Remote Supervisor Adapter User's Guide

for the IBM eserver xSeries 330

Remote Supervisor Adapter User's Guide

for the IBM eserver xSeries 330

Note: Before using this information and the product it supports, be sure to read the general information in Appendix B, “Notices,” on page 57.

Third Edition (May 2001)

Contents

Chapter 1. Introduction

This manual explains how to use the functions of the IBM® Remote Supervisor Adapter when you install it in an IBM @server xSeries 330 server. The IBM Remote Supervisor Adapter is one of the Advanced System Management (ASM) products. This Remote Supervisor Adapter provides around-the-clock remote access and system management of your server and supports the following:

- Remote management independent of the server status
- Remote control of hardware and operating systems
- Web-based management with standard Web browsers (no other software is required)
- Text-based user interface

You can use the ASM Web interface or text-based interface to access the Remote Supervisor Adapter. This manual refers to either the ASM Web interface or the text-based interface for the Remote Supervisor Adapter, depending on the context.

When configuring or managing systems that have both a Remote Supervisor Adapter and an ASM processor (such as the xSeries 330), the ASM processor manages the server, and the Remote Supervisor Adapter provides a Web interface and text-based interface to both components, and acts as an Ethernet network gateway. All system-management information generated by the ASM processor is transmitted to the Remote Supervisor Adapter using the ASM interconnect module connection between the processor and the adapter. The adapter then forwards this information to other systems on the Ethernet network or uses its modem to forward this data using a serial connection. All system-management settings for the server must be configured through the ASM processor. Use the Access Remote ASM feature provided by the Remote Supervisor Adapter to log in to the ASM processor of the server. For more information see, Chapter 2, “Logging into and using the ASM Web interface,” on page 3.

Remote Supervisor Adapter features

When you install a Remote Supervisor Adapter in a server that has an ASM processor, you will have access to the following features:

- Continuous health monitoring and control
- Battery-backed event log showing time-stamped entries
- Remote power control
- Remote firmware update
- Access to critical server settings
- Automatic notification and alerts
- Remote access through Ethernet, point-to-point protocol (PPP), serial, and the ASM interconnect peer-to-peer network
- Simple Network Management Protocol (SNMP) traps
- E-mail alerts
- Alphanumeric or numeric pager alerts
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- Remote power control

- Remote firmware update
- Access to critical server settings
- Text-based user interface terminal access
- Web-based management

Web browser requirements

The ASM Web interface supports the following Web browsers:

- Microsoft® Internet Explorer version 4.0 (with Service Pack 1), or later
- Netscape Navigator version 4.72, or later (version 6.0 is not supported)

The ASM Web interface has the following browser-related requirements:

- Java™ enabled Web browser (see your browser documentation or online Help for instructions about enabling its Java support)
- JavaScript version 1.2, or later (see your browser documentation or online Help for instructions about enabling its JavaScript support)
- HTTP version 1.0, or later
- Minimum display resolution of 800 x 600 with 256 colors

Note: The ASM Web interface and the ASM text-based interface do not support the double byte character set (DBCS) languages.

Notices and statements used in this book

This book contains certain notices to highlight important information.

The notices and their definitions are as follows:

- **Note**: These notices provide important tips, guidance, or advice.
- **Important**: These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention**: These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.

Chapter 2. Logging into and using the ASM Web interface

There are certain features of the ASM Web interface and text-based interface that are available only through the ASM processor that is on your server. You must first log into the Remote Supervisor Adapter and then log into the ASM processor to access these features. This chapter describes the login procedures and the features and functions that are available, depending upon whether you are logged into the Remote Supervisor Adapter or the ASM processor. To log into the ASM processor directly, see “Accessing the ASM processor features” on page 6.

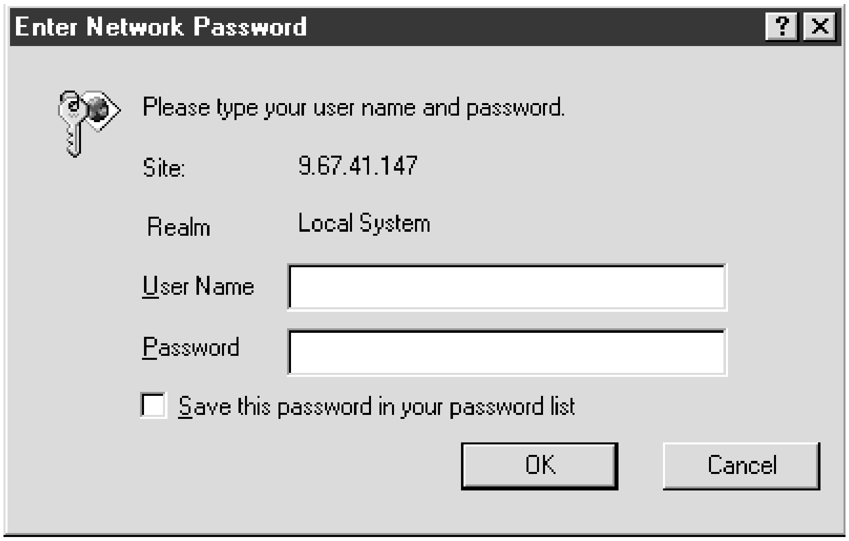
Logging into the Remote Supervisor Adapter

This section explains the features that are accessible when you are logged into the Remote Supervisor Adapter. When you are logged into the Remote Supervisor Adapter and then log into the ASM processor, some of these features are enhanced. To log into the Remote Supervisor Adapter using the ASM Web interface, complete the following steps:

1. Open a Web browser. In the address or URL field, type the IP address or host name of the Remote Supervisor Adapter to which you want to connect.

   The Enter Network Password window opens.

   Note: The values in the following window are examples. Your settings are different.



Enter Network Password

Please type your user name and password.

Site: 9.67.41.147

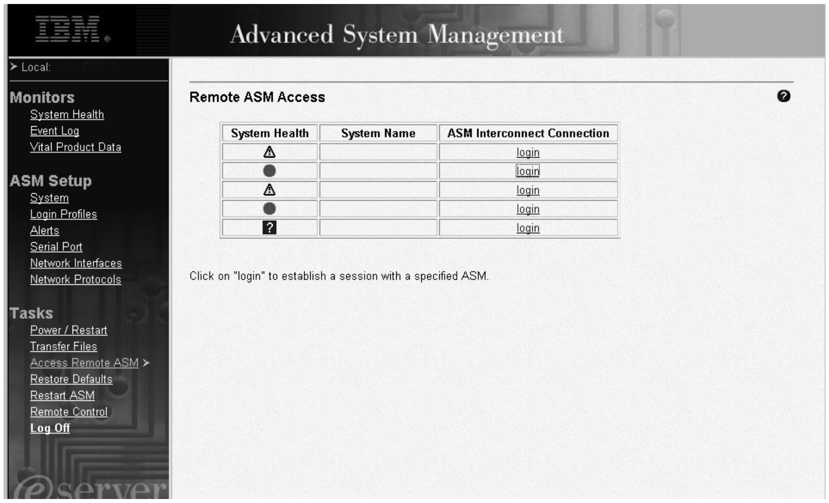
Realm Local System

2. In the Enter Network Password screen, type your user name and password. If you are using the Remote Supervisor Adapter for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. A welcome page opens in your browser.

   Note: The Remote Supervisor Adapter is set initially with a user name of USERID and password of PASSW0RD (with a zero, not an O). This user has read/write access. Change this default during your initial configuration for enhanced security.

3. Select a timeout value, in minutes, in the field provided. If your browser is inactive for the number of minutes you select, the Remote Supervisor Adapter logs you off the Web interface.

4. Click **Continue** to start the session. The browser opens the Remote ASM Access home page.



Remote ASM Access

System Health	System Name	ASM Interconnect Connection
⚠		login
●		login
⚠		login
●		login
?		login

Click on "login" to establish a session with a specified ASM.

You are now logged into the Remote Supervisor Adapter. You have access to the following features through the links provided on the navigation frame:

Note: When you are logged into a Remote Supervisor Adapter or an ASM processor, the link names used by the Web interface are identical; however, the information and functions supported are different. In the following list, these features are explained as they function when you are logged into the Remote Supervisor Adapter.

System Health
You can monitor the power and restart, temperature, voltage, and fan status of your server on the System Health page. This information is available after you log into the ASM processor.

Event Log
The event log page contains information specific to the Remote Supervisor Adapter such as remote access attempts and dial-out events. All events in the log are time-stamped using the ASM date and time settings.

Vital Product Data
You can view information about the Remote Supervisor Adapter firmware levels from the Vital Product Data page.

System
You can configure information about the Remote Supervisor Adapter, such as its name, contact, and location information from the System page.

Login Profiles
You can define up to 12 login profiles that allow access to the Remote Supervisor Adapter from the Login Profiles page.

Alerts
The Remote Supervisor Adapter forwards alerts generated by the ASM processor. It does not generate alerts on its own. You can configure forwarding settings for alerts from the Alerts page.

Serial port
You can configure the serial port and modem settings used by the Remote Supervisor Adapter from the Serial Port page.

Note: The serial port used by the Remote Supervisor Adapter is different from the serial ports used by the ASM processor. The Remote Supervisor Adapter has a dedicated serial port.

Network Interfaces

You can configure network access settings to the Remote Supervisor Adapter from the Network Interfaces page. The Remote Supervisor Adapter supports both Ethernet and point-to-point protocol (PPP) connections thereby allowing remote access using a Web browser or TELNET application.

Network Protocols

You can configure Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP) settings used by the Remote Supervisor Adapter from the Network Protocols page.

Power/restart

The ASM processor provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability. These features are accessed from the Power/Restart page. This information is available after you log into the ASM processor.

Transfer Files

You can update the firmware of the Remote Supervisor Adapter from the Transfer Files page. You can also back up, modify, and restore the configuration of the Remote Supervisor Adapter from this page.

Access Remote ASM

You can view a list of the ASM processors, ASM PCI adapters, and Remote Supervisor Adapters present on the same ASM interconnect network and establish a connection to any of those systems. Use this page to log into the ASM processor within a given server.

Restore Defaults

You can reset the Remote Supervisor Adapter configuration to the factory defaults from this page.

Remote Control

This feature might not be available on all products.

Restart ASM

You can restart the Remote Supervisor Adapter from this page.

Log Off

This link logs you off of the Remote Supervisor Adapter and ends your Web management session.

Note: The following links, although visible in the navigation frame of the Web interface, are not supported by the Remote Supervisor Adapter and you must access them when logged into the ASM processor. You must first log into the Remote Supervisor Adapter and then log into the ASM processor through the Access Remote ASM link on the Advanced System Management home page to manage these features:

- System Health
- Power/Restart

You can click the **View Configuration Summary** link which appears on most pages, to quickly view the configuration of the Remote Supervisor Adapter.

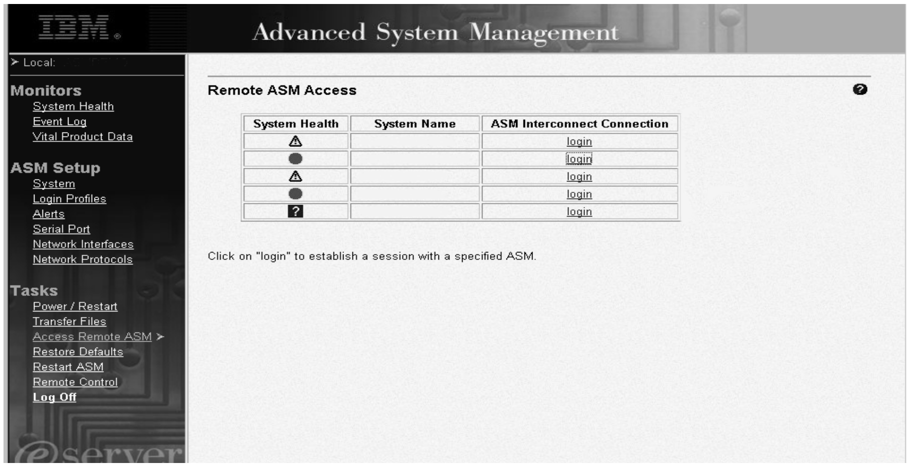
Accessing the ASM processor features

When you initially log into the ASM Web interface of the Remote Supervisor Adapter, you can view a list of the ASM processors, ASM adapters, and Remote Supervisor Adapters in the same interconnect network and in the local system that contains the Remote Supervisor Adapter.

The ASM processor in the xSeries 330 enables you to monitor system health, view the server event log and vital product data, configure alerts and alert recipients, and perform power and restart operations.

To log into an ASM processor through the Remote Supervisor adapter, do the following:

1. If you did not already do so, log into the Remote Supervisor Adapter through the ASM Web interface (see “Logging into the Remote Supervisor Adapter” on page 3).
2. In the navigation frame, click **Access Remote ASM.** The Remote ASM Access page opens.



Remote ASM Access

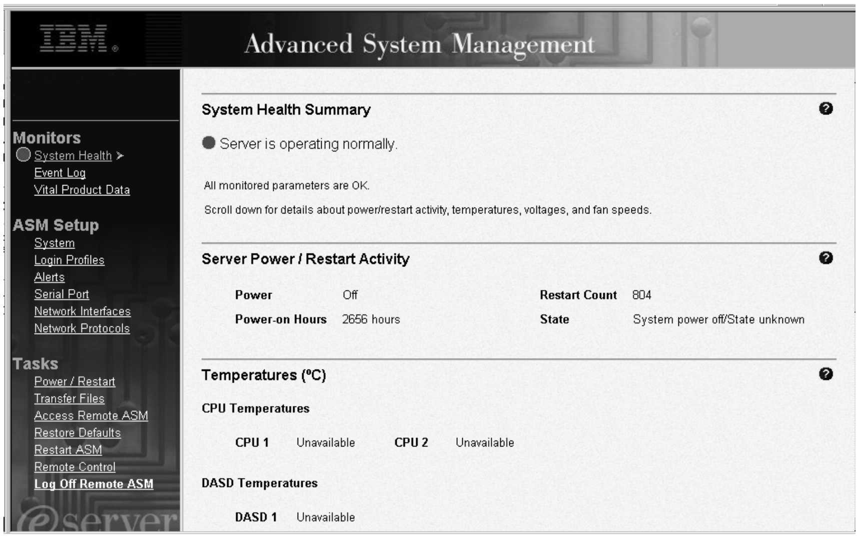
System Health	System Name	ASM Interconnect Connection
⚠		login
●		login
⚠		login
●		login
?		login

Click on "login" to establish a session with a specified ASM.

3. In the ASM Interconnect Connection column, for the entry that matches the ASM processor of the server that you want to monitor, click **login**.

   Note: It is important that you name the ASM processor of each server meaningful names so that you can easily identify the correct server to monitor. The name of the processor is what you select from the table in the ASM Interconnect column. If you are not sure of the name of the ASM processor for the server that you want to monitor, log into each ASM processor individually and view the vital product data (VPD) to determine the serial number of the server in which that ASM processor is located.

4. Log into remote ASM. The System Health page is displayed and shows the system health, system name, and enables you to log into an ASM processor.



System Health Summary

● Server is operating normally.

All monitored parameters are OK.

Scroll down for details about power/restart activity, temperatures, voltages, and fan speeds.

Server Power / Restart Activity

Power	Off	Restart Count	804
Power-on Hours	2656 hours	State	System power off/State unknown

Temperatures (ºC)

CPU Temperatures

CPU 1	Unavailable	CPU 2	Unavailable

DASD Temperatures

DASD 1	Unavailable

The following features are explained as they function when you are logged into the ASM processor. After you log into the ASM processor, you have access to the following features:

System Health
You can monitor the power and restart, temperature, voltage, and fan status of your server on the System Health page.

Event Log
The event log page contains entries that are currently stored in the system event log and POST event log. Information about all remote access attempts and dial-out events that occurred are recorded in the event log. All events in the log are time-stamped using the ASM processor date and time settings. Some events will also generate an alert if configured to do so on the alerts page.

Vital Product Data
Upon server startup, the ASM processor collects system and basic input/output system (BIOS) code, and server component vital product data (VPD) and stores it in nonvolatile memory. This data is available from the Vital Product Data page.

System
You can configure general information such as the name of the ASM processor, contact information, server location, and server time-out settings from the System page.

Login profiles
You can define 12 login profiles that enable access to the ASM processor. For more information on defining login profiles, see “Creating a login profile” on page 17.

Alerts
You can configure the ASM processor to generate and forward alerts for a number of different events. You can configure the alerts that are monitored and the recipients that are notified on the Alerts page. For more information on configuring remote alert recipients and the alerts to send, see “Setting remote alert attempts” on page 18.

Serial port
You can configure the serial ports and modem settings used by the ASM processor from the Serial Port page. For more information on the serial port, see “Configuring the serial port” on page 19.

Note: The serial ports used by the ASM processor are different from the serial port provided on the Remote Supervisor Adapter. The ASM processor uses the serial ports of the server. One of those serial ports can either be shared with the operating system running on the server or it can be dedicated to the ASM processor. The other port is always dedicated to the ASM processor.

Power/restart

The ASM processor provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability. These features are accessed from the Power/Restart page.

Transfer files

Use the options on the Transfer Files page to update firmware of the ASM processor, server BIOS code, and server diagnostics.

Remote Control

This feature might not be available on all products.

Restore defaults

Attention: When you click **Restore Defaults**, all of the modifications you made to the Remote Supervisor Adapter are lost.

You can reset the Remote Supervisor Adapter to its original factory settings. If you click **Restore Defaults**, you will lose your TCP/IP connection to the server where the Remote Supervisor Adapter is installed, and you must reconfigure the network interface locally using the configuration utility (or through the text-based user interface if serial port access is available).

For more information on restoring defaults, see “Restoring ASM defaults” on page 32.

Restart ASM

Attention: When you click **Restart ASM**, you will lose all the modifications you made to the Remote Supervisor Adapter. You also lose remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS setup.

You can restart the ASM processor. However, you will lose your configured connections and data if you do so. For more information on restoring defaults, see “Restarting ASM” on page 32.

Log off Remote ASM

This link logs you off from your connection to the ASM processor and return to the Remote Supervisor Adapter that originated the remote session. For more information on logging off, see “Logging off” on page 32.

Note: The following links, although visible in the navigation frame of the ASM Web interface, are not supported by the ASM processor and instead must be accessed when logged into the Remote Supervisor Adapter:

- Network Interfaces
- Network Protocols
- Access Remote ASM
- Remote Control

You can click the **View Configuration Summary** link which appears on most pages, to quickly view the configuration of the ASM procesor.

Chapter 3. Monitoring the status of remote servers

Use the links under the Monitors heading of the navigation frame to view the status of the server you access.

From the Event Log page, you can:

- View certain Advanced System Management events recorded in the Event Log of the Remote Supervisor Adapter
- View the severity of events

From the Vital Product Data (VPD) page, you can:

- View the vital product data of the ASM and the server in which it is installed

Monitoring the remote server status

You can monitor the power and restart, temperature, voltage, and fan status of your server on the System Health Summary page.

1. Log into the Web interface of the Remote Supervisor Adapter.
2. In the navigation frame, click **Access Remote ASM**.
3. Log into the remote ASM processor. In the ASM Interconnect Connection column, for the table entry that corresponds to the ASM processor of the server that you want to monitor, click **login**. The System Health page is displayed.

   Note: It is important that you name the ASM processor of each server meaningfully so that you can easily identify the ASM processor that you want to access.
4. The status of your server determines the message shown at the top of the System Health Summary page. One of the following headers will appear:
   - `Server is operating normally`
   - `One or more monitored parameters are abnormal`

   The monitored parameters are operating normally if you get the Server is operating normally message and a solid green circle appears.

   The monitored parameters are operating outside normal ranges if you get the One or more monitored parameters are abnormal message. A list of the specific abnormal parameters displays under one or both of the following:

   Critical events
   A red circle containing an “X” appears. The critical events and errors are listed.

   Warnings and System Events
   A yellow triangle containing an exclamation point appears. The Warnings and System Events section lists all warnings received or detected by the Remote Supervisor Adapter from the server.
5. Scroll down to the Server Power/Restart Activity section, which gives the current power status of the system.

   Power
   Indicates the power status of the server.

   Power-on Hours
   Indicates the cumulative number of hours that the server has been turned on.

Restart Count

Indicates the total number of times the server has been restarted.

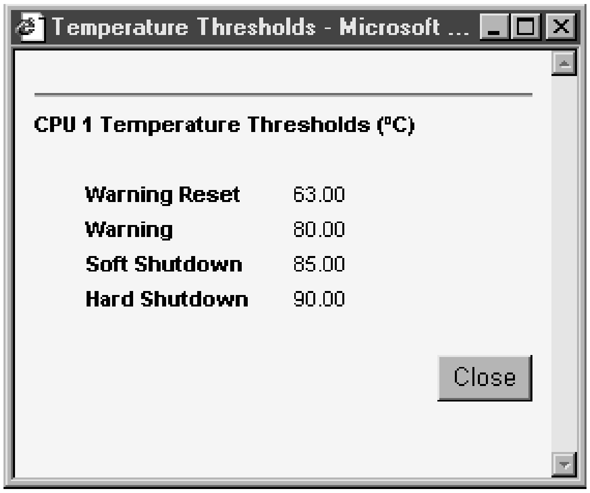
State

Displays the state of the operating system when this Web page was generated. Possible states include:

- `System power off/State unknown`
- `In POST`
- `Stopped in POST (Error detected)`
- `Booted Flash or unknown o/s`
- `Booting OS or in OS (Could be in the OS if the OS or application does not report the new system state.)`
- `In OS`
- `CPU’s held in reset`

6. Scroll down to the Temperatures section. The Remote Supervisor Adapter tracks the current temperature readings and threshold levels for system components such as microprocessors, system board, and hard disk drive backplane.

   If you click a temperature reading, a window similar to the following opens:



CPU 1 Temperature Thresholds (ºC)

Warning Reset	63.00
Warning	80.00
Soft Shutdown	85.00
Hard Shutdown	90.00

The Temperature Thresholds window displays the temperature levels at which the Remote Supervisor Adapter reacts. These levels are preset on the remote server and cannot be changed.

The reported temperature for the CPU, hard disk drive, and system is measured against the following threshold ranges:

Warning

If a temperature reaches a specified value, a temperature warning is sent to remote alert recipients. You must select the **Temperature** option on the Alerts page for the warning to be sent.

Soft Shutdown

Attention: For the operating system on the remote server to receive the shutdown notification from its ASM processor, the remote server must have the IBM System Management device driver installed as well as the IBM Director with UM Server Extensions, or IBM Director with UM Server Extensions for the ASM component. See the documentation that comes with your remote system for instructions on installing the software.

If a temperature reaches a specified value higher than the specified soft shutdown warning value, a second temperature warning is sent to remote alert recipients and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Temperature** option on the Alerts page for the warning to be sent.

Hard Shutdown

Attention: For the operating system on the remote server to receive the shutdown notification from its ASM processor, the remote server must have the IBM System Management device driver installed as well as the IBM Director with UM Server Extensions, or IBM Director with UM Server Extensions for the ASM component. See the documentation that comes with your remote system for instructions on installing the software.

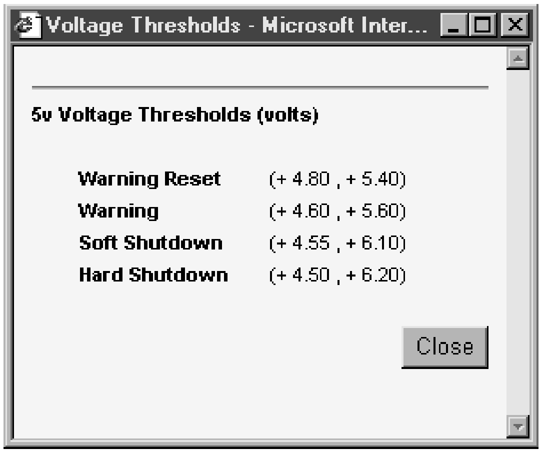
If a temperature reaches a value higher than the specified hard shutdown value, the system immediately shuts down and sends an alert to configured recipients. You must select the **Temperature** option on the Alerts page for the warning to be sent.

Warning Reset

If the temperature returns to any value below the warning reset value, and if a warning was sent, the server assumes the temperature has returned to normal and no further alerts will be generated.

7. Scroll down to the Voltages section. The Remote Supervisor Adapter will send an alert if any monitored power source voltage falls outside their specified operational ranges.

If you click a voltage reading, a window similar to the following opens:



5v Voltage Thresholds (volts)

Warning Reset	(+ 4.80 , + 5.40)
Warning	(+ 4.60 , + 5.60)
Soft Shutdown	(+ 4.55 , + 6.10)
Hard Shutdown	(+ 4.50 , + 6.20)

The Voltage Thresholds window displays the voltage ranges at which the Remote Supervisor Adapter reacts. These levels are preset on the remote server and cannot be changed.

The ASM Web interface displays the voltage readings of the system board and the voltage regulation modules (VRM). The system sets a voltage range at which the following actions are taken:

Warning

If the voltage drops below or exceeds a specified voltage range, a voltage warning is sent to remote alert recipients. You must select the **Voltage** option on the Alerts page for the warning to be sent.

Soft Shutdown

If the voltage drops below or exceeds a specified voltage range, a voltage warning is sent to remote alert recipients and the server begins the shutdown process with an orderly OS shutdown. The server then turns itself off. You must select the **Voltage** option on the Alerts page for the warning to be sent.

Hard Shutdown
If the voltage drops below or exceeds a specified voltage range, the system immediately shuts down and sends an alert to configured recipients. You must select the **Voltage** option on the Alerts page for the warning to be sent.

Warning Reset
If the voltage drops below or exceeds the warning voltage range and then recovers to that range, the server assumes the voltage has returned to normal and generates no further alerts.

8. Scroll down to the Fan Speeds (percent of maximum) section. The ASM Web interface displays the running speed of the system fans (expressed in a percentage of the maximum fan speed). You receive a fan warning (Multiple Fan Failure or Single Fan Failure) if the fan speeds drop to an unacceptable level or stop. You must select the fan options on the Alerts page for the warning to be sent.

Viewing the event log

The Event Log window contains all entries that are currently stored in the System Error log and Post Error log. Information about all remote access attempts and dial-out events is recorded in the adapter or processor event log. The Remote Supervisor Adapter time-stamps all events and logs them into the event log, sending out the following alerts, if configured to do so by the system administrator:

- Event log 75% full
- Event log full

The event log has a limited capacity. When that limit is reached, the older events are deleted in a first-in, first-out order.

Complete the following steps to access and view the event log:

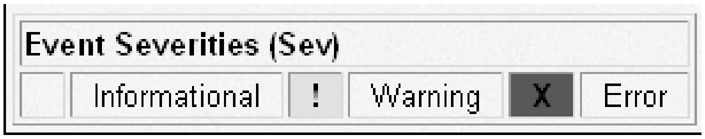
1. In the navigation frame, click the **Event Log** link to view the recent history of events that occured in the server.
2. Scroll down to view the complete contents of the event log. The events are given the following levels of severity:

Informational
This severity level is assigned to an event of which you should take note.

Warning
This severity level is assigned to an event that could affect server performance.

Error This severity level is assigned to an event that needs immediate attention.

The ASM Web interface distinguishes warning events with a yellow exclamation mark (!) in the severity column and error events with a red X.



Event Severities (Sev)					
	Informational	!	Warning	X	Error

Viewing vital product data

Upon server startup, the Remote Supervisor Adapter collects system information. You can access this information at any time from almost any computer. The Vital Product Data page contains key information about the system that the Remote Supervisor Adapter is monitoring.

1. In the navigation frame, click **Vital Product Data** to view the status of the hardware and software components on the server.

   Note: You can only view the ASM vital product data using the Remote Supervisor Adapter. To view all others such as the POST/BIOS data and the Component Activity Log, you need to go through the ASM processor.

2. Scroll down to view the following readings:

   Remote Supervisor Adapter system data
   You can find the VPD for the Remote Supervisor Adapter in this section.

Table 1. Remote Supervisor Adapter vital product data.

Field	Function
Build ID	Identifies the build IDs of the application firmware and the startup ROM firmware.
Revision	Identifies the revision numbers of the application firmware and the startup ROM firmware.
File name	Identifies the file names of the application firmware and the startup ROM firmware.
Release date	Identifies the release dates of the application firmware and the startup ROM firmware.

Chapter 4. Configuring your Remote Supervisor Adapter

Use the links under the ASM Setup heading in the navigation frame to configure your Remote Supervisor Adapter values.

From the System page, you can:

- Set system information
- Set ASM date and time

From the Login Profiles page, you can:

- Set login profiles to control access to the Remote Supervisor Adapter
- Configure modem and dial-in settings

From the Alerts page, you can:

- Set the number of remote alert attempts
- Select the delay between alerts
- Configure alerts on the ASM processor

From the Serial Port page, you can:

- Configure the serial port of the Remote Supervisor Adapter
- Configure advanced modem settings

From the Network Interfaces page, you can:

- Set up an Ethernet connection to the Remote Supervisor Adapter
- Set up a PPP over serial port connection to the Remote Supervisor Adapter

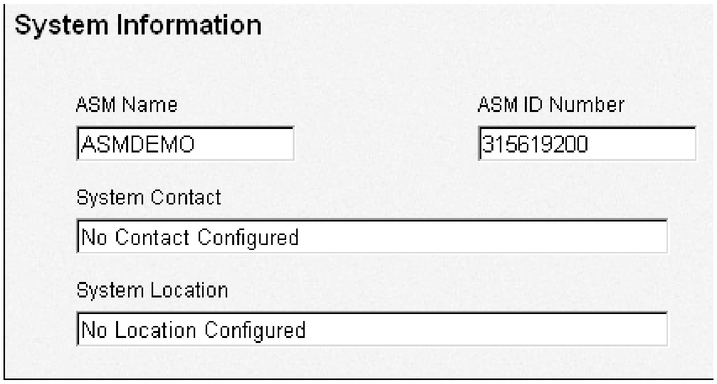
From the Network Protocols page, you can:

- Configure SNMP setup
- Configure DNS setup
- Configure SMTP setup

Setting system information

Complete the following steps to set your Remote Supervisor Adapter system information:

1. In the navigation frame, click **System**. A window similar to the following opens:



System Information

ASM Name: ASMDEMO

ASM ID Number: 315619200

System Contact: No Contact Configured

System Location: No Location Configured

2. In the ASM Name field, type the name of the Remote Supervisor Adapter.

   Use the ASM Name field to specify a name for the Remote Supervisor Adapter in this server. The name is included with e-mail, SNMP, and alphanumeric pager alert notifications to identify the source of the alert.

   Note: Your Remote Supervisor Adapter name (the ASM Name field) and the IP host name of the Remote Supervisor Adapter (the Hostname field on the Network Interfaces page) do not automatically share the same name because the ASM Name field is limited to 15 characters. The Hostname field can consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP host name. The non-qualified IP host name consists of up to the first period of a fully qualified IP hostname. For example, the non-qualified IP host name of `asmcard1.us.company.com` (a fully qualified IP host name) is `asmcard1`. For more information on your host name, see “Configuring an Ethernet connection to ASM” on page 21.

3. In the ASM ID Number field, assign the Remote Supervisor Adapter a unique identification number.
4. In the System Contact field, type contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.
5. In the System Location field, type the location of the server. Include in this field sufficient detail to quickly locate the server for maintenance or other purposes. You can type a maximum of 47 characters in this field.

Setting ASM date and time

The Remote Supervisor Adapter includes its own real-time clock to independently time-stamp all events that are logged in the battery-backed event log. Alerts, sent by e-mail, LAN, and SNMP, use the real-time clock setting to time stamp the alerts. The clock settings support Greenwich mean time (GMT) offsets and daylight saving time (DST) for added ease-of-use for administrators managing systems remotely over different time zones. You can remotely access the battery-backed event log even if the system is turned off or otherwise disabled. This facilitates immediate problem determination and resolution.

Complete the following steps to check the settings of the date and time processor on the Remote Supervisor Adapter, which is independent of the date and time settings of the clock on the server system board:

1. In the navigation frame, click **System**.
2. Scroll down to the ASM Date and Time section, which shows the date and time when this Web page was generated.

   Automatic Daylight Savings Time Update
   Use the Automatic Daylight Savings Time Update field to specify whether the Remote Supervisor Adapter clock will automatically adjust when DST changes.

   GMT offset
   Use the GMT Offset field to specify the offset from GMT corresponding to the time zone where this server is located.

   To set the time field, type the numbers corresponding to the current hour, minutes, and seconds in the appropriate text boxes. The hour (hh) must be a number from 0 to 23 as represented on a 24-hour clock. The minutes (mm) and seconds (ss) must be numbers from 0 to 59.
3. Click **Set Clock** to override the date and time settings, as well as enable DST and set the GMT offset.

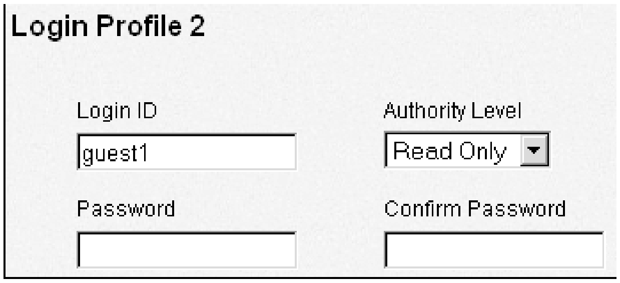
   To set the Date, type the numbers corresponding to the current month, day, and year in the appropriate text boxes.
4. Click **Save**.

Creating a login profile

Complete the following steps to configure a login profile:

1. In the navigation frame, click **Login Profiles**.

   Use this page to view, configure, or change individual login profiles. You can define up to 12 unique profiles. If you have not configured a profile, the name of the profile link by default will be User *nn* where *nn* is an arbitrary number assigned to that profile.
2. Click one of the User nn login profile links. An individual profile page opens:



Login Profile 2

Login ID: guest1

Authority Level: Read Only

Password:

Confirm Password:

3. In the Login ID field, type the name of the profile.

   You can type a maximum of 15 characters in the Login ID field. Valid characters are uppercase and lowercase letters, numbers, periods, and underscores.

   Note: This login ID is used to grant remote access to the Remote Supervisor Adapter.
4. In the Authority Level field, select either **Read Only** or **Read/Write** to set the access rights for this login ID.

Read-Only

The Read-Only option enables the user to view a page but not make changes. Additionally, users who log in with read-only IDs are restricted from performing any file transfers, power and restart actions, or remote control functions.

Read/Write

The Read/Write option enables the user to take any action provided by the interface, including setting up a user ID and turning off the server.

5. In the Password field, assign a password for the login ID.

   Valid passwords must contain at least five characters, one of which must be a nonalphabetic character. Null, or empty, passwords are accepted.

   Note: This password is used with the login ID, to grant remote access to the Remote Supervisor Adapter.

6. In the Confirm Password field, type the password again.
7. To configure the Remote Supervisor Adapter to automatically terminate a successful dial-in attempt and then immediately dial-out to a specified number, in the Status field of the Dialback Settings section, select **Enabled**. Otherwise, go to step 9.

   Note: If this menu is enabled, you must type a phone number in the Number field of this profile.

8. In the Number field, type the phone number for the Remote Supervisor Adapter to use when dialing back to reach the login ID.

   This phone number is dialed when the user defined in this profile successfully logs into the Remote Supervisor Adapter.

   Note: By default, the Remote Supervisor Adapter comes configured with one login profile that enables remote access using a login user ID of USERID and a password of PASSW0RD (the 0 is a zero). To avoid a potential security exposure, change this default login profile during initial setup of the Remote Supervisor Adapter.

9. Click **Save** to save your login ID settings.

Setting the modem and dial-in settings

Complete the following steps to enable your modem to dial out to the remote login profile:

1. In the navigation frame, click **Login Profiles**.
2. Scroll down to the Modem and Dial-in Settings section.
3. If you want to allow remote users to dial into the Remote Supervisor Adapter through a serial connection, in the Dial-in Support Status field, select **Enabled**.
4. In the **Delay Before Next Remote Login** field you can specify how long, in minutes, the Remote Supervisor Adapter will prohibit remote login attempts, if more than five sequential failures to log in remotely are detected.

Setting remote alert attempts

Complete the following steps to set the number of times the Remote Supervisor Adapter attempts to send an alert:

1. In the navigation frame, select **Alerts**.
2. Scroll down to the Remote Alerting Attempts section.

Use these settings to define the number of remote alert attempts and the time between the attempts. The settings apply to all configured remote alert recipients.

Remote alert retry limit

Use the **Remote Alert Retry Limit** field to specify the number of additional times that the Remote Supervisor Adapter will attempt to forward an alert to an alphanumeric pager. All other notification methods are attempted only once.

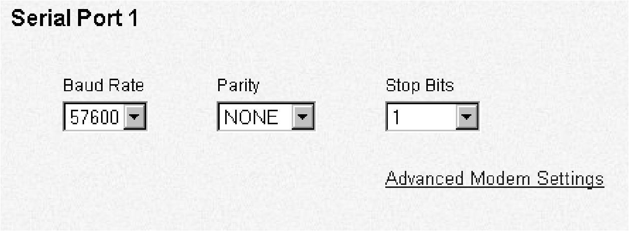
Delay between retries

Use the **Delay Between Retries** field to specify the time interval (in minutes) that the Remote Supervisor Adapter will wait between retries to send an alert.

3. Click **Save**.

Configuring the serial port

The Remote Supervisor Adapter enables a single serial port to conduct normal functions and also maintain out-of-band alerting capabilities.



Serial Port 1

Baud Rate: 57600

Parity: NONE

Stop Bits: 1

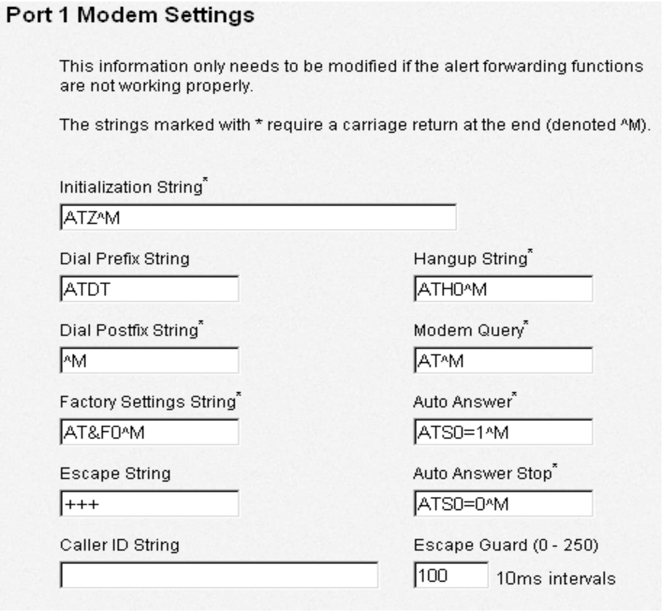
Complete the following steps to configure your serial port setup. For more information on your serial port, see “Configuring PPP access over a serial port” on page 24.

1. In the navigation frame, click **Serial Port**.
2. In the Baud Rate field, select a **data transfer rate**.

   In the Baud Rate field you can specify the data transfer rate of your serial port connection. To set the baud rate, select the data transfer rate in bits per second that corresponds to your serial port connection.
3. In the Parity field, select the error detection to use in your serial connection.

   In the Parity field, you can specify the error detection bit 0 or 1 added to each group of transmitted bits so that it will have either an odd or even number of 1s. This enables your server to know whether received data has been corrupted during transmission.
4. Select the number of data-terminating 1 bit in the Stop Bits field that follows the data or any parity bit to mark the end of a transmission (normally a byte or character).

   Note: The number of data bits is preset to 8 and cannot be changed.
5. Click **Save**.
6. If you need to set advanced settings, click the **Advanced Modem Settings** link.



Port 1 Modem Settings

This information only needs to be modified if the alert forwarding functions are not working properly.

The strings marked with * require a carriage return at the end (denoted ^M).

Initialization String*
ATZ^M

Dial Prefix String
ATDT

Hangup String*
ATH0^M

Dial Postfix String*
^M

Modem Query*
AT^M

Factory Settings String*
AT&F0^M

Auto Answer*
ATS0=1^M

Escape String
+++

Auto Answer Stop*
ATS0=0^M

Caller ID String

Escape Guard (0 - 250)
100 10ms intervals

Set these values only if the alert forwarding functions are not working properly. The strings marked with an asterisk (*) require a carriage return (^M) to be typed at the end of the field value.

Table 2. Port 1 settings.

Field	What you enter
Initialization string	Type the initialization string that will be used for the specified modem. A default string is provided (ATE0). Do not change this string unless your dial-out functions are not working properly.
Dial prefix string	Type the initialization string that is used before the number to be dialed. The default is ATDT.
Dial postfix string	Type the initialization string that is used after the number is dialed to tell the modem to stop dialing. The default is ˆM.
Factory settings string	Type the initialization string that returns the modem to its factory settings when the modem is initialized. The default is AT&F0.
Escape string	Type the initialization string that returns the modem to command mode when it is currently talking to another modem. The default is +++.
Caller ID string	Type the initialization string that will be used to get caller ID information from the modem.
Hangup string	Type the initialization string that will be used to instruct the modem to disconnect. A default string is provided (ATH0). Do not change this string unless your dial-out functions are not working properly.
Modem query	Type the initialization string that is used to find out if the modem is attached. The default is AT.
Auto-answer	Type the initialization string that is used to tell the modem to answer the phone when it rings. The default is to answer after two rings or ATS0=1.
Auto-answer stop	Type the initialization string that is used to tell the modem to stop answering the phone automatically when it rings. The default is ATS0=0.

Table 2. Port 1 settings.

Field	What you enter
Escape guard (0 - 250)	Type the length of time before and after the escape string is issued to the modem. This value is measured in 10 millisecond intervals. The default value is 1 second.

7. Click **Save**.

Initialization-string guidelines

If you need to provide a new initialization string, refer to the documentation that came with your modem. Your initialization string must contain commands that configure your modem as follows:

- Command echoing OFF
- Online character echoing OFF
- Result codes ENABLED
- Verbal result codes ENABLED
- All codes and Connect messages with BUSY and DT detection
- Protocol identifiers added — LAPM/MNP/NONE V42bis/MNP5
- Normal CD operations
- DTR ON-OFF hang-up, disable AA and return to command mode
- CTS hardware flow control
- RTS control of receive data to computer
- Queued and nondestructive break, no escape state

Note: The abbreviations in these commands have the following meanings:

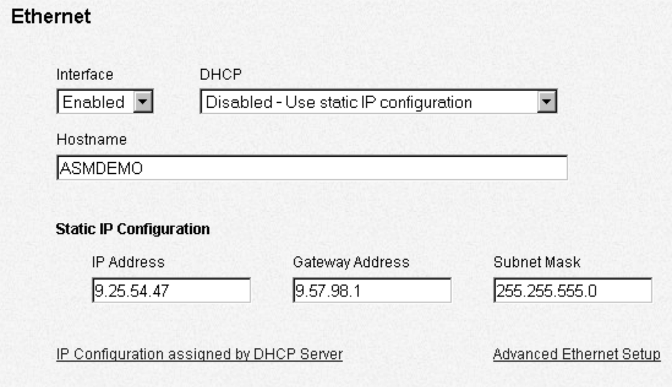
AA	auto answer
CD	carrier detect
CTS	clear to send
DT	data transfer
DTR	data terminal ready
LAPM	link access protocol for modems
MNP	microcom networking protocol
RTS	ready to send

Configuring an Ethernet connection to ASM

Complete the following steps to configure your Ethernet setup:

1. In the navigation frame, click **Network Interfaces**. A window similar to the following opens.

   Note: The values in the following window are examples. Your settings will be different.



Ethernet

Interface: Enabled

DHCP: Disabled - Use static IP configuration

Hostname: ASMDEMO

Static IP Configuration

IP Address: 9.25.54.47

Gateway Address: 9.57.98.1

Subnet Mask: 255.255.555.0

2. If you want to use an Ethernet connection, in the Interface field, select **Enabled**. It is enabled by default.
3. If you want to use a dynamic host configuration protocol (DHCP) server connection, enable the DHCP field. Review the following notes, and then proceed to step 10.

   Note: If DHCP is enabled, the Host Name field is used as follows:

   a. If the Host Name field is set, then the Remote Supervisor Adapter DHCP support will request the DHCP server to allow the use of this hostname.

   b. If the Host Name field is not set, then the Remote Supervisor Adapter DHCP support will request the DHCP server to assign a unique host name to the Remote Supervisor Adapter.

   c. If you enable this setting, you must have an accessible, active, and configured DHCP server on your network. Also, when DHCP is enabled, the automatic configuration will override any manual settings.
4. In the Hostname field, type the IP host name of the Remote Supervisor Adapter.

   You can type a maximum of 63 characters in this field, which represents the IP hostname of the Remote Supervisor Adapter. The hostname by default is “ASMA” followed by the burned-in MAC address of the server in which the ASM is installed.

   Note: The IP host name of the Remote Supervisor Adapter (the host name field) and Remote Supervisor Adapter name (the ASM Name field on the System page) do not automatically share the same name because the ASM Name field is limited to 15 characters. The Hostname field can consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP host name. The non-qualified IP hostname consists of up to the first period of a fully qualified IP host name. For example, the non-qualified IP host name of `asmcard1.us.company.com` (a fully qualified IP host name) is `asmcard1`. For more information on your host name, see “Setting system information” on page 16.
5. In the IP Address field, type the IP address of the Remote Supervisor Adapter. You must do this only if DHCP is disabled. The IP address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
6. In the Gateway Address field, type your network gateway router. You must do this only if DHCP is disabled. The gateway address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces or consecutive periods

7. In the Subnet Mask field, type the subnet mask used by the Remote Supervisor Adapter. You must do this only if DHCP is disabled. The subnet mask must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces or consecutive periods

   The default setting is 255.255.255.0.
8. Click the **Advanced Ethernet Setup** link if you need to set additional Ethernet settings.

Table 3. Advanced Ethernet setup.

Field	Function
Data rate	Use the Data Rate field to specify the amount of data to be transferred per second over your LAN connection. To set the data rate, click the menu and select the data transfer rate in megabits (Mb) that corresponds to the capability of your network. To automatically detect the data transfer rate, select **Auto**, which is the default value.
Duplex	Specify the type of communication channel used in your network in the Duplex field. To set the duplex mode, select one of the following: Full Enables data to be carried in both directions at once. Half Enables data to be carried in either one direction or the other, but not both at the same time. To automatically detect the duplex type, select Auto, which is the default value.
Maximum transmission unit	Use this field to specify the maximum size of a packet (in bytes) for your network interface. For Ethernet, the valid maximum transmission unit (MTU) range is 60 - 1500. The default value for this field is 1500.
Burned-in MAC address	The burned-in MAC address is a unique physical address assigned to this Remote Supervisor Adapter by the manufacturer. The address is also a read-only field.
Locally administered MAC address	Enter a physical address for this Remote Supervisor Adapter in the Locally Administered MAC Address field. If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value between 000000000000 - FFFFFFFFFFFF. This value must be in the form *XX*:*XX*:*XX*:*XX*:*XX*:*XX* where *X* is a number between 0 and 9. The Remote Supervisor Adapter does not support the use of a multicast address. A multicast address has the least significant bit of the first byte set to 1. The first byte, therefore, must be an even number.

9. Make modifications to the advanced Ethernet setup as necessary.
10. Click **Save**.
11. Click **Back** to return to the Network Interfaces page.

    If DHCP is enabled, the hostname, IP address, gateway address, subnet mask, and DNS server IP address will be set automatically.

    Click the **DHCP Information** link to view the current configuration. A table opens that lists the IP address, gateway address, and subnet mask set by the DHCP server, as well as the host name of the server.

12. Click **Save**.
13. In the navigation frame, click the **Restart ASM** link to activate the changes.

Configuring PPP access over a serial port

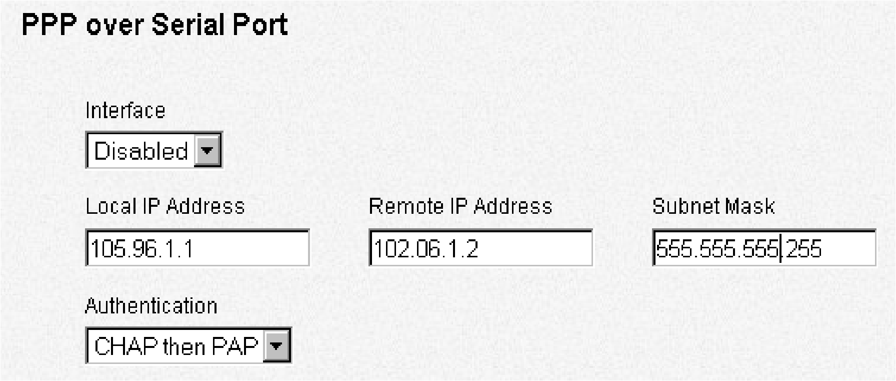
Use the point-to-point protocol (PPP) access method if you do not have Ethernet access. You can use PPP through your serial port to enable access to the Remote Supervisor Adapter through a TELNET session or a Web browser.

Note: If you enable the PPP interface, the Remote Supervisor Adapter cannot use the serial port for serial remote access.

Complete the following steps to configure PPP access over a serial port:

1. In the navigation frame, click **Network Interfaces**. Scroll down to the PPP over Serial Port section.

   Note: The values in the following window are examples. Your settings will be different.



PPP over Serial Port

Interface
Disabled

Local IP Address
105.96.1.1

Remote IP Address
102.06.1.2

Subnet Mask
555.555.555.255

Authentication
CHAP then PAP

2. In the Interface field, select **Enabled**.
3. In the Local IP Address field, type the local IP address for the PPP interface on this Remote Supervisor Adapter. The field defaults to 192.96.1.1. The IP address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
4. In the Remote IP Address field, type the remote IP address that this Remote Supervisor Adapter will assign to a remote user. The field defaults to 192.96.1.2. The remote IP address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
5. In the Subnet Mask field, enter the subnet mask that will be used by the Remote Supervisor Adapter. The default is 255.255.255.255. The subnet mask must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
6. Specify the type of authentication protocol that will be negotiated when a PPP connection is attempted.
   - The PAP Only setting uses a two-way procedure to validate the identity of the originator of the connection. This authentication protocol is necessary if a plain text password must be available to simulate a login at a remote host.

- The CHAP Only setting uses a three-way handshaking procedure to validate the identity of the originator of the connection upon connection at any time later. This is a stronger authentication protocol that protects against playback and trial-and-error attacks.
- The CHAP then PAP setting tries to authenticate using CHAP first. If the originator of the connection does not support CHAP, then PAP is tried as a secondary authentication protocol. The CHAP then PAP setting is the default.

7. Click **Save**.
8. In the navigation frame, click the **Restart ASM** link to activate the changes.

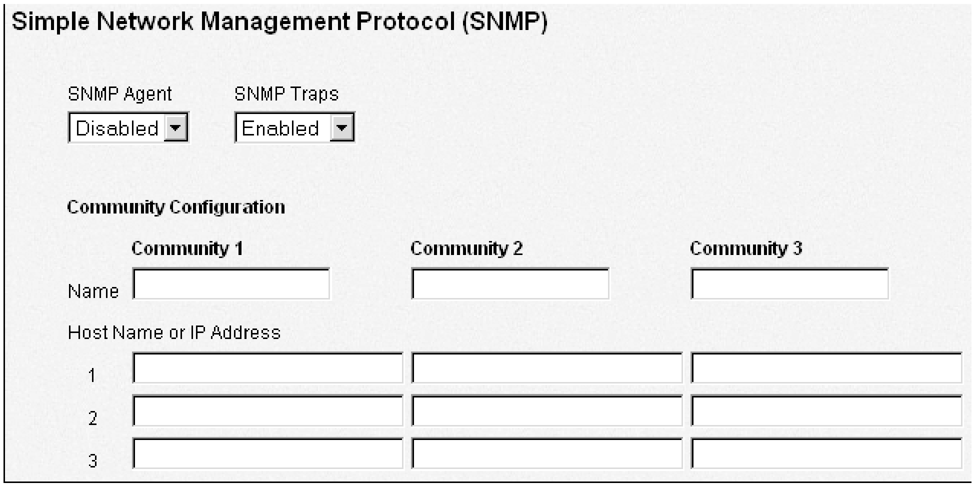
Configuring SNMP

The simple network management protocol (SNMP) enables you to query the SNMP agent to collect the “sysgroup” information and to send configured SNMP alerts to the configured host names or IP addresses.

Note: If you are planning to configure SNMP trap alerts on the Remote Supervisor Adapter, you must install and compile your supplied management information base (MIB) on your SNMP manager. For more information on the MIB file, see your *Remote Supervisor Adapter Installation Guide*.

Complete the following steps to configure your SNMP:

1. If you have not done so already, specify a system contact and the system location information on the System page. For more information on the System page settings, see “Setting system information” on page 16.
2. In the navigation frame, click **Network Protocols**. A window similar to the following opens:



Simple Network Management Protocol (SNMP)

SNMP Agent: Disabled

SNMP Traps: Enabled

Community Configuration

	Community 1	Community 2	Community 3
Name			
Host Name or IP Address			
1			
2			
3			

3. Enable the SNMP Agent and SNMP Traps fields.

   Enabling the SNMP Agent field forwards alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:

   - System contact specified on the System page. For more information on the System page settings, see “Setting system information” on page 16.
   - System location specified on the System page
   - At least one community name specified

- At least one valid IP address or hostname (if DNS is enabled) specified for that community

Note: Alert recipients whose notification method is SNMP will not receive alerts unless both SNMP traps and the SNMP agent are enabled.

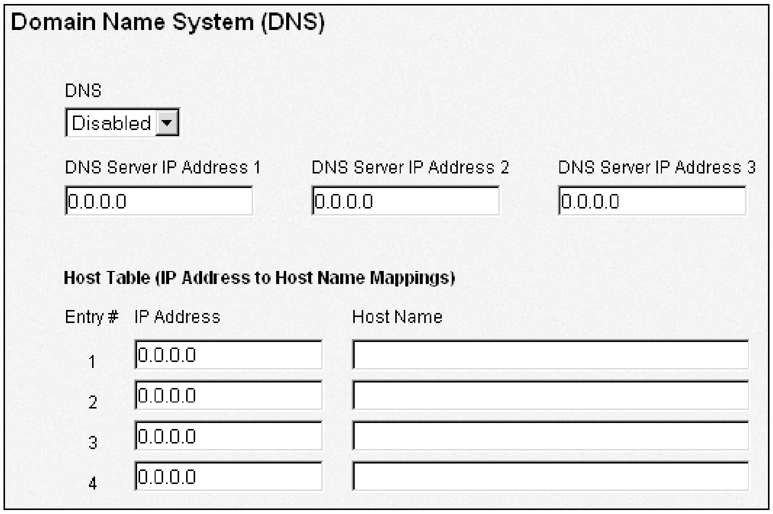
4. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:

   - Name
   - IP address

   If any of these parameters are not correct, you do not receive SNMP management access.

   Note: If an error message window opens, make the necessary adjustments to the fields listed in the error window. Then, click the **Save** button to save your corrected information. Also, you must configure at least one community in order to enable this SNMP agent.

5. In the Name field, type a name or authentication string that corresponds to the desired community.
6. In the corresponding IP Address field, type the Host Name or IP addresses of each community manager.
7. Scroll to the Domain Name System (DNS) section.



Domain Name System (DNS)

DNS: Disabled

DNS Server IP Address 1: 0.0.0.0

DNS Server IP Address 2: 0.0.0.0

DNS Server IP Address 3: 0.0.0.0

Host Table (IP Address to Host Name Mappings)

Entry #	IP Address	Host Name
1	0.0.0.0	
2	0.0.0.0	
3	0.0.0.0	
4	0.0.0.0	

8. Enable the DNS in the DNS field if a DNS server (or servers) is available on your network.

   The DNS field specifies whether you use a DNS server on your network to translate hostnames into IP addresses.

9. If you enabled DNS, enter the IP address of up to three DNS servers in the DNS Server IP Address fields.

   The DNS Server IP Address fields specify the IP addresses of up to three DNS servers on your network. Each IP address should contain integers from 0 to 255, separated by periods.

   Notes:

   a. Type an IP address in the IP Address field and its corresponding host name in the Host Name field. You can define four mappings. You only need to do this if a quick lookup of a host name is required.

Use the fields in the Host Table section to define relationships between an IP address and its corresponding host name in the event that your network DNS server is unreachable. You can also use these mappings for frequently used host names.

b. The Remote Supervisor Adapter examines this table first for an address to host name mapping. If a match is not found, the data will be requested from the DNS server. If the table contains an entry for a given address, the host name defined in the table will override any corresponding entry defined on the DNS server.

10. Click **Save**.
11. In the navigation frame, click the **Restart ASM** link to activate the changes.

Configuring SMTP

Complete the following steps to specify the IP address or host name of the SMTP server:

1. In the navigation frame, click **Network Protocols**.
2. Scroll down to the Simple Mail Transfer Protocol (SMTP) section.
3. In the SMTP Server Host Name or IP Address field, type the host name of the SMTP server.

   Use this field to specify either the IP address or, if DNS is enabled and configured, the host name of the SMTP server.

Chapter 5. Performing Remote Supervisor Adapter tasks

The functions under the Tasks heading in the navigation frame enable you to directly control the actions of the Remote Supervisor Adapter and your server. You can perform the following tasks:

- Update firmware
- Back up and restore the Remote Supervisor Adapter configuration
- Restart the Remote Supervisor Adapter
- Restore factory settings of the Remote Supervisor Adapter
- Access other Remote Supervisor Adapters

Updating firmware

Use the Transfer Files option on the navigation frame to update firmware for the Remote Supervisor Adapter.

Complete the following steps to update the startup or main application files of your Remote Supervisor Adapter or server.

1. In the navigation frame, click **Transfer Files**.
2. Click **Browse**.
3. Navigate to the PKT or PKC file you want to update.
4. Click **Open**.

   The file (including the full path) appears in the box beside Browse.
5. To begin the update process, click **Update**.

   A progress indicator opens as the file is transferred to temporary storage on the Remote Supervisor Adapter. A confirmation page opens when the file transfer is complete.
6. Verify that the PKT or PKC file shown on the Confirm Firmware Update page is what you intend to update. If not, click **Cancel**.
7. To complete the update process, click **Update** again.

   A progress indicator opens as the firmware on the Remote Supervisor Adapter is flashed. A confirmation page opens to verify that the update was successful.
8. After receiving a confirmation that the update process is complete, go to the Restart ASM page. In the navigation frame, click **Restart ASM**.
9. Click **OK** to confirm that you want to restart the Remote Supervisor Adapter.
10. Click **OK** to close the current browser window.
11. To log on to the Remote Supervisor Adapter again, open your browser and follow your regular logon process.

    Note: To cancel this process at any point, click **Cancel** until you return to the Transfer Files page.

Backing up your current configuration

You can download a copy of your current ASM configuration to the computer that is running the ASM Web interface. Use the backup to restore your Remote Supervisor Adapter configuration if it is accidentally changed or damaged. You can use it as a base that you can then modify to configure multiple Remote Supervisor Adapters with similar configurations.

Complete the following steps to back up your current configuration:

1. In the navigation frame, click **Transfer Files**.
2. Click **View the current configuration summary** on the Backup ASM configuration section of the Transfer Files page.
3. Verify that the displayed settings are the ones you want to save, and then, click **Close**.
4. To back up this configuration, click **Backup**.
5. Type a name for the backup, and select a location to save the file; then, click **Save**.

   In Netscape Navigator, click **Save File**.

   In Microsoft Internet Explorer, select **Save this file to disk**, and then click **OK**.

Restoring your ASM configuration

You can restore a saved configuration in full. Complete the following steps to restore your current configuration:

1. Log into the Remote Supervisor Adapter, for the configuration that you want to restore.
2. In the navigation frame, click **Transfer Files**.
3. Click **Browse**.
4. Click the configuration file that you want, and then click **Open**. The file (including the full path) appears in the box beside **Browse**.
5. Click **Restore**. A configuration summary panel displays.
6. Verify that this is the configuration that you want to restore. If it is not the correct file, click **Cancel**.
7. To proceed with restoring this file to the Remote Supervisor Adapter, click **Restore Configuration**.
8. When a confirmation displays that the restore process is complete, go to the Restart ASM page and click **Restart**.
9. Click **OK** to restart your Remote Supervisor Adapter.
10. In the window that opens, click **OK** to close the current browser window.
11. To log into the Remote Supervisor Adapter again, open your browser and follow your regular login process.

Restoring a changed configuration

You can modify key fields in the saved configuration before restoring them to your Remote Supervisor Adapter. Modifying the configuration before restoring helps you to set up multiple Remote Supervisor Adapters with similar configurations. You can quickly specify parameters that require unique values such as names and IP addresses without having to enter common, shared information.

Complete the following steps to restore a changed configuration:

1. Log into the Remote Supervisor Adapter that has the configuration that you want to restore.

2. In the navigation frame, click **Transfer Files**.
3. In the Restore ASM Configuration section, click **Browse**.
4. Navigate to the configuration file and then click **Open**. The file (including the full path) appears in the box beside **Browse**.
5. Click **Modify and Restore** to open an editable configuration summary page. Initially, only the fields that allow changes appear. To change between this view and the complete configuration summary view, click **Toggle View** at the top or bottom of the page.
6. To modify the contents of any field, click in the corresponding text box and type the data.
7. Verify that the displayed configuration is what you want to restore.
8. Click **Restore Configuration**. A progress indicator appears as the firmware on the Remote Supervisor Adapter flashes. A confirmation page appears to verify that the update was successful.
9. After receiving a confirmation that the restore process is complete, go to the Restart ASM page, and click **Restart**.
10. In the window that opens to confirm that you want to restart your ASM Web interface, click **OK**.
11. Click **OK** to close the current browser window.
12. To log into the Remote Supervisor Adapter again, open your browser and follow your regular log in process.

Accessing remote adapters through ASM interconnect network

You can connect to remote systems through the ASM interconnect network on the Access Remote ASM page. The Remote ASM Access table displays color-coded icons to indicate the overall status of each remote system in the System Health column. The system name is the name corresponding to each remote system. To use the full features of the Remote Supervisor Adapter, it is important that you update the Remote Supervisor Adapter firmware. For more information, see “Updating firmware” on page 29.

Complete the following steps to access the ASM processor or adapter on the ASM interconnect network:

1. In the navigation frame, click **Access Remote ASM**. The Remote ASM Access page opens, listing the processors and adapters linked to the host server through the ASM interconnect network. The table also displays the system health and the names of the adapters and processors in the **System Name** field.

   Note: Click the **Display Legends** link to view the icons that can appear in the System Health column.
2. Click the **login** link corresponding to the processors and adapters that you want to access under the ASM Interconnect Connection column heading. The Enter Network Password window opens.

   Note: It might take up to 45 seconds for newly attached servers to be reflected in the table of available remote servers. It might take up to 2 minutes for servers to be removed from the table when detached from the ASM interconnect network.
3. Type your user name and password. The ASM window opens, giving you access. The processor and adapter names appear in orange above the navigation frame identifying the local and remote connections.

Note: Depending on the ASM processor or adapter that is on the remote server, some options might vary.

Restoring ASM defaults

You can restore the Remote Supervisor Adapter if you have read/write access.

Attention: When you click Restore Defaults, you lose all of the modifications you made to the Remote Supervisor Adapter. You also lose the remote control of the remote servers. You must reset the password locally on the remote servers during BIOS code setup if you click Restore Defaults.

1. In the navigation frame, click **Restore Defaults**. A confirmation window opens.
2. Click **Yes**. Your TCP/IP or modem connections are broken and you need to log in again to use the ASM Web interface.

   Note: If this is your local system, your TCP/IP connection is lost. You need to reconfigure the network interface to restore connectivity.

Restarting ASM

You can restart the Remote Supervisor Adapter if you have read/write access.

Attention: When you select the Restart ASM option, you will lose all the modifications you made to the Remote Supervisor Adapter. You also lose the remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS setup.

1. In the navigation frame, click **Restart ASM**. A confirmation window opens.
2. Click **Yes**. Your TCP/IP or modem connections are broken and you need to log in again to use the ASM Web interface.

Logging off

Complete the following steps to logoff from the Remote Supervisor Adapter:

1. In the navigation frame, click **Log Off**.
2. If you are running Internet Explorer, click **Yes** at the confirmation window.

   This closes the current browser window and thereby maintains security. You must manually close any other open browser window, if any, or a cached version of your user ID and password remain available.
3. If you are running Netscape Navigator, click **OK** at the confirmation window.

   This closes the current browser window and thereby maintains security. You must manually close any other open browser window, if any, or a cached version of your user ID and password remain available.

Chapter 6. Accessing ASM through a text-based interface

You can access the Remote Supervisor Adapter using the text-based user interface by establishing a TELNET connection or a direct serial connection. This chapter describes accessing a text-based interface and configuring terminal settings.

Notes:

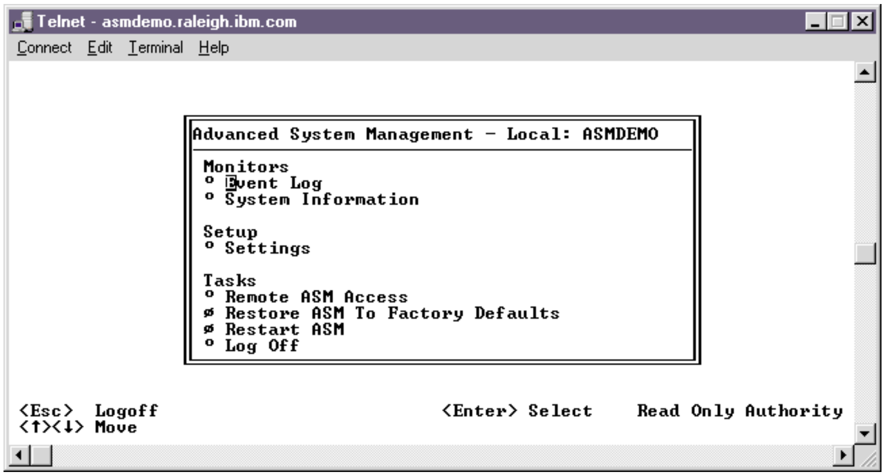
1. There are certain features of the ASM Web interface and text-based interface that are available only through the ASM processor that is on your server. You must first log into the Remote Supervisor Adapter and then log into the ASM processor to access these features.
2. F1 through F4 are the only function keys supported in the text-based interface.

Accessing a text-based interface via a TELNET connection

Complete the following procedure to access the Remote Supervisor Adapter through the TELNET:

1. Open a command prompt.
2. Type `TELNET` and either the host name or IP address at the command prompt.

   A TELNET client opens.
3. Configure the TELNET client for the text-based user interface. For more information on text-based user interface configuration, see “Configuring terminal settings” on page 34.
4. In the Login ID field, type a user name.
5. In the Password field, type the password associated with the user name. The Advanced System Management window opens.



```
Advanced System Management - Local: ASMDEMO

 Monitors
 º Event Log
 º System Information

 Setup
 º Settings

 Tasks
 º Remote ASM Access
 ø Restore ASM To Factory Defaults
 ø Restart ASM
 º Log Off

<Esc>  Logoff                        <Enter> Select    Read Only Authority
<↑><↓> Move
```

Note: Press the Up Arrow and Down Arrow keys to navigate your screen. Press Esc to exit to the Advanced System Management window; if you press Esc at the Advanced System Management window, you log off from your session. Press F3 to exit the window you are viewing.

Accessing a text-based interface via direct serial connection

Complete the following procedure to set a direct serial connection:

1. Connect a null modem cable to the serial port of the Remote Supervisor Adapter.

2. Connect the other end of the cable to a COM port on the client computer.
3. Start a terminal emulation program on the client computer such as Hilgraeve HyperTerminal.
4. Select the **File** → **Properties** menu option. The New Connection Properties window opens.
5. Click **Configure** and set the following values:

Table 4. COM properties.

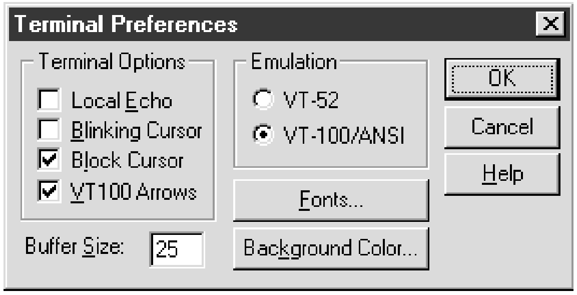
Field	Entry
Bits per second	57600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Click **OK**.
7. Click the **Settings** tab.
8. From the Emulation field, select **Terminal Keys** and **ANSI**.
9. Click **OK**.
10. Select the **View** → **Font** menu option.
11. Select the Terminal font with a point size of 9.
12. Click **OK**.
13. Press Esc to begin your session. The login prompt opens.
14. Enter your login ID and password.

Configuring terminal settings

Complete the following procedure to properly display special characters in the text-based user interface:

1. Select the **Terminal** → **Preferences** menu option. The Terminal Preferences window opens.



Terminal Options
- □ Local Echo
- □ Blinking Cursor
- ☑ Block Cursor
- ☑ VT100 Arrows

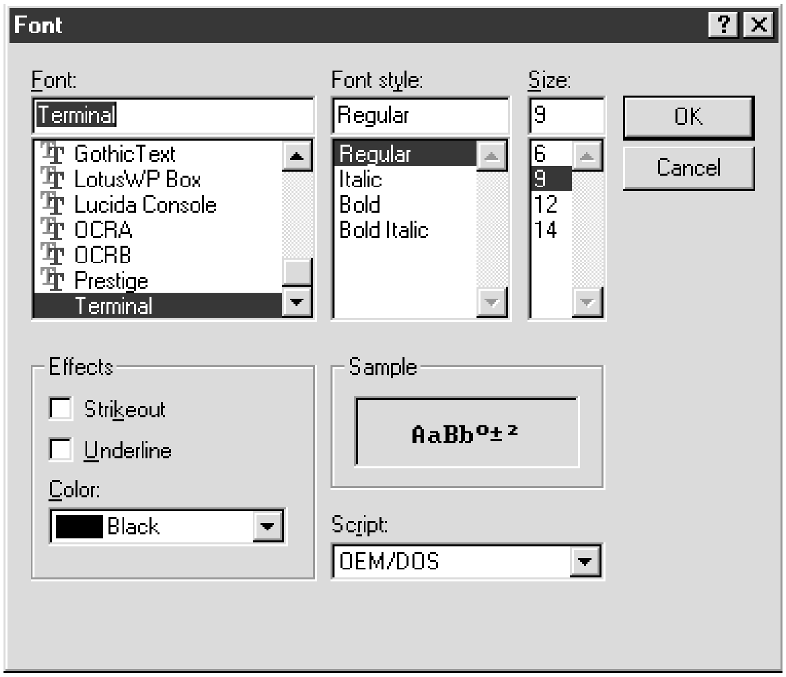
Emulation
- ○ VT-52
- ● VT-100/ANSI

Buffer Size: 25

2. Select the following check box options:
   - **Blinking Cursor**
   - **Block Cursor**

- **VT100 Arrows**
- **VT-100/ANSI**

3. Click **Fonts**. The Font window opens.



Font

Font: Terminal

Font style: Regular

Size: 9

Effects

□ Strikeout

□ Underline

Color: Black

Sample

Script: OEM/DOS

4. From the Font window, select the Terminal font. In the size window, select 9 as the font size.
5. Click **OK**.

Chapter 7. Monitoring system health using a text-based interface

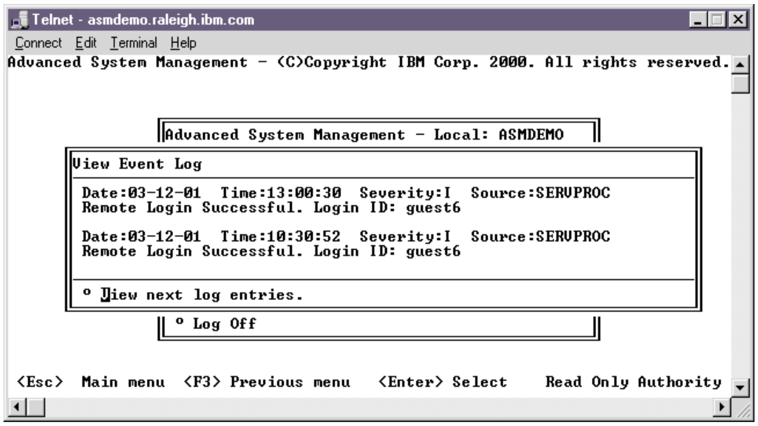
Use the options under the Monitors heading to view the status of the server you want to access.

Note: F1 through F4 are the only function keys supported in the text-based interface.

Viewing the event log

The Event Log window displays the System Error log and Post Error log, two entries at a time. Information about all remote access attempts and dial-out events that have occurred is recorded in the adapter event log. The Remote Supervisor Adapter time stamps all events and logs them into the event log, sending out the appropriate alerts if configured to do so by the system administrator.

1. In the Advanced System Management window, select the **Event Log**.
2. Select the **View Event Log** option to view the two most recent events that have occurred in the server.



```
Advanced System Management - (C)Copyright IBM Corp. 2000. All rights reserved.

              Advanced System Management - Local: ASMDEMO
       View Event Log
        Date:03-12-01  Time:13:00:30  Severity:I  Source:SERVPROC
        Remote Login Successful. Login ID: guest6

        Date:03-12-01  Time:10:30:52  Severity:I  Source:SERVPROC
        Remote Login Successful. Login ID: guest6

        ° View next log entries.
                ° Log Off

 <Esc>  Main menu  <F3> Previous menu   <Enter> Select    Read Only Authority
```

   The events are given the following levels of severity:

   I (Information)
   This severity level is assigned to an event of which you should take note.

   W (Warning)
   This severity level is assigned to an event that could affect server performance.

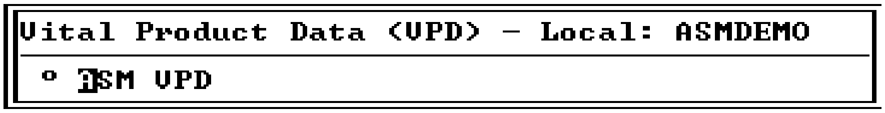
   E (Error)
   This severity level is assigned to an event that needs immediate attention.

3. Select **View next log entry** to view the next two entries.

Viewing vital product data

Upon server startup, the Remote Supervisor Adapter collects the system, BIOS code, and server component vital product data (VPD) and stores it in nonvolatile memory. You can access this information at any time from anywhere. The vital product data option contains key information about the system that the Remote Supervisor Adapter is monitoring.

1. Select **System Information** to view the status of the hardware and software components on the server.
2. Select **Vital Product Data (VPD)**. The Vital Product Data window opens:



```
Vital Product Data (VPD) - Local: ASMDEMO
 ° ISM VPD
```

3. Select the option corresponding to the information that you want:

   Remote Supervisor Adapter system data
   You can find the VPD for the Remote Supervisor Adapter in this section.

Table 5. Remote Supervisor Adapter vital product data.

Field	Function
Build ID	Identifies the build ID of both the application firmware and the startup ROM firmware.
Revision	Identifies the revision number of both the application firmware and the startup ROM firmware.
File name	Identifies the file name of both the application firmware and the startup ROM firmware.
Release date	Identifies the release date of both the application firmware and the startup ROM firmware.

4. Press F3 to return to the System Information window.

Chapter 8. Configuring the Remote Supervisor Adapter using a text-based interface

Use the options under the ASM Setup heading to configure your Remote Supervisor Adapter values.

Note: F1 through F4 are the only function keys supported in the text-based interface.

From the System window, you can:

- Set system information

From the Login & Alert Profiles window, you can:

- Set login profiles to control access to the Remote Supervisor Adapter
- Configure modem and dial-in settings

From the Serial Port 1 window, you can:

- Configure the serial port to the Remote Supervisor Adapter
- Configure advanced modem settings

From the Network Interfaces/Protocols window, you can:

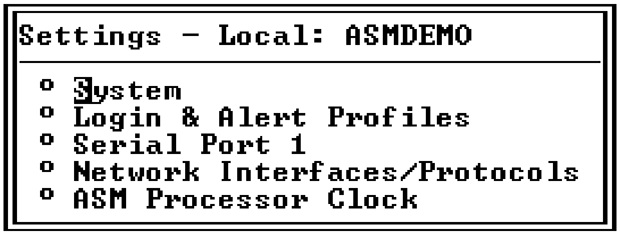
- Set up an Ethernet connection to the Remote Supervisor Adapter
- Set up a PPP over serial port connection to the Remote Supervisor Adapter
- Configure SNMP setup
- Configure DNS setup
- Configure SMTP setup

From the ASM Processor Clock page, you can set the ASM date and time.

Setting system information

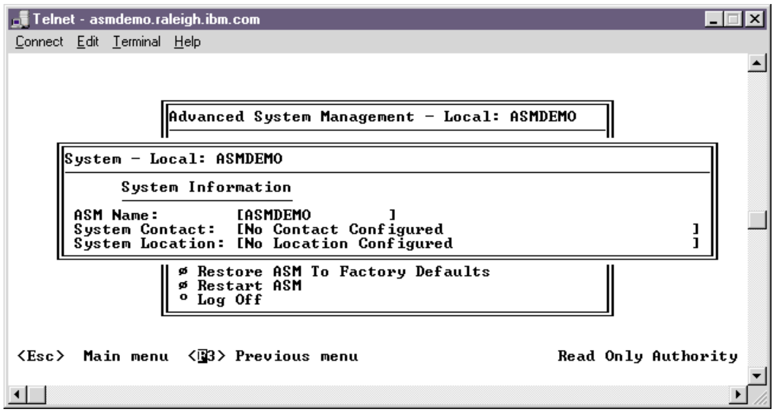
Complete the following steps to set your Remote Supervisor Adapter system information:

1. In the Advanced System Management window, select **Settings**. The Settings window opens:



```
Settings - Local: ASMDEMO

 o System
 o Login & Alert Profiles
 o Serial Port 1
 o Network Interfaces/Protocols
 o ASM Processor Clock
```

2. In the System Settings window, select **System**. A window similar to the following opens:



```
Telnet - asmdemo.raleigh.ibm.com
Connect  Edit  Terminal  Help

          Advanced System Management - Local: ASMDEMO

  System - Local: ASMDEMO
        System Information
   ASM Name:        [ASMDEMO        ]
   System Contact:  [No Contact Configured                         ]
   System Location: [No Location Configured                        ]
          ø Restore ASM To Factory Defaults
          ø Restart ASM
          ° Log Off

<Esc>  Main menu  <F3> Previous menu                 Read Only Authority
```

3. In the ASM Name field, type the name of the Remote Supervisor Adapter.

   Use the ASM Name field to specify a name for the ASM in this server. The name you assign the ASM in this server is included in the e-mail, SNMP, and alphanumeric pager alert notifications to identify the source of the alert.

   Note: Your Remote Supervisor Adapter name (the ASM Name field) and IP host name of the Remote Supervisor Adapter (the Hostname field on the Network Interfaces window) do not automatically share the same name because the ASM Name field is limited to 15 characters. The host name field can consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP host name. The non-qualified IP host name consists of up to the first period of a fully qualified IP host name. For example, the non-qualified IP host name of `asmcard1.us.company.com` (a fully qualified IP host name) is `asmcard1`. For more information on your host name, see "Configuring an Ethernet connection to ASM" on page 45.

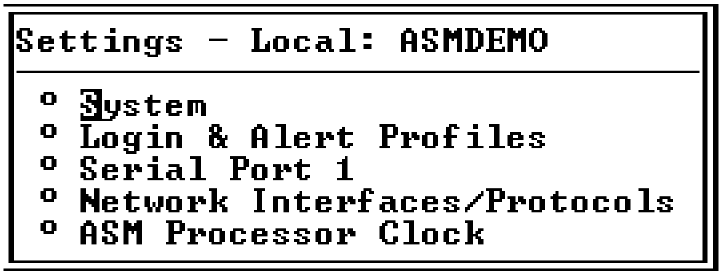
4. In the System Contact field, type contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.

5. In the System Location field, type in the location of the server. Include in this field sufficient detail to quickly locate the server for maintenance or other purposes. You can type a maximum of 47 characters in this field.

Creating a login profile

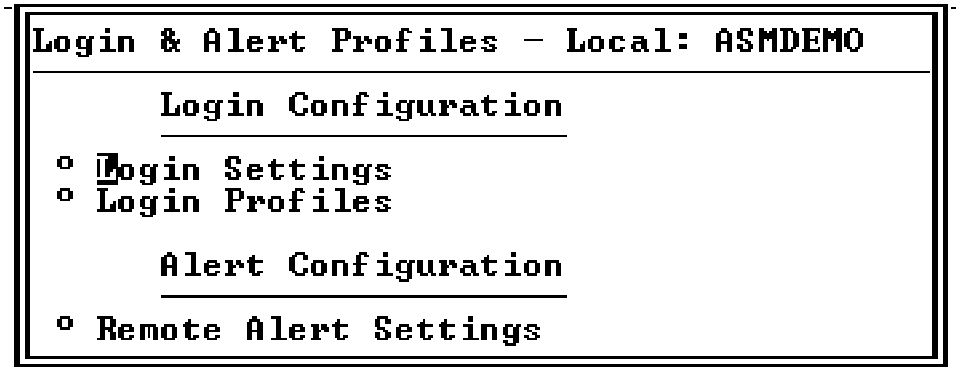
Complete the following steps to configure a login profile:

1. In the Advanced System Management window, select **Settings**. The Settings window opens:



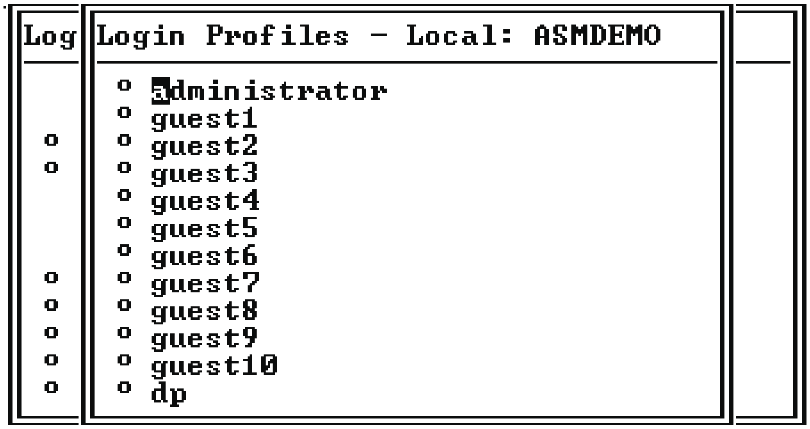
```
Settings - Local: ASMDEMO

 ° System
 ° Login & Alert Profiles
 ° Serial Port 1
 ° Network Interfaces/Protocols
 ° ASM Processor Clock
```

2. In the Settings window, select **Login & Alert Profiles**. The Login & Alert Profiles window opens:



```
Login & Alert Profiles - Local: ASMDEMO

      Login Configuration

 o Login Settings
 o Login Profiles

      Alert Configuration

 o Remote Alert Settings
```

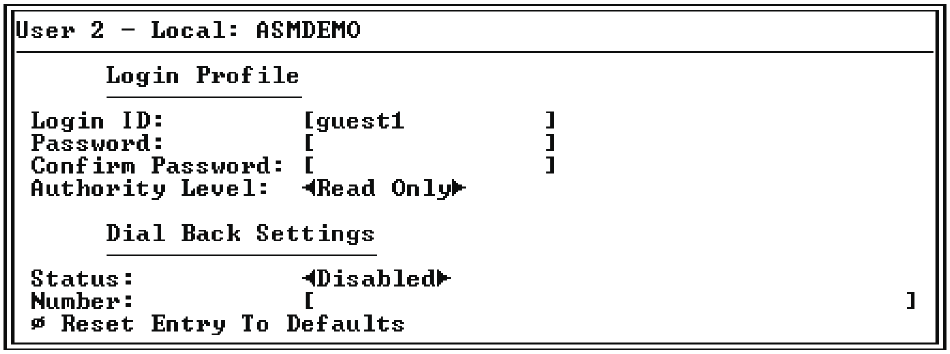
3. In the Login & Alert Profiles section, select the **Login Profiles** option.



```
Login Profiles - Local: ASMDEMO
 o administrator
 o guest1
 o guest2
 o guest3
 o guest4
 o guest5
 o guest6
 o guest7
 o guest8
 o guest9
 o guest10
 o dp
```

Use the Login Profiles window to view, configure, or change individual login profiles. You can define up to 12 unique profiles. If you have not configured a profile, the name of the profile by default will be User *nn* where *nn* is an arbitrary number assigned to that profile.

To work with a login profile, select a profile name. A window similar to the following opens:



```
User 2 - Local: ASMDEMO

      Login Profile

 Login ID:          [guest1          ]
 Password:          [                ]
 Confirm Password:  [                ]
 Authority Level:   ◀Read Only▶

      Dial Back Settings

 Status:            ◀Disabled▶
 Number:            [                                  ]
 ø Reset Entry To Defaults
```

4. In the Login ID field, type the name of the profile.

   You can type a maximum of 15 characters in the Login ID field. Valid characters are uppercase and lowercase letters, numbers, periods, and underscores.

Note: This login ID is used to grant remote access to the Remote Supervisor Adapter.

5. In the Password field, assign a password for the login ID.

   To set the password, in both the Password and Confirm Password fields, type the password.

   Valid passwords must contain at least five characters, one of which must be a nonalphabetic character. Null, or empty, passwords are accepted.

   Note: This password is used with the login ID, to grant remote access to the Remote Supervisor Adapter.

6. In the Authority Level field, select either **Read Only** or **Read/Write**.

   Use the Authority Level field to set the access rights for this login ID.

   Read-Only
   Enables the user to view a window but not to make changes. Additionally, users who log in with read-only IDs are restricted from performing any file transfers, power and restart actions, or remote control functions.

   Read/Write
   Enables the user to take any action provided by the interface, including setting up a user ID and turning off the server.

7. To configure the dial-back settings for the Remote Supervisor Adapter, in the **Status** field of the Dialback Settings section, select **Enabled**. Now, the Remote Supervisor Adapter automatically terminates a successful dial-in attempt and then immediately dials out to a specified number. Then, the Remote Supervisor Adapter terminates the connection and dials out to the login ID. If you do not want to configure dial-back settings, go to step 9.

   Note: If this menu is enabled, you must type a phone number in the **Number** field of this profile.

8. In the Number field, type the phone number that the Remote Supervisor Adapter will use when dialing back.

   This phone number is dialed when the user who is defined in this profile successfully logs into the Remote Supervisor Adapter.

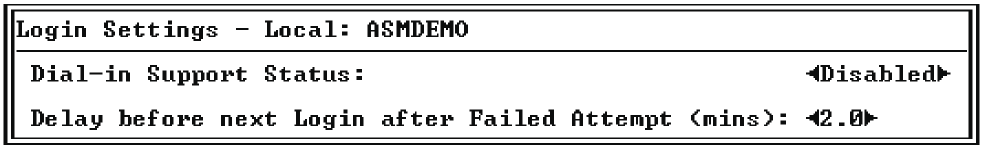
   Note: By default, the Remote Supervisor Adapter comes configured with one login profile that enables remote access using a login user ID of USERID and a password of PASSW0RD (the 0 is a zero). To avoid a potential security exposure, change this default login profile during initial setup of the Remote Supervisor Adapter.

9. If you want a remote user to dial into the Remote Supervisor Adapter through a connection, press F3 twice to return to the Login & Alert Profiles window.

Setting modem and dial-in settings

Complete the following steps to enable your modem to dial out to the remote login profile:

1. Select **Login & Alert Profiles**.
2. In the Login & Alert Profiles window, select **Login Settings**.



```
Login Settings - Local: ASMDEMO

 Dial-in Support Status:                              ◄Disabled►

 Delay before next Login after Failed Attempt (mins): ◄2.0►
```

3. In the Dial-in Support Status field, select **Enabled** to allow remote users to dial into the Remote Supervisor Adapter through a serial connection.
4. In the Delay before next Login after Failed Attempt <mins> field, you can specify how long, in minutes, the Remote Supervisor Adapter will prohibit remote login attempts, if more than five sequential failures to remotely log in are detected.

Setting remote alert attempts

Complete the following steps to set the number of times the Remote Supervisor Adapter attempts to send an alert:

1. Select **Login & Alert Profiles**.
2. From the Login & Alert Profiles window, select **Remote Alert Settings**.

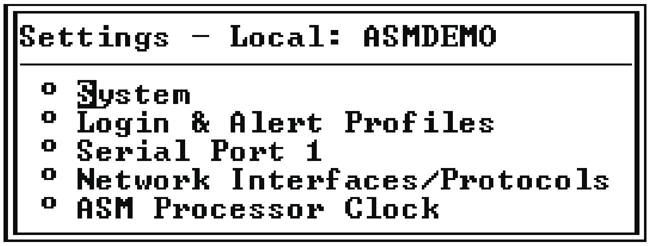
   Use these settings to define the number of remote alert attempts and the time between the attempts.
3. In the **Remote Alert Retry Limit** field, you can specify the number of additional times that the Remote Supervisor Adapter attempts to forward an alert to an alphanumeric pager. All other notification methods are attempted one time.
4. Specify the time interval (in minutes) that the Remote Supervisor Adapter waits between retries to send an alert in the Delay Between Retries field.
5. Press F3 to return to the Login & Alert Profiles window.

Configuring the serial port

You can configure a serial port to enable a single modem to conduct normal functions and also maintain out-of-band alerting capabilities.

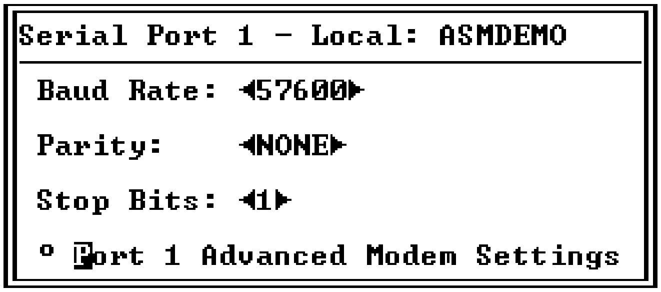
Complete the following steps to configure your serial port setup. For more information on your serial port, see “Configuring PPP access over serial port” on page 49.

1. In the Advanced System Management window, select **Settings**. The Settings window opens:



```
Settings - Local: ASMDEMO

 o System
 o Login & Alert Profiles
 o Serial Port 1
 o Network Interfaces/Protocols
 o ASM Processor Clock
```

2. In the Settings window, select **Serial Port 1**.



```
Serial Port 1 - Local: ASMDEMO
 Baud Rate: ◄57600►
 Parity:    ◄NONE►
 Stop Bits: ◄1►
 ° Port 1 Advanced Modem Settings
```

3. In the Baud Rate field, select the data transfer rate.

   The baud rate specifies the data transfer rate of your serial port connection. To set the baud rate, select the data transfer rate in bits per second that corresponds to your serial port connection.

4. In the Parity field, select the error detection to be used in your serial connection.

   The parity value specifies the error detection bits 0 or 1 added to each group of transmitted bits so that it will have either an odd or even number of 1s. This enables your server to know whether received data has been corrupted during transmission.

5. Select the number of data-terminating 1 bits that will follow the data or any parity bit to mark the end of a transmission.

   Note: The number of data bits is preset to 8 and cannot be changed.

   The stop bits value specifies how many extra “1” bits follow the data and any parity bit to mark the end of a unit of transmission (normally a byte or character).

6. If you need to set advanced settings, select the **Port 1 Advanced Modem Settings** option.

   Set these values only if the alert forwarding functions are not working properly. The strings marked with an asterisk (*) require a carriage return (^M) to be manually entered at the end of the field value.

Table 6. Port 1 settings.

Field	What you type
Initialization string	Type the initialization string that will be used for the specified modem. A default string is provided (ATE0). Do not change this string unless your dial-out functions are not working properly.
Caller ID string	Type the initialization string that will be used to get caller ID information from the modem.
Factory settings string	Type the initialization string that returns the modem to its factory settings when the modem is initialized. The default is AT&F0.
Escape guard (1 - 250 10ms Intervals)	Type the length of time before and after the escape string is issued to the modem. This value is measured in 10 millisecond intervals. The default value is 1 second.
Escape string	Type the initialization string that returns the modem to command mode when it is currently talking to another modem. The default is +++.
Dial prefix string	Type the initialization string that is used before the number to be dialed. The default is ATDT.
Dial postfix string	Type the initialization string that is used after the number is dialed to tell the modem to stop dialing. The default is ˆM.

Table 6. Port 1 settings.

Field	What you type
Auto answer	Type the initialization string that is used to tell the modem to answer the phone when it rings. The default is to answer after two rings or ATS0=1.
Auto answer stop	Type the initialization string that is used to tell the modem to stop answering the phone automatically when it rings. The default is ATS0=0.
Modem query	Type the initialization string that is used to find out if the modem is attached. The default is AT.
Hangup string	Type the initialization string that will be used to instruct the modem to disconnect. A default string is provided (ATH0). Do not change this string unless your dial-out functions are not working properly.

Initialization-string guidelines

If you need to provide a new initialization string, refer to the documentation that came with your modem. Your initialization string must contain commands that configure your modem as follows:

- Command echoing OFF
- Online character echoing OFF
- Result codes ENABLED
- Verbal result codes ENABLED
- All codes and Connect messages with BUSY and DT detection
- Protocol identifiers added — LAPM/MNP/NONE V42bis/MNP5
- Normal CD operations
- DTR ON-OFF hang-up, disable AA and return to command mode
- CTS hardware flow control
- RTS control of receive data to computer
- Queued and nondestructive break, no escape state

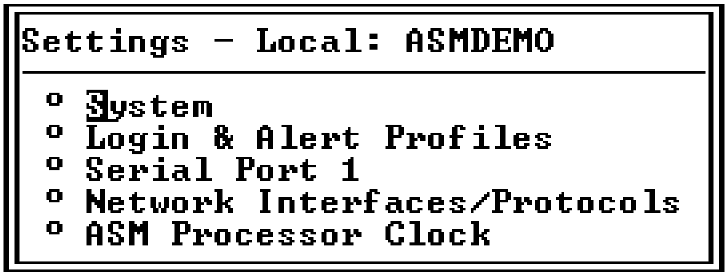
Note: The abbreviations in these commands have the following meanings:

AA	auto answer
CD	carrier detect
CTS	clear to send
DT	data transfer
DTR	data terminal ready
LAPM	link access protocol for modems
MNP	microcom networking protocol
RTS	ready to send

Configuring an Ethernet connection to ASM

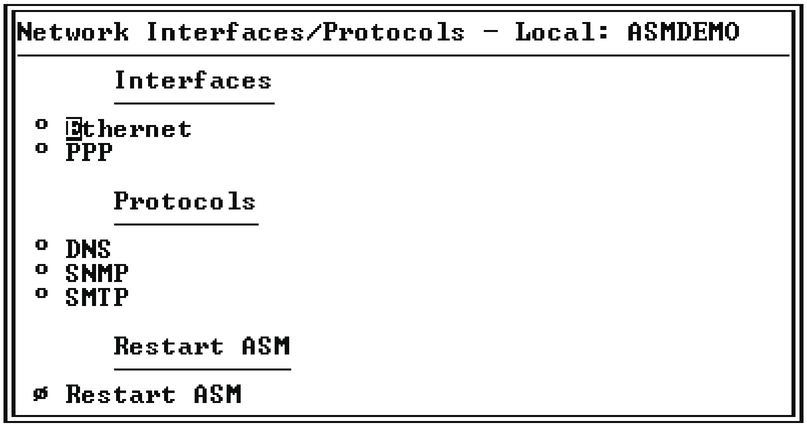
Complete the following steps to configure your Ethernet setup:

1. In the Advanced System Management window, select **Settings**. The Settings window opens:



```
Settings - Local: ASMDEMO

 o System
 o Login & Alert Profiles
 o Serial Port 1
 o Network Interfaces/Protocols
 o ASM Processor Clock
```

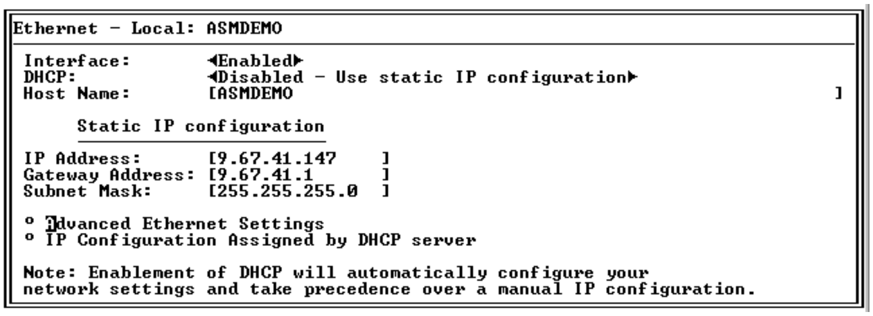
2. In the Settings window, select **Network Interfaces/Protocols**. The following window opens:



```
Network Interfaces/Protocols - Local: ASMDEMO

      Interfaces

 o Ethernet
 o PPP

      Protocols

 o DNS
 o SNMP
 o SMTP

      Restart ASM

 ø Restart ASM
```

3. Select **Ethernet**. A window similar to the following opens.

   Note: The values in the following window are examples. Your settings will be different.



```
Ethernet - Local: ASMDEMO

 Interface:        ◄Enabled►
 DHCP:             ◄Disabled - Use static IP configuration►
 Host Name:        [ASMDEMO                                         ]

      Static IP configuration

 IP Address:       [9.67.41.147    ]
 Gateway Address:  [9.67.41.1      ]
 Subnet Mask:      [255.255.255.0  ]

 o Advanced Ethernet Settings
 o IP Configuration Assigned by DHCP server

 Note: Enablement of DHCP will automatically configure your
 network settings and take precedence over a manual IP configuration.
```

4. In the Interface field, select **Enabled**. It is enabled by default.
5. If you want to use a dynamic host configuration protocol (DHCP) server connection, enable the DHCP field. Review the following notes, and then proceed to step 10.

   Note: If DHCP is enabled, the Host Name field is used as follows:

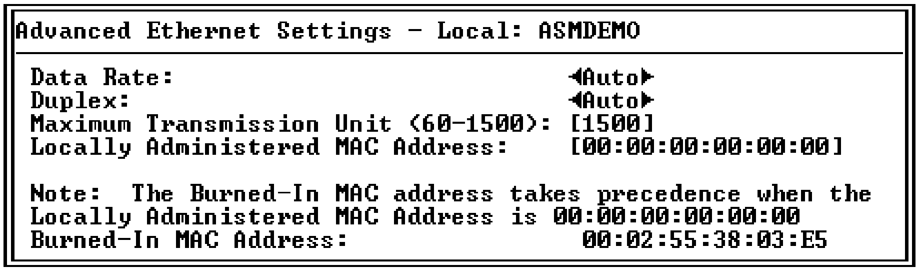
   a. If the Host Name field is set, then the Remote Supervisor Adapter DHCP support will request the DHCP server to allow the use of this hostname.
   b. If the Host Name field is not set, then the Remote Supervisor Adapter DHCP support will request the DHCP server to assign a unique host name to the Remote Supervisor Adapter.
   c. If you enable this setting, you must have an accessible, active, and configured DHCP server on your network. Also, when DHCP is enabled, the automatic configuration will override any manual settings.
6. In the Host Name field, type the IP host name of the Remote Supervisor Adapter. This step is only necessary if you disabled DHCP.

   You can enter a maximum of 63 characters in this field, which represents the IP host name of the Remote Supervisor Adapter. The host name by default is “ASMA” followed by the burned-in MAC address of the server in which the ASM is installed.

Note: The IP host name of the Remote Supervisor Adapter (the Host Name field) and Remote Supervisor Adapter name (the ASM Name field in the System window) do not automatically share the same name because the ASM Name field is limited to 15 characters. The Host Name field can consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP host name. The non-qualified IP host name consists of up to the first period of a fully qualified IP host name. For example, the non-qualified IP host name of `asmcard1.us.company.com` (a fully qualified IP host name) is `asmcard1`. For more information on your host name, see "Setting system information" on page 39.

7. In the IP Address field, type the IP address of the Remote Supervisor Adapter. This step is necessary only if you disabled DHCP. The IP address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
8. In the Gateway Address field, type the address of your network gateway router. This step is necessary only if you disabled DHCP. The gateway address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces or consecutive periods
9. In the Subnet Mask field, type the subnet mask used by the Remote Supervisor Adapter. This step is necessary only if you disabled DHCP. The subnet mask must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces or consecutive periods

   The default setting is 255.255.255.0.
10. Select **Advanced Ethernet Settings** if you need to set additional Ethernet settings. Make modifications as necessary.



```
Advanced Ethernet Settings - Local: ASMDEMO

 Data Rate:                           ◄Auto►
 Duplex:                              ◄Auto►
 Maximum Transmission Unit (60-1500): [1500]
 Locally Administered MAC Address:    [00:00:00:00:00:00]

 Note:  The Burned-In MAC address takes precedence when the
 Locally Administered MAC Address is 00:00:00:00:00:00
 Burned-In MAC Address:                 00:02:55:38:03:E5
```

Table 7. Advanced Ethernet setup.

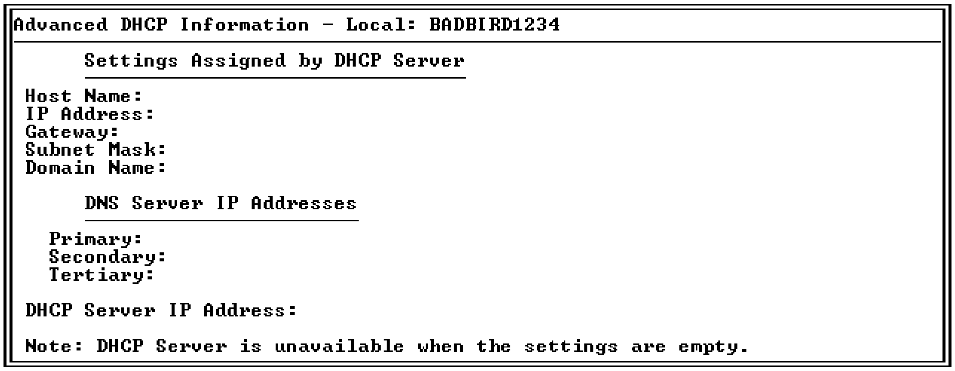
Field	Function
Data rate	Use the **Data Rate** field to specify the amount of data to be transferred per second over your LAN connection. To set the data rate, select the data transfer rate in megabits (Mb) that corresponds to your network capability. To automatically detect the data transfer rate, select Auto, which is the default value.

Table 7. Advanced Ethernet setup.

Field	Function
Duplex	Specify the type of communication channel used in your network in the **Duplex** field. To set the duplex mode, select one of the following: **Full** Enables data to be carried in both directions at once. **Half** Enables data to be carried in either one direction or the other, but not both at the same time. To automatically detect the duplex type, select Auto, which is the default value.
Maximum transmission unit <60-1500>	Use this field to specify the maximum size of a packet (in bytes) for your network interface. For Ethernet, the valid maximum transmission unit (MTU) range is 60 - 1500. The default value for this field is 1500.
Locally administered MAC address	Enter a physical address for this Remote Supervisor Adapter in the **Locally Administered MAC Address** field. If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value between 000000000000 - FFFFFFFFFFFF. This value must be in the form *XX*:*XX*:*XX*:*XX*:*XX*:*XX* where *X* is a number between 0 and 9. The Remote Supervisor Adapter does not support the use of a multicast address. A multicast address has the least significant bit of the first byte set to 1. The first byte, therefore, must be an even number.
Burned-in MAC address	The burned-in MAC address is a unique physical address assigned to this Remote Supervisor Adapter by the manufacturer. The address is also a read-only field.

11. Press F3 until you reach the Network Interfaces/Protocols window and select the **Restart ASM** option.

    Note: If DHCP was enabled prior to your restart, select **Advanced DHCP Information** to view the current DHCP server assigned configuration. A window opens that lists the IP address, gateway address, and subnet mask set by the DHCP server, as well as the domain name, and the server host name.



```
Advanced DHCP Information - Local: BADBIRD1234

      Settings Assigned by DHCP Server

 Host Name:
 IP Address:
 Gateway:
 Subnet Mask:
 Domain Name:

      DNS Server IP Addresses

   Primary:
   Secondary:
   Tertiary:

 DHCP Server IP Address:

 Note: DHCP Server is unavailable when the settings are empty.
```

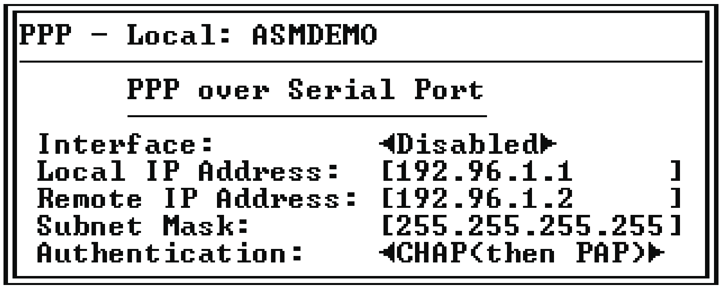
Configuring PPP access over serial port

Use the point-to-point protocol (PPP) access method if you do not have Ethernet access. You can use PPP through your serial port to enable access to the Remote Supervisor Adapter through a TELNET session or a Web browser.

Note: If you enable the PPP interface, the Remote Supervisor Adapter cannot use the serial port for serial remote access.

1. In the Network Interfaces/Protocols window, select **PPP**. The PPP window opens:

   Note: The values in the following window are examples. Your settings will be different.



```
PPP - Local: ASMDEMO

      PPP over Serial Port

 Interface:          ◄Disabled►
 Local IP Address:   [192.96.1.1      ]
 Remote IP Address:  [192.96.1.2      ]
 Subnet Mask:        [255.255.255.255]
 Authentication:     ◄CHAP(then PAP)►
```

2. In the Interface field, select **Enabled**.
3. In the Local IP Address field, enter the local IP address for the PPP interface on this Remote Supervisor Adapter. The field defaults to 192.96.1.1. The IP address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
4. In the Remote IP Address field, enter the remote IP address for this Remote Supervisor Adapter to assign to a remote user. The field defaults to 192.96.1.2. The remote IP address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
5. In the Subnet Mask field, enter the subnet mask that will be used by the Remote Supervisor Adapter. The default is 255.255.255.255. The subnet mask must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces
6. Specify the type of authentication protocol in the Authentication field that will be negotiated when a PPP connection is attempted.
   - The PAP Only setting uses a two-way handshaking procedure to validate the identity of the originator of the connection. This is a weaker authentication protocol, but it is necessary if a plain text password must be available to simulate a login at a remote host.
   - The CHAP Only setting uses a three-way handshaking procedure to validate the identity of the originator of the connection upon connection at any time later. This is a stronger authentication protocol that protects against playback and “trial and error” attacks.

- The CHAP (then PAP) setting tries to authenticate using CHAP first. If the originator of the connection does not support CHAP, then PAP will be tried as a secondary authentication protocol. The CHAP (then PAP) setting is the default.

7. Press F3 until you return to the Network Interfaces/Protocols window, and then select **Restart ASM**.

Configuring SNMP

The simple network management protocol (SNMP) enables you to query the SNMP agent to collect the “sysgroup” information and to send configured SNMP alerts to the configured host names or IP addresses.

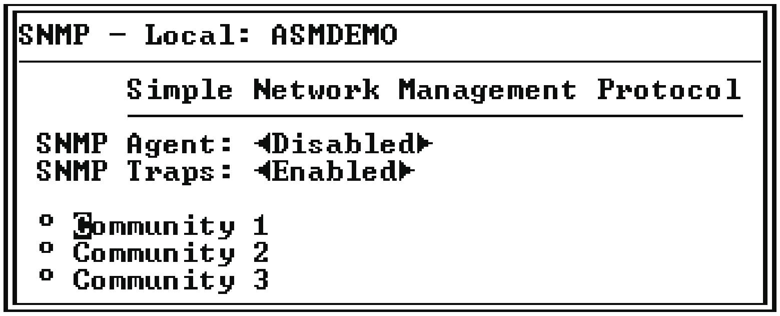
Note: If you are planning to configure SNMP trap alerts on the Remote Supervisor Adapter, you must install and compile your supplied management information base (MIB) on your SNMP manager. For more information on the MIB file, see your Remote Supervisor Adapter Installation Guide.

Complete the following steps to configure your SNMP:

1. From the Settings window, select **System** and enter your system contact and system location information. For more information on the system settings, see “Setting system information” on page 39.

   If these fields are already configured, return to the Network Interfaces/Protocols window and continue with the next step.

2. From the Settings window, select **Network Interfaces/Protocols**.
3. Select **SNMP**. The SNMP window opens:



```
SNMP - Local: ASMDEMO

      Simple Network Management Protocol

 SNMP Agent: ◄Disabled►
 SNMP Traps: ◄Enabled►

 ° Community 1
 ° Community 2
 ° Community 3
```

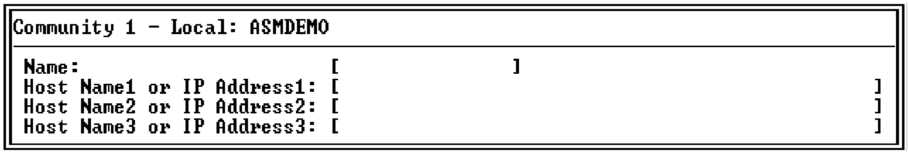
4. Enable the SNMP Agent and SNMP Traps fields.

   Enabling the SNMP Agent field forwards alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:

   - System contact specified in the System window
   - System location specified in the System window
   - At least one community name specified
   - At least one valid IP address or host name (if DNS is enabled) specified for that community

   Alert recipients whose notification method is SNMP do not receive alerts unless both the SNMP Agent and SNMP Traps fields are enabled.

5. Select one of the community options. A Community window opens:



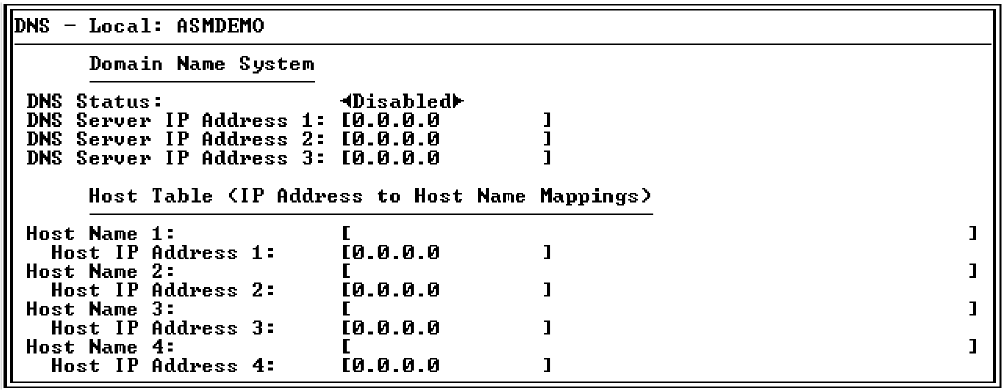
```
Community 1 - Local: ASMDEMO

 Name:                      [                ]
 Host Name1 or IP Address1: [                                                ]
 Host Name2 or IP Address2: [                                                ]
 Host Name3 or IP Address3: [                                                ]
```

You need to set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:

- Name
- Host name or IP address

If any of these parameters are not correct, you will not have SNMP management access.

6. In the Name field, enter a name or authentication string that corresponds to the community that you want.
7. Type the host name or IP addresses of this community in the corresponding Host Name1 or IP Address1 field for this community.
8. Press F3 until you return to the Network Interfaces/Protocols window.
9. In the Network Interfaces/Protocols window, select **DNS**.   A window similar to the following opens:



```
DNS - Local: ASMDEMO

      Domain Name System

 DNS Status:              ◄Disabled►
 DNS Server IP Address 1: [0.0.0.0        ]
 DNS Server IP Address 2: [0.0.0.0        ]
 DNS Server IP Address 3: [0.0.0.0        ]

      Host Table (IP Address to Host Name Mappings)

 Host Name 1:             [                                        ]
   Host IP Address 1:     [0.0.0.0        ]
 Host Name 2:             [                                        ]
   Host IP Address 2:     [0.0.0.0        ]
 Host Name 3:             [                                        ]
   Host IP Address 3:     [0.0.0.0        ]
 Host Name 4:             [                                        ]
   Host IP Address 4:     [0.0.0.0        ]
```

10. In the DNS Status field, enable the DNS.

    The DNS Status field specifies whether you use a DNS server on your network to translate host names into IP addresses.

11. If DNS is enabled, in the DNS Server IP Address fields, type the IP address of up to three DNS servers. You only need to do this if a quick lookup of a host name IP address is required.

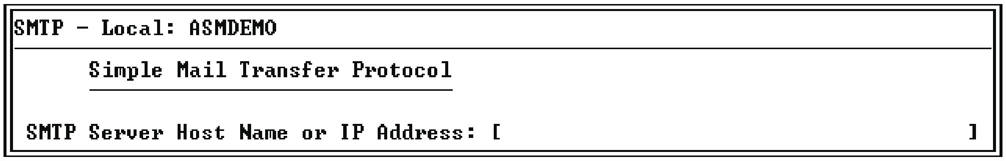
    The DNS Server IP Address fields specify the IP addresses of up to three DNS servers on your network. Each IP address should contain integers from 0 to 255, separated by periods.

12. In the Host Name IP Address field, enter a host name in the Host Name field and its corresponding IP address. You can define four mappings.

    Use the fields in the Host Table section to define relationships between an IP address and its corresponding host name in the event that your network DNS server is unreachable. You can also use these mappings for frequently used host names.

Note: The Remote Supervisor Adapter examines this table first for an address to host name mapping. If a match is not found, the data will be requested from the DNS server. If the table contains an entry for a given address, the host name defined in the table will override any corresponding entry defined on the DNS server.

13. Press F3 until you return to the Network Interfaces/Protocols window.
14. In the Network Interfaces/Protocols window, select **SMTP**. The SMTP window opens:



```
SMTP - Local: ASMDEMO

      Simple Mail Transfer Protocol

 SMTP Server Host Name or IP Address: [                                    ]
```

15. In the SMTP Server Host Name or IP Address field, enter the host name of the SMTP server This field must be defined to enable e-mail alerts to be sent.
16. Press F3 until you return to the Network Interfaces/Protocols window, and then select **Restart ASM**.

Setting the adapter clock

Complete the following steps to set the Remote Supervisor Adapter clock:

1. In the Advanced System Management window, select **Settings**.
2. Select **ASM Processor Clock**, which shows the date and time when this window was generated. Use this information to check the settings of the date and time processor on the Remote Supervisor Adapter, which is independent of the date and time settings of the clock on the server system board.

   The Remote Supervisor Adapter includes its own real-time clock to independently time-stamp all events that are logged in the battery-backed event log. Alerts, sent by e-mail, LAN, and SNMP, use the real-time clock setting to time stamp the alerts. The clock settings support Greenwich Mean Time (GMT) offsets and Daylight Savings Time (DST) for added ease-of-use for administrators managing systems remotely over different time zones. You can remotely access the battery-backed event log even if the system is turned off or otherwise disabled. This facilitates immediate problem determination and resolution.
3. To set the time, type the numbers corresponding to the current hour, minutes, and seconds in the appropriate text boxes. The hour (hh) must be a number from 0 to 23 as represented on a 24-hour clock. The minutes (mm) and seconds (ss) must be numbers from 0 to 59.
4. Set the time zone settings, depending on your location.

   GMT offset

   Use the Offset from GMT field to specify the offset from GMT corresponding to the time zone where this server is located.

   Daylight Savings Time

   Use the Observe daylight savings time? field to specify whether the Remote Supervisor Adapter clock will automatically adjust when DST changes.
5. Press **F6** to save your settings.

Chapter 9. Performing Remote Supervisor Adapter tasks through a text-based interface

The functions under the Tasks heading enable you to directly control the actions of the Remote Supervisor Adapter and your server.

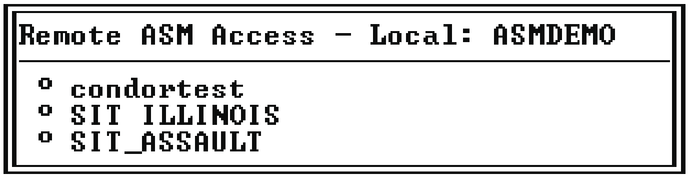
Note: F1 through F4 are the only function keys supported in the text-based interface.

Accessing ASM processors, ASM adapters, or the Remote Supervisor Adapter through the ASM interconnect network

You can connect to the remote system through the ASM interconnect network of ASM processors, ASM adapters, or the Remote Supervisor Adapter found on the Access Remote ASM window. The Remote ASM Access table indicates the overall status of each remote server in the System Health column. The server name is the name corresponding to each remote system.

Complete the following steps to access remote Remote Supervisor Adapters:

1. In the Advanced System Management window, select **Remote ASM Access**. The Remote ASM Access window opens, listing other ASM adapters and processors linked to the host server.



```
Remote ASM Access - Local: ASMDEMO

 ° condortest
 ° SIT ILLINOIS
 ° SIT_ASSAULT
```

2. Select a processor or adapter. The Remote ASM Login window opens.
3. Type your user name and password.

   Note: It might take up to 45 seconds for newly installed ASM processors, ASM adapters, or the Remote Supervisor Adapter to appear in the table of available remote systems. It might take up to 2 minutes for systems to be removed from the table when detached from the ASM interconnect network.
4. The ASM window opens, giving you access to the remote ASM adapter or processor.

   Note: Depending on the adapter you installed, certain ASM processors, ASM adapters, or the Remote Supervisor Adapter options might not be available.

Restoring ASM to factory defaults

The following options enable you to restore the Remote Supervisor Adapter settings if you have read/write access.

Attention: When you select the Restore ASM to Factory Defaults option, you will lose all the modifications you made to the Remote Supervisor Adapter. You also lose the remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS setup.

In the Advanced System Management window, select **Restore ASM To Factory Defaults** to reset the Remote Supervisor Adapter to its original factory settings. You will lose your TCP/IP connection and must reconfigure the network interface.

Restarting ASM

The following option enables you to restart the Remote Supervisor Adapter if you have read/write access.

Attention: When you select the Restart ASM option, you will lose all the modifications you made to the Remote Supervisor Adapter. You also lose the remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS setup.

In the Advanced System Management window, select **Restart ASM**. Your TCP/IP or modem connections will be broken and you will need to log in again to use the ASM Web interface.

Logging off

Complete the following steps to log off from the Remote Supervisor Adapter:

1. In the Advanced System Management window, select **Log Off**.
2. Click **Yes** or **No**.

Appendix A. Getting help, information and service

If you need help, service, technical assistance, or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

With the original purchase of an IBM hardware product, you have access to extensive support coverage. During the IBM hardware product warranty period, you may call the IBM Personal Computer HelpCenter (1-800-772-2227 in the U.S.) for hardware product assistance covered under the terms of the IBM Statement of Limited Warranty.

The following services are available during the warranty period:

- Problem Determination - Trained personnel are available to assist you with determining if you have a hardware problem and deciding what action is necessary to fix the problem.
- IBM Hardware Repair - If the problem is determined to be caused by IBM hardware under warranty, trained service personnel are available to provide the applicable level of service.
- Engineering Change Management - Occasionally, there might be changes that are required after a product has been sold. IBM or your reseller, if authorized by IBM, will make Engineering Changes (ECs) available that apply to your hardware.

Be sure to retain your proof of purchase to obtain warranty service. Refer to the IBM hardware warranty for a full explanation of IBM's warranty terms.

Please have the following information ready when you call:

- Machine type and model
- Serial numbers of your IBM hardware products
- Description of the problem
- Exact wording of any error messages
- Hardware and software configuration information

On the World Wide Web, the IBM Personal Computing Web site has up-to-date information about IBM Personal Computer products and support.

Some helpful addresses are:

Table 1. IBM Personal Computing Web sites.

World Wide Web site Address	Description
http://www.ibm.com	Main IBM home page
http://www.ibm.com/pc	IBM Personal Computing
http://www.ibm.com/pc/support	IBM Personal Computing Support
http://www.ibm.com/pc/us/accessories	Options by IBM (U.S.)
http://www.ibm.com/pc/us/eserver/xseries	IBM xSeries Servers (U.S.)
http://www.ibm.com/pc/techconnect	IBM TechConnect®

You can select a country-specific Web site from these pages.

If you select Profile from the support page, you can create a customized support page that is specific to your hardware, complete with Frequently Asked Questions, Parts Information, Technical Hints and Tips, and Downloadable Files. You will have the information you need, all in one place. In addition, you can choose to receive e-mail notifications whenever new information becomes available about your registered products. You can also access online support forums, which are community sites monitored by IBM support staff.

Appendix B. Notices

This publication was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Edition Notice

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Processing date data

This IBM hardware product and IBM software products that might be packaged with it have been designed, when used in accordance with their associated documentation, to process date data correctly within and between the 20th and 21st centuries, provided all other products (for example, software, hardware, and firmware) used with these products properly exchange accurate date data with them.

IBM cannot take responsibility for the date data processing capabilities of non-IBM products, even if those products are preinstalled or otherwise distributed by IBM. You should contact the vendors responsible for those products directly to determine the capabilities of their products and update them if needed. This IBM hardware product cannot prevent errors that might occur if software, upgrades, or peripheral devices you use or exchange data with do not process date data correctly.

The foregoing is a Year 2000 Readiness Disclosure.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM

Netfinity

Predictive Failure Analysis

TechConnect

the e-business logo

xSeries

Java is a trademark of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

IBM®

Part Number: 25P2574

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

25P2574