Chapter 7
Deploying the Remote Management Infrastructure

Prescriptive Architecture Guide

Abstract
This chapter describes the installation and configuration of remote management technologies in the Microsoft® Systems Architecture (MSA) Internet Data Center (IDC) environment, particularly Microsoft® Windows® 2000 Terminal Services and Dell Remote Assistance Card.
EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Trademark Information

EMC2, EMC, and Symmetrix are registered trademarks and EMC Enterprise Storage, The Enterprise Storage Company, The EMC Effect, Connectrix, CLARiiON, EMC ControlCenter, ESN Manager, and EMC Navisphere are trademarks of EMC Corporation.

Microsoft, Windows, Windows NT, Active Directory, ActiveX, JScript, NetMeeting, SQL Server, and Visual Basic are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
INTRODUCTION

Businesses are continuing to depend on technology to provide critical business services, and Information Technology (IT) management is becoming increasingly integral to a company’s success. When investing in business-critical servers, storage or appliances, Dell believes it is vital to use limited human resources effectively by managing numerous systems – even remote systems – from a single point. The Dell OpenManage™ solution is designed to help enhance systems investment, anticipate problems before they occur, track valuable IT assets, and perform other tasks necessary to deliver information to users for the life of the system.

Management of distributed servers from a remote location is often a requirement in today’s business environment. IT administrators need to easily and effectively manage servers in locations that have no administrative IT staff, or servers that are locked away in a secure data center. This includes performing all management operations remotely, including server-down situations. The best remote management solutions must provide access to the servers, regardless of their status, and enable users to perform all operations associated with server management.

The Dell remote management cards (DRAC II and DRSC) are fully featured remote management solutions that meet customer requirements for most classes of Dell servers. The combination of Dell OpenManage IT Assistant and the DRAC II or DRSC provide IT administrators with continuous access to the servers hosting a card, and provide full control of the server hardware and operating system from any client system running a web browser.

Knowing that servers can be managed regardless of their current state gives IT administrators the freedom to deploy their business-critical servers to the most appropriate locations, such as corporate data centers and remote sites. Remote management tools help IT administrators by allowing them to conduct all necessary scheduled maintenance, and emergency work, from their local workstations, regardless of the server location, greatly reducing recovery time.

Design Considerations

During the planning stages, it is important to determine how your organization is going to manage the Microsoft Internet Information Services (IIS) servers in the IIS server farm. Because these servers have an interface to the Internet, they are considered to be more vulnerable to attack. Security best practices stipulate that all unnecessary services be removed from those servers with the highest risk. Because IIS servers in the Internet Data Center environment are easily replaceable, they do not warrant the installation of Terminal Services. If an IIS server becomes unresponsive, it should be pulled from the Web farm and
replaced with another server. If your environment requires that you maintain your IIS servers and they are located off-site or in a data center with limited access, you may want to consider installing Terminal Services and configuring it only for the internal network interface card (NIC).

**System Requirements**
Before you begin installing and configuring the remote management components, you should complete the infrastructure and informational tasks. These tasks assist you in setting standards and will simplify the configuration of the environment.

**Infrastructure Tasks**
You should have a fully-implemented and functioning physical Internet Data Center infrastructure, security plan, and installations of the Microsoft Windows 2000 Advanced Server operating system on every server.

Next, you need to identify which computers will require the installation of the remote management cards, Terminal Services, or both. This decision is largely based on the specific security requirements of your configuration.
INFORMATIONAL
TASKS

You should complete the following tasks before you deploy remote management:

- Identify the support staff who require access to the servers by using Terminal Services. Make sure these support staff have a user account created in the Internet Data Center installation of the Microsoft Active Directory™ directory service.
- Identify a grouping scheme for the administrators who will use Terminal Services to access the Internet Data Center servers and administer the Internet Data Center domain. If your Internet Data Center server administrator(s) will be a different group of administrators than your domain administrators, create a group name for those administrators who will have remote administration rights to the Internet Data Center servers.
- Determine whether it will be necessary to break up the administration of the Internet Data Center servers by server type. If your environment has different administrators for the IIS server farm than for the infrastructure servers or the database server farm, create group names for the different administrators for each server type.
- Identify the support staff who require access to the servers through the remote management cards. You can create user accounts for these support staff when the remote management cards are configured.
- Establish the Domain Name System (DNS) naming standards for the remote-management cards. Define a common naming standard for the remote-management cards so it is easy to remember how to access the board through the browser interface.
- Identify the Transmission Control Protocol/Internet Protocol (TCP/IP) information for each of the remote-management cards during the Dell Remote Assistance Card configuration. This information should include a TCP/IP address, a subnet mask, and a gateway.
- Create a host file on the management console server with entries for the remote-management cards and all the servers as soon as the DNS name and TCP/IP information have been determined.
- Establish a user name and password standard for the administrator account for the remote management cards. Select a single name and common password for all the remote-management cards to provide ease of administration after the environment is up and running. The default user name and password will be changed during the Remote Insight Lights-Out Edition board configuration.
- Install the management console server on the Data and Management Virtual Local Area Network (VLAN). This management server provides a central point for the management consoles required to manage the overall architecture. The configuration of this server is discussed in
the “Management Console Server” section later in this chapter. The following diagram shows where in the base Internet Data Center architecture the management console server (labeled “Tools”) is installed.

![Diagram of Internet Data Center architecture](Image)

**Figure 7.1 Management Console Server**
To enable the administrators to work remotely on the servers that make up the Internet Data Center architecture, the Terminal Services software has to be installed and configured. The following steps detail how this software is installed and configured to work correctly within the Internet Data Center architecture. The following steps will need to be completed on all the servers you want to manage remotely with Terminal Services.

Terminal Services Software Installation
You can deploy Terminal Services in Remote Administration mode in one of the following two ways:

- Select Remote Administration mode in the Windows Component screen during server setup or after installing the server.
- Enable Terminal Services by using an unattended setup file.

Using the Windows Component Screen
You can enable the Terminal Services component during installation, or later, by using the Windows Components wizard.

To deploy Terminal Services in Remote Administration mode by using the Windows Components wizard:

1. In the Control Panel, click Add/Remove Programs.
2. In the left pane, click Add/Remove Windows Components.
   Note If you are using Windows 2000 Advanced Server or Windows 2000 Datacenter Server, click Components.
3. Select the Terminal Services check box.
   Note If there are other servers running Terminal Services in application-server mode, the Terminal Services Licensing service must be selected. It is not required for remote administration mode.
4. Click Details.
5. If the server being configured is the management console server (Tools), ensure that the Client Creator Files check box is selected. However, these files are not required for all other servers being managed by Terminal Services, so ensure that the Client Creator Files check box is cleared.
6. Click OK.
7. Click Next.
8. In the Terminal Services Setup window, make sure the Remote Administration Mode check box is selected.
9. Click Next.
10. Click Finish.
11. Restart the server. You can do this immediately or schedule it during the next maintenance.
Using the Unattended Setup File
You can also enable Terminal Services by using the TSEnable subkey in the components section of the unattended setup file.

You can specify the Terminal Services configuration mode by using the ApplicationServer subkey. You can find this subkey in the TerminalServices section of the unattended file. If you do not specify this, the value is assumed to be 0 (zero). That is, it is assumed to be the remote administration mode.

The ApplicationServer key is referenced if Terminal Services is enabled (TSEnable = ON).

You should disable the installation of the Terminal Services clients for now. To do this, set the key TSClients = OFF.

```
[Components]
TSEnable = ON | OFF
TSClients = ON | OFF

[TerminalServices]
ApplicationServer = 1 | 0
```

Note For more information about setting up Windows 2000 Server by using an unattended setup, refer to Microsoft Windows 2000 Guide to Unattended Setup. You can find this document, Unattended.doc, on the Windows 2000 Server compact disc at \Support\Tools\Deploy.cab.

Terminal Services Configuration
Configuring Terminal Services involves changing permissions and designating access through a single network adapter.

To create a global-domain, remote-administration group:
2. Right-click the User OU folder, select New, Group.
3. Enter the name of the group in the Group Name field.

Note You should determine the group name before you begin the remote management configuration. For more information, see the System Requirements section earlier in this document.

4. Click Global Group in the Group Scope field, if it is not already selected.
5. Click Security in the Group Type field, if it is not already selected.
6. Click OK.
7. Double-click the newly-created group in the Active Directory Users and Computers dialog box.
8. Click the Members tab.
9. Click Add.
10. Select the users who should be given permission to use remote administration to access the Internet Data Center servers.
11. After you add all the users, click OK.
12. Repeat these steps for every new group that needs to be created.

To add the global-domain, remote-administrators group to the server’s local administrator group:
1. On the taskbar of each server in the Internet Data Center environment, select Start, Programs, Administrative Tools, Computer Management.
2. Click System Tools.
3. In the right pane, double-click Local Users and Group, double-click Groups, and then double-click Administrators group.
4. Click Add.
5. In the Select Users or Groups field, click the domain.
6. Double-click the remote administration group created in the previous step to add this group to the local administrators group.
7. Click OK.

Changing the Permissions
When you enable Terminal Services in Remote Administration mode, only members of the administrators group can access the server through Terminal Server. You can change the permission levels to include other users.

To change permission levels:
1. Select the Start, Programs, Administrative Tools, Terminal Server Configurations.
2. Double-click RDP-TCP in the right pane.
3. Click the Permissions tab.
4. In the Name box, click a user or group name.
5. In the Permissions box, select the check boxes for the permissions you want to assign to the user or group selected in the Name box.
6. To add a user or group, click Add.
   Note It is not necessary to add the Remote Admins group here, because they are included in the server’s local administrators group.
7. To remove a user or a group, click the user or group name, and then click Remove.
Designating Access Through a Single Network Adapter
By default, the server is accessible through Terminal Services through all installed network adapters. You should limit Remote Desktop Protocol (RDP) access to the internal network adapter on VLAN 16 on all the IIS server farm servers by using the Terminal Services configuration utility on the **Network Adapter** tab of the **RDP-Tcp Properties** dialog box.
Remote management cards provide the ability to obtain a wide range of management information and control from a remote connection regardless, generally, of the state of the computer’s operating system. Because the Internet Data Center lab used Dell PowerEdge Servers, it also used the Dell Remote Assistance Card to provide the remote management features.

The following information details the steps required to configure the Dell Remote Assistance Card in the servers that make up the Internet Data Center environment.

**Hardware Installation**

**Dell Remote Access for x6xx servers**

New features include:

**Boot Path Analysis**

Boot path analysis allows users to determine failures during the boot sequence. Boot path analysis displays the success or failure of Power-On Self Tests as the server comes up. This aids in identifying the status of the components before the OS is operational. Any errors in the boot path may be the source of why a server might not boot. By identifying the component early and quickly isolating problems, it may be possible to reduce downtime.

**Graphic Console Redirection**

New and even faster graphic console redirection than DRAC II. Also simplifies keyboard functions—such as control-alt-del, making them easier to use.

**Remote Floppy Process**

Remote floppy performance is enhanced by downloading floppy images to the memory on the card. Functions on the diskette are executed in a DOS environment for 32-bit systems and via the Extensible Firmware Interface partition for PowerEdge 7150 64-bit systems.

**Increased User Access**

Improvements in access allow up to 16 users access to the same card at the same time, four of who may be using console redirection. This allows administrators to work together from different locations to isolate problems more quickly.

**Export Logs to Spreadsheets**

Exporting logs to spreadsheets allows users to massage log data, to create their own report formats and to isolate trends quickly.
Dell Remote Access hardware description for x6xx servers
DRAC III is a half-length PCI card requiring one 33MHz, 32-bit PCI slot. It provides 16MB of memory and 12MB FLASH/NVRAM, onboard 10/100 Mb/sec Ethernet, one serial interface, battery, real-time clock, and ESM3 connector. The card may optionally include a PCMCIA modem and AC power adapter.

ERA provides 16MB of memory and 12MB FLASH/NVRAM, onboard 10/100 Mb/sec Ethernet, one serial interface, real-time clock, and runs on system flea power when the server is down. AC adapter and battery are not required.

Dell Remote Access hardware description for x3xx, x4xx, x5xx servers
The DRAC II occupies a single, full-length PCI slot. In addition to the processor, it includes: 16MB memory, FLASH/NVRAM, on-board NIC (10Mb/sec Ethernet), PC CARD interface, PCI controller, battery, real-time clock, and the Embedded Server Management 2 (ESM2) connector.

The software necessary to use the DRAC II is incorporated into the Dell OpenManage IT Assistant that ships with every Dell server.

Remote Floppy Boot -- Key New Feature for DRAC II
Remote Floppy Boot allows users to insert a bootable DOS diskette into the diskette drive of his/her desktop and boot a remote server to that floppy. Operations may then be run from that floppy, including functions like flash BIOS to recover servers with BIOS problems.

For more information about the physical installation of boards, refer to the documentation provided with the board and to:

http://docs.us.dell.com/docs/software/smdrac/ - DRAC II
http://docs.us.dell.com/docs/software/smdrac3/ - DRAC III
Installing Dell Management Software
Follow these steps to install the Dell Management Station software:

1. Insert the Dell Management Software CD into the CDROM drive. The installation will start automatically. Alternatively, you can run setup.exe from a file share.
2. Click on "Install/Upgrade/Uninstall System Management Software.
3. Click Accept on the Dell Software Agreement screen.
4. Click Management Station.
5. Click Custom Setup.
6. Review the Destination Settings for the software. Click Next.
7. Review the Management Station Software Selections. Click Next.
8. Review the Summary. Click Next.
9. Once the install is finished, make sure Yes, Reboot the Server Now is selected, and click Finish.
10. Click OK to reboot the server.

DRAC II Configuration

Adding a DRAC II Administrator
The DRAC II holds information for up to sixteen administrators. The DRAC II provides out-of-band security by requiring an administrator to provide a user name and password prior to establishing a remote connection. The DRAC II also provides paging services to notify administrators if the system crashes, loses power, or experiences a list of other events. In addition, you can enter an optional callback number to force the DRAC II to hang up on a modem connection and call back to the preconfigured number as an extra security measure.

Note The DRAC II does not have a default user name and password. To establish a remote connection using the DRAC II Web Console, you must assign a user name and password. The defaults for the IT Assistant (root and calvin) do not work unless you assign them.

To create a DRAC II administrator:
1. Launch IT Assistant by selecting Start, Dell OpenManage Applications, IT Assistant, IT Assistant.
2. At the Security Warning window, click Yes. 
   Note If the following prompt appears: Do you want to install the required components for Dell OpenManage IT Assistant?, click Yes.
3. At the Security Warning window, click Yes.
4. At the Logon Information window, select **Read/Write** and enter a **Password**. If no password is set up, the default is a blank password.

5. Click **OK**.

6. You are prompted to configure **Discovery**. Click **Yes**.

7. At the **Default Discovery Configuration** window, accept the defaults and click **OK**.

8. At the **Subnet Discovery** window, click **Add**.

9. At **Subnet Type**, click the drop-down arrow and select the appropriate subnet type for your network and enter the appropriate information in the block(s) that follow.
   **Example**: If you select IP Address, enter 120.120.120.2 or the IP address for the node you are trying to configure.

10. Accept the defaults for the remainder of the screen and click **OK**.

11. Click **Close** at the **Subnet Directory** window.

12. Click **Servers**.

13. Double-click the **Host Name** of the system to be configured.

14. Click the **Users** tab.

15. Click **Add**.

16. Log in if the **Login** dialog box displays.
   - The default login for the agent installed on the server with the DRAC II is: **Username**: root **Password**: calvin
   - If you enter your own password during setup of the DRAC II agents, the **calvin** default is overwritten.

17. Click **OK**.

18. Enter a user name in the **Name** field.

19. Enter a new password in the **New Password** field.

20. Enter the new password again.

21. Click the **Configure DRAC User** check box.

22. Enter a telephone number in the **Session Callback Number** field.
   - The session callback number allows the system to receive a call, hang up, and then call the console back at an assigned number. This security feature limits remote access to a single telephone number to ensure that the system only responds to calls from selected consoles. If a callback number is not entered, the system can respond to calls from any console. This feature is only applicable if you are using a modem.
23. Select the type of pager you have from the **Pager Type** drop-down box. If a pager type is selected, DRAC II issues a page to the user if DRAC II generates an event that meets the maximum pager severity level.

**Note** The DRAC II does not page on an event if the system is being *actively managed* through the DRAC II. If any user has a remote session established with the DRAC II during an event, the DRAC II Web Console displays a flashing red icon in the user interface but no page is issued. All remote sessions with the DRAC II must be closed for paging to occur.

24. Enter a service provider telephone number in the **Service Provider** field. The telephone number of the service provider for alphanumeric paging goes here.

- If numeric paging was selected from the **Pager Type** drop-down box, this box should remain blank.
- If the modem line to which the DRAC II connects for paging requires a number to be dialed to connect to an outside line, this number should be separated from the telephone number by a comma.

  **Example:** 9,5551212

25. Enter a pager number in the **Pager Number** field using one of the following methods:

- For *alphanumeric* paging, enter the unique pager number or personal identification number (PIN) required by the service provider to identify your pager. **Example:** 12345.

- For *numeric* paging, enter the pager number. Again, the number dialed to connect to an outside line (if required) should be separated by a comma and four trailing commas should follow the main telephone number. The trailing commas are required to give the paging service time to answer and respond before the customized pager string is sent. Each comma represents approximately one second of delay.

  **Note** If your numeric pager requires a PIN number, an example might be 9,5551212,,,,12345,,,,. Adjusting the actual number of commas may be required based on the individual service provider.

26. Select the severity level from the **Minimum Pager Severity Level** drop-down box.

27. Enter a pager string in the **Customized Pager String** field, if desired. **Example:** Enter 911 for a numeric pager or a system name for an alphanumeric pager.

28. Click **OK**. The name you entered appears in the **Username** box. A telephone icon next to the name indicates remote access privilege.
Configuring the Network Properties of the DRAC II

The DRAC II contains an integrated 10Base-T Ethernet network interface controller (NIC) and supports Transmission Control Protocol/ Internet Protocol (TCP/IP). The NIC has a default address of 10.0.0.1 and a default gateway of 0.0.0.0.

**Note** If the DRAC II is configured to the same IP address as another NIC on the same network, an IP address conflict occurs. The DRAC II stops responding to network commands until the IP address is changed on the DRAC II. The DRAC II must be changed even if the IP address conflict is resolved by changing the other network interface card.

Changing the IP address of the DRAC II causes the DRAC II to reset. If simple network management protocol (SNMP) polls the DRAC II before the card initializes, a temperature warning is logged because the correct temperature is not transmitted until the card is initialized.

To configure the network properties of the DRAC II:
1. Select **Configuration** from the IT Assistant menu.
2. Select **Remote Access Hardware** from the submenu.
3. Click the **Host Name** of the system housing the DRAC II to be configured.
4. Click the **Network** tab.
5. Enter the required information in the **IP Address**, **Subnet Address** and **Default Gateway** fields of the DRAC II (not the system).
6. Click **Save**.
   **Note** To save the IP address to the DRAC II, you must first reset the DRAC II. If SNMP polls the DRAC II before the card is initialized, a temperature warning is issued. The correct temperature is not transmitted until the card completes the reset.
7. Click **Yes**. It takes a few minutes for the DRAC II to reinitialize.

Configuring the Modem Properties of the DRAC II

Configuring the DRAC II modem properties is an optional feature; however, a modem is required.

To configure the modem properties of the DRAC II:
1. Select **Configuration** from the IT Assistant menu.
2. Select **Remote Access Hardware** from the submenu.
3. Click the **Host Name** of the system housing the DRAC II to be configured.
4. Click the **Modem** tab.
5. Select **Pulse** or **Tone** in the **Dial Mode** field.
6. Enter an initialization string in the **Initialization String** field. If you want to use the DRAC II default string, then leave this field empty.
7. Select a **baud rate** from the **Baud Rate** menu.

8. Click **Save**.
   
   **Note** To save the modem properties to the DRAC II, you must first reset the DRAC II. If SNMP polls the DRAC II before the card is initialized, a temperature warning is issued. The correct temperature is not transmitted until the card completes the reset.

9. Click **Yes**. It takes a few minutes for the DRAC II to reinitialize.

### Configuring the Alert Properties of the DRAC II

The DRAC II can be configured to respond to alert conditions from the system’s embedded server management (ESM) hardware or to other conditions such as operating system crashes or power failures. In addition to paging, the DRAC II can send an SNMP trap to preconfigured destinations. The DRAC II can also dial-out to a remote system and transfer the event information.

**Note** The DRAC II does not alert on an event if the system is being actively managed through the DRAC II. If any user has a remote session established with the DRAC II during an event, the DRAC II Web Console displays a flashing red icon in the user interface but no alerts are issued. All remote sessions with the DRAC II must be closed for alerting to occur.

To configure the alert properties of the DRAC II:

1. Select **Configuration, Remote Access Hardware** from the **IT Assistant** menu.
2. Click the **Host Name** of the system housing the DRAC II to be configured.
3. Click the **Alerts** tab.
4. Enter an IP address in the **Destination IP Address** field of a management station if you want the DRAC II to send SNMP traps to a management station when an event occurs.
5. Enter the name in the **Community Name** field to which to send the trap.
6. Enter the number of a management station in the **Dial-Out Number** field if you want the DRAC II to call a management station and transfer event information.

   If the modem line to which the DRAC II connects for paging requires a number to be dialed to connect to an outside line, separate this number from the telephone number by a comma.

   **Example**: 9,5551212

7. Click **Add**.
Configuring Your Network to Access the DRAC II From the Internet
To access the DRAC II through the Internet, you must first set up a PowerEdge system to act as an address book server (middle-tier management station).

Requirements for Management Stations to Access DRAC II From the Internet
To access DRAC II from the Internet, management stations must have the following components installed:

- Windows 2000 operating system
- HTTP server (Microsoft Internet Information Services (IIS) or equivalent)
- Microsoft Internet Explorer 4.0 or later (Netscape not currently supported)
- Two network interface controllers (NICs) or one NIC and a modem

Notes
If you plan to use a modem to connect to DRAC II on the managed node, the management station must have the Remote Access Server (RAS) — both Routing and RAS for Windows 2000 — installed with dialup networking properly configured. For Internet connections, the DRAC II client connects to the DRAC II command server located on the management station. If the management station is behind a firewall, open the following ports: 6001 (used by the client to communicate with the DRAC II), 6003 (used by the client to communicate with the address book service), and 6005 (used for the dialup connection).

For Intranet and virtual private network (VPN) connections where no http server is used, the DRAC II client does not go through the DRAC II command server to connect to the DRAC II or address book service. If the management station is behind a firewall, open the following ports: 5001 (used by the client to communicate with the DRAC II), 5003 (used by the client to communicate with the address book service), and 5005 (used for the dialup connection).

Setting Up a System as an Address Book System
To set up a system as an address book system:

1. Connect one NIC to the Internet and the other to the LAN for the managed nodes. or  
   Connect the NIC to the Internet and the modem to an analog telephone line.
2. Using the Dell OpenManage Systems Management CD, install Remote Management from the Management Station Applications menu.
3. Restart the system.
4. Launch the DRAC II Web Console by selecting **Start**, **Programs**, **Dell OpenManage Applications**, **Dell Remote Assistant**, **DRAC II Web Console**.
5. Click **New Session** to open the address book.
6. In the **Favorite Management Stations** box, double-click the (LOCAL) management station icon.
7. Click **Add** in the address book.
8. Enter the **Server Name** and **IP Address** of the managed node (or the modem number of the DRAC II) and click **OK**. Enter address book information for all the managed nodes on the LAN.
9. Open a **cmd** window and ping all the IP addresses in the address book to verify that each is receiving messages. If the ping request times-out, verify that your DRAC II network connections and IP addresses are correct.
10. From the DRAC II Web Console, double-click a server name in the address book.
11. Enter the **User Name** and **Password** to verify that you are able to connect to the DRAC II.
12. When four selections appear in the left side of the console window, the connection has been made successfully. Verify each node.
13. Close the **DRAC II Web Console**.

**Configuring a Desktop, Laptop, or PowerEdge System as the DRAC II Web Console**

**Note**  The DRAC II Web Console feature is not supported on Windows 9x.

To set up a system to act as the DRAC II Web Console:

1. Connect the NIC to the Internet, or the modem to an analog telephone line.
2. Using the Dell OpenManage Systems Management CD, install **Remote Management** from the **Management Station Applications** menu.
3. Restart the system.
4. Connect to your Internet service provider (ISP).
5. Launch the **DRAC II Web Console** by selecting **Start**, **Programs**, **Dell OpenManage Applications**, **Dell Remote Assistant**, **DRAC II Web Console**.
6. Click **New Session** to open the address book.
7. Click **Add New Station** in the **Favorite Management Station** dialog box.
8. In the Add New Management Station dialog box, enter http:// and the IP address or system name of the address book server established in the previous section.

9. Click OK. A globe icon with the URL for the address book server appears.

10. Double-click the globe icon. The address book you established in the previous section appears in the Address Book dialog.

11. Double-click the server name of the managed node you want to remotely manage.

12. Enter the requested information in the User Name and Password fields.

13. Click OK. You should now be able to connect to the DRAC II and remotely manage the managed node.

**DRAC III Configuration**

DRAC III cards were used in most of the servers in the Microsoft System Architecture Internet Data Center Environment and come preinstalled in these servers. DRAC card IP addresses are configured by entering the DRAC III Setup program during server boot.

To configure the DRAC III cards:

1. Boot the server machine.

2. While machine is booting, watch for the following message display:
   Dell Remote Access Card III
   Firmware version 1.1
   IP address: 192.168.30.1
   Netmask 255.255.255.0
   Gateway 192.168.30.254
   Press <Ctrl + D> within 5 seconds to enter setup.

3. Press Ctrl+D to enter SETUP once you see the message. This will take you to the Dell Remote Access Card III Setup Network Interface Properties screen. There are only two addresses that can be configured on this screen, Static IP and Gateway.

4. To change the IP address, press the letter <I>. This opens the bottom of the screen. Enter the address and press Enter.

5. To change the Static Gateway, press the letter <G>. Enter the Gateway and press Enter.

6. When all address entries have been completed, press R. A confirmation message will display. Read the message and respond Y to save the changes and reset the card.
Accessing a Server for Remote Management

1. Launch **Internet Explorer** and enter the IP address of the remote network card on the server you want to remotely manage.
   
   **Note** User can update the host file so server name could use instead of IP address. Host file is in C:\\winnt\\system32\\drivers\\etc\\hosts and the instructions for updating are contained within the file.

2. Two Security Warnings will display asking you to confirm installation of **Remote Access Controller User Interface**. Click **Yes** in both dialogs. The Login window will display.

3. Enter the Dell default user name and password in the Login window:
   
   **User Name:** root
   
   **Password:** calvin

4. Two Security Warnings will display asking you to confirm installation of **VNC Viewer** and **JPEG Encoder 1.0**. Click YES in both dialogs.

The Dell Remote Access Card window should now display. For detailed instructions on the functions and features of this screen, refer to your Dell documentation CD for DRAC Remote Management features, or go to the Dell website:

http://docs.us.dell.com/docs/software/smdrac3/ug/index.htm

**Terminal Services Client Installation**

During the installation of Windows 2000 Server, the Terminal Services client installation software is copied to the management-console server. For detailed information, see the “Terminal Services Configuration” section earlier in this document. The management console server is accessed through a VPN connection. You use the Terminal Services client to access the other servers.

**To install the Terminal Services client software on the management console server:**

1. Run the **Setup.exe** file located at C:\\Winnt\\System32\\Clients\\Tsclient\\Win32\\Disks\\Disk1\\.

2. Click **Continue** in the **Welcome to the Terminal Services Client Installation Program** window,

3. In the **Name and Organization** field, enter the appropriate name and organization information, and then click **Next**.

4. Click **OK** to confirm the credentials entered.

5. Review the license information in the **License Agreement** window, and then click **I Agree**.

6. Leave the default location for the Terminal Services client software as it is, and then click the large button to start the installation.
7. The **Terminal Services Client Setup** dialog box prompts you to specify whether you want all Terminal Services users of this computer to have the same initial settings. To install the client software for all users of the computer, click **Yes**.

8. Click **OK** after the installation is complete.

You can access a server through Terminal Services by typing the server’s fully qualified domain name (FQDN) or IP address in the **Server** text box in the Terminal Services client. You can also access a server by selecting the server in the **Available Servers** window of the Terminal Services client.

After establishing a connection to the server, log on to that server with a user account that has administrative privileges on the server.
Remote management tools help IT administrators by allowing them to conduct all necessary scheduled maintenance on servers and any emergency work from their local workstation, thus substantially reducing server down time.

In this chapter, you learned how to use either Terminal Services or a remote management card to perform remote management operations. You also learned to configure Terminal Services by changing the session encryption level, creating a global domain remote administration group, adding the global remote administrators group to the server’s local administrator group, changing permissions, and designing access through a single network adapter. You also learned to install the Terminal Services client, install and configure a remote management card, and access the Dell Remote Assistant Card Web management tool.

**Additional Information**
You can find the latest information about Windows 2000 Server, Terminal Services, and remote administration at:
http://www.microsoft.com/windows2000/server/

You can also find more information in the *Windows 2000 Server Resource Kit*.

You can find the latest information about the Dell Remote Assistant Cards at:
http://www.dell.com/openmanage