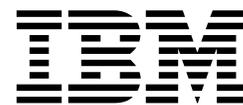IBM® Remote Supervisor Adapter

IBM

User's Guide

IBM® Remote Supervisor Adapter

User's Guide

NOTE

Before using this information and the product it supports, be sure to read the general information in Appendix A, "Notices" on page A-75.

Contents

Chapter 1.   Introduction

The IBM® Remote Supervisor Adapter is part of the Advanced System Management (ASM) family of 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
- Full 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 to access the Remote Supervisor Adapter. This manual refers to either the ASM Web interface or the Remote Supervisor Adapter, depending on the context.

Remote Supervisor Adapter features

Standard features of the Remote Supervisor Adapter are as follows:

- Continuous health monitoring and control
- Automatic notification and alerts
- Event log showing time-stamped entries
- Remote access through Ethernet, point-to-point protocol (PPP), serial, and the ASM interconnect peer-to-peer support
- Simple Network Management Protocol (SNMP)
- E-mail alerts
- Alpha or numeric pager events
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- Remote power control
- Blue screen capture
- Remote firmware update
- Access to critical server settings
- Text-based user interface terminal access

Web browser requirements

The ASM Web interface supports the following Web browsers:

- Microsoft® Internet Explorer 4.0, or later
- Netscape Navigator 4.0, or later

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

- Java™ 1.1 support, or later
- JavaScript 1.2, or later
- HTTP Version 1.0, or later
- Minimum display resolution of 800 x 600 with 256 colors

Notices used in this book

This book contains notices to highlight information or provide safety information. The notice definitions are as follows:

- **Notes:** These notices provide information that might help you avoid inconvenient or problem situations.

- **Important:** These notices provide information 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.   Opening and using the ASM Web interface

Use the following procedure to access the Remote Supervisor Adapter through the ASM Web interface.

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:

2. Type your user name and password in the Enter Network Password window. 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.

   Note: The Remote Supervisor Adapter is set initially with a user name of **USERID** and password of **PASSW0RD** (with a zero). This user has read/write access. Change this default during your initial configuration for enhanced security.

3. A welcome page opens in your browser. Select a value, in minutes, in the **Inactive Session Timeout Value** field. If your browser is inactive for that amount of minutes, the Remote Supervisor Adapter logs you off the Web interface.

4. Click the **Start Session** button. The browser then opens the System Health page, which gives you a quick view of the server status.
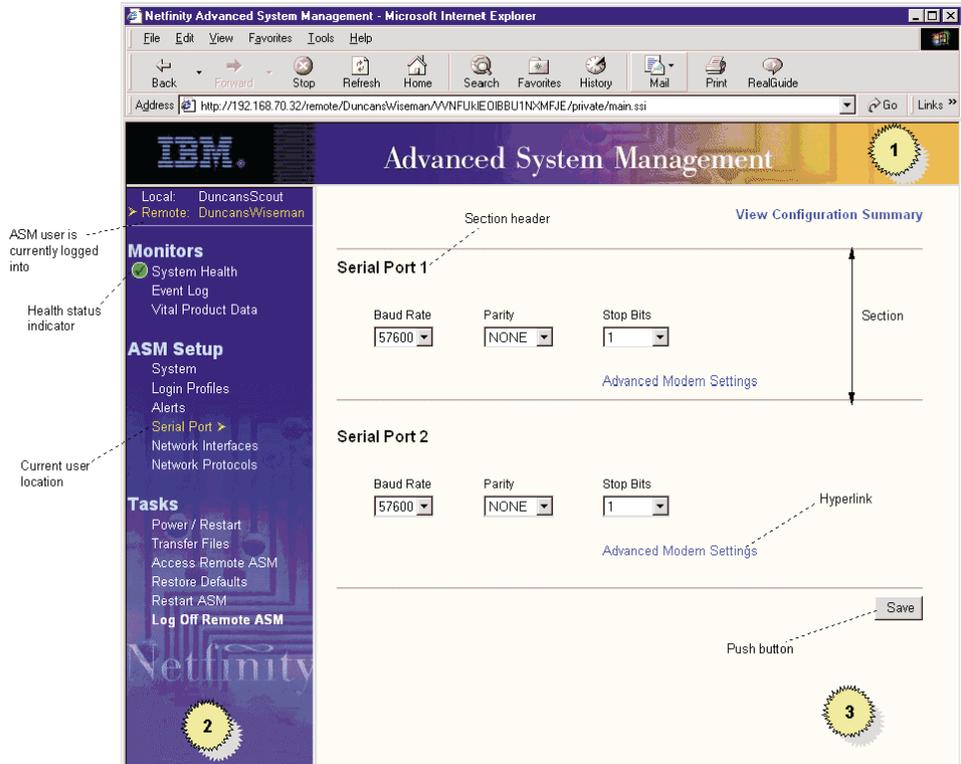
In the browser window, you find the Advanced System Management banner across the top of the page (**1**). Along the left side of the browser is the navigation frame (**2**). To the right of the navigation frame are the contents of the page (**3**) you have opened.

The navigation frame of the ASM window contains the following navigational links that you can click to manipulate your Remote Supervisor Adapter or check the status of a server:

System health
You can monitor the power and restart, temperature, voltage, and fan status of your server on the System Health Summary page. The System Health Summary page serves as the default homepage for the ASM Web interface. For more information on interpreting the system health summary data, see "Monitoring the remote server status" on page 7.

Event log
The Event Log window contains entries that are currently stored in the System Error log and POST Error log. Information about all remote access attempts and dialout events that have occurred 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 appropriate alerts if configured to do so by the system administrator. For more information on checking the event log, see "Viewing the event log" on page 10.

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

monitoring. For more information on viewing vital product data, see "Viewing vital product data" on page 10.

System

You can set general information, including the name for the Remote Supervisor Adapter, contact information for the adapter, and the server location. For more information on setting the system information section, see "Setting system information" on page 13.

Login profiles

You can define 12 login profiles that enable access to the Remote Supervisor Adapter. For more information on defining login profiles, see "Creating a login profile" on page 17.

Alerts

You can set the Remote Supervisor Adapter to provide alerts for a number of different situations. Click the **Alerts** link to set the standards for these alerts, including the remote alert recipients, number of alert attempts, incidents that trigger remote alerts, and local alerts. For more information on configuring remote alert recipients and the alerts to send, see "Configuring remote alert recipients" on page 18.

Serial port

You can set serial port baud rate and modem settings, and either dedicate the integrated serial port on the Remote Supervisor Adapter to system management or share it with the operating system. If dedicated to system management, the serial port is used by the Remote Supervisor Adapter only and is always available for dial-in and dial-out alerting purposes. You will not be able to view the port on the network operating system (NOS) or in any other applications. For more information on dedicating the serial port, see "Configuring the serial port" on page 24.

Network interfaces

You can configure the Remote Supervisor Adapter to have a remote access connection over an Ethernet connection or by point-to-point protocol (PPP). This allows remote access using a Web browser or telnet application. For more information on setting up an Ethernet connection to the Remote Supervisor Adapter, see "Configuring an Ethernet connection to ASM" on page 27. For more information on setting up a PPP using the serial port connection, see "Configuring PPP access over a serial port" on page 29.

Network protocols

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 hostnames or IP addresses. You can also use a Domain Name System (DNS) server to translate hostnames into IP addresses. For more information on setting up the network protocols, see "Configuring SNMP" on page 30.

Power/restart

The Remote Supervisor Adapter 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. For more information on remote restarting, see "Remotely controlling the power status of a server" on page 33.

Transfer files

Use the options on the Transfer Files page to update firmware and to save the ASM configuration file on the remote administrator workstation, transfer it to another adapter, or restore and edit it for application to a new system. You can deploy multiple managed systems without having to re-enter all data for all the systems. You can do this only through the ASM Web interface. For more information on updating firmware, see

"Updating firmware" on page 34. For more information on saving and restoring ASM configurations, see "Restoring your ASM configuration" on page 35.

Access remote ASM
You can access other Remote Supervisor Adapters over the ASM interconnect network. For more information on remotely accessing the Remote Supervisor Adapter, see "Accessing remote adapters through ASM interconnect network" on page 36.

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

Attention: When you click the **Restore Defaults** button, you will lose all the modifications you made to the Remote Supervisor Adapter.

For more information on restoring defaults, see "Restoring ASM" on page 37.

Restart ASM
You can restart the Remote Supervisor Adapter. However, you will lose your configured connections and data if you do so. For more information on restoring defaults, see "Restoring or restarting ASM" on page 36.

Remote control
From the Remote Control page, you can:

- View the server graphical desktop image
- Restart the server and view the POST process in a telnet applet window
- View the POST process and graphical desktop image without restarting the server
- View the image of a blue screen capture

For more information on the remote control options, see "Remote graphical control" on page 37.

Log off
You can log off from your connection to the Remote Supervisor Adapter with this option. For more information on logging off, see "Logging off" on page 39.

Also, you can click the **View Configuration Summary** link, which appears on most pages, to quickly view how your Remote Supervisor Adapter is configured. The information appears in the separate window that opens.

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 System Health page, you can:

- View system health summary
- View server power and restart activity
- View server temperature, voltage, and fan readings

From the Event Log page, you can:

- View all server events recorded in the Event Log of the Remote Supervisor Adapter
- View the severity of events

From the Vital Product Data page, you can:

- View the machine vital product data (VPD)
- View the component VPD
- View the POST/BIOS VPD
- View the ASM VPD
- View the component activity log

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. The System Health Summary page is the default home page for the ASM Web interface.

1. Click **System Health** in the navigation frame to view a dynamically-generated update on the overall health of the server.

   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" is displayed. The critical events and errors are listed.

   Warnings and system events
   > A yellow triangle containing an exclamation point is displayed. The Warnings and System Events section lists all warnings received or detected by the Remote Supervisor Adapter from the server.

2. 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 total 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 System partition`
- `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`

3. 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:
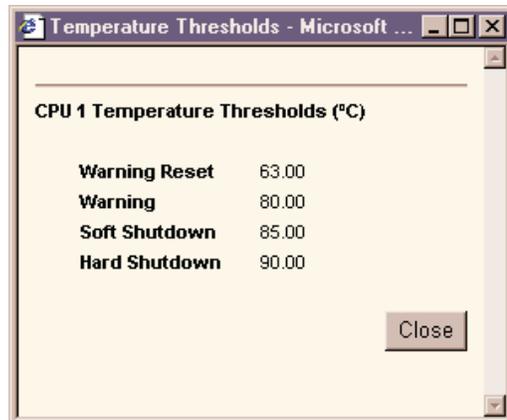
The Temperature Thresholds window displays the temperature levels at which the Remote Supervisor Adapter reacts. These levels are preset on the remote server and cannot be changed.

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

If a temperature reaches a specified value higher than the 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

If a temperature reaches a specified value higher than the soft 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 if a warning was sent, the server assumes the temperature has returned to normal and no further alerts will be generated.

4. 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:
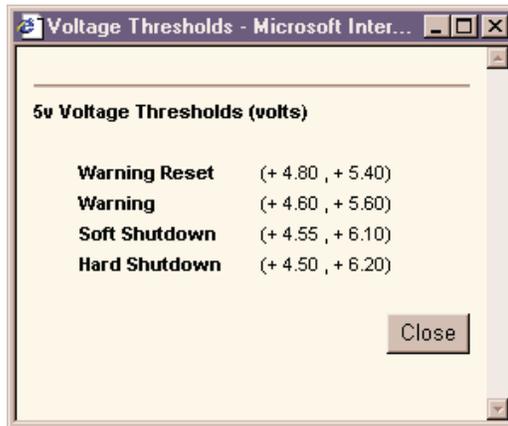
The Voltage Thresholds window displays the voltage ranges at which the Remote Supervisor Adapter reacts. These levels are preset on the remote server and cannot be changed.

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.

5. 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 dialout 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. Click the Event Log link in the navigation frame to view the server's recent history of events.

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.

Viewing vital product data

Upon server startup, the Remote Supervisor Adapter collects system, BIOS, and server component vital product data (VPD) and stores it in nonvolatile memory. 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. Click **Vital Product Data** in the navigation frame to view the status of the hardware and software components on the server.

2. Scroll down to view the following VPD readings:

   Machine level VPD
   The VPD for the server appears in this section.

Table 1. Machine level vital product data

Field	Function
Machine type	Identifies the type of server the Remote Supervisor Adapter is monitoring.
Machine model	Identifies the model number of the server the Remote Supervisor Adapter is monitoring.
Serial number	Identifies the serial number of the server the Remote Supervisor Adapter is monitoring.

Component level VPD

The VPD for the server components appears in this section.

Table 2. Component level vital product data

Field	Function
FRU number	Identifies the field replaceable unit number (a seven-digit alphanumeric number) for each component.
Serial number	Identifies the serial number of each component.
Mfg ID	Identifies the manufacturer ID for each component.
Slot	Identifies the slot number where the component is located.

POST/BIOS data

You can find the VPD for the system power-on self-test (POST) or basic input/output system (BIOS) firmware code in this section.

Table 3. POST/BIOS vital product data

Field	Function
Version	Indicates the version number of the POST/BIOS code.
Build level	Indicates the level of code for the POST/BIOS code.
Build date	Indicates when the POST/BIOS code was built.

Remote Supervisor Adapter system data

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

Table 4. 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.

Component Activity Log

You can find a record of component activity in this section.

Table 5. Component activity log

Field	Function
FRU number	Identifies the field replaceable unit number (a seven-digit alphanumeric number) of the component.
Serial number	Identifies the serial number of the component.
Manufacturer ID	Identifies the manufacturer of the component.
Slot	Identifies the slot number where the component is located.
Action	Identifies the action taken by each component.
Timestamp	Identifies the date and time of the component action. The date is displayed in the MM/DD/YY format. The time is displayed in the HH:MM:SS format.

In addition, the activity log tracks the following components:

- Power supplies
- DIMMs
- CPUs
- Systemboard
- Power backplane

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 server timeouts, which result in automatic corrective action by the Remote Supervisor Adapter
- 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/dial-in settings

From the Alerts page, you can:

- Configure remote alert recipients
- Set the number of remote alert attempts
- Select which alerts will be monitored/sent
- Select local events to track
- Set e-mails to include event log attachment when alerts are generated

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. Click **System** in the navigation frame. 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. Type the name of the Remote Supervisor Adapter in the **ASM Name** field.

   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 IP hostname 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 hostname. The non-qualified IP hostname consists of up to the first period of a fully qualified IP hostname. For example, the non-qualified IP hostname of `asmcard1.us.company.com` (a fully qualified IP hostname) is `asmcard1`. For more information on your hostname, see "Configuring an Ethernet connection to ASM" on page 27.

3. Assign the Remote Supervisor Adapter a unique identification number in the **ASM ID Number** field.

4. Type contact information in the **System Contact** field. 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. Type the location of the server in the **System Location** field. 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 server timeouts

Complete the following steps to set your server timeout values:

1. Click **System** in the navigation frame.

2. Scroll down to the Server Timeouts section. You can set the Remote Supervisor Adapter to respond automatically to these problems:

   • Halted power-on self-test

   • Halted operating system

   • Failure to load operating system

   • Failure to shut down operating system

```
Server Timeouts

    POST Watchdog                    O/S Watchdog
    [Disabled ▼] minutes             [Disabled ▼] minutes

    Loader Watchdog                  Power Off Delay
    [Disabled ▼] minutes             [0.5 ▼] minutes
```

3. Enable the server timeouts that correspond to the problems you want the Remote Supervisor Adapter to respond to automatically.

POST Watchdog

Use the **POST Watchdog** field to specify the number of minutes that the Remote Supervisor Adapter will wait for this server to complete a power-on self-test (POST). If the server being monitored fails to complete a POST within the specified time, the Remote Supervisor Adapter generates a POST time-out alert and automatically restarts the server. The POST watchdog is then disabled automatically until the operating system is shut down and the server is power-cycled (or if the operating system and device drivers successfully load).

Note: Power-cycling differs from shutting down and restarting the operating system in that power-cycling removes power from the server completely. For example, unplugging your server.

To set the POST time-out value, select a number from the menu. To turn off this watchdog, select **Disabled**.

Note: If the **POST Time-out** checkbox is selected in the Remote Alerts section of the Remote Alerts page, the Remote Supervisor Adapter attempts to forward the alert to all enabled remote alert recipients. Also, this watchdog requires a specially constructed POST routine available on only specific IBM servers. If this routine does not exist on your server, all settings in this field will be ignored.

Consult your server documentation for further details.

O/S Watchdog

Use the **O/S Watchdog** field to specify the number of minutes between checks of the operating system by the Remote Supervisor Adapter. If the operating system fails to respond to one of these checks, the Remote Supervisor Adapter generates an O/S time-out alert and automatically restarts the server. After the server is restarted, the O/S watchdog is disabled until the operating system is shut down and the server is power-cycled.

To set the O/S watchdog value, select the time interval from the menu. To turn off this watchdog, select **Disabled**. To capture blue screens, you must enable this field and check the **O/S Time-out** checkbox in the Remote Alerts section of the Alerts page.

Notes:

a. The O/S watchdog feature requires the IBM System Management device driver to be installed on the server.

b. If the **O/S Time-out** checkbox is checked in the Remote Alerts section of the Alerts page, the Remote Supervisor Adapter will attempt to send an alert to all enabled remote alert recipients.

Loader Watchdog

Use the **Loader Watchdog** field to specify the number of minutes that the Remote Supervisor Adapter waits between the completion of POST and the loading of the operating system. If this interval is exceeded, the Remote Supervisor Adapter generates a loader time-out alert and automatically restarts the system. After the system is restarted, the loader time-out is automatically disabled until the operating system is shut down and the server is power-cycled (or if the operating system and device driver successfully loads).

To set the loader time-out value, select the time limit that the Remote Supervisor Adapter will allow for O/S loading to complete. To turn off this watchdog, select **Disabled**.

Note: If the **Loader Time-out** checkbox is selected in the Remote alerts section of the Alerts page, the Remote Supervisor Adapter will send an alert to all enabled remote alert recipients.

Power Off Delay

Use the **Power Off Delay** field to specify how long that the Remote Supervisor Adapter will wait for the operating system to shut down before turning off the system. By default, the Remote Supervisor Adapter waits 30 seconds.

Shut down your server to find the length of time it takes to shut down. Add a time buffer to that value and use it as your power off delay setting to ensure that the operating system has time for an orderly shutdown before power is removed from the server.

Attention: You must have the UM server extension code installed to enable an orderly operating system shutdown. If you do not have the UMS code installed, the server turns off after waiting for the length of time you set in the **Power Off Delay** field. You could lose or corrupt data on your server. For more information on installing UM server extension code for the Remote Supervisor Adapter, see your *Remote Supervisor Adapter Installation Guide*. In order for the operating system on the server to receive the shutdown notification from the Remote Supervisor Adapter, the server must have the IBM System Management device driver installed, as well as Netfinity® Manager with UM Server Extensions for the ASM component.

To set the power-off delay value, select the time from the menu.

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 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.

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. Click **System** in the navigation frame.

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 the **Save** button.

Creating a login profile

Complete the following steps to configure a login profile:

1. Click **Login Profiles** in the navigation frame.

   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:

3. Type the name of the profile in the **Login ID** field.

   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 in your dial-in profile when dialing into the Remote Supervisor Adapter.

4. Select either Read Only or Read/Write in the **Authority Level** field 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, people who log in with read-only IDs are restricted from performing any file transfers, any 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. Assign the login ID a password in the **Password** field.

   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 in your dial-in profile when dialing into the Remote Supervisor Adapter.

6. Reenter the password in the **Confirm Password** field.

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

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

8. Type the phone number that the Remote Supervisor Adapter should use when dialing-back to reach the login ID in the **Number** field.

   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 the **Save** button to save your login ID settings.

Setting the modem/dial-in settings

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

1. Click **Login Profiles** in the navigation frame.

2. Scroll down to the Modem/Dial-in Settings section.

3. If you want to allow remote users to dial into the Remote Supervisor Adapter through a serial connection, select Enabled in the **Dial-in Support Status** field.

4. Use the **Delay Before Next Remote Login** field to 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.

Configuring remote alert recipients

You can set the Remote Supervisor Adapter to provide alerts for a number of different situations, including the remote alert recipients, number of alert attempts, incidents that trigger remote alerts, and local alerts. Use these remote alert recipient links to view, configure, or change individual alert recipients. You can define up to 12 unique recipients. Each link for an alert recipient is labeled with the recipient name.

When you configure a remote alert entry, the Remote Supervisor Adapter, ASM processor, or ASM PCI Adapter sends an alert to a remote system (through a serial connection or a network connection, a numeric pager, or an alphanumeric pager) when any of the events selected from the **Enabled Alerts** group occurs. This alert will contain information about the nature of the event, the time and date of the event, and the name of the system that generated the alert.

The Remote Supervisor Adapter offers alert redundancy for several managed systems at the same location. It sends alerts only once per connection type even when there is more than one active LAN or serial connections. But if one connection device fails, all other interconnected devices route the alerts to the next available connection. This flexibility applies to remote access capabilities.

If the **SNMP Agent** or **SNMP Traps** fields are not enabled, no SNMP type alerts will be sent. For more information on these fields, see "Configuring SNMP" on page 30.

Note: You cannot distinguish between what alerts will be sent to which remote alert recipient. All configured recipients receive each alert you select.

Complete the following steps to configure a remote alert recipient:

1. Click **Alerts** in the navigation frame.
2. Click one of the remote alert recipient links. An individual recipient page similar to the following appears.

3. Select **Enabled** from the **Status** field.
4. Type the name of the recipient or other identifier in the **Name** field. The name you enter appears as the recipient's link on the Alerts page.
5. Select the notification method for reaching the recipient in the **Notification** field. Select from one of the following notification methods:

   - Numeric pager
   - Alphanumeric pager
   - IBM Director over Modem
   - IBM Director over LAN
   - SNMP over LAN
   - E-mail over LAN
   - SNMP over PPP
   - E-mail over PPP

> **Note:** If you select to send remote alerts by the IBM Director over Modem or IBM Director over LAN options, you must have UM Server Extensions installed onto the IBM Director server.

6. Type either the phone number, IP address, or hostname at which to reach the recipient in the **Number** field.

   Type a phone number if you are using one of the following notification methods:

   - Numeric pager (follow the phone number with a comma and the personal identification number [PIN])
   - Alphanumeric pager
   - IBM Director over Modem
   - SNMP over PPP
   - E-mail over PPP

   Type an IP address or hostname if you are using the IBM Director over LAN method.

7. If you chose alphanumeric pager as the notification method, enter the PIN in the **PIN** field.

8. If you selected the E-mail over LAN or E-mail over PPP notification methods, type the recipient's e-mail address in the **E-mail Address** field.

   > **Note:** For the E-mail over LAN and E-mail over PPP notification methods to work properly, configure the Simple Mail Transfer Protocol (SMTP) options on the Network Protocols page. For more information about SMTP options, see "Configuring SNMP" on page 30.

9. If you selected the E-mail over PPP or SNMP over PPP notification methods, type the login ID needed to log onto the recipient's internet service provider (ISP) at the **PPP Login ID** field. The PPP login ID consists of your secure IP address, your account name, and your user ID all separated by periods.

   > **Note:** For the SNMP over LAN and SNMP over PPP notification methods to work properly, configure the SNMP options on the Network Protocols page. For more information on SNMP, see "Simple network management protocol" on page 29.

10. If you selected the E-mail over PPP or SNMP over PPP notification methods, type the password that accompanies the login ID at the **PPP Password** field.

    Enter the password needed to login to the internet service provider (ISP). You must fill in this field for the E-mail over PPP and SNMP over PPP notification methods.

11. Click the **Save** button to save your remote alert recipient profile. Repeat steps 3 through 11 for each remote alert recipient profile.

12. Click the **Generate Test Alert** button to send a test alert to all enabled alert recipients.

    > **Note:** All selected alert events will be sent to all enabled alert recipients.

13. Complete the "Setting remote alert attempts" procedure.

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 **Alerts** in the navigation frame.

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 the **Save** button.
4. Complete the "Setting remote alerts" procedure.

Setting remote alerts

Complete the following steps to select the remote alerts to be sent:

1. Select **Alerts** in the navigation frame.
2. Scroll down to the Remote Alerts section.
3. Select the alerts you want sent.

   The remote alerts are categorized by the following levels of severity:

   - Critical
   - Warning
   - System

   All alerts are tracked in the event log and sent to all configured remote alert recipients.

   Critical alerts

   Critical alerts are generated for events that signal that the server is no longer functioning.

Table 6. Critical remote alerts

Event	Action
Hard disk drive	Generates an alert if one or more of the hard disk drives in the system fail.
Multiple fan failure	Generates an alert if two or more of the cooling fans in the system fail.
Power failure	Generates an alert if any of the system power supplies fail.
Tamper	Generates an alert if physical intrusion of the server box is detected. Tamper monitoring is not available on some servers, in which case this setting is ignored.
Temperature	Generates an alert if any of the monitored temperatures are outside critical threshold values. These threshold values can be found by clicking the temperature readings on the System Health page. If a critical temperature condition is detected, the server will automatically shut down and turn off whether this field is selected or not.

Table 6. Critical remote alerts

Event	Action
Voltage	Generates an alert if the voltages of any of the monitored power supplies fall outside their specified operational ranges. These operational ranges are accessed by clicking the voltage readings on the System Health page. If a critical voltage condition is detected, the server will automatically shut down and turn off whether this field is selected or not.
VRM failure	Generates an alert if one or more VRMs fail. VRMs are not used on some servers, in which case this setting is ignored.

Warning alerts

Warning alerts are generated for events that might progress to a critical/error level.

Table 7. Warning remote alerts

Event	Action
Single fan failure	Generates an alert if one fan fails.
Temperature	Generates an alert if any monitored temperatures are outside the warning threshold values. These temperature threshold values are accessed by clicking the temperature readings on the System Health page. Unlike the critical temperature event, this event will not initiate an automatic system shutdown.
Voltage	Generates an alert if any monitored voltages are outside the warning threshold values. These voltage range values are accessed by clicking the voltage readings on the System Health page. Unlike the critical voltage event, this event will not initiate an automatic system shutdown.
Redundant power supply	Generates an alert if a redundant power supply fails.

System alerts

System alerts are generated for events that occur as a result of system errors.

Note: Hard disk drive Predictive Failure Analysis® (PFA) alerts are not monitored.

Table 8. System remote alerts

Event	Action
Boot failure	Generates an alert if an error occurred that prevented the system from starting.
Loader timeout	Generates an alert if a system loader timeout value is enabled and has been exceeded. The system loader timeout value is configured in the Server Timeouts section on the System page.
O/S timeout	Generates an alert if the operating system timeout value is enabled and has been exceeded. The operating system timeout value is configured in the Server Timeouts section on the System page. This alert must be checked for remote blue screen capture.

Table 8. System remote alerts

Event	Action
PFA	Generates an alert if a PFA notification is generated by the system hardware. This feature is available only on systems that have PFA-enabled hardware. This setting is ignored by systems without PFA-enabled hardware.
POST timeout	Generates an alert if the POST timeout value is enabled and has been exceeded. The POST timeout value is configured in the Server Timeouts section on the System page.
Power off	Generates an alert if the system is turned off.
Power on	Generates an alert if the system is turned on.

4. Click the **Save** button.
5. Complete the "Setting local events" procedure.

Setting local events

Complete the following steps to select the local events to which the Remote Supervisor Adapter will respond:

1. Click **Alerts** in the navigation frame.
2. Scroll down to the Local Events section.
3. Select the events to store in the event log. The Remote Supervisor Adapter stores the notification only in the event log.

    In a future release of the Remote Supervisor Adapter, local events will be sent to the server where the Remote Supervisor Adapter resides. These events will not be sent to remote alert recipients.

Table 9. Local events

Event	Action
Event log 75% full	Generates a local notification if the event log reaches 75% of capacity.
Voltage	Generates a local notification if any of the monitored voltages exceed their thresholds.
Power off	Generates a local notification if the server is powered off.
Power supply failure	Generates a local notification if a power supply failure is detected.
Event log full	Generates a local notification if the event log reaches its capacity. At capacity, the oldest events are deleted.
Redundant power supply	Generates a local notification if the redundant power supply fails.
Tamper	Generates a local notification if the server covers are removed. This feature is only available on some servers.
DASD failure	Generates a local notification if any hard disk drive failures are detected.
Remote login	Generates a local notification if a remote login occurs.
Temperature	Generates a local notification if any of the monitored temperatures exceed thresholds.
Fan failure	Generates a local notification if one or more cooling fans fail.

Table 9. Local events

Event	Action
PFA	Generates a local notification if any of the hardware in the system generates a PFA.

4. Click the **Save** button.

5. Complete the "Adding event log to e-mail alert notifications" procedure.

Adding event log to e-mail alert notifications

Complete the following steps to add the event log as an attachment to remote alert recipients who are selected to receive alert notification:

1. Click **Alerts** in the navigation frame.

2. Scroll down to the E-mail Attachments section.

   You can attach detailed information to alert recipients set up to receive e-mail as their notification method.

3. Select the **Include Event Log With E-mail Alerts** check box in the E-Mail Attachments section to attach the local event log to all e-mail alert notifications. The event log provides a summary of the most recent events and assists with problem identification and fast recovery.

   Notes:

   a. To send the event log as an e-mail attachment, you must select E-mail over LAN or E-mail over PPP as the notification method for at least one remote alert recipient.

   b. Event logs attached in an e-mail are not forwarded to a Remote Supervisor Adapter on the ASM interconnect network.

Configuring the serial port

You can either dedicate the integrated serial port on the Remote Supervisor Adapter to system management or share it with the operating system. If dedicated to system management, the serial port serves only the Remote Supervisor Adapter and is always available for dial-in and dial-out alerting purposes. You will not be able to view the port on the network operating system (NOS) or in any other applications.

This design enables a single serial port 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 a serial port" on page 29.

1. Click **Serial Port** in the navigation frame.

2. Select the data transfer rate at the **Baud Rate** field.

Use the **Baud Rate** field to 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. Select the error detection to be used in your serial connection at the **Parity** field.

   Use the **Parity** field to 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" bits in the **Stop Bits** field that will follow the data or any parity bit to mark the end of a transmission (normally a byte or character).

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

5. Click the **Dedicate to ASM** checkbox to reserve the serial port for the Remote Supervisor Adapter.

   If shared with the operating system, the serial port serves the Remote Supervisor Adapter only while the server is turned off or on during the power-on self-test (POST). The operating system can access it after the POST completes. Only with a critical event will the Remote Supervisor Adapter take over the port from the NOS to dial-out and transmit an alert. The port then remains under the Remote Supervisor Adapter control until the server is restarted.

   Note: If you have configured a PPP interface, dedicate the serial port to the Remote Supervisor Adapter or you will lose the PPP port when the host restarts.

6. Click the **Save** button.

7. 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   Hangup String*
ATDT   ATH0^M

Dial Postfix String*   Modem Query*
^M   AT^M

Factory Settings String*   Auto Answer*
AT&F0^M   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 manually entered at the end of the field value.

Table 10. 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 dialout 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.
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.

8. Click the **Save** button.

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. Click **Network Interfaces** in the navigation frame. A window similar to the following opens:

2. If you want to use an Ethernet connection, select Enabled in the **Interface** field. It is enabled by default.

3. If you want to use a dynamic host configuration protocol (DHCP) server connection, enable the **DHCP** field. It is enabled by default. Go to step 12.

    Note: 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. Type the IP hostname of the Remote Supervisor Adapter in the **Hostname** field. You must only do this if DHCP is disabled.

    You can enter 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 hostname of the Remote Supervisor Adapter (the **Hostname** 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 hostname. The non qualified IP hostname consists of up to the first period of a fully qualified IP hostname. For example, the non qualified IP hostname of `asmcard1.us.company.com` (a fully qualified IP hostname) is `asmcard1`. For more information on your hostname, see "Setting system information" on page 13.

5. Type the IP address of the Remote Supervisor Adapter in the **IP Address** field. You must only do this if DHCP is disabled. The IP address must contain:

    - Four integers from 0 to 255 separated by periods
    - No spaces

6. Type your network gateway router in the **Gateway Address** field. You must only do this if DHCP is disabled. The gateway address must contain:
   - Four integers from 0 to 255 separated by periods
   - No spaces or consecutive periods

7. Type the subnet mask used by the Remote Supervisor Adapter in the **Subnet Mask** field. You must only do this 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 11. 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 your network's capability. 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 - 1514. The default value for this field is 1514.
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 zero and nine. 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 the **Save** button.

11. Click the **Back** button 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 server's hostname.

12. Click the **Save** button.

13. Click the **Restart ASM** link in the navigation frame 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.

1. Click **Network Interfaces** in the navigation frame. Scroll down to the PPP over Serial Port section.

```
PPP over Serial Port

  Interface
  Disabled ▼

  Local IP Address        Remote IP Address        Subnet Mask
  192.96.1.1              192.96.1.2               255.255.255.255

  Authentication
  CHAP then PAP ▼
```

2. Select Enabled in the **Interface** field.

3. Enter the local IP address for the PPP interface on this Remote Supervisor Adapter in the **Local IP Address** field. 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. Enter the remote IP address that this Remote Supervisor Adapter will assign to a remote user in the **Remote IP Address** field. 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. Enter the subnet mask that will be used by the Remote Supervisor Adapter in the **Subnet Mask** field. 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 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.
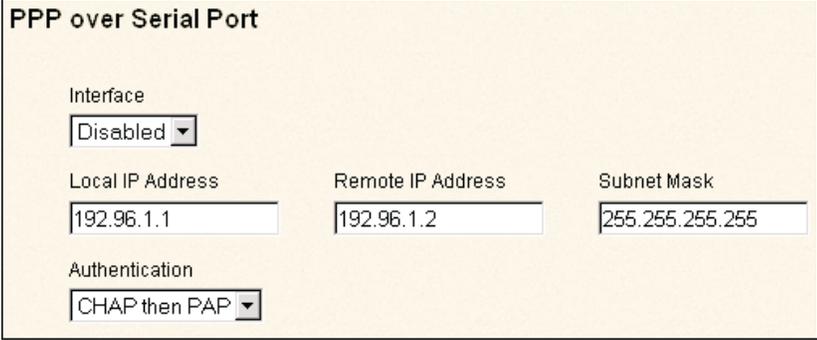
7. Click the **Save** button.

8. Click the **Restart ASM** link in the navigation frame 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 hostnames 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 13.

2. Click **Network Protocols** in the navigation frame. A window similar to the following opens:

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 13.
   - 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. 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
   - 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, enter a name or authentication string that corresponds to the desired community.

6. Enter the hostname or IP addresses of each community manager in the corresponding **IP Address** field.

7. Scroll to the Domain Name System (DNS) section.

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

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

b. The Remote Supervisor Adapter examines this table first for an address to hostname 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 hostname defined in the table will override any corresponding entry defined on the DNS server.

10. Click the **Save** button.

11. Click the **Restart ASM** link in the navigation frame to activate the changes.

Configuring SMTP

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

1. Click **Network Protocols** in the navigation frame.

2. Scroll down to the Simple Mail Transfer Protocol (SMTP) section.

3. Enter the hostname of the of SMTP server in the **SMTP Server Host Name or IP Address** field.

   Use this field to specify either the IP address or, if DNS is enabled and configured, the hostname 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:

- Remotely control the power status of the server
- Update firmware
- Backup 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

Server power and restart activity

This section displays the active status of the system. For more information on this section, see "Monitoring the remote server status" on page 7.

Remotely controlling the power status of a server

The Remote Supervisor Adapter 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.

Power on server immediately
> To turn on this server and start the operating system, click the **Power On Server Immediately** link.

Power off server immediately
> To turn off this server without shutting down the operating system, click the **Power Off Server Immediately** link.

Shutdown O/S and then power off server
> To shut down the operating system and then turn off this server, click the **Shutdown O/S and then Power Off Server** link. This option requires that the IBM System Management device driver is installed on the server, as well as the agent component of Netfinity Director with UM Server Extensions.

Shutdown O/S and then restart server
> To restart the operating system, click the **Shutdown O/S and then Restart Server** link. This option requires that the IBM System Management device driver is installed on the server, as well as the agent component of Netfinity Director with UM Server Extensions.

Restart the server immediately
> To turn off and then turn on this server immediately without shutting down the operating system first, click the **Restart the Server Immediately** link.

A confirmation page opens if you select any of these options, allowing you to cancel the operation if it was selected accidentally.

Attention: You must have the UM server extensions code installed to allow graceful operating system shutdown. If you do not have the UM server extensions code installed, the server powers off after waiting for the length of time you set in the **Power Off Delay** field. You could lose or corrupt data on your server. For more information on installing UMS code for the Remote Supervisor Adapter, see your *Remote Supervisor Adapter Installation Guide*.

To perform any of these actions, you must have read/write access to the Remote Supervisor Adapter. With the operating system shutdown options, the Remote Supervisor Adapter communicates with the system-management software through the device driver and the system-management software initiates the shutdown.

Note: In order for the operating system on the server to receive the shutdown notification from the Remote Supervisor Adapter, the server must have the IBM System Management device driver installed, as well as Netfinity Manager with UM Server Extensions for the ASM component.

Updating firmware

Use the Transfer Files option on the navigation frame to update firmware of the Remote Supervisor Adapter or server.

Complete the following steps to update the startup or main application files of your Remote Supervisor Adapter. Updating firmware also enables BIOS code, diagnostics, power backplane, front panel, and serial peripheral interface (SPI) of the server in which the Remote Supervisor Adapter is installed, to be updated remotely using this function.

1. Click **Transfer Files** in the navigation frame.

2. Click the **Browse** button.

3. Navigate to the .pkt or .pkc file you want to update.

   Note: When you transfer (or flash) the main application packet, you must also flash the remote graphics packet separately.

4. Click **Open**.

   The file (including the full path) appears in the box beside the **Browse** button.

5. To begin the update process, click the **Update** button.

   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 completed.

6. Verify that the .pkt or .pkc file shown on the Confirm Firmware Update page is what you intend to update. If not, click the **Cancel** button.

7. To complete the update process, click the **Update** button again.

   A progress indicator opens as the firmware on the Remote Supervisor Adapter is flashed. A confirmation page opens to verify whether the update was successful.

8. After receiving a confirmation that the update process is complete, go to the Restart ASM page and click the **Restart** button.

9. Click the **OK** button in the window that opens to confirm that you want to restart the Remote Supervisor Adapter.

10. Click the **OK** button in the window that opens to close the current browser window.

11. To log onto the Remote Supervisor Adapter again, open your browser and follow your regular logon process.

    Note: To cancel this process at any point, click the **Cancel** button 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 corrupted. It also can be used as a base that you can modify in order to configure multiple Remote Supervisor Adapters with similar configurations.

Complete the following steps to backup your current configuration:

1. Click **Transfer Files** in the navigation frame.
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 backup this configuration, click **Backup**.
5. Type a name for the backup and choose the location where the file should be saved, 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 onto the Remote Supervisor Adapter, the configuration of which you want to restore.
2. Click **Transfer Files** in the navigation frame.
3. Click the **Browse** button.
4. Click the desired configuration file and then click **Open**. The file (including the full path) appears in the box beside the **Browse** button.
5. Click the **Restore** button. A configuration summary panel will be displayed.
6. Verify that this is the configuration that you want to restore. If it is not the correct file, click the **Cancel** button.
7. To proceed with restoring this file to the Remote Supervisor Adapter, click the **Restore Configuration** button.
8. After receiving a confirmation that the restore process is complete, go to the Restart ASM page and click the **Restart** button.
9. Click the **OK** button in the window that opens to confirm that you want to restart your Remote Supervisor Adapter.
10. Click the **OK** button in the window that opens to close the current browser window.
11. To log onto the Remote Supervisor Adapter again, open your browser and follow your regular logon 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 re-enter common, shared information.

Complete the following steps to restore a changed configuration:

1. Log onto the Remote Supervisor Adapter, the configuration of which you want to restore.

2. Click **Transfer Files** in the navigation frame.

3. Click the **Browse** button in the Restore ASM Configuration section.

4. Navigate to the configuration file and then click the **Open** button. The file (including the full path) appears in the box beside the **Browse** button.

5. Click the **Modify and Restore** button 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 the **Toggle View** button at the top or bottom of the page.

6. To modify the contents of any field, click in the corresponding text box and enter the data.

7. Verify that the displayed configuration is what you want to restore.

8. Click the **Restore Configuration** button. A progress indicator appears as the firmware on the Remote Supervisor Adapter is flashed. A confirmation page will be displayed to verify whether the update was successful.

9. After receiving a confirmation that the restore process is complete, go to the Restart ASM page and click the **Restart** button.

10. Click the **OK** button in the window that opens to confirm that you want to restart your ASM Web interface.

11. Click the **OK** button in the window that opens to close the current browser window.

12. To log onto the Remote Supervisor Adapter again, open your browser and follow your regular logon 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. The ASM Interconnect column provides a link labelled **login** that enables you to quickly access each remote system.

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

1. Click **Access Remote ASM** on the navigation frame. The Remote Access ASM table appears, listing other processors and adapters linked to the host server. The table also displays the system health and processors and adapters name (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 Connection column heading.

   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 two minutes for servers to be removed from the table when detached from the ASM interconnect network.

   The Enter Network Password window opens.

3. Enter your username and password.

4. The ASM window opens, giving you access. The processors and adapters name appears in orange above the navigation frame.

   Note: Depending on the system-management processor or adapter that is on the remote server, some options might not be available.

Restoring ASM

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

1. Click **Power/Restart** in the navigation frame for options on restarting the Remote Supervisor Adapter.

2. Click **Restore Defaults** in the navigation frame to refresh the Remote Supervisor Adapter and click the **Restore Defaults** button. Your TCP/IP or modem connections will be broken and you will need to login again to use the ASM Web interface.

   Attention: When you click the **Restore Defaults** button, 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 code setup if you click the **Restore Defaults** button.

Restarting ASM

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

1. Click **Power/Restart** in the navigation frame for options on restarting the Remote Supervisor Adapter.

2. Click **Restart ASM** in the navigation frame to refresh the Remote Supervisor Adapter and click the **Restart ASM** button. Your TCP/IP or modem connections will be broken and you will need to login again to use the ASM Web interface.

   Attention: When you click the **Restart ASM** button, 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 code setup if you click the **Restart ASM** button.

Remote graphical control

From the Remote Control page, you can:

- View the server graphical desktop image
- Restart the server and view the POST process in a telnet window
- View the image of the blue screen capture

You must log in with a user ID that has read/write access to use any of the remote control features besides viewing blue screen capture. You must also know the remote control password that is set on the remote server during BIOS code setup. After the password is accepted, you gain access to the server desktop. You do not need the remote control password to view the blue screen capture.

Notes:

1. You can have only one remote control session functioning at a time.

2. The keystroke events sent by the remote client will not be received by 16-bit applications (for example, EDIT.COM or DEBUG.COM) running under Windows NT or Windows 2000.

Accessing server graphical console

Click the **Redirect Console** button to view an interactive graphical user interface (GUI) display of the server. You see on your monitor exactly what you see on the server desktop, and you have full keyboard and mouse control of the desktop. Complete the following steps to remotely access a server graphical console.

Note: For best performance, set the server desktop to the following settings:

- Supported resolutions: 640 x 480 pixels, 800 x 600 pixels, 1024 x 768 pixels
- Supported color depths: 256 colors, 65536 colors, True Color
- 800 x 600 pixels provides best results
- 65536 colors provides best color depth

1. Click **Remote Control** on the navigation frame.
2. Click **Redirect Graphical Console**. A Java™ applet opens in a separate browser window.
3. Enter the remote control password in the **Password** field. This password is configured locally on the server during the BIOS code update at the **PAP** field.
4. The server desktop opens on your screen.

   Note: For optimal viewing, set the resolution of the remote system to one setting smaller than the resolution of the monitor you will be viewing. For example, set the remote system resolution to 800 x 600 pixels if the monitor you are remotely viewing on is set to 1024 x 768 pixels.

5. If a Microsoft Windows logon window opens, press **CTRL+ALT+DEL** to proceed. If the remote desktop is already displayed, use the mouse or the keyboard to navigate.

   You can disconnect at any time by closing the applet windows.

Viewing server text console

Click the **Redirect Text Console** button to view an interactive text display of the server. If the server is running an operating system without a graphical user interface (GUI) or the operating system is currently in a text-on mode, this option allows you to see on your monitor exactly what you would see on the server monitor, and have full keyboard and mouse control of the desktop. Selecting the redirect text console does not restart the server.

Complete the following steps to remotely access a server's text console:

1. Click **Remote Control** on the navigation frame.
2. Click the **Redirect Text Console** button to access the server text console. A Java applet launches in a separate browser window.
3. Enter the remote control password. This password is configured locally on the server during the BIOS code update.
4. A telnet session opens, displaying the server text console on your screen.

   You can disconnect at any time by closing the applet window.

Viewing server POST

Click the **View Remote POST** button to restart the server and view the POST within a telnet window. You can interrupt the POST and access the server's BIOS code run. You see on your monitor exactly what you would see on the server desktop, and have full keyboard and mouse control of the desktop. Complete the following steps to remotely access a server POST:

1. Click **Remote Control** on the navigation frame.
2. Click the **View Remote POST** button to access the server POST. A message is displayed, confirming that the server will be restarted.
3. Enter the remote control password. This password is configured on the server during BIOS code setup at the **PAP** field.
4. A telnet session opens, displaying the server text console on your screen.

   You can disconnect at any time by closing the applet windows.

Viewing server blue screen

Click the **View Windows Blue Screen** button to access an image of the blue screen captured when the server stopped functioning. The blue screen image shows the date and time of the capture. To capture a blue screen event, you must enable the **O/S timeout** option on the System page. You also must be using Windows NT or Windows 2000 for this feature to function. The Remote Supervisor Adapter stores only the latest blue screen image. For more information on the **O/S timeout** option, see "Setting server timeouts" on page 14.

If a blue screen event happens while the operating system is up and running, the Remote Supervisor Adapter captures the blue screen and stores it. The image will not be overwritten during the next operating system install because the Remote Supervisor Adapter does not capture the operating system installation screen. Only error conditions are captured and maintained. The Remote Supervisor Adapter stores only the most recent error event information, overwriting older information when a new error event occurs.

Complete the following steps to remotely access a server's blue screen image:

1. Click **Remote Control** on the navigation frame.
2. Click **View Windows Blue Screen**. The blue screen image is displayed on your screen.

Logging off

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

1. Click **Log Off** on the navigation frame.
2. If you are running Internet Explorer, click the **Yes** button in response to 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 the **OK** button in response to 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 also access the Remote Supervisor Adapter via the text-based user interface by establishing a telnet connection or a direct serial connection.

Accessing a text-based interface via a telnet connection

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

1. Open your computer MS-DOS Command Prompt program.

2. Type `telnet` and either the hostname 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 42.

4. Type a user name at the **Login ID** field.

5. Type the password associated with the username at the **Password** field. The Advanced System Management window opens.
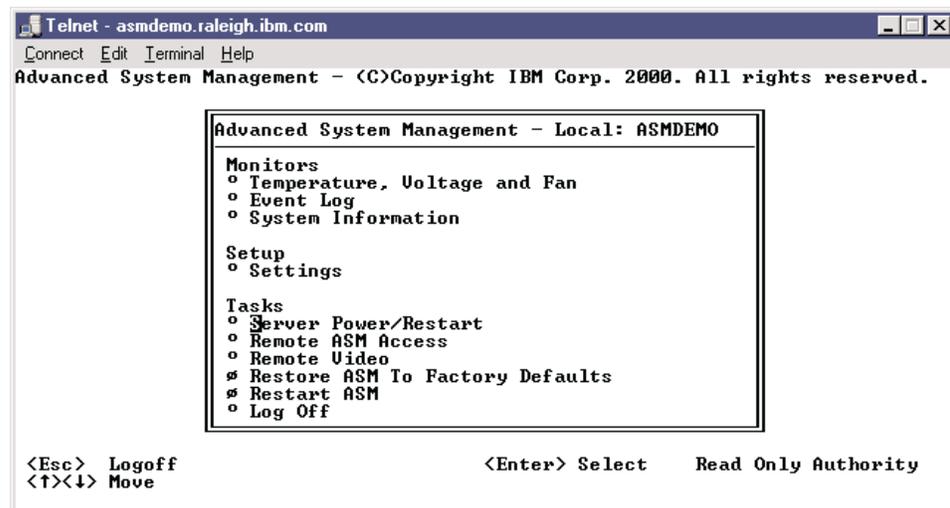
> **Note:** Press the up and down arrows to navigate your screen. Press Esc to exit to the Advanced System Management window; if you press Esc at the Advanced System Management window, you logoff from your session. Press F3 to exit the window you are viewing.

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 the **Configure** button and set the following values:

Table 12. COM properties

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

6. Click the **OK** button.
7. Click the **Settings** tab.
8. Select the **Terminal Keys** option and the **ANSI** option from the **Emulation** field.
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.
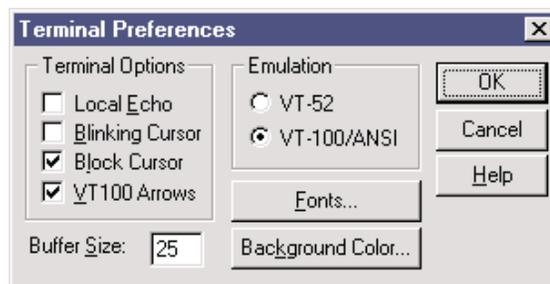
2. Select the following checkbox options:
   - **Blinking Cursor**
   - **Block Cursor**
   - **VT100 Arrows**
   - **VT-100/ANSI**
3. Click the **Fonts** button. The Font window opens.
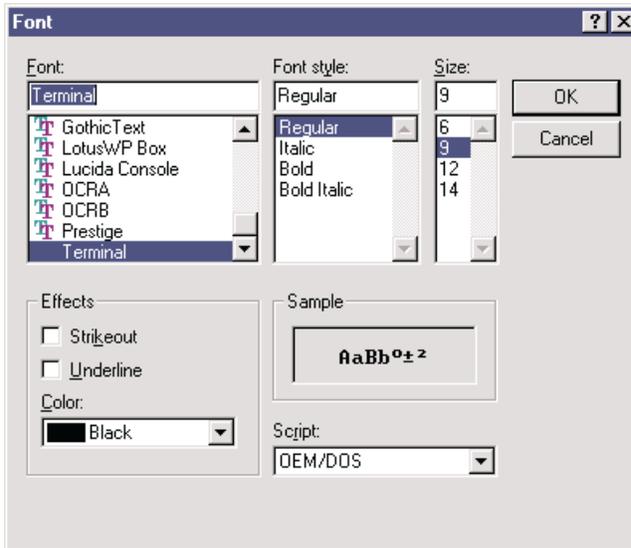
4. Select the Terminal font from the Font window. Select 9 for the font size in the Size window.

5. Click **OK**.

Chapter 7.   Monitoring your system health through a text-based interface

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

Monitoring temperatures, voltage, and fans readings

Complete the following steps to access the temperature, voltage, and fan readings of the remote server. The Remote Supervisor Adapter tracks the current temperature readings and threshold levels for system components such as microprocessors, the system board, and the hard disk drive backplane.

1. Select the **Temperature, Voltage and Fan** option. A window similar to the following opens:

```
Temperature, Voltage and Fan - Local: ASMDEMO

System Power Status: Off
Power On Hours: 0
Reboot Count: 0
System State: System power off/State unknown

These tables will take a few moments to process:
° Temperature Tables
° Voltage Tables
° Fan Table
```

2. Select the **Temperature Tables** option. A window similar to the following opens:

```
Temperature Tables - Local: ASMDEMO

° CPU Temperatures
° Dasd Temperatures
° System Temperatures
```

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

Warning
> If a temperature reaches a certain value, a temperature warning is sent to remote alert recipients if set in the Critical/Warning Remote Alerts window. For more information on setting the Temperature option, see "Configuring remote alert recipients" on page 56.

Soft Shutdown
> If a temperature reaches a certain value higher than the warning value, a second temperature warning is sent to remote alert recipients (if set in the Critical/Warning Remote Alerts window) and the system begins the shutdown process with an orderly operating system shutdown followed by a power off.

Hard Shutdown
> If a temperature reaches a certain value higher than the soft shutdown value, the system immediately shuts down and sends an alert to configured recipients (if set in the Critical/Warning Remote Alerts window).

Warning Reset

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

3. Select the **Voltage Tables** option. The Remote Supervisor Adapter will send an alert if any monitored power source voltage falls outside their specified operational ranges. The system displays the voltage readings of the system board (planar) and the voltage regulation modules (VRM).

The voltage tables windows display the voltage ranges at which the Remote Supervisor Adapter reacts. These levels are preset on the remote server and cannot be changed. The system sets a voltage range at which the following actions are taken:

Warning

If the voltage drops below or exceeds a specific voltage range, a voltage warning is sent to remote alert recipients if set in the Critical/Warning Remote Alerts window. For more information on setting the Temperature option, see "Configuring remote alert recipients" on page 56.

Soft Shutdown

If the voltage drops below or exceeds a specific voltage range, a voltage warning is sent to remote alert recipients (if set in the Critical/Warning Remote Alerts window) and the system begins the shutdown process with an orderly operating system shutdown followed by a power off.

Hard Shutdown

If the voltage drops below or exceeds a specific voltage range, the system immediately shuts down and sends an alert to configured recipients (if set in the Critical/Warning Remote Alerts window).

Warning Reset

If the voltage has dropped below or exceeds the warning voltage range and then recovers to that range, the system temperature assumes the temperature has returned to normal and no further alerts will be generated.

4. Select the **Fan Table** option. The Fan Speeds window displays the running speed of the system fans (converted to 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.

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 dialout 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. Select the **Event Log** option in the Advanced System Management window.

2. Select the **View Event Log** option to view the server's two most recent events.

```
View Event Log - Local: ASMDEMO

 Date:01-01-00  Time:04:14:37  Severity:I   Source:SERVPROC
 TCP connection reset by other host.

 Date:01-01-00  Time:04:07:45  Severity:I   Source:SERVPROC
 Remote Login Successful. Login ID: guest2


 ° View next log entry.
```

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 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 the **System Information** option to view the status of the hardware and software components on the server.

2. Select the **Vital Product Data (VPD)** option. The Vital Product Data windows opens:

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

  ° Machine Level VPD
  ° Component Level VPD
  ° POST/BIOS VPD
  ° ASM VPD
```

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

Machine level VPD
>   The VPD for the system is displayed in this window.

Table 13. Machine level vital product data

Field	Function
Machine type	Identifies the type of server the Remote Supervisor Adapter is monitoring.
Machine model	Identifies the model number of the server the Remote Supervisor Adapter is monitoring.

Table 13. Machine level vital product data

Field	Function
Serial number	Identifies the serial number of the server the Remote Supervisor Adapter is monitoring.

Component level VPD

The VPD for the system components is displayed in this window.

Table 14. Component level vital product data

Field	Function
FRU number	Identifies the field replaceable unit number (a seven-digit alphanumeric number) for each component.
Serial number	Identifies the serial number of each component.
Mfg ID	Identifies the manufacturer ID for each component.
Slot	Identifies the slot number where the component is located.

POST/BIOS data

You can find the VPD for the system POST or BIOS firmware code in this window.

Table 15. POST/BIOS vital product data

Field	Function
Version	Indicates the version number of the POST/BIOS code.
Build level	Indicates the level of code for the POST/BIOS code.
Build date	Indicates when the POST/BIOS code was built.

Remote Supervisor Adapter system data

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

Table 16. 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.

Component Activity Log

You can find a record of component activity.

Table 17. Component activity log

Field	Function
FRU number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric number) of the component.
Serial number	Identifies the serial number of the component.
Manufacturer ID	Identifies the manufacturer of the component.
Slot	Identifies the slot number where the component is located.
Action	Identifies the action taken by each component.
Timestamp	Identifies the date and time of the component action. The date is displayed in the MM/DD/YY format. The time is displayed in the HH:MM:SS format.

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

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

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

From the System window, you can:

- Set system information
- Set server timeouts, which will result in automatic corrective action by the Remote Supervisor Adapter

From the Login & Alert Profiles window, you can:

- Set login profiles to control access to the Remote Supervisor Adapter
- Configure modem/dial-in settings
- Configure remote alert recipients
- Set the number of remote alert attempts
- Select alerts will be monitored/sent
- Select local events to track
- Set e-mails to include event log attachment when alerts are generated

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 ASM date and time.

Setting system information

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

1. Select the **Settings** option in the Advanced System Management window. The Settings window opens:

```
Settings - Local: ASMDEMO

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

51
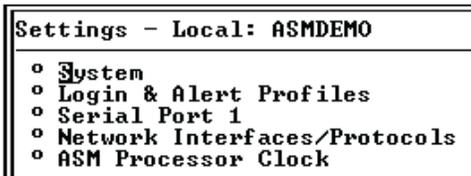
2. Select the **System** option in the System Settings window. A window similar to the following opens:

```
System - Local: ASMDEMO

        System Information
        _____

ASM Name:                 [ASMDEMO        ]
System Contact:           [No Contact Configured                      ]
System Location:          [No Location Configured                     ]

        Server Timeouts
        _____

POST Watchdog (mins):    ◄Disabled►
Loader Watchdog (mins): ◄Disabled►
O/S Watchdog (mins):     ◄Disabled►
Power Off Delay (mins): ◄0.5►
```

3. Type the name of the Remote Supervisor Adapter in the **ASM Name** field.

   Use the **ASM Name** field to specify a name for the ASM in this server. The name is included 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 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 hostname. The non-qualified IP hostname consists of up to the first period of a fully qualified IP hostname. For example, the non-qualified IP hostname of `asmcard1.us.company.com` (a fully qualified IP hostname) is `asmcard1`. For more information on your hostname, see "Configuring an Ethernet connection to ASM" on page 64.

4. Type contact information in the **System Contact** field. 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. Type in the location of the server in the **System Location** field. 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 server timeouts

Complete the following steps to set your server timeout values:

1. Select the **Systems** option in the Advanced System Management window.

2. Use the down arrow key to move down to the Server Timeouts section. You can set the Remote Supervisor Adapter to automatically respond to the following problems:

   - Halted power-on self-test

   - Halted operating system

   - Failure to load operating system

   - Failure to shut down operating system

3. Enable the server timeouts that correspond to the problems you want the Remote Supervisor Adapter to respond to automatically.

   POST Watchdog
   > Use the **POST Watchdog <mins>** field to specify the number of minutes that the Remote Supervisor Adapter will wait for this server to complete a power-on self-test (POST). If the server being monitored fails to complete

a POST within the specified time, the Remote Supervisor Adapter generates a POST time-out alert and automatically restarts the server. The POST watchdog is then automatically disabled until the operating system is shut down and the server is power-cycled (or if the operating system and device driver successfully loads).

Note: Power-cycling differs from shutting down and restarting the operating system in that power-cycling removes power from the server completely. For example, unplugging your server.

To set the POST time-out value, select a number from the menu. To turn off this watchdog, select Disabled.

Note: If the **POST Timeout** option is selected in the System Remote Alerts window, the Remote Supervisor Adapter attempts to forward the alert to all enabled remote alert recipients. Also, this watchdog requires a specially constructed POST routine available on only specific IBM servers. If this routine does not exist on your server, all settings in this field will be ignored.

Consult your server user guide for further details.

Loader Watchdog

Use the **Loader Watchdog <mins>** field to specify the number of minutes that the Remote Supervisor Adapter waits between the completion of POST and the loading of the operating system. If this interval is exceeded, the Remote Supervisor Adapter generates a loader time-out alert and automatically restarts the system. After the system is restarted, the loader time-out is automatically disabled until the operating system is shut down and the server is power-cycled (or if the operating system and device driver successfully loads).

To set the loader time-out value, select the time limit that the Remote Supervisor Adapter will allow for operating system loading to complete. To turn off this watchdog, select **Disabled**.

Note: If the **Loader Timeout** option is selected in the System Remote Alerts window, the Remote Supervisor Adapter will send an alert to all enabled remote alert recipients.

O/S Watchdog

Use the **O/S Watchdog <mins>** field to specify the number of minutes between checks of the operating system by the Remote Supervisor Adapter. If the operating system fails to respond to one of these checks, the Remote Supervisor Adapter generates an operating system time-out alert and automatically restarts the server. After the server is restarted, the operating system watchdog is automatically power-cycled.

To set the operating system watchdog value, select the time interval from the menu. To turn off this watchdog, select **Disabled**. To capture blue screens, you must enable this field and check the **O/S Timeout** option is disabled until the operating system is shut down and the server is power-cycled.

Notes:

a. The operating system watchdog feature requires the IBM System Management device driver to be installed on the server.

b. If the **O/S Time-out** option is selected in the System Remote Alerts window, the Remote Supervisor Adapter will attempt to send an alert to all enabled remote alert recipients.

Power Off Delay

Use the **Power Off Delay** field to specify the number of minutes that the Remote Supervisor Adapter will wait for the operating system to shut

down before turning off the server. By default, the Remote Supervisor Adapter waits 30 seconds.

Shut down your server to find the length of time it takes to shutdown. Add a time buffer to that value and use it as your power-off delay setting.

Attention: You must have the UM server extension code installed to enable an orderly operating system shutdown. If you do not have the UMS code installed, the server turns off after waiting for the length of time you set in the **Power Off Delay** field. You could lose or corrupt data on your server. For more information on installing UM server extension code for the Remote Supervisor Adapter, see your *Remote Supervisor Adapter Installation Guide*. In order for the operating system on the server to receive the shutdown notification from the Remote Supervisor Adapter, the server must have the IBM System Management device driver installed, as well as Netfinity® Manager with UM Server Extensions for the ASM component.

To set the power-off delay value, select the time from the menu.

Creating a login profile

Complete the following steps to configure a login profile:

1. Select the **Settings** option in the Advanced System Management window. The Settings window opens:

```
Settings - Local: ASMDEMO

  ° System
  ° Login & Alert Profiles
  ° Serial Port 1
  ° Network Interfaces/Protocols
  ° ASM Processor Clock
```
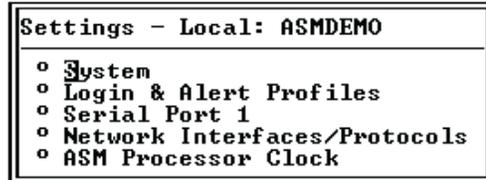
2. Select **Login & Alert Profiles** option in the Settings window. The Login & Alerts Profiles window opens:

```
Login & Alert Profiles - Local: ASMDEMO

         Login Configuration
        _____

  ° Login Settings
  ° Login Profiles

         Alert Configuration
        _____

  ° Remote Alert Settings
  ° Remote Alert Recipients
  ° Critical/Warning Remote Alerts
  ° System Remote Alerts
  ° Events For Local Notification
```
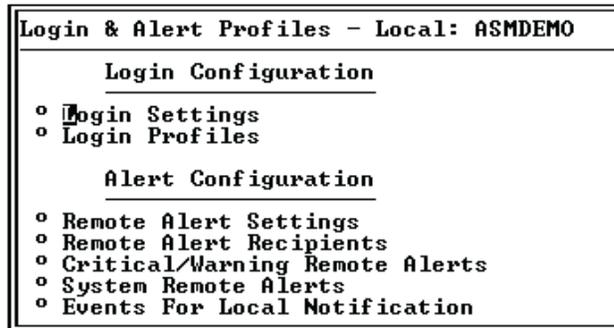
3. Select the **Login Profiles** option in the Login & Alerts Profiles section.

```
┌───┬─────────────────────────────────┬───┐
│Log││Login Profiles - Local: ASMDEMO  │   │
│   ││                                 │   │
│   ││  ° Administrator                │   │
│   ││  ° guest1                       │   │
│ ° ││  ° guest2                       │   │
│ ° ││  ° guest3                       │   │
│   ││  ° guest4                       │   │
│   ││  ° guest5                       │   │
│   ││  ° guest6                       │   │
│ ° ││  ° guest7                       │   │
│ ° ││  ° guest8                       │   │
│ ° ││  ° guest9                       │   │
│ ° ││  ° guest10                      │   │
│ ° ││  ° dp                           │   │
└───┴─────────────────────────────────┴───┘
```
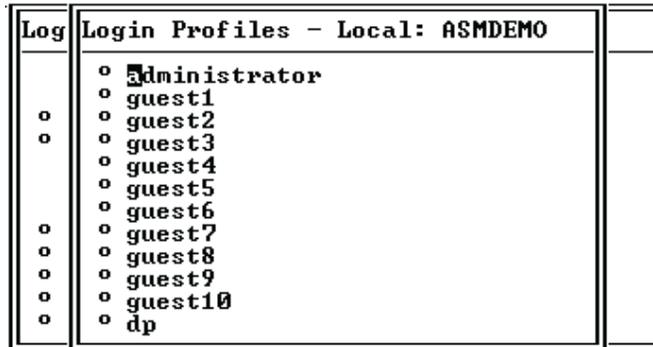
Use the Login Profiles window to view, configure, or change individual login profiles. You can define up to 12 unique profiles. If you have not configured a profile, the name of the option by default will be User *nn* where *nn* is an arbitrary number assigned to that profile.

To work with a login profile, select a profile name. A window similar to the following opens:
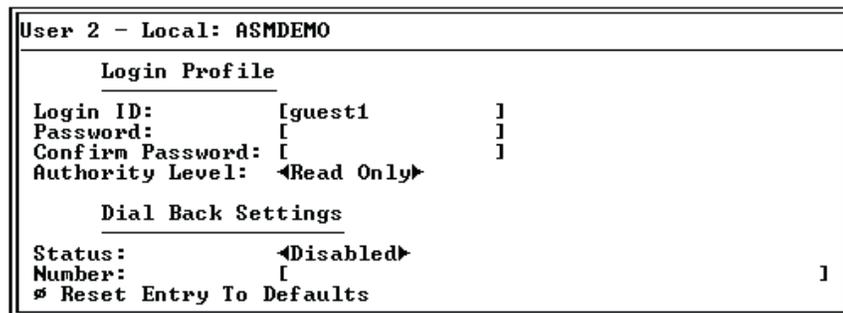
```
┌────────────────────────────────────────────────────┐
│User 2 - Local: ASMDEMO                             │
│                                                    │
│        Login Profile                               │
│        ─────────────                               │
│ Login ID:          [guest1            ]            │
│ Password:          [                  ]            │
│ Confirm Password: [                   ]            │
│ Authority Level:   ◄Read Only►                     │
│                                                    │
│        Dial Back Settings                          │
│        ──────────────────                          │
│ Status:            ◄Disabled►                      │
│ Number:            [                              ]│
│ ø Reset Entry To Defaults                          │
└────────────────────────────────────────────────────┘
```

4. Type the name of the profile in the **Login ID** field.

   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 in your dial-in profile when dialing into the Remote Supervisor Adapter.

5. Assign the login ID a password in the **Password** field.

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

   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 in your dial-in profile when dialing into the Remote Supervisor Adapter.

6. Select either Read Only or Read/Write in the **Authority Level** field.

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

   Read-Only
   > Enables the user to view a page but not to make changes. Additionally, people who log in with read-only IDs are restricted from performing any file transfers or any 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 Remote Supervisor Adapter to automatically terminate a successful dial-in attempt and then immediately dial-out to a specified number, select **Enabled** in the **Status** field of the Dialback Settings section to automatically terminate the connection and then dial out to the login ID. Otherwise, continue with step 9.

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

8. Type the phone number that the Remote Supervisor Adapter should use when dialing-back in the **Number** field.

   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 the **Login & Alert Profiles** option.

2. Select the **Login Settings** option in the Login & Alert Profiles window.

```
Login Settings - Local: ASMDEMO

Dial-in Support Status:                              ◄Disabled►

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

3. Select **Enabled** in the **Dial-in Support Status** field to allow remote users to dial into the Remote Supervisor Adapter through a serial connection.

4. Use the **Delay before next Login after Failed Attempt <mins>** field to specify how long, in minutes, the Remote Supervisor Adapter will prohibit remote login attempts, if more than five sequential failures to remotely login are detected.

Configuring remote alert recipients

You can set the Remote Supervisor Adapter to provide alerts for a number of different situations, including the remote alert recipients, number of alert attempts, incidents that trigger remote alerts, and local alerts. Use these remote alert recipient links to view, configure, or change individual alert recipients. You can define up to 12 unique recipients. Each link for an alert recipient is labeled with the recipient name.

When you configure a remote alert entry, the Remote Supervisor Adapter, ASM processor, or ASM PCI Adapter sends an alert to a remote system (through a serial connection or a network connection), a numeric pager, or an alphanumeric pager when any of the events selected from the Enabled Alerts group occurs. This alert will contain information about the nature of the event, the time and date of the event, and the name of the system that generated the alert.

If the **SNMP Agent** or **SNMP Traps** fields are not enabled, no SNMP type alerts will be sent. For more information on these fields, see "Configuring SNMP" on page 68.

Note: You cannot distinguish between what alerts will be sent to which remote alert recipient. All configured recipients receive each alert you select.

Complete the following steps to configure a remote alert recipient:

1. Select the **Remote Alert Recipients** option in the Login & Alert Profiles window.

```
Advanced System Management - Local: ASMDEMO
┌─────────────────────────────────────────────┐
│ Remote Alert Recipients - Local: ASMDEMO     │
│ ─────────────────────────────────────────    │
│   ° Recipient 1                               │
│   ° Recipient 2                               │
│   ° Recipient 3                               │
│   ° Recipient 4                               │
│   ° Recipient 5                               │
│   ° Recipient 6                               │
│   ° Recipient 7                               │
│   ° Recipient 8                               │
│   ° Recipient 9                               │
│   ° Recipient 10                              │
│   ° Recipient 11                              │
│   ° Recipient 12                              │
└─────────────────────────────────────────────┘
```
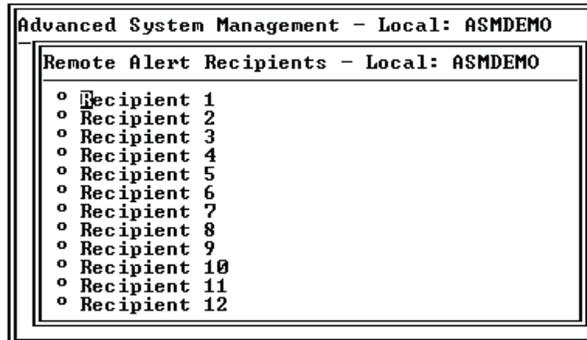
2. Select one of the remote alert recipient options. An individual recipient page appears.

```
Recipient 1 - Local: ASMDEMO

Name:                              [                    ]
Number:                            [                         ]
Status:                            ◄Disabled►
Notification Method:               ◄Numeric Pager►
PIN (alpha-numeric pager only):    [              ]

PPP Login ID:                      [                         ]
PPP Password:                      [              ]

E-mail Address(userid@hostname): [                          ]
⌀ Reset Entry To Defaults
```
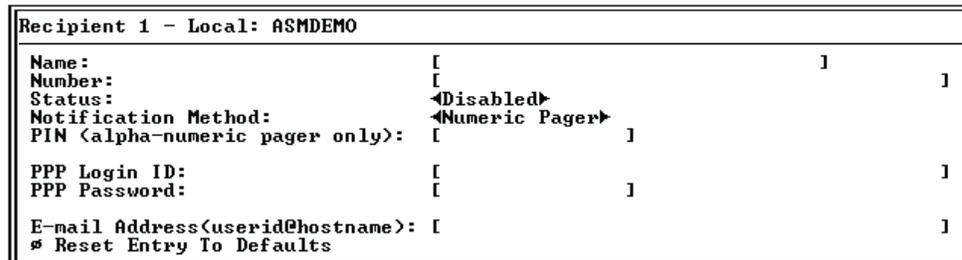
3. Type the name of the recipient or the transmission method in the **Name** field. The name that you enter appears as the recipient's name on the Remote Alert Recipients window.

4. Type either the phone number, IP address, or hostname at which to reach the recipient in the **Number** field.

   Type the phone number if you are using one of the following notification methods:

   - Numeric pager (follow the phone number with a comma and the personal identification number [PIN])
   - Alphanumeric pager
   - IBM Director over modem
   - SNMP over PPP
   - E-mail over PPP

   Type the IP address or hostname if you are using the Netfinity Manager over LAN method.

5. Select **Enabled** from the **Status** field. You can activate or deactivate remote alert recipients with the **Status** field.

6. Select the notification method for reaching the recipient in the **Notification Method** field. Select from one of the following notification methods:

- Numeric pager
- Alphanumeric pager
- IBM Director over Modem
- IBM Director over LAN
- SNMP over LAN
- E-mail over LAN
- SNMP over PPP
- E-mail over PPP

   Note: If you select to send remote alerts by the IBM Director over Modem or IBM Director over LAN options, you must have UM Server Extensions installed onto the Netfinity Director server.

7. If you chose alphanumeric pager as the notification method, enter the PIN in the **PIN (alpha-numeric pager only)** field.

8. If you select the **E-mail over PPP** or **SNMP over PPP** notification methods, type the login ID needed to log onto the recipient's internet service provider (ISP) at the **PPP Login ID** field.

   Note:

   For the SNMP over LAN and SNMP over PPP notification methods to work properly, configure the SNMP options on the Network Interfaces/Protocols window. For more information on SNMP, see "Simple network management protocol" on page 29.

9. If you select the **E-mail over PPP** or **SNMP over PPP** notification methods, type the password that accompanies the login ID in the **PPP Password** field.

   Enter the password needed to login to the internet service provider (ISP). You must fill in this field for the **E-mail over PPP** and **SNMP over PPP** notification methods.

10. If you select the **E-mail over LAN** or **E-mail over PPP** notification methods, type the recipient's e-mail address in the **E-mail Address** field.

    Note: For the **E-mail over LAN** and **E-mail over PPP** notification methods to work properly, configure the SMTP options on the Network Interfaces/Protocols window.

11. Press F3 twice to return to the Login & Alert Profiles window.

12. Complete the "Setting remote alert attempts" procedure.

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 the **Login & Alert Profiles** option.

2. Select the **Remote Alert Settings** option from the Login & Alert Profiles window.

   Use these settings to define the number of remote alert attempts and the time between the attempts.

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

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

5. Select **Yes** or **No** in the **Include event log with email alerts?** field.

You can attach detailed information to alert recipients who are set up to receive e-mail as their notification method. The event log provides a summary of the most recent event and assists with problem identification and fast recovery.
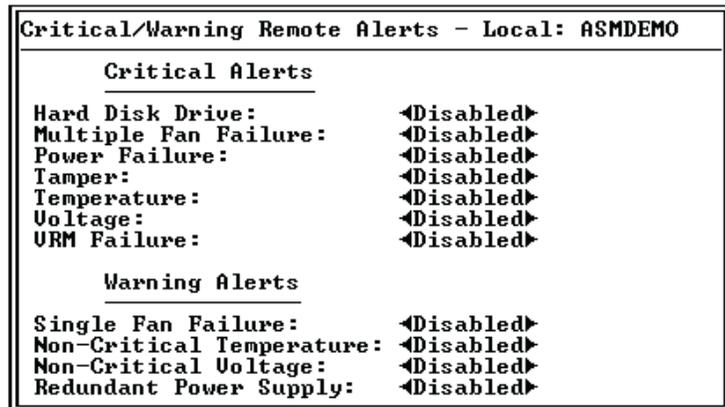
Notes:

a. To send the event log as an e-mail attachment, you must select **E-mail over LAN** or **E-mail over PPP** as the notification method for at least one remote alert recipient.

b. Event logs attached to an e-mail are not forwarded to a Remote Supervisor Adapter on the ASM interconnect network.

6. Press F3 to return to the Login & Alert Profiles window.

7. Complete the "Setting remote alerts" procedure.

Setting remote alerts

Complete the following steps to select which remote alerts are to be sent by the Remote Supervisor Adapter:

1. Select the **Login & Alert Profiles** option.

2. Select the **Critical/Warning Remote Alerts** option in the Login & Alert Profiles window.

```
Critical/Warning Remote Alerts - Local: ASMDEMO

        Critical Alerts
        ─────────────

Hard Disk Drive:            ◄Disabled►
Multiple Fan Failure:       ◄Disabled►
Power Failure:              ◄Disabled►
Tamper:                     ◄Disabled►
Temperature:                ◄Disabled►
Voltage:                    ◄Disabled►
VRM Failure:                ◄Disabled►

        Warning Alerts
        ─────────────

Single Fan Failure:         ◄Disabled►
Non-Critical Temperature:   ◄Disabled►
Non-Critical Voltage:       ◄Disabled►
Redundant Power Supply:     ◄Disabled►
```

The remote alerts are categorized by the following levels of severity:

- Critical
- Warning

All alerts are tracked in the event log and sent to all configured remote alert recipients.

Critical alerts are generated for events that signal that the server is no longer functioning.

Table 18. Critical remote alerts

Event	Action
Hard disk drive	Generates an alert if one or more of the hard disk drives in the server fails.
Multiple fan failure	Generates an alert if two or more of the cooling fans in the server fail.
Power failure	Generates an alert if any of the server power supplies fail.

Table 18. Critical remote alerts

Event	Action
Tamper	Generates an alert if physical intrusion of the server enclosure is detected. Tamper monitoring is not available on some servers, in which case this setting is ignored.
Temperature	Generates an alert if any of the monitored temperatures is outside critical threshold values. These threshold values can be found by selecting the temperature readings on the System Health page. If a critical temperature condition is detected, the server will automatically shut down and turn off whether this field is selected or not.
Voltage	Generates an alert if the voltages of any of the monitored power supplies falls outside their specified operational ranges. These operational ranges are found by selecting the voltage readings on the System Health page. If a critical voltage condition is detected, the server will automatically shut down and turn off whether this field is selected or not.
VRM failure	Generates an alert if one or more VRMs fail. VRMs are not used on some servers, in which case this setting is ignored.

Warning alerts are generated for events that might progress to a critical/error level.

Table 19. Warning remote alerts

Event	Action
Single fan failure	Generates an alert if one fan fails.
Non-critical temperature	Generates an alert if any of the monitored temperatures is outside the warning threshold values. These temperature threshold values can be accessed by selecting the temperature readings on the System Health page. Unlike the critical temperature event, this event will not initiate an automatic system shutdown.
Non-critical voltage	Generates an alert if any monitored voltages is outside the warning threshold values. These voltage range values can be accessed by selecting the voltage readings on the System Health page. Unlike the critical voltage event, this event will not initiate an automatic system shutdown.
Redundant power supply	Generates an alert if a redundant power supply fails.

Note: Hard disk drive Predictive Failure Analysis® (PFA) alerts are not monitored.

3. Press F3 and select the **System Remote Alerts** option.

System alerts
System alerts are generated for events that occur as a result of system errors.

Table 20. System remote alerts

Event	Action
Boot failure	Generates an alert if an error occurred that prevented the server from starting.

Table 20. System remote alerts

Event	Action
Loader timeout	Generates an alert if the system loader timeout value is enabled and has been exceeded. The system loader timeout value is configured in the Server Timeouts section on the System page.
O/S timeout	Generates an alert if the operating system timeout value is enabled and has been exceeded. The operating system timeout value is configured in the Server Timeouts section on the System page. This alert must be checked for remote blue screen capture.
POST timeout	Generates an alert if the POST timeout value is enabled and has been exceeded. The POST timeout value is configured in the Server Timeouts section on the System page.
PFA	Generates an alert if a PFA notification is generated by the system hardware. This feature is available only on systems that have PFA-enabled hardware. This setting is ignored by systems without PFA-enabled hardware.
Power on	Generates an alert if the system is turned on.
Power off	Generates an alert if the system is turned off.

4. Press F3 and select the **Events For Local Notification** option.
5. Select the events to store in the event log. The Remote Supervisor Adapter stores the notification only in the event log.

   Eventually, local events will be sent to the server where the Remote Supervisor Adapter resides. These events will not be sent to remote alert recipients.

Table 21. Local events

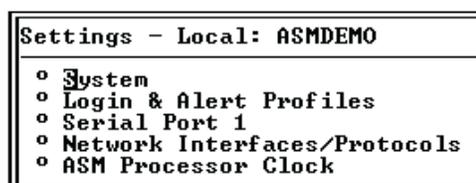| Event	Action
Temperature	Generates a local notification if any of the monitored temperatures exceeds threshold.
Voltage	Generates a local notification if any of the monitored voltages exceeds their threshold.
Redundant power supply	Generates a local notification if the redundant power supply fails.
Power off	Generates a local notification if the server is turned off.
Remote login	Generates a local notification if a remote login occurs.
System tamper	Generates a local notification if the server covers are removed. This feature is only available on certain servers.
Event log 75% full	Generates a local notification if the event log reaches 75% of capacity.
Event log full	Generates a local notification if the event log fills. When the event log fills, the oldest events are deleted.
Fan failure	Generates a local notification if one or more cooling fans fails.
Power supply failure	Generates a local notification if a power supply failure is detected.
DASD failure	Generates a local notification if any hard disk drive failure is detected.
PFA	Generates a local notification if any of the hardware in the system generates a PFA.

Configuring the serial port

You can either dedicate the integrated serial port on the Remote Supervisor Adapter to system management or share it with the operating system. If dedicated to system management, the serial port serves only the Remote Supervisor Adapter and is always available for dial-in and dial-out alerting purposes. You will not be able to view the port on the network operating system (NOS) or in any other applications.
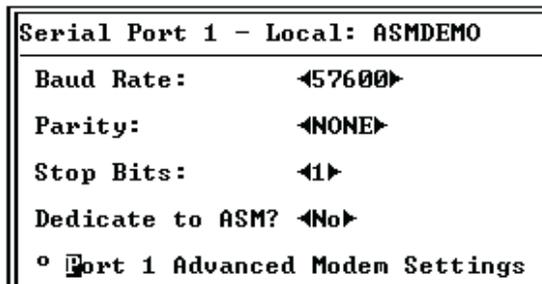
This design enables a single modem to conduct normal functions and also maintain out-of-band alerting capabilities.

Complete the following steps to configure your serial port setup. For more information on your serial port, see 67.

1. Select the **Settings** option in the Advanced System Management window. The Settings window opens:

```
┌─────────────────────────────────────┐
│ Settings - Local: ASMDEMO           │
├─────────────────────────────────────┤
│  ° System                           │
│  ° Login & Alert Profiles           │
│  ° Serial Port 1                    │
│  ° Network Interfaces/Protocols     │
│  ° ASM Processor Clock              │
└─────────────────────────────────────┘
```

2. Select the **Serial Port 1** option in the Settings window.

```
┌─────────────────────────────────────┐
│ Serial Port 1 - Local: ASMDEMO      │
├─────────────────────────────────────┤
│ Baud Rate:        ◄57600►           │
│                                     │
│ Parity:           ◄NONE►            │
│                                     │
│ Stop Bits:        ◄1►               │
│                                     │
│ Dedicate to ASM?  ◄No►              │
│                                     │
│  ° Port 1 Advanced Modem Settings   │
└─────────────────────────────────────┘
```

3. Select the data transfer rate in the **Baud Rate** field.

   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. Select the error detection to be used in your serial connection at the **Parity** field.

   The parity value specifies 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.

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. Select **Yes** in the **Dedicate to ASM** field to reserve the serial port for the Remote Supervisor Adapter.

If shared with the operating system, the serial port serves the Remote Supervisor Adapter only while the server is turned off or on during the power-on self-test (POST). The operating system can access it after the POST completes. Only with a critical event will the Remote Supervisor Adapter take over the port from the NOS to dial-out and transmit an alert. The port then remains under the Remote Supervisor Adapter control until the server is restarted.

Note: If you have configured a PPP interface, dedicate the serial port to the Remote Supervisor Adapter or you will lose the PPP port when the host restarts.

7. 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 22. 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.
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 ^M.
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 dialout 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
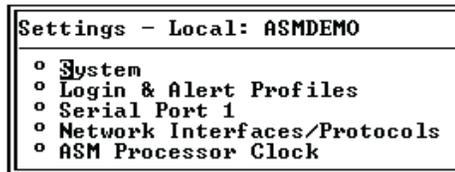- Queued and nondestructive break, no escape state

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

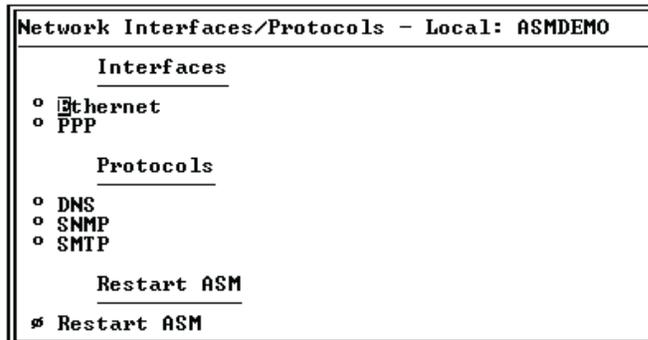|	
AA	auto answer
CD	carrier detect
CTS	clear to send
DT	data transfer
DTR	data terminal ready
LAPM	link access protocol for modems
MNP	microcom networking protocol
RTS	ready to send

Configuring an Ethernet connection to ASM

Complete the following steps to configure your Ethernet setup:

1. Select the **Settings** option in the Advanced System Management window. The Settings window opens:

```
Settings - Local: ASMDEMO

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

2. Select **Network Interfaces/Protocols** in the Settings window. The following window opens:

```
Network Interfaces/Protocols - Local: ASMDEMO

        Interfaces
        ──────────
 ° Ethernet
 ° PPP

        Protocols
        ─────────
 ° DNS
 ° SNMP
 ° SMTP

        Restart ASM
        ───────────
 ø Restart ASM
```

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

```
Ethernet - Local: ASMDEMO

Interface:         ◄Enabled►
DHCP:              ◄Disabled►
Host Name:         [ASMDEMO                                    ]
IP Address:        [9.67.41.147   ]
Gateway Address:   [9.67.41.1     ]
Subnet Mask:       [255.255.255.0 ]

°  Advanced Ethernet Settings
°  Advanced DHCP Information

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

4. Select **Enabled** in the **Interface** field. It is enabled by default.

5. If you want to use a dynamic host configuration protocol (DHCP) server connection, enable the **DHCP** field. Go to step 11.

   Note: If you enable this setting, you must have an accessible, active, and config- ured DHCP server on your network. Also, when DHCP is enabled, the automatic configuration will override any manual settings.

6. Type the IP hostname of the Remote Supervisor Adapter in the **Host Name** field. This step is only necessary if you disabled DHCP.

   You can enter 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 hostname of the Remote Supervisor Adapter (the **Host Name** field) and Remote Supervisor Adapter name (the **ASM Name** field on the Sys- tem page) 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 hostname. The non-qualified IP hostname consists of up to the first period of a fully qualified IP hostname. For exam- ple, the non-qualified IP hostname of `asmcard1.us.company.com` (a fully qualified IP hostname) is `asmcard1`. For more information on your host- name, see "Setting system information" on page 51.

7. Type the IP address of the Remote Supervisor Adapter in the **IP Address** field. This step is only necessary if you disabled DHCP. The IP address must contain:

   • Four integers from 0 to 255 separated by periods

   • No spaces

8. Type your network gateway router in the **Gateway Address** field. This step is only necessary if you disabled DHCP. The gateway address must contain:

   • Four integers from 0 to 255 separated by periods

   • No spaces or consecutive periods

9. Type the subnet mask used by the Remote Supervisor Adapter in the **Subnet Mask** field. This step is only necessary 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 the **Advanced Ethernet Settings** option if you need to set additional Ethernet settings. Make modifications as necessary.

Table 23. 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's capability. 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 <60-1514>	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 - 1514. The default value for this field is 1514.
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 zero and nine. 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. Select the **Advanced DHCP Information** option to view the current configuration. It is enabled by default. A table opens that lists the IP address, gateway address, and subnet mask set by the DHCP server, as well as the server hostname.

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

```
Ethernet - Local: ASMDEMO

Advanced DHCP Information - Local: ASMDEMO

 DHCP Server Assigned Host Name:
 DHCP Server Assigned IP Address:
 DHCP Server Assigned Gateway Address:
 DHCP Server Assigned Subnet Mask:

 Note: The DHCP Server is not available when the DHCP settings
 are empty.
```

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

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. Select the **PPP** option in the Network Interfaces/Protocols window. The PPP window opens:

```
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. Select **Enabled** in the **Interface** field.

3. Enter the local IP address for the PPP interface on this Remote Supervisor Adapter in the Local IP Address field. 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. Enter the remote IP address that this Remote Supervisor Adapter will assign to a remote user in the **Remote IP address** field. 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. Enter the subnet mask that will be used by the Remote Supervisor Adapter in the **Subnet Mask** field. 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 the **Restart ASM** option.

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 hostnames 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. Select the **System** option from the Settings window and enter your system contact and system location information. For more information on the system settings, see "Setting system information" on page 51.

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

2. Select the **Network Interface/Protocols** option from the Settings window.

3. Select the **SNMP** option. 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 hostname (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.

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

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. Select the **DNS** option in the Network Interfaces/Protocols window. 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. Enable the DNS in the **DNS Status** field.

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

11. If DNS is enabled, enter the IP address of the up to three DNS servers in the **DNS Server IP Address** fields. 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. Enter a hostname in the **Host Name** field and its corresponding IP address in the **Host Name IP Address** field. You can define four mappings.

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

Note: The Remote Supervisor Adapter examines this table first for an address to hostname 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 hostname 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. Select the **SMTP** option in the Network Interfaces/Protocols window. The SMTP window opens:

```
SMTP - Local: ASMDEMO

        Simple Mail Transfer Protocol

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

15. Enter the hostname of the SMTP server in the **SMTP Server Host Name or IP Address** field. 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 the **Restart ASM** option.

Setting adapter clock

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

1. Select the **ASM Processor Clock** option, which shows the date and time when this Web page 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.

2. 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.

3. 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.

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.

Remotely controlling the power status of a server

The Remote Supervisor Adapter 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. Select the following options only in case of an emergency, or if you are offsite and the server is nonresponsive:

Power on server immediately
> To turn on this server and start the operating system, select the **Power On Server Immediately** option.

Power off server immediately
> To turn off this server without shutting down the operating system, select the **Power Off Server Immediately** option.

Shutdown O/S and then power off server
> To shut down the operating system and then turn off this server, select the **Shutdown O/S and then Power Off Server** option. This option requires the IBM System Management device driver to be installed on the server, as well as Netfinity Manager with UM Server Extensions for the ASM component.

Shutdown O/S and then restart server
> To restart the operating system, select the **Shutdown O/S and then Restart Server** option. This option requires the IBM System Management device driver to be installed on the server, as well as Netfinity Manager with UM Server Extensions for the ASM component.

Restart the server immediately
> To turn off and then turn on this server immediately without shutting down the operating system first, select the **Restart the Server Immediately** option.

To perform any of these actions, you must have read/write access to the Remote Supervisor Adapter. With the operating system shutdown options, the Remote Supervisor Adapter communicates with the system management software through the device driver and the system management software initiates the shutdown.

Attention: You must have the UM server extensions code installed to enable an orderly operating system shutdown. If you do not have the UM server extensions code installed, the server turn off after waiting for the length of time you set in the **Power Off Delay** field. You could lose or corrupt data on your server. For more information on installing UM server extensions code for the Remote Supervisor Adapter, see your *Remote Supervisor Adapter Installation Guide*.

Accessing remote adapters through ASM interconnect network

You can connect to remote systems through the ASM interconnect network on the Access Remote ASM window. The Remote ASM Access table indicates the overall status of each remote server in the System Health column using color-coded icons. The server name is the name corresponding to each remote system.

Complete the following steps to access remote Remote Supervisor Adapters:

1. Select the **Remote ASM Access** option in the Advanced System Management window. The Remote ASM Access window opens, listing other system management adapters and processors linked to the host server.

```
Remote ASM Access - Local: ASMDEMO

  ° condortest
  ° SIT ILLINOIS
  ° SIT_ASSAULT
```
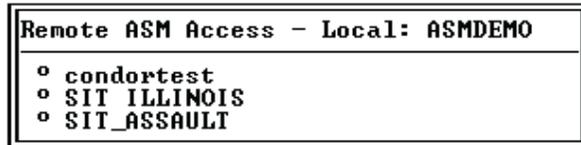
2. Select a processor or adapter. The Remote ASM Login window opens.

3. Enter your username and password.

   Note: It might take up to 45 seconds for newly attached servers to be reflected 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 system management adapter or processor.

   Note: Depending on the adapter on the remote server, some options might not be available.

Viewing remote POST

Complete the following steps to remotely view a server POST. You have complete keyboard access.

1. Access a remote server using the steps in "Accessing remote adapters through ASM interconnect network" on page 71.

2. Press F3 to return to the Advanced System Management window.

3. Select the **Remote Video** option. The Remote Video window opens and the remote server restarts. The text that is displayed during the server POST displays on your screen.

4. Press CTRL R+E+T to return to the Advanced System Management window.

   Note: After you exit, if you return to the server POST by reselecting the Remote Video option, the screen does not refresh. The server POST text will appear within the Remote Video window text.

Restoring ASM to factory defaults

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

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

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.

Restarting ASM

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

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

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.

Logging off

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

1. Select **Log Off** in the Advanced System Management window.
2. Click either the **Yes** or **No** buttons.

Appendix A.   Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. 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. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter 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.

This section contains trademarks and other important information.

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.

Edition Notice

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 MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This publication 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.

This publication was developed for products and services offered in the United States of America and the United Kingdom. It is possible that this publication may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming, or services in your country.

Requests for technical information about IBM products should be made to your IBM reseller or IBM marketing representative. No part of this publication may be reproduced or distributed in any form or by any means without prior permission in writing from the International Business Machines Corporation.

Trademarks

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

IBM

Netfinity

Predictive Failure Analysis

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.

IBM

Part Number: 21P8724
File Number:

21P8724

SC21-P872-40