

Select a Unit and Port:
Allows you to select the port to be placed in the aggregated link. To do this:

1. From the *Unit* listbox, select a unit. When a unit is selected, the *Port* listbox is updated to display only the ports in that unit that can be added to aggregated links.
2. From the *Port* listbox, select a port.

3. Click *OK*. The port is assigned to the aggregated link and the Add Port window is closed.

Related Operations

Admin State	Modifying the Administrative State of an Aggregated Link
Partner ID	Setting or Modifying the Partner ID for an Aggregated Link
LACP State	Enabling or Disabling LACP on a Port
Remove Port	Removing a Port from an Aggregated Link

Back to Top

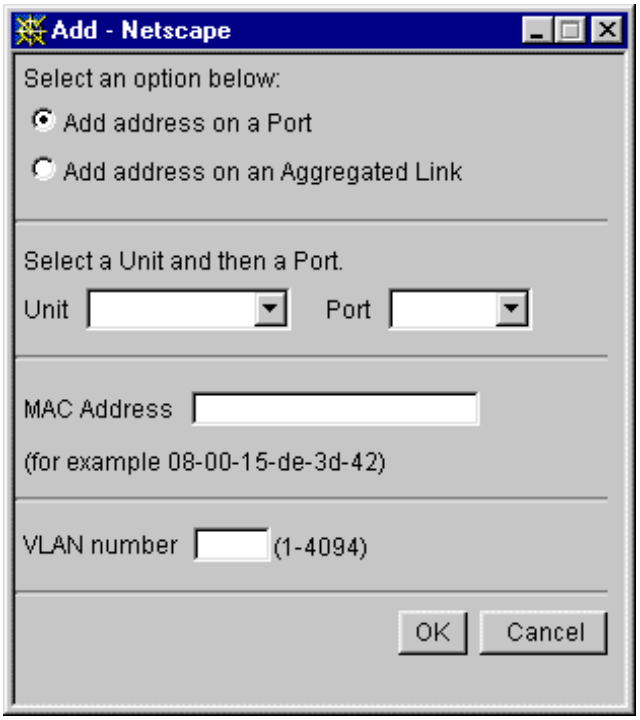
Bridge Address Database Add

Adding a MAC Address

You can add a new MAC address to the Address Database using the Add window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Address Database-> Add** in the Navigation Tree.
3. The Add window is displayed.



To add a new address to the Address Database:

1. From the *Select an option below:* radio buttons, select if the address is to be stored on a Port or an Aggregated Link.

   If you select *Add address on a Port*, you are prompted to select a unit and a port from the *Unit and Port* listboxes.

   If you select *Add address on an Aggregated Link*, you are prompted to select an aggregated link from the *Link* listbox.
2. In the *MAC Address* field, enter the MAC (Ethernet) address.
3. In the *VLAN number* field, enter the VLAN number.
4. Click *OK*. The address is added to the Address Database and the Add window closes.

Related Operations

AgingTime	Enabling and Disabling Aging Time
Find	Finding a MAC Address
Remove	Removing a MAC Address
Summary	Displaying Summary Information for MAC Addresses

Back to Top

Bridge Link Aggregation Modify LACP State

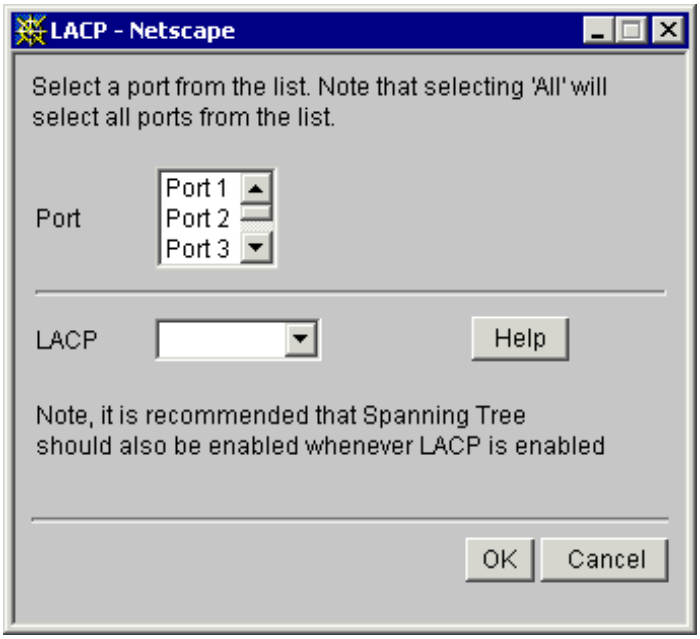
Enabling or Disabling LACP on a Port

You can enable or disable Link Aggregation Control Protocol (LACP IEEE 802.3ad) on individual ports on all units in a stack using the LACP window.

You can only enable or disable LACP on physical ports rather than logical bridge ports. Hence aggregated links do not appear in the port list.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Link Aggregation -> Modify -> LACP State** in the Navigation Tree.
3. The LACP window is displayed.



The LACP window contains the following elements:

Port
Select the port for which you wish to enable or disable LACP.

LACP
Select whether you want to enable or disable LACP for the selected port.

it is recommended that Spanning Tree should also be enabled when LACP is enabled.

Related Operations

Add Port	Setting Up Aggregated Links
Admin State	Modifying the Administrative State of an Aggregated Link
Partner ID	Setting or Modifying the Partner ID for an Aggregated Link


Back to Top

Bridge Link Aggregation Modify Partner ID

Setting or Modifying the Partner ID for an Aggregated Link

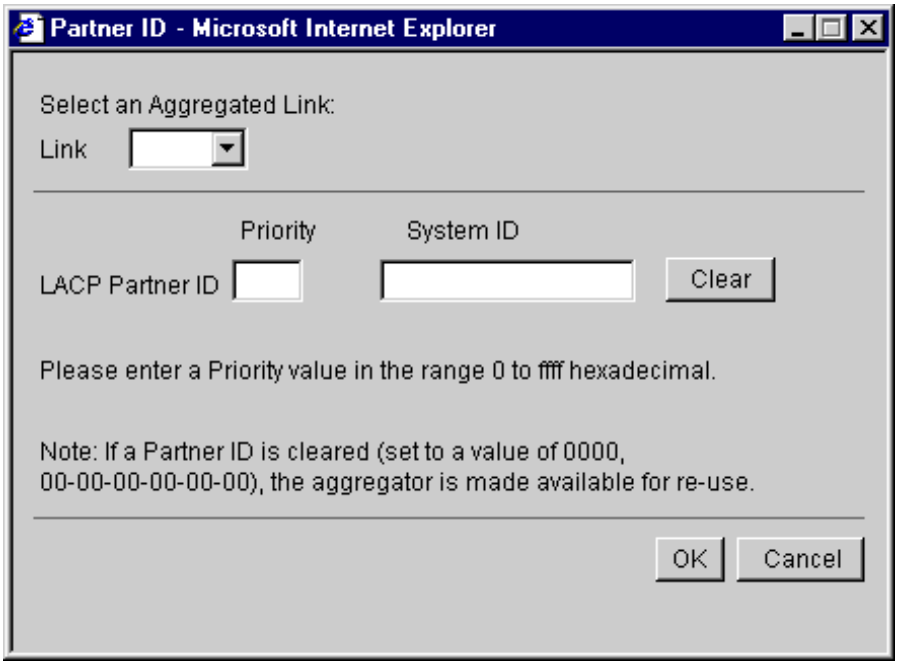
You can set or modify the identity of a partner unit at the remote end of an aggregated link on the current Switch unit using the Partner ID window.

This command is used for IEEE Std 802.3-2002 (incorporating 802.3ad) LACP Pre-Configured Aggregations. This allows you to manually configure a Partner ID (that is, the MAC address of a partner device) to an aggregated link, such as AL1 or AL2 and so on, so that you know which aggregated link is associated with which device in your network. LACP will then automatically determine the port membership for the aggregated link. On detecting an active port with a matching Partner ID, LACP will automatically add the port to the pre-configured aggregated link.

The aggregated link should also be manually configured with appropriate configuration settings, such as VLAN membership, to match the partner device.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Link Aggregation -> Modify -> Partner ID** in the Navigation Tree.
3. The Partner ID window is displayed.



The Partner ID window contains the following elements:

Select an Aggregated Link:
Allows you to select the aggregated link that you wish to set the unit partner identity for.

LACP Partner ID

Allows you to enter the system priority and system ID (MAC Address) of the partner unit. These values taken together make up the LACP Partner ID.

Related Operations

Add Port	Setting Up Aggregated Links
Admin State	Modifying the Administrative State of an Aggregated Link
LACP State	Enabling or Disabling LACP on a Port
Remove Port	Removing a Port from an Aggregated Link

 Back to Top

Bridge Link Aggregation Modify Remove Port

Removing a Port from an Aggregated Link

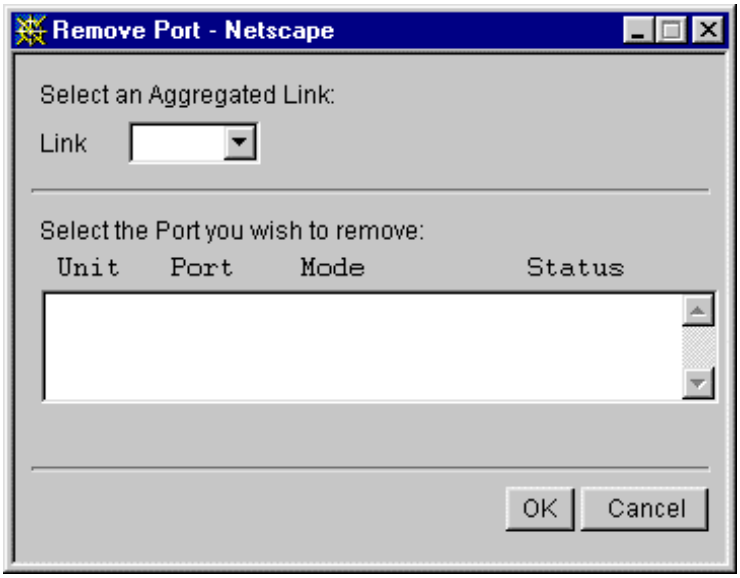
Aggregated links are connections that allow devices to communicate using up to two links in parallel. Aggregated links provide two benefits:

- They can potentially double the bandwidth of a connection.
- They can provide redundancy — if one link is broken, the other link shares the traffic for that link.

You can remove a single port from an aggregated link using the Remove Port window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Link Aggregation -> Modify -> Remove Port** in the Navigation Tree.
3. The Remove Port window is displayed.



The Remove Port window contains the following elements:

Select an Aggregated Link:
Allows you to select the aggregated link from which the port is to be removed. Only non-empty links are available for selection. When an aggregated link is selected, the *Select the Port you wish to remove* listbox is updated to display only the ports in that link that can be removed.

If all aggregated links are empty then the message All Aggregated Links are empty. You cannnot remove any ports *is displayed when you try to open the Remove Port window.*

Select the Port you wish to remove.
Allows you to select the port to be removed from the aggregated link.

Click *OK*. The port is removed from the aggregated link and the Remove Port window is closed.

Related Operations

Add Port	Setting Up Aggregated Links
Admin State	Modifying the Administrative State of an Aggregated Link
Partner ID	Setting or Modifying the Partner ID for an Aggregated Link
LACP State	Enabling or Disabling LACP on a Port

Back to Top

System Management Monitor Modify

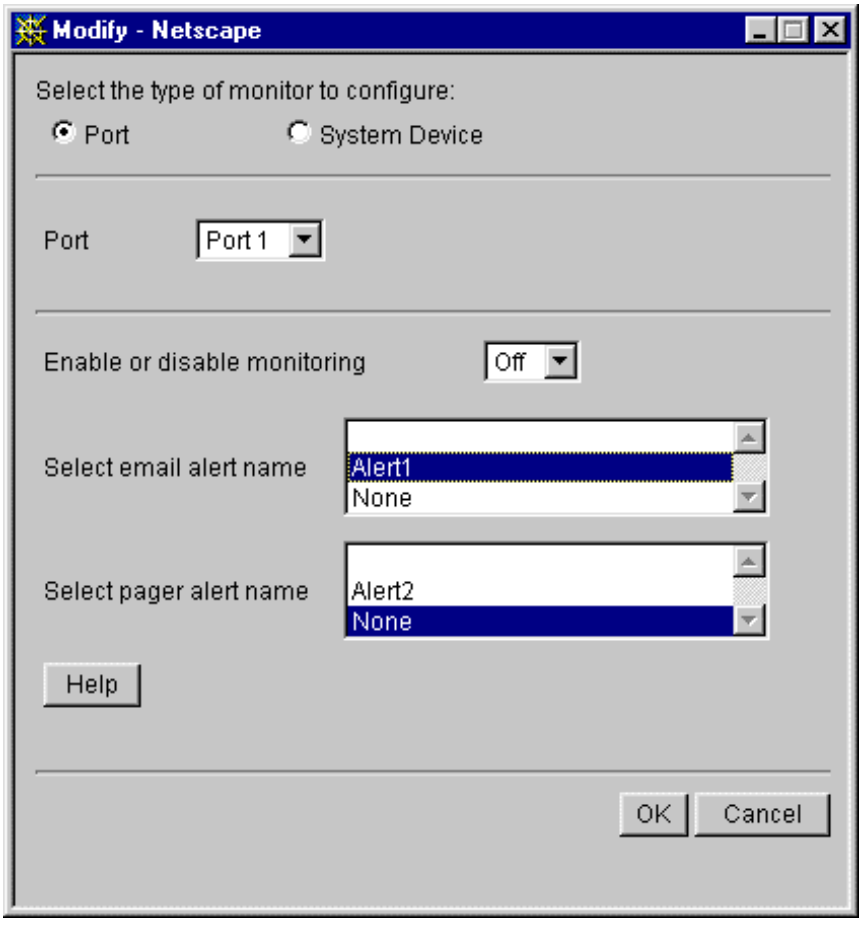
Modifying a Monitored Item

A monitored item is either a Switch unit or a port(s) that you can select to be monitored so that you can receive email or pager notification when certain events occur. This operation should be used in conjunction with the Alert operation.

You can modify a monitored item using the Modify window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Monitor -> Modify** in the Navigation Tree.
3. The Modify window is displayed.



4. Select the type of monitored item you wish to configure: Port or System Device. Any currently configured parameters will be displayed for you to select and modify.
5. Enter the new details for the monitored item that you wish to modify.
6. Click *OK*.

Related Operations

Summary	Displaying Summary Information for Monitored Items.
Create	Creating an Alert
Modify	Modifying an Alert
Test	Sending a test Alert
Delete	Deleting an Alert
Summary	Displaying Summary Information for Alerts

Back to Top

System Management Monitor Summary

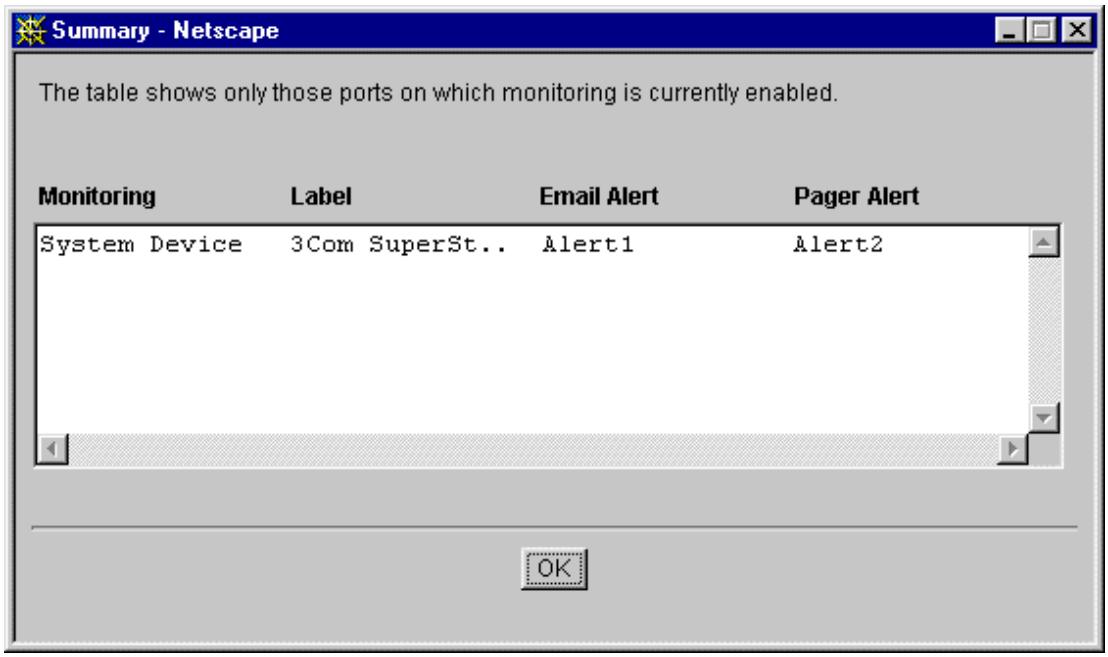
Displaying Monitor Summary Information

You can display summary information for all monitored items defined for the unit using the Summary window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Management -> Monitor -> Summary** in the Navigation Tree.

   The Summary window is displayed.



3. Click *OK*.

Related Operations

Modify	Modifying a Monitored Item
Create	Creating an Alert
Modify	Modifying an Alert
Test	Sending a test Alert
Delete	Deleting an Alert
Summary	Displaying Summary Information for Alerts



Back to Top

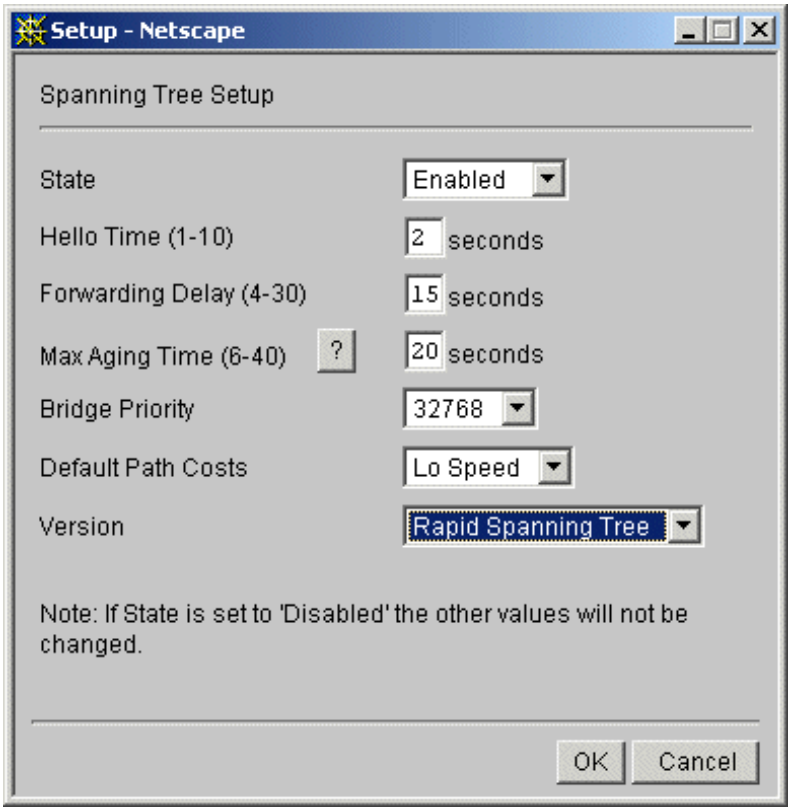
Bridge Spanning Tree Setup

Configuring Spanning Tree Parameters

You can configure spanning tree parameters using the Setup window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Bridge -> Spanning Tree -> Setup** in the Navigation Tree.
3. The Setup window is displayed.



The Setup window contains the following elements:

State *Enabled / Disabled*
Allows you to specify whether the unit uses the Spanning Tree Protocol (STP). Using STP makes your network more resilient to link failure and also provides a protection from loops — one of the major causes of broadcast storms. The default state is *Enabled*.

Hello Time (1-10)
Allows you to specify the time in seconds that elapses between the configuration messages (also known as Hello BPDUs) generated by a bridge that assumes itself to be the Root Bridge. The default *Hello Time* is *6* seconds.

Forwarding Delay (4-30)
Allows you to specify the time in seconds that a bridge spends in the listening and learning states, that is, listening for configuration messages. The default *Forwarding Delay* is *15* seconds.

Max Aging Time (6-40)
Allows you to specify the maximum age in seconds at which the stored configuration message information is judged to be too old and is discarded. The default *Max Aging Time* is *20* seconds.

If a bridge does not receive a configuration message after the Max Aging Time, the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. The bridge then reconfigures the network to cater for the change.

Bridge Priority *32768*
Allows you to specify the configurable value that is appended as the most significant portion of a Bridge Identifier.

The Bridge Identifier is calculated using the priority defined for the bridge and the MAC address of the bridge. The Bridge Identifier specifies which bridge acts as the central reference point, or Root Bridge, for the STP system — the lower the Bridge Identifier, the more likely the bridge is to become the Root Bridge. The default priority of your Switch is *32768*.

Default Path Costs
Allows you to set the bridge spanning tree default path costs for the current Switch. The default setting is *Lo Speed*.

Version
Allows you to select the Spanning Tree version.

Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) are bridge-based systems that makes your network more resilient to link failure and also provides protection from network loops — one of the major causes of broadcast storms.

RSTP is an enhanced version of the STP feature and is enabled by default. RSTP can restore a network connection quicker than the STP feature. The default setting is *Rapid Spanning Tree*.

If you enter an incorrect value then the message Invalid value for... *is displayed when you click* OK. *You must enter a valid value before the settings can be saved.*

CAUTION: *If you enable STP, the* unit *takes several seconds to configure itself. During this time, you cannot communicate with the* unit.

Back to Top

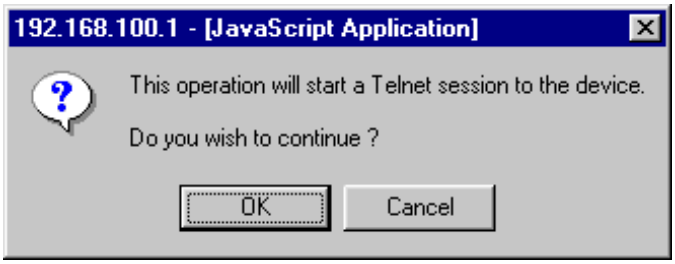
System Telnet Connect

Starting a Telnet Session

You can start a Telnet session to the unit using the Connect window.

To start a Telnet session:

1. Click *Device View* on the Toolbar.
2. Select **System -> Telnet -> Connect** in the Navigation Tree.
3. The following window is displayed.



4. To launch the Telnet session, click *OK*.

Back to Top

System Unit Alert LED

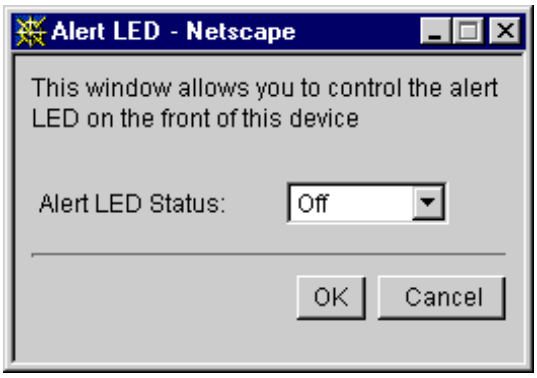
Changing the State of the Alert LED

You can set the status of the Alert LED using the Alert LED window.

The Alert LED can be set to *Flashing* or to *Off*. When set to *Flashing* the Alert LED on the front of the unit will flash on and off twice every second. This enables a particular unit to be identified within a stack. The default state for the Alert LED is *Off*.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Unit -> Alert LED** in the Navigation Tree;
3. The Alert LED window is displayed.



4. Select *Flashing* or *Off* from the Alert LED dialog box.
5. Click *OK* the set the state of the Alert LED or *Cancel* to exit without changing the state of the Alert LED.

Related Operations

Name	Specifying a Descriptive Name
Notepad	Entering Notes About the Unit

Back to Top

System Unit Name

Specifying a Descriptive Name

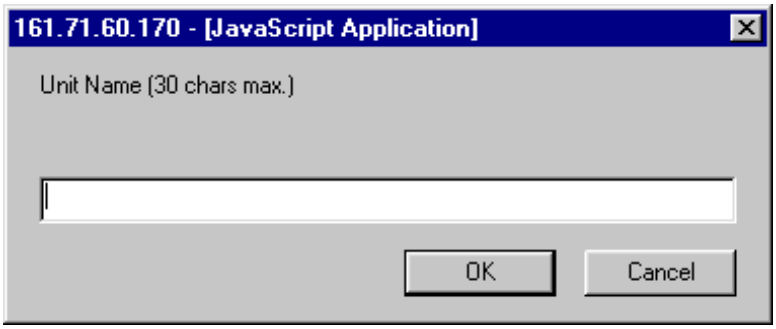
You can specify a descriptive name for the unit using the Name window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Unit -> Name** in the Navigation Tree;

   or

   Click any grey area on the Switch graphic and select *Name*.
3. The Unit Name window is displayed.



4. Enter a descriptive name for the unit in the Unit Name field. The name can be up to 30 characters long.

Related Operations

Alert LED	Setting the State of the Alert LED
Notepad	Entering Notes About the Unit

Back to Top

System Unit Notepad

Entering Notes About the Unit

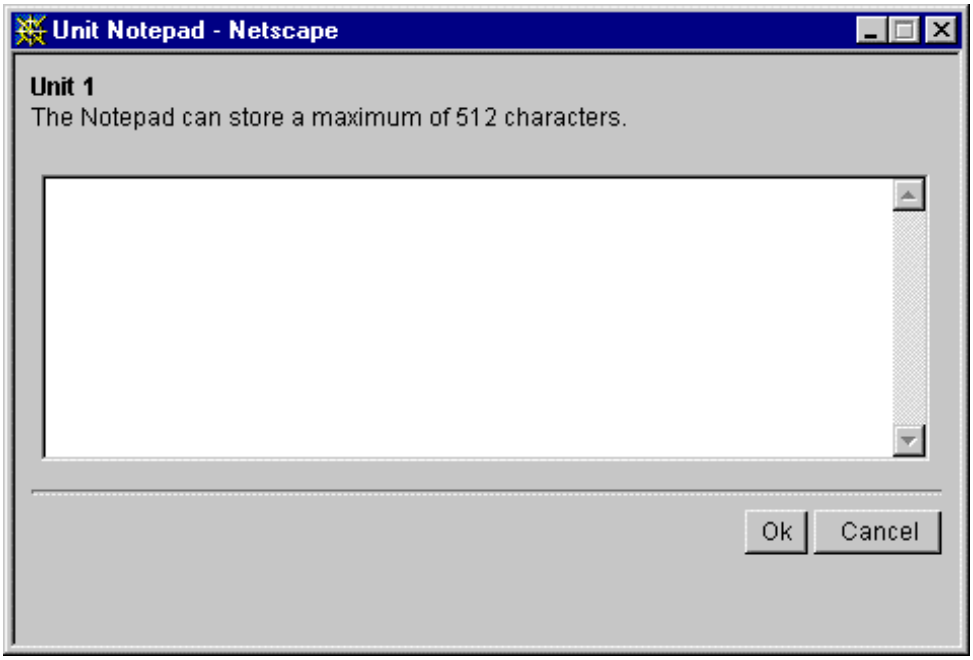
You can enter notes about the unit using the Notepad window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **System -> Unit -> Notepad** in the Navigation Tree;

   or

   Click any grey area on the Switch graphic and select *Notepad*.
3. The Notepad window is displayed.



4. The Notepad window allows you to enter up to 512 characters.
5. To save the text that you have entered, click *OK*.

Related Operations

Alert LED	Setting the State of the Alert LED
Name	Specifying a Descriptive Name

Back to Top

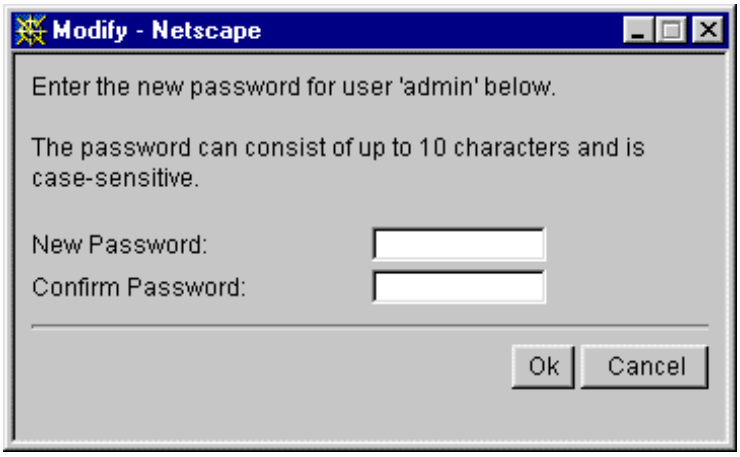
Security Device User Modify

Changing Your Password

You can change the password for your user using the Modify window.

To access the window:

1. Click *Device View* on the Toolbar.
2. Select **Security -> Device -> User -> Modify** in the Navigation Tree.
3. The Modify window is displayed.



The Modify window contains the following elements:

New Password:
Allows you to enter a new password for your user. The password can be up to 10 characters long and is case-sensitive.

Passwords must only contain alpha-numeric characters.

Confirm Password:
Allows you to re-enter the new password. The password does not change unless you enter it in this field.

Back to Top